Threat Group Cards: A Threat Actor Encyclopedia

Compiled by ThaiCERT, a member of the Electronic Transactions Development Agency

TLP:WHITE

Version 1.0 (12 June 2019)

Contents

Introduction

When analyzing security incidents we always face the question which adversary we are possibly dealing with and what we know about their prior engagements and TTP, to get a better understanding of how to approach and what else to look for.

This document aims to create full profiles of all threat groups worldwide that have been identified with all research generously shared by anti-virus and security research organizations over the years. It can be used as "threat group cards", as the document title suggests, to have everything together in an elaborate profile for each threat group. All dates shown in the cards are the dates when the stated activities started, not necessarily when the reports about them came out.

All information in this document comes from public sources (OSINT). The difficult part of attributing campaigns to actors has been done by those security research organizations as well. What makes this difficult is the fact that there may be some overlap between threat groups, where they share tools or people move between groups, or when groups suddenly change tactics or type of target.

Not all groups have been publicly documented as well as others; most groups have remained rather obscure and, of course, not all individual campaigns resulted in public knowledge – targeted companies usually don't welcome such exposure.

As a National CERT, ThaiCERT has a strictly neutral role and everything collected in this document does in no way signify specific endorsements, placing blame on countries or taking sides.

With that said, compiling this document has been a tremendously interesting journey into the dark world of cybercrime and the groups associated with it.

Note: Users of the MISP can also use the MISP Threat Actor cluster (galaxy) located at
<https://github.com/MISP/misp-galaxy/blob/master/clusters/threat-actor.json>

Approach

In order to obtain an initial set of actors, we perused the public archives from MISP, MITRE and the volunteer overview on Google Docs (resource 1-3 in the APPENDIX: Sources Used).

Generally, those, as well as media reports about threats, tend to lump everything together as aliases or synonyms – be it actual group names as tracked by research organizations, alleged (state) sponsor names, individual campaigns run by the group or specific pieces of malware used by the group. In this report, aliases are only listed as such if we could realistically determine it to be a fact, generally because we found which organization gave it that name. Everything else known about each actor has been split off into the relevant fields (sponsors, operations, tools).

The next step was to search our Risk Intelligence archive and after that, using our favorite Internet search engine for any public news about each and every actor to find all their campaigns and other activities that have been discovered. Analysis of those (thousands of) reports created the total overview of all tools used and where this actor has been observed in terms of countries and sectors.

Lastly, we went over the entire rich archive known as Malpedia to augment the set with malware names that had not appeared in the reports we saw.

In each step we took great care to make sure only Open Source Intelligence appeared in this document.

Legal Notice

This encyclopedia has been developed to catalog all known important adversaries to information security, with the aim to get a better understanding of international threats and to aid in faster response to future incidents. The content is based on the public knowledge of the security community and not solely the view of ThaiCERT and ETDA. It may not necessarily represent state-of-the-art and it might be updated from time to time.

Third party sources are quoted as appropriate. ThaiCERT is not responsible for the content of the external sources, including external websites, nor their continued availability, referenced in this encyclopedia.

Where specific vendors or product names are given, those do not mean endorsement from ThaiCERT, but serve to document history only.

This encyclopedia is intended for educational and information purposes only. Neither ThaiCERT nor any person acting on its behalf is responsible for the use that might be made of the information contained in this encyclopedia. All information contained herein is provided on an "As Is" basis with no warranty whatsoever. ThaiCERT/ETDA does not promise any specific result, effects or outcome from the use of the information herein.

Acknowledgements

---

[1] Creative Commons License: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

Advanced Persistent Threat (APT) Groups

Cybereason provides the following definition of an Advanced Persistent Threat:

An advanced persistent threat is a stealthy cyberattack in which a person or group gains unauthorized access to a network and remains undetected for an extended period. The term's definition was traditionally associated with nation-state sponsorship, but over the last few years we've seen multiple examples of non-nation state groups conducting large-scale targeted intrusions for specific goals.

Apart from all the APT groups profiled in this chapter, there are of course others, but no public information is available about them. Especially CrowdStrike has been very active in researching APT groups and mentioned the following names in passing, in summary reports: Big Panda, Foxy Panda, Hammer Panda, Impersonating Panda, Judgement Panda, Karma Panda, Keyhole Panda, Kryptonite Panda, Maverick Panda, Nomad Panda, Poisonous Panda, Predator Panda, Toxic Panda, Union Panda, Wet Panda, Corsair Jackal and Ghost Jackal.

Anchor Panda, APT 14

Names	Anchor Panda *(CrowdStrike)* APT 14 *(Mandiant)* Aluminium *(Microsoft)* QAZTeam
Country	China
Sponsor	State-sponsored, PLA Navy
Motivation	Information theft and espionage
Description	(CrowdStrike) Anchor Panda is an adversary that CrowdStrike has tracked extensively over the last year targeting both civilian and military maritime operations in the green/brown water regions primarily in the area of operations of the South Sea Fleet of the PLA Navy. In addition to maritime operations in this region, Anchor Panda also heavily targeted western companies in the US, Germany, Sweden, the UK, and Australia, and other countries involved in maritime satellite systems, aerospace companies, and defense contractors. Not surprisingly, embassies and diplomatic missions in the region, foreign intelligence services, and foreign governments with space programs were also targeted.
Observed	Sectors: Aerospace, Defense, Engineering, Government, Industrial and NGOs in the green/brown water regions primarily in the area of operations of the South Sea Fleet of the PLA Navy. Countries: Australia, Germany, Sweden, UK, USA and others.
Tool used	Gh0st RAT, Poison Ivy and Torn RAT.
Information	<https://www.crowdstrike.com/blog/whois-anchor-panda/>

Allanite

Names	Allanite *(Dragos)* Palmetto Fusion *(DHS)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(Dragos) Allanite accesses business and industrial control (ICS) networks, conducts reconnaissance, and gathers intelligence in United States and United Kingdom electric utility sectors. Dragos assesses with moderate confidence that Allanite operators continue to maintain ICS network access to: (1) understand the operational environment necessary to develop disruptive capabilities, (2) have ready access from which to disrupt electric utilities. Allanite uses email phishing campaigns and compromised websites called watering holes to steal credentials and gain access to target networks, including collecting and distributing screenshots of industrial control systems. Allanite operations limit themselves to information gathering and have not demonstrated any disruptive or damaging capabilities. Allanite conducts malware-less operations primarily leveraging legitimate and available tools in the Windows operating system.
Observed	Sectors: Energy. Countries: UK and USA.
Tools used	Inveigh, Powershell scripts, PSExec, SecreetsDump and THC Hydra.
Information	<https://dragos.com/resource/allanite/>

APT 3, Gothic Panda, Buckeye

Names	APT 3 *(Mandiant)* Gothic Panda *(CrowdStrike)* Buckeye *(Symantec)* TG-0110 *(SecureWorks)* UPS Team *(Symantec)* Group 6 *(Talos)*
Country	China
Sponsor	State-sponsored, Ministry of State Security and Internet security firm Guangzhou Bo Yu Information Technology Company Limited ("Boyusec").
Motivation	Information theft and espionage
Description	(Recorded Future) APT3 (also known as UPS, Gothic Panda, and TG-011) is a sophisticated threat group that has been active since at least 2010. APT3 utilizes a broad range of tools and techniques including spear-phishing attacks, zero-day exploits, and numerous unique and publicly available remote access tools (RAT). Victims of APT3 intrusions include companies in the defense, telecommunications, transportation, and advanced technology sectors — as well as government departments and bureaus in Hong Kong, the U.S., and several other countries.
Observed	Sectors: Aerospace, Construction, Defense, High-Tech, Manufacturing, Technology, Telecommunications and Transportation. Countries: Belgium, Hong Kong, Italy, Luxembourg, Philippines, Sweden, UK, USA and Vietnam.
Tools used	APT3 Keylogger, Bemstour, CookieCutter, DoublePulsar, EternalBlue, HTran, Hupigon, Kaba, LaZagne, OSInfo, Pirpi, PlugX, shareip, SHOTPUT, TTCalc, w32times and several 0-days for IE, Firefox and Flash.
Operations performed	2007	Hupigon and Pirpi Backdoors <https://www.fireeye.com/blog/threat-research/2010/11/ie-0-day-hupigon-joins-the-party.html>
	Apr 2014	Operation "Clandestine Fox" FireEye Research Labs identified a new Internet Explorer (IE) zero-day exploit used in targeted attacks. The vulnerability affects IE6 through IE11, but the attack is targeting IE9 through IE11. This zero-day bypasses both ASLR and DEP. Microsoft has assigned CVE-2014-1776 to the vulnerability and released security advisory to track this issue. <https://www.fireeye.com/blog/threat-research/2014/04/new-zero-day-exploit-targeting-internet-explorer-versions-9-through-11-identified-in-targeted-attacks.html>
	Jun 2014	Operation "Clandestine Fox", Part Deux While Microsoft quickly released a patch to help close the door on future compromises, we have now observed the threat actors behind "Operation Clandestine Fox" shifting their point of attack and using a new vector to target their victims: social networking. <https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html>
	Nov 2014	Operation "Double Tap"

		This actor initiated their most recent campaign on November 19, 2014 targeting multiple organizations. The attacker leveraged multiple exploits, targeting both CVE-2014-6332 and CVE-2014-4113. <https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html>
	Jun 2015	Operation "Clandestine Wolf" In the last several weeks, APT3 actors launched a large-scale phishing campaign against organizations in the following industries: Aerospace and Defense, Construction and Engineering, High Tech, Telecommunications and Transportation. <https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html>
	Mar 2016	Variant of the DoublePulsar Backdoor Beginning in March 2016, Buckeye began using a variant of DoublePulsar (Backdoor.Doublepulsar), a backdoor that was subsequently released by the Shadow Brokers in 2017. DoublePulsar was delivered to victims using a custom exploit tool (Trojan.Bemstour) that was specifically designed to install DoublePulsar. <https://www.symantec.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit>
Counter operations	• DOJ reveals indictment against Chinese cyber spies that stole U.S. business secrets (2017) <https://www.cyberscoop.com/boyusec-china-doj-indictment/> • U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage (2017) <https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations>	
Information	<https://www.recordedfuture.com/chinese-mss-behind-apt3/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0022/>	

APT 5

Names	APT 5 *(FireEye)*
Country	China
Motivation	Information theft and espionage
Description	(FireEye) We have observed one APT group, which we call APT5, particularly focused on telecommunications and technology companies. More than half of the organizations we have observed being targeted or breached by APT5 operate in these sectors. Several times, APT5 has targeted organizations and personnel based in Southeast Asia. APT5 has been active since at least 2007. It appears to be a large threat group that consists of several subgroups, often with distinct tactics and infrastructure. APT5 has targeted or breached organizations across multiple industries, but its focus appears to be on telecommunications and technology companies, especially information about satellite communications. APT5 targeted the network of an electronics firm that sells products for both industrial and military applications. The group subsequently stole communications related to the firm's business relationship with a national military, including inventories and memoranda about specific products they provided. In one case in late 2014, APT5 breached the network of an international telecommunications company. The group used malware with keylogging capabilities to monitor the computer of an executive who manages the company's relationships with other telecommunications companies
Observed	Sectors: Defense, High-Tech, Industrial, Technology and Telecommunications. Countries: Southeast Asia.
Tools used	LEOUNCIA.
Information	<https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-southeast-asia-threat-landscape.pdf>

APT 6

Names	APT 6 *(FireEye)* 1.php Group *(Zscaler)*
Country	China
Motivation	Information theft and espionage
Description	(Kaspersky) The FBI issued a rare bulletin admitting that a group named Advanced Persistent Threat 6 (APT6) hacked into US government computer systems as far back as 2011 and for years stole sensitive data. The FBI alert was issued in February and went largely unnoticed. Nearly a month later, security experts are now shining a bright light on the alert and the mysterious group behind the attack. "This is a rare alert and a little late, but one that is welcomed by all security vendors as it offers a chance to mitigate their customers and also collaborate further in what appears to be an ongoing FBI investigation," said Deepen Desai, director of security research at the security firm Zscaler in an email to Threatpost. Details regarding the actual attack and what government systems were infected are scant. Government officials said they knew the initial attack occurred in 2011, but are unaware of who specifically is behind the attacks. "Given the nature of malware payload involved and the duration of this compromise being unnoticed – the scope of lateral movement inside the compromised network is very high possibly exposing all the critical systems," Deepen said.
Observed	Sectors: Government. Countries: USA.
Tools used	Poison Ivy.
Information	<https://threatpost.com/fbi-quietly-admits-to-multi-year-apt-attack-sensitive-data-stolen/117267/>

APT 12, Numbered Panda

Names	APT 12 *(Mandiant)* Numbered Panda *(CrowdStrike)* TG-2754 *(SecureWorks)* BeeBus *(FireEye)* Calc Team *(Symantec)* Group 22 *(Talos)* Crimson Iron *(ThreatConnect)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	(CrowdStrike) Numbered Panda has a long list of high-profile victims and is known by a number of names including: DYNCALC, IXESHE, JOY RAT, APT-12, etc. Numbered Panda has targeted a variety of victims including but not limited to media outlets, high-tech companies, and multiple governments. Numbered Panda has targeted organizations in time-sensitive operations such as the Fukushima Reactor Incident of 2011, likely filling intelligence gaps in the ground cleanup/mitigation operations. Screen saver files, which are binary executables and PDF documents, are common Numbered Panda weaponization tactics. One of the most interesting techniques that Numbered Panda likes to use is to dynamically calculate the Command and Control (C2) port by resolving a DNS. This effectively helps Numbered Panda bypass egress filtering implemented to prevent unauthorized communications on some enterprises. The malware will typically use two DNS names for communication: one is used for command and control; the other is used with an algorithm to calculate the port to communicate to.
Observed	Sectors: Defense, Electronics, Government, High-Tech, Telecommunications and journalists. Countries: East Asia (mostly Japan and Taiwan).
Tools used	AUMLIB, DynCalc/DNSCalc, ETUMBOT, HIGHTIDE, IXESHE, RapidStealer, RIPTIDE, THREEBYTE and WaterSpout.
Operations performed	Jul 2009	"IXESHE" campaign Target: East Asian governments, Taiwanese electronics manufacturers and a telecommunications company. <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf>
	May 2011	"AUMLIB" campaign <https://www.fireeye.com/blog/threat-research/2013/08/survival-of-the-fittest-new-york-times-attackers-evolve-quickly.html>
	2011	"ETUMBOT" campaign Target: Taiwan Once the malicious file was downloaded and extracted by the victim, Etumbot uses a right-to-left override exploit to trick the victim to download the malware installer. According to Arbor Security, the "technique is a simple way for malware writers to disguise names of malicious files. A hidden Unicode character in the filename will reverse the order of the characters that follow it, so that a .scr binary file appears to be a .xls document, for example."

		<https://www.arbornetworks.com/blog/asert/wp-content/uploads/2014/06/ASERT-Threat-Intelligence-Brief-2014-07-Illuminating-Etumbot-APT.pdf>
	Oct 2012	Breach of The New York Times "For the last four months, Chinese hackers have persistently attacked The New York Times, infiltrating its computer systems and getting passwords for its reporters and other employees." The attack occurred after the New York Times published a story about how the relatives of Wen Jiabao, the sixth Premier of the State Council of the People's Republic of China, "accumulated a fortune worth several billion dollars through business dealings." The computers used to launch the attack are believed to be the same university computers used by the Chinese military to attack United States military contractors. <https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all>
	Oct 2012	"RIPTIDE" campaign Spear-phishing on Taiwanese Government
	Aug 2014	"HIGHTIDE" campaign Spear-phishing on Taiwanese Government Uses an updated version of ETUMBOT.
	Aug 2014	"THREEBYTE" campaign Spear-phishing on Taiwanese Government
	Aug 2014	"WATERSPOUT" campaign Spear-phishing on Taiwanese Government
	Nov 2016	"CNACOM" campaign On November 7, we spotted a malicious injection on the registration page of a major Taiwanese public service website. An iframe was injected into the footer of the page, which then loaded a unique landing page containing the CVE-2016-0189 exploit code. <https://www.zscaler.com/blogs/research/cnacom-open-source-exploitation-strategic-web-compromise>
Information		<https://www.crowdstrike.com/blog/whois-numbered-panda/> <https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html> <https://en.wikipedia.org/wiki/Numbered_Panda>
MITRE ATT&CK		<https://attack.mitre.org/groups/G0005/>

APT 16, SVCMONDR

Names	APT 16 *(Mandiant)* SVCMONDR *(Kaspersky)*
Country	China
Motivation	Information theft and espionage
Description	(FireEye) Between November 26, 2015, and December 1, 2015, known and suspected China-based APT groups launched several spear-phishing attacks targeting Japanese and Taiwanese organizations in the high-tech, government services, media and financial services industries. Each campaign delivered a malicious Microsoft Word document exploiting the aforementioned EPS *dict* copy use-after-free vulnerability, and the local Windows privilege escalation vulnerability CVE-2015-1701. The successful exploitation of both vulnerabilities led to the delivery of either a downloader that we refer to as IRONHALO, or a backdoor that we refer to as ELMER.
Observed	Sectors: Financial, Government, High-Tech and Media. Countries: Japan, Taiwan and Thailand.
Tools used	ELMER, IRONHALO and SVCMONDR.
Information	<https://securelist.com/cve-2015-2545-overview-of-current-threats/74828/> <https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0023/>

APT 17, Deputy Dog

Names	APT 17 *(Mandiant)* Tailgater Team *(Symantec)* Dogfish *(iDefense)* Deputy Dog *(iDefense)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	APT 17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations. This group appears to be closely associated with Hidden Lynx, Aurora Panda.
Observed	Sectors: Defense, Government, IT, Mining, NGOs and lawyers. Countries: Belgium, China, Germany, Indonesia, Italy, Japan, Netherlands, Switzerland, Russia, UK and USA.
Tools used	9002 RAT, BLACKCOFFEE, DeputyDog, HiKit, PlugX and several 0-days for IE.
Operations performed	Jul 2012	Breach of Bit9 Bit9, a company that provides software and network security services to the U.S. government and at least 30 Fortune 100 firms, has suffered an electronic compromise that cuts to the core of its business: helping clients distinguish known "safe" files from computer viruses and other malicious software. <https://krebsonsecurity.com/tag/bit9-breach/>
	Aug 2013	Operation "DeputyDog" Target: Organizations in Japan Method: Campaign leveraging the then recently announced zero-day CVE-2013-3893. <https://www.fireeye.com/blog/threat-research/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html>
	Nov 2013	Operation "Ephemeral Hydra" Method: Inserting a zero-day exploit into a strategically important website, known to draw visitors that are likely interested in national and international security policy. <https://www.fireeye.com/blog/threat-research/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html>
	Aug 2017	Operation "RAT Cook" Method: Spear-phishing attack using a *Game of Thrones* lure. <https://www.proofpoint.com/us/threat-insight/post/operation-rat-cook-chinese-apt-actors-use-fake-game-thrones-leaks-lures>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0025/>

APT 18, Dynamite Panda, Wekby

Names	APT 18 *(Mandiant)* Dynamite Panda *(CrowdStrike)* TG-0416 *(SecureWorks)* Wekby *(Palo Alto)* Scandium *(Microsoft)*
Country	China
Sponsor	State-sponsored, PLA Navy
Motivation	Information theft and espionage
Description	Wekby was described by Palo Alto Networks in a 2015 report as: 'Wekby is a group that has been active for a number of years, targeting various industries such as healthcare, telecommunications, aerospace, defense, and high tech. The group is known to leverage recently released exploits very shortly after those exploits are available, such as in the case of Hacking Team's Flash zero – day exploit.' This threat group has been seen since 2009.
Observed	Sectors: Aerospace, Biotechnology, Construction, Defense, Education, Engineering, Healthcare, High-Tech, Telecommunications and Transportation. Countries: USA.
Tools used	Gh0st RAT, hcdLoader, HTTPBrowser, Pisloader, Roseam, StickyFingers and 0-day exploits for Flash.
Operations performed	Apr 2014	Community Health Systems data breach <https://threatpost.com/apt-gang-branches-out-to-medical-espionage-in-community-health-breach/107828/> <https://www.venafi.com/blog/infographic-how-an-attack-by-a-cyber-espionage-operator-bypassed-security-controls>
	Jun 2015	Attacks using DNS Requests as Command and Control Mechanism Method: Phishing with obfuscated variants of the HTTPBrowser tool. <https://www.anomali.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop> <https://www.fireeye.com/blog/threat-research/2015/07/demonstrating_hustle.html>
	May 2016	Attacks using DNS Requests as Command and Control Mechanism Target: Organizations in the USA. Method: Phishing with Pisloader dropper. <https://unit42.paloaltonetworks.com/unit42-new-wekby-attacks-use-dns-requests-as-command-and-control-mechanism/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0026/>

APT 19, C0d0so

Names	APT 19 *(Mandiant)* Codoso *(CrowdStrike)* Sunshop Group *(FireEye)*
Country	China
Sponsor	A group likely composed of freelancers, with some degree of sponsorship by the Chinese government. (FireEye)
Motivation	Information theft and espionage
Description	APT 19 is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing campaign was used to target seven law and investment firms. Some analysts track APT19 and DarkHydrus as the same group, but it is unclear from open source information if the groups are the same.
Observed	Sectors: Defense, Education, Energy, Financial, Government, High-Tech, Manufacturing, Pharmaceutical, Telecommunications, Think Tanks, political dissidents and Forbes.
Tools used	C0d0so, Cobalt Strike, Empire, Derusbi and a 0-day for Flash.
Operations performed	Feb 2015	Attack using Forbes.com as Watering Hole Method: Compromise of Forbes.com, in which the site was used to compromise selected targets via a watering hole to a zero-day Adobe Flash exploit. <https://www.darkreading.com/attacks-breaches/chinese-hacking-group-codoso-team-uses-forbescom-as-watering-hole-/d/d-id/1319059>
	Jan 2016	Several Watering Hole Attacks <https://unit42.paloaltonetworks.com/new-attacks-linked-to-c0d0s0-group/>
	May 2017	Phishing campaign targeting at least seven global law and investment firms. Method: In early May, the phishing lures leveraged RTF attachments that exploited the Microsoft Windows vulnerability described in CVE 2017-0199. Toward the end of May, APT19 switched to using macro-enabled Microsoft Excel (XLSM) documents. In the most recent versions, APT19 added an application whitelisting bypass to the XLSM documents. At least one observed phishing lure delivered a Cobalt Strike payload. <https://www.fireeye.com/blog/threat-research/2017/06/phished-at-the-request-of-counsel.html>
	Jun 2017	Attacks on Australian law firms and research body <https://www.abc.net.au/news/2017-12-01/chinese-hackers-targeting-australian-law-firms/9213520>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0073/>

APT 20, Violin Panda

Names	APT 20 *(FireEye)* APT 8 *(Mandiant)* Violin Panda *(Crowdstrike)* TH3Bug *(Palo Alto)*
Country	China
Motivation	Information theft and espionage
Description	(Palo Alto) We've uncovered some new data and likely attribution regarding a series of APT watering hole attacks this past summer. Watering hole attacks are an increasingly popular component of APT campaigns, as many people are more aware of spear phishing and are less likely to open documents or click on links in unsolicited emails. Watering hole attacks offer a much better chance of success because they involve compromising legitimate websites and installing malware intended to compromise website visitors. These are often popular websites frequented by people who work in specific industries or have political sympathies to which the actors want to gain access. In contrast to many other APT campaigns, which tend to rely heavily on spear phishing to gain victims, "th3bug" is known for compromising legitimate websites their intended visitors are likely to frequent. Over the summer they compromised several sites, including a well-known Uyghur website written in that native language.
Observed	Sectors: Chemical, Construction, Defense, Energy, Engineering, Financial, Government, Healthcare, High-Tech, Pharmaceutical, Telecommunications and Transportation. Countries: East Asia, Thailand, USA and Uyghur sympathizers.
Tools used	CAKELOG, CANDYCLOG, CETTRA, COOKIECLOG, PlugX and Poison Ivy.
Information	<https://unit42.paloaltonetworks.com/recent-watering-hole-attacks-attributed-apt-group-th3bug-using-poison-ivy/>

APT 29, Cozy Bear, The Dukes

Names	APT 29 *(Mandiant)* Cozy Bear *(CrowdStrike)* The Dukes *(F-Secure)* Group 100 *(Talos)* Yttrium *(Microsoft)* Iron Hemlock *(SecureWorks)* Minidionis *(Palo Alto)* CloudLook *(Kaspersky)* Grizzly Steppe *(US Government)* together with Sofacy, APT 28, Fancy Bear, Sednit
Country	Russia
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	(F-Secure) The Dukes are a well-resourced, highly dedicated and organized cyberespionage group that we believe has been working for the Russian Federation since at least 2008 to collect intelligence in support of foreign and security policy decision-making. The Dukes primarily target Western governments and related organizations, such as government ministries and agencies, political think tanks, and governmental subcontractors. Their targets have also included the governments of members of the Commonwealth of Independent States; Asian, African, and Middle Eastern governments; organizations associated with Chechen extremism; and Russian speakers engaged in the illicit trade of controlled substances and drugs. The Dukes are known to employ a vast arsenal of malware toolsets, which we identify as MiniDuke, CosmicDuke, OnionDuke, CozyDuke, CloudDuke, SeaDuke, HammerDuke, PinchDuke, and GeminiDuke. In recent years, the Dukes have engaged in apparently biannual large-scale spear-phishing campaigns against hundreds or even thousands of recipients associated with governmental institutions and affiliated organizations. These campaigns utilize a smash-and-grab approach involving a fast but noisy break-in followed by the rapid collection and exfiltration of as much data as possible. If the compromised target is discovered to be of value, the Dukes will quickly switch the toolset used and move to using stealthier tactics focused on persistent compromise and long-term intelligence gathering. In addition to these large-scale campaigns, the Dukes continuously and concurrently engage in smaller, much more targeted campaigns, utilizing different toolsets. These targeted campaigns have been going on for at least 7 years. The targets and timing of these campaigns appear to align with the known foreign and security policy interests of the Russian Federation at those times.
Observed	Sectors: Defense, Energy, Government, Imagery, Law Enforcement, Media, NGOs, Pharmaceutical, Telecommunications, Think Tanks and Transportation. Countries: Australia, Azerbaijan, Belarus, Belgium, Brazil, Bulgaria, China, Cyprus, Czech, France, Georgia, Germany, Hungary, India, Ireland, Israel, Japan, Kazakhstan, Kyrgyzstan, Latvia, Lebanon, Lithuania, Luxembourg, Mexico, Montenegro, Netherlands, New Zealand, Portugal, Romania, Russia, Slovenia, Spain, South Korea, Turkey, Uganda, Ukraine, USA, Uzbekistan and NATO.

Tools used	ATI-Agent, CloudDuke, Cobalt Strike, CosmicDuke, CozyDuke, CozyCar, GeminiDuke, HammerDuke, HAMMERTOSS, meek, Mimikatz, MiniDuke, OnionDuke, PinchDuke, POSHSPY, PowerDuke, SeaDaddy, SeaDuke and tDiscoverer.	
Operations performed	Feb 2013	Since the original announcement, we have observed several new attacks using the same exploit (CVE-2013-0640) which drop other malware. Between these, we've observed a couple of incidents which are so unusual in many ways that we-ve decided to analyse them in depth. <https://securelist.com/the-miniduke-mystery-pdf-0-day-government-spy-assembler-0x29a-micro-backdoor/31112/>
	2013	While the old style Miniduke implants were used to target mostly government victims, the new style CosmicDuke implants have a somehow different typology of victims. The most unusual is the targeting of individuals that appear to be involved in the traffic and reselling of controlled and illegal substances, such as steroids and hormones. These victims in the NITRO project have been observed only in Russia. <https://securelist.com/miniduke-is-back-nemesis-gemina-and-the-botgen-studio/64107/>
	Mar 2014	Operation "Office monkeys" In March 2014, a Washington, D.C.-based private research institute was found to have CozyDuke (Trojan.Cozer) on their network. Cozy Bear then started an email campaign attempting to lure victims into clicking on a flash video of office monkeys that would also include malicious executables. By July the group had compromised government networks and directed CozyDuke-infected systems to install MiniDuke onto a compromised network. <https://www.symantec.com/connect/blogs/forkmeiamfamous-seaduke-latest-weapon-duke-armory>
	Aug 2015	Attack on the Pentagon in the USA In August 2015 Cozy Bear was linked to a spear-phishing cyberattack against the Pentagon email system causing the shutdown of the entire Joint Staff unclassified email system and Internet access during the investigation. <https://www.cnbc.com/2015/08/06/russia-hacks-pentagon-computers-nbc-citing-sources.html>
	Jun 2016	Breach of Democratic National Committee In June 2016, Cozy Bear was implicated alongside the hacker group Sofacy, APT 28, Fancy Bear, Sednit had only been there a few weeks. Cozy Bear's more sophisticated tradecraft and interest in traditional long-term espionage suggest that the group originates from a separate Russian intelligence agency. <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>
	Aug 2016	Attacks on US think tanks and NGOs After the United States presidential election, 2016, Cozy Bear was linked to a series of coordinated and well-planned spear-phishing campaigns against U.S.-based think tanks and non-governmental organizations (NGOs).

		<https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/>
	Jan 2017	Attacks on the Norwegian Government On February 3, 2017, the Norwegian Police Security Service (PST) reported that attempts had been made to spear-phish the email accounts of nine individuals in the Ministry of Defense, Ministry of Foreign Affairs, and the Labour Party. The acts were attributed to Cozy Bear, whose targets included the Norwegian Radiation Protection Authority, PST section chief Arne Christian Haugstøyl, and an unnamed college. <https://www.usatoday.com/story/news/2017/02/03/norway-russian-hackers-hit-spy-agency-defense-labour-party/97441782/>
	Feb 2017	Attack on Dutch ministries In February 2017, the General Intelligence and Security Service (AIVD) of the Netherlands revealed that Fancy Bear and Cozy Bear had made several attempts to hack into Dutch ministries, including the Ministry of General Affairs, over the previous six months. Rob Bertholee, head of the AIVD, said on EenVandaag that the hackers were Russian and had tried to gain access to secret government documents. <https://www.volkskrant.nl/cultuur-media/russen-faalden-bij-hackpogingen-ambtenaren-op-nederlandse-ministeries~b77ff391/>
	Nov 2018	Phishing campaign in the USA Target: Multiple industries, including think tank, law enforcement, media, U.S. military, imagery, transportation, pharmaceutical, national government, and defense contracting. Method: Phishing email appearing to be from the U.S. Department of State with links to zip files containing malicious Windows shortcuts that delivered Cobalt Strike Beacon. <https://www.fireeye.com/blog/threat-research/2018/11/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign.html>
Counter operations	• Dutch agencies provide crucial intel about Russia's interference in US-elections (2014) <https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/> • Mueller indicts 12 Russians for DNC hacking as Trump-Putin summit looms (2018) <https://www.politico.com/story/2018/07/13/mueller-indicts-12-russians-for-hacking-into-dnc-718805>	
Information	<https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf> <https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf> <https://en.wikipedia.org/wiki/Cozy_Bear>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0016/>	

APT 30, Override Panda

Names	APT 30 *(Mandiant)* Override Panda *(CrowdStrik)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	APT 30 is a threat group suspected to be associated with the Chinese government. While Naikon shares some characteristics with APT 30, the two groups do not appear to be exact matches. (FireEye) When our Singapore-based FireEye labs team examined malware aimed predominantly at entities in Southeast Asia and India, we suspected that we were peering into a regionally focused cyber espionage operation. The malware revealed a decade-long operation focused on targets—government and commercial—who hold key political, economic, and military information about the region. This group, who we call APT30, stands out not only for their sustained activity and regional focus, but also for their continued success despite maintaining relatively consistent tools, tactics, and infrastructure since at least 2005. Based on our knowledge of APT30's targeting activity and tools, their objective appears to be data theft as opposed to financial gain. APT30 has not been observed to target victims or data that can be readily monetized (for example, credit card data, personally identifiable information, or bank transfer credentials). Instead, their tools include functionality that allows them to identify and steal documents, including what appears to be an interest in documents that may be stored on air-gapped networks. The group expresses a distinct interest in organizations and governments associated with ASEAN, particularly so around the time of official ASEAN meetings. Many of APT30's decoy documents use topics related to Southeast Asia, India, border areas, and broader security and diplomatic issues. Decoy documents attached to spear phishing emails are frequently indicators of intended targeting because threat actors generally tailor these emails to entice their intended targets —who typically work on related issues—to click on the attachments and infect themselves. In addition to APT30's Southeast Asia and India focus, we've observed APT30 target journalists reporting on issues traditionally considered to be focal points for the Chinese Communist Party's sense of legitimacy, such as corruption, the economy, and human rights. In China, the Communist Party has the ultimate authority over the government. China-based threat groups have targeted journalists before; we believe they often do so to get a better understanding on developing stories to anticipate unfavorable coverage and better position themselves to shape public messaging.
Observed	Sectors: Defense, Government and ASEAN.

	Countries: Bhutan, Brunei, Cambodia, India, Indonesia, Japan, Laos, Malaysia, Myanmar, Nepal, Philippines, Saudi Arabia, Singapore, South Korea, Thailand, Vietnam and USA.
Tool used	BACKBEND, BACKSPACE, CREAMSICLE, FLASHFLOOD, GEMCUTTER, MILKMAID, NETEAGLE, ORANGEADE, SHIPSHAPE and SPACESHIP.
Information	<https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0013/>

APT 32, OceanLotus, SeaLotus

Names	APT 32 *(Mandiant)* OceanLotus *(SkyEye Labs)* SeaLotus APT-C-00 *(360)* Ocean Buffalo *(CrowdStrike)*
Country	Vietnam
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	([FireEye](#)) Since at least 2014, FireEye has observed APT32 targeting foreign corporations with a vested interest in Vietnam's manufacturing, consumer products, and hospitality sectors. Furthermore, there are indications that APT32 actors are targeting peripheral network security and technology infrastructure corporations. In addition to focused targeting of the private sector with ties to Vietnam, APT32 has also targeted foreign governments, as well as Vietnamese dissidents and journalists since at least 2013.
Observed	Sectors: Government, Hospitality, Manufacturing, Retail, dissidents, journalists and ASEAN. Countries: Australia, Brunei, Cambodia, China, Germany, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, USA and Vietnam.
Tool used	CACTUSTORCH, Cobalt Strike, Cuegoe, Denis, fingerprintjs2, Goopy, KerrDown, KOMPROGO, Mimikatz, Nishang, OSX_OCEANLOTUS.D, PHOREAL, PowerSploit, Salgorea, SOUNDBITE, Terracotta VPN, WINDSHIELD and 0-day exploits in MS Office.
Operations performed	Aug 2015	Terracotta VPN Dubbed by RSA as "Terracotta VPN" (a reference to the Chinese Terracotta Army), this satellite array of VPN services "may represent the first exposure of a PRC-based VPN operation that maliciously, efficiently and rapidly enlists vulnerable servers around the world," the company said in a report released today. <https://krebsonsecurity.com/2015/08/chinese-vpn-service-as-attack-platform/>
	Mar 2017	Breach of the ASEAN website Steven Adair, founder and CEO, said the hacking group was still active, and had compromised the website of the Association of South East Asian Nations (ASEAN) over several high-profile summit meetings. ASEAN is holding another summit of regional leaders in the Philippines capital Manila this week. <https://www.reuters.com/article/us-cyber-attack-vietnam/vietnams-neighbors-asean-targeted-by-hackers-report-idUSKBN1D70VU>
	May 2017	Operation "Cobalt Kitty" Dubbed Operation Cobalt Kitty, the APT targeted a global corporation based in Asia with the goal of stealing proprietary business information. The threat actor targeted the company's top-level management by using spear-phishing attacks as the initial penetration vector, ultimately compromising the computers of vice presidents,

		senior directors and other key personnel in the operational departments. During Operation Cobalt Kitty, the attackers compromised more than 40 PCs and servers, including the domain controller, file servers, Web application server and database server. <https://www.cybereason.com/blog/operation-cobalt-kitty-apt>
	May 2017	Mass Digital Surveillance and Attacks Targeting ASEAN, Asian Nations, the Media, Human Rights Groups, and Civil Society In May 2017, Volexity identified and started tracking a very sophisticated and extremely widespread mass digital surveillance and attack campaign targeting several Asian nations, the ASEAN organization, and hundreds of individuals and organizations tied to media, human rights and civil society causes. These attacks are being conducted through numerous strategically compromised websites and have occurred over several high-profile ASEAN summits. <https://www.volexity.com/blog/2017/11/06/oceanlotus-blossoms-mass-digital-surveillance-and-exploitation-of-asean-nations-the-media-human-rights-and-civil-society/>
	Early 2018	KerrDown downloader We identified two methods to deliver the KerrDown downloader to targets. One is using the Microsoft Office Document with a malicious macro and the other is RAR archive which contains a legitimate program with DLL side-loading. For RAR archive files, the file names used to trick targets are all in Vietnamese as shown in Figure 11. Our analysis shows that the primary targets of the ongoing campaign discussed in this blog are either in Vietnam or Vietnamese speaking individuals. <https://unit42.paloaltonetworks.com/tracking-oceanlotus-new-downloader-kerrdown/>
	Mar 2018	OceanLotus ships new backdoor using old tricks <https://www.welivesecurity.com/2018/03/13/oceanlotus-ships-new-backdoor/>
	Apr 2018	New MacOS Backdoor The MacOS backdoor was found in a malicious Word document presumably distributed via email. The document bears the filename "2018-PHIẾU GHI DANH THAM DỰ TĨNH HỘI HMDC 2018.doc," which translates to "2018-REGISTRATION FORM OF HMDC ASSEMBLY 2018.doc." The document claims to be a registration form for an event with HDMC, an organization in Vietnam that advertises national independence and democracy. <https://blog.trendmicro.com/trendlabs-security-intelligence/new-macos-backdoor-linked-to-oceanlotus-found/>
	Apr 2018	Steganography to Shroud Payloads The OceanLotus APT is using two new loaders which use steganography to read their encrypted payloads. <https://threatpost.com/oceanlotus-apt-uses-steganography-to-shroud-payloads/143373/>
	May 2018	Watering Hole Attack using the Phnom Penh Post website The attack started just days after Australian mining magnate Bill Clough sold the newspaper to Malaysian spin doctor Sivakumar Ganapathy, who specializes in "covert PR".

		"Since last Tuesday [May 8], computers in our office were targeted by a malicious piece of code when we visited the Phnom Penh Post website," said Naly Pilorge, director of Licadho — one of Cambodia's leading human rights groups. <https://www.abc.net.au/news/2018-05-15/hackers-trigger-software-trap-after-phnom-penh-post-sale/9763906>
	Mid-2018	Equation Editor exploit In mid-2018, OceanLotus carried out a campaign using documents abusing the weakness exposed by the CVE-2017-11882 vulnerability. Indeed, several Proofs-of-Concept were made available. The vulnerability resides in the component responsible for rendering and editing mathematical equations. <https://www.welivesecurity.com/2019/03/20/fake-or-fake-keeping-up-with-oceanlotus-decoys/>
	Sep 2018	Watering Hole Attack in Southeast Asia ESET researchers have discovered a new watering hole campaign targeting several websites in Southeast Asia, and that is believed to have been active since September 2018. This campaign stands out because of its large scale, as we were able to identify 21 compromised websites, some of which are particularly notable. Among the compromised websites were the Ministry of Defense of Cambodia, the Ministry of Foreign Affairs and International Cooperation of Cambodia and several Vietnamese newspaper or blog websites. <https://www.welivesecurity.com/2018/11/20/oceanlotus-new-watering-hole-attack-southeast-asia/>
	Jan 2019	Self-Extracting archives After using RTF files, the group started using self-extracting (SFX) archives that use common document icons in an attempt to further mislead their victims. It was briefly documented by Threatbook (in Chinese). When run, these self-extracting RAR files drop and execute DLL files (with a .ocx extension) with the final payload being the previously documented {A96B020F-0000-466F-A96D-A91BBF8EAC96}.dll. Since the middle of January 2019, OceanLotus began reusing the technique but changed some configuration over time.
	Mar 2019	macOS malware update Early in March 2019, a new macOS malware sample from the OceanLotus group was uploaded to VirusTotal, a popular online multi-scanner service. This backdoor executable bears the same features as the previous macOS variant we looked at, but its structure has changed and its detection was made harder. Unfortunately, we couldn't find the dropper associated with this sample so we do not know the initial compromise vector. <https://www.welivesecurity.com/2019/04/09/oceanlotus-macos-malware-update/>
	Mar 2019	Malicious macro armed documents likely targeting ASEAN affairs and meeting members. Telemetry and spreading statistics related to these decoy documents highlight their diffusion in the geographical area of Thailand.

		<https://brica.de/alerts/alert/public/1258637/oceanlotus-on-asean-affairs/>
	Mar 2019	Breach of Toyota in Australia, Japan, Thailand and Vietnam Toyota said the servers that hackers accessed stored sales information on up to 3.1 million customers. The carmaker said there's an ongoing investigation to find out if hackers exfiltrated any of the data they had access to. <https://www.zdnet.com/article/toyota-announces-second-security-breach-in-the-last-five-weeks/>
	May 2019	Attacks to Indochinese Peninsula In this report, we share our summary of the latest attack techniques, attack payloads and related attacks of the OceanLotus, hoping that we can jointly improve understanding of OceanLotus group, an extremely active APT group. <https://ti.qianxin.com/blog/articles/oceanlotus-attacks-to-indochinese-peninsula-evolution-of-targets-techniques-and-procedure/>
Information		<https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html> <https://www.welivesecurity.com/wp-content/uploads/2018/03/ESET_OceanLotus.pdf> <https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/SpyRATsofOceanLotusMalwareWhitePaper.pdf> <https://www.riskiq.com/blog/analyst/oceanlotus/> <https://github.com/eset/malware-research/tree/master/oceanlotus>
MITRE ATT&CK		<https://attack.mitre.org/groups/G0050/>

APT 33, Elfin

Names	APT 33 *(Mandiant)* Elfin *(Symantec)* Magnallium *(Dragos)*
Country	Iran
Sponsor	State-sponsored
Motivation	Information theft, espionage and sabotage
Description	(FireEye) When discussing suspected Middle Eastern hacker groups with destructive capabilities, many automatically think of the suspected Iranian group that previously used SHAMOON – aka Disttrack – to target organizations in the Persian Gulf. However, over the past few years, we have been tracking a separate, less widely known suspected Iranian group with potential destructive capabilities, whom we call APT33. Our analysis reveals that APT33 is a capable group that has carried out cyber espionage operations since at least 2013. We assess APT33 works at the behest of the Iranian government. APT33 has targeted organizations – spanning multiple industries – headquartered in the United States, Saudi Arabia and South Korea. APT33 has shown particular interest in organizations in the aviation sector involved in both military and commercial capacities, as well as organizations in the energy sector with ties to petrochemical production. APT 33 seems to be closely related to OilRig, APT 34, Helix Kitten.
Observed	Sectors: Aviation, Defense, Energy, Petrochemical and others. Countries: Saudi Arabia, South Korea and USA.
Tools used	AutoIt backdoor, DarkComet, DROPSHOT, Empire, LaZagne, Mimikatz, NanoCore RAT, NETWIRE RC, PoshC2, PowerSploit, POWERTON, PupyRAT, QuasarRAT, Remcos, Ruler, Shamoon, SHAPESHIFT and TURNEDUP.
	Mar 2019	Attacks on Multiple Organizations in Saudi Arabia and U.S. The Elfin espionage group (aka APT33) has remained highly active over the past three years, attacking at least 50 organizations in Saudi Arabia, the United States, and a range of other countries. <https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage>
Information	<https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0064/>

Axiom, Group 72

Names	Axiom *(Novetta)*
	Group 72 *(Talos)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	(Talos) Group 72 is a long standing threat actor group involved in Operation SMN, named Axiom by Novetta. The group is sophisticated, well funded, and possesses an established, defined software development methodology. The group targets high profile organizations with high value intellectual property in the manufacturing, industrial, aerospace, defense, media sectors. Geographically, the group almost exclusively targets organizations based in United States, Japan, Taiwan, and Korea. The preferred tactics of the group include watering-hole attacks, spear-phishing, and other web-based tactics.
	The tools and infrastructure used by the attackers are common to a number of other threat actor groups which may indicate some degree of overlap. We have seen similar patterns used in domain registration for malicious domains, and the same tactics used in other threat actor groups leading us to believe that this group may be part of a larger organization that comprises many separate teams, or that different groups share tactics, code and personnel from time to time.
	Though both this group and Winnti Group, Blackfly, Wicked Panda use the malware Winnti, the two groups appear to be distinct based on differences in reporting on the groups' TTPs and targeting.
Observed	Sectors: High profile organizations with high value intellectual property in Aerospace, Defense, Industrial, Manufacturing and Media.
	Countries: Japan, South Korea, Taiwan and USA.
Tools used	Cobalt Strike, DeputyDog, Derusbi, Gh0st RAT, Hikit, HydraQ, PlugX, Poison Ivy, ShadowPad Winnti and ZXShell.
Operations performed	2008-2014	Operation "SMN" Axiom is responsible for directing highly sophisticated cyberespionage against numerous Fortune 500 companies, journalists, environmental groups, pro-democracy groups, software companies, academic institutions and government agencies worldwide for at least the last six years. In our coordinated effort, we performed the first ever-private sponsored interdiction against a sophisticated state sponsored advanced threat group. Our efforts detected and cleaned 43,000 separate installations of Axiom tools, including 180 of their top tier implants. <http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf>
Information	<https://blogs.cisco.com/security/talos/threat-spotlight-group-72>
	<http://www.novetta.com/wp-content/uploads/2015/04/novetta_winntianalysis.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0001/>

Bahamut

Names	Bahamut *(Bellingcat)*
Country	[Middle East]
Motivation	Information theft and espionage
Description	(Bellingcat) Bahamut was first noticed when it targeted a Middle Eastern human rights activist in the first week of January 2017. Later that month, the same tactics and patterns were seen in attempts against an Iranian women's activist – an individual commonly targeted by Iranian actors, such as Charming Kitten, Newscaster, NewsBeef and the Sima campaign documented in our 2016 Black Hat talk. Recurrent patterns in hostnames, registrations, and phishing scripts provided a strong link between the two incidents, and older attempts were found that directly overlapped with these attacks. Over the course of the following months, several more attempts against the same individuals were observed, intended to steal credentials for iCloud and Gmail accounts. Bahamut was also observed engaging in reconnaissance and counter-reconnaissance attempts, intended to harvest IP addresses of emails accounts. One attempt impersonated BBC News Alerts, using timely content related to the diplomatic conflict between Qatar and other Gulf states as bait. This message used external images embedded in the email to track where the lure would be opened.
Observed	Sectors: Political, economic and social. Countries: Egypt, Iran, Palestine, Qatar, Tunisia, Turkey and UAE.
Tools used	Bahamut and DownPaper.
Operations performed	Dec 2016	Beginning in December 2016, unconnected Middle Eastern human rights activists began to receive spear-phishing messages in English and Persian that were not related to any previously-known groups. These attempts differed from other tactics seen by us elsewhere, such as those connected to Iran, with better attention paid to the operation of the campaign. <https://www.bellingcat.com/news/mena/2017/06/12/bahamut-pursuing-cyber-espionage-actor-middle-east/>
	Oct 2017	For three months there was no apparent further activity from the actor. However, in the same week of September a series of spear-phishing attempts once again targeted a set of otherwise unrelated individuals, employing the same tactics as before. Bahamut remains active, and its operations are more extensive than first disclosed. <https://www.bellingcat.com/resources/case-studies/2017/10/27/bahamut-revisited-cyber-espionage-middle-east-south-asia/>
	Jun 2018	Cisco Talos has identified a highly targeted campaign against 13 iPhones which appears to be focused on India. The attacker deployed an open-source mobile device management (MDM) system to control enrolled devices. <https://blog.talosintelligence.com/2018/07/Mobile-Malware-Campaign-uses-Malicious-MDM.html>
	Jul 2018	The Bahamut group was discovered and detailed by Bellingcat, an open-source news website. In this post, the author was discussing

		Android-based malware with some similarities to the iOS malware we identified. That post kickstarted our investigation into any potential overlap between these campaigns and how they are potentially linked. The new MDM platform we identified has similar victimology with Middle Eastern targets, namely Qatar, using a U.K. mobile number issued from LycaMobile. Bahamut targeted similar Qatar-based individuals during their campaign. <https://blog.talosintelligence.com/2018/07/Mobile-Malware-Campaign-uses-Malicious-MDM-Part2.html>

Barium

Names	Barium *(Microsoft)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	([Microsoft](#)) Barium begins its attacks by cultivating relationships with potential victims—particularly those working in Business Development or Human Resources—on various social media platforms. Once Barium has established rapport, they spear-phish the victim using a variety of unsophisticated malware installation vectors, including malicious shortcut (.lnk) files with hidden payloads, compiled HTML help (.chm) files, or Microsoft Office documents containing macros or exploits. Initial intrusion stages feature the Win32/Barlaiy implant—notable for its use of social network profiles, collaborative document editing sites, and blogs for C&C. Later stages of the intrusions rely upon Winnti for persistent access. The majority of victims recorded to date have been in electronic gaming, multimedia, and Internet content industries, although occasional intrusions against technology companies have occurred.
Observed	Sectors: Multimedia, Online video game companies and Technology.
Tools used	Barlaiy, Cobalt Strike, PlugXL and Winnti.
Operations performed	Jul 2017	ShadowPad is one of the largest known supply-chain attacks. Had it not been detected and patched so quickly, it could potentially have targeted hundreds of organizations worldwide. <https://www.kaspersky.com/about/press-releases/2017_shadowpad-how-attackers-hide-backdoor-in-software-used-by-hundreds-of-large-companies-around-the-world>
	Jun 2018	Operation "ShadowHammer" A supply-chain attack dubbed "Operation ShadowHammer" has been uncovered, targeting users of the ASUS Live Update Utility with a backdoor injection. The China-backed BARIUM APT is suspected to be at the helm of the project. According to Kaspersky Lab, the campaign ran from June to at least November 2018 and may have impacted more than a million users worldwide – though the adversaries appear to have been after specific victims in Asia. <https://threatpost.com/asus-pc-backdoors-shadowhammer/143129/>
	Sep 2018	CCleaner supply-chain attack Talos recently observed a case where the download servers used by software vendor to distribute a legitimate software package were leveraged to deliver malware to unsuspecting victims. For a period of time, the legitimate signed version of CCleaner 5.33 being distributed by Avast also contained a multi-stage malware payload that rode on top of the installation of CCleaner. <https://blog.talosintelligence.com/2017/09/avast-distributes-malware.html>
Counter operations	• Microsoft Asks Judge to Take Down Barium Hackers (2017) <https://www.courthousenews.com/wp-content/uploads/2017/11/barium.pdf>

Information	<https://arstechnica.com/information-technology/2018/05/researchers-link-a-decade-of-potent-hacks-to-chinese-intelligence-group/> <https://www.kaspersky.com/about/press-releases/2019_operation-shadowhammer-new-supply-chain-attack> <https://www.microsoft.com/security/blog/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/>

Berserk Bear, Dragonfly 2.0

Names	Berserk Bear *(CrowdStrike)* Dragonfly 2.0 *(Symantec)* Dymalloy *(Dragos)*
Country	Russia
Motivation	Sabotage and destruction
Description	Dragonfly 2.0 is a suspected Russian group that has targeted government entities and multiple U.S. critical infrastructure sectors since at least March 2016. There is debate over the extent of overlap between Dragonfly 2.0 and Energetic Bear, Dragonfly, but there is sufficient evidence to lead to these being tracked as two separate groups.
Observed	Sectors: Energy. Countries: Germany, Switzerland and Turkey and USA.
Tools used	Bitsadmin, Goodor, Impacket, Karagany and Phisherly.
Operations performed	Dec 2015	Symantec has evidence indicating that the Dragonfly 2.0 campaign has been underway since at least December 2015 and has identified a distinct increase in activity in 2017. <https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks>
	May 2017	Attack on nuclear facilities in the US Since May, hackers have been penetrating the computer networks of companies that operate nuclear power stations and other energy facilities, as well as manufacturing plants in the United States and other countries. Among the companies targeted was the Wolf Creek Nuclear Operating Corporation, which runs a nuclear power plant near Burlington, Kan., according to security consultants and an urgent joint report issued by the Department of Homeland Security and the Federal Bureau of Investigation last week. <https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html> <http://fortune.com/2017/09/06/hack-energy-grid-symantec/>
	May 2017	Attacks on critical infrastructure and energy companies around the world Since at least May 2017, Talos has observed attackers targeting critical infrastructure and energy companies around the world, primarily in Europe and the United States. These attacks target both the critical infrastructure providers, and the vendors those providers use to deliver critical services. Attacks on critical infrastructure are not a new concern for security researchers, as adversaries are keen to understand critical infrastructure ICS networks for reasons unknown, but surely nefarious. <https://blog.talosintelligence.com/2017/07/template-injection.html> <https://www.us-cert.gov/ncas/alerts/TA18-074A>
Information	<https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0074/>

Blackgear

Names	Blackgear *(Trend Micro)* Topgear
Country	China
Motivation	Information theft and espionage
Description	(Trend Micro) Blackgear is an espionage campaign which has targeted users in Taiwan for many years. Multiple papers and talks have been released covering this campaign, which used the ELIRKS backdoor when it was first discovered in 2012. It is known for using blogs and microblogging services to hide the location of its actual command-and-control (C&C) servers. This allows an attacker to change the C&C server used quickly by changing the information in these posts. Like most campaigns, Blackgear has evolved over time. Our research indicates that it has started targeting Japanese users. Two things led us to this conclusion: first, the fake documents that are used as part of its infection routines are now in Japanese. Secondly, it is now using blogging sites and microblogging services based in Japan for its C&C activity.
Observed	Countries: Japan, South Korea and Taiwan.
Tools used	Comnie, Elirks and Protux.
Operations performed	Jul 2018	Resurfaces, Abuses Social Media for C&C Communication <https://blog.trendmicro.com/trendlabs-security-intelligence/blackgear-cyberespionage-campaign-resurfaces-abuses-social-media-for-cc-communication/>
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/blackgear-espionage-campaign-evolves-adds-japan-target-list/>

BlackOasis

Names	BlackOasis *(Kaspersky)*
Country	[Middle East]
Motivation	Information theft and espionage
Description	BlackOasis is a Middle Eastern threat group that is believed to be a customer of Gamma Group. The group has shown interest in prominent figures in the United Nations, as well as opposition bloggers, activists, regional news correspondents, and think tanks. A group known by Microsoft as Neodymium is reportedly associated closely with BlackOasis operations, but evidence that the group names are aliases has not been identified.
Observed	Sectors: Media, Think Tanks, activists and the UN. Countries: Afghanistan, Angola, Bahrain, Iran, Iraq, Jordan, Libya, Netherlands, Nigeria, Russia, Saudi Arabia, Tunisia and UK.
Tools used	FinFisher, FinSpy, WingBird and 0-day vulnerabilities in Flash.
Operations performed	Jun 2015	Leveraging data from Kaspersky Security Network, we identified two other similar exploit chains used by BlackOasis in June 2015 which were zero days at the time. Those include CVE-2015-5119 and CVE-2016-0984, which were patched in July 2015 and February 2016 respectively. These exploit chains also delivered FinSpy installation packages. <https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/>
	May 2016	We first became aware of BlackOasis' activities in May 2016, while investigating another Adobe Flash zero day. On May 10, 2016, Adobe warned of a vulnerability (CVE-2016-4117) affecting Flash Player 21.0.0.226 and earlier versions for Windows, Macintosh, Linux, and Chrome OS. The vulnerability was actively being exploited in the wild.
	Sep 2017	FireEye recently detected a malicious Microsoft Office RTF document that leveraged CVE-2017-8759, a SOAP WSDL parser code injection vulnerability. This vulnerability allows a malicious actor to inject arbitrary code during the parsing of SOAP WSDL definition contents. <https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html>
	Oct 2017	On October 10, 2017, Kaspersky Lab's advanced exploit prevention systems identified a new Adobe Flash zero day exploit used in the wild against our customers. The exploit was delivered through a Microsoft Office document and the final payload was the latest version of FinSpy malware. <https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0063/>

BlackTech

Names	BlackTech *(Trend Micro)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(Trend Micro) BlackTech is a cyber espionage group operating against targets in East Asia, particularly Taiwan, and occasionally, Japan and Hong Kong. Based on the mutexes and domain names of some of their C&C servers, BlackTech's campaigns are likely designed to steal their target's technology. Following their activities and evolving tactics and techniques helped us uncover the proverbial red string of fate that connected three seemingly disparate campaigns: PLEAD, Shrouded Crossbow, and of late, Waterbear.
Observed	Sectors: Financial, Government, Healthcare and Technology Countries: Hong Kong, Japan and Taiwan.
Tools used	BIFROST, DRIGO, KIVARS, PLEAD and XBOW.
Operations performed	2010	Operation "Shrouded Crossbow" This campaign, first observed in 2010, is believed to be operated by a well-funded group given how it appeared to have purchased the source code of the BIFROST backdoor, which the operators enhanced and created other tools from. Shrouded Crossbow targeted privatized agencies and government contractors as well as enterprises in the consumer electronics, computer, healthcare, and financial industries. <https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/>
	2012	Operation "PLEAD" PLEAD is an information theft campaign with a penchant for confidential documents. Active since 2012, it has so far targeted Taiwanese government agencies and private organizations.
	2014	Operation "Waterbear" Waterbear has actually been operating for a long time. The campaign's name is based on its malware's capability to equip additional functions remotely.
	Jul 2018	ESET researchers have discovered a new malware campaign misusing stolen digital certificates. We spotted this malware campaign when our systems marked several files as suspicious. Interestingly, the flagged files were digitally signed using a valid D-Link Corporation code-signing certificate. The exact same certificate had been used to sign non-malicious D-Link software; therefore, the certificate was likely stolen. <https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/>
	Apr 2019	At the end of April 2019, ESET researchers utilizing ESET telemetry observed multiple attempts to deploy Plead malware in an unusual way. Specifically, the Plead backdoor was created and executed by a legitimate process named AsusWSPanel.exe. This process belongs to the Windows client for a cloud storage service called ASUS WebStorage.

		<https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/>
Information		<https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/>

Blind Eagle

Names	Blind Eagle *(360)* APT-C-36 *(360)*
Country	[Latin America]
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	(360) Since April 2018, an APT group (Blind Eagle, APT-C-36) suspected coming from South America carried out continuous targeted attacks against Colombian government institutions as well as important corporations in financial sector, petroleum industry, professional manufacturing, etc. Till this moment, 360 Threat Intelligence Center captured 29 bait documents, 62 Trojan samples and multiple related malicious domains in total. Attackers are targeting Windows platform and aiming at government institutions as well as big companies in Colombia.
Observed	Sectors: Financial, Government and large domestic companies and multinational corporation branches. Countries: Colombia.
Tools used	Imminent Monitor RAT.
Information	<https://ti.360.net/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations-en/>

Blue Termite, Cloudy Omega

Names	Blue Termite *(Kaspersky)* Cloudy Omega *(Symantec)*
Country	China
Motivation	Information theft and espionage
Description	(Kaspersky) In October 2014, Kaspersky Lab started to research "Blue Termite", an Advanced Persistent Threat (APT) targeting Japan. The oldest sample we've seen up to now is from November 2013. This is not the first time the country has been a victim of an APT. However, the attack is different in two respects: unlike other APTs, the main focus of Blue Termite is to attack Japanese organizations; and most of their C2s are located in Japan. One of the top targets is the Japan Pension Service, but the list of targeted industries includes government and government agencies, local governments, public interest groups, universities, banks, financial services, energy, communication, heavy industry, chemical, automotive, electrical, news media, information services sector, health care, real estate, food, semiconductor, robotics, construction, insurance, transportation and so on. Unfortunately, the attack is still active and the number of victims has been increasing.
Observed	Sectors: Automotive, Chemical, Construction, Education, Energy, Financial, Food and Agriculture, Government, Healthcare, High-Tech, Industry, IT, Media, Real estate, Telecommunications, Transportation and several others. Countries: Japan.
Tools used	Emdivi and 0-days from the Hacking Team breach.
Information	<https://securelist.com/new-activity-of-the-blue-termite-apt/71876/> <https://www.symantec.com/connect/blogs/operation-cloudyomega-ichitaro-zero-day-and-ongoing-cyberespionage-campaign-targeting-japan>

Bookworm

Names	Bookworm *(Palo Alto)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(Palo Alto) Threat actors have delivered Bookworm as a payload in attacks on targets in Thailand. Readers who are interested in this campaign should start with our first blog that lays out the overall functionality of the malware and introduces its many components. Unit 42 does not have detailed targeting information for all known Bookworm samples, but we are aware of attempted attacks on at least two branches of government in Thailand. We speculate that other attacks delivering Bookworm were also targeting organizations in Thailand based on the contents of the associated decoys documents, as well as several of the dynamic DNS domain names used to host C2 servers that contain the words "Thai" or "Thailand". Analysis of compromised systems seen communicating with Bookworm C2 servers also confirms our speculation on targeting with a majority of systems existing within Thailand.
Observed	Sectors: Government. Countries: Thailand.
Tools used	Bookworm, FFRAT, Poison Ivy, PlugX and Scieron.
Information	<https://unit42.paloaltonetworks.com/attack-campaign-on-the-government-of-thailand-delivers-bookworm-trojan/> <https://unit42.paloaltonetworks.com/bookworm-trojan-a-model-of-modular-architecture/>

Bronze Butler, Tick

Names	Bronze Bulter *(SecureWorks)* Tick *(Symantec)* RedBaldNight *(Trend Micro)*
Country	China
Motivation	Information theft and espionage
Description	(SecureWorks) CTU analysis indicates that Bronze Bulter primarily targets organizations located in Japan. The threat group has sought unauthorized access to networks of organizations associated with critical infrastructure, heavy industry, manufacturing, and international relations. Secureworks analysts have observed Bronze Bulter exfiltrating the following categories of data: • Intellectual property related to technology and development • Product specification • Sensitive business and sales-related information • Network and system configuration files • Email messages and meeting minutes The focus on intellectual property, product details, and corporate information suggests that the group seeks information that they believe might be of value to competing organizations. The diverse targeting suggests that Bronze Bulter may be tasked by multiple teams or organizations with varying priorities.
Observed	Sectors: Critical infrastructure, Defense, Government, Industry, International relations, Manufacturing and Technology. Countries: China, Japan, Russia, Singapore and South Korea.
Tools used	Daserf, Datper, gsecdump, Mimikatz, Minzen, Muirim, Nioupale, rarstar, Windows Credential Editor and xxmm.
Information	<https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses> <https://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/> <https://www.symantec.com/connect/blogs/tick-cyberespionage-group-zeros-japan>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0060/>

Buhtrap

Names	Buhtrap *(Group-IB)*
Country	Russia
Motivation	Financial gain
Description	(Group-IB) Buhtrap has been active since 2014, however their first attacks against financial institutions were only detected in August 2015. Earlier, the group had only focused on targeting banking clients. At the moment, the group is known to target Russian and Ukrainian banks. From August 2015 to February 2016 Buhtrap managed to conduct 13 successful attacks against Russian banks for a total amount of 1.8 billion rubles ($25.7 mln). The number of successful attacks against Ukrainian banks has not been identified. Buhtrap is the first hacker group using a network worm to infect the overall bank infrastructure that significantly increases the difficulty of removing all malicious functions from the network. As a result, banks have to shut down the whole infrastructure which provokes delay in servicing customers and additional losses. Malicious programs intentionally scan for machines with an automated Bank-Customer system of the Central Bank of Russia (further referred to as BCS CBR). We have not identified incidents of attacks involving online money transfer systems, ATM machines or payment gates which are known to be of interest for other criminal groups.
Observed	Sectors: Financial. Countries: Russia and Ukraine.
Tools used	AmmyyRAT, Buhtrap, Niteris EK, NSIS and Ratopak.
Operations performed	2014	On October 20, 2014 we notified Group-IB Bot-Trek Intelligence subscribers about phishing emails which were sent from the info@beeline-mail.ru address with the subject "Invoice No 522375-ФЛОРЛ-14-115" (pic. 1). The beeline-mail.ru domain name was also registered on October 20, 2014. <https://www.group-ib.com/brochures/gib-buhtrap-report.pdf>
	Oct 2015	We noticed in late October that users visiting the Ammyy website to download the free version of its remote administrator software were being served a bundle containing not only the legitimate Remote Desktop Software Ammyy Admin, but also an NSIS (Nullsoft Scriptable Installation Software) installer ultimately intended to install the tools used by the Buhtrap gang to spy on and control their victims' computers. <https://www.welivesecurity.com/2015/11/11/operation-buhtrap-malware-distributed-via-ammyy-com/>
	Dec 2015	In December 2015, employees from several Russian banks were targeted with spoofed emails, a common technique in attack campaigns. The emails were made to look like they were from the Central Bank of Russia and offered employment to their recipients. Instead of being an actual employment offer, the emails were an attempt to deliver Trojan.Ratopak onto the target's computer.

		<https://www.symantec.com/connect/blogs/russian-bank-employees-received-fake-job-offers-targeted-email-attack>
	Sep 2016	Breach of the Russian boxing side allboxing[.]ru <https://www.forcepoint.com/blog/security-labs/highly-evasive-code-injection-awaits-user-interaction-delivering-malware>
	2017	Operation "TwoBee" Buhtrap resurfaced in the beginning of 2017 in the TwoBee campaign, where it served primarily as means of malware delivery. In March of last year, it hit the news (literally), spreading through several compromised major news outlets in whose main pages malicious actors implanted scripts. This scripts executed an exploit for Internet Explorer in visitor's browsers. <https://www.kaspersky.com/blog/financial-trojans-2019/25690/>
Information		<https://www.group-ib.com/brochures/gib-buhtrap-report.pdf> <https://www.welivesecurity.com/2015/04/09/operation-buhtrap/>

Cadelle

Names	Cadelle *(Symantec)*
Country	Iran
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	(Symantec) Symantec telemetry identified Cadelle and Chafer, APT 39 activity dating from as far back as July 2014, however, it's likely that activity began well before this date. Command-and-control (C&C) registrant information points to activity possibly as early as 2011, while executable compilation times suggest early 2012. Their attacks continue to the present day. Symantec estimates that each team is made up of between 5 and 10 people. There is evidence to suggest that the two teams may be connected in some way, though we cannot confirm this. A number of computers experienced both Cadelspy and Remexi infections within a small time window. In one instance, a computer was compromised with Backdoor.Cadelspy just minutes after being infected with Backdoor.Remexi. The Cadelle and Chafer groups also keep the same working hours and focus on similar targets. However, no sharing of C&C infrastructure between the teams has been observed. If Cadelle and Chafer are not directly linked, then they may be separately working for a single entity. Their victim profile may be of interest to a nation state.
Observed	Countries: Germany, Iran, Iraq, Netherlands, Pakistan, Saudi Arabia, Singapore, Sudan, Tajikistan, Thailand, Turkey, UAE, UK and USA.
Tools used	ANTAK and Cadelspy.
Information	<https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets>

Callisto Group

Names	Callisto Group *(F-Secure)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(F-Secure) The most obvious common theme between all known targets of the Callisto Group is an involvement in European foreign and security policy, whether as a military or government official, being employed by a think tank, or working as a journalist . More specifically, many of the known targets have a clear relation to foreign and security policy involving both Eastern Europe and the South Caucasus. This targeting suggests the Callisto Group is interested in intelligence gathering related to foreign and security policy. Furthermore, we are unaware of any targeting in the described attacks that would suggest a financial motive It is worth noting that during our investigation we uncovered links between infrastructure associated with the Callisto Group and infrastructure used to host online stores selling controlled substances. While we don't yet know enough to fully understand the nature of these links, they do suggest the existence of connections between the Callisto Group and criminal actors. While the targeting would suggest that the main benefactor of the Callisto Group's activity is a nation state with specific interest in the Eastern Europe and South Caucasus regions, the link to infrastructure used for the sale of controlled substances hints at the involvement of a criminal element. Finally, the infrastructure associated with the Callisto Group and related infrastructure contain links to at least Russia, Ukraine, and China in both the content hosted on the infrastructure, and in WHOIS information associated with the infrastructure. It is possible to come up with a number of plausible theories to explain the above findings. For example, a cybercrime group with ties to a nation state, such as acting on behalf of or for the benefit of a government agency, is one potential explanation. However, we do not believe it is possible to make any definitive assertions regarding the nature or affiliation of the Callisto Group based on the currently available information.
Observed	Sectors: Defense, Government, Think Tanks and journalists. Countries: Europe and the South Caucasus.
Tools used	RCS Callisto.
Information	<https://www.f-secure.com/documents/996508/1030745/callisto-group>

Carbanak, Anunak

Names	Carbanak *(Kaspersky)* Anunak *(Group-IB)* Carbon Spider *(CrowdStrike)*
Country	Ukraine
Motivation	Financial gain
Description	Carbanak is a threat group that mainly targets banks. It also refers to malware of the same name (Carbanak). It is sometimes referred to as FIN7, but these appear to be two groups using the same Carbanak malware and are therefore tracked separately. (Kaspersky) From late 2013 onwards, several banks and financial institutions have been attacked by an unknown group of cybercriminals. In all these attacks, a similar modus operandi was used. According to victims and the law enforcement agencies (LEAs) involved in the investigation, this could result in cumulative losses of up to 1 billion USD. The attacks are still active. This report provides a technical analysis of these attacks. The motivation for the attackers, who are making use of techniques commonly seen in Advanced Persistent Threats (APTs), appears to be financial gain as opposed to espionage. An analysis of the campaign has revealed that the initial infections were achieved using spear phishing emails that appeared to be legitimate banking communications, with Microsoft Word 97 – 2003 (.doc) and Control Panel Applet (.CPL) files attached. We believe that the attackers also redirected to exploit kits website traffic that related to financial activity.
Observed	Sectors: Financial. Countries: Australia, Austria, Brazil, Bulgaria, Canada, China, Czech, France, Germany, Hong Kong, Iceland, India, Luxemburg, Morocco, Nepal, Norway, Pakistan, Poland, Russia, Spain, Sweden, Switzerland, Taiwan, UK, Ukraine, USA and Uzbekistan.
Tools used	Agent ORM, AmmyyRAT, ANTAK, Ave Maria, BABYMETAL, Backdoor Batel, Bateleur, BELLHOP, MBR Eraser, Cain & Abel, Carbanak, Cobalt Strike, DNSMessenger, DNSRat, DRIFTPIN, Griffon, HALFBAKED, JS Flash, KLRD, Mimikatz, MBR Eraser, Netscan, Odinaff, POWERPIPE, POWERSOURCE, PSExec, Sekur, SocksBot, SoftPerfect Network Scanner, SQLRat, Team Viewer, TinyMet and VB Flash.
Counter operations	• Mastermind behind EUR 1 billion cyber bank robbery arrested in Spain (2018) <https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain> • Three Carbanak cyber heist gang members arrested (2018) <https://www.computerweekly.com/news/252446153/Three-Carbanak-cyber-heist-gang-members-arrested>
Information	<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf> <https://www.group-ib.com/resources/threat-research/Anunak_APT_against_financial_institutions.pdf> <https://www.bitdefender.com/files/News/CaseStudies/study/262/Bitdefender-WhitePaper-An-APT-Blueprint-Gaining-New-Visibility-into-Financial-Threats-interactive.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0008/>

Careto, The Mask

Names	Careto *(Kaspersky)* The Mask *(Kaspersky)* Mask *(Kaspersky)* Ugly Face *(Kaspersky)*
Country	Spain
Motivation	Information theft and espionage
Description	(Kaspersky) The Mask is an advanced threat actor that has been involved in cyber-espionage operations since at least 2007. The name "Mask" comes from the Spanish slang word "Careto" ("Ugly Face" or "Mask") which the authors included in some of the malware modules. More than 380 unique victims in 31 countries have been observed to date. What makes "The Mask" special is the complexity of the toolset used by the attackers. This includes an extremely sophisticated malware, a rootkit, a bootkit, 32-and 64-bit Windows versions, Mac OS X and Linux versions and possibly versions for Android and iPad/iPhone (Apple iOS).
Observed	Sectors: Diplomatic missions, Education, Energy and Government. Countries: Brazil, France, Germany, Iran, Libya, Morocco, Poland, South Africa, Spain, Switzerland, Tunisia, UK, USA and Venezuela.
Tools used	Careto.
Information	<https://d2538mqrb7brka.cloudfront.net/wp-content/uploads/sites/43/2018/03/20133638/unveilingthemask_v1.0.pdf> <https://securelist.com/the-caretomask-apt-frequently-asked-questions/58254/>

Chafer, APT 39

Names	Chafer *(Symantec)* APT 39 *(Mandiant)*
Country	Iran
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	(FireEye) APT39 was created to bring together previous activities and methods used by this actor, and its activities largely align with a group publicly referred to as "Chafer." However, there are differences in what has been publicly reported due to the variances in how organizations track activity. APT39 primarily leverages the SEAWEED and CACHEMONEY backdoors along with a specific variant of the POWBAT backdoor. While APT39's targeting scope is global, its activities are concentrated in the Middle East. APT39 has prioritized the telecommunications sector, with additional targeting of the travel industry and IT firms that support it and the high-tech industry. APT39's focus on the telecommunications and travel industries suggests intent to perform monitoring, tracking, or surveillance operations against specific individuals, collect proprietary or customer data for commercial or operational purposes that serve strategic requirements related to national priorities, or create additional accesses and vectors to facilitate future campaigns. Government entities targeting suggests a potential secondary intent to collect geopolitical data that may benefit nation-state decision making. Targeting data supports the belief that APT39's key mission is to track or monitor targets of interest, collect personal information, including travel itineraries, and gather customer data from telecommunications firms.
Observed	Sectors: Airlines, Airports, Engineering, Government, High-Tech, IT, Shipping and Logistics, Telecommunications and Transportation. Countries: Israel, Jordan, Middle East, Saudi Arabia, Spain, Turkey, UAE and USA.
Tools used	ASPXSpy, CACHEMONEY, EternalBlue, HTTPTunnel, MechaFlounder Mimikatz, NBTScan, Non-sucking Service Manager (NSSM), Plink, POWBAT, Pwdump, Remcom, Remexi, SEAWEED, SMB hacking tools, UltraVNC and Windows Credential Editor.
Operations performed	2017	Chafer appears to have been undeterred by its exposure in 2015 and continued to be very active during 2017, using seven new tools, rolling out new infrastructure, and attacking nine new target organizations in the region. The group hit organizations in Israel, Jordan, the United Arab Emirates, Saudi Arabia, and Turkey. Sectors targeted included airlines; aircraft services; software and IT services companies serving the air and sea transport sectors; telecoms services; payroll services; engineering consultancies; and document management software. Outside of the Middle East, Symantec has also found evidence of attacks against one African airline and attempts to compromise an international travel reservations firm. <https://www.symantec.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions>

	Feb 2018	Turkish Government Targeting This new secondary payload is Python-based and compiled into executable form using the PyInstaller utility. This is the first instance where Unit 42 has identified a Python-based payload used by these operators. We've also identified code overlap with OilRig's Clayside VBScript but at this time track Chafer and OilRig as separate threat groups. We have named this payload MechaFlounder for tracking purposes. <https://unit42.paloaltonetworks.com/new-python-based-payload-mechaflounder-used-by-chafer/>
	Autumn 2018	Spying on Iran-based foreign diplomatic entities Throughout the autumn of 2018 we analyzed a long-standing (and still active at that time) cyberespionage campaign that was primarily targeting foreign diplomatic entities based in Iran. The attackers were using an improved version of Remexi in what the victimology suggests might be a domestic cyberespionage operation. <https://securelist.com/chafer-used-remexi-malware/89538/>
Information		<https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html> <https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets>
MITRE ATT&CK		<https://attack.mitre.org/groups/G0087/>

Charming Kitten, Newscaster, NewsBeef

Names	Charming Kitten *(CrowdStrike)* Newscaster *(Symantec)* NewsBeef *(Kaspersky)* Group 83 *(Talos)* Parastoo *(Flashpoint)*
Country	Iran
Motivation	Information theft and espionage
Description	Charming Kitten is an Iranian cyberespionage group that has been active since approximately 2014. They appear to focus on targeting individuals of interest to Iran who work in academic research, human rights, and media, with most victims having been located in Iran, the US, Israel, and the UK. Charming Kitten usually tries to access private email and Facebook accounts, and sometimes establishes a foothold on victim computers as a secondary objective. The group's TTPs overlap extensively with another group, Magic Hound, APT 35, Cobalt Gypsy, Rocket Kitten, resulting in reporting that may not distinguish between the two groups' activities.
Observed	Sectors: Defense and Government. Countries: Afghanistan, Algeria, Brazil, China, Denmark, France, Germany, India, Iran, Iraq, Israel, Japan, Romania, Russia, Switzerland, Syria, Turkey, UAE, UK, Ukraine and USA.
Tools used	DownPaper, FireMalv, MacDownloader and Stealer Builder.
Operations performed	2011	Operation "Newscaster" The research firm iSight dubbed the operation Newscaster and said hackers used social-media sites like Twitter, Facebook and LinkedIn to draw their targets and then lure them to check out a bogus news site, NewsOnAir.org, filled with foreign policy and defense articles, The Post reported. The overall aim is that the social-media platform would give the hackers connections with those at the top of public policy — and position them to tap into that information network. <https://www.washingtontimes.com/news/2014/may/29/iranian-hackers-sucker-punch-us-defense-heads-crea/>
	Feb 2016	In late February 2016, a University website in Iran stood out for thoroughly vetting its current and potential students and staff. The University's web site served repackaged content from the Browser Exploitation Framework (BeEF) with embedded JavaScript content. <https://securelist.com/freezer-paper-around-free-meat/74503/>
	Aug 2017	Breach of HBO On August 7 a small treasure trove of HBO content was posted publicly to the web by a hacker who is now demanding a $6 million payment to stop any further release of data. The hacker who goes by Mr. Smith posted five scripts for Game of Thrones and a month's worth of email from HBO Vice President for Film Programming Leslie Cohen along with some other corporate information, according to the Associated Press.

		<https://www.scmagazine.com/home/security-news/cybercrime/hbo-breach-accomplished-with-hard-work-by-hacker-poor-security-practices-by-victim/>
	2017	Fake news website BritishNews to infect visitors On the same note, we identified a fake-news agency "established" by the attackers, called "The British news agency" or "Britishnews" (inspired by BBC). Its website domain is britishnews.com[.]co and two other domains, broadcastbritishnews[.]comand britishnews[.]org redirected to it.
	2017	Blackmailing BBC reporter with 'naked photo' threats Iranian agents blackmailed a BBC Persian journalist by threatening to publish revealing photos of her as part of a wider campaign against the British media outlet, staff at the broadcaster told Arab News. New details emerged on Saturday about alleged harassment of BBC Persian reporters' family members and loved ones at the hands of the Iranian security services. <http://www.arabnews.com/node/1195681/media>
	Jun 2018	Impersonating ClearSky, the security firm that uncovered its campaigns Iranian cyberespionage group Charming Kitten, which has been operating since 2014, has impersonated the cybersecurity firm that exposed its operations and campaigns. Israeli firm ClearSky Security said the group managed to copy its official website hosted on a similar-looking domain - clearskysecurity[.]net. ClearSky's actual website is Clearskysec.com. <https://cyware.com/news/iranian-apt-charming-kitten-impersonates-clearsky-the-security-firm-that-uncovered-its-campaigns-7fea0b4f>
	Oct 2018	The Return of The Charming Kitten In this campaign, hackers have targeted individuals who are involved in economic and military sanctions against the Islamic Republic of Iran as well as politicians, civil and human rights activists and journalists around the world. Our review in Certfa demonstrates that the hackers - knowing that their victims use two-step verification - target verification codes and also their email accounts such as Yahoo! and Gmail. <https://blog.certfa.com/posts/the-return-of-the-charming-kitten/>
Counter operation	• Former U.S. Counterintelligence Agent Charged With Espionage on Behalf of Iran; Four Iranians Charged With a Cyber Campaign Targeting Her Former Colleagues (2019) <https://www.justice.gov/opa/pr/former-us-counterintelligence-agent-charged-espionage-behalf-iran-four-iranians-charged-cyber> • Microsoft slaps down 99 APT35/Charming Kitten domains (2019) <https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/>	
Information	<https://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf> <https://securelist.com/freezer-paper-around-free-meat/74503/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0058/>	

Clever Kitten

Names	Clever Kitten *(CrowdStrike)* Group 41 *(Talos)*
Country	Iran
Motivation	Information theft and espionage
Description	(CrowdStrike) Clever Kitten primarily targets global companies with strategic importance to countries that are contrary to Iranian interests. Clever Kitten actors have a strong affinity for PHP server-side attacks to make access; this is relatively unique amongst targeted attackers who often favor targeting a specific individual at a specific organization using social engineering. Some attackers have moved to leveraging strategic web compromises. The reason for this is likely the availability of exploits against web browsers, which for a variety of reasons allows an attacker to bypass security features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR).
Observed	Global companies with strategic importance to countries that are contrary to Iranian interests.
Tools used	Acunetix Web Vulnerability Scanner, PHP Webshell RC SHELL
Information	<https://www.crowdstrike.com/blog/whois-clever-kitten/>

Cobalt Group

Names	Cobalt Group *(Group-IB)* Cobalt Gang *(Palo Alto)* Cobalt Spider *(CrowdStrike)* Gold Kingswood *(SecureWorks)*	
Country	Russia	
Motivation	Financial gain	
Description	Cobalt Group is a financially motivated threat group that has primarily targeted financial institutions. The group has conducted intrusions to steal money via targeting ATM systems, card processing, payment systems and SWIFT systems. Cobalt Group has mainly targeted banks in Eastern Europe, Central Asia, and Southeast Asia. The group has been known to target organizations in order to use their access to then compromise additional victims. Reporting indicates there may be links between Cobalt Group and both the malware Carbanak and the group Carbanak, Anunak.	
Observed	Sectors: Financial. Countries: Argentina, Armenia, Austria, Azerbaijan, Belarus, Bulgaria, Canada, China, Czech, Estonia, Georgia, Italy, Jordan, Kazakhstan, Kuwait, Kyrgyzstan, Malaysia, Moldova, Netherlands, Poland, Romania, Russia, Spain, Taiwan, Tajikistan, Thailand, Turkey, UK, Ukraine, USA and Vietnam.	
Tools used	AmmyyRAT, ATMSpitter, ATMRipper Cobalt Strike, CobInt, Cyst Downloader, Mimikatz, Metasploit Stager, More_eggs, SDelete, SoftPerfect Network Scanner and SpicyOmelette.	
Operations performed	Jun 2016	In June 2016, the first attack conducted by the Cobalt group was tracked at a large Russian bank, where hackers attempted to steal money from ATMs. The attackers infiltrated the bank's network, gained control over it, compromised the domain administrator's account, and reached the ATM control server. <https://www.group-ib.com/blog/cobalt>
	Jul 2016	ATM heist at the First Commercial Bank in Taiwan <https://www.reuters.com/article/us-taiwan-cyber-atms/taiwan-atm-heist-linked-to-european-hacking-spree-security-firm-idUSKBN14P0CX>
	Aug 2016	ATM heist at the Government Saving Bank in Thailand[2]
	May 2017	In May, Proofpoint observed multiple campaigns using a new version of Microsoft Word Intruder (MWI). MWI is a tool sold on underground markets for creating exploit-laden documents, generally used in targeted attacks. We previously reported about MWI when it added support for CVE-2016-4117. After the latest update, MWI is now using CVE-2017-0199 to launch an HTML Application (HTA) used for both information collection and payload execution. This activity targets organizations in the financial vertical including banks, banking software vendors, and ATM software and hardware vendors. The emails are sent to technology and security personnel working in departments including Fraud and Information Security.

[2] See ThaiCERT Whitepaper "ATM Heist GSB August 2016"

		<https://www.proofpoint.com/us/threat-insight/post/microsoft-word-intruder-integrates-cve-2017-0199-utilized-cobalt-group-target>
	Aug 2017	The first spam run on August 31 used a Rich Text Format (RTF) document laden with malicious macros. The second, which ran from September 20 to 21, used an exploit for CVE-2017-8759 (patched last September), a code injection/remote code execution vulnerability in Microsoft's .NET Framework. The vulnerability was used to retrieve and execute Cobalt Strike from a remote server they controlled. <https://blog.trendmicro.com/trendlabs-security-intelligence/cobalt-spam-runs-use-macros-cve-2017-8759-exploit/>
	Nov 2017	On Tuesday, November 21, a massive spear-phishing campaign began targeting individual employees at various financial institutions, mostly in Russia and Turkey. Purporting to provide info on changes to 'SWIFT' terms, the email contained a single attachment with no text in the body. It was an attempt by the Cobalt Group to gain a foothold in the networks of the targeted individuals' organizations <https://www.riskiq.com/blog/labs/cobalt-strike/>
	Jan 2018	Spear-phishing attacks to Russian banks The emails were sent in the name of a large European bank in an attempt to social engineer the receiver into trusting the email. The emails were quite plain with only a single question in the body and an attachment with the name once.rtf. In other cases, we saw a file with the name Заявление.rtf attached to an email that was also written in Russian. <https://www.riskiq.com/blog/labs/cobalt-group-spear-phishing-russian-banks/>
	May 2018	On May 23, 1:21 p.m (Moscow time) Group-IB tracked a new large-scale Cobalt cyberattack on the leading banks of Russia and the CIS. It was like a challenge: phishing emails were sent acting as a major anti-virus vendor. Bank employees received a "complaint", in English, that their computers allegedly violated legislation. <https://www.group-ib.com/blog/renaissance>
	Sep 2018	In 2018, CTU researchers observed several GOLD KINGSWOOD campaigns involving SpicyOmelette, a tool used by the group during initial exploitation of an organization. This sophisticated JavaScript remote access tool is generally delivered via phishing, and it uses multiple defense evasion techniques to hinder prevention and detection activities. <https://www.secureworks.com/blog/cybercriminals-increasingly-trying-to-ensnare-the-big-financial-fish>
	Oct 2018	One of the latest examples related to the campaign under analysis was used in attacks just a few days ago. It shows the simplicity of the attack delivery employed by this group. The attack reinforces the fact that email is still one of the primary attack vectors we continuously observe. This attack begins by targeting employees at several banking entities across the globe using an email with subject "Confirmations on October 16, 2018". <https://unit42.paloaltonetworks.com/unit42-new-techniques-uncover-attribute-cobalt-gang-commodity-builders-infrastructure-revealed/>

Counter operations	• Mastermind behind EUR 1 billion cyber bank robbery arrested in Spain (2018) <https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain> • Three Carbanak cyber heist gang members arrested (2018) <https://www.computerweekly.com/news/252446153/Three-Carbanak-cyber-heist-gang-members-arrested>
Information	<https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cobalt-2017-eng.pdf> <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-september-cobalt-spider/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0080/>

Cold River

Names	Cold River *(Lastline)* Nahr el bared *(original place)* Nahr Elbard *(transliteration)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(Lastline) While reviewing some network anomalies, we recently uncovered Cold River, a sophisticated threat actor making malicious use of DNS tunneling for command and control activities. We have been able to decode the raw traffic in command and control, find sophisticated lure documents used in the campaign, connect other previously unknown samples, and associate a number of legitimate organizations whose infrastructure is referenced and used in the campaign. The campaign targets Middle Eastern organizations largely from the Lebanon and United Arab Emirates, though, Indian and Canadian companies with interests in those Middle Eastern countries are also targeted. There are new TTPs used in this attack – for example Agent_Drable is leveraging the Django python framework for command and control infrastructure, the technical details of which are outlined later in the blog.
Observed	Countries: Canada, India and Middle East (mostly Lebanon and UAE).
Tools used	Agent_Drable.
Information	<https://www.lastline.com/labsblog/threat-actor-cold-river-network-traffic-analysis-and-a-deep-dive-on-agent-drable/>

Comment Crew, APT 1

Names	Comment Crew *(Symantec)* Comment Panda *(CrowdStrike)* TG-8223 *(SecureWorks)* APT 1 *(Mandiant)* BrownFox *(Symantec)* Group 3 *(Talos)* Byzantine Hades *(US State Department)* Byzantine Candor *(US State Department)* Shanghai Group *(SecureWorks)* GIF89a *(Kaspersky)*
Country	China
Sponsor	State-sponsored, 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398.
Motivation	Information theft and espionage
Description	Also known as APT1, Comment Crew is an advanced persistent threat (APT) group with links to the Chinese military. The threat actors, which were active from roughly 2006 to 2010, managed to strike over 140 US companies in the quest for sensitive corporate and intellectual property data. The group earned their name through their use of HTML comments to hide communication to the command-and-control servers. The usual attack vector was via spear-phishing campaigns utilizing emails which contained documents with names tailored for the potential victims, such as "ArmyPlansConferenceOnNewGCVSolicitation.pdf," or "Chinese Oil Executive Learning From Experience.doc."
Observed	Sectors: Aerospace, Chemical, Construction, Education, Energy, Engineering, Entertainment, Financial, Food and Agriculture, Government, Healthcare, High-Tech, IT, Manufacturing, Media, Mining, Navigation, Non-profit organizations, Research, Satellites, Telecommunications, Transportation and lawyers. Countries: Belgium, Canada, France, India, Israel, Japan, Luxembourg, Norway, Singapore, South Africa, Switzerland, Taiwan, UAE, UK and USA.
Tools used	Auriga, bangat, BISCUIT, Bouncer, Cachedump, CALENDAR, Combos, CookieBag, Dairy, GetMail, GLOOXMAIL, Goggles, gsecdump, Hacksfase, Helauto, Kurton, Lslsass, ManItsMe, MAPIget, Mimikatz, MiniASP, NewsReels, Pass-The-Hash Toolkit, Poison Ivy, pwdump, SeaSalt, ShadyRAT, StarsyPound, Sword, TabMsgSQL, Tarsip, Tasklist, WebC2-AdSpace, WebC2-Ausov, WebC2-Bolid, WebC2-Cson, WebC2-DIV, WebC2-GreenCat, WebC2-Head, WebC2-Kt3, WebC2-Qbp, WebC2-Rave, WebC2-Table, WebC2-UGX and WebC2-Yahoo.
Operations performed	2006-2010	Operation "Seasalt" Target: 140 US companies in the quest for sensitive corporate and intellectual property data. Method: Spear-phishing with malicious documents.
	2011-2012	Hackers Plundered Israeli Defense Firms that Built 'Iron Dome' Missile Defense System <https://krebsonsecurity.com/2014/07/hackers-plundered-israeli-defense-firms-that-built-iron-dome-missile-defense-system/>

	Feb 2014	Operation "Siesta" FireEye recently looked deeper into the activity discussed in TrendMicro's blog and dubbed the "Siesta" campaign. The tools, modus operandi, and infrastructure used in the campaign present two possibilities: either the Chinese cyberespionage unit APT 1 is perpetrating this activity, or another group is using the same tactics and tools as the legacy APT 1. <https://blog.trendmicro.com/trendlabs-security-intelligence/the-siesta-campaign-a-new-targeted-attack-awakens/> <https://www.fireeye.com/blog/threat-research/2014/03/a-detailed-examination-of-the-siesta-campaign.html>
	May 2018	Operation "Oceansalt" Target: Oceansalt appears to have been part of an operation targeting South Korea, United States, and Canada in a well-focused attack. A variation of this malware has been distributed from two compromised sites in South Korea. Method: Oceansalt appears to be the first stage of an advanced persistent threat. The malware can send system data to a control server and execute commands on infected machines, but we do not yet know its ultimate purpose. Note: It is possible that this operation was not performed by the actual Comment Crew group (as they are supposedly in jail). <https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-oceansalt-delivers-wave-after-wave/> <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf>
Counter operations	• 5 in China Army Face U.S. Charges of Cyberattacks (2014) <https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html>	
Information	<https://www.symantec.com/connect/blogs/apt1-qa-attacks-comment-crew>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0006/>	

Confucius

Names	Confucius *(Palo Alto)*
Country	[South Asia]
Motivation	Information theft and espionage
Description	(Trend Micro) Confucius' campaigns were reportedly active as early as 2013, abusing Yahoo! And Quora forums as part of their command-and-control (C&C) communications. We stumbled upon Confucius, likely from South Asia, while delving into Patchwork's cyberespionage operations. Confucius' operations include deploying bespoke backdoors and stealing files from their victim's systems with tailored file stealers. The stolen files are then exfiltrated by abusing a cloud service provider. Some of these file stealers specifically target files from USB devices, probably to overcome air-gapped environments. This group seems to be associated with Patchwork, Dropping Elephant.
Observed	Countries: Most of the South and Southeast Asian countries (including Mongolia), most of the Middle Eastern countries, with a focus on Pakistan, most of the African countries, Trinidad, Tobago and Ukraine.
Tools used	ApacheStealer, ByeBye Shell, Confucius, MY24, sctrls, remote-access-c3 and sip_telephone, swissknife2 and Sneepy.
Operations performed	Oct 2017	In recent weeks, Unit 42 has discovered three documents crafted to exploit the InPage program. InPage is a word processor program that supports languages such as Urdu, Persian, Pashto, and Arabic. The three InPage exploit files are linked through their use of very similar shellcode, which suggests that either the same actor is behind these attacks, or the attackers have access to a shared builder. <https://unit42.paloaltonetworks.com/unit42-recent-inpage-exploits-lead-multiple-malware-families/>
	End 2017	Probing Confucius' infrastructure, we came across websites offering Windows and Android chat applications, most likely iterations of its predecessor, Simple Chat Point: Secret Chat Point, and Tweety Chat. We are admittedly uncertain of the extent — and success — of their use, but it's one of the ingredients of the group's operations. <https://blog.trendmicro.com/trendlabs-security-intelligence/deciphering-confucius-cyberespionage-operations/>
	May 2018	During their previous campaign, we found Confucius using fake romance websites to entice victims into installing malicious Android applications. This time, the threat actor seems to have a new modus operandi, setting up two new websites and new payloads with which to compromise its targets. <https://blog.trendmicro.com/trendlabs-security-intelligence/confucius-update-new-tools-and-techniques-further-connections-with-patchwork/>
Information	<https://unit42.paloaltonetworks.com/unit42-confucius-says-malware-families-get-further-by-abusing-legitimate-websites/> <https://documents.trendmicro.com/assets/research-deciphering-confucius-cyberespionage-operations.pdf>

CopyKittens, Slayer Kitten

Names	CopyKittens *(Trend Micro)* Slayer Kitten *(CrowdStrike)*
Country	Iran
Motivation	Information theft and espionage
Description	CopyKittens is an Iranian cyberespionage group that has been operating since at least 2013. It has targeted countries including Israel, Saudi Arabia, Turkey, the U.S., Jordan, and Germany. The group is responsible for the campaign known as Operation Wilted Tulip.
Observed	Sectors: Defense, Education, Government, IT and Media. Countries: Germany, Israel, Jordan, Saudi Arabia, Turkey and USA.
Tools used	Cobalt Strike, Empire, Matryoshka, TDTESS, Vminst and ZPP.
Operations performed	2013	Operation "Wilted Tulip" In this report, Trend Micro and ClearSky expose a vast espionage apparatus spanning the entire time the group has been active. It includes recent incidents as well as older ones that have not been publicly reported; new malware; exploitation, delivery and command and control infrastructure; and the group's modus operandi. We dubbed this activity Operation Wilted Tulip <https://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf>
	2015	CopyKittens has conducted at least three waves of cyber-attacks in the past year. In each of the attacks the infection method was almost identical and included an extraordinary number of stages used to avoid detection. As with other common threat actors, the group relies on social engineering methods to deceive its targets prior to infection. <https://s3-eu-west-1.amazonaws.com/minervaresearchpublic/CopyKittens/CopyKittens.pdf>
	Jan 2017	Breach of the Israeli newspaper Jerusalem Post As part of our monitoring of Iranian threat agents activities, we have detected that since October 2016 and until the end of January 2017, the Jerusalem Post, as well as multiple other Israeli websites and one website in the Palestinian Authority were compromised by Iranian threat agent CopyKittens. <https://www.clearskysec.com/copykitten-jpost/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0052/>

Corkow, Metel

Names	Corkow *(Group-IB)* Metel *(Kaspersky)*
Country	Russia
Motivation	Financial gain
Description	(Group-IB) In February 2015 the first major successful attack on a Russian trading system took place, when hackers gained unsanctioned access to trading system terminals using a Trojan resulting in trades of more than $400million. The criminals made purchases and sales of US dollars in the Dollar/Ruble exchange program on behalf of a bank using malware. The attack itself lasted only 14 minutes, however, it managed to cause a high volatility in the exchange rate of between 55/62 (Buy/Sell) rubles per 1 dollar instead of the 60-62 stable range. To conduct the attack criminals used the Corkow malware, also known as Metel, containing specific modules designed to conduct thefts from trading systems, such as QUIK operated by ARQA Technologies and TRANSAQ from ZAO "Screen market systems". Corkow provided remote access to the ITS-Broker system terminal by «Platforma soft» Ltd., which enabled the fraud to be committed. In August 2015 a new incident related to the Corkow (Metel) Trojan was detected. An attack on a bank card systems, which included about 250 banks which used the bank card system to service cash withdrawals from Visa and MasterCard cards under a special tariff. This attack resulted in the hundreds of millions of rubles being stolen via ATMs of the systems members.
Observed	Sectors: Financial. Countries: Argentina, Austria, Belarus, Brazil, Croatia, Cyprus, Denmark, Estonia, France, Germany, Italy, Kazakhstan, Latvia, Mexico, Peru, Poland, Singapore, Spain, Switzerland, Russia, Thailand, Turkey, UK, Ukraine and USA.
Tools used	Corkow, Metel.
Information	<https://www.group-ib.ru/brochures/Group-IB-Corkow-Report-EN.pdf> <https://www.welivesecurity.com/2014/02/27/corkow-analysis-of-a-business-oriented-banking-trojan/> <https://www.kaspersky.com/resource-center/threats/metel>

Covellite

Names	Covellite *(Dragos)*
Country	North Korea
Motivation	Information theft and espionage
Description	(Dragos) Covellite compromises networks associated with civilian electric energy worldwide and gathers intelligence on intellectual property and internal industrial operations. Covellite lacks an industrial control system (ICS) specific capability at this time. Covellite operates globally with targets primarily in Europe, East Asia, and North America. US targets emerged in September 2017 with a small, targeted phishing campaign directed at select U.S. electric companies. The phishing emails contained a malicious Microsoft Word document and infected computers with malware. The malicious emails discovered in the fall masqueraded as resumes or invitations. They delivered a remote access tool (RAT) payload which was used to conduct reconnaissance and enable persistent, covert access to victims' machines. Covellite's infrastructure and malware are similar to the hacking organization known as Lazarus Group, Hidden Cobra, Labyrinth Chollima by Novetta and Hidden Cobra by the U.S. Department of Homeland Security. Lazarus Group is responsible for attacks ranging from the 2014 attack on Sony Pictures to a number of Bitcoin heists in 2017. Technical analysis of Covellite malware indicates an evolution from known Lazarus toolkits. However, aside from technical overlap, it is not known how the capabilities and operations between Covellite and Lazarus are related. Covellite remains active but appears to have abandoned North American targets, with indications of activity in Europe and East Asia. Given the group's specific interest in infrastructure operations, rapidly improving capabilities, and history of aggressive targeting, Dragos considers this group a primary threat to the ICS industry.
Observed	Sectors: Energy. Countries: East Asia, Europe and USA.
Tools used	
Information	<https://dragos.com/resource/covellite/>

Cutting Kitten, TG-2889

Names	Cutting Kitten *(CrowdStrike)* TG-2889 *(SecureWorks)*
Country	Iran
Sponsor	State-sponsored, security company ITSecTeam
Motivation	Information theft and espionage
Description	Cleaver is a threat group that has been attributed to Iranian actors and is responsible for activity tracked as Operation Cleaver. Strong circumstantial evidence suggests Cleaver is linked to Threat Group 2889 (TG-2889). This group evolved into Magic Hound, APT 35, Cobalt Gypsy, Rocket Kitten.
Observed	Sectors: Aerospace, Airlines, Airports, Chemical, Defense, Education, Energy, Financial (banks: Bank of America, US Bancorp, Fifth Third Bank, Citigroup, PNC, BB&T, Wells Fargo, Capital One and HSBC), Government, Healthcare, Oil and gas, Technology, Telecommunications, Transportation and Utilities. Countries: Canada, China, France, Germany, India, Israel, Kuwait, Mexico, Netherlands, Pakistan, Qatar, Saudi Arabia, South Korea, Turkey, UAE, UK and USA.
Tools used	CsExt, Jasus, KAgent, Net Crawler, PvcOut, SynFlooder, TinyZBot, WndTest and ZhMimikatz.
Operations performed	2012	Operation "Cleaver" Operation Cleaver has, over the past several years, conducted a significant global surveillance and infiltration campaign. To date it has successfully evaded detection by existing security technologies. The group is believed to work from Tehran, Iran, although auxiliary team members were identified in other locations including the Netherlands, Canada, and the UK. The group successfully leveraged both publicly available, and customized tools to attack and compromise targets around the globe. The targets include military, oil and gas, energy and utilities, transportation, airlines, airports, hospitals, telecommunications, technology, education, aerospace, Defense Industrial Base (DIB), chemical companies, and governments. <https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf>
	2013	Attack on the Bowman Avenue Dam Iranian hackers infiltrated the control system of a small dam less than 20 miles from New York City two years ago, sparking concerns that reached to the White House, according to former and current U.S. officials and experts familiar with the previously undisclosed incident. <https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559>
	2015	Network of Fake LinkedIn Profiles While tracking a suspected Iran-based threat group known as Threat Group-2889 (TG-2889), Dell SecureWorks Counter Threat Unit (CTU) researchers uncovered a network of fake LinkedIn profiles. These convincing profiles form a self-referenced network of seemingly established LinkedIn users. CTU researchers assess with high

		confidence the purpose of this network is to target potential victims through social engineering. <https://www.secureworks.com/research/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles>
Counter operations		• U.S. indicts Iranians for hacking dozens of banks, New York dam (2016) <https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0003/>	

Dark Caracal

Names	Dark Caracal *(Lookout)*
Country	Lebanon
Sponsor	State-sponsored, General Directorate of General Security (GDGS)
Motivation	Information theft and espionage
Description	(Lookout) Lookout and Electronic Frontier Foundation (EFF) have discovered Dark Caracal[3], a persistent and prolific actor, who at the time of writing is believed to be administered out of a building belonging to the Lebanese General Security Directorate in Beirut. At present, we have knowledge of hundreds of gigabytes of exfiltrated data, in 21+ countries, across thousands of victims. Stolen data includes enterprise intellectual property and personally identifiable information. We are releasing more than 90 indicators of compromise (IOC) associated with Dark Caracal including 11 different Android malware IOCs; 26 desktop malware IOCs across Windows, Mac, and Linux; and 60 domain/IP based IOCs. Dark Caracal targets include individuals and entities that a nation state might typically attack, including governments, military targets, utilities, financial institutions, manufacturing companies, and defense contractors. We specifically uncovered data associated with military personnel, enterprises, medical professionals, activists, journalists, lawyers, and educational institutions during this investigation. Types of data include documents, call records, audio recordings, secure messaging client content, contact information, text messages, photos, and account data.
Observed	Sectors: Defense, Education, Financial, Government, Healthcare, Manufacturing, Utilities, activists, lawyers and journalists. Countries: China, France, Germany, India, Italy, Jordan, Lebanon, Nepal, Netherlands, Pakistan, Philippines, Qatar, Russia, Saudi Arabia, South Korea, Switzerland, Syria, Thailand, USA, Venezuela and Vietnam.
Tools used	Bandook, CrossRAT, FinFisher and Pallas.
Information	<https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0070/>

---

[3] See ThaiCERT Whitepaper "Dark Caracal Campaign"

DarkHotel

Names	DarkHotel *(Kaspersky)* APT-C-06 *(360)* SIG25 *(NSA)* Dubnium *(Microsoft)* Fallout Team *(FireEye)* Shadow Crane *(CrowdStrike)*
Country	North Korea
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	(SecurityWeek) The activities of the DarkHotel advanced persistent threat (APT) actor came to light in November 2014, when Kaspersky published a report detailing a sophisticated cyberespionage campaign targeting business travelers in the Asia-Pacific region. The group has been around for nearly a decade and some researchers believe its members are Korean speakers. The attackers targeted their victims using several methods, including through their hotel's Wi-Fi, zero-day exploits and peer-to-peer (P2P) file sharing websites. Nearly one year later, the threat group was observed using new attack techniques and an exploit leaked from Italian spyware maker Hacking Team. DarkHotel victims have been spotted in several countries, including North Korea, Russia, South Korea, Japan, Bangladesh, Thailand, Taiwan, China, the United States, India, Mozambique, Indonesia and Germany. Up until recently, the attacks appeared to focus on company executives, researchers and development personnel from sectors such as defense industrial base, military, energy, government, NGOs, electronics manufacturing, pharmaceutical, and medical. In more recent DarkHotel attacks it has dubbed "Inexsmar," security firm Bitdefender said the hackers targeted political figures, and they appeared to be using some new methods.
Observed	Sectors: Defense, Energy, Government, Healthcare, NGOs, Pharmaceutical, Research and Technology. Countries: Bangladesh, Belgium, China, Germany, Greece, Hong Kong, India, Indonesia, Ireland, Italy, Japan, Kazakhstan, Lebanon, North Korea, Mexico, Mozambique, Pakistan, Philippines, Russia, Serbia, Singapore, South Korea, Taiwan, Thailand, UAE, USA and others.
Tools used	DarkHotel, GreezeBackdoor, Luder, Nemim, Pioneer and Tapaoux.
Operations performed	2010	Operation "DarkHotel" Target: The travelers are often top executives from a variety of industries doing business and outsourcing in the APAC region. Targets have included CEOs, senior vice presidents, sales and marketing directors and top R&D staff. Method: spear-phishing targets with highly advanced Flash zero-day exploits that effectively evade the latest Windows and Adobe defenses, and yet they also imprecisely spread among large numbers of vague targets with peer-to-peer spreading tactics. Moreover, this crew's most unusual characteristic is that for several years the Darkhotel APT has maintained a capability to

		use hotel networks to follow and hit selected targets as they travel around the world. <https://securelist.com/the-darkhotel-apt/66779/>
	2015	Darkhotel's attacks in 2015 <https://securelist.com/darkhotels-attacks-in-2015/71713/>
	Dec 2015	Operation "Daybreak" Method: Uses Flash zero-day exploit for CVE-2015-8651. Note: not the same operation as ScarCruft's Operation "Daybreak".
	Sep 2016	Operation "Inexsmar" Target: seems to be used in a campaign that targets political figures rather than the usual corporate research and development personnel, CEOs and other senior corporate officials. Method: This attack uses a new payload delivery mechanism rather than the consecrated zero-day exploitation techniques, blending social engineering with a relatively complex Trojan to infect its selected pool of victims. <https://labs.bitdefender.com/2017/07/inexsmar-an-unusual-darkhotel-campaign/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0012/>	

DarkHydrus, LazyMeerkat

Names	DarkHydrus *(Palo Alto)* LazyMeerkat *(Kaspersky)*	
Country	Iran	
Motivation	Information theft and espionage	
Description	DarkHydrus is a threat group that has targeted government agencies and educational institutions in the Middle East since at least 2016. The group heavily leverages open-source tools and custom payloads for carrying out attacks.	
Observed	Sectors: Education and Government. Countries: Middle East.	
Tools used	Cobalt Strike, Mimikatz, Phishery and RogueRobin.	
Operations performed	Jun 2018	On June 24, 2018, Unit 42 observed DarkHydrus carrying out a credential harvesting attack on an educational institution in the Middle East. The attack involved a spear-phishing email with a subject of "Project Offer" and a malicious Word document as an attachment. <https://unit42.paloaltonetworks.com/unit42-darkhydrus-uses-phishery-harvest-credentials-middle-east/>
	Jul 2018	Attack on Middle East Government This attack diverged from previous attacks we observed from this group as it involved spear-phishing emails sent to targeted organizations with password protected RAR archive attachments that contained malicious Excel Web Query files (.iqy). <https://unit42.paloaltonetworks.com/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/>
	Jan 2019	New Attacks in the Middle East 360 Threat Intelligence Center captured several lure Excel documents written in Arabic in January 9, 2019. A backdoor dropped by macro in the lure documents can communicate with C2 server through DNS tunnel, as well as Google Drive API. <https://ti.360.net/blog/articles/latest-target-attack-of-darkhydruns-group-against-middle-east-en/> <https://unit42.paloaltonetworks.com/darkhydrus-delivers-new-trojan-that-can-use-google-drive-for-c2-communications/>
Information	<https://unit42.paloaltonetworks.com/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0079/>	

Deep Panda, APT 26, Shell Crew, WebMasters, KungFu Kittens

Names	Deep Panda *(CrowdStrike)* APT 26 *(Mandiant)* Shell Crew *(RSA)* WebMasters *(Kaspersky)* KungFu Kittens *(FireEye)* Group 13 *(Talos)* PinkPanther (*RSA*) Black Vine *(Symantec)*
Country	China
Motivation	Information theft, espionage and financial gain
Description	Deep Panda is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications. The intrusion into healthcare company Anthem has been attributed to Deep Panda. This group is also known as Shell Crew, WebMasters, KungFu Kittens, and PinkPanther. Deep Panda also appears to be known as Black Vine based on the attribution of both group names to the Anthem intrusion. Some analysts track Deep Panda and APT 19, C0d0so as the same group, but it is unclear from open source information if the groups are the same.
Observed	Sectors: Defense, Financial, Government, Non-profit organizations, Telecommunications and Think Tanks. Countries: Australia, Southeast Asia and USA.
Tools used	Cobalt Strike, Derusbi, JerseyMikes, Mivast, PlugX, Sakula, StreamEx and Tasklist.
Operations performed	Dec 2012	Attack and IE 0day Information Used Against Council on Foreign Relations Regarding information's posted on the Washington Free Beacon, infected CFR.org website was used to attack visitors in order to extract valuable information's. The "drive-by" attack was detected around 2:00 pm on Wednesday 26 December and CFR members who visited the website between Wednesday and Thursday could have been infected and their data compromised, the specialists said. <https://eromang.zataz.com/2012/12/29/attack-and-ie-0day-informations-used-against-council-on-foreign-relations/>
	Dec 2012	Capstone Turbine Corporation Also Targeted in the CFR Watering Hole Attack <https://eromang.zataz.com/2013/01/02/capstone-turbine-corporation-also-targeted-in-the-cfr-watering-hole-attack-and-more/>
	Mar 2013	Breach of the US Department of Labor website On April 30, 2013, CrowdStrike was alerted to a strategic web compromise on a US Department of Labor website that was redirecting visitors to an attacker's infrastructure. Eight other compromised sites were also reported to be similarly compromised with the data suggesting that this campaign began in mid-March. <https://www.crowdstrike.com/blog/department-labor-strategic-web-compromise/>
	Early 2014	Breaches of National Security Think Tanks

		This actor, who was engaged in targeting and collection of Southeast Asia policy information, suddenly began targeting individuals with a tie to Iraq/Middle East issues. This is undoubtedly related to the recent Islamic State of Iraq and the Levant (ISIS) takeover of major parts of Iraq and the potential disruption for major Chinese oil interests in that country. In fact, Iraq happens to be the fifth-largest source of crude oil imports for China and the country is the largest foreign investor in Iraq's oil sector. <https://www.crowdstrike.com/blog/deep-thought-chinese-targeting-national-security-think-tanks/>
	Mar 2014	Breach of the US Office of Personnel Management OPM investigates a breach of its computer networks dating back to March 2014. Authorities trace the intrusion to China. OPM offers employees free credit monitoring and assures employees that no personal data appears to have been stolen. <https://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/>
	Apr 2014	Breach of health insurance company Anthem <https://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/>
	Aug 2014	Breach of USIS It emerges that USIS, a background check provider for the U.S. Department of Homeland Security, was hacked. USIS offers 27,000 DHS employees credit monitoring through AllClearID (full disclosure: AllClear is an advertiser on this blog). Investigators say Chinese are hackers responsible, and that the attackers broke in by exploiting a vulnerability in an enterprise management software product from SAP. <https://www.nextgov.com/cybersecurity/2015/05/third-party-software-was-entry-point-background-check-system-hack/112354/>
	Jul 2014	Sakula Malware to Target Organizations in Multiple Sectors Over the last few months, the CrowdStrike Intelligence team has been tracking a campaign of highly targeted events focused on entities in the U.S. Defense Industrial Base (DIB), healthcare, government, and technology sectors. This campaign infected victims with Sakula malware variants that were signed with stolen certificates. <https://www.crowdstrike.com/blog/ironman-deep-panda-uses-sakula-malware-target-organizations-multiple-sectors/>
	Nov 2014	Breaches of Australian media organizations ahead of G20 "We started to see activity over the last couple of weeks targeting Australian media organizations and we believe that's related to the G20," Dmitri Alperovitch, co-founder of US computer security company CrowdStrike, told the ABC's 7.30 program. <https://www.abc.net.au/news/2014-11-13/g20-china-affliliated-hackers-breaches-australian-media/5889442>
	Dec 2014	Breach of KeyPoint Government Solutions KeyPoint Government Solutions, which took over the bulk of federal background checks after one of its competitors was hacked, also recently suffered a computer network breach, officials said Thursday. <https://www.washingtonpost.com/business/economy/keypoint-suffers-network-breach-thousands-of-fed-workers-could-be-

		affected/2014/12/18/e6c7146c-86e1-11e4-a702-fa31ff4ae98e_story.html>
	May 2015	Breach of health insurance company Premera Blue Cross Premera Blue Cross, one of the insurance carriers that participates in the Federal Employees Health Benefits Program, discloses a breach affecting 11 million customers. Federal auditors at OPM warned Premera three weeks prior to the breach that its network security procedures were inadequate. <https://www.seattletimes.com/business/local-business/feds-warned-premera-about-security-flaws-before-breach/>
	May 2015	Breach of health insurance company Carefirst Blue Cross CareFirst BlueCross BlueShield on Wednesday said it had been hit with a data breach that compromised the personal information on approximately 1.1 million customers. There are indications that the same attack methods may have been used in this intrusion as with breaches at Anthem and Premera, incidents that collectively involved data on more than 90 million Americans. <https://krebsonsecurity.com/2015/05/carefirst-blue-cross-breach-hits-1-1m/>
	May 2015	StreamEx malware Cylance SPEAR has identified a newer family of samples deployed by Shell Crew that has flown under AV's radar for more than a year and a half. Simple programmatic techniques continue to be effective in evading signature-based detection. <https://threatvector.cylance.com/en_us/home/shell-crew-variants-continue-to-fly-under-big-avs-radar.html>
Counter operations	• US Arrests Chinese Man Involved With Sakula Malware Used in OPM and Anthem Hacks (2017) <https://www.bleepingcomputer.com/news/security/us-arrests-chinese-man-involved-with-sakula-malware-used-in-opm-and-anthem-hacks/> • U.S. Indicts Chinese Hacker-Spies in Conspiracy to Steal Aerospace Secrets (2018) <https://gizmodo.com/u-s-indicts-chinese-hacker-spies-in-conspiracy-to-stea-1830111695> • Chinese national indicted for 2015 Anthem breach (2019) <https://www.cyberscoop.com/anthem-breach-indictment-chinese-national/>	
Information	<http://cybercampaigns.net/wp-content/uploads/2013/06/Deep-Panda.pdf> <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0009/>	

Desert Falcons

Names	Desert Falcons *(Kaspersky)* APT-C-23 *(360)* Two-tailed Scorpion *(360)*
Country	Gaza
Motivation	Information theft and espionage
Description	(Kaspersky) The Global Research and Analysis Team (GReAT) at Kaspersky Lab has uncovered new targeted attacks in the Middle East. Native Arabic-speaking cybercriminals have built advanced methods and tools to deliver, hide and operate malware that they have also developed themselves. This malware was originally discovered during an investigation of one of the attacks in the Middle East. Political activities and news are being actively used by the cybercriminals to entice victims into opening files and attachments. Content has been created with professionalism, with well-designed visuals and interesting, familiar details for the victims, as if the information were long awaited. The victims of the attacks to date have been carefully chosen; they are active and influential in their respective cultures, but also attractive to the cybercriminals as a source of intelligence and a target for extortion. The attackers have been operating for more than two years now, running different campaigns, targeting different types of victims and different types of devices (including Windows- and Android-based). We suspect that at least 30 people distributed across different countries are operating the campaigns
Observed	Sectors: Defense, Education, Government and Infrastructure. Countries: Albania, Algeria, Australia, Belgium, Bosnia and Herzegovina, Canada, China, Cyprus, Denmark, Egypt, France, Germany, Greece, Hungary, India, Iran, Iraq, Israel, Italy, Japan, Jordan, Kuwait, Lebanon, Libya, Mali, Mauritania, Mexico, Morocco, Netherlands, Norway, Pakistan, Palestine, Portugal, Qatar, Romania, Russia, Saudi Arabia, South Korea, Sudan, Sweden, Syria, Taiwan, Turkey, UAE, Ukraine, USA, Uzbekistan, Yemen and Zimbabwe.
Tools used	FrozenCell, GlanceLove, GnatSpy, KASPERAGENT, MICROPSIA, VAMP and ViperRAT.

Operations performed	Jan 2015	Operation "Arid Viper" Operation Arid Viper attacked five Israeli-based organizations in the government, transport, infrastructure, military, and academic industries, and one organization in Kuwait using spear-phishing emails that dropped a pornographic video on a victim's computer. <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/sexually-explicit-material-used-as-lures-in-cyber-attacks?linkId=12425812> <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-arid-viper.pdf>
	Sep 2015	Proofpoint researchers recently intercepted and analyzed phishing emails distributing Arid Viper malware payloads with some noteworthy updates.

		As with the originally documented examples, these messages were part of narrow campaigns targeting specific industry verticals: telecoms, high tech, and business services, primarily in Israel. <https://www.proofpoint.com/us/threat-insight/post/Operation-Arid-Viper-Slithers-Back-Into-View>
	Jul 2016	Around July last year, more than a 100 Israeli servicemen were hit by a cunning threat actor. The attack compromised their devices and exfiltrated data to the attackers' command and control server. In addition, the compromised devices were pushed Trojan updates, which allowed the attackers to extend their capabilities. The operation remains active at the time of writing this post, with attacks reported as recently as February 2017. <https://securelist.com/breaking-the-weakest-link-of-the-strongest-chain/77562/>
	Apr 2017	ThreatConnect has identified a KASPERAGENT malware campaign leveraging decoy Palestinian Authority documents. The samples date from April – May 2017, coinciding with the run up to the May 2017 Palestinian Authority elections. <https://threatconnect.com/kasperagent-malware-campaign/>
	Apr 2017	We identified one specific spear phishing campaign launched against targets within Palestine, and specifically against Palestinian law enforcement agencies. This campaign started in April 2017, using a spear phishing campaign to deliver the MICROPSIA payload in order to remotely control infected systems. <https://blog.talosintelligence.com/2017/06/palestine-delphi.html>
	Sep 2017	FrozenCell is the mobile component of a multi-platform attack we've seen a threat actor known as "Two-tailed Scorpion/APT-C-23," use to spy on victims through compromised mobile devices and desktops. <https://blog.lookout.com/frozencell-mobile-threat>
	Dec 2017	Recently, Trend Micro researchers came across a new mobile malware family which we have called GnatSpy. We believe that this is a new variant of VAMP, indicating that the threat actors behind APT-C-23 are still active and continuously improving their product. Some C&C domains from VAMP were reused in newer GnatSpy variants, indicating that these attacks are connected. We detect this new family as ANDROIDOS_GNATSPY. <https://blog.trendmicro.com/trendlabs-security-intelligence/new-gnatspy-mobile-malware-family-discovered/>
Information		<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064309/The-Desert-Falcons-targeted-attacks.pdf>

DNSpionage

Names	DNSpionage *(Talos)*
Country	Iran
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	(Talos) Cisco Talos recently discovered a new campaign targeting Lebanon and the United Arab Emirates (UAE) affecting .gov domains, as well as a private Lebanese airline company. Based on our research, it's clear that this adversary spent time understanding the victims' network infrastructure in order to remain under the radar and act as inconspicuous as possible during their attacks. Based on this actor's infrastructure and TTPs, we haven't been able to connect them with any other campaign or actor that's been observed recently. This particular campaign utilizes two fake, malicious websites containing job postings that are used to compromise targets via malicious Microsoft Office documents with embedded macros. The malware utilized by this actor, which we are calling "DNSpionage," supports HTTP and DNS communication with the attackers.
Observed	Sectors: Airlines, Government, Law Enforcement, Telecommunications and Internet infrastructure. Countries: Albania, Cyprus, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, North Africa, Sweden, UAE and USA.
Tools used	DNSpionage and Karkoff.
Operations performed	Apr 2019	DNSpionage brings out the Karkoff <https://blog.talosintelligence.com/2019/04/dnspionage-brings-out-karkoff.html>
Information	<https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html> <https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html> <https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/> <https://krebsonsecurity.com/tag/dnspionage/>

Domestic Kitten

Names	Domestic Kitten *(Check Point)*
Country	Iran
Motivation	Information theft and espionage
Description	(Check Point) Recent investigations by Check Point researchers reveal an extensive and targeted attack that has been taking place since 2016 and, until now, has remained under the radar due to the artful deception of its attackers towards their targets. Through the use of mobile applications, those behind the attack use fake decoy content to entice their victims to download such applications, which are in fact loaded with spyware, to then collect sensitive information about them. Interestingly, these targets include Kurdish and Turkish natives and ISIS supporters. Most interesting of all, though, is that all these targets are actually Iranians citizens. Considering the nature of the target, the data collected about these groups provides those behind the campaign with highly valuable information that will no doubt be leveraged in further future action against them. Indeed, the malware collects data including contact lists stored on the victim's mobile device, phone call records, SMS messages, browser history and bookmarks, geo-location of the victim, photos, surrounding voice recordings and more.
Observed	Countries: Afghanistan, Iran, Iraq and UK. The targets are Kurdish and Turkish natives and ISIS supporters.
Tools used	
Information	<https://research.checkpoint.com/domestic-kitten-an-iranian-surveillance-operation/>

Donot Team

Names	Donot Team *(ASERT)* APT-C-35 *(360)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(ASERT) In late January 2018, ASERT discovered a new modular malware framework we call "yty". The framework shares a striking resemblance to the EHDevel framework. We believe with medium confidence that a team we call internally as "Donot Team" is responsible for the new malware and will resume targeting of South Asia. In a likely effort to disguise the malware and its operations, the authors coded several references into the malware for football—it is unclear whether they mean American football or soccer. The theme may allow the network traffic to fly under the radar. The actors use false personas to register their domains instead of opting for privacy protection services. Depending on the registrar service chosen, this could be seen as another cost control measure. The actors often used typo-squatting to slightly alter a legitimate domain name. In contrast, the registration information used accurate spelling, possibly indicating the domain naming was intentional, typos included. Each unique registrant usually registered only a few domains, but mistakenly reused phone numbers or the registration data portrayed a similar pattern across domains.
Observed	Sectors: Government. Countries: Pakistan.
Tools used	EHDevel and yty.
Operations performed	Apr 2019	StealJob: New Android Malware Recently, we have observed a large-scale upgrade of its malicious Android APK framework to make it more stable and practical. Since the new APK framework is quite different from the one used in the past, we named it as StealJob since "job" is frequently used in the code. <https://ti.360.net/blog/articles/stealjob-new-android-malware-used-by-donot-apt-group-en/>
Information	<https://www.netscout.com/blog/asert/donot-team-leverages-new-modular-malware-framework-south-asia>

DragonOK

Names	DragonOK *(FireEye)*
Country	China
Motivation	Information theft and espionage
Description	DragonOK is a threat group that has targeted Japanese organizations with phishing emails. Due to overlapping TTPs, including similar custom tools, DragonOK is thought to have a direct or indirect relationship with the threat group Moafee. It is known to use a variety of malware, including Sysget/HelloBridge, PlugX, Poison Ivy, FormerFirstRat, NFlog, and NewCT.
Observed	Sectors: High-Tech and Manufacturing. Countries: Cambodia, Japan, Russia, Taiwan and Tibet.
Tools used	FormerFirstRAT, HelloBridge, HTRAN, IsSpace, KHRAT, NewCT, NFlog, PlugX, Poison Ivy, Rambo, Sysget and TidePool.
Operations performed	Jan 2015	This campaign involved five separate phishing attacks, each carrying a different variant of Sysget malware, also known as HelloBridge. The malware was included as an attachment intended to trick the user into opening the malware. All five phishing campaigns targeted a Japanese manufacturing firm over the course of two months, but the final campaign also targeted a separate Japanese high-tech organization. <https://unit42.paloaltonetworks.com/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/>
	2016	In recent months, Unit 42 has observed a number of attacks that we attribute to this group. Multiple new variants of the previously discussed sysget malware family have been observed in use by DragonOK. Sysget malware was delivered both directly via phishing emails, as well as in Rich Text Format (RTF) documents exploiting the CVE-2015-1641 vulnerability that in turn leveraged a very unique shellcode. <https://unit42.paloaltonetworks.com/unit42-dragonok-updates-toolset-targets-multiple-geographic-regions/>
	Jan 2017	Cybersecurity expert Niklas Femerstrand in an email yesterday pointed out that while servers in several different countries appear to be the origin the attack, it has been linked to the DragonOK campaign. "The DragonOK campaign has previously [in 2014] targeted organizations in Taiwan, Japan, Tibet and Russia, and political organizations in Cambodia since at least January, 2017," he wrote, adding that there are "strong indications" the campaign is "an operation funded by China". <https://www.phnompenhpost.com/national/kingdom-targeted-new-malware>
Information	<https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0017/>

DustSquad

Names	DustSquad *(Kaspersky)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(Kaspersky) For the last two years we have been monitoring a Russian-language cyberespionage actor that focuses on Central Asian users and diplomatic entities. We named the actor DustSquad and have provided private intelligence reports to our customers on four of their campaigns involving custom Android and Windows malware. In this blogpost we cover a malicious program for Windows called Octopus that mostly targets diplomatic entities. The name was originally coined by ESET in 2017 after the 0ct0pus3.php script used by the actor on their old C2 servers. We also started monitoring the malware and, using Kaspersky Attribution Engine based on similarity algorithms, discovered that Octopus is related to DustSquad, something we reported in April 2018. In our telemetry we tracked this campaign back to 2014 in the former Soviet republics of Central Asia (still mostly Russian-speaking), plus Afghanistan.
Observed	Sectors: Government. Countries: Afghanistan and Central Asia.
Tools used	Octopus.
Information	<https://securelist.com/octopus-infested-seas-of-central-asia/88200/>

Dust Storm

Names	Dust Storm *(Cylance)*
Country	[Unknown]
Sponsor	Seems state-sponsored
Motivation	Information theft and espionage
Description	(Cylance) Very little public information was available throughout 2010 on this threat, despite the group's primary backdoor gaining some level of prominence in targeted Asian attacks. This may be explained by the group's early reliance on Dynamic DNS domains for their command and control (C2) infrastructure, as well as their use of public RATs like Poison Ivy and Gh0st RAT for second-stage implants. It wasn't until June 2011 that Operation Dust Storm started to garner some notoriety from a series of attacks which leveraged an unpatched Internet Explorer 8 vulnerability, CVE-2011-1255, to gain a foothold into victim networks. In these attacks, a link to the exploit was sent via a spear phishing email from a purported Chinese student seeking advice or asking the target a question following a presentation. As to other documented cases, the attacker started interacting with the infected machine within minutes of compromise to begin manual network and host enumeration. In October 2011, the group attempted to take advantage of the ongoing Libyan crisis at the time and phish the news cycle regarding Muammar Gaddafi's death on October 20, 2011. It appears that in addition to some US defense targets, this campaign was also directed at a Uyghur mailing list. This time, the group used a specially crafted malicious Windows Help (.hlp) file, which exploited CVE-2010-1885.
Observed	Sectors: Energy and Oil and gas. Countries: Japan, South Korea, USA, Europe and Southeast Asia.
Tools used	Gh0st RAT, Misdat, MiS-Type, Poison Ivy and S-Type.
Information	<https://www.cylance.com/content/dam/cylance/pdfs/reports/Op_Dust_Storm_Report.pdf> <https://www.symantec.com/connect/blogs/inside-back-door-attack>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0031/>

Elderwood, Sneaky Panda

Names	Elderwood *(Symantec)* Elderwood Gang *(Symantec)* Sneaky Panda *(CrowdStrike)* SIG22 *(NSA)* Beijing Group *(SecureWorks)*
Country	China
Motivation	Information theft and espionage
Description	(Symantec) In 2009, Google was attacked by a group using the Hydraq (Aurora) Trojan horse. Symantec has monitored this group's activities for the last three years as they have consistently targeted a number of industries. Interesting highlights in their method of operations include: the use of seemingly an unlimited number of zero-day exploits, attacks on supply chain manufacturers who service the target organization, and a shift to "watering hole" attacks (compromising certain websites likely to be visited by the target organization). The targeted industry sectors include, but are not restricted to; defense, various defense supply chain manufacturers, human rights and non-governmental organizations (NGOs), and IT service providers. These attackers are systematic and re-use components of an infrastructure we have termed the "Elderwood platform". The name "Elderwood" comes from a source code variable used by the attackers. This attack platform enables them to quickly deploy zero-day exploits. Attacks are deployed through spear phishing emails and also, increasingly, through Web injections in watering hole attacks. It is likely the attackers have gained access to the source code for some widely used applications, or have thoroughly reverse-engineered the compiled applications in order to discover these vulnerabilities. The vulnerabilities are used as needed, often within close succession of each other if exposure of any of the vulnerabilities is imminent. The scale of the attacks, in terms of the number of victims and the duration of the attacks, are another indication of the resources available to the attackers. Victims are attacked, not for petty crime or theft, but for the wholesale gathering of intelligence and intellectual property. The resources required to identify and acquire useful information—let alone analyze that information—could only be provided by a large criminal organization, attackers supported by a nation state, or a nation state itself.
Observed	Sectors: Defense, Education, Energy, Financial, and Government. Countries: Australia, Canada, China, Denmark, Hong Kong, India, Switzerland, Taiwan, UK and USA.
Tools used	Briba, Gh0st RAT, Hydraq, Linfo, Naid, Nerex, Pasam, Poison Ivy, Vasport and Wiarp.
Operations performed	2009	Operation Aurora First publicly disclosed by Google on January 12, 2010, in a blog post, the attacks began in mid-2009 and continued through December 2009. The attack has been aimed at dozens of other organizations, of which Adobe Systems, Juniper Networks and Rackspace have publicly confirmed that they were targeted. According to media reports, Yahoo, Symantec, Northrop Grumman, Morgan Stanley and Dow Chemical were also among the targets. <https://en.wikipedia.org/wiki/Operation_Aurora>

		<https://googleblog.blogspot.com/2010/01/new-approach-to-china.html>
	Nov 2010	Visitors to Amnesty International's Hong Kong website are being bombarded with a host of lethal exploits, including one that attacks an unpatched vulnerability in Microsoft's Internet Explorer browser, researchers at security firm Websense said. <https://www.theregister.co.uk/2010/11/11/amnesty_international_hosts_ie_exploit/>
	May 2012	Amnesty International UK's website was hacked early this week in an assault ultimately geared towards planting malware onto the PCs of visiting surfers. <https://www.theregister.co.uk/2012/05/11/amnesty_malware_rat/>
Information		<http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf>
MITRE ATT&CK		<https://attack.mitre.org/groups/G0066/>

El Machete

Names	El Machete *(Kaspersky)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(Kaspersky) "Machete" is a targeted attack campaign with Spanish speaking roots. We believe this campaign started in 2010 and was renewed with an improved infrastructure in 2012. The operation may be still "active". The malware is distributed via social engineering techniques, which includes spear-phishing emails and infections via Web by a fake Blog website. We have found no evidence of exploits targeting zero-day vulnerabilities. Both the attackers and the victims appear to be Spanish-speaking.
Observed	Sectors: Defense, Embassies, Government, and Telecommunications. Countries: Argentina, Belgium, Bolivia, Brazil, Canada, China, Colombia, Cuba, Dominican Republic, Ecuador, France, Germany, Guatemala, Malaysia, Nicaragua, Mexico, South Korea, Spain, Peru, Russia, Spain, Sweden, UK, Ukraine, USA and Venezuela among others. In some cases, such as Russia, the target appears to be an embassy from one of the countries of this list.
Tools used	Machete.
Operations performed	Mar 2017	We've found that this group has continued to operate successfully, predominantly in Latin America, since 2014. All attackers simply moved to new C2 infrastructure, based largely around dynamic DNS domains, in addition to making minimal changes to the malware in order to evade signature-based detection. <https://threatvector.cylance.com/en_us/home/el-machete-malware-attacks-cut-through-latam.html>
Information	<https://securelist.com/el-machete/66108/>

Energetic Bear, Dragonfly

Names	Energetic Bear *(CrowdStrike)* Dragonfly *(Symantec)* Crouching Yeti *(Kaspersky)* Group 24 *(Talos)* Koala Team *(iSight)* Iron Liberty *(SecureWorks)* Electrum *(Dragos)*
Country	Russia
Motivation	Sabotage and destruction
Description	Dragonfly is a cyberespionage group that has been active since at least 2011. They initially targeted defense and aviation companies but shifted to focus on the energy sector in early 2013. They have also targeted companies related to industrial control systems. According to Kaspersky, Crouching Yeti has been operating since at least 2010 and has infected roughly 2,800 targets in 38 countries, and in industries as diverse as education and pharmaceuticals. A similar group emerged in 2015 and was identified by Symantec as Berserk Bear, Dragonfly 2.0. There is debate over the extent of the overlap between Dragonfly and Berserk Bear, Dragonfly 2.0, but there is sufficient evidence to lead to these being tracked as two separate groups.
Observed	Sectors: Construction, Education, Energy, Industrial, IT, Manufacturing, Oil and gas and Pharmaceutical. Countries: Canada, France, Germany, Greece, Italy, Poland, Romania, Russia, Serbia, Spain, Turkey, UK, Ukraine and USA.
Tools used	Commix, CrashOverride, Dirsearch, Dorshel, Havex RAT, Hello, Heriplor, Impacket, Industroyer, Inveigh, Karagany, Lightsout, Listrix, nmap, Oldrea, PHPMailer, PSExec, SMBTrap, Sqlmap, Subbrute, Sublist3r, Sysmain, Wpscan and WSO.
Operations performed	Feb 2013	Spam campaign The Dragonfly group has used at least three infection tactics against targets in the energy sector. The earliest method was an email spear phishing campaign, which saw selected executives and senior employees in target companies receive emails containing a malicious PDF attachment. Infected emails had one of two subject lines: "The account" or "Settlement of delivery problem". <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf>
	Jun 2013	Watering Hole Attacks using Lightsout In June 2013, the attackers shifted their focus to watering hole attacks. They compromised a number of energy-related websites and injected an iframe into each of them. This iframe then redirected visitors to another compromised legitimate website hosting the Lightsout exploit kit. This in turn exploited either Java or Internet Explorer in order to drop Oldrea or Karagany on the victim's computer.
	Sep 2013	Watering Hole Attacks using Hello

		In September 2013, Dragonfly began using a new version of this exploit kit, known as the Hello exploit kit. The landing page for this kit contains JavaScript which fingerprints the system, identifying installed browser plugins. The victim is then redirected to a URL which in turn determines the best exploit to use based on the information collected.
	2013	Trojanized software The most ambitious attack vector used by Dragonfly was the compromise of a number of legitimate software packages. Three different ICS equipment providers were targeted and malware was inserted into the software bundles they had made available for download on their websites
	Feb 2014	LightsOut EK Targets Energy Sector Late last year, the story broke that threat actors were targeting the energy sector with Remote Access Tools and Intelligence gathering malware. It would seem that the attackers responsible for this threat are back for more. This particular APT struck late February between 2/24-2/26. <https://www.zscaler.com/blogs/research/lightsout-ek-targets-energy-sector>
	Dec 2015	Attack on Energy Companies in the Ukraine According to a statement posted this week on the official website of the Ukrainian security service SBU, Russian special services allegedly planted malware on the networks of several regional power companies. The malicious software is said to have been discovered by employees of the SBU. The SBU said the attackers also flooded the targeted companies' technical support phone lines. The agency removed the malware and launched an investigation. Just before Christmas, power outages were reported in the Ivano-Frankivsk Oblast region of Ukraine. The outages were blamed on outsiders who remotely tampered with automatic control systems. The power company responsible for the region also reported that its call center suffered a technical failure caused by a barrage of calls. <https://ssu.gov.ua/sbu/control/uk/publish/article?art_id=170951&cat_id=39574>
	2016	This report by Kaspersky Lab ICS CERT presents information on identified servers that have been infected and used by the group. The report also includes the findings of an analysis of several webservers compromised by the Energetic Bear group during 2016 and in early 2017. <https://securelist.com/energetic-bear-crouching-yeti/85345/>
	Dec 2016	Power outage at Ukrenergo in the Ukraine Preliminary findings indicate that workstations and Supervisory Control and Data Acquisition (SCADA) systems, linked to the 330 kilowatt sub-station "North", were influenced by external sources outside normal parameters, Ukrenergo said in comments emailed to Reuters. <https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA> <https://dragos.com/wp-content/uploads/CrashOverride-01.pdf>

	Apr 2017	Breach of EirGrid in the UK The breach of the Vodafone network allowed the hackers to create a type of wiretap known as Generic Routing Encapsulation (GRE) to tunnel into EirGrid's Vodafone router located in Shotton. <https://www.independent.ie/irish-news/statesponsored-hackers-targeted-eirgrid-electricity-network-in-devious-attack-36005921.html>
	May 2017	Watering Hole Attack on Turkish critical infrastructure Through our web crawling network, we were able to determine that a website belonging to a Turkish energy company was being used in a watering hole attack targeting people associated with Turkish critical infrastructure. Compromised via a supply chain attack, the site was injected with SMB credential-harvesting malware. <https://www.riskiq.com/blog/labs/energetic-bear/>
Information	<https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks> <https://www.kaspersky.com/resource-center/threats/crouching-yeti-energetic-bear-malware-threat> <https://www.sans.org/reading-room/whitepapers/ICS/impact-dragonfly-malware-industrial-control-systems-36672>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0035/>	

Equation Group

Names	Equation Group *(real name)* Tilded Team *(CrySys)*
Country	USA
Sponsor	State-sponsored, believed to be tied to the NSA's Tailored Access Operations unit.
Motivation	Sabotage and destruction
Description	(Ars Technica) Kaspersky researchers have documented 500 infections by Equation Group in at least 42 countries, with Iran, Russia, Pakistan, Afghanistan, India, Syria, and Mali topping the list. Because of a self-destruct mechanism built into the malware, the researchers suspect that this is just a tiny percentage of the total; the actual number of victims likely reaches into the tens of thousands. A long list of almost superhuman technical feats illustrate Equation Group's extraordinary skill, painstaking work, and unlimited resources. They include: • The use of virtual file systems, a feature also found in the highly sophisticated Regin malware. Recently published documents provided by Ed Snowden indicate that the NSA used Regin to infect the partly state-owned Belgian firm Belgacom. • The stashing of malicious files in multiple branches of an infected computer's registry. By encrypting all malicious files and storing them in multiple branches of a computer's Windows registry, the infection was impossible to detect using antivirus software. • Redirects that sent iPhone users to unique exploit Web pages. In addition, infected machines reporting to Equation Group command servers identified themselves as Macs, an indication that the group successfully compromised both iOS and OS X devices. • The use of more than 300 Internet domains and 100 servers to host a sprawling command and control infrastructure. • USB stick-based reconnaissance malware to map air-gapped networks, which are so sensitive that they aren't connected to the Internet. Both Stuxnet and the related Flame malware platform also had the ability to bridge airgaps. • An unusual if not truly novel way of bypassing code-signing restrictions in modern versions of Windows, which require that all third-party software interfacing with the operating system kernel be digitally signed by a recognized certificate authority. To circumvent this restriction, Equation Group malware exploited a known vulnerability in an already signed driver for CloneCD to achieve kernel-level code execution. Taken together, the accomplishments led Kaspersky researchers to conclude that Equation Group is probably the most sophisticated computer attack group in the world, with technical skill and resources that rival the groups that developed Stuxnet and the Flame espionage malware. Their arsenal of 0-day cyber weapons was stolen by an actor Shadow Brokers, who leaked a large section on the internet[4] and tried to sell the rest afterward. Most notable among the dumps were 0-days such as ETERNALBLUE and ETERNALROMANCE that were used by other groups for the creation of infamous ransomware explosions such as WannaCry and NotPetya.

---

[4] See ThaiCERT Whitepaper "Shadow Broker - Equation Group Hack"

	Equation Group is also linked to the creation of the Stuxnet worm that aimed to sabotage nuclear reactors in Iran in 2010, and/or the "follow-up" threats Duqu, Flame or Gauss. Although neither country has openly admitted responsibility, Stuxnet is believed to be a jointly built American/Israeli (allegedly, Unit 8200) cyber weapon. <https://en.wikipedia.org/wiki/Stuxnet>
Observed	Sectors: Aerospace, Defense, Energy, Government, Media, Nanotechnology, Nuclear research, Oil and gas, Telecommunications, Transportation, Islamic activists and scholars, and companies developing cryptographic technologies. Countries: Afghanistan, Bangladesh, Belgium, Brazil, Ecuador, France, Germany, Hong Kong, India, Iran, Iraq, Israel, Kazakhstan, Lebanon, Libya, Malaysia, Mali, Mexico, Nigeria, Pakistan, Palestine, Philippines, Qatar, Russia, Singapore, Somalia, South Africa, Sudan, Switzerland, Syria, UAE, UK, USA and Yemen.
Tools used	DarkPulsar, DOUBLEFANTASY, DoublePulsar, EQUATIONDRUG, EQUATIONLASER, EQUESTRE, FANNY, GROK, Lambert, Plexor, Regin, TRIPLEFANTASY and many others.
Information	<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0020/>

Emissary Panda, APT 27, LuckyMouse, Bronze Union

Names	Emissary Panda *(CrowdStrike)* APT 27 *(Mandiant)* LuckyMouse *(Kaspersky)* Bronze Union *(Scureworks)* TG-3390 *(SecureWorks)* TEMP.Hippo *(Symantec)* Group 35 *(Talos)*
Country	China
Motivation	Information theft and espionage
Description	Threat Group-3390 is a Chinese threat group that has extensively used strategic Web compromises to target victims. The group has been active since at least 2010 and has targeted organizations in the aerospace, government, defense, technology, energy, and manufacturing sectors.
Observed	Sectors: Defense, Education, Embassies, Government, Technology, Telecommunications and Think Tanks. Countries: Australia, Canada, China, Hong Kong, India, Iran, Israel, Japan, Middle East, Philippines, Russia, South Korea, Taiwan, Thailand, Tibet, UK and USA.
Tools used	Antak, ASPXSpy, China Chopper, Gh0st RAT, gsecdump, HTTPBrowser, Hunter, HyperBro, Mimikatz, Nishang, OwaAuth, PlugX, PSExec, Upatre, Windows Credential Editor and ZipToken.
Operations performed	2010	Operation "Iron Tiger" Operation Iron Tiger is a targeted attack campaign discovered to have stolen trillions of data from defense contractors in the US, including stolen emails, intellectual property, strategic planning documents – data and records that could be used to destabilize an organization. <https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/blob/master/2015/2015.09.17.Operation_Iron_Tiger/wp-operation-iron-tiger.pdf> <https://www.cfr.org/interactive/cyber-operations/iron-tiger>
	2015	Penetration of networks for industrial espionage Designated as Threat Group 3390 and nicknamed "Emissary Panda" by researchers, the hacking group has compromised victims' networks largely through "watering hole" attacks launched from over 100 compromised legitimate websites, sites picked because they were known to be frequented by those targeted in the attack. <https://arstechnica.com/information-technology/2015/08/newly-discovered-chinese-hacking-group-hacked-100-websites-to-use-as-watering-holes/>
	Jul 2017	Operation "PZChao" The past few years have seen high-profile cyber-attacks shift to damaging the targets' digital infrastructures to stealing highly sensitive data, silently monitoring the victim and constantly laying the ground for a new wave of attacks. This is also the case of a custom-built piece of malware that we have been monitoring for several months as it wrought havoc in Asia. Our threat intelligence systems picked up the first indicators of

		compromise in July last year, and we have kept an eye on the threat ever since. <https://labs.bitdefender.com/2018/02/operation-pzchao-a-possible-return-of-the-iron-tiger-apt/>
	Mar 2018	Campaign targeting a national data center in the Central Asia The choice of target made this campaign especially significant – it meant the attackers gained access to a wide range of government resources at one fell swoop. We believe this access was abused, for example, by inserting malicious scripts in the country's official websites in order to conduct watering hole attacks. <https://securelist.com/luckymouse-hits-national-data-center/86083/>
	Apr 2019	In April 2019, Unit 42 observed the Emissary Panda (AKA APT27, TG-3390, Bronze Union, Lucky Mouse) threat group installing webshells on Sharepoint servers to compromise Government Organizations of two different countries in the Middle East. <https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/>
Information		<https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage> <https://www.secureworks.com/research/bronze-union>
MITRE ATT&CK		<https://attack.mitre.org/groups/G0027/>

FIN4, Wolf Spider

Names	FIN4 *(FireEye)* Wolf Spider *(CrowdStrike)*
Country	Romania
Motivation	Financial gain
Description	(FireEye) FireEye tracks a threat group that we call "FIN4," whose intrusions seem to have a different objective: to obtain an edge in stock trading. FIN4 appears to conduct intrusions that are focused on a single objective: obtaining access to insider information capable of making or breaking the stock prices of public companies. The group specifically targets the emails of C-level executives, legal counsel, regulatory, risk, and compliance personnel, and other individuals who would regularly discuss confidential, market-moving information. FIN4 has targeted over 100 companies since at least mid-2013. All of the targeted organizations are either public companies or advisory firms that provide services to public companies (such as investor relations, legal, and investment banking firms). Over two-thirds of the targeted organizations are healthcare and pharmaceutical companies. FIN4 probably focuses on these types of organizations because their stocks can move dramatically in response to news of clinical trial results, regulatory decisions, or safety and legal issues.
Observed	Sectors: Financial, Healthcare and Pharmaceutical.
Tools used	
Information	<https://www.fireeye.com/blog/threat-research/2014/11/fin4_stealing_insid.html>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0085/>

FIN5

Names	FIN5 *(FireEye)*
Country	[Unknown]
Motivation	Financial gain
Description	FIN5 is a financially motivated threat group that has targeted personally identifiable information and payment card information. The group has been active since at least 2008 and has targeted the restaurant, gaming, and hotel industries. The group is made up of actors who likely speak Russian. (DarkReading) No 0days. No spear-phishing, either: The cybercriminal group tied to numerous payment card breaches including Goodwill and best known by its so-called "RawPOS" malware employed legitimate user credentials to access its targets' networks. Researchers at FireEye here today shared their recent findings on this prolific and long-running cybercrime gang that has been the subject of multiple Visa security alerts to merchants. The RawPOS memory scraper malware has been infecting the lodging industry in epidemic proportions over the past year, and is considered one of the first memory scrapers to target point-of-sale systems. FireEye has dubbed the cybercrime gang FIN5. "One of the most unique things about FIN5 is that in every intrusion we responded to where FIN5 has been active, legitimate access was identified. They had valid user credentials to remotely log into the network," said Barry Vengerik, principal threat analyst at FireEye. "No sexy zero-days, no remote exploits -- not even spear-phishing. They had credentials from somewhere." FIN5, which earlier this year was profiled by researchers at Trend Micro and has been in action since at least 2008, uses real credentials from the victim organization's virtual private network, Remote Desktop Protocol, Citrix, or VNC. Vengerik says the attackers got those credentials via third parties associated with the victims' POS systems.
Observed	Sectors: Gaming and Hospitality.
Tools used	FLIPSIDE, pwdump, RawPOS, SDelete and Windows Credential Editor.
MITRE ATT&CK	<https://attack.mitre.org/groups/G0053/>

FIN6, Skeleton Spider

Names	FIN6 *(FireEye)* Skeleton Spider *(CrowdStrike)*
Country	[Unknown]
Motivation	Financial gain
Description	FIN6 is a cybercrime group that has stolen payment card data and sold it for profit on underground marketplaces. This group has aggressively targeted and compromised point of sale (PoS) systems in the hospitality and retail sectors. (FireEye) FIN6 is a cybercriminal group intent on stealing payment card data for monetization. In 2015, FireEye Threat Intelligence supported several Mandiant Consulting investigations in the hospitality and retail sectors where FIN6 actors had aggressively targeted and compromised point-of-sale (POS) systems, making off with millions of payment card numbers. Through iSIGHT, we learned that the payment card numbers stolen by FIN6 were sold on a "card shop" — an underground criminal marketplace used to sell or exchange payment card data.
Observed	Sectors: Hospitality and Retail.
Tools used	AbaddonPOS, Cobalt Strike, FrameworkPOS, GRABNEW, Grateful POS, LockerGoga, Ryuk, Windows Credential Editor and WMI.
Operations performed	Jan 2019	Over the past 8-10 weeks, Morphisec has been tracking multiple sophisticated attacks targeting Point of Sale thin clients globally. More specifically, on the 6th of February we identified an extremely high number of prevention events stopping Cobalt Strike backdoor execution, with some of the attacks expressly targeting Point of Sale VMWare Horizon thin clients. <http://blog.morphisec.com/new-global-attack-on-point-of-sale-systems>
Information	<https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html> <https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin6.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0037/>

FIN7

Names	FIN7 *(FireEye)*
Country	Russia
Motivation	Financial gain
Description	FIN7 is a financially-motivated threat group that has primarily targeted the U.S. retail, restaurant, and hospitality sectors since mid-2015. They often use point-of-sale malware. A portion of FIN7 was run out of a front company called Combi Security. FIN7 is sometimes referred to as Carbanak, Anunak, but these appear to be two groups using the same Carbanak malware and are therefore tracked separately. The reports about arrests made of the mastermind of Carbanak, Anunak instead of FIN7. However, security research teams keep referring to this arrest for all FIN7 activities since.
Observed	Sectors: Casinos and Gaming, Construction, Education, Energy, Financial, Government, High-Tech, Hospitality, Retail, Technology, Telecommunications, Transportation and Travel. Countries: Europe and USA.
Tools used	Astra, Bateleur, Carbanak, Cobalt Strike, Griffon, HALFBAKED, POWERSOURCE, SQLRAT and TEXTMATE.
Operations performed	Feb 2017	In late February 2017, FireEye as a Service (FaaS) identified a spear phishing campaign that appeared to be targeting personnel involved with United States Securities and Exchange Commission (SEC) filings at various organizations. All of the observed intended recipients of the spear phishing campaign appeared to be involved with SEC filings for their respective organizations. <https://www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html>
	Mar 2017	Two recent fileless malware campaigns targeting financial institutions, government agencies and other enterprises have been linked to the same attack group. The campaigns, disclosed by Kaspersky Lab and Cisco's Talos research outfit in the last five weeks, made extensive use of fileless malware and known penetration testing tools and utilities to spy on organizations and move data and money off of networks. <https://threatpost.com/fileless-malware-campaigns-tied-to-same-attacker/124369/>
	Apr 2017	In a newly-identified campaign, FIN7 modified their phishing techniques to implement unique infection and persistence mechanisms. FIN7 has moved away from weaponized Microsoft Office macros in order to evade detection. This round of FIN7 phishing lures implements hidden shortcut files (LNK files) to initiate the infection and VBScript functionality launched by mshta.exe to infect the victim. <https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html>

	Jul 2017	Proofpoint researchers have uncovered that the threat actor commonly referred to as FIN7 has added a new JScript backdoor called Bateleur and updated macros to its toolkit. <https://www.proofpoint.com/us/threat-insight/post/fin7carbanak-threat-actor-unleashes-bateleur-jscript-backdoor>
	2017	Leveraging Shim Databases for Persistence A unique aspect of the incidents was how the group installed the CARBANAK backdoor for persistent access. Mandiant identified that the group leveraged an application shim database to achieve persistence on systems in multiple environments. The shim injected a malicious in-memory patch into the Services Control Manager ("services.exe") process, and then spawned a CARBANAK backdoor process. <https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-databases-persistence.html>
	Jun 2017	Highly sophisticated fileless attack targeting restaurants across the US On June 7, 2017, Morphisec Lab identified a new, highly sophisticated fileless attack targeting restaurants across the US. The ongoing campaign allows hackers to seize system control and install a backdoor to steal financial information at will. It incorporates some never before seen evasive techniques that allow it to bypass most security solutions – signature and behavior based. <http://blog.morphisec.com/fin7-attacks-restaurant-industry>
	Oct 2017	Attack to target banks and the enterprise Like clockwork, FIN7 again unleashed a new attack able to bypass almost every security solution. The attack, which took place between October 8 to 10, 2017, is yet another demonstration of the high-paced innovation by threat actors. <http://blog.morphisec.com/fin7-attack-modifications-revealed>
	May 2018	New Attack Panel and Malware Samples Flashpoint analysts recently uncovered a new attack panel used by this group in campaigns they have called Astra. The panel, written in PHP, functions as a script-management system, pushing attack scripts down to compromised computers. <https://www.flashpoint-intel.com/blog/fin7-revisited-inside-astra-panel-and-sqlrat-malware/>
	2018	High-profile breaches including Red Robin, Chili's, Arby's, Burgerville, Omni Hotels and Saks Fifth Avenue, among many others. Fifth Avenue, Saks Off 5th, and Lord & Taylor department stores—all owned by The Hudson's Bay Company—acknowledged a data breach impacting more than five million credit and debit card numbers. The culprits? The same group that's spent the last few years pulling off data heists from Omni Hotels & Resorts, Trump Hotels, Jason's Deli, Whole Foods, Chipotle: A mysterious group known as Fin7. <http://blog.morphisec.com/fin7-not-finished-morphisec-spots-new-campaign>
	Nov 2018	In this blog post, we present our findings on two campaigns, which occurred in the first and second weeks of November. These campaigns follow patterns similar to those presented by FireEye in

		August but with just enough variations to bypass many security vendors. <http://blog.morphisec.com/fin7-not-finished-morphisec-spots-new-campaign>
	2018-2019	In 2018-2019, researchers of Kaspersky Lab's Global Research and Analysis Team analyzed various campaigns that used the same Tactics Tools and Procedures (TTPs) as the historic FIN7, leading the researchers to believe that this threat actor had remained active despite the 2018 arrests. In addition, during the investigation, we discovered certain similarities to other attacker groups that seemed to share or copy the FIN7 TTPs in their own operations. <https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/>
Information		<https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html> <https://atr-blog.gigamon.com/2017/07/25/footprints-of-fin7-tracking-actor-patterns-part-1> <https://atr-blog.gigamon.com/2017/07/26/footprints-of-fin7-tracking-actor-patterns-part-2/>
MITRE ATT&CK		<https://attack.mitre.org/groups/G0046/>

FIN8

Names	FIN8 *(FireEye)*
Country	[Unknown]
Motivation	Financial gain
Description	(FireEye) We attribute the use of this EoP to a financially motivated threat actor. In the past year, not only have we observed this group using similar infrastructure and tactics, techniques, and procedures (TTPs), but they are also the only group we have observed to date who uses the downloader PUNCHBUGGY and POS malware PUNCHTRACK. Designed to scrape both Track 1 and Track 2 payment card data, PUNCHTRACK is loaded and executed by a highly obfuscated launcher and is never saved to disk.

This actor has conducted operations on a large scale and at a rapid pace, displaying a level of operational awareness and ability to adapt their operations on the fly. These abilities, combined with targeted usage of an EoP exploit and the reconnaissance required to individually tailor phishing emails to victims, potentially speaks to the threat actors' operational maturity and sophistication.

FireEye identified more than 100 organizations in North America that fell victim to this campaign. |
Observed	Sectors: Hospitality and Retail. Countries: USA.
Tools used	PunchBuggy, PunchTrack and ShellTea.
Operations performed	Mar 2016	Tailored spear-phishing campaigns In March 2016, a financially motivated threat actor launched several tailored spear phishing campaigns primarily targeting the retail, restaurant, and hospitality industries. The emails contained variations of Microsoft Word documents with embedded macros that, when enabled, downloaded and executed a malicious downloader that we refer to as PUNCHBUGGY. <https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html>
	2018	In early 2017, FIN8 began using environment variables paired with PowerShell's ability to receive commands via stdin (standard input) to evade detection based on process command line arguments. In the February 2017 phishing document "COMPLAINT Homer Glynn.doc" <https://www.fireeye.com/blog/threat-research/2017/06/obfuscation-in-the-wild.html>
	Mar 2019	During the period of March to May 2019, Morphisec Labs observed a new, highly sophisticated variant of the ShellTea / PunchBuggy backdoor malware that attempted to infiltrate a number of machines within the network of a customer in the hotel-entertainment industry. It is believed that the malware was deployed as a result of several phishing attempts. <http://blog.morphisec.com/security-alert-fin8-is-back>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0061/>

FIN10

Names	FIN10 *(FireEye)*
Country	[Unknown]
Motivation	Financial gain
Description	(FireEye) FireEye has observed multiple targeted intrusions occurring in North America — predominately in Canada — dating back to at least 2013 and continuing through at least 2016, in which the attacker(s) have compromised organizations' networks and sought to monetize this illicit access by exfiltrating sensitive data and extorting victim organizations. In some cases, when the extortion demand was not met, the attacker(s) destroyed production Windows systems by deleting critical operating system files and then shutting down the impacted systems. Based on near parallel TTPs used by the attacker(s) across these targeted intrusions, we believe these clusters of activity are linked to a single, previously unobserved actor or group that we have dubbed FIN10.
Observed	Sectors: Casinos and Mining. Countries: Canada and USA.
Tools used	Empire and SplinterRAT.
Information	<https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin10.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0051/>

Flying Kitten, Ajax Security Team

Names	Flying Kitten *(CrowdStrike)* Ajax Security Team *(FireEye)* Group 26 *(Talos)*
Country	Iran
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	(FireEye) Members of this group have accounts on popular Iranian hacker forums such as ashiyane[.]org and shabgard[.]org, and they have engaged in website defacements under the group name "AjaxTM" since 2010. By 2014, the Ajax Security Team had transitioned from performing defacements (their last defacement was in December 2013) to malware-based espionage, using a methodology consistent with other advanced persistent threat actors in this region. (Crowdstrike) CrowdStrike Intelligence has also been tracking and reporting internally on this threat group since mid-January 2014 under the name FLYING KITTEN, and since that time has seen targeting of multiple U.S.-based defense contractors as well as political dissidents.
Observed	Sectors: Defense and dissidents. Countries: USA.
Tools used	Sayyad and Stealer.
Operations performed	2013	Operation "Saffron Rose" <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf>
Information	<https://www.crowdstrike.com/blog/cat-scratch-fever-crowdstrike-tracks-newly-reported-iranian-actor-flying-kitten/>

Gallmaker

Names	Gallmaker *(Symantec)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(Symantec) Symantec researchers have uncovered a previously unknown attack group that is targeting government and military targets, including several overseas embassies of an Eastern European country, and military and defense targets in the Middle East. This group eschews custom malware and uses living off the land (LotL) tactics and publicly available hack tools to carry out activities that bear all the hallmarks of a cyber espionage campaign. The group, which we have given the name Gallmaker, has been operating since at least December 2017, with its most recent activity observed in June 2018.
Observed	Sectors: Defense, Embassies and Government. Countries: Eastern Europe and Middle East.
Tools used	
Information	<https://www.symantec.com/blogs/threat-intelligence/gallmaker-attack-group>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0084/>

Gamaredon Group

Names	Gamaredon Group *(Palo Alto)*
Country	Russia
Sponsor	State-sponsored, FSB 16th & 18th Centers
Motivation	Information theft and espionage
Description	(Lookingglass) The Lookingglass Cyber Threat Intelligence Group (CTIG) has been tracking an ongoing cyber espionage campaign named "Operation Armageddon". The name was derived from multiple Microsoft Word documents used in the attacks. "Armagedon" (spelled incorrectly) was found in the "Last Saved By" and "Author" fields in multiple Microsoft Word documents. Although continuously developed, the campaign has been intermittently active at a small scale, and uses unsophisticated techniques. The attack timing suggests the campaign initially started due to Ukraine's decision to accept the Ukraine---European Union Association Agreement (AA). The agreement was designed to improve economic integrations between Ukraine and the European Union. Russian leaders publicly stated that they believed this move by Ukraine directly threatened Russia's national security. Although initial steps to join the Association occurred in March 2012, the campaign didn't start until much later (mid-2013), as Ukraine and the EU started to more actively move towards the agreement. Russian actors began preparing for attacks in case Ukraine finalized the AA. The earliest identified modification timestamp of malware used in this campaign is June 26, 2013. A group of files with modification timestamps between August 12 and September 16, 2013 were used in the first wave of spear-phishing attacks, targeting government officials prior to the 10th Yalta Annual Meeting: "Changing Ukraine in a Changing World: Factors of Success."
Observed	Sectors: Defense, Government and Law enforcement. Countries: Ukraine
Tools used	FRAUDROP, Gamaredon, Pteranodon and Resetter.

Operations performed	Apr 2019	The discovered attack appears to be designed to lure military personnel: it leverages a legit document of the "State of the Armed Forces of Ukraine" dated back in the 2nd April 2019. <https://blog.yoroi.company/research/the-russian-shadow-in-eastern-europe-ukrainian-mod-campaign/>
	May 2019	The Gamaredon attacks against Ukraine doesn't seem to have stopped. After a month since our last report we spotted a new suspicious email potentially linked to the Gamaredon group. <https://blog.yoroi.company/research/the-russian-shadow-in-eastern-europe-a-month-later/>

Information	<https://www.lookingglasscyber.com/wp-content/uploads/2015/08/Operation_Armageddon_Final.pdf> <https://unit42.paloaltonetworks.com/unit-42-title-gamaredon-group-toolset-evolution/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0047/>

GCMAN

Names	GCMAN *(Kaspersky)*
Country	[Unknown]
Motivation	Financial gain
Description	(Kaspersky) A second group, which we call GCMAN because the malware is based on code compiled on the GCC compiler, emerged recently using similar techniques to the Corkow, Metel Group to infect banking institutions and attempt to transfer money to e-currency services. The initial infection mechanism is handled by spear-phishing financial institution targets with e-mails carrying a malicious RAR archive to. Upon opening the RAR archive, an executable is started instead of a Microsoft Word document, resulting in infection. Once inside the network, the GCMAN group uses legitimate and penetration testing tools such as Putty, VNC, and Meterpreter for lateral movement. Our investigation revealed an attack where the group then planted a cron script into bank's server, sending financial transactions at the rate of $200 per minute. A time-based scheduler was invoking the script every minute to post new transactions directly to upstream payment processing system. This allowed the group to transfer money to multiple e-currency services without these transactions being reported to any system inside the bank.
Observed	Sectors: Financial. Country: Russia.
Tools used	Malicious RAR archives, Putty, VNC and Meterpreter.
Information	<https://securelist.com/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/73638/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0036/>

GhostNet, Snooping Dragon

Names	GhostNet *(Information Warfare Monitor)* Snooping Dragon (*UCAM*)
Country	China
Motivation	Information theft and espionage
Description	(Information Warfare Monitor) Cyber espionage is an issue whose time has come. In this second report from the Information Warfare Monitor, we lay out the findings of a 10-month investigation of alleged Chinese cyber spying against Tibetan institutions. The investigation, consisting of fieldwork, technical scouting, and laboratory analysis, discovered a lot more. The investigation ultimately uncovered a network of over 1,295 infected hosts in 103 countries. Up to 30% of the infected hosts are considered high-value targets and include computers located at ministries of foreign affairs, embassies, international organizations, news media, and NGOs. The Tibetan computer systems we manually investigated, and from which our investigations began, were conclusively compromised by multiple infections that gave attackers unprecedented access to potentially sensitive information. (UCAM) Attacks on the Dalai Lama's Private Office The OHHDL started to suspect it was under surveillance while setting up meetings be-tween His Holiness and foreign dignitaries. They sent an email invitation on behalf of His Holiness to a foreign diplomat, but before they could follow it up with a courtesy telephone call, the diplomat's office was contacted by the Chinese government and warned not to go ahead with the meeting. The Tibetans wondered whether a computer compromise might be the explanation; they called ONI Asia who called us. (Until May 2008, the first author was employed on a studentship funded by the OpenNet Initiative and the second author was a principal investigator for ONI.) Also see Shadow Network.
Observed	Sectors: Embassies, Government, Media and NGOs. 1,295 infected computers in 103 countries, including the Dalai Lama, the ministries of foreign affairs of Bangladesh, Barbados, Bhutan, Brunei, Indonesia, Iran, Latvia and Philippines; embassies of Cyprus, Germany, India, Indonesia, Malta, Pakistan, Portugal, Romania, South Korea, Taiwan and Thailand; the ASEAN (Association of Southeast Asian Nations) Secretariat, SAARC (South Asian Association for Regional Cooperation), and the Asian Development Bank; news organizations; and an unclassified computer located at NATO headquarters.
Tools used	Gh0st RAT and Skype.
Counter operations	Taken down by the Shadowserver Foundation.
Information	<http://www.nartv.org/mirror/ghostnet.pdf> <https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf> <https://en.wikipedia.org/wiki/GhostNet>

Goblin Panda, Cycldek

Names	Goblin Panda *(CrowdStrike)* Cycldek *(Kaspersky)*
Country	China
Motivation	Information theft and espionage
Description	(CrowdStrike) CrowdStrike first observed Goblin Panda activity in September 2013 when indicators of its activity were discovered on the network of a technology company operating in multiple sectors. Malware variants primarily used by this actor include PlugX and HttpTunnel. This actor focuses a significant amount of its targeting activity on entities in Southeast Asia, particularly Vietnam. Heavy activity was observed in the late spring and early summer of 2014 when tensions between China and other Southeast Asian nations were high, due to conflict over territory in the South China Sea. Goblin Panda targets have been primarily observed in the defense, energy, and government sectors.
Observed	Sectors: Defense and Energy and Government. Countries: India, Indonesia, Laos, Malaysia, Philippines, USA and Vietnam.
Tools used	HttpTunnel, NewCore, PlugX, QCRat, Sisfader and ZeGhost.
Information	<https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-august-goblin-panda/> <https://www.fortinet.com/blog/threat-research/cta-security-playbook--goblin-panda.html>

Goldmouse

Names	Goldmouse *(360)* APT-C-27 *(360)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(360) On March 17, 2019, 360 Threat Intelligence Center captured a target attack sample against the Middle East by exploiting WinRAR vulnerability (CVE-2018-20250), and it seems that the attack is carried out by the Goldmouse APT group (APT-C-27). There is a decoy Word document inside the archive regarding terrorist attacks to lure the victim into decompressing. When the archive gets decompressed on the vulnerable computer, the embedded njRAT backdoor (Telegram Desktop.exe) will be extracted to the startup folder and then triggered into execution if the victim restarts the computer or performs re-login. After that, the attacker is capable to control the compromised device.
Observed	Countries: Middle East.
Tool used	GoldenRAT, njRAT and a WinRAR exploit.
Information	<https://ti.360.net/blog/articles/apt-c-27-(goldmouse):-suspected-target-attack-against-the-middle-east-with-winrar-exploit-en/>

Gorgon Group

Names	Gorgon Group *(Palo Alto)* Subaat *(Palo Alto)*
Country	Pakistan
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	Gorgon Group is a threat group consisting of members who are suspected to be Pakistan-based or have other connections to Pakistan. The group has performed a mix of criminal and targeted attacks, including campaigns against government organizations in the United Kingdom, Spain, Russia, and the United States.
Observed	Sectors: Government. Countries: Russia, Spain, UK and USA.
Tools used	Crimson, LokiBot, NanoCore RAT, njRAT, QuasarRAT, Remcos and Revenge RAT.
Operations performed	Jul 2017	Small wave of phishing emails targeting a US-based government organization. Within the 43 emails we observed, we found that three unique files were delivered, which consisted of two RTFs and a Microsoft Excel file. Both RTFs exploited CVE-2012-0158 and acted as downloaders to ultimately deliver the QuasarRAT malware family. The downloaders made use of the same shellcode, with minor variances witnessed between them. Additionally, the RTFs made use of heavy obfuscation within the documents themselves, making it more difficult to extract the embedded shellcode. <https://unit42.paloaltonetworks.com/unit42-tracking-subaat-targeted-phishing-attacks-point-leader-threat-actors-repository/>
	Feb 2018	In addition to the numerous targeted attacks, Unit 42 discovered that the group also performed a litany of attacks and operations around the globe, involving both criminal as well as targeted attacks. Starting in February 2018, Palo Alto Networks Unit 42 identified a campaign of attacks performed by members of Gorgon Group targeting governmental organizations in the United Kingdom, Spain, Russia, and the United States. Additionally, during that time, members of Gorgon Group were also performing criminal operations against targets across the globe, often using shared infrastructure with their targeted attack operations. <https://unit42.paloaltonetworks.com/unit42-gorgon-group-slithering-nation-state-cybercrime/>
	Mar 2019	[Attribution unconfirmed] Aggah Campaign: Bit.ly, BlogSpot, and Pastebin Used for C2 in Large Scale Campaign In March 2019, Unit 42 began looking into an attack campaign that appeared to be primarily focused on organizations within a Middle Eastern country. Further analysis revealed that this activity is likely part of a much larger campaign impacting not only that region but also the United States, and throughout Europe and Asia. <https://unit42.paloaltonetworks.com/aggah-campaign-bit-ly-blogspot-and-pastebin-used-for-c2-in-large-scale-campaign/>

| MITRE ATT&CK | <https://attack.mitre.org/groups/G0078/> |

GozNym

Names	GozNym *(IBM)*
Country	[Several]
Motivation	Financial gain
Description	(IBM) IBM X-Force Research uncovered a Trojan hybrid spawned from the Nymaim and Gozi ISFB malware. It appears that the operators of Nymaim have recompiled its source code with part of the Gozi ISFB source code, creating a combination that is being actively used in attacks against more than 24 U.S. and Canadian banks, stealing millions of dollars so far. X-Force named this new hybrid GozNym. The new GozNym hybrid takes the best of both the Nymaim and Gozi ISFB malware to create a powerful Trojan. From the Nymaim malware, it leverages the dropper's stealth and persistence; the Gozi ISFB parts add the banking Trojan's capabilities to facilitate fraud via infected Internet browsers. The end result is a new banking Trojan in the wild.
Observed	Sectors: Financial. Countries: Canada, Poland and USA.
Tools used	GozNym, Nymaim and Gozi ISFB.
Operations performed	Apr 2016	Attacks against more than 24 U.S. and Canadian banks <https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/>
	Apr 2016	Attacks on banks in Poland <https://threatpost.com/attackers-behind-goznym-trojan-set-sights-on-europe/117647/>
	Jun 2016	Attacks on banks in the USA
	Aug 2016	Attacks on banks in Germany <https://threatpost.com/goznym-banking-trojan-targeting-german-banks/120075/>
Counter operations	• GozNym Malware: Cybercriminal Network Dismantled in International Operation (2019) <https://www.europol.europa.eu/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation>

Group5

Names	Group5 *(Citizen Lab)*
Country	Iran
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	(SecurityWeek) A threat actor using Iranian-language tools, Iranian hosting companies, operating from the Iranian IP space at times was observed targeting the Syrian opposition in an elaborately staged malware operation, Citizen Lab researchers reveal. The operation was first noticed in late 2015, when a member of the Syrian opposition flagged a suspicious email containing a PowerPoint slideshow, which led researchers to a watering hole website with malicious programs, malicious PowerPoint files, and Android malware. The threat actor was targeting Windows and Android devices of well-connected individuals in the Syrian opposition, researchers discovered. They called the actor Group5, because it targets Syrian opposition after regime-linked malware groups, the Syrian Electronic Army, ISIS (also known as the Islamic State or ISIL), and a group linked to Lebanon did the same in the past.
Observed	Countries: Syria.
Tools used	DroidJack, NanoCore RAT and njRAT.
MITRE ATT&CK	<https://attack.mitre.org/groups/G0043/>

Hidden Lynx, Aurora Panda

Names	Hidden Lynx *(Symantec)* Aurora Panda (CrowdStrike) Group 8 *(Talos)*
Country	China
Motivation	Information theft and espionage
Description	(Symantec) The Hidden Lynx group has been in operation since at least 2009 and is most likely a professional organization that offers a "hackers for hire" service. They have the capability to attack many organizations with concurrently running campaigns. They operate efficiently and move quickly and methodically. Based on these factors, the Hidden Lynx group would need to be a sizeable organization made up of between 50 and 100 individuals. Much of the attack infrastructure and tools used during these campaigns originate from network infrastructure in China. The Hidden Lynx group makes regular use of zero-day exploits and has the ability to rework and customize exploits quickly. They are methodical in their approach and they display a skillset far in advance of some other attack groups also operating in that region, such as the Comment Crew (also known as APT1). The Hidden Lynx group is an advanced persistent threat that has been in operation for at least four years and is breaking into some of the best-protected organizations in the world. With a zero-day attack already under their belt in 2013, they continue to operate at the leading edge of targeted attacks. This group appears to be closely associated with APT 17, Deputy Dog.
Observed	Sectors: Construction, Defense, Education, Financial, Food and Agriculture, Engineering, Healthcare, IT, Government, Media, Non-profit organizations, Pharmaceuticals, Retail and lawyers. Countries: Australia, Canada, China, France, Germany, Hong Kong, India, Japan, Russia, Singapore, South Korea, Taiwan, UK, Ukraine and USA.
Tools used	HiKit, Moudoor and Naid.
Operations performed	Jun 2012	VOHO campaign The VOHO campaign, first publicized by RSA, is one of the largest and most successful watering-hole attacks to date. The campaign combined both regional and industry-specific attacks and predominantly targeted organizations that operate in the United States. In a rapidly spreading two-phase attack, which started on June 25 and finished July 18, nearly 4,000 machines had downloaded a malicious payload. These payloads were being delivered to unsuspecting victims from legitimate websites that were strategically compromised. <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf>
	Jul 2012	Breach of the Bit9 website <https://blog.bit9.com/2013/02/08/bit9-and-our-customers-security/>
Counter operations	• Security vendors take action against Hidden Lynx malware (2014) <https://www.symantec.com/connect/blogs/security-vendors-take-action-against-hidden-lynx-malware>

Information	<https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf> <https://www.symantec.com/connect/blogs/hidden-lynx-professional-hackers-hire> <https://www.recordedfuture.com/hidden-lynx-analysis/>

Honeybee

Names	Honeybee *(McAfee)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(McAfee) McAfee Advanced Threat Research analysts have discovered a new operation targeting humanitarian aid organizations and using North Korean political topics as bait to lure victims into opening malicious Microsoft Word documents. Our analysts have named this Operation Honeybee, based on the names of the malicious documents used in the attacks. Advanced Threat Research analysts have also discovered malicious documents authored by the same actor that indicate a tactical shift. These documents do not contain the typical lures by this actor, instead using Word compatibility messages to entice victims into opening them. The Advanced Threat Research team also observed a heavy concentration of the implant in Vietnam from January 15–17.
Observed	Sectors: Those involved in humanitarian aid and inter-Korean affairs. Countries: South Korea to target Argentina, Canada, Indonesia, Japan, Singapore and Vietnam.
Tools used	SYSCON, Systeminfo and Tasklist
Information	<https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-uncovers-operation-honeybee-malicious-document-campaign-targeting-humanitarian-aid-groups/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0072/>

Hurricane Panda, Zirconium, APT 31

Names	Hurricane Panda *(CrowdStrike)* Zirconium *(Confiant)* APT 31 *(Mandiant)* TEMP.Avengers *(Symantec)*
Country	China
Motivation	Information theft and espionage
Description	(CrowdStrike) We have investigated their intrusions since 2013 and have been battling them nonstop over the last year at several large telecommunications and technology companies. The determination of this China-based adversary is truly impressive: they are like a dog with a bone. Hurricane Panda's preferred initial vector of compromise and persistence is a China Chopper webshell – a tiny and easily obfuscated 70 byte text file that consists of an 'eval()' command, which is then used to provide full command execution and file upload/download capabilities to the attackers. This script is typically uploaded to a web server via a SQL injection or WebDAV vulnerability, which is often trivial to uncover in a company with a large external web presence. Once inside, the adversary immediately moves on to execution of a credential theft tool such as Mimikatz (repacked to avoid AV detection). If they are lucky to have caught an administrator who might be logged into that web server at the time, they will have gained domain administrator credentials and can now roam your network at will via 'net use' and 'wmic' commands executed through the webshell terminal.
Observed	Sectors: Technology and Telecommunications.
Tools used	9002 RAT, China Chopper, Gh0st RAT, HiKit, Mimikatz, PlugX, Sakula RAT and Trochilus RAT.
Operations performed	2016	Malvertising Operation The Zirconium group successfully created and operated 28 fake ad agencies to distribute malvertising campaigns through 2017, buying an estimate of 1 billion ad views throughout the year, and reaching 62% of ad-monetized websites on a weekly basis. <https://blog.confiant.com/uncovering-2017s-largest-malvertising-operation-b84cd38d6b85> <https://blog.confiant.com/zirconium-was-one-step-ahead-of-chromes-redirect-blocker-with-0-day-2d61802efd0d>
Information	<https://www.crowdstrike.com/blog/cyber-deterrence-in-action-a-story-of-one-long-hurricane-panda-campaign/>

Icefog, Dagger Panda

Names	Icefog *(Kaspersky)* Dagger Panda *(CrowdStrike)*
Country	China, South Korea and Japan
Motivation	Information theft and espionage
Description	(Kaspersky) "Icefog" is an Advanced Persistent Threat that has been active since at least 2011, targeting mostly Japan and South Korea. Known targets include governmental institutions, military contractors, maritime and shipbuilding groups, telecom operators, industrial and high-tech companies and mass media. The name "Icefog" comes from a string used in the command-and-control server name in one of the samples. The command-and-control software is named "Dagger Three", in the Chinese language. During Icefog attacks, several other malicious tools and backdoors were uploaded to the victims' machines, for data exfiltration and lateral movement.
Observed	Sectors: Defense, Government, High-Tech, Maritime and Shipbuilding, Media, Telecommunications, Water and others. Countries: Australia, Austria, Belarus, Canada, China, France, Germany, Hong Kong, India, Italy, Japan, Kazakhstan, Malaysia, Maldives, Mongolia, Netherlands, Pakistan, Philippines, Russia, Singapore, South Korea, Sri Lanka, Taiwan, Tajikistan, Turkey, UK, USA and Uzbekistan.
Tools used	Dagger Three, Fucobha, Icefog and Javafog.
Operations performed	Jan 2014	The Icefog APT Hits US Targets With Java Backdoor Since the publication of our report, the Icefog attackers went completely dark, shutting down all known command-and-control servers. Nevertheless, we continued to monitor the operation by sinkholing domains and 119nalyzing victim connections. During this monitoring, we observed an interesting type of connection which seemed to indicate a Java version of Icefog, further to be referenced as "Javafog". <https://securelist.com/the-icefog-apt-hits-us-targets-with-java-backdoor/58209/>
	2015	"TOPNEWS" Campaign Target: Government, media, and finance organizations in Russia and Mongolia.
	2016	"APPER" Campaign Target: Kazach officials.
	2018	"WATERFIGHT" Campaign Target: Water source provider, banks, and government entities in Turkey, India, Kazakhstan, Uzbekistan, and Tajikistan.
	2018	"PHKIGHT" Campaign Target: An unknown entity in the Philippines
	2018-2019	"SKYLINE" Campaign Target: Organizations in Turkey and Kazakhstan. <https://www.zdnet.com/article/ancient-icefog-apt-malware-spotted-again-in-new-wave-of-attacks/>

Information	<https://media.kaspersky.com/en/icefog-apt-threat.pdf> <https://d2538mqrb7brka.cloudfront.net/wp-content/uploads/sites/43/2018/03/20133739/icefog.pdf> <https://speakerdeck.com/ashley920/into-the-fog-the-return-of-icefog-apt>

Inception Framework

Names	Inception Framework *(Symantec)*
Country	Russia
Motivation	Information theft and espionage
Description	(Symantec) Researchers from Blue Coat Labs have identified the emergence of a previously undocumented attack framework that is being used to launch highly targeted attacks in order to gain access to, and extract confidential information from, victims' computers. Because of the many layers used in the design of the malware, we've named it Inception—a reference to the 2010 movie "Inception" about a thief who entered peoples' dreams and stole secrets from their subconscious. Targets include individuals in strategic positions: Executives in important businesses such as oil, finance and engineering, military officers, embassy personnel and government officials. The Inception attacks began by focusing on targets primarily located in Russia or related to Russian interests, but have since spread to targets in other locations around the world. The preferred malware delivery method is via phishing emails containing trojanized documents. • Initially targeted at Russia, but expanding globally • Masterful identity cloaking and diversionary tactics • Clean and elegant code suggesting strong backing and top-tier talent • Includes malware targeting mobile devices: Android, Blackberry and iOS • Using a free cloud hosting service based in Sweden for command and control
Observed	Sectors: Defense, Embassies, Engineering, Financial, Government and Oil and gas. Countries: Afghanistan, Armenia, Austria, Azerbaijan, Belarus, Belgium, Brazil, Congo, Cyprus, France, Georgia, Germany, Greece, India, Indonesia, Iran, Italy, Jordan, Kazakhstan, Kenya, Kyrgyzstan, Lebanon, Lithuania, Malaysia, Moldova, Morocco, Mozambique, Oman, Pakistan, Paraguay, Qatar, Romania, Russia, Saudi Arabia, South Africa, Suriname, Switzerland, Tajikistan, Tanzania, Turkey, Turkmenistan, Uganda, Ukraine, UAE, USA, Uzbekistan, Venezuela and Vietnam.
Tools used	Inception, Lastacloud and many 0-day exploits.
Operations performed	Oct 2012	Operation "RedOctober" In October 2012, Kaspersky Lab's Global Research & Analysis Team initiated a new threat research after a series of attacks against computer networks of various international diplomatic service agencies. A large scale cyber-espionage network was revealed and analyzed during the investigation, which we called "Red October" (after famous novel "The Hunt For The Red October"). <https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/#8>
	May 2014	Hiding Behind Proxies Since 2014, Symantec has found evidence of a steady stream of attacks from the Inception Framework targeted at organizations on several continents. As time has gone by, the group has become ever more secretive, hiding behind an increasingly complex framework of proxies and cloud services. <https://www.symantec.com/blogs/threat-intelligence/inception-framework-hiding-behind-proxies>

	Aug 2014	Operation "Cloud Atlas" In August 2014, some of our users observed targeted attacks with a variation of CVE-2012-0158 and an unusual set of malware. We did a quick analysis of the malware and it immediately stood out because of certain unusual things that are not very common in the APT world. <https://securelist.com/cloud-atlas-redoctober-apt-is-back-in-style/68083/>
Information		<https://www.symantec.com/connect/blogs/blue-coat-exposes-inception-framework-very-sophisticated-layered-malware-attack-targeted-milit> <https://www.akamai.com/uk/en/multimedia/documents/white-paper/upnproxy-blackhat-proxies-via-nat-injections-white-paper.pdf>

Infy, Prince of Persia

Names	Infy *(Palo Alto)* Prince of Persia *(Palo Alto)* Operation Mermaid *(360)*	
Country	Iran	
Sponsor	State-sponsored	
Motivation	Information theft and espionage	
Description	Since early 2013, we have observed activity from a unique threat actor group, which we began to investigate based on increased activities against human right activists in the beginning of 2015. In line5with other research on the campaign, released prior to publication of this document, we have adopted the name "Infy", which is based on labels used in the infrastructure and its two families of malware agents. Thanks to information we have been able to collect during the course of our research, such as characteristics of the group's malware and development cycle, our research strongly supports the claim that the Infy group is of Iranian origin and potentially connected to the Iranian state. Amongst a backdrop of other incidents, Infy became one of the most frequently observed agents for attempted malware attacks against Iranian civil society beginning in late 2014, growing in use up to the February 2016 parliamentary election in Iran. After the conclusion of the parliamentary election, the rate of attempted intrusions and new compromises through the Infy agent slowed, but did not end. The trends witnessed in reports from recipients are reinforced through telemetry provided by design failures in more recent versions of the Infy malware.	
Observed	Sectors: Government and private sectors. Countries: Bahrain, Canada, China, Denmark, France, Germany, Iran, Israel, Italy, Russia, Saudi Arabia, Sweden, Syria, UK and USA.	
Tools used	Foudre and Infy.	
Operations performed	May 2015	In May 2015, Palo Alto Networks WildFire detected two e-mails carrying malicious documents from a genuine and compromised Israeli Gmail account, sent to an Israeli industrial organization. One e-mail carried a Microsoft PowerPoint file named "thanks.pps", the other a Microsoft Word document named "request.docx". <https://unit42.paloaltonetworks.com/prince-of-persia-infy-malware-active-in-decade-of-targeted-attacks/>
	Feb 2017	In February 2017, we observed an evolution of the "Infy" malware that we're calling "Foudre" ("lightning", in French). The actors appear to have learned from our previous takedown and sinkholing of their Command and Control (C2) infrastructure – Foudre incorporates new anti-takeover techniques in an attempt to avoid their C2 domains being sinkholed as we did in 2016. <https://unit42.paloaltonetworks.com/unit42-prince-persia-ride-lightning-infy-returns-foudre/>
Counter operation	• Prince of Persia – Game Over (2016) <https://unit42.paloaltonetworks.com/unit42-prince-of-persia-game-over/>	

Information	<https://www.blackhat.com/docs/us-16/materials/us-16-Guarnieri-Iran-And-The-Soft-War-For-Internet-Dominance-wp.pdf>

Iridium

Names	Iridium *(Resecurity)*
Country	Iran
Motivation	Information theft and espionage
Description	(Kaspersky) Iridium is an APT that uses proprietary techniques to bypass two-factor authentication for critical applications, according to security firm Resecurity. A researcher has attributed a recently publicized attack on Citrix' internal network to the Iranian-linked group known as Iridium – and said that the data heist involved 6 terabytes of sensitive data. The culprit is an APT that uses proprietary techniques to bypass two-factor authentication for critical applications and services for further unauthorized access to virtual private networks and single sign-on systems, according to Resecurity. "[Iridium] has hit more than 200 government agencies, oil and gas companies and technology companies, including Citrix Systems Inc.," they said. Threatpost has reached out for further details as to how the firm is linking the APT to the attack and will update this post accordingly.
Observed	Sectors: Government, Oil and gas and Technology.
Tools used	China Chopper, Ckife Webshells, LazyCat and reGeorge.
Operations performed	Dec 2018	Attacks on Australian government <https://www.scmagazine.com/home/security-news/apts-cyberespionage/iridium-cyberespionage-gang-behind-aussie-parliament-attacks/>
	Dec 2018	Breach of Citrix <https://threatpost.com/ranian-apt-6tb-data-citrix/142688/>
Information	<https://hub.packtpub.com/resecurity-reports-iriduim-behind-citrix-data-breach-200-government-agencies-oil-and-gas-companies-and-technology-companies-also-targeted/>

Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon

Names	Ke3chang *(FireEye)* Vixen Panda *(CrowdStrike)* APT 15 *(Mandiant)* GREF *(SecureWorks)* Playful Dragon *(FireEye)* Royal APT *(NCC Group)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	Ke3chang is a threat group attributed to actors operating out of China. Ke3chang has targeted several industries, including oil, government, military, and more.
Observed	Sectors: Aerospace, Airlines, Chemicals, Defense, Embassies, Energy, Government, High-Tech, Industry, Manufacturing, Mining, Oil and gas and Utilities. Countries: European Union, India and UK.
Tools used	Cobalt Strike, Metushy, Mimikatz, MirageFox, MS Exchange Tool, Royal DNS, RoyalCli, spwebmember, Systeminfo, Tasklist, TidePool and Winnti.
Operations performed	2010	Operation "Ke3chang" As the crisis in Syria escalates, FireEye research-ers have discovered a cyber espionage campaign, which we call "Ke3chang," that falsely advertises information updates about the ongoing crisis to compromise MFA networks in Europe. We believe that the Ke3chang attackers are operating out of China and have been active since at least 2010. However, we believe specific Syria-themed attacks against MFAs (codenamed by Ke3chang as "moviestar") began only in August 2013. The timing of the attacks precedes a G20 meeting held in Russia that focused on the crisis in Syria. <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf>
	May 2016	Little has been published on the threat actors responsible for Operation Ke3chang since the report was released more than two years ago. However, Unit 42 has recently discovered the actors have continued to evolve their custom malware arsenal. We've discovered a new malware family we've named TidePool. It has strong behavioral ties to Ke3chang and is being used in an ongoing attack campaign against Indian embassy personnel worldwide. This targeting is also consistent with previous attacker TTPs; Ke3chang historically targeted the Ministry of Affairs, and also conducted several prior campaigns against India. <https://unit42.paloaltonetworks.com/operation-ke3chang-resurfaces-with-new-tidepool-malware/>
	May 2017	Attack on a company that provides a range of services to UK Government A number of sensitive documents were stolen by the attackers during the incident and we believe APT15 was targeting information related to UK government departments and military technology.

		During our analysis of the compromise, we identified new backdoors that now appear to be part of APT15's toolset. The backdoor BS2005 – which has traditionally been used by the group – now appears alongside the additional backdoors RoyalCli and RoyalDNS. <https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/>
	Jun 2018	Operation "MirageFox" The malware involved in this recent campaign, MirageFox, looks to be an upgraded version of a tool, a RAT believed to originate in 2012, known as Mirage. <https://www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/>
Information	<https://github.com/nccgroup/Royal_APT>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0004/>	

Kimsuky, Velvet Chollima

Names	Kimsuky *(Kaspersky)* Velvet Chollima *(CrowdStrike)*
Country	North Korea
Motivation	Information theft and espionage
Description	(Kaspersky) For several months, we have been monitoring an ongoing cyber-espionage campaign against South Korean think-tanks. There are multiple reasons why this campaign is extraordinary in its execution and logistics. It all started one day when we encountered a somewhat unsophisticated spy program that communicated with its "master" via a public e-mail server. This approach is rather inherent to many amateur virus-writers and these malware attacks are mostly ignored.
Observed	Ministry of Unification, Sejong Institute and Korea Institute for Defense Analyses. Countries: South Korea.
Tools used	Grease, KPortScan, MailPassView, Mechanical, Mimikatz, Network Password Recovery, Procdump, PSExec, Remote Desktop PassView, SniffPass and WebBrowserPassView.
Information	<https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915/>

Lazarus Group, Hidden Cobra, Labyrinth Chollima

Names	Lazarus Group *(Kaspersky)* Labyrinth Chollima *(CrowdStrike)* Group 77 *(Talos)* Hastati Group *(SecureWorks)* Whois Hacking Team *(McAfee)* NewRomanic Cyber Army Team *(McAfee)* Zinc *(Microsoft)* Hidden Cobra *(Trend Micro)* Nickel Academy *(SecureWorks)* APT-C-26 *(360)*
Country	North Korea
Sponsor	State-sponsored, Bureau/Unit 211
Motivation	Information theft, espionage, disruption, sabotage and financial gain
Description	(Malwarebytes) Lazarus Group is commonly believed to be run by the North Korean government, motivated primarily by financial gain as a method of circumventing long-standing sanctions against the regime. They first came to substantial media notice in 2013 with a series of coordinated attacks against an assortment of South Korean broadcasters and financial institutions using DarkSeoul, a wiper program that overwrites sections of the victims' master boot record. In November 2014, a large scale breach of Sony Pictures was attributed to Lazarus. The attack was notable due to its substantial penetration across Sony networks, the extensive amount of data exfiltrated and leaked, as well of use of a wiper in a possible attempt to erase forensic evidence. Attribution on the attacks was largely hazy, but the FBI released a statement tying the Sony breach to the earlier DarkSeoul attack, and officially attributed both incidents to North Korea. Fast forward to May 2017 with the widespread outbreak of WannaCry, a piece of ransomware that used an SMB exploit as an attack vector. Attribution to North Korea rested largely on code reuse between WannaCry and previous North Korean attacks, but this was considered to be thin grounds given the common practice of tool sharing between regional threat groups. Western intelligence agencies released official statements to the public reaffirming the attribution, and on September 6, 2018, the US Department of Justice charged a North Korean national with involvement in both WannaCry and the Sony breach.
Observed	Sectors: Engineering, Financial, Government, Technology and BitCoin exchanges. Countries: Australia, Bangladesh, Brazil, Canada, Chile, China, Ecuador, France, Germany, Guatemala, Hong Kong, India, Israel, Japan, Mexico, Philippines, Poland, South Korea, Taiwan, Thailand, UK, USA, Vietnam and worldwide (WannaCry).
Tools used	AuditCred, AlphaNC, Alreay, AppleJeus, Appleworm, BADCALL, Bankshot, BanSwift, Bitsran, Brambul, BravoNC, Castov, Contopee, DeltaNC, Destover, Dozer, DoublePulsar, Duuzer, ELECTRICFISH, EternalBlue, FallChill RAT, FASTCash, Fimlis, Gh0st RAT, HARDRAIN, Hawup, Hermes, HOPLIGHT, HtDnDownLoader, Joanap, Jokra, KEYMARBLE, KillDisk, Koredos, Lazarus, Manuscrypt, Mimikatz, Mydoom, Mytob, NukeSped, PhanDoor, PowerRatankba, PowerSpritz, Proxysvc, RatabankaPOS, RawDisk, Rifdoor, Rising Sun, RomeoNC, SHARPKNOT, SheepRAT, SierraNC, Tdrop, Tdrop2, Troy, TYPEFRAME, Volgmer, WannaCry, WolfRAT and Yort.

Operations performed	2007	Operation "Flame" Target: South Korean government. Method: Disruption and sabotage.
	Jul 2009	Operation "Troy" North Korean hackers are suspected of launching a cyber-attack on some of the most important government offices in the US and South Korea in recent days, including the White House, the Pentagon, the New York Stock Exchange and the presidential Blue House in Seoul. The attack took out some of South Korea's most important websites, including those of the Blue House, the defense ministry, the national assembly, Shinhan bank, Korea Exchange bank and the top internet portal Naver. Target: Government, financial and media institutions in South Korea and USA. Method: DdoS attacks. <https://www.theguardian.com/world/2009/jul/08/south-korea-cyber-attack>
	Mar 2011	Attack on South Korean banks and media Recent Distributed Denial of Service (DdoS) attacks on a number South Korean websites have been in news for the past week. The threat responsible for carrying out these attacks is Trojan.Koredos. Target: South Korean organizations. Method: DdoS attacks and destruction of infected machines. <https://www.symantec.com/connect/blogs/trojankoredos-comes-unwelcomed-surprise>
	Mar 2013	Operation "Ten Days of Rain" / "DarkSeoul" Computer networks running three major South Korean banks and the country's two largest broadcasters were paralyzed Wednesday in attacks that some experts suspected originated in North Korea, which has consistently threatened to cripple its far richer neighbor. The attacks, which left many South Koreans unable to withdraw money from A.T.M.'s and news broadcasting crews staring at blank computer screens, came as the North's official Korean Central News Agency quoted the country's leader, Kim Jong-un, as threatening to destroy government installations in the South, along with American bases in the Pacific. Target: Three broadcasting stations and a bank in South Korea. Method: Infecting with viruses, stealing and wiping information. <https://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html>
	May 2013	South Korean Financial Companies Targeted by Castov In the past few months we have been actively monitoring an exploit kit, called Gongda, which is mainly targeting South Korea. Interestingly, we have come across a piece of malware, known as Castov, being delivered by this exploit kit that targets specific South Korean financial companies and their customers. The cybercriminals in this case have done their research on the South Korean online financial landscape. <https://www.symantec.com/connect/blogs/south-korean-financial-companies-targeted-castov>

	Jun 2013	DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War Yesterday, June 25, the Korean peninsula observed a series of cyberattacks coinciding with the 63rd anniversary of the start of the Korean War. While multiple attacks were conducted by multiple perpetrators, one of the distributed denial-of-service (DdoS) attacks observed yesterday against South Korean government websites can be directly linked to the DarkSeoul gang and Trojan.Castov. <https://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war>
	Nov 2014	Breach of Sony Pictures Entertainment The attack on Sony Pictures became public knowledge on November 24, 2014, when Sony employees turned on their computers to be greeted with the sight of a neon red skeleton and the words "Hacked by GOP", which stood for "Guardians of the Peace". The message also threatened to release data later that day if an unspecified request was not met. Over the following weeks, huge swathes of information stolen from Sony were released, including: personal information about employees and their families; email correspondence between employees at the company; information about company salaries, unreleased Sony films, and other information. Target: Sony Pictures Entertainment (released the "Interview" movie, ridiculing the North Korean leader). Method: Infecting with malware, stealing and wiping data of the company's employees, correspondence, copies of unreleased films. <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know>
	Jun 2015	Using the Palo Alto Networks AutoFocus threat intelligence platform, we identified several samples of malicious code with behavior similar to the aforementioned Operation Troy campaign dating back to June 2015, over two years after the original attacks in South Korea. Session data revealed a live attack targeting the transportation and logistics sector in Europe. <https://unit42.paloaltonetworks.com/tdrop2-attacks-suggest-dark-seoul-attackers-return/>
	Mar 2017	The Blockbuster Sequel This recently identified activity is targeting Korean speaking individuals, while the threat actors behind the attack likely speak both Korean and English. This blog will detail the recently discovered samples, their functionality, and their ties to the threat group behind Operation Blockbuster. <https://unit42.paloaltonetworks.com/unit42-the-blockbuster-sequel/>
	May 2017	WannaCry ransomware[5].
	Aug 2017	The Blockbuster Saga Continues Unit 42 researchers at Palo Alto Networks have discovered new attack activity targeting individuals involved with United States defense contractors.

---

[5] See ThaiCERT Whitepaper "WannaCry Ransomware"

		<https://unit42.paloaltonetworks.com/unit42-blockbuster-saga-continues/>
	Late 2017	Several financial sector and a casino breaches using KillDisk wiping malware in Latin America and USA. <https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-financial-organizations-in-latin-america/> <https://www.welivesecurity.com/2018/04/03/lazarus-killdisk-central-american-casino/>
	2017-2018	Cryptocurrency attacks on South Korean exchanges. <https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf> <https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/lazarus-resurfaces-targets-global-banks-bitcoin-users/>
	Mar 2018	APT attack on Turkish Financial Sector. Target: Turkish Financial Sector. Method: Spear-phishing with Bankshot implant. <https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/hidden-cobra-targets-turkish-financial-sector-new-bankshot-implant/>
	Apr 2018	Operation "GhostSecret" Target: The impacted organizations are in industries such as telecommunications, health, finance, critical infrastructure, and entertainment. Method: Spear-phishing with Destover-like implant. <https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/>
	Aug 2018	Operation "AppleJeus" Target: Cryptocurrency exchange. Method: Fake installer and macOS malware. <https://securelist.com/operation-applejeus/87553/>
	Oct 2018	Operation "Sharpshooter" Target: 87 organizations in many different sectors (majority Government and Defense) across the globe, predominantly in the United States. Method: Rising Sun implant to gather intelligence. <https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-sharpshooter-targets-global-defense-critical-infrastructure/>
	Nov 2018	More Attacks on Cryptocurrency Businesses Target: Some of the documents (for instance one entitled "sample document for business plan evaluation of venture company") were prepared in Korean, presumably to target South Korean businesses. Another contains a business overview of what seems to be a Chinese technology consulting group named LAFIZ ("we couldn't confirm if it's a legitimate business or another fake company made up by Lazarus," Kaspersky Lab researchers said). Yet another provided information for coin listings with a translation in Korean, researchers said.

		Method: Documents containing weaponized macros, "carefully prepared to attract the attention of cryptocurrency professionals." It utilizes PowerShell to control Windows systems and macOS malware for Apple users. <https://securelist.com/cryptocurrency-businesses-still-being-targeted-by-lazarus/90019/>
	Mar 2019	The infamous Lazarus threat actor group has been found targeting an Israeli defense company, according to new research outlined by a cybersecurity firm ClearSky. The campaign is carried out with an intention to steal military and commercial secrets. <https://cyware.com/news/lazarus-hacking-group-expand-their-attack-horizon-by-targeting-an-israeli-defense-company-02e2ec77>
	Apr 2019	"Hoplight" Malware Campaign Known as "Hoplight," the malware is a collection of nine files, though most of those are designed to work as obfuscation layers to keep admins and security software from spotting the attack. <https://www.theregister.co.uk/2019/04/10/lazarus_group_malware/>
	May 2019	North Korean Tunneling Tool: ELECTRICFISH This report provides analysis of one malicious 32-bit Windows executable file. The malware implements a custom protocol that allows traffic to be funneled between a source and a destination Internet Protocol (IP) address. The malware continuously attempts to reach out to the source and the designation system, which allows either side to initiate a funneling session. The malware can be configured with a proxy server/port and proxy username and password. This feature allows connectivity to a system sitting inside of a proxy server, which allows the actor to bypass the compromised system's required authentication to reach outside of the network. <https://www.us-cert.gov/ncas/analysis-reports/AR19-129A>
Counter operations	• Operation "Blockbuster" (2016) <https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf> • Microsoft and Facebook disrupt ZINC malware attack to protect customers and the internet from ongoing cyberthreats (2017) <https://blogs.microsoft.com/on-the-issues/2017/12/19/microsoft-facebook-disrupt-zinc-malware-attack-protect-customers-internet-ongoing-cyberthreats/> • North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions (2018) <https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and>	
Information	<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-look-into-the-lazarus-groups-operations> <https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies> <https://medium.com/threat-intel/lazarus-attacks-wannacry-5fdeddee476c> <https://content.fireeye.com/apt/rpt-apt38> <https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0032/>	

Subgroup: Andariel, Silent Chollima

Names	Andariel *(Trend Micro)* Silent Chollima *(CrowdStrike)*	
Country	North Korea	
Operations performed	2014	Operation "BLACKMINE" Target: South Korean organizations. Method: Information theft and espionage.
	2014	Operation "GHOSTRAT" Target: Defense industry Method: Information theft and espionage.
	2014	Operation "XEDA" Target: Foreign defense industries Method: Information theft and espionage.
	2015	Operation "INITROY"/Phase 1 Target: South Korean organizations. Method: Information theft/early phase operation.
	2015	Operation "DESERTWOLF"/Phase 3 Target: South Korean defense industry. Method: Information theft and espionage.
	2015	Operation "BLACKSHEEP"/Phase 3. Target: Defense industry Method: Information theft and espionage
	2016	Operation "INITROY"/Phase 2 Target: South Korean organizations. Method: Information theft/early phase operation.
	2016	Operation "VANXATM" Target: ATM companies Method: Financial theft/BPC
	2017	Operation "Mayday" Target: South Koran Financial Company. Method: Information theft and espionage.

Subgroup: Bluenoroff, APT 38, Stardust Chollima

Names	Bluenoroff *(Kaspersky)* Stardust Chollima *(CrowdStrike)* APT 38 *(Mandiant)*
Country	North Korea
Description	([Kaspersky](#)) The Lazarus Group, a nation-state level of attacker tied to the 2014 attacks on Sony Pictures Entertainment, has splintered off a portion of its operation to concentrate on stealing money to fund itself. The group, widely believed to be North Korean, has been linked to a February 2016 attack against the Bangladesh Central bank that resulted in more than $850 million in fraudulent SWIFT network transactions, $80 million of which still has not been recovered.

Operations performed	Oct 2015	Duuzer backdoor Trojan targets South Korea to take over computers Symantec has found that South Korea is being impacted by an active back door Trojan, detected as Backdoor.Duuzer. While the malware attack has not been exclusively targeting the region, it has been focusing on the South Korean manufacturing industry. Duuzer is a well-designed threat that gives attackers remote access to the compromised computer, downloads additional files, and steals data. It's clearly the work of skilled attackers looking to obtain valuable information. <https://www.symantec.com/connect/blogs/duuzer-back-door-trojan-targets-south-korea-take-over-computers>
	2015	SWIFT Attack on a bank in the Philippines <https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks>
	Dec 2015	Attempted Vietnamese TPBank SWIFT Attack <https://www.bankinfosecurity.com/vietnamese-bank-blocks-1-million-online-heist-a-9105>
	May 2016	SWIFT Attack on Banco del Austro in Ecuador <https://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD>
	2016-2018	Operation "FASTCash" On October 2, 2018, an alert was issued by US-CERT, the Department of Homeland Security, the Department of the Treasury, and the FBI. According to this new alert, Hidden Cobra (the U.S. government's code name for Lazarus) has been conducting "FASTCash" attacks, stealing money from Automated Teller Machines (ATMs) from banks in Asia and Africa since at least 2016. <https://www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware>
	Feb 2016	Bangladeshi Bank Attack <https://blog.trendmicro.com/trendlabs-security-intelligence/what-we-can-learn-from-the-bangladesh-central-bank-cyber-heist/>
	Oct 2016	Mexican and Polish Financial Attack Organizations in 31 countries have been targeted in a new wave of attacks which has been underway since at least October 2016. The

		attackers used compromised websites or "watering holes" to infect pre-selected targets with previously unknown malware. There has been no evidence found yet that funds have been stolen from any infected banks. <https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0>
	Oct 2017	SWIFT Attack on Far Eastern International Bank (FEIB) in Taiwan <https://baesystemsai.blogspot.com/2017/10/taiwan-heist-lazarus-tools.html>
	Jan 2018	Attempted heist at Bancomext in Mexico <https://www.bloomberg.com/news/articles/2018-05-29/mexico-foiled-a-110-million-bank-heist-then-kept-it-a-secret>
	May 2018	SWIFT attack on Banco de Chile in Chile <https://threatpost.com/banco-de-chile-wiper-attack-just-a-cover-for-10m-swift-heist/132796/>
	Aug 2018	SWIFT attack on Cosmos Bank in India <https://www.darkreading.com/attacks-breaches/north-korean-hacking-group-steals-$135-million-from-indian-bank-/d/d-id/1332678>
	Dec 2018	ATM breach of Redbanc in Chile <https://www.zdnet.com/article/north-korean-hackers-infiltrate-chiles-atm-network-after-skype-job-interview/>

Lead

Names	Lead *(Microsoft)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	(Microsoft) In the past few years, Lead's victims have included: • Multinational, multi-industry companies involved in the manufacture of textiles, chemicals, and electronics • Pharmaceutical companies • A company in the chemical industry • University faculty specializing in aeronautical engineering and research • A company involved in the design and manufacture of motor vehicles • A cybersecurity company focusing on protecting industrial control systems During these intrusions, Lead's objective was to steal sensitive data, including research materials, process documents, and project plans. Lead also steals code-signing certificates to sign its malware in subsequent attacks. In most cases, Lead's attacks do not feature any advanced exploit techniques. The group also does not make special effort to cultivate victims prior to an attack. Instead, the group often simply emails a Winnti installer to potential victims, relying on basic social engineering tactics to convince recipients to run the attached malware. In some other cases, Lead gains access to a target by brute-forcing remote access login credentials, performing SQL injection, or exploiting unpatched web servers, and then they copy the Winnti installer directly to compromised machines.
Observed	Sectors: Online videogame companies, Pharmaceutical, Technology and Telecommunications. Countries: Japan and USA.
Tool used	Cobalt Strike and Winnti.
Information	<https://www.microsoft.com/security/blog/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/>

Leafminer, Raspite

Names	Leafminer *(Symantec)*
	Raspite *(Dragos)*
Country	Iran
Motivation	Information theft and espionage
Description	(Symantec) Symantec has uncovered the operations of a threat actor named Leafminer that is targeting a broad list of government organizations and business verticals in various regions in the Middle East since at least early 2017. The group tends to adapt publicly available techniques and tools for their attacks and experiments with published proof-of-concept exploits. Leafminer attempts to infiltrate target networks through various means of intrusion: watering hole websites, vulnerability scans of network services on the internet, and brute-force/dictionary login attempts. The actor's post-compromise toolkit suggests that the group is looking for email data, files, and database servers on compromised target systems.
	(Dragos) Analysis of Raspite tactics, techniques, and procedures (TTPs) indicate the group has been active in some form since early- to mid-2017. Raspite targeting includes entities in the US, Middle East, Europe, and East Asia. Operations against electric utility organizations appear limited to the US at this time.
	Raspite leverages strategic website compromise to gain initial access to target networks. Raspite uses the same methodology as Berserk Bear, Dragonfly 2.0 and Allanite in embedding a link to a resource to prompt an SMB connection, from which it harvests Windows credentials. The group then deploys install scripts for a malicious service to beacon back to Raspite -controlled infrastructure, allowing the adversary to remotely access the victim machine.
Observed	Sectors: Energy, Financial, Government and Transportation.
	Countries: Europe, East Asia, Israel, Kuwait, Lebanon and USA.
Tools used	Imecab, LaZagne, PhpSpy and Mimikatz.
Information	<https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east>
	<https://dragos.com/resource/raspite/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0077/>

Leviathan, APT 40, TEMP.Periscope

Names	Leviathan *(CrowdStrike)* APT 40 *(Mandiant)* TEMP.Periscope *(FireEye)* TEMP.Jumper *(FireEye)* Bronze Mohawk *(SecureWorks)* Mudcarp *(iDefense)*
Country	China
Motivation	Information theft and espionage
Description	(FireEye) FireEye is highlighting a cyber espionage operation targeting crucial technologies and traditional intelligence targets from a China-nexus state sponsored actor we call APT40. The actor has conducted operations since at least 2013 in support of China's naval modernization effort. The group has specifically targeted engineering, transportation, and the defense industry, especially where these sectors overlap with maritime technologies. More recently, we have also observed specific targeting of countries strategically important to the Belt and Road Initiative including Cambodia, Belgium, Germany, Hong Kong, Philippines, Malaysia, Norway, Saudi Arabia, Switzerland, the United States, and the United Kingdom. This China-nexus cyber espionage group was previously reported as TEMP.Periscope and TEMP.Jumper.
Observed	Sectors: Maritime-related targets across multiple verticals, including Defense, Engineering, Government, Manufacturing, Research Shipping and Transportation. Countries: Belgium, Cambodia, Germany, Hong Kong, Malaysia, Norway Philippines, Saudi Arabia, Switzerland, USA and UK, and Asia Pacific Economic Cooperation (APEC).
Tools used	AIRBREAK, BADFLICK, Beacon, BITSAdmin, BLACKCOFFEE, China Chopper, Cobalt Strike, Derusbi, Gh0st RAT, GRILLMARK, HOMEFRY, LUNCHMONEY, MURKYTOP, NanHaiShu, Orz, PHOTO, PlugX, scanbox, SeDLL, Windows Credential Editor and ZXShell.
Operations performed	2014	Spear-phishing maritime and defense targets Proofpoint researchers are tracking an espionage actor targeting organizations and high-value targets in defense and government. Active since at least 2014, this actor has long-standing interest in maritime industries, naval defense contractors, and associated research institutions in the United States and Western Europe. <https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets>
	May 2017	Targeting UK-Based Engineering Company Using Russian APT Techniques Employees of a U.K.-based engineering company were among the targeted victims of a spear-phishing campaign in early July 2018. The campaign also targeted an email address possibly belonging to a freelance journalist based in Cambodia who covers Cambodian politics, human rights, and Chinese development. We believe both attacks used the same infrastructure as a reported campaign by Chinese threat actor TEMP.Periscope (also known as Leviathan), which targeted Cambodian entities in the run-up to their July 2018 elections. Crucially, TEMP.Periscope's interest in the U.K. engineering

		company they targeted dates back to attempted intrusions in May 2017. <https://www.recordedfuture.com/chinese-threat-actor-tempperiscope/>
	2017	The current campaign is a sharp escalation of detected activity since summer 2017. Like multiple other Chinese cyber espionage actors, TEMP.Periscope has recently re-emerged and has been observed conducting operations with a revised toolkit. Known targets of this group have been involved in the maritime industry, as well as engineering-focused entities, and include research institutes, academic organizations, and private firms in the United States. <https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html>
	Jul 2018	Targeting Cambodia Ahead of July 2018 Elections FireEye has examined a range of TEMP.Periscope activity revealing extensive interest in Cambodia's politics, with active compromises of multiple Cambodian entities related to the country's electoral system. This includes compromises of Cambodian government entities charged with overseeing the elections, as well as the targeting of opposition figures. This campaign occurs in the run up to the country's July 29, 2018, general elections. <https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html>
Information		<https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html>
MITRE ATT&CK		<https://attack.mitre.org/groups/G0065/>

Longhorn, The Lamberts

Names	Longhorn *(Symantec)* The Lamberts *(Kaspersky)*
Country	USA
Sponsor	State-sponsored, CIA
Motivation	Information theft and espionage
Description	Some operations and tooling used by this group were exposed in the [Vault 7/8] leaks on WikiLeaks in 2017. (Symantec) Longhorn has been active since at least 2011. It has used a range of back door Trojans in addition to zero-day vulnerabilities to compromise its targets. Longhorn has infiltrated governments and internationally operating organizations, in addition to targets in the financial, telecoms, energy, aerospace, information technology, education, and natural resources sectors. All of the organizations targeted would be of interest to a nation-state attacker. Longhorn has infected 40 targets in at least 16 countries across the Middle East, Europe, Asia, and Africa. On one occasion a computer in the United States was compromised but, following infection, an uninstaller was launched within hours, which may indicate this victim was infected unintentionally. Longhorn's malware appears to be specifically built for espionage-type operations, with detailed system fingerprinting, discovery, and exfiltration capabilities. The malware uses a high degree of operational security, communicating externally at only select times, with upload limits on exfiltrated data, and randomization of communication intervals—all attempts to stay under the radar during intrusions. For C&C servers, Longhorn typically configures a specific domain and IP address combination per target. The domains appear to be registered by the attackers; however they use privacy services to hide their real identity. The IP addresses are typically owned by legitimate companies offering virtual private server (VPS) or webhosting services. The malware communicates with C&C servers over HTTPS using a custom underlying cryptographic protocol to protect communications from identification.
Observed	Sectors: Aerospace, Education, Energy, Financial, Government, IT and Telecommunications. Countries: 16 countries in the Middle East, Europe, Asia and Africa.
Tools used	Black Lambert, Blue Lambert, Corentry, Gray Lambert, Green Lambert, Green OS X Lambert, LH1, LH2, Pink Lambert, Plexor and White Lambert.
Information	<https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7> <https://securelist.com/unraveling-the-lamberts-toolkit/77990/>

Lotus Blossom, Spring Dragon

Names	Lotus Blossom *(Palo Alto)* Spring Dragon *(Kaspersky)* Dragonfish *(iDefense)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	(Kaspersky) Spring Dragon is a long running APT actor that operates on a massive scale. The group has been running campaigns, mostly in countries and territories around the South China Sea, since as early as 2012. The main targets of Spring Dragon attacks are high profile governmental organizations and political parties, education institutions such as universities, as well as companies from the telecommunications sector. Spring Dragon is known for spear phishing and watering hole techniques and some of its tools have previously been analyzed and reported on by security researchers, including Kaspersky Lab.
Observed	Sectors: Defense, Education, Government and Telecommunications. Countries: Brunei, Cambodia, Hong Kong, Indonesia, Japan, Laos, Malaysia, Myanmar, Philippines, Singapore, Taiwan, Thailand and Vietnam.
Tools used	Elise and Emissary.
Operations performed	Jun 2015	Operation "Lotus Blossom" Today Unit 42 published new research identifying a persistent cyber espionage campaign targeting government and military organizations in Southeast Asia. The adversary group responsible for the campaign, which we named "Lotus Blossom," is well organized and likely state-sponsored, with support from a country that has interests in Southeast Asia. The campaign has been in operation for some time; we have identified over 50 different attacks taking place over the past three years. <https://unit42.paloaltonetworks.com/operation-lotus-blossom/>
	Nov 2015	Attack on French Diplomat We observed a targeted attack in November directed at an individual working for the French Ministry of Foreign Affairs. The attack involved a spear-phishing email sent to a single French diplomat based in Taipei, Taiwan and contained an invitation to a Science and Technology support group event. <https://unit42.paloaltonetworks.com/attack-on-french-diplomat-linked-to-operation-lotus-blossom/>
	2017	In the beginning of 2017, Kaspersky Lab became aware of new activities by an APT actor we have been tracking for several years called Spring Dragon (also known as LotusBlossom). Information about the new attacks arrived from a research partner in Taiwan and we decided to review the actor's tools, techniques and activities.

		Using Kaspersky Lab telemetry data we detected the malware in attacks against some high-profile organizations around the South China Sea. <https://securelist.com/spring-dragon-updated-activity/79067/>
	Jan 2018	Attacks on Association of South East Asian Nations (ASEAN) countries During the last weeks of January (2018), nation state actors from Lotus Blossom conducted a targeted malware spam campaign against the Association of South East Asian Nations (ASEAN) countries. <https://community.rsa.com/community/products/netwitness/blog/2018/02/13/lotus-blossom-continues-asean-targeting> <https://www.accenture.com/t20180127T003755Z_w_/us-en/_acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0030/>	

Lucky Cat

Names	Lucky Cat *(Symantec)*
Country	China
Motivation	Information theft and espionage
Description	(Symantec) A series of attacks, targeting both Indian military research and south Asian shipping organizations, demonstrate the minimum level of effort required to successfully compromise a target and steal sensitive information. The attackers use very simple malware, which required little development time or skills, in conjunction with freely available Web hosting, to implement a highly effective attack. It is a case of the attackers obtaining a maximum return on their investment. The attack shows how an intelligent attacker does not need to be particularly technically skilled in order to steal the information they are after. The attack begins, as is often the case, with an email sent to the victim. A malicious document is attached to the email, which, when loaded, activates the malware. The attackers use tailored emails to encourage the victim to open the email. For example, one email sent to an academic claimed to be a call for papers for a conference (CFP). The vast majority of the victims were based in India, with some in Malaysia. The victim industry was mostly military research and also shipping based in the Arabian and South China seas. In some instances the attackers appeared to have a clear goal, whereby specific files were retrieved from certain compromised computers. In other cases, the attackers used more of a 'shotgun' like approach, copying every file from a computer. Military technologies were obviously the focus of one particular attack with what appeared to be source code stolen. 45 different attacker IP addresses were observed. Out of those, 43 were within the same IP address range based in Sichuan province, China. The remaining two were based in South Korea. The pattern of attacker connections implies that the IP addresses are being used as a VPN, probably in an attempt to render the attackers anonymous. The attacks have been active from at least April 2011 up to February 2012. The attackers are intelligent and focused, employing the minimum amount of work necessary for the maximum gain. They do not use zero day exploits or complicated threats, instead they rely on effective social engineering and lax security measures on the part of the victims.
Observed	Sectors: Aerospace, Defense, Engineering, Shipping and Tibetan activists. Countries: India, Japan, Malaysia and Tibet.
Tools used	Sojax and Wimmie.
Information	<https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_luckycat_hackers.pdf> <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf>

Lurk

Names	Lurk *(Kaspersky)*
Country	Russia
Motivation	Financial gain
Description	(Kaspersky) When we first encountered Lurk, in 2011, it was a nameless Trojan. It all started when we became aware of a number of incidents at several Russian banks that had resulted in the theft of large sums of money from customers. To steal the money, the unknown criminals used a hidden malicious program that was able to interact automatically with the financial institution's remote banking service (RBS) software; replacing bank details in payment orders generated by an accountant at the attacked organization, or even generating such orders by itself.

In 2016, it is hard to imagine banking software that does not demand some form of additional authentication, but things were different back in 2011. In most cases, the attackers only had to infect the computer on which the RBS software was installed in order to start stealing the cash. Russia's banking system, like those of many other countries, was unprepared for such attacks, and cybercriminals were quick to exploit the security gap.

So we decided to take a closer look at the malware. The first attempts to understand how the program worked gave our analysts nothing. Regardless of whether it was launched on a virtual or a real machine, it behaved in the same way: it didn't do anything. This is how the program, and later the group behind it, got its name. To "lurk" means to hide, generally with the intention of ambush.

We were soon able to help investigate another incident involving Lurk. This time we got a chance to explore the image of the attacked computer. There, in addition to the familiar malicious program, we found a .dll file with which the main executable file could interact. This was our first piece of evidence that Lurk had a modular structure.

Later discoveries suggest that, in 2011, Lurk was still at an early stage of development. It was formed of just two components, a number that would grow considerably over the coming years. |
Observed	Sectors: Financial and Media. Countries: Russia.
Tools used	Lurk.
Counter operations	• Russia arrests 50, shuts down 5-year, $25m cyber bank robbery (2016) <https://nakedsecurity.sophos.com/2016/06/06/russia-arrests-50-shuts-down-5-year-25m-cyber-bank-robbery/>
Information	<https://securelist.com/the-hunt-for-lurk/75944/>

Mabna Institutem, Silent Librarian

Names	Mabna Institute *(real name)* Silent Librarian *(SecureWorks)*
Country	Iran
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	According to the Treasury Department, since 2013, the Mabna Institute hit 144 US universities and 176 universities in 21 foreign countries. Geoffrey Berman, US Attorney for the Southern District of New York revealed that the spear phishing campaign targeted more than 100,000 university professors worldwide and about 8,000 accounts were compromised. The Iranian hackers exfiltrated 31 terabytes, roughly 15 billion pages of academic projects were stolen. The hackers also targeted the US Department of Labor, the US Federal Energy Regulatory Commission, and many private and non-governmental organizations. The sanctions also hit the Mabna Institute, an Iran-based company that had a critical role in coordinating the attacks on behalf of Iran's Revolutionary Guards.
Observed	Sectors: Universities. Countries: Australia, Canada, China, Israel, Japan, Switzerland, Turkey, UK and USA.
Tools used	
Operations performed	Aug 2018	Operation "Cobalt Dickens" Despite indictments in March 2018, the Iranian threat group is likely responsible for a large-scale campaign that targeted university credentials using the same spoofing tactics as previous attacks. In August 2018, members of university communities worldwide may have been providing access to more than just homework assignments. Secureworks Counter Threat Unit (CTU) researchers discovered a URL spoofing a login page for a university. Further research into the IP address hosting the spoofed page revealed a broader campaign to steal credentials. Sixteen domains contained over 300 spoofed websites and login pages for 76 universities located in 14 countries, including Australia, Canada, China, Israel, Japan, Switzerland, Turkey, the United Kingdom, and the United States. <https://www.secureworks.com/blog/back-to-school-cobalt-dickens-targets-universities>
Counter operations	• Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps (2018) <https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary>

Madi

Names	Madi *(Kaspersky)* Mahdi *(Kaspersky)*
Country	Iran
Motivation	Information theft and espionage
Description	(Kaspersky) Kaspersky Lab and Seculert worked together to sinkhole the Madi Command & Control (C&C) servers to monitor the campaign. Kaspersky Lab and Seculert identified more than 800 victims located in Iran, Israel and select countries across the globe connecting to the C&Cs over the past eight months. Statistics from the sinkhole revealed that the victims were primarily business people working on Iranian and Israeli critical infrastructure projects, Israeli financial institutions, Middle Eastern engineering students, and various government agencies communicating in the Middle East. Common applications and websites that were spied on include accounts on Gmail, Hotmail, Yahoo! Mail, ICQ, Skype, Google+, and Facebook. Surveillance is also performed over integrated ERP/CRM systems, business contracts, and financial management systems.
Observed	Sectors: Education, Engineering, Financial, Government, Oil and gas and Think Tanks. Countries: Australia, Ecuador, Greece, Iran, Iraq, Israel, Mozambique, New Zealand, Pakistan, Saudi Arabia, Switzerland, USA and Vietnam.
Tools used	Madi.
Operations performed	Jul 2012	New and Improved Madi Spyware Campaign Continues Madi, the religiously-titled spyware that was discovered last week and thought to be dead, appears to be making a comeback, complete with updates. <https://threatpost.com/new-and-improved-madi-spyware-campaign-continues-072512/76849/>
Counter operations	The C&C servers have been sinkholed by Kaspersky and Seculert.
Information	<https://www.symantec.com/connect/blogs/madi-attacks-series-social-engineering-campaigns> <https://securelist.com/the-madi-campaign-part-i-5/33693/> <https://securelist.com/the-madi-campaign-part-ii-53/33701/>

Magic Hound, APT 35, Cobalt Gypsy, Rocket Kitten

Names	Magic Hound *(Palo Alto)* APT 35 *(Mandiant)* Cobalt Gypsy *(SecureWorks)* Rocket Kitten *(CrowdStrike)* TEMP.Beanie *(FireEye)* Timberworm *(Symantec)* Tarh Andishan *(Cylance)*
Country	Iran
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	Magic Hound is an Iranian-sponsored threat group operating primarily in the Middle East that dates back as early as 2014. The group behind the campaign has primarily targeted organizations in the energy, government, and technology sectors that are either based or have business interests in Saudi Arabia. This group appears to be the evolvement of Covellite

Names	Covellite *(Dragos)*
Country	North Korea
Motivation	Information theft and espionage
Description	(Dragos) Covellite compromises networks associated with civilian worldwide and gathers intelligence on intellectual property and in operations. Covellite lacks an industrial control system (ICS) spe this time. Covellite operates globally with targets primarily in Europe, East America. US targets emerged in September 2017 with a small, ta campaign directed at select U.S. electric companies. The phishin a malicious Microsoft Word document and infected computers wi The malicious emails discovered in the fall masqueraded as resu They delivered a remote access tool (RAT) payload which was u reconnaissance and enable persistent, covert access to victims' Covellite's infrastructure and malware are similar to the hacking as Lazarus Group, Hidden Cobra, Labyrinth Chollima by Novetta by the U.S. Department of Homeland Security. Lazarus Group is responsible for attacks ranging from the 2014 a Pictures to a number of Bitcoin heists in 2017. Technical analysis malware indicates an evolution from known Lazarus toolkits. How technical overlap, it is not known how the capabilities and operat Covellite and Lazarus are related. Covellite remains active but appears to have abandoned North A with indications of activity in Europe and East Asia. Given the gro interest in infrastructure operations, rapidly improving capabilities

		aggressive targeting, Dragos considers this group a primary threat to the ICS industry.
	Observed	Sectors: Energy. Countries: East Asia, Europe and USA.
	Tools used	
	Information	<https://dragos.com/resource/covellite/>

Cutting Kitten, TG-2889.

Observed	Sectors: Energy, Government and Technology sectors that are either based or have business interests in Saudi Arabia. Countries: Afghanistan, Canada, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Morocco, Pakistan, Saudi Arabia, Spain, Syria, Turkey, UAE, UK, Venezuela and Yemen	
Tools used	CWoolger, DistTrack, FileMalv, Ghambar, Ghole, Havij, Leash, Matryoshka RAT, Mimikatz, MPKBot, NETWoolger, PupyRAT, sqlmap, TDTESS and Woolger.	
Operations performed	Mid-2014	Operation "Thamar Reservoir" This report reviews an ongoing cyber-attack campaign dating back to mid-2014. Additional sources indicate it may date as far back as 2011. We call this campaign Thamar Reservoir, named after one of the targets, Thamar E. Gindin, who exposed new information about the attack and is currently assisting with the investigation. <https://www.clearskysec.com/thamar-reservoir/>
	Feb 2015	Operation "Woolen-GoldFish" <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-woolen-goldfish-when-kittens-go-phishing>
	2016	Unit 42 has discovered a persistent attack campaign operating primarily in the Middle East dating back to at least mid-2016 which we have named Magic Hound. This appears to be an attack campaign focused on espionage. Based upon our visibility it has primarily targeted organizations in the energy, government, and technology sectors that are either based or have business interests in Saudi Arabia. The adversaries appear to have evolved their tactics and techniques throughout the tracked time-period, iterating through a diverse toolset across different waves of attacks. <https://unit42.paloaltonetworks.com/unit42-magic-hound-campaign-attacks-saudi-targets/>
	Jan 2017	PupyRAT campaign SecureWorks Counter Threat Unit (CTU) researchers analyzed a phishing campaign that targeted a Middle Eastern organization in early January 2017. Some of messages were sent from legitimate email addresses belonging to several Middle Eastern organizations. <https://www.secureworks.com/blog/iranian-pupyrat-bites-middle-eastern-organizations>
	2017	The Curious Case of Mia Ash In early 2017, SecureWorks Counter Threat Unit (CTU) researchers observed phishing campaigns targeting several entities in the Middle

		East and North Africa (MENA), with a focus on Saudi Arabian organizations. The campaigns delivered PupyRAT, an open-source cross-platform remote access Trojan. <https://www.secureworks.com/research/the-curious-case-of-mia-ash>
Counter operations		• Microsoft slaps down 99 APT35/Charming Kitten domains (2019) <https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/>
Information		<https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-spy-kittens-are-back.pdf> <https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf>
MITRE ATT&CK		<https://attack.mitre.org/groups/G0059/>

Moafee

Names	Moafee *(FireEye)*
Country	China
Motivation	Information theft and espionage
Description	Moafee is a threat group that appears to operate from the Guandong Province of China. Due to overlapping TTPs, including similar custom tools, Moafee is thought to have a direct or indirect relationship with the threat group DragonOK. (FireEye) The attack group "Moafee" (named after their command and control infrastructure) appears to operate out of the Guangdong province in China and is known to target the governments and military organizations of countries with national interests in the South China Sea. The seas in this region have multiple claims of sovereignty and hold high significance, as it is the second busiest sea-lane in the world and are known to be rich in resources such as rare earth metals, crude oil, and natural gas. We have also observed the Moafee group target organizations within the US defense industrial base.
Observed	Sectors: Defense and Government. Countries: USA and "countries with national interests in the South China Sea."
Tools used	HTRAN, Mongall, NewCT2, Nflog and Poison Ivy.
Information	<https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0002/>

Mofang

Names	Mofang *(Fox-IT)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	(Fox-IT) Mofang is a threat actor that almost certainly operates out of China and is probably government-affiliated. It is highly likely that Mofang's targets are selected based on involvement with investments, or technological advances that could be perceived as a threat to the Chinese sphere of influence. This is most clearly the case in a campaign focusing on government and critical infrastructure of Myanmar that is described in this report. Chances are about even, though, that Mofang is a relevant threat actor to any organization that invests in Myanmar or is otherwise politically involved. In addition to the campaign in Myanmar, Mofang has been observed to attack targets across multiple sectors (government, military, critical infrastructure and the automotive and weapon industries) in multiple countries.
Observed	Sectors: Automotive, Critical infrastructure, Defense, Government and weapon industries. Countries: Canada, Germany, India, Myanmar, Singapore, South Korea and USA.
Tools used	ShimRAT, ShimRatReporter and Superman.
Information	<https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf>

Molerats, Extreme Jackal, Gaza Cybergang

Names	Molerats *(FireEye)* Extreme Jackal *(CrowdStrike)* Gaza Cybergang *(Kaspersky)* Gaza Hackers Team *(Kaspersky)*
Country	Gaza
Sponsor	Hamas
Motivation	Information theft and espionage
Description	(Kaspersky) The Gaza cybergang is an Arabic-language, politically-motivated cybercriminal group, operating since 2012 and actively targeting the MENA (Middle East North Africa) region. The Gaza cybergang's attacks have never slowed down and its typical targets include government entities/embassies, oil and gas, media/press, activists, politicians, and diplomats. One of the interesting new facts, uncovered in mid-2017, is its discovery inside an oil and gas organization in the MENA region, infiltrating systems and pilfering data, apparently for more than a year.
Observed	Sectors: Aerospace, Defense, Embassies, Financial, Government, Oil and gas, journalists and software developers. Countries: China, Egypt, Iran, Iraq, Israel, Jordan, Latvia, Libya, Macedonia, New Zealand, Palestine, Saudi Arabia, Slovenia, Turkey, UAE, UK, USA and Yemen, the BBC and the Office of the Quartet Representative.
Tools used	DustySky, Molerat Loader, NeD Worm, njRAT, Poison Ivy, Scote and XtremeRAT.

Operations performed	Jan 2012	Defacement of Israel fire service website Hackers claiming to be from the Gaza Strip defaced the website of the Israel Fire and Rescue services, posting a message saying "Death to Israel," a spokesman said on Friday. <https://middle-east-online.com/en/cyber-war-gaza-hackers-deface-israel-fire-service-website>
	Oct 2012	Operation "Molerats" In October 2012, malware attacks against Israeli government targets grabbed media attention as officials temporarily cut off Internet access for its entire police force and banned the use of USB memory sticks. Security researchers subsequently linked these attacks to a broader, yearlong campaign that targeted not just Israelis but Palestinians as well — and as discovered later, even the U.S. and UK governments. <https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html>
	Jun 2013	We observed several attacks in June and July 2013 against targets in the Middle East and the U.S. that dropped a PIVY payload that connected to command-and-control (CnC) infrastructure used by the Molerats attackers. <https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html>
	Apr 2014	Between 29 April and 27 May, FireEye Labs identified several new Molerats attacks targeting at least one major U.S. financial institution and multiple, European government organizations.

		<https://www.fireeye.com/blog/threat-research/2014/06/molerats-here-for-spring.html>
	Summer 2014	Attacks against Israeli & Palestinian interests The decoy documents and filenames used in the attacks suggest the intended targets include organizations with political interests or influence in Israel and Palestine. <https://pwc.blogs.com/cyber_security_updates/2015/04/attacks-against-israeli-palestinian-interests.html>
	2014	Operation "Moonlight" Vectra Threat Labs researchers have uncovered the activities of a group of individuals currently engaged in targeted attacks against entities in the Middle East. We identified over 200 samples of malware generated by the group over the last two years. These attacks are themed around Middle Eastern political issues and the motivation appears to relate to espionage, as opposed to opportunistic or criminal intentions. <https://blog.vectra.ai/blog/moonlight-middle-east-targeted-attacks>
	May 2015	One interesting new fact about Gaza Cybergang activities is that they are actively sending malware files to IT (Information Technology) and IR (Incident Response) staff; this is also obvious from the file names they are sending to victims, which reflect the IT functions or IR tools used in cyberattack investigations. <https://securelist.com/gaza-cybergang-wheres-your-ir-team/72283/>
	Sep 2015	Operation "DustySky" These attacks are targeted, but not spear-phished. I.e., malicious email messages are sent to selected targets rather than random mass distribution, but are not tailored specifically to each and every target. Dozens of targets may receive the exact same message. The email message and the lure document are written in Hebrew, Arabic or English –depending on the target audience. Targeted sectors include governmental and diplomatic institutions, including embassies; companies from the aerospace and defense Industries; financial institutions; journalists; software developers. The attackers have been targeting software developers in general, using a fake website pretending to be a legitimate iOS management software, and linking to it in an online freelancing marketplace. <https://www.clearskysec.com/wp-content/uploads/2016/01/Operation%20DustySky_TLP_WHITE.pdf>
	Apr 2016	Operation "DustySky" Part 2 Attacks against all targets in the Middle East stopped at once, after we published our first report. However, the attacks against targets in the Middle East (except Israel) were renewed in less than 20 days. In the beginning of April 2016, we found evidence that the attacks against Israel have been renewed as well. Based on the type of targets, on Gaza being the source of the attacks, and on the type of information the attackers are after –we estimate with medium-high certainty that the Hamas terrorist organization is behind these attacks. <https://www.clearskysec.com/wp-content/uploads/2016/06/Operation-DustySky2_-6.2016_TLP_White.pdf>

		<https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/26000/PD26760/en_US/McAfee_Labs_Threat_Advisory_GazaCybergang.pdf>
	Nov 2016	PwC analysts have been tracking the same malware campaign, which has seen a noticeable spike since at least April 2016. The attackers have targeted Arabic news websites, political figures and other targets that possess influence in the Palestinian territories and other neighbouring Arab countries. Our investigation began by analysing around 20 executable files associated with the attacks. Several of these files opened decoy documents and audio files, which were exclusively in Arabic-language. <https://pwc.blogs.com/cyber_security_updates/2016/11/molerats-theres-more-to-the-naked-eye.html>
	Mid-2017	New targets, use of MS Access Macros and CVE 2017-0199, and possible mobile espionage One of the interesting new facts, uncovered in mid-2017, is its discovery inside an oil and gas organization in the MENA region, infiltrating systems and pilfering data, apparently for more than a year. Another interesting finding is the use of the recently discovered CVE 2017-0199 vulnerability, and Microsoft Access files into which the download scripts were embedded to reduce the likelihood of their detection. Traces of mobile malware that started to appear from late April 2017, are also being investigated. <https://securelist.com/gaza-cybergang-updated-2017-activity/82765/>
	Sep 2017	"TopHat" Campaign In recent months, Palo Alto Networks Unit 42 observed a wave of attacks leveraging popular third-party services Google+, Pastebin, and bit.ly. The attacks we found within the TopHat campaign began in early September 2017. In a few instances, original filenames of the identified samples were written in Arabic. <https://unit42.paloaltonetworks.com/unit42-the-tophat-campaign-attacks-within-the-middle-east-region-using-popular-third-party-services/>
	Feb 2019	New Attack in the Middle East Recently, 360 Threat Intelligence Center captured a bait document designed specifically for Arabic users. It is an Office Word document with malicious macros embedded to drop and execute a backdoor packed by Enigma Virtual Box. The backdoor program has a built-in keyword list containing names of people or opera movies to communicate with C2, distributes control commands to further control the victim's computer device. After investigation, we suspect this attack is carried out by Molerats. <https://ti.360.net/blog/articles/suspected-molerats-new-attack-in-the-middle-east-en/>
	Apr 2019	"SneakyPastes" Campaign The campaign is multistage. It begins with phishing, using letters from one-time addresses and one-time domains. Sometimes the letters contain links to malware or infected attachments. If the victim

		executes the attached file (or follows the link), their device receives Stage One malware programmed to activate the infection chain. <https://www.kaspersky.com/blog/gaza-cybergang/26363/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0021/>	

MoneyTaker

Names	MoneyTaker *(Group-IB)*
Country	Russia
Motivation	Financial gain
Description	(Group-IB) In less than two years, this group has conducted over 20 successful attacks on financial institutions and legal firms in the USA, UK and Russia. The group has primarily been targeting card processing systems, including the AWS CBR (Russian Interbank System) and purportedly SWIFT (US). Given the wide usage of STAR in LATAM, financial institutions in LATAM could have particular exposure to a potential interest from the MoneyTaker group. Although the group has been successful at targeting a number of banks in different countries, to date, they have gone unreported. In addition to banks, the MoneyTaker group has attacked law firms and also financial software vendors. In total, Group-IB has confirmed 20 companies as MoneyTaker victims, with 16 attacks on US organizations, 3 attacks on Russian banks and 1 in the UK.
Observed	Sectors: Financial. Countries: Russia, UK and USA.
Tools used	Citadel, Kronos, Metasploit, MoneyTaker and Screenshotter.
Information	<https://www.group-ib.com/blog/moneytaker>

MuddyWater, Seedworm, TEMP.Zagros, Static Kitten

Names	MuddyWater *(Palo Alto)* Seedworm *(Symantec)* TEMP.Zagros *(FireEye)* Static Kitten *(CrowdStrike)*
Country	Iran
Motivation	Information theft and espionage
Description	([Reaqta](#)) MuddyWater is an APT group that has been active throughout 2017, targeting victims in Middle East with in-memory vectors leveraging on Powershell, in a family of attacks now identified as "Living off the land", as they don't require the creation of new binaries on the victim's machine, thus maintaining a low detection profile and a low forensic footprint. The operators behind MuddyWater are likely espionage motivated, we derive this information from the analysis of data and backdoors behaviors. We also find that despite the strong preponderance of victims from Pakistan, the most active targets appear to be in: Saudi Arabia, UAE and Iraq. Amongst the victims we identify a variety of entities with a stronger focus at Governments, Telcos and Oil companies. By tracking the operations we finally figure out that the originating country is likely to be Iran, while it remains harder to ascertain whether MuddyWater is state sponsored or a criminal organization incline to espionage.
Observed	Sectors: Defense, Education, Food, Gaming, Government, IT, Media, NGOs, Oil and gas, Telecommunications and Transportation. Countries: Afghanistan, Armenia, Bahrein, Belarus, Egypt, Georgia, India, Iraq, Israel, Jordan, Lebanon, Mali, Netherlands, Oman, Pakistan, Russia, Saudi Arabia, Tajikistan, Tunisia, Turkey, UAE, Ukraine and USA.
Tools used	ChromeCookiesView, chrome-passwords, CLOUDSTATS, CrackMapExec, DELPHSTATS, EmpireProject, FruityC2, Koadic, LaZagne, Meterpreter, Mimikatz. MZCookiesView, PowerSploit, POWERSTATS, SHARPSTATS, Shoorback and Smbmap.
Operations performed	Feb 2017	The MuddyWater attacks are primarily against Middle Eastern nations. However, we have also observed attacks against surrounding nations and beyond, including targets in India and the USA. <https://unit42.paloaltonetworks.com/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/>
	Jan 2018	Updated Tactics, Techniques and Procedures in Spear Phishing Campaign We attribute this activity to TEMP.Zagros (reported by Palo Alto Networks and Trend Micro as MuddyWater), an Iran-nexus actor that has been active since at least May 2017. This actor has engaged in prolific spear phishing of government and defense entities in Central and Southwest Asia. <https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.html>
	Mar 2018	Campaign Possibly Connected to "MuddyWater" Surfaces in the Middle East and Central Asia

		We discovered a new campaign targeting organizations in Turkey, Pakistan and Tajikistan that has some similarities with an earlier campaign named MuddyWater, which hit various industries in several countries, primarily in the Middle East and Central Asia. <https://blog.trendmicro.com/trendlabs-security-intelligence/campaign-possibly-connected-muddywater-surfaces-middle-east-central-asia/>
	May 2018	Another Potential MuddyWater Campaign uses Powershell-based PRB-Backdoor In May 2018, we found a new sample (Detected as W2KM_DLOADR.UHAOEEN) that may be related to this campaign. Like the previous campaigns, these samples again involve a Microsoft Word document embedded with a malicious macro that is capable of executing PowerShell (PS) scripts leading to a backdoor payload. One notable difference in the analyzed samples is that they do not directly download the Visual Basic Script(VBS) and PowerShell component files, and instead encode all the scripts on the document itself. The scripts will then be decoded and dropped to execute the payload without needing to download the component files. <https://blog.trendmicro.com/trendlabs-security-intelligence/another-potential-muddywater-campaign-uses-powershell-based-prb-backdoor/>
	May 2018	We recently noticed a large amount of spear phishing documents that appear to be targeting government bodies, military entities, telcos and educational institutions in Jordan, Turkey, Azerbaijan and Pakistan, in addition to the continuous targeting of Iraq and Saudi Arabia, other victims were also detected in Mali, Austria, Russia, Iran and Bahrain.. These new documents have appeared throughout 2018 and escalated from May onwards. The attacks are still ongoing. <https://securelist.com/muddywater/88059/>
	Sep 2018	Group remains highly active with more than 130 victims in 30 organizations hit since September 2018. Seedworm's motivations are much like many cyber espionage groups that we observe—they seek to acquire actionable information about the targeted organizations and individuals. They accomplish this with a preference for speed and agility over operational security, which ultimately led to our identification of their key operational infrastructure. <https://www.symantec.com/blogs/threat-intelligence/seedworm-espionage-group>
	Nov 2018	Operations in Lebanon and Oman MuddyWater has recently been targeting victims likely from Lebanon and Oman, while leveraging compromised domains, one of which is owned by an Israeli web developer. The investigation aimed to uncover additional details regarding the compromise vector. Further, we wished to determine the infection vector, which is currently unknown. With that in mind, past experience implies that this might be a two-stage spear-phishing campaign. <https://www.clearskysec.com/wp-content/uploads/2018/11/MuddyWater-Operations-in-Lebanon-and-Oman.pdf>
	Apr 2019	Targeting Kurdish Political Groups and Organizations in Turkey

		However, unlike the previous vector, we did not identify this time any compromised servers used to host the malware's code. Instead, the lure document already contains the malicious code. We also detected five additional files that operate in a similar file to the aforementioned document; but unlike that file, these do not have any content. <https://www.clearskysec.com/muddywater-targets-kurdish-groups-turkish-orgs/>
	Apr 2019	The Iranian APT, MuddyWater, has been active since at least 2017. Most recently though, a new campaign, targeting Belarus, Turkey and Ukraine, has emerged that caught the attention of Check Point researchers. <https://research.checkpoint.com/the-muddy-waters-of-apt-attacks/>
	Apr 2019	Operation "BlackWater" Newly associated samples from April 2019 indicate attackers have added three distinct steps to their operations, allowing them to bypass certain security controls and suggesting that MuddyWater's tactics, techniques and procedures (TTPs) have evolved to evade detection. <https://blog.talosintelligence.com/2019/05/recent-muddywater-associated-blackwater.html>
	Jun 2019	Clearsky has detected new and advanced attack vector used by MuddyWater to target governmental entities and the telecommunication sector. Notably, the TTP includes decoy documents exploiting CVE-2017-0199 as the first stage of the attack. This is followed by the second stage of the attack – communication with the hacked C2 servers and downloading a file infected with the macros. <https://www.clearskysec.com/muddywater2/>
	Jun 2019	We came across new campaignsthat seem to bear the markings of MuddyWater –a threat actor group with a history of targeting organizations in Middle Eastern and Asian countries. The group used new tools and payloads in campaigns over the first half of 2019, pointing to the continued work the group has put in since our last report on MuddyWaterin November 2018. <https://documents.trendmicro.com/assets/white_papers/wp_new_muddywater_findings_uncovered.pdf>
Counter operations	• New leaks of Iranian cyber-espionage operations hit Telegram and the Dark Web (2019) <https://www.zdnet.com/article/new-leaks-of-iranian-cyber-espionage-operations-hit-telegram-and-the-dark-web/>	
Information	<https://reaqta.com/2017/11/muddywater-apt-targeting-middle-east/> <https://www.symantec.com/blogs/threat-intelligence/seedworm-espionage-group>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0069/>	

Mustang Panda

Names	Mustang Panda *(CrowdStrike)*
Country	China
Motivation	Information theft and espionage
Description	(CrowdStrike) In April 2017, CrowdStrike Falcon Intelligence observed a previously unattributed actor group with a Chinese nexus targeting a U.S.-based think tank. Further analysis revealed a wider campaign with unique tactics, techniques, and procedures (TTPs). This adversary targets non-governmental organizations (NGOs) in general, but uses Mongolian language decoys and themes, suggesting this actor has a specific focus on gathering intelligence on Mongolia. These campaigns involve the use of shared malware like Poison Ivy or PlugX. Recently, Falcon Intelligence observed new activity from Mustang Panda, using a unique infection chain to target likely Mongolia-based victims. This newly observed activity uses a series of redirections and fileless, malicious implementations of legitimate tools to gain access to the targeted systems. Additionally, Mustang Panda actors reused previously-observed legitimate domains to host files.
Observed	US Think Tank. NGOs in Mongolia.
Tools used	PlugX and Poison Ivy.
Information	<https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/>

Naikon, Lotus Panda

Names	Naikon *(Kaspersky)* Hellsing *(Kaspersky)* Lotus Panda *(CrowdStrike)*
Country	China
Sponsor	State-sponsored, PLA Unit 78020
Motivation	Information theft and espionage
Description	Naikon is a threat group that has focused on targets around the South China Sea. The group has been attributed to the Chinese People's Liberation Army's (PLA) Chengdu Military Region Second Technical Reconnaissance Bureau (Military Unit Cover Designator 78020). While Naikon shares some characteristics with APT 30, the two groups do not appear to be exact matches.
Observed	Sectors: Defense, Energy, Government, Law Enforcement and Media. Countries: Cambodia, China, India, Indonesia, Laos, Malaysia, Myanmar, Nepal, Philippines, Saudi Arabia, Singapore, South Korea, Thailand, USA and Vietnam.
Tools used	Hdoor, Naikon, JadeRAT, NewCore RAT, PlugX, RARSTONE, Sisfader, SslMM, Sys10, Systeminfo, Tasklist, TeamViewer, WinMM and xsPlus.

Operations performed	2012	Naikon downloader/backdoor
	2013	"MsnMM" Campaigns <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205555/TheNaikonAPT-MsnMM1.pdf>
	Feb 2013	BKDR_RARSTONE RAT Last year, we reported about PlugX a breed of Remote Access Trojan (RAT) used in certain high-profile APT campaigns. We also noted some of its noteworthy techniques, which include its capability to hide its malicious codes by decrypting and loading a backdoor "executable file" directly into memory, without the need to drop the actual "executable file". Recently, we uncovered a RAT using the same technique. The new sample detected by Trend Micro as BKDR_RARSTONE.A is similar (but not) PlugX, as it directly loads a backdoor "file" in memory without dropping any "file". However, as we proceeded with our analysis, we found that BKDR_RARSTONE has some tricks of its own. <https://blog.trendmicro.com/trendlabs-security-intelligence/bkdr_rarstone-new-rat-to-watch-out-for/>
	Mar 2014	Campaign in the wake of the MH370 tragedy By March 11th, the Naikon group was actively hitting most of the nations involved in the search for MH370. The targets were extremely wide-ranging but included institutions with access to information related to the disappearance of MH370. <https://securelist.com/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/69567/>
	Sep 2015	Operation "CameraShy" <https://threatconnect.com/tag/naikon/>

Information	<https://securelist.com/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/69567/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0019/>

Neodymium

Names	Neodymium *(Microsoft)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	Neodymium is an activity group that conducted a campaign in May 2016 and has heavily targeted Turkish victims. The group has demonstrated similarity to another activity group called Promethium due to overlapping victim and campaign characteristics. Neodymium is reportedly associated closely with BlackOasis operations, but evidence that the group names are aliases has not been identified. (Microsoft) Neodymium is an activity group that is known to use a backdoor malware detected by Microsoft as Wingbird. This backdoor's characteristics closely match FinFisher, a government-grade commercial surveillance package. Data about Wingbird activity indicate that it is typically used to attack individual computers instead of networks.
Observed	Countries: Europe.
Tools used	Wingbird.
Information	<https://www.microsoft.com/security/blog/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0055/>

NetTraveler, APT 21

Names	NetTraveler *(Kaspersky)* APT 21 *(Mandiant)*
Country	China
Motivation	Information theft and espionage
Description	(Kaspersky) Over the last few years, we have been monitoring a cyber-espionage campaign that has successfully compromised more than 350 high profile victims in 40 countries. The main tool used by the threat actors during these attacks is NetTraveler, a malicious program used for covert computer surveillance. The name NetTraveler comes from an internal string which is present in early versions of the malware: NetTraveler Is Running! This malware is used by APT actors for basic surveillance of their victims. Earliest known samples have a timestamp of 2005, although references exist indicating activity as early as 2004. The largest number of samples we observed were created between 2010 and 2013.
Observed	Sectors: Defense, Embassies, Government, Oil and gas, Scientific research centers and institutes and Tibetan/Uyghur activists. Countries: Afganistan, Australia, Austria, Bangladesh, Belarus, Belgium, Cambodia, Canada, Chile, China, Germany, Greece, Hong Kong, India, Indonesia, Iran, Japan, Jordan, Kazakhstan, Kyrgyzstan, Lithuania, Malaysia, Mongolia, Morocco, Nepal, Pakistan, Qatar, Russia, Slovenia, South Korea, Spain, Suriname, Syria, Tajikistan, Thailand, Turkey, Turkmenistan, UK, Ukraine, USA and Uzbekistan.
Tools used	NetTraveler/TravNet and PlugX.
Operations performed	Aug 2014	NetTraveler Gets a Makeover for 10th Anniversary Most recently, the main focus of interest for cyber-espionage activities revolved around diplomatic (32%), government (19%), private (11%), military (9%), industrial and infrastructure (7%), airspace (6%), research (4%), activism (3%), financial (3%), IT (3%), health (2%) and press (1%). <https://www.kaspersky.com/about/press-releases/2014_nettraveler-gets-a-makeover-for-10th-anniversary>
	Dec 2015	Spear-Phishing Email Targets Diplomat of Uzbekistan Unit 42 recently identified a targeted attack against an individual working for the Foreign Ministry of Uzbekistan in China. A spear-phishing email was sent to a diplomat of the Embassy of Uzbekistan who is likely based in Beijing, China. <https://unit42.paloaltonetworks.com/nettraveler-spear-phishing-email-targets-diplomat-of-uzbekistan/>
Information	<https://www.kaspersky.com/about/press-releases/2013_kaspersky-lab-uncovers--operation-nettraveler--a-global-cyberespionage-campaign-targeting-government-affiliated-organizations-and-research-institutes> <https://www.proofpoint.com/us/threat-insight/post/nettraveler-apt-targets-russian-european-interests>

Night Dragon

Names	Night Dragon *(McAfee)*
Country	China
Motivation	Information theft and espionage
Description	(McAfee) Starting in November 2009, coordinated covert and targeted cyberattacks have been conducted against global oil, energy, and petrochemical companies. These attacks have involved social engineering, spear-phishing attacks, exploitation of Microsoft Windows operating systems vulnerabilities, Microsoft Active Directory compromises, and the use of remote administration tools (RATs) in targeting and harvesting sensitive competitive proprietary operations and project-financing information with regard to oil and gas field bids and operations. Attackers using several locations in China have leveraged C&C servers on purchased hosted services in the United States and compromised servers in the Netherlands to wage attacks against global oil, gas, and petrochemical companies, as well as individuals and executives in Kazakhstan, Taiwan, Greece, and the United States to acquire proprietary and highly confidential information. The primary operational technique used by the attackers comprised a variety of hacker tools, including privately developed and customized RAT tools that provided complete remote administration capabilities to the attacker. RATs provide functions similar to Citrix or Microsoft Windows Terminal Services, allowing a remote individual to completely control the affected system. To deploy these tools, attackers first compromised perimeter security controls, through SQL-injection exploits of extranet web servers, as well as targeted spear-phishing attacks of mobile worker laptops, and compromising corporate VPN accounts to penetrate the targeted company's defensive architectures (DMZs and firewalls) and conduct reconnaissance of targeted companies' networked computers.
Observed	Sectors: Energy, Oil and gas and Petrochemical. Countries: Greece, Kazakhstan, Netherlands, Taiwan and USA.
Tools used	ASPXSpy, Cain & Abel, gsecdump and zwShell.
Information	<https://securingtomorrow.mcafee.com/wp-content/uploads/2011/02/McAfee_NightDragon_wp_draft_to_customersv1-1.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0014/>

Nightshade Panda, APT 9, Group 27

Names	Nightshade Panda *(CrowdStrike)* APT 9 *(Mandiant)* Group 27 *(ASERT)*
Country	China
Motivation	Information theft and espionage
Description	(Softpedia) Arbor's ASERT team is now reporting that, after looking deeper at that particular campaign, and by exposing a new trail in the group's activities, they managed to identify a new RAT that was undetectable at that time by most antivirus vendors. Named Trochilus, this new RAT was part of Group 27's malware portfolio that included six other malware strains, all served together or in different combinations, based on the data that needed to be stolen from each victim. This collection of malware, dubbed the Seven Pointed Dagger by ASERT experts, included two different PlugX versions, two different Trochilus RAT versions, one version of the 3012 variant of the 9002 RAT, one EvilGrab RAT version, and one unknown piece of malware, which the team has not entirely decloaked just yet.
Observed	Sectors: Energy and Government. Countries: Myanmar and Thailand.
Tools used	9002 RAT, EvilGrab, MoonWind RAT, PlugX and Trochilus RAT.

Operations performed	Aug 2015	Operation "Seven Pointed Dagger" During that campaign, the threat actor identified as Group 27 used watering hole attacks on official Myanmar government websites to infect unsuspecting users with the PlugX malware (an RAT) when accessing information on the upcoming Myanmar elections. <https://news.softpedia.com/news/trochilus-rat-evades-antivirus-detection-used-for-cyber-espionage-in-south-east-asia-498776.shtml>
	Sep 2016	From September 2016 through late November 2016, a threat actor group used both the Trochilus RAT and a newly idenfied RAT we've named MoonWind to target organizations in Thailand, including a utility organization. We chose the name 'MoonWind' based on debugging strings we saw within the samples, as well as the compiler used to generate the samples. The attackers compromised two legitimate Thai websites to host the malware, which is a tactic this group has used in the past. <https://unit42.paloaltonetworks.com/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/>

Nitro, Covert Grove

Names	Nitro *(Symantec)* Covert Grove *(Symantec)*
Country	China
Motivation	Information theft and espionage
Description	(Symantec) The Nitro Attacks: Stealing Secrets from the Chemical Industry The attackers have changed their targets over time. From late April to early May, the attackers focused on human rights related NGOs. They then moved on to the motor industry in late May. From June until mid-July no activity was detected. At this point, the current attack campaign against the chemical industry began. This particular attack has lasted much longer than previous attacks, spanning two and a half months. A total of 29 companies in the chemical sector were confirmed to be targeted in this attack wave and another 19 in various other sectors, primarily the defense sector, were seen to be affected as well. These 48 companies are the minimum number of companies targeted and likely other companies were also targeted. In a recent two week period, 101 unique IP addresses contacted a command and control server with traffic consistent with an infected machine. These IPs represented 52 different unique Internet Service Providers or organizations in 20 countries.
Observed	Sectors: Chemical, Human Rights NGOs, Motor industry and Technology. Countries: Argentina, Bangladesh, Canada, China, Czech, Finland, France, Germany, Hong Kong, India, Japan, Netherlands, Norway, Russia, Singapore, South Korea, Sweden, Taiwan, UK and USA.
Tools used	Farfli, PCClient, Poison Ivy and Spindest.
Operations performed	Jul 2014	New Indicators of Compromise found Historically, Nitro is known for targeted spear phishing campaigns and using Poison Ivy malware, which was not seen in these attacks. Since at least 2013, Nitro appears to have somewhat modified their malware and delivery methods to include Spindest and legitimate compromised websites, as reported by Cyber Squared's TCIRT. <https://unit42.paloaltonetworks.com/new-indicators-compromise-apt-group-nitro-uncovered/>
Information	<https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf> <https://blog.trendmicro.com/trendlabs-security-intelligence/the-significance-of-the-nitro-attacks/>

OilRig, APT 34, Helix Kitten

Names	OilRig *(Palo Alto)* APT 34 *(FireEye)* Helix Kitten *(CrowdStrike)* Twisted Kitten *(CrowdStrike)* Crambus *(Symantec)* Chrysene *(Dragos)*
Country	Iran
Motivation	Information theft and espionage
Description	OilRig is a threat group with suspected Iranian origins that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East. It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. FireEye assesses that the group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests. This group was previously tracked under two distinct groups, APT 34 and OilRig, but was combined due to additional reporting giving higher confidence about the overlap of the activity. OilRig seems to be closely related to APT 33, Elfin.
Observed	Sectors: Chemical, Energy, Financial, Government and Telecommunications. Countries: Iraq, Israel, Kuwait, Lebanon, Pakistan, Qatar, Saudi Arabia. Turkey, UAE, UK and USA.
Tools used	Alma Communicator, BONDUPDATER, certutil, DistTrack, Fox Panel, Glimpse, GoogleDrive RAT, Helminth, HighShell, HyperShell, IRN2, ISMAgent, ISMDoor, ISMInjector, Jason, LaZagne, Mimikatz, OopsIE, PoisonFrog, POWRUNER, QUADAGENT, RGDoor, SEASHARPEE, Shamoon, SpyNote, StoneDrill, Systeminfo, Tasklist, TwoFace and Webmask.
Operations performed	Aug 2012	Shamoon Attacks W32.Disttrack is a new threat that is being used in specific targeted attacks against at least one organization in the energy sector. It is a destructive malware that corrupts files on a compromised computer and overwrites the MBR (Master Boot Record) in an effort to render a computer unusable. Target: Saudi Aramco and Rasgas. <https://www.symantec.com/connect/blogs/shamoon-attacks>
	May 2016	Targeted Attacks against Banks in the Middle East In the first week of May 2016, FireEye's DTI identified a wave of emails containing malicious attachments being sent to multiple banks in the Middle East region. The threat actors appear to be performing initial reconnaissance against would-be targets, and the attacks caught our attention since they were using unique scripts not commonly seen in crimeware campaigns. <https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksaga.html> <https://unit42.paloaltonetworks.com/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/>

	Nov 2016	Shamoon v2 The malware used in the recent attacks (W32.Disttrack.B) is largely unchanged from the variant used four years ago. In the 2012 attacks, infected computers had their master boot records wiped and replaced with an image of a burning US flag. The latest attacks instead used a photo of the body of Alan Kurdi, the three year-old Syrian refugee who drowned in the Mediterranean last year. <https://www.symantec.com/connect/blogs/shamoon-back-dead-and-destructive-ever>
	Jun 2016	We have identified two separate testing efforts carried out by the OilRig actors, one occurring in June and one in November of 2016. The sample set associated with each of these testing activities is rather small, but the changes made to each of the files give us a chance to understand what modifications the actor performs in an attempt to evade detection. This testing activity also suggests that the threat group responsible for the OilRig attack campaign have an organized, professional operations model that includes a testing component to the development of their tools. <https://unit42.paloaltonetworks.com/unit42-oilrig-actors-provide-glimpse-development-testing-efforts/>
	Oct 2016	In recent weeks we've discovered that the group have been actively updating their Clayslide delivery documents, as well as the Helminth backdoor used against victims. Additionally, the scope of organizations targeted by this group has expanded to not only include organizations within Saudi Arabia, but also a company in Qatar and government organizations in Turkey, Israel and the United States. <https://unit42.paloaltonetworks.com/unit42-oilrig-malware-campaign-updates-toolset-and-expands-targets/>
	Jan 2017	Delivers Digitally Signed Malware, Impersonates University of Oxford In recent attacks they set up a fake VPN Web Portal and targeted at least five Israeli IT vendors, several financial institutes, and the Israeli Post Office. Later, the attackers set up two fake websites pretending to be a University of Oxford conference sign-up page and a job application website. In these websites they hosted malware that was digitally signed with a valid, likely stolen code signing certificate. <https://www.clearskysec.com/oilrig/>
	Jun 2017	In July 2017, we observed the OilRig group using a tool they developed called ISMAgent in a new set of targeted attacks. The OilRig group developed ISMAgent as a variant of the ISMDoor Trojan. In August 2017, we found this threat group has developed yet another Trojan that they call 'Agent Injector' with the specific purpose of installing the ISMAgent backdoor. We are tracking this tool as ISMInjector. <https://unit42.paloaltonetworks.com/unit42-oilrig-group-steps-attacks-new-delivery-documents-new-injector-trojan/>
	Jul 2017	The web server logs on the system we examined that was compromised with the TwoFace shell gave us a glimpse into the commands the actor executed through their malware. These commands also enabled us to create a profile of the actor, specifically

		their intentions and the tools and techniques used to carry out their operation. <https://unit42.paloaltonetworks.com/unit42-twoface-webshell-persistent-access-point-lateral-movement/>
	Sep 2017	While expanding our research into the TwoFace webshell from this past July, we were able to uncover several IP addresses that logged in and directly interfaced with the shell we discovered and wrote about. Investigating deeper into these potential adversary IPs revealed a much larger infrastructure used to execute the attacks. <https://unit42.paloaltonetworks.com/unit42-striking-oil-closer-look-adversary-infrastructure/>
	Nov 2017	New Targeted Attack in the Middle East In this latest campaign, APT34 leveraged the recent Microsoft Office vulnerability CVE-2017-11882 to deploy POWRUNER and BONDUPDATER. <https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html>
	Jan 2018	On January 8, 2018, Unit 42 observed the OilRig threat group carry out an attack on an insurance agency based in the Middle East. Just over a week later, on January 16, 2018, we observed an attack on a Middle Eastern financial institution. In both attacks, the OilRig group attempted to deliver a new Trojan that we are tracking as OopsIE. The January 8 attack used a variant of the ThreeDollars delivery document, which we identified as part of the OilRig toolset based on attacks that occurred in August 2017. <https://unit42.paloaltonetworks.com/unit42-oopsie-oilrig-uses-threedollars-deliver-new-trojan/>
	Jan 2018	While investigating files uploaded to a TwoFace webshell, Unit 42 discovered actors installing an Internet Information Services (IIS) backdoor that we call RGDoor. Our data suggests that actors have deployed the RGDoor backdoor on webservers belonging to eight Middle Eastern government organizations, as well as one financial and one educational institution. <https://unit42.paloaltonetworks.com/unit42-oilrig-uses-rgdoor-iis-backdoor-targets-middle-east/>
	May 2018	Technology Service Provider and Government Agency Between May and June 2018, Unit 42 observed multiple attacks by the OilRig group appearing to originate from a government agency in the Middle East. Based on previously observed tactics, it is highly likely the OilRig group leveraged credential harvesting and compromised accounts to use the government agency as a launching platform for their true attacks. <https://unit42.paloaltonetworks.com/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/>
	Dec 2018	Shamoon v3 After a two-year absence, the destructive malware Shamoon (W32.Disttrack.B) re-emerged on December 10 in a new wave of attacks against targets in the Middle East. These latest Shamoon attacks are doubly destructive, since they involve a new wiper

		(Trojan.Filerase) that deletes files from infected computers before the Shamoon malware wipes the master boot record. <https://www.symantec.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail> <https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/shamoon-attackers-employ-new-tool-kit-to-wipe-infected-systems/>
	Mar 2019	In an incident reminiscent of the Shadow Brokers leak that exposed the NSA's hacking tools, someone has now published similar hacking tools belonging to one of Iran's elite cyber-espionage units, known as APT34, Oilrig, or HelixKitten. <https://www.zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram/>
	Jun 2019	A new hacking tool believed to have been in the arsenal of Iranian state hackers has been published today online, in a Telegram channel. This new tool is named Jason and was published online earlier today in the same Telegram channel where the leaker -- going by the name of Lab Dookhtegan -- dumped the six other previous hacking tools. <https://www.zdnet.com/article/new-iranian-hacking-tool-leaked-on-telegram/>
Information		<https://unit42.paloaltonetworks.com/unit42-striking-oil-closer-look-adversary-infrastructure/> <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-november-helix-kitten/>
MITRE ATT&CK		<https://attack.mitre.org/groups/G0049/>

Subgroup: Greenbug

Names	Greenbug *(Symantec)*
Country	Iran
Description	(Symantec) Symantec discovered the Greenbug cyberespionage group during its investigation into previous attacks involving W32.Disttrack.B (aka Shamoon). Shamoon (W32.Disttrack) first made headlines in 2012 when it was used in attacks against energy companies in Saudi Arabia. It recently resurfaced in November 2016 (W32.Disttrack.B), again attacking targets in Saudi Arabia. While these attacks were covered extensively in the media, how the attackers stole these credentials and introduced W32.Disttrack on targeted organizations' networks remains a mystery. Could Greenbug be responsible for getting Shamoon those stolen credentials? Although there is no definitive link between Greenbug and Shamoon, the group compromised at least one administrator computer within a Shamoon-targeted organization's network prior to W32.Disttrack.B being deployed on November 17, 2016.
Operations performed	Nov 2016	Greenbug cyberespionage group targeting Middle East, possible links to Shamoon <https://www.symantec.com/connect/blogs/greenbug-cyberespionage-group-targeting-middle-east-possible-links-shamoon>
	May 2017	Researchers have identified a possible new collaborator in the continued Shamoon attacks against Saudi organizations. Called Greenbug, this group is believed to be instrumental in helping Shamoon steal user credentials of targets ahead of Shamoon's destructive attacks. <https://threatpost.com/shamoon-collaborator-greenbug-adopts-new-communication-tool/125383/>
	Jul 2017	OilRig Uses ISMDoor Variant; Possibly Linked to Greenbug Threat Group In July 2017, we observed an attack on a Middle Eastern technology organization that was also targeted by the OilRig campaign in August 2016. Initial inspection of this attack suggested this was again the OilRig campaign using their existing toolset, but further examination revealed not only new variants of the delivery document we named Clayslide, but also a different payload embedded inside it. <https://unit42.paloaltonetworks.com/unit42-oilrig-uses-ismdoor-variant-possibly-linked-greenbug-threat-group/>
	Oct 2017	Iranian Threat Agent Greenbug has been registering domains similar to those of Israeli High-Tech and Cyber Security Companies. On 15 October 2017 a sample of ISMdoor was submitted to VirusTotal from Iraq. <https://www.clearskysec.com/greenbug/>

Operation BugDrop

Names	Operation BugDrop *(CyberX)*
Country	Russia
Motivation	Information theft and espionage
Description	(CyberX) CyberX has discovered a new, large-scale cyber-reconnaissance operation targeting a broad range of targets in the Ukraine. Because it eavesdrops on sensitive conversations by remotely controlling PC microphones – in order to surreptitiously "bug" its targets – and uses Dropbox to store exfiltrated data, CyberX has named it "Operation BugDrop." CyberX has confirmed at least 70 victims successfully targeted by the operation in a range of sectors including critical infrastructure, media, and scientific research. The operation seeks to capture a range of sensitive information from its targets including audio recordings of conversations, screen shots, documents and passwords. Unlike video recordings, which are often blocked by users simply placing tape over the camera lens, it is virtually impossible to block your computer's microphone without physically accessing and disabling the PC hardware.
Observed	Sectors: Engineering, Oil and gas, Media and Research. Countries: Austria, Saudi Arabia, Russia and Ukraine.
Tool used	Dropbox.
Information	<https://cyberx-labs.com/blog/operation-bugdrop-cyberx-discovers-large-scale-cyber-reconnaissance-operation/>

Operation Ghoul

Names	Operation Ghoul *(Kaspersky)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(Kaspersky) Kaspersky Lab has observed new waves of attacks that started on the 8th and the 27th of June 2016. These have been highly active in the Middle East region and unveiled ongoing targeted attacks in multiple regions. The attackers try to lure targets through spear phishing emails that include compressed executables. The malware collects all data such as passwords, keystrokes and screenshots, then sends it to the attackers. We found that the group behind this campaign targeted mainly industrial, engineering and manufacturing organizations in more than 30 countries. In total, over 130 organizations have been identified as victims of this campaign. Using the Kaspersky Security Network (KSN) and artifacts from malware files and attack sites, we were able to trace the attacks back to March 2015. Noteworthy is that since the beginning of their activities, the attackers' motivations are apparently financial, whether through the victims' banking accounts or through selling their intellectual property to interested parties, most infiltrated victim organizations are considered SMBs (Small to Medium size businesses, 30-300 employees), the utilization of commercial off-the-shelf malware makes the attribution of the attacks more difficult.
Observed	Sectors: Education, Engineering, Industrial, Manufacturing, IT, Pharmaceutical, Shipping and Logistics, Tourism and Trading. Countries: Azerbaijan, China, Egypt, France, Germany, Gilbraltar, India, Iran, Iraq, Italy, Pakistan, Portugal, Romania, Qatar, Saudi Arabia, Spain, Sweden, Switzerland, Taiwan, Turkey, UAE, UK and USA.
Tool used	ShopBot.
Information	<https://securelist.com/operation-ghoul-targeted-attacks-on-industrial-and-engineering-organizations/75718/>

Operation Groundbait

Names	Operation Groundbait *(ESET)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(ESET) After BlackEnergy, which has, most infamously, facilitated attacks that resulted in power outages for hundreds of thousands of Ukrainian civilians, and Operation Potao Express, where attackers went after sensitive TrueCrypt-protected data from high value targets, ESET researchers have uncovered another cyberespionage operation in Ukraine: Operation Groundbait. The main point that sets Operation Groundbait apart from the other attacks is that it has mostly been targeting anti-government separatists in the self-declared Donetsk and Luhansk People's Republics. While the attackers seem to be more interested in separatists and the self-declared governments in eastern Ukrainian war zones, there have also been a large number of other targets, including, among others, Ukrainian government officials, politicians and journalists.
Observed	Sectors: Government, politicians and journalists. Countries: Ukraine.
Tool used	Prikormka.
Information	<https://www.welivesecurity.com/2016/05/18/groundbait/>

Operation Parliament

Names	Operation Parliament *(Kaspersky)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(Kaspersky) Based on our findings, we believe the attackers represent a previously unknown geopolitically motivated threat actor. The campaign started in 2017, with the attackers doing just enough to achieve their goals. They most likely have access to additional tools when needed and appear to have access to an elaborate database of contacts in sensitive organizations and personnel worldwide, especially of vulnerable and non-trained staff. The victim systems range from personal desktop or laptop systems to large servers with domain controller roles or similar. The nature of the targeted ministries varied, including those responsible for telecommunications, health, energy, justice, finance and so on. Operation Parliament appears to be another symptom of escalating tensions in the Middle East region. The attackers have taken great care to stay under the radar, imitating another attack group in the region. They have been particularly careful to verify victim devices before proceeding with the infection, safeguarding their command and control servers. The targeting seems to have slowed down since the beginning of 2018, probably winding down when the desired data or access was obtained. The targeting of specific victims is unlike previously seen behavior in regional campaigns by Gaza Cybergang or Desert Falcons and points to an elaborate information-gathering exercise that was carried out before the attacks (physical and/or digital). With deception and false flags increasingly being employed by threat actors, attribution is a hard and complicated task that requires solid evidence, especially in complex regions such as the Middle East.
Observed	Sectors: Defense, Education, Energy, Financial, Government, Healthcare, Media, Research, Shipping and Logistics, Sports and Telecommunications. Countries: Afghanistan, Canada, Chile, Denmark, Djibouti, Egypt, Germany, India, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Morocco, Oman, Palestine, Qatar, Russia, Saudi Arabia, Serbia, Somalia, South Korea, Syria, UAE, UK and USA.
Tool used	Remote CMD/PowerShell terminal.
Information	<https://securelist.com/operation-parliament-who-is-doing-what/85237/> <https://blog.talosintelligence.com/2018/02/targeted-attacks-in-middle-east.html>

Operation Potao Express

Names	Operation Potao Express *(ESET)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(ESET) We presented our initial findings based on research into the Win32/Potao malware family in June, in our CCCC 2015 presentation in Copenhagen. Today, we are releasing the full whitepaper on the Potao malware with additional findings, the cyberespionage campaigns where it was employed, and its connection to a backdoor in the form of a modified version of the TrueCrypt encryption software. Like BlackEnergy, the malware used by the so-called Sandworm APT group (also known as Quedagh), Potao is an example of targeted espionage malware directed mostly at targets in Ukraine and a number of other post-Soviet countries, including Russia, Georgia and Belarus.
Observed	Countries: Belarus, Georgia, Russia and Ukraine.
Tool used	FakeTC and Patao.
Information	<https://www.welivesecurity.com/wp-content/uploads/2015/07/Operation-Potao-Express_final_v2.pdf>

Orangeworm

Names	Orangeworm *(Symantec)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(Symantec) Symantec has identified a previously unknown group called Orangeworm that has been observed installing a custom backdoor called Trojan.Kwampirs within large international corporations that operate within the healthcare sector in the United States, Europe, and Asia. First identified in January 2015, Orangeworm has also conducted targeted attacks against organizations in related industries as part of a larger supply-chain attack in order to reach their intended victims. Known victims include healthcare providers, pharmaceuticals, IT solution providers for healthcare and equipment manufacturers that serve the healthcare industry, likely for the purpose of corporate espionage. Based on the list of known victims, Orangeworm does not select its targets randomly or conduct opportunistic hacking. Rather, the group appears to choose its targets carefully and deliberately, conducting a good amount of planning before launching an attack. According to Symantec telemetry, almost 40 percent of Orangeworm's confirmed victim organizations operate within the healthcare industry. The Kwampirs malware was found on machines which had software installed for the use and control of high-tech imaging devices such as X-Ray and MRI machines. Additionally, Orangeworm was observed to have an interest in machines used to assist patients in completing consent forms for required procedures. The exact motives of the group are unclear.
Observed	Sectors: Healthcare, as well as related industries as part of a larger supply-chain attack such as Healthcare providers, Manufacturing, IT and Pharmaceuticals. Countries: Belgium, Brazil, Canada, Chile, China, France, Germany, Hong Kong, Hungary, India, Malaysia, Netherlands, Norway, Philippines, Poland, Saudi Arabia, Spain, Sweden, Switzerland, Turkey, UK and USA.
Tools used	Kwampirs and Systeminfo.
Information	<https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0071/>

PassCV

Names	PassCV *(Blue Coat Systems)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	(Cylance) Snorre Fagerland of Blue Coat Systems first coined the term PassCV in a blog post. His post provides a good introduction to the group and covers some of the older infrastructure, stolen code-signing certificate reuse, and other connections associated with the PassCV malware. There are several clues alluding to the possibility that multiple groups may be utilizing the same stolen signing certificates, but at this time SPEAR believes the current attacks are more likely being perpetrated by a single group employing multiple publicly available Remote Administration Tools (RATs). The PassCV group has been operating with continued success and has already started to expand their malware repertoire into different off-the-shelf RATs and custom code. SPEAR identified eighteen previously undisclosed stolen Authenticode certificates. These certificates were originally issued to companies and individuals scattered across China, Taiwan, Korea, Europe, the United States and Russia. The PassCV group typically utilized publicly available RATs in addition to some custom code, which ultimately provided backdoor functionality to affected systems via phony resumes and curriculum vitae (CVs). PassCV continues to maintain a heavy reliance on obfuscated and signed versions of older RATs like ZxShell and Ghost RAT, which have remained a favorite of the wider Chinese criminal community since their initial public release.
Observed	Sectors: Online videogame companies. Countries: China, Europe, Russia, South Korea, Taiwan and USA.
Tools used	Cobalt Strike, Gh0st RAT, Kitkiot, Netwire, Sabresac, Winnti and ZXShell
Information	<https://threatvector.cylance.com/en_us/home/digitally-signed-malware-targeting-gaming-companies.html>

Patchwork, Dropping Elephant

Names	Patchwork *(Cymmetria)*
	Dropping Elephant *(Kaspersky)*
	Chinastrats *(Kaspersky)*
	APT-C-09 *(360)*
	Monsoon *(Forcepoint)*
	Quilted Tiger *(CrowdStrike)*
Country	India
Motivation	Information theft and espionage
Description	(Cymmetria) Patchwork is a targeted attack that has infected an estimated 2,500 machines since it was first observed in December 2015. There are indications of activity as early as 2014, but Cymmetria has not observed any such activity first hand.
	Patchwork targets were chosen worldwide with a focus on personnel working on military and political assignments, and specifically those working on issues relating to Southeast Asia and the South China Sea. Many of the targets were governments and government-related organizations.
	The code used by this threat actor is copy-pasted from various online forums, in a way that reminds us of a patchwork quilt –hence the name we've given the operation.
	In active victim systems, Patchwork immediately searches for and uploads documents to their C&C, and only if the target is deemed valuable enough, proceeds to install a more advanced second stage malware.
	This group seems to be associated with Confucius.
Observed	Sectors: Aviation, Defense, Energy, Financial, Government, IT, Media, NGOs, Pharmaceutical and Think Tanks.
	Countries: China, Japan, Middle East, UK, USA and Southeast Asia, many of the target countries are in the area surrounding the Indian subcontinent (Bangladesh, Sri Lanka and Pakistan).
Tools used	AndroRAT, AutoIt backdoor, BADNEWS, Bahamut, MazeRunner, NdiskMonitor, PowerSploit, QuasarRAT, Sarit, Socksbot, Steladoc, TINYTYPHON WSCSPL and Unknown Logger.
Operations performed	2015	The attack was detected as part of a spear phishing against a government organization in Europe in late May 2016. The target was an employee working on Chinese policy research and the attack vector was a PowerPoint presentation file. The content of the presentation was on issues relating to Chinese activity in the South China Sea. <https://s3-us-west-2.amazonaws.com/cymmetria-blog/public/Unveiling_Patchwork.pdf>
	Mar 2018	Targeting US Think Tanks
		In March and April 2018, Volexity identified multiple spear phishing campaigns attributed to Patchwork, an Indian APT group also known as Dropping Elephant. This increase in threat activity was consistent with other observations documented over the last few months in blogs by 360 Threat Intelligence Center analyzing attacks on Chinese organizations and Trend Micro noting targets in South Asia.

		<https://www.volexity.com/blog/2018/06/07/patchwork-apt-group-targets-us-think-tanks/>
Information		<https://s3-us-west-2.amazonaws.com/cymmetria-blog/public/Unveiling_Patchwork.pdf> <https://www.symantec.com/connect/blogs/patchwork-cyberespionage-group-expands-targets-governments-wide-range-industries> <https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf> <https://securelist.com/the-dropping-elephant-actor/75328/> <https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0040/>	

Pirate Panda, APT 23, KeyBoy

Names	Pirate Panda *(CrowdStrike)* APT 23 (*Mandiant)* KeyBoy *(Rapid7)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	(Rapid7) In this blog post we'll analyze two specific incidents apparently targeting victims in Vietnam and in India and we'll describe the capabilities of the custom backdoor being used that for convenience (and to our knowledge, for a lack of an existing name) we call KeyBoy, due to a string present in one of the samples.
Observed	Countries: India and Vietnam.
Tools used	CREDRIVER.
Information	<https://blog.rapid7.com/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india/> <https://blogs.cisco.com/security/scope-of-keyboy-targeted-malware-attacks> <https://citizenlab.ca/2016/11/parliament-keyboy/>

PittyTiger, Pitty Panda

Names	PittyTiger *(FireEye)* Pitty Panda *(CrowdStrike)* Manganese *(Microsoft)*
Country	China
Motivation	Information theft and espionage
Description	(Airbus) Pitty Tiger is a group of attackers that have been active since at least 2011. They have targeted private companies in several sectors, such as defense and telecommunications, but also at least one government. We have been able to track down this group of attackers and can provide detailed information about them. We were able to collect and reveal their "malware arsenal". We also analyzed their technical organization. Our investigations indicate that Pitty Tiger has not used any 0day vulnerability so far, rather they prefer using custom malware, developed for the group's exclusive usage. Our discoveries indicate that Pitty Tiger is a group of attackers with the ability to stay under the radar, yet still not as mature as other groups of attackers we monitor. Pitty Tiger is probably not a state-sponsored group of attackers. They lack the experience and financial support that one would expect from state-sponsored attackers. We suppose this group is opportunistic and sells its services to probable competitors of their targets in the private sector. We have been able to leverage several attackers profiles, showing that the Pitty Tiger group is fairly small compared to other APT groups, which is probably why we saw them work on a very limited amount of targets.
Observed	Sectors: Defense, Government, Telecommunications and Web development. Countries: Europe and Taiwan.
Tools used	Gh0st RAT, gsecdump, Lurid, Mimikatz, Paladin, pgift, Pitty and Poison Ivy.

Operations performed	2011	Operation "The Eye of the Tiger" <https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/2014.07.11.Pitty_Tiger/Pitty_Tiger_Final_Report.pdf>
	Jun 2014	We discovered this malware sample in June 2014, leading to a command & control (c&c) server still in activity. Our researches around the malware family revealed the "Pitty Tiger" group has been active since 2011, yet we found traces which makes us believe the group is active since 2010. <http://blog.cassidiancybersecurity.com/post/2014/07/The-Eye-of-the-Tiger2>
	Jul 2014	During the last month, McAfee Labs researchers have uncovered targeted attacks carried out via spear phishing email against a French company. We have seen email sent to a large group of individuals in the organization. <https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/targeted-attacks-on-french-company-exploit-multiple-word-vulnerabilities/>

	2014	In a recent attack against a French company, the attackers sent simple, straightforward messages in English and French from free email addresses using names of actual employees of the targeted company. <https://www.fireeye.com/blog/threat-research/2014/07/spy-of-the-tiger.html>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0011/>	

Platinum

Names	Platinum *(Microsoft)* TwoForOne *(Kaspersky)*
Country	China
Motivation	Information theft and espionage
Description	(Microsoft) Platinum has been targeting its victims since at least as early as 2009, and may have been active for several years prior. Its activities are distinctly different not only from those typically seen in untargeted attacks, but from many targeted attacks as well. A large share of targeted attacks can be characterized as opportunistic: the activity group changes its target profiles and attack geographies based on geopolitical seasons, and may attack institutions all over the world. Like many such groups, Platinum seeks to steal sensitive intellectual property related to government interests, but its range of preferred targets is consistently limited to specific governmental organizations, defense institutes, intelligence agencies, diplomatic institutions, and telecommunication providers in South and Southeast Asia. The group's persistent use of spear-phishing tactics (phishing attempts aimed at specific individuals) and access to previously undiscovered zero-day exploits have made it a highly resilient threat.
Observed	Sectors: Defense, Government, Intelligence agencies and Telecommunications. Countries: China, India, Indonesia, Malaysia, Singapore and Thailand.
Tools used	adbupd, AMTsol, Dipsind and JPIN.
Operations performed	2017	Since the 2016 publication, Microsoft has come across an evolution of PLATINUM's file-transfer tool, one that uses the Intel Active Management Technology (AMT) Serial-over-LAN (SOL) channel for communication. This channel works independently of the operating system (OS), rendering any communication over it invisible to firewall and network monitoring applications running on the host device. Until this incident, no malware had been discovered misusing the AMT SOL feature for communication. <https://www.microsoft.com/security/blog/2017/06/07/platinum-continues-to-evolve-find-ways-to-maintain-invisibility>
	Middle 2017	Operation "EasternRoppels" In the middle of 2017, Kaspersky Lab experts discovered a new malicious threat that is believed to be related to the famous PLATINUM APT group, which had been widely regarded as inactive. They named the campaign 'EasternRoppels'. <https://aavar.org/avar2018/index.php/the-easternroppels-operation-platinum-group-is-back/> <https://securelist.com/platinum-is-back/91135/>
Information	<https://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0068/>

Poseidon Group

Names	Poseidon Group *(Kaspersky)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(Kaspersky) During the latter part of 2015, Kaspersky researchers from GreAT (Global Research and Analysis Team) got hold of the missing pieces of an intricate puzzle that points to the dawn of the first Portuguese-speaking targeted attack group, named "Poseidon." The group's campaigns appear to have been active since at least 2005, while the very first sample found points to 2001. This signals just how long ago the Poseidon threat actor was already working on its offensive framework. The Poseidon Group is a long-running team operating on all domains: land, air, and sea. They are dedicated to running targeted attacks campaigns to aggressively collect information from company networks through the use of spear-phishing packaged with embedded, executable elements inside office documents and extensive lateral movement tools. The information exfiltrated is then leveraged by a company front to blackmail victim companies into contracting the Poseidon Group as a security firm. Even when contracted, the Poseidon Group may continue its infection or initiate another infection at a later time, persisting on the network to continue data collection beyond its contractual obligation. The Poseidon Group has been active, using custom code and evolving their toolkit since at least 2005. Their tools are consistently designed to function on English and Portuguese systems spanning the gamut of Windows OS, and their exfiltration methods include the use of hijacked satellite connections. Poseidon continues to be active at this time.
Observed	Sectors: Energy, Financial, Government, Media, Manufacturing, Telecommunications and Utilities. Countries: Brazil, France, India, Kazakhstan, Russia, UAE and USA.
Tools used	IGT supertool.
Information	<https://securelist.com/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/73673/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0033/>

Promethium

Names	Promethium *(Microsoft)* StrongPity *(Kaspersky)*
Country	Turkey
Motivation	Information theft and espionage
Description	Promethium is an activity group that has been active since at least 2012. The group conducted a campaign in May 2016 and has heavily targeted Turkish victims. Promethium has demonstrated similarity to another activity group called Neodymium due to overlapping victim and campaign characteristics. (Microsoft) Promethium is an activity group that has been active as early as 2012. The group primarily uses Truvasys, a first-stage malware that has been in circulation for several years. Truvasys has been involved in several attack campaigns, where it has masqueraded as one of server common computer utilities, including WinUtils, TrueCrypt, WinRAR, or SanDisk. In each of the campaigns, Truvasys malware evolved with additional features—this shows a close relationship between the activity groups behind the campaigns and the developers of the malware.
Observed	Countries: Europe and Turkey.
Tools used	Truvasys.
Information	<https://www.microsoft.com/security/blog/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0056/>

Putter Panda, APT 2

Names	Putter Panda *(CrowdStrike)* TG-6952 *(SecureWorks)* APT 2 *(Mandiant)* Group 36 (Talos) Sulphur *(Microsoft)*
Country	China
Sponsor	State-sponsored, Unit 61486 of the 12th Bureau of the PLA's 3rd General Staff Department (GSD).
Motivation	Information theft and espionage
Description	Putter Panda is the name of bad actor responsible for a series of cyberespionage operations originating in Shanghai, security experts linked its operation to the activity of the People's Liberation Army 3rd General Staff Department 12th Bureau Unit 61486. A fake yoga brochure was one of different emails used for a spear-phishing campaign conducted by the stealth Chinese cyber unit according an investigation conducted by researchers at the CrowdStrike security firm. Also in this case the experts believe that we are facing with a large scale cyberespionage campaign targeting government entities, contractors and research companies in Europe, USA and Japan. The group has been operating since at least 2007 and appears very interested in research companies in the space and satellite industry, experts at CrowdStrike have collected evidence of a numerous attacks against these industries.
Observed	Sectors: Defense, Government, Research and Technology (Communications, Space, Aerospace). Countries: USA.
Tools used	3PARA RAT, 4H RAT, httpclient, MSUpdater, pngdowner and SearchFire.
Information	<https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0024/>

Rancor

Names	Rancor *(Palo Alto)* Rancor Group *(Palo Alto)*
Country	China
Motivation	Information theft and espionage
Description	(Palo Alto) Throughout 2017 and 2018 Unit 42 has been tracking and observing a series of highly targeted attacks focused in South East Asia, building on our research into the KHRAT Trojan. Based on the evidence, these attacks appear to be conducted by the same set of attackers using previously unknown malware families. In addition, these attacks appear to be highly targeted in their distribution of the malware used, as well as the targets chosen. Based on these factors, Unit 42 believes the attackers behind these attacks are conducting their campaigns for espionage purposes. We believe this group is previously unidentified and therefore have we have dubbed it "Rancor". The Rancor group's attacks use two primary malware families which we describe in depth later in this blog and are naming DDKONG and PLAINTEE. DDKONG is used throughout the campaign and PLAINTEE appears to be new addition to these attackers' toolkit.
Observed	Sectors, Government and political entities. Countries: Southeast Asia (at least Cambodia and Singapore).
Tools used	certutil, DDKONG and PLAINTEE.
Information	<https://unit42.paloaltonetworks.com/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0075/>

Reaper, APT 37, Ricochet Chollima

Names	Reaper *(FireEye)* APT 37 *(Mandiant)* Ricochet Chollima *(CrowdStrike)* Group 123 *(Talos)* Red Eyes *(AhnLab)* Venus 121 *(ESRC)*
Country	North Korea
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	Some research organizations link this group to Lazarus Group, Hidden Cobra, Labyrinth Chollima. (FireEye) Read our report, APT37 (Reaper): The Overlooked North Korean Actor, to learn more about our assessment that this threat actor is working on behalf of the North Korean government, as well as various other details about their operations: • Targeting: Primarily South Korea – though also Japan, Vietnam and the Middle East – in various industry verticals, including chemicals, electronics, manufacturing, aerospace, automotive, and healthcare. • Initial Infection Tactics: Social engineering tactics tailored specifically to desired targets, strategic web compromises typical of targeted cyberespionage operations, and the use of torrent file-sharing sites to distribute malware more indiscriminately. • Exploited Vulnerabilities: Frequent exploitation of vulnerabilities in Hangul Word Processor (HWP), as well as Adobe Flash. The group has demonstrated access to zero-day vulnerabilities (CVE-2018-0802), and the ability to incorporate them into operations. • Command and Control Infrastructure: Compromised servers, messaging platforms, and cloud service providers to avoid detection. The group has shown increasing sophistication by improving their operational security over time. • Malware: A diverse suite of malware for initial intrusion and exfiltration. Along with custom malware used for espionage purposes, APT37 also has access to destructive malware.
Observed	Sectors: Aerospace, Automotive, Chemical, Financial, Government, Healthcare, Manufacturing and Technology. Countries: China, India, Japan, Kuwait, Nepal, Romania, Russia, South Korea, UK and Vietnam.
Tools used	CORALDECK, DOGCALL, Final1stSpy, Freenki Loader, HAPPYWORK, KARAE, KevDroid, N1stAgent, NavRAT, Nokki, PoohMilk Loader, POORAIM, ROKRAT, SHUTTERSPEED, SLOWDRIFT, WINERACK and several 0-day Flash and MS Office exploits.
Operations performed	2012	Spying on South Korean users.
	Aug 2016	Operation "Golden Time" Target: South Korean users. Method: spear-phishing emails combined with malicious HWP documents created using Hancom Hangul Office Suite.

	Nov 2016	Operation "Evil New Year" Target: South Korean users. Method: spear-phishing emails combined with malicious HWP documents created using Hancom Hangul Office Suite.
	Mar 2017	Operation "Are You Happy?" Target: South Korean users. Method: Not only to gain access to the remote infected systems but to also wipe the first sectors of the device.
	May 2017	Operation "FreeMilk" Target: Several non-Korean financial institutions. Method: A malicious Microsoft Office document, a deviation from their normal use of Hancom documents. <https://unit42.paloaltonetworks.com/unit42-freemilk-highly-targeted-spear-phishing-campaign/>
	Nov 2017	Operation "North Korean Human Right" Target: South Korean users. Method: Spear-phishing emails combined with malicious HWP documents created using Hancom Hangul Office Suite.
	Jan 2018	Operation "Evil New Year 2018" Target: South Korean users. Method: Spear-phishing emails combined with malicious HWP documents created using Hancom Hangul Office Suite.
	May 2018	Operation "Onezero" <https://brica.de/alerts/alert/public/1215993/analysis-of-apt-attack-on-operation-onezero-conducted-as-a-document-on-panmunjom-declaration/>
	Aug 2018	Operation "Rocket Man" <https://brica.de/alerts/alert/public/1226363/the-latest-apt-campaign-of-venus-121-group-operation-rocket-man/>
	Nov 2018	Operation "Korean Sword" <https://brica.de/alerts/alert/public/1252896/venus-121-apt-organization-operation-high-expert/>
	Jan 2019	Operation "Holiday Wiper" <https://brica.de/alerts/alert/public/1252896/venus-121-apt-organization-operation-high-expert/>
	Mar 2019	Operation "Golden Bird" <https://brica.de/alerts/alert/public/1252896/venus-121-apt-organization-operation-high-expert/>
	Mar 2019	Operation "High Expert" <https://brica.de/alerts/alert/public/1252896/venus-121-apt-organization-operation-high-expert/>
	Apr 2019	Operation "Black Banner" <https://brica.de/alerts/alert/public/1257351/venus-121-rocketman-campaign-operation-black-banner-apt-attack/>
Information	<https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html>	

| MITRE ATT&CK | <https://attack.mitre.org/groups/G0067/> |

Roaming Tiger

Names	Roaming Tiger *(ESET)*
Country	Russia
Motivation	Information theft and espionage
Description	(Palo Alto) In late 2014, ESET presented an attack campaign that had been observed over a period of time targeting Russia and other Russian speaking nations, dubbed "Roaming Tiger". The attack was found to heavily rely on RTF exploits and at the time, thought to make use of the PlugX malware family.
Observed	Countries: Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, Ukraine and Uzbekistan.
Tools used	BBSRAT, Gh0st RAT and PlugX.
Operations performed	Aug 2015	<https://unit42.paloaltonetworks.com/bbsrat-attacks-targeting-russian-organizations-linked-to-roaming-tiger/>
Information	<http://2014.zeronights.org/assets/files/slides/roaming_tiger_zeronights_2014.pdf>

RTM

Names	RTM *(ESET)*
Country	Russia
Motivation	Financial gain
Description	(ESET) There are several groups actively and profitably targeting businesses in Russia. A trend that we have seen unfold before our eyes lately is these cybercriminals' use of simple backdoors to gain a foothold in their targets' networks. Once they have this access, a lot of the work is done manually, slowly getting to understand the network layout and deploying custom tools the criminals can use to steal funds from these entities. Some of the groups that best exemplify these trends are Buhtrap, Cobalt Group and Corkow, Metel. The group discussed in this white paper is part of this new trend. We call this new group RTM; it uses custom malware, written in Delphi, that we cover in detail in later sections. The first trace of this tool in our telemetry data dates back to late 2015. The group also makes use of several different modules that they deploy where appropriate to their targets. They are interested in users of remote banking systems (RBS), mainly in Russia and neighboring countries.
Observed	That this group is mostly targeting businesses is apparent from the processes they are looking for on a compromised system. They look for software that is usually only installed on accountants' computers, such as remote banking software or tools to help with accounts pay. Countries: Czech, Germany, Kazakhstan, Russia and Ukraine.
Tools used	RTM.
Information	<https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0048/>

Sandworm Team, Iron Viking, Voodoo Bear

Names	Sandworm Team *(Trend Micro)* Iron Viking *(SecureWorks)* Voodoo Bear *(CrowdStrike)* Quedagh *(F-Secure)* TEMP.Noble *(FireEye)*
Country	Russia
Motivation	Sabotage and destruction
Description	Sandworm Team is a Russian cyberespionage group that has operated since approximately 2009. The group likely consists of Russian pro-hacktivists. Sandworm Team targets mainly Ukrainian entities associated with energy, industrial control systems, SCADA, government, and media. Sandworm Team has been linked to the Ukrainian energy sector attack in late 2015. This group appears to be closely associated with, or evolved into, TeleBots.
Observed	Sectors: Education, Energy, Government and Telecommunications. Countries: Azerbaijan, Belarus, Georgia, Iran, Israel, Kazakhstan, Kyrgyzstan, Lithuania, Poland, Russia and Ukraine.
Tools used	BlackEnergy, Gcat and PassKillDisk.
Operations performed	Oct 2014	The vulnerability was disclosed by iSIGHT Partners, which said that the vulnerability had already been exploited in a small number of cyberespionage attacks against NATO, several unnamed Ukrainian government organizations, a number of Western European governmental organizations, companies operating in the energy sector, European telecoms firms, and a US academic organization. <https://www.symantec.com/connect/blogs/sandworm-windows-zero-day-vulnerability-being-actively-exploited-targeted-attacks>
	Dec 2015	Widespread power outages on the Ukraine The power outage was described as technical failures taking place on Wednesday, December 23 that impacted a region around Ivano-Frankivisk Oblast. One report suggested the utility began to disconnect power substations for no apparent reason. The same report goes on to describe a virus was launched from the outside and it brought down the "remote management system" (a reference to the SCADA and or EMS). The outage was reported to have lasted six hours before electrical service was restored. At least two reports suggest the utility had initiated manual controls for restoration of service and the SCADA system was still off-line due to the infection. <https://ics.sans.org/blog/2015/12/30/current-reporting-on-the-cyber-attack-in-ukraine-resulting-in-power-outage>
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/timeline-of-sandworm-attacks/> <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-january-voodoo-bear/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0034/>

Samurai Panda, APT 4

Names	Samurai Panda *(CrowdStrike)* APT 4 *(Mandiant)* APT 4 *(FireEye)* Wisp Team *(Symantec)*
Country	China
Sponsor	State-sponsored, PLA Navy
Motivation	Information theft and espionage
Description	(CrowdStrike) Samurai Panda is interesting in that their target selection tends to focus on Asia Pacific victims in Japan, the Republic of Korea, and other democratic Asian victims. Beginning in 2009, we've observed this actor conduct more than 40 unique campaigns that we've identified in the malware configurations' campaign codes. These codes are often leveraged in the malware used by coordinated targeted attackers to differentiate victims that were successfully compromised from different target sets. The implant delivered by Samurai Panda uses a typical installation process whereby they: 1. Leverage a spear-phish with an exploit to get control of the execution flow of the targeted application. This file "drops" an XOR-encoded payload that unpacks itself and a configuration file. 2. Next, the implant, which can perform in several different modes, typically will install itself as a service and then begin beaconing out to an adversary-controlled host. 3. If that command-and-control host is online, the malicious service will download and instantiate a backdoor that provides remote access to the attacker, who will see the infected host's identification information as well as the campaign code.
Observed	Sectors: Defense and Government. Countries: Hong Kong, Japan, South Korea, UK and USA.
Tools used	Getkys, Sykipot and Wkysol.
Information	<https://www.crowdstrike.com/blog/whois-samurai-panda/>

ScarCruft

Names	ScarCruft *(Kaspersky)*
Country	North Korea
Sponsor	State-sponsored
Motivation	Financial gain
Description	(Kaspersky) A few of months ago, we deployed a new set of technologies into our products designed to identify and block zero day attacks. These technologies already proved its effectiveness earlier this year, when they caught an Adobe Flash zero day exploit, CVE-2016-1010. Earlier this month, we caught another zero-day Adobe Flash Player exploit deployed in targeted attacks. We believe these attacks are launched by an APT Group we call "ScarCruft". ScarCruft is a relatively new APT group; victims have been observed in several countries, including Russia, Nepal, South Korea, China, India, Kuwait and Romania. The group has several ongoing operations utilizing multiple exploits — two for Adobe Flash and one for Microsoft Internet Explorer. Currently, the group is engaged in two major operations: Operation Daybreak and Operation Erebus. The first of them, Operation Daybreak, appears to have been launched by ScarCruft in March 2016 and employs a previously unknown (0-day) Adobe Flash Player exploit, focusing on high profile victims. The other one, "Operation Erebus" employs an older exploit, for CVE-2016-4117 and leverages watering holes. It is also possible that the group deployed another zero day exploit, CVE-2016-0147, which was patched in April.
Observed	Countries: China, Hong Kong, India, Kuwait, Nepal, North Korea, Romania, Russia and Vietnam.
Tools used	ROKRAT and several 0-days.

Operations performed	2016	Operation "Erebus"
	Mar 2016	Operation "Daybreak" Target: High profile victims. Method: Previously unknown (0-day) Adobe Flash Player exploit. It is also possible that the group deployed another zero day exploit, CVE-2016-0147, which was patched in April. <https://securelist.com/operation-daybreak/75100/> Note: not the same operation as DarkHotel's Operation "Daybreak".
	May 2019	We recently discovered some interesting telemetry on this actor, and decided to dig deeper into ScarCruft's recent activity. This shows that the actor is still very active and constantly trying to elaborate its attack tools. Based on our telemetry, we can reassemble ScarCruft's binary infection procedure. It used a multi-stage binary infection to update each module effectively and evade detection. <https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/>

Information	<https://securelist.com/cve-2016-4171-adobe-flash-zero-day-used-in-targeted-attacks/75082/>

	<https://threatpost.com/scarcruft-apt-group-used-latest-flash-zero-day-in-two-dozen-attacks/118642/>

Scarlet Mimic

Names	Scarlet Mimic *(Palo Alto)*
Country	China
Motivation	Information theft and espionage
Description	Scarlet Mimic is a threat group that has targeted minority rights activists. This group has not been directly linked to a government source, but the group's motivations appear to overlap with those of the Chinese government. While there is some overlap between IP addresses used by Scarlet Mimic and Putter Panda, APT 2, it has not been concluded that the groups are the same. (Palo Alto) The attacks began over four years ago and their targeting pattern suggests that this adversary's primary mission is to gather information about minority rights activists. We do not have evidence directly linking these attacks to a government source, but the information derived from these activities supports an assessment that a group or groups with motivations similar to the stated position of the Chinese government in relation to these targets is involved. The attacks we attribute to Scarlet Mimic have primarily targeted Uyghur and Tibetan activists as well as those who are interested in their causes. Both the Tibetan community and the Uyghurs, a Turkic Muslim minority residing primarily in northwest China, have been targets of multiple sophisticated attacks in the past decade. Both also have history of strained relationships with the government of the People's Republic of China (PRC), though we do not have evidence that links Scarlet Mimic attacks to the PRC. Scarlet Mimic attacks have also been identified against government organizations in Russia and India, who are responsible for tracking activist and terrorist activities. While we do not know the precise target of each of the Scarlet Mimic attacks, many of them align to the patterns described above.
Observed	Tibetan and Uyghur activists as well as those who are interested in their causes.
Tools used	CallMe, FakeM, MobileOrder and Psylo.
Information	<https://unit42.paloaltonetworks.com/scarlet-mimic-years-long-espionage-targets-minority-activists/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0029/>

Sea Turtle

Names	Sea Turtle *(Talos)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(Talos) Cisco Talos has discovered a new cyber threat campaign that we are calling "Sea Turtle," which is targeting public and private entities, including national security organizations, located primarily in the Middle East and North Africa. The ongoing operation likely began as early as January 2017 and has continued through the first quarter of 2019. Our investigation revealed that at least 40 different organizations across 13 different countries were compromised during this campaign. We assess with high confidence that this activity is being carried out by an advanced, state-sponsored actor that seeks to obtain persistent access to sensitive networks and systems. The actors behind this campaign have focused on using DNS hijacking as a mechanism for achieving their ultimate objectives. DNS hijacking occurs when the actor can illicitly modify DNS name records to point users to actor-controlled servers. The Department of Homeland Security (DHS) issued an alert about this activity on Jan. 24 2019, warning that an attacker could redirect user traffic and obtain valid encryption certificates for an organization's domain names.
Observed	Sectors: Defense, Energy, Government and Intelligence agencies. Countries: Albania, Armenia, Cyprus, Egypt, Iraq, Jordan, Lebanon, Libya, Sweden, Syria, Turkey, UAE and USA.
Tools used	DNS hijacking and Drupalgeddon.
Information	<https://blog.talosintelligence.com/2019/04/seaturtle.html>

Shadow Network

Names	Shadow Network *(Information Warfare Monitor)*
Country	China
Motivation	Information theft and espionage
Description	(Information Warfare Monitor) Shadows in the Cloud documents a complex ecosystem of cyber espionage that systematically compromised government, business, academic, and other computer network systems in India, the Offices of the Dalai Lama, the United Nations, and several other countries. The report also contains an analysis of data which were stolen from politically sensitive targets and recovered during the course of the investigation. These include documents from the Offices of the Dalai Lama and agencies of the Indian national security establishment. Data containing sensitive information on citizens of numerous third-party countries, as well as personal, financial, and business information, were also exfiltrated and recovered during the course of the investigation. The report analyzes the malware ecosystem employed by the Shadows' attackers, which leveraged multiple redundant cloud computing systems, social networking platforms, and free web hosting services in order to maintain persistent control while operating core servers located in the People's Republic of China (PRC). Although the identity and motivation of the attackers remain unknown, the report is able to determine the location (Chengdu, PRC) as well as some of the associations of the attackers through circumstantial evidence. The investigation is the product of an eight month, collaborative activity between the Information Warfare Monitor (Citizen Lab and SecDev) and the Shadowserver Foundation. The investigation employed a fusion methodology, combining technical interrogation techniques, data analysis, and field research, to track and uncover the Shadow cyber espionage network. Also see GhostNet, Snooping Dragon.
Observed	Sectors: Education, Government and others. Countries: Afghanistan, Australia, Azerbaijan, Canada, China, France, Germany, Greece, Hong Kong, India, Israel, Italy, Japan, Lithuania, Malaysia, Mexico, Nepal, Netherlands, New Guinea, New Zealand, Pakistan, Philippines, Qatar, Romania, Russia, South Korea, Sweden, Taiwan, Thailand, Tibet, UAE, UK, USA and Vietnam.
Tools used	ShadowNet.
Counter operations	Taken down by the Shadowserver Foundation.
Information	<https://citizenlab.ca/wp-content/uploads/2017/05/shadows-in-the-cloud.pdf>

Silence

Names	Silence *(Kaspersky)*
Country	[Unknown]
Motivation	Financial gain
Description	(Group-IB) Group-IB has exposed the attacks committed by Silence cybercriminal group. While the gang had previously targeted Russian banks, Group-IB experts also have discovered evidence of the group's activity in more than 25 countries worldwide. Group-IB has published its first detailed report on tactics and tools employed by Silence. Group-IB security analysts' hypothesis is that at least one of the gang members appears to be a former or current employee of a cyber security company. The confirmed damage from Silence activity is estimated at 800 000 USD. Silence is a group of Russian-speaking hackers, based on their commands language, the location of infrastructure they used, and the geography of their targets (Russia, Ukraine, Belarus, Azerbaijan, Poland, and Kazakhstan). Although phishing emails were also sent to bank employees in Central and Western Europe, Africa, and Asia). Furthermore, Silence used Russian words typed on an English keyboard layout for the commands of the employed backdoor. The hackers also used Russian-language web hosting services.
Observed	Sectors: Financial. Countries: more than 25, including Armenia, Azerbaijan, Belarus, Kazakhstan, Malaysia, Poland, Russia and Ukraine.
Tools used	Atmosphere and Silence.
Information	<https://www.group-ib.com/blog/silence> <https://securelist.com/the-silence/83009/> <https://reaqta.com/2019/01/silence-group-targeting-russian-banks/>

Sima

Names	Sima *(Amnesty International)*
Country	Iran
Motivation	Information theft and espionage
Description	In February 2016, Iran-focused individuals received messages purporting to be from Human RightsWatch's (HRW) Emergencies Director, requesting that they read an article about Iran pressing Afghan refugees to fight in Syria. While referencing a real report published by HRW, the links provided for the Director's biography and article directed the recipient to malware hosted elsewhere. These spear-phishing attempts represent an evolution of Iranian actors based on their social engineering tactics and narrow targeting. Although the messages still had minor grammatical and stylistic errors that would be obvious to a native speaker, the actors demonstrated stronger English-language proficiency than past intrusion sets and a deeper investment in background research prior to the attempt. The actors appropriated a real identity that would be expected to professionally interact with the subject, then offered validation through links to their biography and social media, the former of which itself was malware as well. The bait documents contained a real article relevant to their interests and topic referenced, and the message attempted to address to how it aligned with their professional research or field of employment. The referenced documents sent were malware binaries posing as legitimate files using the common right-to-left filenames tactic in order to conceal the actual file extension. All of these techniques, while common pretexting mechanisms, are a refinement compared to a tendency amongst other groups to simply continually send different forms of generic malware or phishing, in the hopes that one would eventually be successful.
Observed	This group targets Iranians in diaspora.
Tools used	Sima.
Information	<https://www.blackhat.com/docs/us-16/materials/us-16-Guarnieri-Iran-And-The-Soft-War-For-Internet-Dominance-wp.pdf>

Slingshot

Names	Slingshot *(Kaspersky)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(Kaspersky) While analysing an incident which involved a suspected keylogger, we identified a malicious library able to interact with a virtual file system, which is usually the sign of an advanced APT actor. This turned out to be a malicious loader internally named 'Slingshot', part of a new, and highly sophisticated attack platform that rivals Project Sauron and Regin in complexity. While for most victims the infection vector for Slingshot remains unknown, we were able to find several cases where the attackers got access to MikroTik routers and placed a component downloaded by Winbox Loader, a management suite for MikroTik routers. In turn, this infected the administrator of the router. We believe this cluster of activity started in at least 2012 and was still active at the time of this analysis (February 2018).
Observed	Countries: Afghanistan, Congo, Iraq, Jordan, Kenya, Libya, Somalia, Sudan, Tanzania, Turkey and Yemen.
Tools used	Cahnadr, GollumApp, Slingshot and WinBox (a utility used for MikroTik router configuration).
Information	<https://securelist.com/apt-slingshot/84312/>

Snake Wine

Names	Snake Wine *(Cylance)*
Country	China
Motivation	Information theft and espionage
Description	(Cylance) While investigating some of the smaller name servers that Sofacy, APT 28, Fancy Bear, Sednit routinely use to host their infrastructure, Cylance discovered another prolonged campaign that appeared to exclusively target Japanese companies and individuals that began around August 2016. The later registration style was eerily close to previously registered APT28 domains, however, the malware used in the attacks did not seem to line up at all. During the course of our investigation, JPCERT published this analysis of one of the group's backdoors. Cylance tracks this threat group internally as 'Snake Wine'. The Snake Wine group has proven to be highly adaptable and has continued to adopt new tactics in order to establish footholds inside victim environments. The exclusive interest in Japanese government, education, and commerce will likely continue into the future as the group is just starting to build and utilize their existing current attack infrastructure.
Observed	Sectors: Commerce, Education and Government. Countries: Japan.
Tools used	Ham Backdoor and Tofu Backdoor.
Information	<https://threatvector.cylance.com/en_us/home/the-deception-project-a-new-japanese-centric-threat.html> <https://www.jpcert.or.jp/magazine/acreport-ChChes.html>

Snowglobe, Animal Farm

Names	Snowglobe *(CSEC)* Animal Farm *(Kaspersky)*
Country	France
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	(GData) The revelation about the existence of yet another potentially nation-state driven spyware occurred in March 2014 when Le Monde first published information about top secret slides originating from 2011 and part of their content . But the slides Le Monde published revealed only a small part of the picture – several slides were cut out, some information was redacted. Germany's Der Spiegel re-published the slide set with far less deletions recently, in January 2015, and therefore gave a deeper insight about what CSEC actually says they have tracked down. The newly published documents reveal: the so called operation SNOWGLOBE, was discovered in 2009 (slide 9) and consists of three different "implants", two were dubbed snowballs and one "more sophisticated implant, discovered in mid-2010" is tagged as snowman (slide 7). According to slide 22, "CSEC assesses, with moderate certainty, SNOWGLOBE to be a state-sponsored CNO [Cyber Network Operation] effort, put forth by a French intelligence agency." The information given dates back to 2011 and nothing else has been published since. Now that specific Babar samples have been identified and analyzed, there might be new information, also with regards to similarities or differences between the two Remote Administration Tools (RATs) EvilBunny and Babar.
Observed	Sectors: Government and private sectors. Countries: Algeria, China, Germany, Greece, Iran, Ivory Coast, Malaysia, Netherlands, Norway, Russia, Spain, Syria, Turkey, UK and USA.
Tools used	Babar, Casper, Dino, EvilBunny, Tafacalou, Nbot and Chocopop.
Information	<https://www.gdatasoftware.com/blog/2015/02/24270-babar-espionage-software-finally-found-and-put-under-the-microscope> <https://resources.infosecinstitute.com/animal-farm-apt-and-the-shadow-of-france-intelligence/>

Sofacy, APT 28, Fancy Bear, Sednit

Names	Sofacy *(Kaspersky)* APT 28 *(Mandiant)* Fancy Bear *(CrowdStrike)* Sednit *(ESET)* Group 74 *(Talos)* TG-4127 *(SecureWorks)* Pawn Storm *(Trend Micro)* Tsar Team *(iSight)* Strontium *(Microsoft)* Swallowtail *(Symantec)* SIG40 *(NSA)* Snakemackerel *(iDefense)* Iron Twilight *(SecureWorks)* Grizzly Steppe *(US Government)* together with APT 29, Cozy Bear, The Dukes
Country	Russia
Sponsor	State-sponsored, two GRU units known as Unit 26165 and Unit 74455.
Motivation	Information theft and espionage
Description	APT 28 is a threat group that has been attributed to Russia's Main Intelligence Directorate of the Russian General Staff by a July 2018 U.S. Department of Justice indictment. This group reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. APT 28 has been active since at least January 2007. (FireEye) APT28 likely seeks to collect intelligence about Georgia's security and political dynamics by targeting officials working for the Ministry of Internal Affairs and the Ministry of Defense. APT28 has demonstrated interest in Eastern European governments and security organizations. These victims would provide the Russian government with an ability to predict policymaker intentions and gauge its ability to influence public opinion. APT28 appeared to target individuals affiliated with European security organizations and global multilateral institutions. The Russian government has long cited European security organizations like NATO and the OSCE as existential threats, particularly during periods of increased tension in Europe.
Observed	Sectors: Chemical, Defense, Embassies, Engineering, Government, Industrial, Intelligence organizations, Media, NGOs and Think Tanks. Countries: Afghanistan, Armenia, Belgium, Bulgaria, Canada, Chile, China, Croatia, Cyprus, France, Georgia, Germany, Hungary, Iran, Iraq, Japan, Jordan, Kazakhstan, Mexico, Mongolia, Netherlands, Norway, Pakistan, Poland, South Africa, South Korea, Tajikistan, Turkey, Uganda, UAE, UK, Ukraine, USA, Uzbekistan, APEC, OSCE and NATO.
Tools used	ADVSTORESHELL, Cannon, certutil, CHOPSTICK, Computrace, CORESHELL, DealersChoice, Downdelph, DownRange, Dropper, EVILTOSS, Foozer, Forfiles, HIDEDRV, JHUHUGIT, Koadic, Komplex, LoJax, Mimikatz, OLDBAIT, PocoDown, Responder, Sedkit, Sednit, Sedreco, Seduploader, Sofacy, SOURFACE, USBStealer, Winexe, WinIDS, X-Agent, X-Agent for Android, X-Agent OSX, X-Tunnel and Zebrocy.

Operations performed	2011-2012	Back in 2011-2012, the group used a relatively tiny implant (known as "Sofacy" or SOURFACE) as its first stage malware. The implant shared certain similarities with the old Miniduke implants. This led us to believe the two groups were connected, at least to begin with, although it appears they parted ways in 2014, with the original Miniduke group switching to the CosmicDuke implant.
	2013	At some point during 2013, the Sofacy group expanded its arsenal and added more backdoors and tools, including CORESHELL, SPLM (aka Xagent, aka CHOPSTICK), JHUHUGIT (which is built with code from the Carberp sources), AZZY (aka ADVSTORESHELL, NETUI, EVILTOSS, and spans across four to five generations) and a few others. We've seen quite a few versions of these implants and they were relatively widespread for a time.
	Oct 2014	Operation "Pawn Storm" Target: Several foreign affairs ministries from around the globe. Method: Spear-phishing e-mails with links leading to an Adobe Flash exploit. <https://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/>
	Dec 2014	Six-month-long cyberattack on the German parliament <http://www.lse.co.uk/AllNews.asp?code=kwdwehme&headline=Russian_Hackers_Suspected_In_Cyberattack_On_German_Parliament>
	Feb 2015	U.S. military wives' death threats Five military wives received death threats from a hacker group calling itself "CyberCaliphate", claiming to be an Islamic State affiliate, on February 10, 2015. This was later discovered to have been a false flag attack by Fancy Bear, when the victims' email addresses were found to have been in the Fancy Bear phishing target list. <https://www.apnews.com/4d174e45ef5843a0ba82e804f080988f>
	Apr 2015	Compromise of TV5Monde in France "A group calling itself the Cyber Caliphate, linked to so-called Islamic State, first claimed responsibility. But an investigation now suggests the attack was in fact carried out by a group of Russian hackers." <https://www.bbc.com/news/technology-37590375>
	Apr 2015	Operation "Russian Doll" Method: Adobe Flash 0-day <https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html>
	Aug 2015	EFF spoof, White House and NATO attack Method: zero-day exploit of Java, spoofing the Electronic Frontier Foundation and launching attacks on the White House and NATO. The hackers used a spear-phishing attack, directing emails to the false url electronicfrontierfoundation.org. <https://www.eff.org/deeplinks/2015/08/new-spear-phishing-campaign-pretends-be-eff>
	Sep 2015	Bootstrapped Firefox Add-on <https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/>

	Oct 2015	Attack on Bellingcat Eliot Higgins and other journalists associated with Bellingcat, a group researching the shoot down of Malaysia Airlines Flight 17 over Ukraine, were targeted by numerous spear-phishing emails. The messages were fake Gmail security notices with Bit.ly and TinyCC shortened URLs. <https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-mh17-investigation-team/>
	Oct 2015	Attack on Dutch Safety Board The group targeted the Dutch Safety Board, the body conducting the official investigation into the crash, before and after the release of the board's final report. They set up fake SFTP and VPN servers to mimic the board's own servers, likely for the purpose of spear-phishing usernames and passwords. <https://www.msn.com/en-au/news/world/russia-tried-to-hack-mh17-inquiry-system/ar-BBmmuuT>
	Jun 2016	Breach of Democratic National Committee Fancy Bear carried out spear-phishing attacks on email addresses associated with the Democratic National Committee in the first quarter of 2016. On March 10, phishing emails that were mainly directed at old email addresses of 2008 Democratic campaign staffers began to arrive. One of these accounts may have yielded up to date contact lists. The next day, phishing attacks expanded to the non-public email addresses of high level Democratic Party officials. Hillaryclinton.com addresses were attacked, but required two factor authentication for access. The attack redirected towards Gmail accounts on March 19th. Podesta's Gmail account was breached the same day, with 50,000 emails stolen. Another sophisticated hacking group attributed to the Russian Federation, nicknamed APT 29, Cozy Bear, The Dukes appears to be a different agency, one more interested in traditional long-term espionage. <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>
	Jun 2016	"Exercise Noble Partner 2016" spear-phishing e-mail Method: Spear-phishing e-mail Target: USA government <https://unit42.paloaltonetworks.com/unit42-new-sofacy-attacks-against-us-government-agency/>
	Jun 2016	Compromise of the Bundestag website in Germany <https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/>
	Aug 2016	Spear-phishing attack members of the Bundestag and multiple political parties such as Linken-faction leader Sahra Wagenknecht, Junge Union and the CDU of Saarland. Authorities feared that sensitive information could be gathered by hackers to later manipulate the public ahead of elections such as Germany's next federal election which was due in September 2017. <http://www.dw.com/en/hackers-lurking-parliamentarians-told/a-19564630>

	Aug 2016	World Anti-Doping Agency Method: Phishing emails sent to users of its database claiming to be official WADA communications requesting their login details. <http://www.ibtimes.co.uk/russian-hackers-fancy-bear-likely-breached-olympic-drug-testing-agency-dnc-experts-say-1577508>
	Sep 2016	Operation "Komplex" <https://unit42.paloaltonetworks.com/unit42-sofacys-komplex-os-x-trojan/>
	Oct 2016	Operation "DealersChoice" <researchcenter.paloaltonetworks.com/2016/10/unit42-dealerschoice-sofacys-flash-player-exploit-platform/> <https://unit42.paloaltonetworks.com/unit42-let-ride-sofacy-groups-dealerschoice-attacks-continue/> The global reach that coincided with this focus on NATO and the Ukraine couldn't be overstated. Our KSN data showed spear-phishing targets geo-located across the globe into 2017. AM, AZ, FR, DE, IQ, IT, KG, MA, CH, UA, US, VN DealersChoice emails, like the one above, that we were able to recover from third party sources provided additional targeting insight, and confirmed some of the targeting within our KSN data: TR, PL, BA, AZ, KR, LV, GE, LV, AU, SE, BE
	Early 2017	GAMEFISH backdoor Target: Europe. Method: They took advantage of the Syrian military conflict for thematic content and file naming "Trump's_Attack_on_Syria_English.docx". Again, this deployment was likely a part of their focus on NATO targets.
	Early 2017	LoJax: First UEFI rootkit found in the wild <https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/>
	Feb 2017	Attack on Dutch ministries In February 2017, the General Intelligence and Security Service (AIVD) of the Netherlands revealed that Fancy Bear and Cozy Bear had made several attempts to hack into Dutch ministries, including the Ministry of General Affairs, over the previous six months. Rob Bertholee, head of the AIVD, said on EenVandaag that the hackers were Russian and had tried to gain access to secret government documents. <https://www.volkskrant.nl/cultuur-media/russen-faalden-bij-hackpogingen-ambtenaren-op-nederlandse-ministeries~b77ff391/>
	Feb 2017	IAAF Hack The officials of International Association of Athletics Federations (IAAF) stated in April 2017 that its servers had been hacked by the "Fancy Bear" group. The attack was detected by cybersecurity firm Context Information Security which identified that an unauthorized remote access to IAAF's servers had taken place on February 21. IAAF stated that the hackers had accessed the *Therapeutic Use Exemption* applications, needed to use medications prohibited by WADA.

		<https://www.voanews.com/a/iaaf-hack-fancy-bears/3793874.html>
	Apr 2017	German elections They targeted the German Konrad Adenauer Foundation and Friedrich Ebert Foundation, groups that are associated with Angela Merkel's Christian Democratic Union and opposition Social Democratic Party, respectively. Fancy Bear set up fake email servers in late 2016 to send phishing emails with links to malware. <https://www.handelsblatt.com/today/politics/election-risks-russia-linked-hackers-target-german-political-foundations/23569188.html?ticket=ST-2696734-GRHgtQukDIEXeSOwksXO-ap1>
	Early to mid 2017	SPLM backdoor Target: included defense related commercial and military organizations, and telecommunications. Targeting included TR, KZ, AM, KG, JO, UK, UZ Method: SPLM/CHOPSTICK/Xagent
	Jun 2017	Heavy Zebrocy deployments Targeting profiles, spear-phish filenames, and lures carry thematic content related to visa applications and scanned images, border control administration, and various administrative notes. Targeting appears to be widely spread across the Middle East, Europe, and Asia: • Business accounting practices and standards • Science and engineering centers • Industrial and hydro chemical engineering and standards/certification • Ministry of foreign affairs • Embassies and consulates • National security and intelligence agencies • Press services • Translation services • NGO – family and social service • Ministry of energy and industry Method: the Zebrocy chain follows a pattern: spear-phish attachment -> compiled Autoit script (downloader) -> Zebrocy payload. In some deployments, we observed Sofacy actively developing and deploying a new package to a much smaller, specific subset of targets within the broader set.
	Jan 2018	Breach of the International Olympic Committee On January 10, 2018, the "Fancy Bears Hack Team" online persona leaked what appeared to be stolen International Olympic Committee (IOC) and U.S. Olympic Committee emails, dated from late 2016 to early 2017, were leaked in apparent retaliation for the IOC's banning of Russian athletes from the 2018 Winter Olympics as a sanction for Russia's systematic doping program. The attack resembles the earlier World Anti-Doping Agency (WADA) leaks. It is not known whether the emails are fully authentic, because of Fancy Bear's history of salting stolen emails with disinformation. The mode of attack was also not known, but was probably phishing. <https://www.wired.com/story/russian-fancy-bears-hackers-release-apparent-ioc-emails/>

	Feb 2018	Attacks on Multiple Government Entities Target: Ministries of Foreign Affairs of the USA and Romania. Method: Spear-phishing using the subject line of Upcoming Defense events February 2018 and a sender address claiming to be from Jane's 360 defense events. <https://unit42.paloaltonetworks.com/unit42-sofacy-attacks-multiple-government-entities/>
	Mar 2018	On March 12 and March 14, we observed the Sofacy group carrying out an attack on a European government agency involving an updated variant of DealersChoice. The updated DealersChoice documents used a similar process to obtain a malicious Flash object from a C2 server, but the inner mechanics of the Flash object contained significant differences in comparison to the original samples we analyzed. <https://unit42.paloaltonetworks.com/unit42-sofacy-uses-dealerschoice-target-european-government-agency/>
	May 2018	Breach of the Swedish Sports Confederation The Swedish Sports Confederation reported Fancy Bear was responsible for an attack on its computers, targeting records of athletes' doping tests. <https://www.reuters.com/article/us-sweden-doping/swedish-sports-body-says-anti-doping-unit-hit-by-hacking-attack-idUSKCN1IG2GN>
	May 2018	VPNFilter IoT botnet[6]
	Jun 2018	This third campaign is consistent with two previously reported attack campaigns in terms of targeting: the targets were government organizations dealing with foreign affairs. In this case however the targets were in different geopolitical regions. <https://unit42.paloaltonetworks.com/unit42-sofacy-groups-parallel-attacks/>
	Aug 2018	Attacks on United States Conservative Groups The software company Microsoft reported in August 2018 that the group had attempted to steal data from political organizations such as the International Republican Institute and the Hudson Institute think tanks. The attacks were thwarted when Microsoft security staff won control of six net domains. In its announcement Microsoft advised that "we currently have no evidence these domains were used in any successful attacks before the DCU transferred control of them, nor do we have evidence to indicate the identity of the ultimate targets of any planned attack involving these domains". <https://www.bbc.co.uk/news/technology-45257081>
	Oct 2018	Operation "Dear Joohn" Target: The weaponized documents targeted several government entities around the globe, including North America, Europe, and a former USSR state. Method: new 'Cannon' Trojan <https://unit42.paloaltonetworks.com/dear-joohn-sofacy-groups-global-campaign/>

---

[6] See ThaiCERT Whitepaper "VPNFilter IoT botnet seized by the FBI"

		<https://unit42.paloaltonetworks.com/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/>
	2018	BREXIT-themed lure document Brexit-themed bait documents to deliver the Zekapab (also known as Zebrocy) first-stage malware, sent on the same day the UK Prime Minister Theresa May announced the initial BREXIT draft agreement with the European Union (EU). "As the United Kingdom (UK) Prime Minister Theresa May announced the initial BREXIT draft agreement with the European Union (EU). <https://www.accenture.com/t20181129T203820Z__w__/us-en/_acnmedia/PDF-90/Accenture-snakemackerel-delivers-zekapab-malware.pdf>
	Feb 2019	2019 Think Tank Attacks In February 2019, Microsoft announced that it had detected spear-phishing attacks from APT28, aimed at employees of the German Marshall Fund, Aspen Institute Germany, and the German Council on Foreign Relations. Hackers from the group purportedly sent phishing e-mails to 104 email addresses across Europe in an attempt to gain access to employer credentials and infect sites with malware. <https://www.washingtonpost.com/technology/2019/02/20/microsoft-says-it-has-found-another-russian-operation-targeting-prominent-think-tanks/?utm_term=.870ff11468ae>
	Feb 2019	Threat Campaign Likely Targeting NATO Members, Defense and Military Outlets iDefense assesses with moderate confidence that the actors may be targeting attendees and sponsors of the upcoming Underwater Defense & Security 2019 event occurring March 5-7, 2019, in Southampton, United Kingdom. This event draws attendees from government, military and private sector entities across the globe. <https://www.accenture.com/t20190213T141124Z__w__/us-en/_acnmedia/PDF-94/Accenture-SNAKEMACKEREL-Threat-Campaign-Likely-Targeting-NATO-Members-Defense-and-Military-Outlets.pdf>
Counter operations	- Mueller indicts 12 Russians for DNC hacking as Trump-Putin summit looms (2018) <https://www.politico.com/story/2018/07/13/mueller-indicts-12-russians-for-hacking-into-dnc-718805> - US charges Russian military officers over international hacking and disinformation campaigns (2018) <https://www.zdnet.com/article/us-charges-russian-military-officers-over-international-hacking-and-disinformation-campaigns/> - Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices (2018) <https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected>	
Information	<https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/> <https://securelist.com/a-slice-of-2017-sofacy-activity/83930/> <https://www.symantec.com/blogs/election-security/apt28-espionage-military-government>	

	<https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf> <https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf> <https://en.wikipedia.org/wiki/Fancy_Bear>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0007/>

Sowbug

Names	Sowbug *(Symantec)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(Symantec) Symantec has identified a previously unknown group called Sowbug that has been conducting highly targeted cyberattacks against organizations in South America and Southeast Asia and appears to be heavily focused on foreign policy institutions and diplomatic targets. Sowbug has been seen mounting classic espionage attacks by stealing documents from the organizations it infiltrates. Symantec saw the first evidence of Sowbug-related activity with the discovery in March 2017 of an entirely new piece of malware called Felismus used against a target in Southeast Asia. We have subsequently identified further victims on both sides of the Pacific Ocean. While the Felismus tool was first identified in March of this year, its association with Sowbug was unknown until now. Symantec has also been able to connect earlier attack campaigns with Sowbug, demonstrating that it has been active since at least early-2015 and may have been operating even earlier. To date, Sowbug appears to be focused mainly on government entities in South America and Southeast Asia and has infiltrated organizations in Argentina, Brazil, Ecuador, Peru, Brunei and Malaysia. The group is well resourced, capable of infiltrating multiple targets simultaneously and will often operate outside the working hours of targeted organizations in order to maintain a low profile.
Observed	Sectors: Government. Countries: Argentina, Brazil, Brunei, Ecuador, Malaysia and Peru.
Tools used	Felismus and StarLoader.
Information	<https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0054/>

Stalker Panda

Names	Stalker Panda *(Raytheon Blackbird Technologies)*
Country	China
Sponsor	State-sponsored, National University of Defense and Technology
Motivation	Information theft and espionage
Description	(Raytheon) The group appears to have close ties to the Chinese National University of Defense and Technology, which is possibly linked to the PLA. Stalker Panda has been observed conducting targeted attacks against Japan, Taiwan, Hong Kong, and the United States. The attacks appear to be centered on political, media, and engineering sectors. The group appears to have been active since around 2010 and they maintain and upgrade their tools regularly. A fairly unique aspect of the observed Stalker Panda attacks is their use of social media and blog sites as first stage (cutout) command and control (C2) infrastructure. This 2-stage C2 infrastructure provides some obfuscation of the main C2 servers and provides some flexibility in communications because the first stage social media/blog site nodes can be reconfigured at will. Stalker Panda seems to favor spear phishing email campaigns as their attack vector.
Observed	Sectors: Engineering, Media and political. Countries: Hong Kong, Japan, Taiwan and USA.
Tools used	Elirks, SharpServer, Blogspot, and the XUni platform.
Information	<https://wikileaks.org/vault7/document/2015-08-20150814-256-CSIR-15005-Stalker-Panda/2015-08-20150814-256-CSIR-15005-Stalker-Panda.pdf>

Stealth Falcon, FruityArmor

Names	Stealth Falcon *(Citizen Lab)* FruityArmor *(Kaspersky)*
Country	UAE
Motivation	Information theft and espionage
Description	(Citizen Lab) This report describes a campaign of targeted spyware attacks carried out by a sophisticated operator, which we call Stealth Falcon. The attacks have been conducted from 2012 until the present, against Emirati journalists, activists, and dissidents. We discovered this campaign when an individual purporting to be from an apparently fictitious organization called "The Right to Fight" contacted Rori Donaghy. Donaghy, a UK-based journalist and founder of the Emirates Center for Human Rights, received a spyware-laden email in November 2015, purporting to offer him a position on a human rights panel. Donaghy has written critically of the United Arab Emirates (UAE) government in the past, and had recently published a series of articles based on leaked emails involving members of the UAE government. Circumstantial evidence suggests a link between Stealth Falcon and the UAE government. We traced digital artifacts used in this campaign to links sent from an activist's Twitter account in December 2012, a period when it appears to have been under government control. We also identified other bait content employed by this threat actor. We found 31 public tweets sent by Stealth Falcon, 30 of which were directly targeted at one of 27 victims. Of the 27 targets, 24 were obviously linked to the UAE, based on their profile information (e.g., photos, "UAE" in account name, location), and at least six targets appeared to be operated by people who were arrested, sought for arrest, or convicted in absentia by the UAE government, in relation to their Twitter activity.
Observed	Sectors: Civil society groups and Emirati journalists, activists and dissidents. Countries: UAE and UK.
Tools used	0-day exploits.

Operations performed	Oct 2016	Windows zero-day exploit used in targeted attacks by FruityArmor APT <https://securelist.com/windows-zero-day-exploit-used-in-targeted-attacks-by-fruityarmor-apt/76396/>
	Oct 2018	Zero-day exploit (CVE-2018-8453) used in targeted attacks <https://securelist.com/cve-2018-8453-used-in-targeted-attacks/88151/>
	Oct 2018	Zero-day in Windows Kernel Transaction Manager (CVE-2018-8611) <https://securelist.com/zero-day-in-windows-kernel-transaction-manager-cve-2018-8611/89253/>

Information	<https://citizenlab.ca/2016/05/stealth-falcon/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0038/>

Stolen Pencil

Names	Stolen Pencil *(ASERT)*
Country	North Korea
Motivation	[Uncertain]
Description	(ASERT) ASERT has learned of an APT campaign, possibly originating from DPRK, we are calling Stolen Pencil that is targeting academic institutions since at least May 2018. The ultimate motivation behind the attacks is unclear, but the threat actors are adept at scavenging for credentials. Targets are sent spear phishing e-mails that lead them to a web site displaying a lure document and are immediately prompted to install a malicious Google Chrome extension. Once gaining a foothold, the threat actors use off-the-shelf tools to ensure persistence, including Remote Desktop Protocol (RDP) to maintain access. Key Findings • A wide variety of phishing domains imply other targets, but those focused on academia were intended to install a malicious Chrome extension. • A large number of the victims, across multiple universities, had expertise in biomedical engineering, possibly suggesting a motivation for the attackers targeting. • Poor OPSEC led to users finding open web browsers in Korean, English-to-Korean translators open, and keyboards switched to Korean. • The threat actors use built-in Windows administration tools and commercial off-the-shelf software to "live off the land". The threat actor at the keyboard uses RDP to access compromised systems rather than a backdoor or Remote Access Trojan (RAT). • Post-exploitation persistence is maintained by harvesting passwords from a wide variety of sources such as process memory, web browsers, network sniffing, and keyloggers. • There is no evidence of data theft, leaving the motivation behind Stolen Pencil largely uncertain.
Observed	Sectors: Education and Think Tanks.
Tools used	Mimikatz.
Information	<https://www.netscout.com/blog/asert/stolen-pencil-campaign-targets-academia> <https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0086/>

Stone Panda, APT 10, menuPass

Names	Stone Panda *(CrowdStrike)* APT 10 *(Mandiant)* menuPass Team *(Symantec)* menuPass *(Palo Alto)* Red Apollo *(PwC)* CVNX *(BAE Systems)* Potassium *(Microsoft)* Hogfish *(iDefense)* Happyyongzi *(FireEye)*
Country	China
Motivation	Information theft and espionage
Description	menuPass is a threat group that appears to originate from China and has been active since approximately 2009. The group has targeted healthcare, defense, aerospace, and government sectors, and has targeted Japanese victims since at least 2014. In 2016 and 2017, the group targeted managed IT service providers, manufacturing and mining companies, and a university.
Observed	Sectors: Aerospace, Defense, Government, Healthcare, MSPs and Pharmaceutical. Countries: Australia, Brazil, Canada, Finland, France, India, Japan, Norway, Philippines, South Africa, South Korea, Sweden, Switzerland, Thailand, UK and USA.
Tools used	Anel, certutil, ChChes, Cobalt Strike, Emdivi, EvilGrab, Impacket, Mimikatz, PlugX, Poison Ivy, PowerSploit, pwdump, QuasarRAT, RedLeaves, SNUGRIDE, Trochilus RAT and UPPERCUT.
Operations performed	Sep 2016	Spear-phishing attack Method: The attackers spoofed several sender email addresses to send spear-phishing emails, most notably public addresses associated with the Sasakawa Peace Foundation and The White House. Target: Japanese academics working in several areas of science, along with Japanese pharmaceutical and a US-based subsidiary of a Japanese manufacturing organizations. <https://unit42.paloaltonetworks.com/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/>
	2014	Operation "Cloud Hopper" The campaign, which we refer to as Operation Cloud Hopper, has targeted managed IT service providers (MSPs), allowing APT10 unprecedented potential access to the intellectual property and sensitive data of those MSPs and their clients globally. A number of Japanese organizations have also been directly targeted in a separate, simultaneous campaign by the same actor <https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf>
	2016-2017	Leveraging its global footprint, FireEye has detected APT10 activity across six continents in 2016 and 2017. APT10 has targeted or compromised manufacturing companies in India, Japan and Northern Europe; a mining company in South America; and multiple IT service

		providers worldwide. We believe these companies are a mix of final targets and organizations that could provide a foothold in a final target. <https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html>
	Feb 2017	Operation "TradeSecret" The National Foreign Trade Council (NFTC) website was allegedly infiltrated by Chinese nation-state threat actors, according to a new report from Fidelis Cybersecurity. The attack against the NFTC site has been dubbed 'Operation TradeSecret' by Fidelis and is seen as an attempt to gain insight into individuals closely associated with U.S trade policy activities. <https://www.eweek.com/security/chinese-nation-state-hackers-target-u.s-in-operation-tradesecret>
	2017	Operation "ChessMaster" Take for instance the self-named ChessMaster, a campaign targeting Japanese academe, technology enterprises, media outfits, managed service providers, and government agencies. It employs various poisoned pawns in the form of malware-laden spear-phishing emails containing decoy documents. <https://blog.trendmicro.com/trendlabs-security-intelligence/chessmaster-cyber-espionage-campaign/>
	Nov 2017	Targeted Norwegian MSP and US Companies in Sustained Campaign A sustained cyberespionage campaign targeting at least three companies in the United States and Europe was uncovered by Recorded Future and Rapid7 between November 2017 and September 2018. <https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf>
	2018	Operation "New Battle" This report provides a technical overview of the bespoke RedLeaves implants leveraged by the actor in their "new battle" campaign. <https://www.accenture.com/t20180423T055005Z_w_/se-en/_acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf> <https://www.us-cert.gov/sites/default/files/publications/IR-ALERT-MED-17-093-01C-Intrusions_Affecting_Multiple_Victims_Across_Multiple_Sectors.pdf>
	Jul 2018	Attack on the Japanese media sector In July 2018, FireEye devices detected and blocked what appears to be APT10 (menuPass) activity targeting the Japanese media sector. <https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html>
	Apr 2019	In April 2019, enSilo detected what it believes to be new activity by Chinese cyber espionage group APT10. The variants discovered by enSilo are previously unknown and deploy malware that is unique to the threat actor. <https://blog.ensilo.com/uncovering-new-activity-by-apt10>
Counter operations	• Chinese Hackers Indicted (2018) <https://www.fbi.gov/news/stories/chinese-hackers-indicted-122018>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0045/>	

Strider, ProjectSauron

Names	Strider *(Symantec)* ProjectSauron *(Kaspersky)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(Symantec) Strider has been active since at least October 2011. The group has maintained a low profile until now and its targets have been mainly organizations and individuals that would be of interest to a nation state's intelligence services. Symantec obtained a sample of the group's Remsec malware from a customer who submitted it following its detection by our behavioral engine. Remsec is primarily designed to spy on targets. It opens a back door on an infected computer, can log keystrokes, and steal files. Strider has been highly selective in its choice of targets and, to date, Symantec has found evidence of infections in 36 computers across seven separate organizations. The group's targets include a number of organizations and individuals located in Russia, an airline in China, an organization in Sweden, and an embassy in Belgium.
Observed	Sectors: Defense, Embassies, Financial, Government, Scientific research centers and Telecommunications. Countries: Belgium, China, Iran, Russia, Rwanda and Sweden.
Tools used	Remsec.
Information	<https://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets> <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07190154/The-ProjectSauron-APT_research_KL.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0041/>

Suckfly

Names	Suckfly *(Symantec)*
Country	China
Motivation	Information theft and espionage
Description	(Symantec) In March 2016, Symantec published a blog on Suckfly, an advanced cyberespionage group that conducted attacks against a number of South Korean organizations to steal digital certificates. Since then we have identified a number of attacks over a two-year period, beginning in April 2014, which we attribute to Suckfly. The attacks targeted high-profile targets, including government and commercial organizations. These attacks occurred in several different countries, but our investigation revealed that the primary targets were individuals and organizations primarily located in India. While there have been several Suckfly campaigns that infected organizations with the group's custom malware Backdoor.Nidiran, the Indian targets show a greater amount of post-infection activity than targets in other regions. This suggests that these attacks were part of a planned operation against specific targets in India.
Observed	Sectors: E-commerce, Entertainment, Financial, Government, Healthcare, Media, Shipping, Software development and Video game development. Countries: India.
Tools used	gsecdump, Nidiran, rcpscan, smbscan and wce.
Operations performed	Apr 2014	The first known Suckfly campaign began in April of 2014. During our investigation of the campaign, we identified a number of global targets across several industries who were attacked in 2015. Many of the targets we identified were well known commercial organizations located in India. <https://www.symantec.com/connect/blogs/indian-organizations-targeted-suckfly-attacks>
	Late 2015	We discovered Suckfly, an advanced threat group, conducting targeted attacks using multiple stolen certificates, as well as hacktools and custom malware. The group had obtained the certificates through pre-attack operations before commencing targeted attacks against a number of government and commercial organizations spread across multiple continents over a two-year period. This type of activity and the malicious use of stolen certificates emphasizes the importance of safeguarding certificates to prevent them from being used maliciously. <https://www.symantec.com/connect/blogs/suckfly-revealing-secret-life-your-code-signing-certificates>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0039/>

TA459

Names	TA459 *(Proofpoint)*
Country	China
Motivation	Information theft and espionage
Description	(Proofpoint) On April 20 [2017], Proofpoint observed a targeted campaign focused on financial analysts working at top global financial firms operating in Russia and neighboring countries. These analysts were linked by their coverage of the telecommunications industry, making this targeting very similar to, and likely a continuation of, activity described in our "In Pursuit of Optical Fibers and Troop Intel" blog. This time, however, attackers opportunistically used spear-phishing emails with a Microsoft Word attachment exploiting the recently patched CVE-2017-0199 to deploy the ZeroT Trojan, which in turn downloaded the PlugX Remote Access Trojan (RAT). Proofpoint is tracking this attacker, believed to operate out of China, as TA459. The actor typically targets Central Asian countries, Russia, Belarus, Mongolia, and others. TA549 possesses a diverse malware arsenal including PlugX, NetTraveler, and ZeroT.
Observed	Sectors: Financial Analysts. Countries: Central Asian countries, Belarus, Mongolia, Russia and others.
Tools used	Gh0st RAT, NetTraveler, PlugX and ZeroT.
Information	<https://www.proofpoint.com/us/threat-insight/post/apt-targets-financial-analysts>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0062/>

TA505

Names	TA505 *(Proofpoint)*
Country	[Unknown]
Motivation	Financial gain
Description	(Proofpoint) Proofpoint researchers track a wide range of threat actors involved in both financially motivated cybercrime and state-sponsored actions. One of the more prolific actors that we track - referred to as TA505 - is responsible for the largest malicious spam campaigns we have ever observed, distributing instances of the Dridex banking Trojan, Locky ransomware, Jaff ransomware, The Trick banking Trojan, and several others in very high volumes. Because TA505 is such a significant part of the email threat landscape, this blog provides a retrospective on the shifting malware, payloads, and campaigns associated with this actor. We examine their use malware such as Jaff, Bart, and Rockloader that appear to be exclusive to this group as well as more widely distributed malware like Dridex and Pony. Where possible, we detail the affiliate models with which they are involved and outline the current state of TA505 campaigns. TA505 is arguably one of the most significant financially motivated threat actors because of the extraordinary volumes of messages they send. The variety of malware delivered by the group also demonstrates their deep connections to the underground malware scene. At the time of writing, Locky ransomware remains their malware of choice, even as the group continues to experiment with a variety of additional malware.
Observed	Sectors: Financial, Hospitality and Retail. Countries: Chile, China, France, Germany, Hungary, India, Italy, Mexico, Malawi, Pakistan, South Korea, Taiwan, UK, Ukraine and USA.
Tools used	Bart, Dridex, FlawedAmmy, FlawedGrace, GlobeImposter, Jaff, Kegotip, Locky, LOLBins, Necurs, Neutrino, Philadelphia, RockLoader, RMS, ServHelper, Shifu and The Trick.
Operations performed	Oct 2017	On October 10, TA505 introduced their first geo-targeted campaign dropping either Locky or The Trick banking Trojan. In this campaign, HTML files were attached to emails inquiring about the status of an invoice. <https://www.proofpoint.com/us/threat-insight/post/ta505-shifts-times>
	Jun 2018	We first observed an actor embedding SettingContent-ms inside a PDF on June 18. However, on July 16 we observed a particularly large campaign with hundreds of thousands of messages attempting to deliver PDF attachments with an embedded SettingContent-ms file. <https://www.proofpoint.com/us/threat-insight/post/ta505-abusing-settingcontent-ms-within-pdf-files-distribute-flawedammyy-rat>
	Nov 2018	Since November 15, 2018, Proofpoint began observing email campaigns from a specific actor targeting large retail chains, restaurant chains and grocery chains, as well as other organizations in the food and beverage industries. <https://www.proofpoint.com/us/threat-insight/post/ta505-targets-us-retail-industry-personalized-attachments>

	Nov 2018	ServHelper and FlawedGrace - New malware introduced by TA505 <https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505>
	Dec 2018	In mid-December 2018 a spear-phishing campaign was detected as targeting large US-based retailers along with organizations in the food and beverage industry. Masquerading as a legitimate communication sent from a Ricoh printer, the initial email lured victims into opening an attached malicious Microsoft Word document.
	Dec 2018	Last month, 360 Threat Intelligence Center captured multiple phishing emails sent by TA505 Group to target financial institutions. These phishing emails contain Excel attachments with Excel 4.0 Macro embedded and download Backdoor at last. <https://ti.360.net/blog/articles/excel-4.0-macro-utilized-by-ta505-to-target-financial-institutions-recently-en/>
	Apr 2019	LOLBins and a New Backdoor Malware <https://www.cybereason.com/blog/threat-actor-ta505-targets-financial-enterprises-using-lolbins-and-a-new-backdoor-malware>
	May 2019	During the last month our Threat Intelligence surveillance team spotted increasing evidence of an operation intensification against the Banking sector. <https://blog.yoroi.company/research/the-stealthy-email-stealer-in-the-ta505-arsenal/>
	May 2019	In the last few days, during monitoring activities, Yoroi CERT noticed a suspicious attack against an Italian organization. The malicious email contains a highly suspicious sample which triggered the ZLAB team to investigate its capabilities and its possible attribution, discovering a potential expansion of the TA505 operation. <https://blog.yoroi.company/research/ta505-is-expanding-its-operations/>
Information		<https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter> <https://e.cyberint.com/hubfs/Report%20Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors%20Tools/CyberInt_Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors'%20Tools_Report.pdf> <https://www.cybereason.com/blog/threat-actor-ta505-targets-financial-enterprises-using-lolbins-and-a-new-backdoor-malware> <https://threatpost.com/ta505-servhelper-malware/140792/>

Taidoor

Names	Taidoor *(Trend Micro)*
Country	China
Motivation	Information theft and espionage
Description	(Trend Micro) The Taidoor attackers have been actively engaging in targeted attacks since at least March 4, 2009. Despite some exceptions, the Taidoor campaign often used Taiwanese IP addresses as C&C servers and email addresses to send out socially engineered emails with malware as attachments. One of the primary targets of the Taidoor campaign appeared to be the Taiwanese government. The attackers spoofed Taiwanese government email addresses to send out socially engineered emails in the Chinese language that typically leveraged Taiwan-themed issues. The attackers actively sent out malicious documents and maintained several IP addresses for command and control. As part of their social engineering ploy, the Taidoor attackers attach a decoy document to their emails that, when opened, displays the contents of a legitimate document but executes a malicious payload in the background. We were only able to gather a limited amount of information regarding the Taidoor attackers' activities after they have compromised a target. We did, however, find that the Taidoor malware allowed attackers to operate an interactive shell on compromised computers and to upload and download files. In order to determine the operational capabilities of the attackers behind the Taidoor campaign, we monitored a compromised honeypot. The attackers issued out some basic commands in an attempt to map out the extent of the network compromise but quickly realized that the honeypot was not an intended targeted and so promptly disabled the Taidoor malware running on it. This indicated that while Taidoor malware were more widely distributed compared with those tied to other targeted campaigns, the attackers could quickly assess their targets and distinguish these from inadvertently compromised computers and honeypots.
Observed	Sectors: Government. Countries: Taiwan.
Tools used	Taidoor.
Information	<https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_taidoor_campaign.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0015/>

TeamSpy Crew

Names	TeamSpy Crew *(Kaspersky)* SIG39 *(NSA)*
Country	Russia
Motivation	Information theft and espionage
Description	(Kaspersky) Researchers have uncovered a long-term cyber-espionage campaign that used a combination of legitimate software packages and commodity malware tools to target a variety of heavy industry, government intelligence agencies and political activists. Known as the TeamSpy crew because of its affinity for using the legitimate TeamViewer application as part of its toolset, the attackers may have been active for as long as 10 years, researchers say. The attack appears to be a years-long espionage campaign, but experts who have analyzed the victim profile, malware components and command-and-control infrastructure say that it's not entirely clear what kind of data the attackers are going after. What is clear, though, is that the attackers have been at this for a long time and that they have specific people in mind as targets. Researchers at the CrySyS Lab in Hungary were alerted by the Hungarian National Security Authority to an attack against a high-profile target in the country and began looking into the campaign. They quickly discovered that some of the infrastructure being used in the attack had been in use for some time and that the target they were investigating was by no means the only one.
Observed	Countries: Worldwide.
Tools used	Malicious versions of TeamViewer and JAVA RATs.
Information	<https://www.crysys.hu/publications/files/teamspy.pdf> <https://d2538mqrb7brka.cloudfront.net/wp-content/uploads/sites/43/2018/03/20134928/theteamspystory_final_t2.pdf>

TeleBots

Names	TeleBots *(ESET)*
Country	Russia
Motivation	Sabotage and destruction
Description	(ESET) In the second half of 2016, ESET researchers identified a unique malicious toolset that was used in targeted cyberattacks against high-value targets in the Ukrainian financial sector. We believe that the main goal of attackers using these tools is cybersabotage. This blog post outlines the details about the campaign that we discovered. We will refer to the gang behind the malware as TeleBots. However it's important to say that these attackers, and the toolset used, share a number of similarities with the BlackEnergy group, which conducted attacks against the energy industry in Ukraine in December 2015 and January 2016. In fact, we think that the BlackEnergy group has evolved into the TeleBots group. This group appears to be closely associated with, or evolved from, Sandworm Team, Iron Viking, Voodoo Bear.
Observed	Sectors: Financial, Software companies and Transportation. Countries: Ukraine and Worldwide (NotPetya).
Tools used	Felixroot, GreyEnergy, NotPetya and TeleDoor.
Operations performed	Dec 2016	These recent ransomware KillDisk variants are not only able to target Windows systems, but also Linux machines, which is certainly something we don't see every day. This may include not only Linux workstations but also servers, amplifying the damage potential. <https://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt/>
	Mar 2017	In 2017, the TeleBots group didn't stop their cyberattacks; in fact, they became more sophisticated. In the period between January and March 2017 the TeleBots attackers compromised a software company in Ukraine (not related to M.E. Doc), and, using VPN tunnels from there, gained access to the internal networks of several financial institutions. <https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/>
	May 2017	XData ransomware making rounds amid global WannaCryptor scare A week after the global outbreak of WannaCryptor, also known as WannaCry, another ransomware variant has been making the rounds. Detected by ESET as Win32/Filecoder.AESNI.C, and also known as XData ransomware, the threat has been most prevalent in Ukraine, with 96% of the total detections between May 17th and May 22nd, and peaking on Friday, May 19th. ESET has protected its customers against this threat since May 18th. <https://www.welivesecurity.com/2017/05/23/xdata-ransomware-making-rounds-amid-global-wannacryptor-scare/>

	Jun 2017	NotPetya ransomware[7] <https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine/>
	Oct 2017	Bad Rabbit ransomware[8] <https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/>
Information		<https://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/> <https://blog.trendmicro.com/trendlabs-security-intelligence/timeline-of-sandworm-attacks/>

---

[7] See ThaiCERT Whitepaper "NotPetya Ransomware"
[8] See ThaiCERT Whitepaper "BadRabbit Ransomware"

Temper Panda, admin@338

Names	Temper Panda *(Crowdstrike)* admin@338 *(FireEye)* Team338 *(Kaspersky)* Magnesium *(Microsoft)*
Country	China
Motivation	Information theft and espionage
Description	(FireEye) The threat group has previously used newsworthy events as lures to deliver malware. They have largely targeted organizations involved in financial, economic and trade policy, typically using publicly available RATs such as Poison Ivy, as well some non-public backdoors. The group started targeting Hong Kong media companies, probably in response to political and economic challenges in Hong Kong and China. The threat group's latest activity coincided with the announcement of criminal charges against democracy activists. During the past 12 months, Chinese authorities have faced several challenges, including large-scale protests in Hong Kong in late 2014, the precipitous decline in the stock market in mid-2015, and the massive industrial explosion in Tianjin in August 2015. In Hong Kong, the pro-democracy movement persists, and the government recently denied a professor a post because of his links to a pro-democracy leader.
Observed	Sectors: Defense, Financial, Government, Media and Think Tanks. Countries: Hong Kong and USA.
Tools used	Bozok, BUBBLEWRAP, LOWBALL, Poison Ivy and Systeminfo.
Information	<https://www.fireeye.com/blog/threat-research/2013/10/know-your-enemy-tracking-a-rapidly-evolving-apt-actor.html> <https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0018/>

TEMP.Veles

Names	TEMP.Veles *(FireEye)* Xenotime *(Dragos)*
Country	Russia
Sponsor	State-sponsored, Central Scientific Research Institute of Chemistry and Mechanics
Motivation	Sabotage and destruction
Description	TEMP.Veles is a Russia-based threat group that has targeted critical infrastructure. The group has been observed utilizing TRITON, a malware framework designed to manipulate industrial safety systems.
Observed	Sectors: Critical infrastructure and Oil and gas.
Tools used	Cryptcat, HatMan, Mimikatz, NetExec, PSExec, SecHack, TRISIS, TRITON and Wii.
Operations performed	2014	TRISIS malware <https://dragos.com/resource/trisis-analyzing-safety-system-targeting-malware/>
	2017	TRITON malware <https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html> <https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html>
Information	<https://dragos.com/resource/xenotime/> <https://www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html> <https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%E2%80%94Safety%20System%20Targeted%20Malware_S508C.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0088/>

Terbium

Names	Terbium *(Microsoft)*
Country	[Unknown]
Motivation	Sabotage and destruction
Description	(Microsoft) A few weeks ago, multiple organizations in the Middle East fell victim to targeted and destructive attacks that wiped data from computers, and in many cases rendering them unstable and unbootable. Destructive attacks like these have been observed repeatedly over the years and the Windows Defender and Windows Defender Advanced Threat Protection Threat Intelligence teams are working on protection, detection, and response to these threats. Microsoft Threat Intelligence identified similarities between this recent attack and previous 2012 attacks against tens of thousands of computers belonging to organizations in the energy sector. Microsoft Threat Intelligence refers to the activity group behind these attacks as Terbium, following our internal practice of assigning rogue actors chemical element names.
Observed	Countries: Middle East.
Tools used	Depriz.
Information	<https://www.microsoft.com/security/blog/2016/12/09/windows-10-protection-detection-and-response-against-recent-attacks/>

Thrip

Names	Thrip *(Symantec)*
Country	China
Motivation	Information theft, espionage and sabotage
Description	(Symantec) Perhaps the most worrying discovery we made was that Thrip had targeted a satellite communications operator. The attack group seemed to be particularly interested in the operational side of the company, looking for and infecting computers running software that monitors and controls satellites. This suggests to us that Thrip's motives go beyond spying and may also include disruption. Another target was an organization involved in geospatial imaging and mapping. Again, Thrip seemed to be mainly interested in the operational side of the company. It targeted computers running MapXtreme Geographic Information System (GIS) software which is used for tasks such as developing custom geospatial applications or integrating location-based data into other applications. It also targeted machines running Google Earth Server and Garmin imaging software. The satellite operator wasn't the only communications target Thrip was interested in. The group had also targeted three different telecoms operators, all based in Southeast Asia. In all cases, based on the nature of the computers infected by Thrip, it appeared that the telecoms companies themselves and not their customers were the targets of these attacks. In addition, there was a fourth target of interest, a defense contractor.
Observed	Sectors: Defense, Satellite and Telecommunications. Countries: Southeast Asia and USA.
Tools used	Catchamas, Mimikatz, Rikamanu, Spedear and WMI Ghost.
Information	<https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0076/>

Transparent Tribe, APT 36

Names	Transparent Tribe *(Proofpoint)* APT 36 *(Mandiant)* ProjectM *(Palo Alto)* Mythic Leopard *(CrowdStrike)* TEMP.Lapis *(FireEye)*
Country	Pakistan
Motivation	Information theft and espionage
Description	(Proofpoint) Proofpoint researchers recently uncovered evidence of an advanced persistent threat (APT) against Indian diplomatic and military resources. Our investigation began with malicious emails sent to Indian embassies in Saudi Arabia and Kazakstan but turned up connections to watering hole sites focused on Indian military personnel and designed to drop a remote access Trojan (RAT) with a variety of data exfiltration functions. Our analysis shows that many of the campaigns and attacks appear related by common IOCs, vectors, payloads, and language, but the exact nature and attribution associated with this APT remain under investigation. At this time, the background and analysis in this paper provide useful forensics and detail our current thinking on the malware that we have dubbed "MSIL/Crimson".
Observed	Sectors: Defense, Embassies and Government. Countries: India.
Tools used	Andromeda, beendoor, Bezigate, Bozok, BreachRAT, Crimson RAT, DarkComet, Luminosity RAT, njRAT, Peppy Trojan and UPDATESEE.
Operations performed	Feb 2016	Operation "Transparent Tribe" On February 11, 2016, we discovered two attacks minutes apart directed towards officials at Indian embassies in both Saudi Arabia and Kazakhstan. Both e-mails (Fig. 1, 2) were sent from the same originating IP address (5.189.145[.]248) belonging to Contabo GmbH, a hosting provider that seems to be currently favored by these threat actors. The e-mails also likely utilized Rackspace's MailGun service and both of them were carrying the same exact attachment. <https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf>
	Mar 2016	Indian TV station CNN-IBN has discovered that Pakistani officials were collecting data about Indian troop movements using an Android app called SmeshApp. <https://news.softpedia.com/news/smeshapp-removed-from-play-store-because-pakistan-used-it-to-spy-on-indian-army-501936.shtml>
	Mar 2016	Operation "C-Major" Trend Micro is reporting on a third campaign, which they've named Operation C-Major. According to the security firm, this campaign targeted Indian military officials via spear-phishing emails, distributing spyware to its victims via an Adobe Reader vulnerability. <https://news.softpedia.com/news/another-case-of-a-pakistani-apt-spying-on-indian-military-personnel-502093.shtml> <https://blog.trendmicro.com/trendlabs-security-intelligence/operation-c-major-actors-also-used-android-blackberry-mobile-spyware-targets/>

	Feb 2017	This blog post describes another attack campaign where attackers impersonated identity of Indian think tank IDSA (Institute for Defence Studies and Analyses) and sent out spear-phishing emails to target officials of the Central Bureau of Investigation (CBI) and possibly the officials of Indian Army. <https://cysinfo.com/cyber-attack-targeting-cbi-and-possibly-indian-army-officials/>
Information		<https://www.fireeye.com/blog/threat-research/2016/06/apt_group_sends_spea.html> <https://www.crowdstrike.com/blog/adversary-of-the-month-for-may/>

Tropic Trooper

Names	Tropic Trooper *(Trend Micro)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	Tropic Trooper is an unaffiliated threat group that has led targeted campaigns against targets in Taiwan, the Philippines, and Hong Kong. Tropic Trooper focuses on targeting government, healthcare, transportation, and high-tech industries and has been active since 2011.
Observed	Sectors: Defense, Government, Healthcare, High-Tech and Transportation. Countries: Hong Kong, Philippines and Taiwan.
Tools used	KeyBoy, PCShare, Poison Ivy, Titan, Yahoyah and Winsloader.
Operations performed	2012	Operation "Tropic Trooper" Taiwan and the Philippines have become the targets of an ongoing campaign called "Operation Tropic Trooper." Active since 2012, the attackers behind the campaign have set their sights on the Taiwanese government as well as a number of companies in the heavy industry. The same campaign has also targeted key Philippine military agencies. <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-tropic-trooper.pdf>
	2014	New Strategy Tropic Trooper (also known as KeyBoy) levels its campaigns against Taiwanese, Philippine, and Hong Kong targets, focusing on their government, healthcare, transportation, and high-tech industries. <https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-trooper-new-strategy/>
	Aug 2016	In early August, Unit 42 identified two attacks using similar techniques. The more interesting one was a targeted attack towards the Secretary General of Taiwan's Government office – Executive Yuan. The Executive Yuan has several individual boards which are formed to enforce different executing functions of the government. The Executive Yuan Council evaluates statutory and budgetary bills and bills concerning martial law, amnesty, declaration of war, conclusion of peace and treaties, and other important affairs. <https://unit42.paloaltonetworks.com/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/>
	2017	Tropic Trooper goes mobile with Titan surveillanceware The latest threat to follow this trend is Titan, a family of sophisticated Android surveillanceware apps surfaced by Lookout's automated analysis that, based on command and control infrastructure, is linked to the same actors behind Operation Tropic Trooper. <https://blog.lookout.com/titan-mobile-threat>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0081/>

Turla, Waterbug, Venomous Bear

Names	Turla *(Kaspersky)* Waterbug *(Symantec)* Venomous Bear *(CrowdStrike)* Group 88 *(Talos)* SIG23 *(NSA)* Iron Hunter *(SecureWorks)* Pacifier APT *(Bitdefender)*
Country	Russia
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	Turla is a Russian-based threat group that has infected victims in over 45 countries, spanning a range of industries including government, embassies, military, education, research and pharmaceutical companies since 2004. Heightened activity was seen in mid-2015. Turla is known for conducting watering hole and spear-phishing campaigns and leveraging in-house tools and malware. Turla's espionage platform is mainly used against Windows machines, but has also been seen used against macOS and Linux machines.
Observed	Sectors: Defense, Education, Embassies, Energy, Government, High-Tech, Media, NGOs, Pharmaceutical, Research and Retail. Countries: Afghanistan, Algeria, Armenia, Australia, Austria, Azerbaijan, Belarus, Belgium, Bolivia, Botswana, Brazil, China, Chile, Denmark, Ecuador, Estonia, Finland, France, Georgia, Germany, Hong Kong, Hungary, India, Indonesia, Iran, Iraq, Italy, Jamaica, Jordan, Kazakhstan, Kyrgyzstan, Kuwait, Latvia, Mexico, Netherlands, Pakistan, Paraguay, Poland, Qatar, Romania, Russia, Serbia, Spain, Saudi Arabia, South Africa, Sweden, Switzerland, Syria, Tajikistan, Thailand, Tunisia, Turkmenistan, UK, Ukraine, Uruguay, USA, Uzbekistan, Venezuela, Vietnam and Yemen.
Tools used	AdobeARM, Agent.BTZ, Agent.DNE, ATI-Agent, Cobra Carbon System, ComRAT, Empire, Epic, Gazer, gpresult, HTML5 Encoding, IcedCoffeer, Kazuar, KopiLuwak, KRYPTON, KSL0T, LightNeuron, Maintools.js, Metasploit, Mimikatz, MiniDionis, Mosquito, Nautilus, nbtstat, Neuron, Outlook Backdoor, Penguin Turla, Pfinet, Popeye, pwdump, Skipper, Snake, Systeminfo, Tasklist, Tavdig, Turla, Uroburos, wce, WhiteAtlas, WhiteBear, Wipbot, WITCHCOVEN and WRAITH.
Operations performed	1996	Operation "Moonlight Maze" That is why our experts, aided by researchers from King's College London, have carefully studied Moonlight Maze — one of the first widely known cyberespionage campaigns, active since at least 1996. It is of particular interest because several independent experts from countries have voiced the proposition that it is associated with a much more modern — and still active — group, the authors of the Turla APT attack. <https://www.kaspersky.com/blog/moonlight-maze-the-lessons/6713/>
	Nov 2008	Breach of the US Department of Defense <https://www.nytimes.com/2010/08/26/technology/26cyber.html>
	2013	Breach of the Finnish Foreign Ministry

		<https://yle.fi/uutiset/osasto/news/russian_group_behind_2013_foreign_ministry_hack/8591548>
	2013	Operation "Epic Turla" Over the last 10 months, Kaspersky Lab researchers have analyzed a massive cyber-espionage operation which we call "Epic Turla". The attackers behind Epic Turla have infected several hundred computers in more than 45 countries, including government institutions, embassies, military, education, research and pharmaceutical companies. <https://securelist.com/the-epic-turla-operation/65545/>
	2014	Breach of the Swiss military firm RUAG <https://www.melani.admin.ch/melani/en/home/dokumentation/reports/technical-reports/technical-report_apt_case_ruag.html>
	Dec 2014	Operation "Penguin Turla" The Turla APT campaigns have a broader reach than initially anticipated after the recent discovery of two modules built to infect servers running Linux. Until now, every Turla sample in captivity was designed for either 32- or 64-bit Windows systems, but researchers at Kaspersky Lab have discovered otherwise. <https://threatpost.com/linux-modules-connected-to-turla-apt-discovered/109765/>
	2015	Operation "Satellite Turla" Obviously, such incredibly apparent and large-scale attacks have little chance of surviving for long periods of time, which is one of the key requirements for running an APT operation. It is therefore not very feasible to perform the attack through MitM traffic hijacking, unless the attackers have direct control over some high-traffic network points, such as backbone routers or fiber optics. There are signs that such attacks are becoming more common, but there is a much simpler way to hijack satellite-based Internet traffic. <https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/>
	2015	Operation "WITCHCOVEN" When an unsuspecting user visits any of the over 100 compromised websites, a small piece of inserted code—embedded in the site's HTML and invisible to casual visitors—quietly redirects the user's browser to a second compromised website without the user's knowledge. This second website hosts the WITCHCOVEN script, which uses profiling techniques to collect technical information on the user's computer. As of early November 2015, we identified a total of 14 websites hosting the WITCHCOVEN profiling script. <https://www2.fireeye.com/rs/848-DID-242/images/rpt-witchcoven.pdf>
	Nov 2016	Operation "Skipper Turla" On 28 January 2017, John Lambert of Microsoft (@JohnLaTwC) tweeted about a malicious document that dropped a "very interesting .JS backdoor". Since the end of November 2016, Kaspersky Lab has observed Turla using this new JavaScript payload and specific macro variant.

		<https://securelist.com/kopiluwak-a-new-javascript-payload-from-turla/77429/> <https://securelist.com/introducing-whitebear/81638/>
	2017	Operation "Turla Mosquito" ESET researchers have observed a significant change in the campaign of the infamous espionage group <https://www.welivesecurity.com/2018/05/22/turla-mosquito-shift-towards-generic-tools/>
	Mar 2017	New versions of Carbon The Turla espionage group has been targeting various institutions for many years. Recently, we found several new versions of Carbon, a second stage backdoor in the Turla group arsenal. <https://www.welivesecurity.com/2017/03/30/carbon-paper-peering-turlas-second-stage-backdoor/>
	May 2017	New backdoor Kazuar <https://unit42.paloaltonetworks.com/unit42-kazuar-multiplatform-espionage-backdoor-api-access/>
	Jun 2017	Some of the tactics used in APT attacks die hard. A good example is provided by Turla's watering hole campaigns. Turla, which has been targeting governments, government officials and diplomats for years – see, as an example, this recent paper – is still using watering hole techniques to redirect potentially interesting victims to their C&C infrastructure. In fact, they have been using them since at least 2014 with very few variations in their modus operandi. <https://www.welivesecurity.com/2017/06/06/turlas-watering-hole-campaign-updated-firefox-extension-abusing-instagram/>
	Jul 2017	Russian malware link hid in a comment on Britney Spears' Instagram The Slovak IT security company ESET Security released a report yesterday detailing a cleverly hidden example of such a post. And its hideout? A Britney Spears photo. Among the nearly 7,000 comments written on the performer's post (shown below) was one that could easily pass as spam. <https://www.engadget.com/2017/06/07/russian-malware-hidden-britney-spears-instagram/>
	Aug 2017	New backdoor Gazer <https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf>
	Aug 2017	In this case, the dropper is being delivered with a benign and possibly stolen decoy document inviting recipients to a G20 task force meeting on the "Digital Economy". The Digital Economy event is actually scheduled for October of this year in Hamburg, Germany. <https://www.proofpoint.com/us/threat-insight/post/turla-apt-actor-refreshes-kopiluwak-javascript-backdoor-use-g20-themed-attack>
	Jan 2018	A notorious hacking group is targeting the UK with an updated version of malware designed to embed itself into compromised networks and stealthily conduct espionage. Both the Neuron and Nautilus malware variants have previously been attributed to the Turla advanced persistent threat group, which regularly carries out cyber-espionage against a range of targets,

		including government, military, technology, energy, and other commercial organisations. <https://www.zdnet.com/article/this-hacking-gang-just-updated-the-malware-it-uses-against-uk-targets/>
	Mar 2018	Starting in March 2018, we observed a significant change in the campaign: it now leverages the open source exploitation framework Metasploit before dropping the custom Mosquito backdoor. <https://www.welivesecurity.com/2018/05/22/turla-mosquito-shift-towards-generic-tools/>
	2018	Much of our 2018 research focused on Turla's KopiLuwak javascript backdoor, new variants of the Carbon framework and meterpreter delivery techniques. Also interesting was Mosquito's changing delivery techniques, customized PoshSec-Mod open-source powershell use, and borrowed injector code. We tied some of this activity together with infrastructure and data points from WhiteBear and Mosquito infrastructure and activity in 2017 and 2018. <https://securelist.com/shedding-skin-turlas-fresh-faces/88069/>
	May 2019	Turla, also known as Snake, is an infamous espionage group recognized for its complex malware. To confound detection, its operators recently started using PowerShell scripts that provide direct, in-memory loading and execution of malware executables and libraries. This allows them to bypass detection that can trigger when a malicious executable is dropped on disk. <https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/>
Information		<https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf> <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-march-venomous-bear/>
MITRE ATT&CK		<https://attack.mitre.org/groups/G0010/>

Urpage

Names	Urpage *(Trend Micro)*
Country	[Middle East]
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	(Trend Micro) In the process of monitoring changes in the threat landscape, we get a clearer insight into the way threat actors work behind the schemes. In this case we dig deeper into the possible connection between cyberattacks by focusing on the similarities an unnamed threat actor shares with Confucius, Patchwork, Dropping Elephant, and another threat actor called Bahamut. For the sake of this report, we will call this unnamed threat actor "Urpage."
Observed	Countries: Pakistan.
Tools used	Trojaned Android applications.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/the-urpage-connection-to-bahamut-confucius-and-patchwork/>

Volatile Cedar

Names	Volatile Cedar *(Check Point)* Dancing Salome *(Kaspersky)*
Country	Lebanon
Motivation	Information theft and espionage
Description	(Check Point) Beginning in late 2012, the carefully orchestrated attack campaign we call Volatile Cedar has been targeting individuals, companies and institutions worldwide. This campaign, led by a persistent attacker group, has successfully penetrated a large number of targets using various attack techniques, and specifically, a custom-made malware implant codenamed Explosive. This report provides an extended technical analysis of Volatile Cedar and the Explosive malware. We have seen clear evidence that Volatile Cedar has been active for almost 3 years. While many of the technical aspects of the threat are not considered "cutting edge", the campaign has been continually and successfully operational throughout this entire timeline, evading detection by the majority of AV products. This success is due to a well-planned and carefully managed operation that constantly monitors its victims' actions and rapidly responds to detection incidents.
Observed	Sectors: Education, Government and Hosting. Countries: Canada, Israel, Lebanon, Russia, Saudi Arabia, UK and USA.
Tools used	Explosive.
Operations performed	Jun 2015	After going public with our findings, we were provided with a new configuration belonging to a newly discovered sample we have never seen before. <https://blog.checkpoint.com/2015/06/09/new-data-volatile-cedar/>
Information	<https://www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf> <https://securelist.com/sinkholing-volatile-cedar-dga-infrastructure/69421/>

Whitefly

Names	Whitefly *(Symantec)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(Symantec) Symantec researchers have discovered that this attack group, which we call Whitefly, has been operating since at least 2017, has targeted organizations based mostly in Singapore across a wide variety of sectors, and is primarily interested in stealing large amounts of sensitive information. Whitefly compromises its victims using custom malware alongside open-source hacking tools and living off the land tactics, such as malicious PowerShell scripts. From mid-2017 to mid-2018, Whitefly launched targeted attacks against multiple organizations. While most of these organizations were based in Singapore, some were multinational organizations with a presence in Singapore.
Observed	Sectors: Engineering, Healthcare, Media and Telecommunications. Countries: Singapore.
Tools used	Mimikatz, Nibatad, Termite and Vcrodat.
Operations performed	Jul 2018	Breach of SingHealth <https://www.reuters.com/article/us-singapore-cyberattack/cyberattack-on-singapore-health-database-steals-details-of-1-5-million-including-pm-idUSKBN1KA14J>
Information	<https://www.symantec.com/blogs/threat-intelligence/whitefly-espionage-singapore>

Wicked Spider, APT 22

Names	Wicked Spider *(CrowdStrike)* APT 22 *(Mandiant)*
Country	China
Motivation	Financial gain
Description	(CrowdStrike) Winnti Group, Blackfly, Wicked Panda refers to the targeted intrusion operations of the actor publicly known as "Winnti," whereas Wicked Spider represents this group's financially-motivated criminal activity. Originally, Wicked Spider was observed exploiting a number of gaming companies and stealing code-signing certificates for use in other operations associated with the malware known as Winnti. Now, Winnti is commonly associated with the interests of the government of the People's Republic of China (PRC). Wicked Spider has been observed targeting technology companies in Germany, Indonesia, the Russian Federation, South Korea, Sweden, Thailand, Turkey, the United States, and elsewhere. Notably, Wicked Spider has often targeted gaming companies for their certificates, which can be used in future PRC-based operations to sign malware. Ongoing analysis is still evaluating how these certificates are used — whether Wicked Spider hands the certificates off to other adversaries for use in future campaigns or stockpiles them for its own use.
Observed	Sectors: Technology. Countries: Germany, Indonesia, Russia, South Korea, Sweden, Thailand, Turkey, USA and elsewhere.
Tools used	ETERNALBLUE, DOUBLEPULSAR and PlugX.
Information	<https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-july-wicked-spider/>

Wild Neutron, Butterfly, Sphinx Moth

Names	Wild Neutron *(Kaspersky)* Butterfly *(Symantec)* Morpho *(Symantec)* Sphinx Moth *(Kudeslski)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(Symantec) A corporate espionage group has compromised a string of major corporations over the past three years in order to steal confidential information and intellectual property. The gang, which Symantec calls Butterfly, is not-state sponsored, rather financially motivated. It has attacked multi-billion dollar companies operating in the internet, IT software, pharmaceutical, and commodities sectors. Twitter, Facebook, Apple, and Microsoft are among the companies who have publicly acknowledged attacks. Butterfly is technically proficient and well resourced. The group has developed a suite of custom malware tools capable of attacking both Windows and Apple computers, and appears to have used at least one zero-day vulnerability in its attacks. It keeps a low profile and maintains good operational security. After successfully compromising a target organization, it cleans up after itself before moving on to its next target. This group operates at a much higher level than the average cybercrime gang. It is not interested in stealing credit card details or customer databases and is instead focused on high-level corporate information. Butterfly may be selling this information to the highest bidder or may be operating as hackers for hire. Stolen information could also be used for insider-trading purposes.
Observed	Sectors: Bitcoin-related companies, Healthcare, Investment companies, IT, Real estate, lawyers and individual users. Countries: Algeria, Austria, Canada, France, Germany, Kazakhstan, Palestine, Russia, Slovenia, Switzerland, UAE and USA.
Tools used	HesperBot, JripBot, WildNeutron and many 0-days vulnerabilities.
Operations performed	Jan 2013 — Attack on Twitter <https://blog.twitter.com/official/en_us/a/2013/keeping-our-users-secure.html>
	Feb 2013 — Attack on Facebook <https://www.facebook.com/notes/facebook-security/protecting-people-on-facebook/10151249208250766>
	Feb 2013 — Attack on Apple <https://www.reuters.com/article/us-apple-hackers/exclusive-apple-macs-hit-by-hackers-who-targeted-facebook-idUSBRE91I0920130219>
	Feb 2013 — Attack on Microsoft <https://blogs.technet.microsoft.com/msrc/2013/02/22/recent-cyberattacks/>
Information	<https://www.symantec.com/connect/blogs/butterfly-profiting-high-level-corporate-attacks>

	<https://securelist.com/wild-neutron-economic-espionage-threat-actor-returns-with-new-tricks/71275/> <https://research.kudelskisecurity.com/2015/11/05/sphinx-moth-expanding-our-knowledge-of-the-wild-neutron-morpho-apt/>

Winnti Group, Blackfly, Wicked Panda

Names	Winnti Group *(Kaspersky)* Blackfly *(Symantec)* Wicked Panda *(CrowdStrike)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	Winnti Group is a threat group with Chinese origins that has been active since at least 2010. The group has heavily targeted the gaming industry, but it has also expanded the scope of its targeting. Some reporting suggests a number of other groups, including Axiom, Group 72, APT 17, Deputy Dog, and Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon, are closely linked to Winnti Group. (Trend Micro) The group behind the Winnti malware (which we will call the Winnti group for brevity) sprung up as a band of traditional cyber crooks, comprising black hats whose technical skills were employed to perpetrate financial fraud. Based on the use of domain names they registered, the group started out in the business of fake/rogue anti-virus products in 2007. In 2009, the Winnti group shifted to targeting gaming companies in South Korea using a self-named data- and file-stealing malware. The group, which was primarily motivated by profit, is noted for utilizing self-developed technically-proficient tools for their attacks. They once attacked a game server to illicitly farm in-game currency ("gaming gold", which also has real-world value) and stole source codes of online game projects. The group also engaged in the theft of digital certificates which they then used to sign their malware to make them stealthier. The Winnti group diversified its targets to include enterprises such as those in pharmaceutics and telecommunications. The group has since earned infamy for being involved in malicious activities associated with targeted attacks, such as deploying spear-phishing campaigns and building a backdoor.
Observed	Sectors: Online video game companies, Pharmaceutical and Telecommunications. Countries: Belarus, Brazil, China, Germany, India, Indonesia, Japan, Peru, Philippines, Russia, South Korea, Taiwan, Thailand, USA and Vietnam.
Tools used	Cobalt Strike and Winnti.
Operations performed	2010	HBGary investigated an information security incident at an American video game company.
	2011	In the autumn of 2011, a Trojan was detected on a huge number of computers – all of them linked by the fact that they were used by players of a popular online game. It emerged that the piece of malware landed on users' computers as part of a regular update from the game's official update server. Some even suspected that the publisher itself was spying on players. However, it later became clear that the malicious program ended up on the users' computers by mistake: the cybercriminals were in fact targeting the companies that develop and release computer games. <https://securelist.com/winnti-more-than-just-a-game/37029/>

	Aug 2014	This time the operators put such tag in the configuration and it turned out to be the name of the well-known global pharmaceutical company headquartered in Europe. <https://securelist.com/games-are-over/70991/>
	Oct 2015	Breach of a Vietnamese gaming company <https://blog.vsec.com.vn/apt/initial-winnti-analysis-against-vietnam-game-company.html> During the investigation, a Linux version of Winnti was found. <https://medium.com/chronicle-blog/winnti-more-than-just-windows-and-gates-e4f03436031a>
	Feb 2016	Breach of German Steelmaker ThyssenKrupp <https://www.dw.com/en/thyssenkrupp-victim-of-cyber-attack/a-36695341>
	Autumn 2016	Breach of TeamViewer <https://www.bleepingcomputer.com/news/security/teamviewer-confirms-undisclosed-breach-from-2016/>
	Mar 2017	Recently, the Winnti group, a threat actor with a past of traditional cybercrime -particularly with financial fraud, has been seen abusing GitHub by turning it into a conduit for the command and control (C&C) communications of their seemingly new backdoor (detected by Trend Micro as BKDR64_WINNTI.ONM). <https://blog.trendmicro.com/trendlabs-security-intelligence/winnti-abuses-github/>
	Early 2018	Breach of German chemicals giant Bayer <https://www.dw.com/en/bayer-points-finger-at-wicked-panda-in-cyberattack/a-48196004>
	Mar 2019	Although the malware uses different configurations in each case, the three affected software products included the same backdoor code and were launched using the same mechanism. While two of the compromised products no longer include the backdoor, one of the affected developers is still distributing the trojanized version: ironically, the game is named Infestation, and is produced by Thai developer Electronics Extreme. <https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia/>
Information		<https://blog.trendmicro.com/trendlabs-security-intelligence/pigs-malware-examining-possible-member-winnti-group/> <https://securelist.com/winnti-more-than-just-a-game/37029/> <https://401trg.com/burning-umbrella/>
MITRE ATT&CK		<https://attack.mitre.org/groups/G0044/>

WindShift

Names	WindShift *(DarkMatter)*
Country	[Unknown]
Motivation	Information theft and espionage
Description	(Palo Alto) In August of 2018, DarkMatter released a report entitled "In the Trails of WindShift APT", which unveiled a threat actor with TTPs very similar to those of Bahamut. Subsequently, two additional articles were released by Objective-See which provide an analysis of some validated WindShift samples targeting OSX systems. Pivoting on specific file attributes and infrastructure indicators, Unit 42 was able to identify and correlate additional attacker activity and can now provide specific details on a targeted WindShift attack as it unfolded at a Middle Eastern government agency.
Observed	Sectors: Government. Countries: Middle East.
Tools used	WindTail.
Information	<https://unit42.paloaltonetworks.com/shifting-in-the-wind-windshift-attacks-target-middle-eastern-governments/> <https://gsec.hitb.org/materials/sg2018/D1%20COMMSEC%20-%20In%20the%20Trails%20of%20WINDSHIFT%20APT%20-%20Taha%20Karim.pdf>

[Unnamed group]

Names	[Unnamed group]
Country	Iran
Sponsor	State-sponsored
Motivation	Information theft and espionage
Description	(ClearSky) Over the last few weeks, several significant leaks regarding a number of Iranian APTs took place. After analyzing and investigating the documents we conclude that they are authentic. Consequently, this causes considerable harm to the groups and their operation. The identity of the actor behind the leak is currently unknown, however based on the scope and the quality of the exposed documents and information, it appears that they are professional and highly capable. This leak will likely hamstring the groups' operation in the near future. Accordingly, in our assessment this will minimize the risk of potential attacks in the next few months and possibly even year. Note -most of the leaks are posted on Telegram channels that were created specifically for this purpose. Below are the three main Telegram groups on which the leaks were posted: • Lab Dookhtegam pseudonym ("The people whose lips are stitched and sealed" –translation from Persian) –In this channel attack tools attributed to the group 'OilRig' were leaked; including a webshell that was inserted into the Technion, various tools that were used for DNS attacks, and more. • Green Leakers–In this channel attack tools attributed to the group 'MuddyWatter' were leaked. The group's name and its symbol are identified with the "green movement", which led the protests in Iran after the Presidential elections in 2009. These protests were heavily repressed by the revolutionary guards (IRGC) • Black Box–Unlike the previous two channels this has been around for a long time. On Friday May 5th, dozens of confidential documents labeled as "secret" (a high confidentiality level in Iran, one before the highest -top secret) were posted on this channel. The documents were related to Iranian attack groups' activity.
Observed	Sectors: Airlines, Government, IT and Telecommunications. Countries: Afghanistan, Australia, Azerbaijan, Bahrain, Colombia, Dubai, Egypt, Ethiopia, Fiji, Hong Kong, India, Indonesia, Iraq, Israel, Kenia, Kuwait, Kyrgyzstan, Lebanon, Malaysia, Mauritius, Morocco, New Zealand, Oman, Pakistan, Philippines, Qatar, South Africa, Sri Lanka, Syria, Thailand, Turkey and UAE.
Tools used	
Information	<https://www.clearskysec.com/wp-content/uploads/2019/05/Iranian-Nation-State-APT-Leak-Analysis-and-Overview.pdf>

Some Other Prolific Criminal Groups

Achilles

Names	Achilles *(AdvIntel)*
Country	[Unknown]
Motivation	Financial gain
Description	This actor may be related to Iridium. (AdvIntel) "Achilles" is an English-speaking threat actor primarily operating on various English-language underground hacking forums as well as through secure messengers. Achilles specializes in obtaining accesses to high-value corporate internal networks. On May 4, 2019, Achilles claimed to have access to UNICEF network as well as networks of several high-profile corporate entities. They were able to provide evidence of their presence within the UNICEF network and two private sector companies. It is noteworthy that they provided access to networks at a relatively low price range of $5,000 USD to $2,000 USD. The majority of Achilles offers are related to breaches into multinational corporate networks via external VPN and compromised RDPs. Targets include private companies and government organizations, primarily in the British Commonwealth. Achilles has been particularly active on forums through the last seven months, with rising spikes in activities in Fall 2018 and Spring 2019.
Observed	Sectors: Defense, Government and private sectors. Countries: Australia, UK and USA.
Tools used	RDP.
Operations performed	Oct 2018	Breach of Navy shipbuilder Austal <https://www.abc.net.au/news/2018-11-13/iranian-hackers-suspected-in-austal-cyber-breach/10489310>
Information	<https://www.advanced-intel.com/blog/achilles-hacker-behind-attacks-on-military-shipbuilders-unicef-international-corporations> <https://www.bleepingcomputer.com/news/security/another-hacker-selling-access-to-charity-antivirus-firm-networks/>

Dungeon Spider

Names	Dungeon Spider *(CrowdStrike)*
Country	[Unknown]
Motivation	Financial gain
Description	(CrowdStrike) Dungeon Spider is a criminal group operating the ransomware most commonly known as Locky, which has been active since February 2016 and was last observed in late 2017. Locky is a ransomware tool that encrypts files using a combination of cryptographic algorithms: RSA with a key size of 2,048 bits, and AES with a key size of 128 bits. Locky targets a large number of file extensions and is able to encrypt data on shared network drives. In an attempt to further impact victims and prevent file recovery, Locky deletes all of the Shadow Volume Copies on the machine. Dungeon Spider primarily relies on broad spam campaigns with malicious attachments for distribution. Locky is the community/industry name associated with this actor.
Observed	
Tools used	Locky.
Information	<https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-october-dungeon-spider/>

Fxmsp

Names	Fxmsp *(self given)*
Country	Russia
Motivation	Financial gain
Description	(AdvIntel) Throughout 2017 and 2018, Fxmsp established a network of trusted proxy resellers to promote their breaches on the criminal underground. Some of the known Fxmsp TTPs included accessing network environments via externally available remote desktop protocol (RDP) servers and exposed active directory. Most recently, the actor claimed to have developed a credential-stealing botnet capable of infecting high-profile targets in order to exfiltrate sensitive usernames and passwords. Fxmsp has claimed that developing this botnet and improving its capabilities for stealing information from secured systems is their main goal.
Observed	
Tools used	RDP and exposed AD.
Operations performed	May 2019	Breaches of Three Major Anti-Virus Companies <https://www.advanced-intel.com/blog/top-tier-russian-hacking-collective-claims-breaches-of-three-major-anti-virus-companies>
Information	<https://www.advanced-intel.com/blog/top-tier-russian-hacking-collective-claims-breaches-of-three-major-anti-virus-companies>

Gnosticplayers

Names	Gnosticplayers *(self given)*
Country	[Unknown]
Motivation	Financial gain
Description	(ZDNet) The hacker said that he put up the data for sale mainly because these companies had failed to protect passwords with strong encryption algorithms like bcrypt. Most of the hashed passwords the hacker put up for sale today can cracked with various levels of difficulty --but they can be cracked. "I got upset because I feel no one is learning," the hacker told ZDNet in an online chat earlier today. "I just felt upset at this particular moment, because seeing this lack of security in 2019 is making me angry." In a conversation with ZDNet last month, the hacker told us he wanted to hack and put up for sale more than one billion records and then retire and disappear with the money. But in a conversation today, the hacker says this is not his target anymore, as he learned that other hackers have already achieved the same goal before him. Gnosticplayers also revealed that not all the data he obtained from hacked companies had been put up for sale. Some companies gave into extortion demands and paid fees so breaches would remain private. "I came to an agreement with some companies, but the concerned startups won't see their data for sale," he said. "I did it that's why I can't publish the rest of my databases or even name them."
Observed	
Tools used	
Operations performed	Feb 2019	620 million accounts stolen from 16 hacked websites now for sale on dark web, seller boasts <https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/>
	Feb 2019	127 million user records from 8 companies put up for sale on the dark web <https://www.zdnet.com/article/127-million-user-records-from-8-companies-put-up-for-sale-on-the-dark-web/>
	Feb 2019	Hacker is selling 93 million user records from eight companies, including GfyCat. <https://www.zdnet.com/article/hacker-puts-up-for-sale-third-round-of-hacked-databases-on-the-dark-web/>
	Mar 2019	Round 4: Hacker returns and puts 26Mil user records for sale on the Dark Web <https://www.zdnet.com/article/round-4-hacker-returns-and-puts-26mil-user-records-for-sale-on-the-dark-web/>

	Apr 2019	Hacker Gnosticplayers has stolen over 932 million user records from 44 companies <https://www.zdnet.com/article/a-hacker-has-dumped-nearly-one-billion-user-records-over-the-past-two-months/>
	May 2019	Australian tech unicorn Canva suffers security breach <https://www.zdnet.com/article/australian-tech-unicorn-canva-suffers-security-breach/>

Gold Lowell, Boss Spider

Names	Gold Lowell *(SecureWorks)* Boss Spider *(CrowdStrike)*
Country	Iran
Motivation	Financial gain
Description	(SecureWorks) In late 2015, Secureworks Counter Threat Unit (CTU) researchers began tracking financially motivated campaigns leveraging SamSam ransomware (also known as Samas and SamsamCrypt). CTU researchers associate this activity with the Gold Lowell threat group. Gold Lowell typically scans for and exploits known vulnerabilities in Internet-facing systems to gain an initial foothold in a victim's network. The threat actors then deploy the SamSam ransomware and demand payment to decrypt the victim's files. The consistent tools and behaviors associated with SamSam intrusions since 2015 suggest that Gold Lowell is either a defined group or a collection of closely affiliated threat actors. Applying security updates in a timely manner and regularly monitoring for anomalous behaviors on Internet-facing systems are effective defenses against these tactics. Organizations should also create and test response plans for ransomware incidents and use backup solutions that are resilient to corruption or encryption attempts.
Observed	Sectors: Government and Healthcare.
Tools used	Mimikatz, PSExec and SamSam.
Counter operations	• Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses (2018) <https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public>
Information	<https://www.secureworks.com/research/samsam-ransomware-campaigns> <https://www.crowdstrike.com/blog/an-in-depth-analysis-of-samsam-ransomware-and-boss-spider/>

Grim Spider

Names	Grim Spider *(CrowdStrike)* TEMP.MixMaster *(FireEye)*
Country	Russia
Motivation	Financial gain
Description	Grim Spider is reportedly associated with Lunar Spider and Wizard Spider. (CrowdStrike) Grim Spider is a sophisticated eCrime group that has been operating the Ryuk ransomware since August 2018, targeting large organizations for a high-ransom return. This methodology, known as "big game hunting," signals a shift in operations for Wizard Spider, a criminal enterprise of which Grim Spider appears to be a cell. The Wizard Spider threat group, known as the Russia-based operator of the TrickBot banking malware, had focused primarily on wire fraud in the past. Similar to Samas and BitPaymer, Ryuk is specifically used to target enterprise environments. Code comparison between versions of Ryuk and Hermes ransomware indicates that Ryuk was derived from the Hermes source code and has been under steady development since its release. Hermes is commodity ransomware that has been observed for sale on forums and used by multiple threat actors. However, Ryuk is only used by Grim Spider and, unlike Hermes, Ryuk has only been used to target enterprise environments. Since Ryuk's appearance in August, the threat actors operating it have netted over 705.80 BTC across 52 transactions for a total current value of $3,701,893.98 USD.
Observed	
Tools used	Ryuk.
Information	<https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/> <https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html>

Hacking Team

Names	Hacking Team *(real name)*
Country	Italy
Motivation	Financial gain
Description	The many 0-days that had been collected by Hacking Team and which became publicly available during the breach of their organization in 2015, have been used by several APT groups since.

(ESET) Since being founded in 2003, the Italian spyware vendor Hacking Team gained notoriety for selling surveillance tools to governments and their agencies across the world.

The capabilities of its flagship product, the Remote Control System (RCS), include extracting files from a targeted device, intercepting emails and instant messaging, as well as remotely activating a device's webcam and microphone. The company has been criticized for selling these capabilities to authoritarian governments – an allegation it has consistently denied.

When the tables turned in July 2015, with Hacking Team itself suffering a damaging hack, the reported use of RCS by oppressive regimes was confirmed. With 400GB of internal data – including the once-secret list of customers, internal communications, and spyware source code – leaked online, Hacking Team was forced to request its customers to suspend all use of RCS, and was left facing an uncertain future.

Following the hack, the security community has been keeping a close eye on the company's efforts to get back on its feet. The first reports suggesting Hacking Team's resumed operations came six months later – a new sample of Hacking Team's Mac spyware was apparently in the wild. A year after the breach, an investment by a company named Tablem Limited brought changes to Hacking Team's shareholder structure, with Tablem Limited taking 20% of Hacking Team's shareholding. Tablem Limited is officially based in Cyprus; however, recent news suggests it has ties to Saudi Arabia. |
Observed	
Tools used	
Information	<https://en.wikipedia.org/wiki/Hacking_Team> <https://www.vice.com/en_us/article/gvye3m/spy-tech-company-hacking-team-gets-hacked>

Indrik Spider

Names	Indrik Spider *(CrowdStrike)*
Country	[Unknown]
Motivation	Financial gain
Description	(CrowdStrike) Indrik Spider is a sophisticated eCrime group that has been operating Dridex since June 2014. In 2015 and 2016, Dridex was one of the most prolific eCrime banking trojans on the market and, since 2014, those efforts are thought to have netted Indrik Spider millions of dollars in criminal profits. Throughout its years of operation, Dridex has received multiple updates with new modules developed and new anti-analysis features added to the malware. In August 2017, a new ransomware variant identified as BitPaymer was reported to have ransomed the U.K.'s National Health Service (NHS), with a high ransom demand of 53 BTC (approximately $200,000 USD). The targeting of an organization rather than individuals, and the high ransom demands, made BitPaymer stand out from other contemporary ransomware at the time. Though the encryption and ransom functionality of BitPaymer was not technically sophisticated, the malware contained multiple anti-analysis features that overlapped with Dridex. Later technical analysis of BitPaymer indicated that it had been developed by Indrik Spider, suggesting the group had expanded its criminal operation to include ransomware as a monetization strategy.
Observed	
Tools used	Dridex and BitPaymer.
Information	<https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/>

Lunar Spider

Names	Lunar Spider *(CrowdStrike)*
Country	Russia
Motivation	Financial gain
Description	Lunar Spider is reportedly associated with Grim Spider and Wizard Spider. (CrowdStrike) On March 17, 2019, CrowdStrike Intelligence observed the use of a new BokBot (developed and operated by Lunar Spider) proxy module in conjunction with TrickBot (developed and operated by Wizard Spider), which may provide Wizard Spider with additional tools to steal sensitive information and conduct fraudulent wire transfers. This activity also provides further evidence to support the existence of a flourishing relationship between these two actors.
Observed	
Tools used	BokBot and Vawtrak.
Information	<https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/> <https://www.crowdstrike.com/blog/wizard-spider-lunar-spider-shared-proxy-module/>

Mummy Spider, TA542

Names	Mummy Spider *(CrowdStrike)* TA542 *(Proofpoint)*
Country	[Unknown]
Motivation	Financial gain
Description	(Crowdstrike) Mummy Spider is a criminal entity linked to the core development of the malware most commonly known as Emotet or Geodo. First observed in mid-2014, this malware shared code with the Bugat (aka Feodo) banking Trojan. However, Mummy Spider swiftly developed the malware's capabilities to include an RSA key exchange for command and control (C2) communication and a modular architecture. Mummy Spider does not follow typical criminal behavioral patterns. In particular, Mummy Spider usually conducts attacks for a few months before ceasing operations for a period of between three and 12 months, before returning with a new variant or version. After a 10 month hiatus, Mummy Spider returned Emotet to operation in December 2016 but the latest variant is not deploying a banking Trojan module with web injects, it is currently acting as a 'loader' delivering other malware packages. The primary modules perform reconnaissance on victim machines, drop freeware tools for credential collection from web browsers and mail clients and a spam plugin for self-propagation. The malware is also issuing commands to download and execute other malware families such as the banking Trojans Dridex and Qakbot. Mummy Spider advertised Emotet on underground forums until 2015, at which time it became private. Therefore, it is highly likely that Emotet is operated solely for use by Mummy Spider or with a small trusted group of customers.
Observed	Sectors: Energy, Financial, Government, Healthcare, Manufacturing, Shipping and Logistics, Utilities and Technology. Countries: Canada and USA.
Tools used	Emotet and Geodo.
Operations performed	2019	Between January 1, 2019, to May 1, 2019, threat actors conducted thousands of malicious email campaigns, hundreds of which were sent to Canadian organizations. While discussions of threats in this region often focus on "North America" generally or just the United States, nearly 100 campaigns during this period were either specifically targeted at Canadian organizations or were customized for Canadian audiences. <https://www.proofpoint.com/us/threat-insight/post/beyond-north-america-threat-actors-target-canada-specifically>
Information	<https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-february-mummy-spider/>

Operation Comando

Names	Operation Comando *(Palo Alto)*
Country	[Unknown]
Motivation	Financial gain
Description	(Palo Alto) In December 2018, Palo Alto Networks Unit 42 researchers identified an ongoing campaign with a strong focus on the hospitality sector, specifically on hotel reservations. Although our initial analysis didn't show any novel or advanced techniques, we did observe strong persistence during the campaign that triggered our curiosity. We followed network traces and pivoted on the information left behind by this actor, such as open directories, document metadata, and binary peculiarities, which enabled us to find a custom-made piece of malware, that we named "CapturaTela". Our discovery of this malware family shows the reason for the persistent focus on hotel reservations as a primary vector: stealing credit card information from customers. We profiled this threat actor and that has resulted in uncovering not only their delivery mechanisms, but also their arsenal of remote access tools and info-stealing trojans, both acquired from underground forums as well as open source tools found in GitHub repositories.
Observed	Sectors: Hospitality, specifically on hotel reservations. Countries: Brazil.
Tools used	CapturaTela.
Information	<https://unit42.paloaltonetworks.com/operation-comando-or-how-to-run-a-cheap-and-effective-credit-card-business/>

OurMine

Names	OurMine *(real name)*
Country	Saudi Arabia
Motivation	Financial gain
Description	OurMine is known for celebrity internet accounts, often causing cyber vandalism, to advertise their commercial services. (Trend Micro) In light of the recent report detailing its willingness to pay US$250,000 in exchange for the 1.5 terabytes' worth of data swiped by hackers from its servers, HBO finds itself dealing with yet another security breach. Known for hijacking prominent social media accounts, the self-styled white hat hacking group OurMine took over a number of verified Twitter and Facebook accounts belonging to the cable network. These include accounts for HBO shows, such as "Game of Thrones," "Girls," and "Ballers." This is not the first time that OurMine has claimed responsibility for hacking high-profile social networking accounts. Last year, the group victimized Marvel, The New York Times, and even the heads of some of the biggest technology companies in the world. Mark Zuckerberg, Jack Dorsey, Sundar Pichai, and Daniel Ek — the CEOs of Facebook, Twitter, Google and Spotify, respectively — have also fallen victim to the hackers, dispelling the notion that a career in software and technology exempts one from being compromised.
Observed	
Tools used	
Operations performed	Aug 2017	Breach of VEVO Vevo, the joint venture between Universal Music Group, Sony Music Entertainment, Abu Dhabi Media, Warner Music Group, and Alphabet Inc. (Google's parent company), was just hacked. Roughly 3.12TB worth of internal files have been posted online, and a couple of the documents reviewed by Gizmodo appear sensitive. <https://gizmodo.com/welp-vevo-just-got-hacked-1813390834>
	Sep 2017	Breach of DNS records of WikiLeaks <https://www.grahamcluley.com/despite-appearances-wikileaks-wasnt-hacked/>
Information	<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hbo-twitter-and-facebook-accounts-hacked-by-ourmine> <https://en.wikipedia.org/wiki/OurMine>

Pacha Group

Names	Pacha Group *(Intezer)*
Country	China
Motivation	Financial gain
Description	(Intezer) Antd is a miner found in the wild on September 18, 2018. Recently we discovered that the authors from Antd are actively delivering newer campaigns deploying a broad number of components, most of them completely undetected and operating within compromised third party Linux servers. Furthermore, we have observed that some of the techniques implemented by this group are unconventional, and there is an element of sophistication to them. We believe the authors behind this malware are from Chinese origin. We have labeled the undetected Linux.Antd variants, Linux.GreedyAntd and classified the threat actor as Pacha Group.
Observed	
Tools used	Antd, DDG, GreedyAntd, Korkerds and XMRig.
Operations performed	Sep 2018	Intezer has evidence dating back to September 2018 which shows Pacha Group has been using a cryptomining malware that has gone undetected on other engines. <https://www.intezer.com/blog-pacha-group-deploying-undetected-cryptojacking-campaigns/>
	May 2019	Pacha Group Competing against Rocke Group for Cryptocurrency Mining Foothold on the Cloud <https://www.intezer.com/blog-technical-analysis-cryptocurrency-mining-war-on-the-cloud/>
Information	<https://www.intezer.com/blog-technical-analysis-pacha-group/>

Pinchy Spider

Names	Pinchy Spider *(CrowdStrike)*
Country	Russia
Motivation	Financial gain
Description	(CrowdStrike) CrowdStrike Intelligence has recently observed Pinchy Spider affiliates deploying GandCrab ransomware in enterprise environments, using lateral movement techniques and tooling commonly associated with nation-state adversary groups and penetration testing teams. This change in tactics makes Pinchy Spider and its affiliates the latest eCrime adversaries to join the growing trend of targeted, low-volume/high-return ransomware deployments known as "big game hunting." Pinchy Spider is the criminal group behind the development of the ransomware most commonly known as GandCrab, which has been active since January 2018. Pinchy Spider sells access to use GandCrab ransomware under a partnership program with a limited number of accounts. The program is operated with a 60-40 split in profits (60 percent to the customer), as is common among eCrime actors, but Pinchy Spider is also willing to negotiate up to a 70-30 split for "sophisticated" customers.
Observed	
Tools used	GandCrab.

Operations performed	Jun 2019	Yesterday night, a source in the malware community has told ZDNet that the GandCrab RaaS operator formally announced plans to shut down their service within a month. The announcement was made in an official thread on a well-known hacking forum, where the GandCrab RaaS has advertised its service since January 2018, when it formally launched. <https://www.zdnet.com/article/gandcrab-ransomware-operation-says-its-shutting-down/>
Information		<https://www.crowdstrike.com/blog/pinchy-spider-adopts-big-game-hunting/>

Rocke

Names	Rocke *(Talos)*
Country	China
Motivation	Financial gain
Description	(Talos) This threat actor initially came to our attention in April 2018, leveraging both Western and Chinese Git repositories to deliver malware to honeypot systems vulnerable to an Apache Struts vulnerability. In late July, we became aware that the same actor was engaged in another similar campaign. Through our investigation into this new campaign, we were able to uncover more details about the actor.
Observed	
Tools used	Apache Struts and Xbash.
Operations performed	Jan 2019	Palo Alto Networks Unit 42 recently captured and investigated new samples of the Linux coin mining malware used by the Rocke group. The family was suspected to be developed by the Iron cybercrime group and it's also associated with the Xbash malware we reported on in September of 2018. The threat actor Rocke was originally revealed by Talos in August of 2018 and many remarkable behaviors were disclosed in their blog post. The samples described in this report were collected in October of 2018, and since that time the command and control servers they use have been shut down. <https://unit42.paloaltonetworks.com/malware-used-by-rocke-group-evolves-to-evade-detection-by-cloud-security-products/>
	May 2019	Pacha Group Competing against Rocke Group for Cryptocurrency Mining Foothold on the Cloud <https://www.intezer.com/blog-technical-analysis-cryptocurrency-mining-war-on-the-cloud/>
	May 2019	Over the past month we have seen new features constantly being added to the malware. For instance, in their latest major update, they have added a function that exploits systems running the software development automation server Jenkins to increase their chance of infecting more systems, thereby generating more profits. In addition, they have also evolved their malware by adding new attack stages, as well as new redundancies in its multi-component execution to make it more dynamic and flexible. <https://www.fortinet.com/blog/threat-research/rocke-variant-ready-to-box-mining-challengers.html>
Information	<https://blog.talosintelligence.com/2018/08/rocke-champion-of-monero-miners.html>

Shadow Brokers

Names	Shadow Brokers (self given)
Country	USA
Motivation	Financial gain
Description	Breached a server where zero-days accumulated by Equation Group were held, leaked a large section on the internet[9] and tried to sell the rest afterward. Most of the published vulnerabilities have since been fixed by the respective vendors, but many have been used by other threat actors. Most notably among the dumps were zero-days such as ETERNALBLUE that were used for the creation of infamous ransomware explosions such as WannaCry and NotPetya. Shadow Brokers turned out to be an ex-NSA contractor.
Observed	
Tools used	
Operations performed	Aug 2016	Initial public dump <https://musalbas.com/blog/2016/08/16/equation-group-firewall-operations-catalogue.html>
	Oct 2016	'Shadow Brokers' Whine That Nobody Is Buying Their Hacked NSA Files <https://www.vice.com/en_us/article/53djj3/shadow-brokers-whine-that-nobody-is-buying-their-hacked-nsa-files>
	Oct 2016	Second Shadow Brokers dump released <https://www.scmagazineuk.com/second-shadow-brokers-dump-released/article/1476023>
	Mar 2017	In March 2017, the ShadowBrokers published a chunk of stolen data that included two frameworks: DanderSpritz and FuzzBunch. <https://securelist.com/darkpulsar/88199/>
	Apr 2017	Shadow Brokers leaks show U.S. spies successfully hacked Russian, Iranian targets <https://www.cyberscoop.com/nsa-shadow-brokers-leaks-iran-russia-optimusprime-stoicsurgeon/>
	Apr 2017	New NSA leak may expose its bank spying, Windows exploits <https://www.csoonline.com/article/3190055/new-nsa-leak-may-expose-its-bank-spying-windows-exploits.html>
	Apr 2017	ShadowBrokers Dump More Equation Group Hacks, Auction File Password <https://threatpost.com/shadowbrokers-dump-more-equation-group-hacks-auction-file-password/124882/>
	Sep 2017	ShadowBrokers are back demanding nearly $4m and offering 2 dumps per month <http://securityaffairs.co/wordpress/62770/hacking/shadowbrokers-return.html>

---

[9] See ThaiCERT Whitepaper "Shadow Broker - Equation Group Hack"

	Sep 2017	ShadowBrokers Release UNITEDRAKE Malware <https://www.hackread.com/nsa-data-dump-shadowbrokers-expose-unitedrake-malware/>
Counter operations		• Who Was the NSA Contractor Arrested for Leaking the 'Shadow Brokers' Hacking Tools? (2017) <https://blacklakesecurity.com/who-was-the-nsa-contractor-arrested-for-leaking-the-shadow-brokers-hacking-tools/>

[Vault 7/8]

Names	[Vault 7/8]
Country	USA
Motivation	Financial gain
Description	An unnamed source leaked almost 10,000 documents describing a large number of 0-day vulnerabilities, methodologies and tools that had been collected by the CIA, such as, specifically, the group known as Longhorn, The Lamberts. This leaking was done through WikiLeaks, since March 2017. In weekly publications, the dumps were said to come from Vault 7 and later Vault 8, until his arrest in 2018. Most of the published vulnerabilities have since been fixed by the respective vendors, but many have been used by other threat actors. This actor turned out to be a former CIA software engineer. (WikiLeaks) Today, Tuesday 7 March 2017, WikiLeaks begins its new series of leaks on the U.S. Central Intelligence Agency. Code-named "Vault 7" by WikiLeaks, it is the largest ever publication of confidential documents on the agency. The first full part of the series, "Year Zero", comprises 8,761 documents and files from an isolated, high-security network situated inside the CIA's Center for Cyber Intelligence in Langley, Virgina. It follows an introductory disclosure last month of CIA targeting French political parties and candidates in the lead up to the 2012 presidential election. Recently, the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized "zero day" exploits, malware remote control systems and associated documentation. This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA. The archive appears to have been circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive. "Year Zero" introduces the scope and direction of the CIA's global covert hacking program, its malware arsenal and dozens of "zero day" weaponized exploits against a wide range of U.S. and European company products, include Apple's iPhone, Google's Android and Microsoft's Windows and even Samsung TVs, which are turned into covert microphones.
Observed	
Tools used	
Counter operations	• Joshua Adam Schulte Charged with the Unauthorized Disclosure of Classified Information and Other Offenses Relating to the Theft of Classified Material from the Central Intelligence Agency (2018) <https://www.justice.gov/opa/pr/joshua-adam-schulte-charged-unauthorized-disclosure-classified-information-and-other-offenses>
Information	<https://wikileaks.org/ciav7p1/> and all updates.

Wizard Spider

Names	Wizard Spider *(CrowdStrike)*
Country	Russia
Motivation	Financial gain
Description	Wizard Spider is reportedly associated with Grim Spider and Lunar Spider. (Crowdstrike) The Wizard Spider threat group is the Russia-based operator of the TrickBot banking malware. This group represents a growing criminal enterprise of which Grim Spider appears to be a subset. The Lunar Spider threat group is the Eastern European-based operator and developer of the commodity banking malware called BokBot (aka IcedID), which was first observed in April 2017. The BokBot malware provides Lunar Spider affiliates with a variety of capabilities to enable credential theft and wire fraud, through the use of webinjects and a malware distribution function.
Observed	
Tools used	Dyre and TrickBot.
Information	<https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/> <https://www.crowdstrike.com/blog/wizard-spider-lunar-spider-shared-proxy-module/>

Zombie Spider

Names	Zombie Spider *(CrowdStrike)*
Country	Russia
Motivation	Financial gain
Description	(CrowdStrike) The primary threat actor, who was tracked by CrowdStrike as Zombie Spider, rose to prominence in the criminal underground under the moniker Peter Severa. The individual behind this handle is Peter Yuryevich LEVASHOV who was arrested in Spain when the final version of Kelihos was taken over in April 2017, and who recently pleaded guilty to operating the botnet for criminal purposes. For several years, pump-and-dump stock scams, dating ruses, credential phishing, money mule recruitment and rogue online pharmacy advertisements were the most common spam themes. In 2017, however, Kelihos was frequently used to spread other malware such as LuminosityLink, Zyklon HTTP, Neutrino, Nymaim, Gozi/ISFB, Panda Zeus, Kronos, and TrickBot. It was also observed spreading ransomware families including Shade, Cerber, and FileCrypt2.
Observed	Countries: Worldwide.
Tools used	Kelihos.
Counter operations	• Justice Department Announces Actions to Dismantle Kelihos Botnet (2017) <https://www.justice.gov/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0>
Information	<https://www.crowdstrike.com/blog/inside-the-takedown-of-zombie-spider-and-the-kelihos-botnet/> <https://www.crowdstrike.com/blog/farewell-to-kelihos-and-zombie-spider/>

APPENDIX: Sources Used

The following sources have been used to compile this encyclopedia:

1. MISP Threat Actors galaxy
   <https://github.com/MISP/misp-galaxy/blob/master/clusters/threat-actor.json>

2. MITRE ATT&CK Framework – Groups
   <https://attack.mitre.org/groups/>

3. APT Groups and Operations
   <https://apt.threattracking.com>

4. Malpedia
   <https://malpedia.caad.fkie.fraunhofer.de/>

5. ThaiCERT Risk Intelligence archive and extensive searches on the Internet.