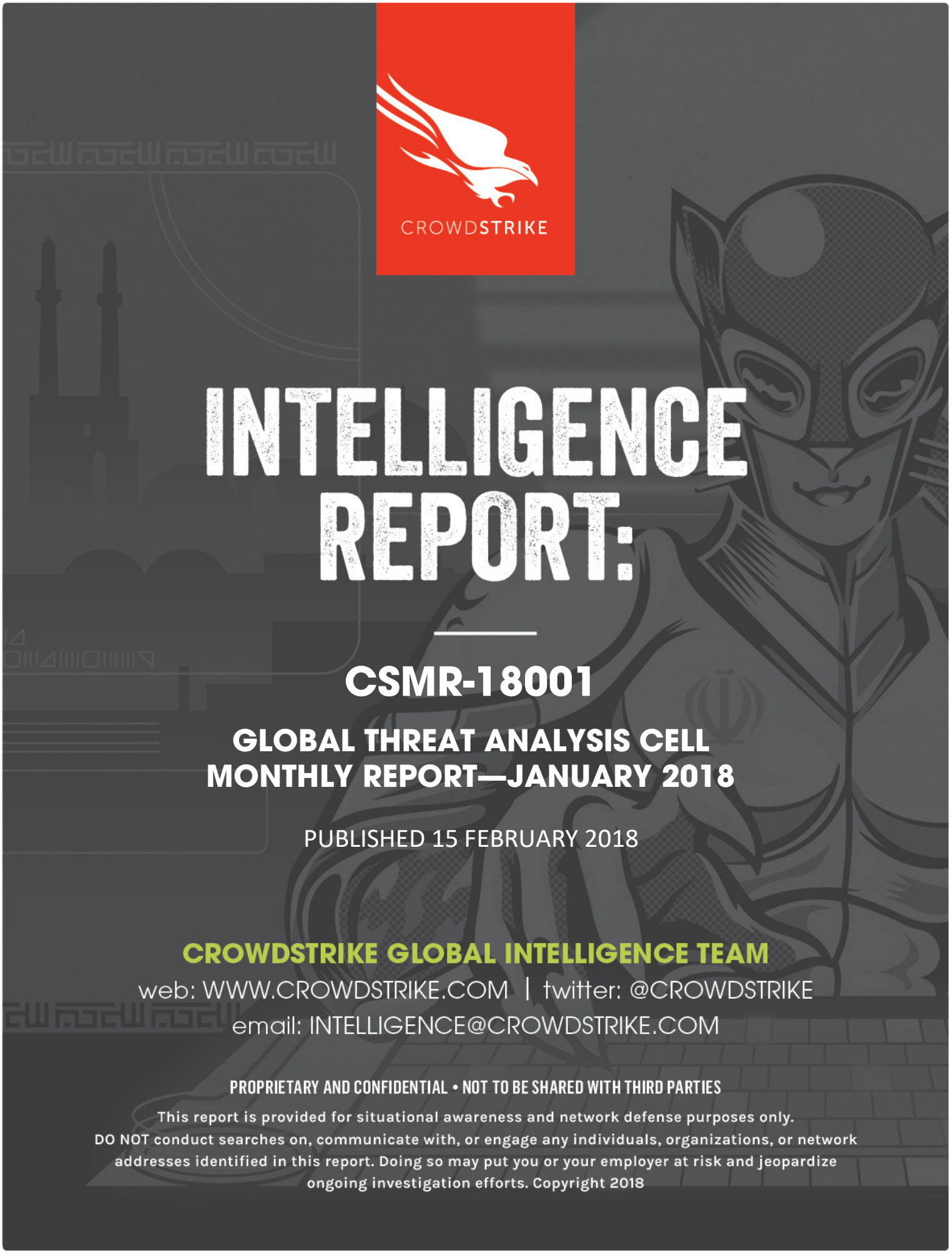

INTELLIGENCE REPORT:

CSMR-18001

GLOBAL THREAT ANALYSIS CELL MONTHLY REPORT—JANUARY 2018

PUBLISHED 15 FEBRUARY 2018

CROWDSTRIKE GLOBAL INTELLIGENCE TEAM

web: WWW.CROWDSTRIKE.COM | twitter: @CROWDSTRIKE

email: INTELLIGENCE@CROWDSTRIKE.COM

EXECUTIVE SUMMARY

Targeted Intrusion

Targeted intrusion incidents observed in January 2018 included activity from Russian, Chinese, Iranian, Indian, and North Korean adversaries. Many incidents detected featured newly observed or recently updated malware. CrowdStrike Intelligence continues to find evidence of a robust development cycle supporting Russian adversaries FANCY BEAR and VENOMOUS BEAR. China-based adversaries continue to use CVE-2017-11882, but have also incorporated CVE-2018-0802 into their operations within the last month. In addition, CrowdStrike Intelligence published three targeted intrusion actor profiles in January 2018—OCEAN BUFFALO, QUILTED TIGER, and RICOCHET CHOLLIMA.

eCrime

Incidents of *Samas* ransomware appeared to increase in January 2018. As further evidence that the ransomware market continues to be strong, new malware families *GandCrab* and *Rapid Ransomware* have been observed. Ransomware is one of many methods criminal adversaries have used to acquire cryptocurrency; however, in January 2018, eCrime threats continued to seek other avenues of cryptocurrency revenue generation. These tactics include deploying mineware and incorporating Bitcoin-stealing code into existing malware families. In January 2018, CrowdStrike Intelligence published three actor profiles to assist in the tracking and reporting of established botnet threats *Sality* (SALTY SPIDER) and *Cutwail*, versions 1 and 2 (TIDAL SPIDER and NARWHAL SPIDER, respectively).

Hacktivism

Pro-Russia hacktivist front Fancy Bears' International Hack Team (FBIHT) took aim at international sports organizations ahead of the 2018 XXIII Winter Olympics; this activity was largely expected after the International Olympic Committee (IOC) banned Russian athletes from participating under the Russian flag. Turkish hacktivist groups—both nationalist group Ayyildiz Tim and anti-government group CRIMSON JACKAL—were also active in January 2018.

TARGETED INTRUSION

January 2018 targeted intrusion activity shows several adversaries upgrading known tools and developing new Tactics, Techniques, and Procedures (TTPs). China-based adversaries continue to leverage new vulnerabilities as they are released, and possibly prior to public knowledge of them. CrowdStrike observed Russia-based adversaries VENOMOUS BEAR and FANCY BEAR continue to update their toolsets; North Korea and Iran-based adversaries conducted operations against Western targets and entities in Bahrain, respectively. Finally, with the occurrence of the 2018 Winter Olympics in South Korea, the chances for related cyber activity increase.

Olympics Venue Targeting

In January 2018, CrowdStrike Intelligence analyzed an unattributed spear phishing campaign targeting South Korean users in sectors likely providing support to the Olympic Winter Games, with 11.9 percent of spear phishing victims in the Olympic venue category.[1] This incident made heavy use of PowerShell scripts; in one sample, a PowerShell script downloads, likely from a compromised legitimate website, and reads an image file that was created using the open-source steganography tool *Invoke-PSImage*. This tool is used to embed additional scripts in the image. In this case, the PowerShell script, embedded in the image, is a heavily obfuscated loader that retrieves additional scripts. While attribution for this incident has not been confirmed, CrowdStrike has assessed that actors from China, the Democratic People's Republic of Korea (DPRK), and Russia may target the sporting event.

- Chinese adversaries have demonstrated interest in conducting operations against targets on the Korean peninsula and the Olympics may increase this interest as it will draw delegations from across the international community.
- DPRK adversaries consistently target South Korean interests. This interest may be enhanced with a high-profile event such as the Olympics, and the possibility exists for use of destructive tactics. However, the participation of North Korean athletes in the games may temper the use of cyber operations.
- In the case of Russia, CrowdStrike has previously observed credential harvesting activity against an entity with interests in the Olympics and attributed it to Russian adversary FANCY BEAR with medium confidence. Although that activity represents a separate incident, it serves to demonstrate Russian adversary interest in targeting sports organizations, following extensive reporting on state-wide doping scandals.

RUSSIA

CrowdStrike Intelligence continues to see tool development from Russia-based adversaries VENOMOUS BEAR and FANCY BEAR. Additionally, in January 2018, CrowdStrike Intelligence identified a new variant of the *PSCrypt* ransomware family, which infected networks in Ukraine via spam emails that contain weaponized Microsoft Word documents.[2] As part of a series of pseudo-ransomware attacks targeting Ukraine, a variant of PSCrypt was previously linked to Ukraine targeting in

[1] CSA-18015, *Malicious Spear Phishing Campaign Observed Targeting Entities Involved in the Upcoming XXIII Olympic Winter Games in South Korea*

[2] CSA-18037, *New Version of PSCrypt Identified Targeting Ukraine; Potentially Used For Destructive Purposes*

June 2017, days before the *NotPetya* wiper attack. CrowdStrike continues to investigate this incident, as well as other Ukraine-targeted crimeware campaigns. The motivation behind this activity is undetermined, but Russian adversaries have previously used crimeware in destructive attacks targeting Ukraine.

VENOMOUS BEAR Updates Neuron Implant

An updated version of *Neuron* was identified in early January 2018. Compile time stamps of this sample indicate a creation date of 28 November 2017, just five days after previous public reporting on Neuron.[3] This indicates that the actor actively monitors industry reporting and is able to quickly adapt to evade detection. While some basic functionality remains intact in this latest sample, large parts of the framework have been rewritten from scratch.

Neuron is an implant that enables tasking and data exfiltration by synchronizing a distributed storage pool of command scripts between infected machines. Operators may periodically connect to an infected system on the outer network boundary over the internet, upload new tasking, and retrieve results. This new variant of Neuron retains this functionality with the following changes:

- The file transfer and command protocols that were formerly handled separately have been merged into a single randomized command channel.
- The command-and-control (C2) protocol still uses key-value pairs for communication; however, the previously hard-coded names have been abandoned and replaced with randomized patterns.
- Previous Neuron versions used RC4 with a hard-coded key to encrypt C2 communications. This has been changed to AES, with two different keys for different functions.
- While command scripts are still used to distribute tasking, their instruction set has been drastically reduced from eight to four different instructions.
- An encrypted logfile that records executed commands, proxy requests, and other diagnostic data has been added.

FANCY BEAR Adopts Additional Toolset

Based on ongoing analysis into FANCY BEAR operations in late 2017, CrowdStrike Intelligence identified additional tools used by this adversary—*SveMse* downloader and *XmasDown* implant. Timestamps for the SveMse downloader samples are 2017-10-30 05:29:53 UTC and 2017-11-13 06:04:31 UTC, indicating possible use in late 2017. One of these files was downloaded by a version of the threat actor's *Zekapab* downloader, which was extracted from a malicious document, likely delivered via spear phishing.[4] The XmasDown implant is also likely delivered via a macro-enabled document dropper attached to a spear phishing email. This malware appears to have been in development since at least August 2016. In December 2016, it was used in an attack against multiple German think tanks that specialize in foreign policy issues.[5]

[3] CSA-18060, *VENOMOUS BEAR Updates Neuron Implant*
[4] CSA-18004, *SnvMse Downloader Tool Identified; Attributed to FANCY BEAR*
[5] CSA-18056, *New FANCY BEAR Implant Discovered*

CHINA

CrowdStrike Intelligence continues to investigate Chinese adversary use of vulnerabilities and the possibility that in some cases, China-based actors have early access to exploits. CrowdStrike Intelligence has recently reported instances in which China's Ministry of State Security (MSS) likely leveraged its domestic clout to harvest high-threat vulnerabilities from Chinese private-sector companies conducting research in intrusion operations. Separately, the MSS has been known to source non-domestic tools and databases from underground marketplaces under commercial cover.

Chinese Adversaries Adopt CVE-2018-0802

On 9 January 2018, CVE-2018-0802 was publicly identified, and like CVE-2017-11882, suspected China-based adversaries have adopted this exploit into their operations. While both CVE-2017-11882 and CVE-2018-0802 manipulate similar flaws in the Microsoft Equation Editor, only the latter allows attackers to leverage Object Linking and Embedding (OLE) package objects. CrowdStrike reported this technique in CSA-17140 as a variation of CVE-2017-11882 activity. However, it is probable that this activity was in fact a zero-day exploitation of CVE-2018-0802. CrowdStrike Intelligence has observed evidence that Chinese adversaries are using a shared exploit builder tool. Listed below are some notable CVE-2018-0802 campaigns linked to suspected China-based adversaries:

- CrowdStrike Intelligence observed a new campaign possibly targeting activist groups or non-governmental organizations (NGOs) that are associated with Tibetan independence causes. Utilizing weaponized Microsoft Word and PowerPoint documents, incidents associated with these campaigns used exploits both CVE-2017-11882 and CVE-2018-0802.[6]
- CrowdStrike Intelligence also observed CVE-2018-0802 delivering an obfuscated version of *Syndicasec*, an implant that was previously used by China-based adversaries in the 2014-2015 timeframe. Decoy content for these incidents were related to Indian government.[7]

The targeting in these incidents—based on observed lure themes or content—demonstrate an interest in regional affairs. The recent rise of Tibetan themes in Chinese spear phishing is notable amid numerous crackdowns targeting Buddhist sites in Tibet. In late January, Chinese officials also recalled Tibetan pilgrims who were participating in a month-long series of spiritual teachings in India. Although the campaign may target Tibetan dissidents themselves, in some cases China may target foreign governments who receive the Dalai Lama, the exiled Buddhist leader.

[6] CSA-18045, *Tibetan Activism Themed Intrusion Activity Using Exploit Code for Newly Identified Vulnerability CVE-2018-0802*
[7] CSWR-18001, *GTAC Weekly Wrap-Up: Week of 1/13/2018*

OTHER ADVERSARY ACTIVITY

CrowdStrike Intelligence has released three new actor profiles, describing ongoing activity from targeted intrusion adversaries.

ADVERSARY	OVERVIEW	RECENT ACTIVITY
OCEAN BUFFALO (aka OceanLotus, APT32)	OCEAN BUFFALO is a Vietnam-based targeted intrusion adversary reportedly active since 2012. The actor's toolset is highly variable and their TTPs are constantly evolving, which can pose a challenge to network defenders.	In late-December 2017, open-source information emerged detailing new phishing activity reportedly leveraged documents bearing a "curriculum vitae" (CV) theme, which were used to retrieve and load malicious scripts.
QUILTED TIGER (aka Patchwork)	Active since at least mid-2016, QUILTED TIGER focuses a significant part of its activity in Pakistan and China, but has exhibited interest in Western targets as well. The actor favors open-source tools but uses custom C2 protocols, including a dead-drop resolver (DDR) system for enhanced operational security.	In early January 2018, CrowdStrike Intelligence observed this adversary adopt CVE-2017-11882 for the first time. After a multi-stage infection process, the final payload was a newly observed implant.[8]
RICOCHET CHOLLIMA (aka ScarCruft)	RICOCHET CHOLLIMA operations have included spear phishing operations leveraging malicious Hangul Word Processor (HWP) documents to drop custom implants. This adversary appears to focus on government sector targets, as well as dissident and human rights organizations.	In January 2018, a malicious Hangul Word Processor (HWP) document was linked to this adversary. The Korean-language document was used to deliver a fileless executable that uses cloud services as C2.[9]

Table 1. New Targeted Intrusion Actor Profiles Released—January 2018

North Korea: LABYRINTH CHOLLIMA

January 2018 saw the DPRK-based adversary LABYRINTH CHOLLIMA continue their "Job"-themed spear phishing campaigns, which began in mid-2017. CrowdStrike Intelligence identified a spear phishing message targeting the financial sector. This incident leveraged English-language lure content and the malware *HtDnLoader*. English-language lures in this campaign have historically been used with variants of LABYRINTH CHOLLIMA's *Hawup* malware, while the HtDnLoader malware has been historically used with Korean-language financial and Bitcoin-theme lures. Interestingly, in late November 2017, US-CERT

[8] CSA-18007, *QUILTED TIGER Adopts CVE-2017-11882 in a Japanese Government Themed Campaign*
[9] CSA-18019, *Newly Observed Implant Leverages Cloud Services for C2 Channel, Possible Link to ScarCruft Adversary*

released reporting and campaign indicators on LABYRINTH CHOLLIMA (also known as HIDDEN COBRA) and its use of the *FALLCHILL* malware, which appears to be a subset of the Hawup. The identification of HtDnLoader in this recent effort instead of Hawup is a possible indication that LABYRINTH CHOLLIMA is attempting to increase obfuscation efforts in reaction to public disclosure, particularly against English-speaking targets.

Iran: HELIX KITTEN

In early January 2018, CrowdStrike Intelligence identified a malicious Microsoft Compiled HTML Help (CHM) file linked to HELIX KITTEN. The identified file is structured similarly to previously identified CHM files linked to HELIX KITTEN. However, this file has implemented Base64-encoding of portions of the resource containing the malicious code, whereas previously identified CHM files did not use any encoding. The file name used for the CHM file was translated as "Minutes of a meeting on the Kingdom of Bahrain." Notably, relations between Sunni-run Bahrain and Iran have been strained, particularly since late last year when a pipeline explosion resulted in the arrest of dozens of individuals. Officials in Bahrain have publicly stated the accused were Shi'a dissidents trained in Iran by the Islamic Revolutionary Guard Corps (IRGC).

OUTLOOK FOR TARGETED INTRUSIONS

In February 2018, CrowdStrike Intelligence continues to observe and report on unattributed activity targeting Winter Olympics venues. The most recent activity consists of attempted destructive attack using a previously unknown wiper malware. Analysis into this incident is ongoing.

Russia

The discoveries of new tools in use by Russia-based adversaries are possibly part of a larger strategy to diversify tools. CrowdStrike Intelligence observed constant additions and updates to the tool chain maintained by FANCY BEAR throughout 2017, and uncovered evidence that VENOMOUS BEAR has continued to develop TTPs to support a steady operational pace. This activity is expected to continue in the new year.

China

CrowdStrike Intelligence expects China-based adversaries to continue the use of CVE-2018-0802, likely using this vulnerability in operations that previously used CVE-2017-11882. Although China-based activity has historically shown a decline around the Lunar New Year (scheduled for 16 February), some high-priority operations will likely continue.

North Korea

Activity from January 2018 suggests DPRK-based adversaries are intent on continuing campaigns that began in 2017. Additionally, recent reporting on RICOCHET CHOLLIMA suggests this adversary is behind the use of a Flash zero-day CVE-2018-4878, which was observed in early February 2018.

ECRIME

In January 2018, operators of criminal campaigns continue to pursue the acquisition of various cryptocurrencies, including Bitcoin, Monero, and Dash. Several crimeware campaigns were launched or reinvigorated in the new year. New ransomware families, *GandCrab*[10] and *Rapid Ransomware*, have been detected in the wild, and the operators of *Samas* ransomware have demonstrated an increased operational pace. CrowdStrike Intelligence also observed a rise in instances of *Formbook*, an information stealer. To facilitate the tracking of established botnets, CrowdStrike Intelligence has published actor profiles for *Sality* (SALTY SPIDER) and *Cutwail* (TIDAL SPIDER and NARWHAL SPIDER).

INCREASING INSTANCES OF FORMBOOK

eCrime Actors Combine Use of Formbook with Other Information Stealers

In January 2018, CrowdStrike Intelligence observed an increase in the rate of distribution for the *Formbook* information stealer. Since the release of the latest version—version 3.8—in mid-December 2017, a significant number of variants are now in operation, with distribution campaigns being observed daily.[11] Campaigns distributing Formbook vary in regards to the phishing themes and infection chains used, but through supplementary analysis it was identified that many of the actors operating this malware combine the use of Formbook with other information stealers, particularly *LokiBot* and *Pony*.

CrowdStrike Intelligence did not observe any major changes to the malware code with the release of version 3.8.[12] The builder for Formbook has been leaked; however, it remains unclear if other criminal actors have managed to obtain the full source code. Version 3.8 appeared shortly after the regular seller of Formbook stopped the sale of the tool in the beginning of December, declaring he never intended it to be used for malicious purposes. Two hypotheses for these mixed messages include:

- The usual seller is still selling Formbook, but privately; the withdrawal messages on forums may be a ruse to evade law enforcement.
- A new developer of Formbook has obtained the source code and is now releasing new versions.

Formbook is an information stealer and form grabber criminal tool that has been advertised in underground criminal forums since early 2016. Capabilities of Formbook also include keystroke logging, stealing clipboard contents, and extracting data from HTTP sessions. The malware can be used to execute commands from a command-and-control (C2) server, such as downloading and executing malware, starting processes, and rebooting the victim machine. The developers of Formbook are currently offering two operating models: one where the criminal user gets access to a shared server, and a "pro" version where the criminal user can deploy their own panel for data collection and other capabilities.

[10] CSA-18082, *GandCrab Ransomware Hits Criminal Market; First to Use the DASH Cryptocurrency for Ransom Payment*
[11] CSA-18071, *Marked Increase in Formbook Malware Campaigns; Diversity in Distribution Themes Observed*
[12] CSA-18011, *New Version of Formbook Malware; Possible New Developer*

ADVERSARY SPOTLIGHT

TIDAL SPIDER & NARWHAL SPIDER

In January 2018, CrowdStrike Intelligence published the actor profiles for the operators behind the spam botnet *Cutwail*, an established botnet that has survived several takedown operations. This spam engine first came on the criminal market in 2007. Following a separation of the original developers, there are now two versions of Cutwail, run by separate adversaries—TIDAL SPIDER and NARWHAL SPIDER.

TIDAL SPIDER is the criminal adversary who develops and operates Cutwail version 1. This version retained many similarities from the flagship version, including using the same network encryption key and request format. NARWHAL SPIDER operates Cutwail version 2, which was developed with string obfuscation, a slightly different request format, and a new encryption key. Cutwail, version 2, was observed in January 2018 supporting a *Panda Zeus* campaign. NARWHAL SPIDER appears to have a large customer base, including operators of banking Trojan malware.

TIDAL SPIDER	NARWHAL SPIDER
Campaigns: • Mostly used for Russian-language spam, mostly for advertisements • Money mule recruitment • Distribution of *TrickBot* (operated by WIZARD SPIDER)	**Campaigns:** • Although also used for spam and advertisements, in 2017, mostly delivered malware • Customers include established banking Trojan operators, such as affiliates of WIZARD SPIDER and BAMBOO SPIDER • Distribution of *Pony*, *Gozi ISFB*, *URLZone*, *Nymaim*, *Chthonic*, and *ZLoader*

Table 2. TIDAL SPIDER vs. NARWHAL SPIDER

RECENT REPORTING ON CUTWAIL

CSIT-18013 Malware Analysis of the Cutwail Spam Botnet

CSIT-18019 Cutwail Persists as a Distribution Method for eCrime Campaigns

SUSTAINED ECRIME INTEREST IN ACQUIRING CRYPTOCURRENCY

In December 2017, interest in Bitcoin increased so dramatically that the valuation in USD briefly hit $20,000. Since then, Bitcoin steadily lost value over the course of January, ending the month at just over $10,000 USD. The volatility and investor interest in this cryptocurrency has prompted several national governments to take steps toward regulating the use of cryptocurrency and Bitcoin in particular. CrowdStrike Intelligence has assessed that cyber criminals may switch to alternative cryptocurrencies if the use of Bitcoin proves to become too cumbersome and unprofitable.

The growth in Monero mining, among other incidents observed this month, may herald more diverse cryptocurrency use among eCrime actors. Still, established eCrime threats continue to use Bitcoin as a method of payment for ransom operations (e.g., data ransom, ransomware), or to engineer ways to steal Bitcoin from other cryptocurrency users, as was most recently observed from SALTY SPIDER this month. Additionally, the actors behind the development of the GandCrab ransomware are requesting ransom payment using the cryptocurrency called DASH, which was introduced to the cryptocurrency market in January 2014. Interestingly, in line with peaking interest in cryptocurrency, the value of DASH also increased during the last 12 months, a staggering increase in value of 9275%.

Monero Mineware Observed Across Multiple Sectors

Monero mineware continues to proliferate in the new year, particularly the open-source miner *XMRig*. CrowdStrike OverWatch has detected numerous incidents of XMRig being deployed to compromised hosts. Due to the open-source nature of this tool,[13] these campaigns are likely the result of several actors operating separate campaigns.

In mid-January, CrowdStrike OverWatch began identifying malicious PowerShell scripts deployed via vulnerable versions of the Kaseya Virtual System Administrator (VSA) software; these scripts were used to download and install XMRig.[14] On 29 January 2018, Kaseya notified users of the security vulnerability in the VSA product, released patches, and confirmed that this vulnerability was used to deploy Monero miners on some clients.

CrowdStrike OverWatch also detected activity from an unknown criminal actor installing XMRig with other crimeware, including *RDP Patch*.[15] The RDP Patch tool is offered by the xDedic criminal marketplace to facilitate the compromise of RDP servers; access to these servers is then offered for sale to be used in activities such as spam email, or as a VPN endpoint. Deploying XMRig with RDP Patch is likely intended to increase overall revenue for this criminal actor, as the compromised server can mine Monero when not being used by a downstream customer.

CrowdStrike Intelligence has also identified instances of XMRig being modified or improved. In one case, the unidentified actor modified XMRig mining script to add persistence and self-protection techniques:

- Killing other mining processes to ensure that CPU usage is not exhausted and highlighted on the victim machine.
- Checking running processes on the victim machine and reducing CPU usage by keeping mining activity to a minimum.

This actor used *Quant Loader* to enable the distribution of his custom mineware, further emphasizing the myriad of methods these adversaries have to spread their miners. CrowdStrike Intelligence has also previously observed WIZARD SPIDER use XMRig for the development and introduction of a Monero mining module,[16] which is downloaded by the Trickbot malware onto infected victim machines. It is clear

[13] Available on GitHub: *https://github.com/xmrig/xmrig*
[14] CSA-18066, *XMRig Monero CPU Miner Delivered Via Compromised Kaseya Virtual System Administrator Software*
[15] CSA-18072, *Monero Cryptocurrency Miner Used in Conjunction with xDedic RDP Tool*
[16] CSA-17223, *WIZARD SPIDER Introduces Monero Cryptocurrency Mining Module*

that XMRig is a diverse tool that is used by both novice and sophisticated eCrime actors to sustain or increase criminal revenue.

SALTY SPIDER Targets Bitcoin Users

In early January 2018, CrowdStrike Intelligence identified the *Sality* peer-to-peer (P2P) botnet, version 4, distributing two executables designed to target Bitcoin users.[17] The first tool scans victim machines for the presence of directories associated with Electrum Bitcoin Wallets and exfiltrates all files in these directories. The second file queries the clipboard of the targeted machine for strings that match the format of Bitcoin addresses.

This month, CrowdStrike Intelligence named the adversary behind the Sality botnet as SALTY SPIDER. Currently, there are two Sality botnets—version 3 and version 4—which co-exist as separate botnets with bot populations of approximately equal sizes in the six-figure range. All secondary payloads, including these Bitcoin stealer files, carry similarities to the Sality malware, indicating they were developed by SALTY SPIDER.

Although initial payouts to SALTY SPIDER-associated Bitcoin wallets were paltry, the adversary received several high value amounts late in January 2018. The total accumulated profit was over $50,000 USD at time of transaction (although this value has decreased somewhat with the falling price of Bitcoin).

SALTY SPIDER	
Attribution	Group likely operating in Russia
Functionality of Sality	• Centralized P2P network • Digitally signed payloads • Polymorphic file infector • Credential brute forcing • ETERNALBLUE/SMB spreader
Secondary Payloads	• SOCKS proxy malware • Spambot known as *Pramro* • Bitcoin stealers • DDoS malware • Credential stealing/bruteforcing tools

Table 3. SALTY SPIDER Actor Profile Quick Facts

[17] CSA-18008, *Sality Peer-to-Peer Botnet Propagates Bitcoin-Stealing Malware*

BOTNETS INVOLVED IN CRYPTOCURRENCY REVENUE GENERATION

According to industry researchers, other botnets have been linked to cryptocurrency revenue generation operations. A new variant of the Satori botnet, labeled Satori.Coin.Robber, was identified on 8 January 2018, following the take-down of the previous Satori version in December 2017. This variant reportedly targets Ethereum (ETH) mining systems, replacing the original miner's credentials with the attacker's.

The CraP2P spam botnet, operated by MONTY SPIDER, has been used to advertise an obscure cryptocurrency called Swisscoin, which is arguably not a cryptocurrency at all, just a pyramid scheme. Regardless, this campaign is a sign that cryptocurrency—or cryptocurrency-like operations—remain lucrative.

Source: CSA-18043, *Multiple Botnets Targeting Cryptocurrency Users*

RANSOMWARE

CrowdStrike Intelligence has identified several new ransomware operations in January 2018. The operators of Samas ransomware have reinvigorated their operations, largely by targeting organizations in the healthcare sector, a previous and well established target of Samas campaigns. Additionally, new malware families have entered the eCrime ecosystem; these include *Rapid Ransomware*, which appeared late in December 2017, and *GandCrab*, which was observed in late January.

Rapid Ransomware

Rapid Ransomware does not appear to present a particularly new type of ransomware threat. However, it does not have a known cryptographic weakness; therefore, encrypted files may be unrecoverable without prior backups. A Bitcoin wallet associated with this campaign has received payments

GandCrab

Distributed by RIG and GrandSoft exploit kits, GandCrab is notable because it is one of the first ransomware families to accept DASH cryptocurrency for a method of payment and to utilize the cryptocurrency Namecoin top-level domain (TLD) `.bit`.

Samas Operational Tempo Increases

Multiple *Samas* ransomware campaigns were reported in January 2018. Victims in early January included Hancock Health and Adams Memorial hospitals in Indiana, and the city of Farmington, New Mexico. A different variant of the ransomware was used in an attack on AllScripts, an electronic health record provider.

The actors behind Samas use targeted eCrime TTPs and often request high ransoms. From BTC addresses identified by CrowdStrike Intelligence associated with Samas, the criminal actor netted around $500,000 USD in December 2017 and around $200,000 USD in January 2018 (based on actual BTC value at time of payment). The actors often gain a foothold within a company's network by exploiting externally-facing infrastructure, then elevate their privileges until they can access a sufficient

number of hosts. Once the network is compromised, they deploy ransomware to the most impactful areas of a network, targeting key servers and systems to limit the operations of an organization, likely increasing the pressure on infected organizations to pay the ransom.

In the attack on Hancock Health, this adversary reportedly targeted the hospital via the hospital's remote access portal and used stolen third-party vendor credentials to gain access. This incident underscores the continued threat of compromise through a third-party's authorized access, which may remain, even after the company's internal security may attempt to protect the networks from future attacks through various methods.[18]

OUTLOOK FOR ECRIME

CrowdStrike Intelligence continues to identify new samples of CARBON SPIDER implants *Sekur* and *Bateleur*. Analysis on the target scope for these campaigns is ongoing, although in 2017 this adversary focused on targeting the hospitality and food & beverage sectors. CrowdStrike also continues to investigate the various groups operating within the overarching organization behind CARBON SPIDER activity.

The healthcare sector remains vulnerable to data ransom and data breaches due to the sensitive nature of the data these organizations possess. In January 2018, the U.S. Department of Health and Human Services released a cybersecurity newsletter highlighting the rise of data extortion attacks and encouraging organizations in this sector to take robust and overlapping measures in protecting user data.[19] Data breaches in the healthcare sector can lead to fines, loss of business, and interrupted operations. The Samas infection that affected AllScripts resulted in a class action lawsuit, filed last week in the U.S. District Court for the Northern District of Illinois, demonstrating yet another possible consequence to lapses in data security.

This trend was also noted in recent media reports regarding a July 2017 *BitPaymer* ransomware infection that affected the UK National Health Service. CrowdStrike Intelligence has subsequently confirmed that this ransomware was developed by INDRIK SPIDER, the adversary behind *Dridex* banking Trojan, suggesting this actor group may be diversifying their means of acquiring criminal revenue. Considering previous evidence of eCrime operators adopting mineware and other

[18] CSA-18042, *Samas Ransomware Infection of Indiana Hospital; Infection Delivered Via Compromised Third-Party Credentials*
[19] https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-january-2018.pdf

HACKTIVISM

The most notable hacktivist activity in January 2018 includes the return of Fancy Bears' International Hack Team (FBIHT) after a five month hiatus. Turkey-based hacktivist groups were also active in the new year. CRIMSON JACKAL (or *Red Hack*) had previously been inactive operationally for much of 2017, although their social media accounts regularly posted rhetoric espousing the group's ideology.

REGIONAL HIGHLIGHT: TURKEY

Turkey-based hacktivist activity in January 2018 was notable due to the different ideologies expressed by the groups conduction operations. Turkish hacktivist groups like *Turk Hack* Team, *Aslan Nefer Tim*, and *Ayyildiz Tim*, espouse nationalist rhetoric. At the same time, some hardline policies have motivated *Anonymous*-styled campaigns from activists critical of the Turkish government.

IDEOLOGY	Nationalist, Pro-Turkey	Socialist, Anti-Government
ACTOR GROUP	Ayyildiz Tim	CRIMSON JACKAL
JANUARY 2018 ACTIVITY	Compromised the social media accounts of two Fox News commenters[20]	Defaced the website of the Turkish Interior Ministry, a TTP used in the past in response to allegations of corruption in Turkish government[21]
CONTEXT	U.S. opposes Turkey's operations against Kurds along the Turkey-Syria border.	Turkey's interior Minster Süleyman SOYLU is fighting multiple allegations of abuse of power.

Table 4. Turkish Hacktivism—Summary of January 2018 Activity

FBIHT

Pro-Russia Hacktivist Front Group Takes Aim at International Sporting Community

On 10 January 2018, after a nearly five-month hiatus, FBIHT resurfaced with claims of Olympic-themed data leaks under a new post titled "WADA vs. IOC: Fight for Clean Sport or Fight for Power?". Activity from Russian adversaries or pro-Russia hacktivists was anticipated after the IOC suspended the Russian Olympic Committee's participation in the 2018 Winter Olympics. FBIHT followed this initial post with two others in January 2018, as noted in the table below.

[20] CSA-18040, *Turkish Nationalist Hacktivists Compromise U.S. Media Personality Accounts; Subsequent Posts Suggest Possibility of Forthcoming Leaks*

[21] CSA-18012, *CRIMSON JACKAL Defaces Turkish Interior Ministry Website Amid Controversy Surrounding Interior Minister*

DATE OF ACTIVITY	TARGET ORGANIZATION(s)	NARRATIVE
10 January	IOC, World Anti-Doping Agency (WADA)	Claims there is discord between IOC and WADA, as well as European and North American sporting organizations
24 January	International Luge Federation	Accuses the organization of violating principles of fair play, citing widespread use of therapeutic-use exemptions and missed anti-doping tests[22]
31 January	Canadian Olympic Committee	Accuses Canadian sporting sector of corruption and misdeeds over doping allegations[23]

Table 5. Summary of FBIHT January 2018 Activity

CrowdStrike Intelligence assesses that FBIHT plays an active role in Russian information operations (IO) against sports organizations with the goal of redeeming the international perception of Russia as a sports nation through hacking-enabled discreditation campaigns against other athletes and organizations.

OUTLOOK FOR HACKTIVIST ACTIVITY

CrowdStrike Intelligence continued to see FBIHT in early February, as the Olympic Games kicked off. On 1 February 2018, the Court of Arbitration for Sport overturned the ruling that 13 Russian athletes should be banned from the Olympics. However, these athletes continued to wait for an invitation to participate, and others had their appeals postponed. As such, additional FBIHT activity will likely continue during the Winter Games.

As Turkey-U.S. relations continue to be tense, pro-Turkey hacktivist groups may launch additional campaigns against high-profile U.S.-based organizations, likely focusing on opportunistic attacks. These groups claim to support the Turkish government, although it remains unclear whether a direct relationship exists. Until last month, CRIMSON JACKAL remained relatively inactive operationally, with its last significant activity occurring in September 2016. However, throughout 2017, social media accounts related to this actor group published rhetoric opposing the Turkish government. The activity in January 2018 may be a prelude to more operations from this adversary.

In addition to the incidents reported above, CrowdStrike Intelligence continues to see activity from MENA-based groups, supporting various sides in the ongoing tensions among members of the Gulf Cooperation Council (GCC). This activity is highly likely to continue in the near-term, and may persist throughout 2018 should compromise continue to be elusive, particularly between Qatar and Saudi Arabia.

[22] CSA-18061, *Hacktivist Front Fancy Bears' International Hack Team Continues Information Operations against the 2018 Winter Olympic Games by Claiming Data Leak from the International Luge Federation*
[23] CSWR-18003, *GTAC Weekly Wrap-Up: Week of 1/27/2018*

APPENDIX

The following tables provide a summary of recent observed activity and/or updates to named adversary profiles.

Targeted Intrusion Adversaries

ADVERSARY	RECENT TARGETING		UPDATES, TTPs, and OBSERVED ACTIVITY
	by Region	by Sector	
FANCY BEAR	N/A	N/A	• SvnMse downloader identified • XmasDown implant identified
HELIX KITTEN	*Possibly* Bahrain	*Suspected* Government	• Bahrain-themed decoy • Malicious CHM files • New implant, known as *IntelSecurityManager*, identified
OCEAN BUFFALO	N/A	N/A	Actor profile created for adversary publicly known as OceanLotus and APT32
QUILTED TIGER	*Suspected* Japan	*Suspected* Government	Use of CVE-2017-11882
RICOCHET CHOLLIMA	South Korea	N/A	• Actor profile created for adversary publicly known as "ScarCruft" • Updated *Cirrus* implant detected • Possible use of Flash zero-day and implant called *ROKRAT* • Uses cloud service provider PCloud for C2
VENOMOUS BEAR	N/A	N/A	Update to *Neuron* implant detected

Table 6. Summary of Targeted Intrusion Adversary Updates—January 2018

eCrime Adversaries

ADVERSARY	RECENT TARGETING		UPDATES, TTPs, and OBSERVED ACTIVITY
	by Region	by Sector	
BAMBOO SPIDER	North America	Financial, Retail, Travel	Latest version released 2.6.1
CARBON SPIDER	N/A	N/A	New samples of *Sekur* and *Bateleur* implants observed
COBALT SPIDER	Russia	Financial	Continued use of spear phishing, *Cobalt Strike*, and CVE-2017-11882
GURU SPIDER	N/A	N/A	• Release of major version 1.6 of *Quant Loader* • Observed instance of Quant Loader downloading mineware
MONTY SPIDER	N/A	N/A	*CraP2P* observed spreading advertising for Swisscoin
NARWHAL SPIDER	Global	Individuals	Actor profile created for operators of spam botnet *Cutwail* (v2)
SALTY SPIDER	Global	Financial, Technology	• Actor profile created for operators/ developers of *Sality* • Sality version 4 propagating Bitcoin-stealing malware
SKELETON SPIDER	U.S.	Retail	• Actor profile created • *FrameworkPOS* activity observed in December 2017, as reported in CSMR-17012
TIDAL SPIDER	Global	Individuals	Actor profile created for operators of spam botnet *Cutwail* (v1)
WIZARD SPIDER	N/A	Financial	Observed overlap with *BokBot*

Table 7. Summary of eCrime Adversary Updates—January 2018