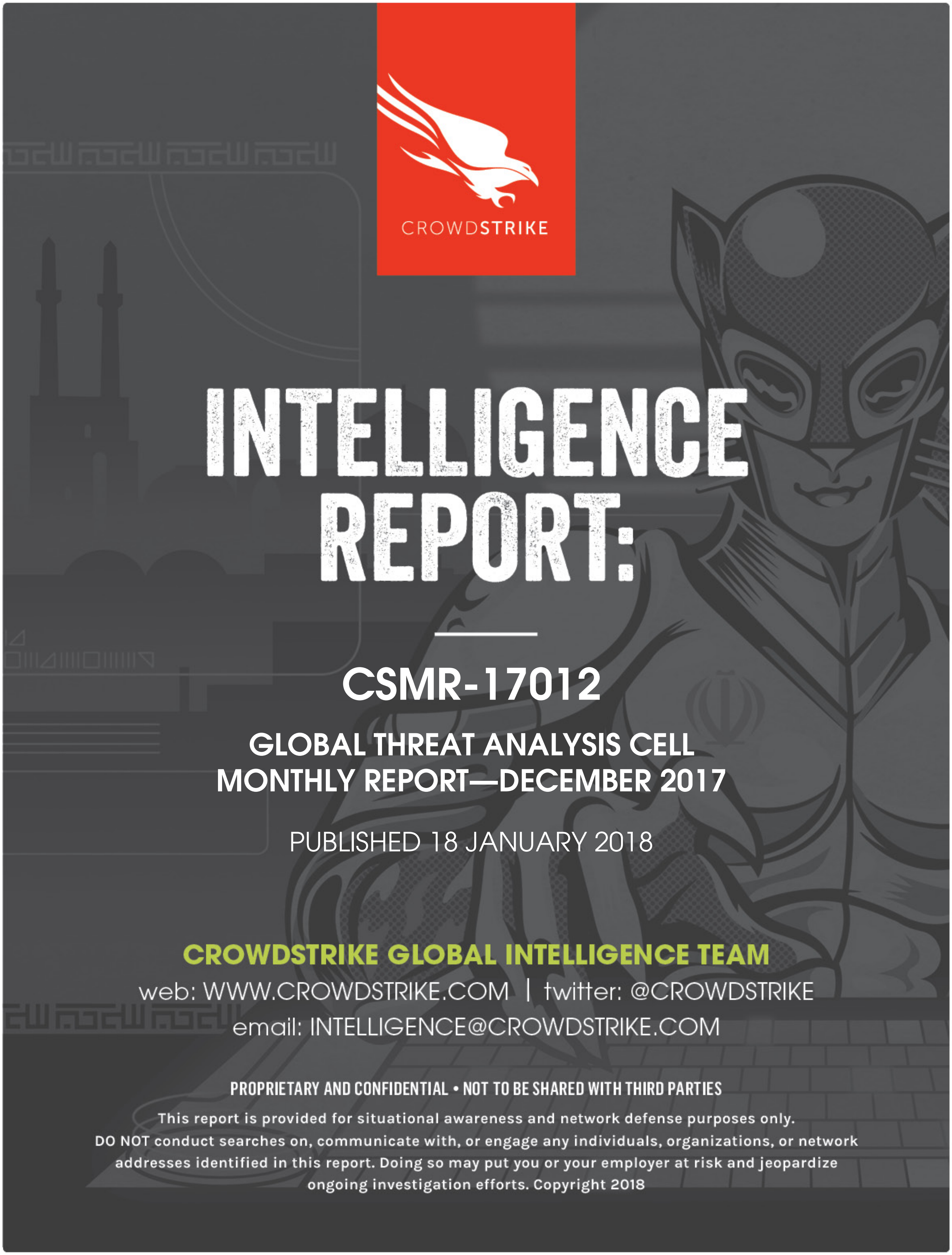


CROWDSTRIKE

INTELLIGENCE REPORT:

CSMR-17012

GLOBAL THREAT ANALYSIS CELL MONTHLY REPORT—DECEMBER 2017

PUBLISHED 18 JANUARY 2018

CROWDSTRIKE GLOBAL INTELLIGENCE TEAM

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

PROPRIETARY AND CONFIDENTIAL • NOT TO BE SHARED WITH THIRD PARTIES

This report is provided for situational awareness and network defense purposes only. DO NOT conduct searches on, communicate with, or engage any individuals, organizations, or network addresses identified in this report. Doing so may put you or your employer at risk and jeopardize ongoing investigation efforts. Copyright 2018

EXECUTIVE SUMMARY

Targeted Intrusion

Targeted intrusion incidents observed in December 2017 included activity from Russian, Chinese, and North Korean adversaries. In many respects, these operations appear to be part of ongoing initiatives that were observed throughout the year. North Korean actors, for example, continued the resume and finance themed spear phishing campaigns that began in Summer 2017. Russia-based adversary FANCY BEAR targeted Belarus, continuing a pattern of targeting the Eastern Europe government sector. This actor also used a NATO-themed lure, another common practice observed throughout the latter half of 2017. Finally, suspected Chinese actors launched multiple, separate campaigns using Tactics, Techniques, and Procedures (TTPs) previously observed within the calendar year. These campaigns targeted a variety of regions, including Vietnam, Russia, U.S., Japan, and possibly Hong Kong.

eCrime

In December 2017, CrowdStrike Intelligence observed several overlaps between various criminal enterprises, as both malware loaders and spambot distribution services continue to find customers among operators of ransomware families and banking Trojans. However, a law enforcement operation, called Operation Bakovia, may have some effect on HOUND SPIDER and the distribution of *Cerber* ransomware in the near future; affiliates of this adversary were arrested in Romania. CrowdStrike continues to observe updates to loader and banking Trojan malware families, as developers vie to remain competitive and maximize their profits.

Hacktivism

In December 2017, CrowdStrike Intelligence observed an increase in activity from the *Anonymous* collective, fueled by recent U.S. policy decisions regarding Israel and Net Neutrality. After several months of inactivity, the pro-Russia group Beregini Female Hackers Team targeted Ukraine media entities. The pro-Saudi hacktivist group Saudi Electronic Army claimed two defacement campaigns in December; this group arose following tension between Saudi Arabia and the Gulf Cooperation Council (GCC) in Summer 2017.

TARGETED INTRUSION

CrowdStrike Intelligence observed several targeted intrusion incidents from both Russian and Chinese adversaries. Russian activity has been attributed to FANCY BEAR based on the tools used and the target scope. Incidents attributed to Chinese actors showed similarities to campaigns observed earlier in 2017. One such repeat operation appears to be a DEEP PANDA-linked campaign targeting the U.S. legal services sector. An adversary based in the Democratic People's Republic of Korea (DPRK) has continued to use *Manuscrypt* malware to likely target entities in the finance sector of the Republic of Korea (RoK). This operation also shows similarities to what has previously been observed from LABYRINTH CHOLLIMA, although definitive attribution has not been confirmed.

RUSSIA

In previous years, December has been a time of increased activity for Russian adversaries. Observed incidents in 2015 and 2016 included the use of wiper malware targeting Ukraine; however, no destructive activity was observed in December 2017. The adversary behind the previous wiper incidents—VOODOO BEAR—may have changed TTPs, as there is some overlap between this adversary and the disruptive, pseudo-ransomware attacks, *NotPetya* and *BadRabbit*, observed earlier in the year. Therefore, it is possible that persistent operations throughout the year have replaced the annual wiping attacks.

Adversary: FANCY BEAR
Target: Europe & NATO

Identified FANCY BEAR incidents in December 2017 were in line with this adversary's target scope—North Atlantic Treaty Organization (NATO) and European government sector:

NATO-THEMED	EASTERN EUROPE
On 6 December, CrowdStrike Intelligence discovered a document created on 18 September 2017, which contains malicious macro code. When opened, the document displays a schedule for the 15th anniversary of the Joint Analysis and Lessons Learned Centre (JALLC), a NATO entity that organizes training and exercises. The victim profile suggests that this attack is part of ongoing campaigns targeting NATO and NATO-adjacent organizations.[1]	On 22 December, FANCY BEAR spear phishing activity targeted the Belarusian Ministry of Defense, delivering a "Merry Christmas"-themed decoy which deploys an instance of *Zekapab* malware.[2] The email content included a message purporting to come from the United Nations' Secretariat of the Human Rights Council. Although Belarus is seen as a Soviet hold-out and friendly with Russia, cyber operations are likely one of many capabilities used to ensure Moscow maintains control over Belarus's sovereignty.

[1] CSA-17386, *Suspected FANCY BEAR Campaign Targeting NATO Leverages Malicious Macros and PowerShell Scripts*

[2] CSA-17414, *FANCY BEAR Spear Phish Activity Targets Belarusian Ministry of Defense*

Adversary: VENOMOUS BEAR
TTP: New Dropper for Snake Malware

On 12 December 2017, CrowdStrike Intelligence identified a new dropper for *Snake*, an implant uniquely attributed to VENOMOUS BEAR.[3] Although there was no information regarding targeting or command-and-control (C2) infrastructure, the compile time for this sample (2017-12-12 10:30 UTC) suggests this adversary has recently been active. Throughout 2017, CrowdStrike Intelligence examined evidence of VENOMOUS BEAR re-tooling efforts, with technical analysis suggesting that this adversary has a larger and more diverse toolset than was previously observed. A summary of these tool updates is provided in Table 1 below.

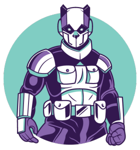
MALWARE	NOTABLE ACTIVITY
KopiLuwak	*KopiLuwak* is a JavaScript-based, first-stage implant with persistence features that are likely used to profile and select victims for the delivery of advanced payloads. Initial industry reporting on this tool appeared in February 2017, with another KopiLuwak instance observed in October.
MacOS X variant of Snake	A Trojanized MacOS X installer was identified in May 2017. The installer contained a variant of Snake. At the time, CrowdStrike Intelligence assessed that the MacOS variant of Snake was still in development.
Neuron	As reported in November 2017, this malware was deployed via malicious macro documents, notably against Middle Eastern targets.
Nautilus	This implant is designed to run on systems running web services. Public reporting on this tool was released in November 2017.

Table 1. VENOMOUS BEAR Tooling Reported Throughout 2017

Rise in Russian Internet Surveillance

Russia continues to show signs of increasing internet surveillance and tightening control over news and social media sites. Between 12 and 13 December 2017, internet communications associated with some U.S. and international social media, technology, communications, gaming, and cloud storage providers were temporarily rerouted to likely Russian communications providers, leveraging a technique known as Border Gateway Protocol (BGP) hijacking. CrowdStrike Intelligence assesses that the cases of BGP hijacking reveal a potential risk for traffic monitoring and capture by the Russian government, which maintains a vast system of domestic tools for monitoring. One such tool—GosSOPKA—is designed to detect and eliminate cyber threats, but also likely gives the Russian government greater visibility into activity on domestic networks. On 22 December 2017, Russian President Vladimir PUTIN signed a decree ordering improvements to GosSOPKA. This decree grants the Federal Security Service (FSB) authoritative control over GosSOPKA and codifies goals associated with this system. The present order underscores the FSB mandate to protect information security and encryption systems, including those which have been developed via supercomputing and grid computing.

[3] CSA-17413, *New Dropper for VENOMOUS BEAR Snake Malware Identified*



CHINA

CrowdStrike Intelligence observed several China-based operations in December 2017. Following the rapid assimilation of CVE-2017-11882 into China-based intrusion operations in late November 2017, CrowdStrike Intelligence observed a new implementation of this vulnerability by a suspected Chinese adversary.[4] This actor used CVE-2017-11882 exploit documents containing Package objects that are written directly to disk. This differs from previously observed CVE-2017-1182 documents that retrieve malicious code from remote servers. Other December activity, both attributed and unattributed, show similarities to incidents observed previously in 2017.

MALWARE	TARGET REGION	TARGET SECTOR	ATTRIBUTION	PREVIOUS ACTIVITY
RedLeaves	Japan	Defense	*Possible* STONE PANDA	Early 2017 activity using *RedLeaves* and targeting Japan was reported as the "CloudHopper" campaign.
ZeroT	Russia	*Unknown*	HAMMER PANDA	In August, infrastructure previously associated with HAMMER PANDA and *ZeroT* malware was used to target a Russian nuclear organization.
ARCHY variant	*Possibly* Hong Kong	NGOs	*Unknown*	The December incident used a theme referencing a Hong Kong human rights organization. Activity in Spring 2017 used an *ARCHY* variant known as *ChilArchy* and targeted Hong Kong-based targets.
Enfal	Vietnam	Government	*Unknown*	The *Enfal* downloader was previously observed targeting Vietnam in May 2017.
Empire PowerShell	U.S.	Legal Services	*Suspected* DEEP PANDA	TTPs of the activity observed in December 2017 were previously seen in June. The June campaign also targeted the legal sector, but used *Cobalt Strike* malware.

Table 2. Summary of China-Based Campaign—December 2017

U.S. Targeting Focused on Legal Sector

As noted in Table 2 above, China-based incidents targeting the U.S. focused on the legal services sector. This activity used spear phishing emails with themes related to current controversial issues involving Hillary CLINTON and U.S. Senate candidate Roy MOORE.[5] These emails contain malicious Microsoft Word attachments that retrieve second-stage payloads from malicious infrastructure. Although

[4] CSA-17410, *New Implementation of CVE-2017-11882 Writes and Executes Malware Directly on Victim Machine; Links to Previous Targeted Intrusion Activity*

[5] CSA-17388, *Recent Targeting of U.S. Legal Sector Appears Related to Law Firm-Focused DEEP PANDA Activity From June*

CrowdStrike was unable to retrieve the second stage, third-party information indicates that it is a copy of the publicly available post-exploitation framework known as *Empire PowerShell*.

The TTPs for this activity are similar to those observed in a June 2017 campaign also targeting the U.S. legal sector, which CrowdStrike Intelligence linked to DEEP PANDA. Similarities include:

- Use of malicious, macro-enable documents to deliver publicly available malware (in recent activity payload was Empire PowerShell and in June payload was *Cobalt Strike*)
- Use of actor-controlled infrastructure to send spear-phish emails
- Both waves of activity made use of current event themes
- Associated infrastructure uses similar naming convention

Law firms may be subject to cyber operations because of the intellectual property and sensitive corporate information they protect on behalf of their clients. An adversary interested in obtaining information on a company or a specific merger, may be successful against outside council, circumventing protections otherwise in place for privileged client-attorney communications. In some cases, law firms may be easier targets than the clients they represent, and the compromise of law firm servers may offer a foothold for follow-on operations targeting those clients.

NORTH KOREA

On 18 December 2017, the U.S. government directly attributed the creation and distribution of *WannaCry* ransomware to North Korea. This official announcement followed months of open-source articles stating that U.S. and UK intelligence agencies had attributed the attack, and reaffirms the assessment made by CrowdStrike Intelligence shortly after the attack. As published in mid-May 2017, technical overlaps between WannaCry and DPRK-based malware strongly suggested that North Korea was behind the operation.[6]

No additional ransomware campaigns have been linked to DPRK in the latter half of 2017. However, DPRK adversaries have used spear phishing to target finance and cryptocurrency entities, suggesting that the regime's interest in alternative methods of raising income has not waned. As part of efforts to directly compromise cryptocurrency exchanges, North Korea is suspected of being behind attacks on Youbit, a major Korean cryptocurrency exchange. On 19 December, Youbit announced that it is filing for bankruptcy as a result of these compromises, the most recent of which resulted in a loss of nearly a fifth of its clients' holdings.

In December 2017, CrowdStrike Intelligence identified another Hangul Word Processor (HWP) document delivering *Manuscrypt* malware.[7] This campaign, which uses Korean-language filenames, has been ongoing since at least October 2017. The resume and finance themes are similar to those used by LABYRINTH CHOLLIMA in a campaign that began in July and uses the implant *Hawup*. Activity associated with this Hawup campaign was last observed on 28 November, when three resume-themed HWP

[6] See CSA-17124, CSA-17127, CSA-17130, and CSMR-17005

[7] CSWR-17049, *GTAC Weekly Wrap-Up: Week of 12/16/17*

documents were identified.[8] In addition to the common theme, both campaigns use an Encapsulated PostScript (EPS)-based exploit to weaponize the malicious HWP files. These operations suggest DPRK actors maintain an interest in compromising the finance sector in the RoK.

OUTLOOK FOR TARGETED INTRUSIONS

In January 2018, CrowdStrike Intelligence observed unattributed activity targeting South Korea, and specifically Winter Olympics venues. The PyeongChang Winter Olympic Games will be held from 9 to 25 February 2018. CrowdStrike Intelligence has assessed that adversaries linked to Russia or the DPRK may target the event. In December 2017, the IOC banned the Russian national team from officially competing under their own flag at the PyeongChang Olympics after reports of state-sponsored doping. In response, Russian adversaries may attempt to target Olympic-related organizations, anti-doping regulators, or individual athletes. Recent reporting has suggested that North Korea will send a delegation to the event; however, DPRK adversaries may still take advantage of the surge of visitors to the Korean Peninsula and launch cyber operations designed to raise revenue for the regime.

Russia

CrowdStrike Intelligence expects activity supporting Russian foreign intelligence operations will continue in the new year. Evidence suggests that VENOMOUS BEAR has consistently developed new tools and improvements to existing implants. Although the details of how and where these tools are used is not always clear, the constant development suggests this adversary remains active. Domestic targeting may also increase ahead of the March 2018 presidential election. In addition to censorship, the Putin administration may leverage Russian adversaries to launch specific disinformation campaigns or targeted intrusions.

China

CrowdStrike Intelligence expects China-based adversaries to use CVE-2017-11882 in the early part of 2018, particularly against sectors and regions where campaigns incorporating this exploit have already been successful. 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. The use of publicly available malware, as was seen in the suspected DEEP PANDA targeting of the U.S. legal sector, increased in 2017. CrowdStrike Intelligence has assessed that this trend will also continue in 2018, as adversaries look for ways to undermine security vendor attribution efforts.

[8] CSA-17369, *Newly Identified LABYRINTH CHOLLIMA Activity Suggests Continued Campaign Targeting South Korea Bitcoin Entities*

ECRIME

Developers of established banking Trojans, including WIZARD SPIDER and BAMBOO SPIDER, closed out 2017 with updates and version releases. Both adversaries have been prolific in 2017, with WIZARD SPIDER scaling quickly beginning in Spring 2017 and BAMBOO SPIDER increasing the pace of development in September 2017. CrowdStrike Intelligence also analyzed an update to the banking Trojan malware *QakBot*, which incorporated a PowerShell script containing a variant of *Mimikatz*.

In December 2017, CrowdStrike Intelligence reported on two legal actions taken against cybercriminal operations. Operation Bakovia, described below, resulted in the arrest of ransomware operators. On 12 December, a court decision led to the sentencing of a UK national named Jinal PETHAD who opened bank accounts under false identities to assist in laundering funds stolen using the *Dridex* malware, developed and operated by the eCrime adversary INDRIK SPIDER. CrowdStrike continues to monitor the effects of the law enforcement takedown of Andromeda, observing some evidence that eCrime threats have begun to retool. In one case, operators behind the malware *Lethic* have switched to using the loader functionality of *Neutrino Bot* after the Andromeda takedown.

As the eCrime market for malware loader and spam services continues to be strong, CrowdStrike Intelligence has noted several overlapping criminal enterprises, demonstrated in Figure 1 below. This snapshot is not inclusive of all activity, but a sample observed and reported by CrowdStrike Intelligence.

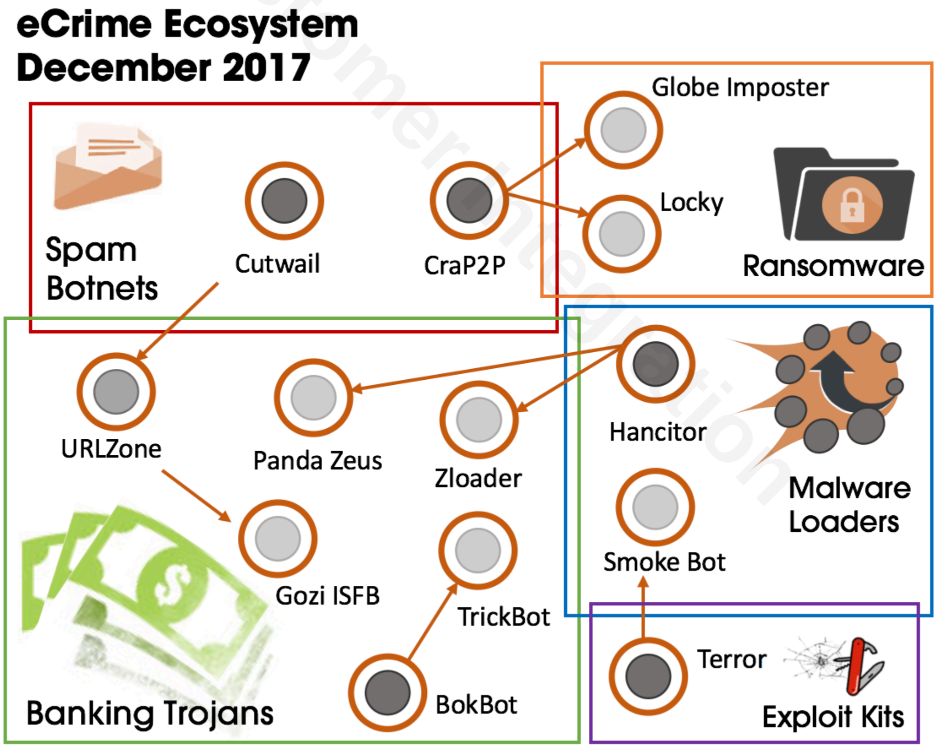
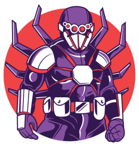


Figure 1. A Snapshot of Overlapping Criminal Operations—December 2017



ADVERSARY SPOTLIGHT: SKELETON SPIDER

In December 2017, CrowdStrike Intelligence provided support for an active incident response engagement involving malware known as *FrameworkPoS*. First reported in CSIT-14078, this malware has been used for stealing credit card track data from Point-of-Sale(PoS) devices. During CrowdStrike Intelligence's investigation into this activity, three additional tools were identified related to this version of FrameworkPoS. The first was a copy of the public tool `timestomp.exe`,[9] which can be used to modify when a file was created, modified, and last written. The second tool was identified as a DLL version of FrameworkPoS, and the third tool was a Windows Portable Executable, which acts as a dropper for FrameworkPoS.

FrameworkPoS is probably exclusively used by an actor tracked by CrowdStrike as SKELETON SPIDER, also known publicly as FIN6. Based on the actor's use of code-signing certificates from a Moscow based company, language artifacts in malware samples, and the use of Russian domain registrars, it is assessed with medium confidence that this actor is based out of Russia.

SKELETON SPIDER	
Suspected Russian-speaking criminal group	**Technical Tradecraft:** • Use of file logging and encoded DNS requests for data exfiltration • Deployment of time stamp modification tools • Use of XOR and substitution cipher for encoding data • Use of C2 infrastructure named after content-delivery-network providers • Customized malware per target designed to blend in with legitimate processes
Regional Target: U.S.	
Sector Target: Hospitality, Retail	

Table 3. SKELETON SPIDER Actor Profile Quick Facts

RECENT REPORTING ON SKELETON SPIDER

CSIT-18008 Version of FrameworkPoS Targeting Retail Sector

RANSOMWARE

HOUND SPIDER Affiliates Arrest May Lead to a Temporary Decrease in Cerber Distribution

On 20 December 2017, a EuroPol press release revealed that an international law enforcement operation—*Operation Bakovia*—has led to the arrest of five individuals for their involvement in the distribution of *CTB-Locker* (CTB meaning Curve-Tor-Bitcoin) and *Cerber* ransomware.[10] During searches

[9] https://www.jonrajewski.com/resources/

[10] CSA-17407, *Operation Bakovia Results in Arrests for Distribution of CTB-Locker and Cerber Ransomware Families*

of the individuals homes, police were able to seize a significant amount of equipment, likely used to support the criminal operation, including a large number of hard drives, external storage, laptops, cryptocurrency mining devices, numerous documents, and hundreds of SIM cards.

CTB-Locker (aka *Critroni*) came onto the criminal scene in 2014 and was one of the first ransomware variants to use Tor to hide its command-and-control (C2) infrastructure. Its underlying code was based on the infamous ransomware strain *CryptoLocker*, campaigns of which were highly successful until its demise following a law enforcement operation in June 2014 (Operation Tovar).

CrowdStrike Intelligence tracks the developer of Cerber ransomware as HOUND SPIDER. Alongside *Locky*, Cerber ransomware has been one of the most prolific ransomware families on the eCrime market since 2016, based on the rate of distribution throughout the last two years. HOUND SPIDER offers Cerber ransomware under an affiliate program, known as Ransomware-as-a-service (RaaS). It is believed that the payment made to HOUND SPIDER for the use of the malware is 30 percent of the profit made from successful ransom payments. Based on the information currently available, these arrests are solely for a criminal group of affiliates of HOUND SPIDER and do not relate to any arrest of HOUND SPIDER.

CrowdStrike Intelligence noted a recent reduction in spam emails distributing Cerber ransomware. This decline is likely to continue, as affiliates take time to assess their risk of arrest following Operation Bakovia. It is also expected that HOUND SPIDER, as the Cerber developer, will take a step back for a short period of time and review their operational security (OPSEC) posture. Information relating to HOUND SPIDER may be available on the equipment seized in this operation.

Additional Ransomware Incidents

Despite this law enforcement operation and short-term decline in Cerber distribution, ransomware operations will continue to affect entities of varying sizes—individuals, small businesses, and large organizations. Throughout 2017, CrowdStrike Intelligence has reported on ransomware attacks targeting government entities, particularly at the local (i.e., county and state) level. Such attacks can leave residents facing delays in receiving basic services, as was demonstrated by a *LockCrypt* attack against Mecklenburg County in North Carolina, where the attacker encrypted servers affecting email, printing, and other county applications.[11]

RANSOMWARE	NOTABLE ACTIVITY
Globe Imposter	CrowdStrike observed this ransomware being delivered by the *CraP2P* spambot, which is operated by MONTY SPIDER.
StorageCrypt	A StorageCrypt campaign targeted Network Attached Storage (NAS) devices by exploiting the *SambaCry* vulnerability in Linux.
LockCrypt	Mecklenburg County, NC servers were targeted by *LockCrypt*. This attack demonstrates how crippling ransomware can be to local government, as officials stated that restoring the county's computer system would take weeks.

[11] CSWR-17047, *GTAC Weekly Wrap-Up: Week of 12/2/17*

Hidden Tear	This open-source ransomware was used in a campaign that appeared to target Vietnam's Ministry of Justice.

Table 4. Recent Ransomware Incidents

LOADER MARKET

In November 2017, CrowdStrike Intelligence reported on regular updates to, and new releases of, *Quant Loader*, a malware loader developed by GURU SPIDER. CrowdStrike Intelligence continued to see the use of Quant in eCrime campaigns; a new variant using version 1.53 (released in November) was observed on 9 December and linked to *DiamondFox* operations by mid-December. As detailed in the table below, several established actors have continued to develop and sell their malware, and new threats appear to be ready to acquire a portion of market share.

MALWARE	NOTABLE ACTIVITY
Hancitor (aka Chanitor)	This loader has been observed supporting *Panda Zeus* and *Zloader* campaigns. Hancitor has been on the criminal market since 2013, but there has been a resurgence of activity from this malware since late 2016.
Quant Loader	GURU SPIDER released the latest version, v.1.54+, on 11 December. Shortly thereafter, the actor also launched a promotion on the latest version, reducing all purchase options by fifty percent for a period of two weeks. A variant using version 1.53 was observed downloading the multi-purpose *DiamondFox* malware on 14 December 2017.
Smoke Loader	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.
Godzilla Loader	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.
ARS VBS	In mid-December 2017, a known Russian eCrime threat actor introduced *ARS VBS*. According to CrowdStrike Intelligence sensitive sources, it sold numerous copies in just over five days, and has received numerous positive reviews from satisfied customers.

Table 5. Loader Market Updates

BANKING TROJANS

TrickBot—WIZARD SPIDER

WIZARD SPIDER reached their centenary numbered version in early December, then released regular updates through to the end of the month. Webinject URL patterns added recently focused on German and Swiss financial institutions. Specific German target revealed WIZARD SPIDER's understanding of the banking infrastructure for this country, as URL patterns incorporated vehicle lending and online banking for smaller, regional organizations.[12] CrowdStrike Intelligence observed an instance of TrickBot being distributed by *BokBot*, which has recently been reported by industry sources under the name *IceID*. This TrickBot affiliate continues to use group tags (`gtag`) prefixed with `mom`.

Panda Zeus—BAMBOO SPIDER

In mid-December, BAMBOO SPIDER released major version 2.6.0 of the *Panda Zeus* malware. The previous major version release, 2.5.0, occurred on 1 September 2017, with minor versions up to 2.5.7 being released thereafter.[13] Version 2.6.0 introduced new cryptography for the base configuration of the malware, initializing the RC4 Sbox with 30 rounds of encrypting null bytes before decrypting. To further inhibit analysis, the malware strings are also RC4-encrypted. CrowdStrike Intelligence initially observed Panda Zeus 2.6.0 being delivered by the *Cutwail* spam botnet in an Italian-language spam campaign, but more recent campaigns have included webinjects for North American financial institutions, suggesting the target scope across all affiliates is, and will be, much broader.

QakBot—Unnamed Adversary

CrowdStrike Intelligence continues to track new developments from the *QakBot* banking Trojan. The developers of QakBot introduced an update that downloads a PowerShell script that contains an embedded *Mimikatz* tool. This new development may have been influenced by high-profile campaigns, such as *NotPetya* and *BadRabbit*, which used SMB to spread, in part with credentials obtained through a custom tool based on Mimikatz. Similarly, QakBot was one of the first banking Trojans to feature a network spreader via SMB by using brute-force password guessing. By combining brute force password guessing with credentials extracted from memory using Mimikatz, QakBot increases the risk of spreading laterally across a local network.

Credential harvesting is a key technique for enabling lateral movement, and thus, Mimikatz has been incorporated into both financially motivated and espionage-driven operations. The use of this tool has been linked to eCrime adversaries CARBON SPIDER and COBALT SPIDER, but CrowdStrike Intelligence has not observed other banking Trojan malware families use this technique for propagating within a victim network. Interestingly, MUMMY SPIDER's *Emotet* malware delivery platform currently deploys a plugin that uses the exact same password dictionary used by QakBot to spread over SMB.

[12] Details of WIZARD SPIDER targeting are available in GTAC Weekly Reports CSWR-17047, CSWR-17048, and CSWR-17050.

[13] CSA-17400, *BAMBOO SPIDER Release New Major Version of Panda Zeus Malware*

ECRIME OUTLOOK

BAMBOO SPIDER's release of 2.5.0 in September 2017 marked the beginning of a significant uptick in the pace of development from this actor. 2.6.0 will almost certainly lead to similar updates as BAMBOO SPIDER makes adjustments to the Panda Zeus malware in the new year. Version 2.6.1 of Panda Zeus has already been observed targeting major retailers.

Law enforcement organizations have been effective in targeting select segments of the eCrime ecosystem, as well as individual operators; thus, collaborative, international operations to takedown infrastructure that supports cyber crime will continue in 2018. Despite these successes, customers in all sectors are advised to remain vigilant, as an overall reduction in eCrime will continue to be elusive in the new year. The PETHAD money laundering case is likely one of many relationships that exist to support INDRIK SPIDER operations, specifically monetization efforts resulting from the Dridex banking Trojan. Other criminal enterprises that operate banking Trojans likely require similar money laundering efforts.

Law enforcement operations may only temporarily stem criminal activity, as operators assess their risks and possibly move to more private forums. Criminal affiliates of HOUND SPIDER will likely reinvigorate Cerber ransomware campaigns after reviewing their operational security (OPSEC) posture. In a report released by Google in July 2017, it was estimated that Cerber ransomware had resulted in $6.9m USD worth of ransom payments since its inception. Although this profit is spread across HOUND SPIDER affiliates, this could have yielded a profit of circa $2.07m USD for the developer. Despite the risk of arrest, the potential for future profits remain a draw for HOUND SPIDER, their affiliates, and other ransomware operators.

In the highly competitive loader market, ARS VBS has gained quick popularity, which suggests this product is at least of moderate quality. Likewise, during the months that Godzilla Loader was being sold in the underground marketplace, it was a popular strain of malware, owing to its effectiveness, frequent updates from the developer, and a highly useful admin panel. However, as noted above, there are several effective loaders available. The ability for ARS VBS and Godzilla to remain relevant will depend on the developers providing regular and relevant updates at a competitive price point.

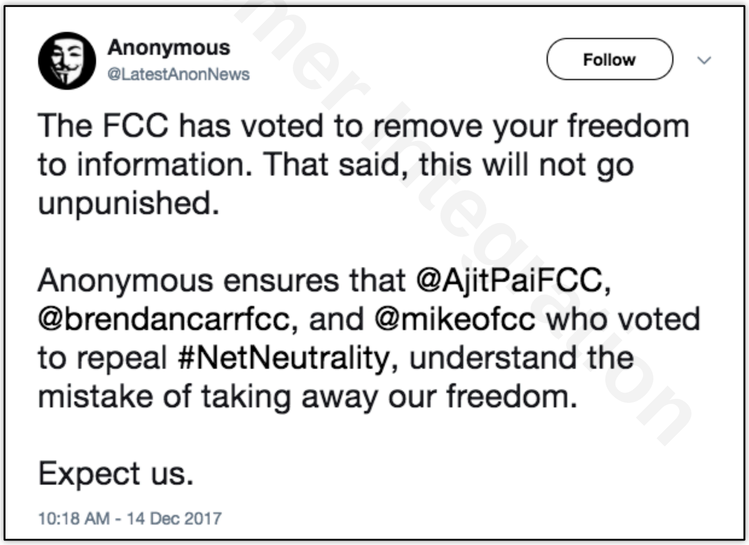
HACKTIVISM

Two policy announcements from the U.S. government—the recognition of Jerusalem as the capital of Israel and the repeal of Net Neutrality—prompted hacktivist activity and rhetoric in December 2017. Although the overall influence of the *Anonymous* collective appeared to decrease in 2017, these current events late in the year prompted small-scale organization efforts. December was also the anniversary of the 2016 destructive attacks against networks in Ukraine, which included activity from pro-Russia hacktivist groups. This year, the month came and went with no incident of that scale, although the pro-Russia group Beregini Female Hackers Team targeted the media sector in Ukraine after a five-month hiatus. CrowdStrike Intelligence also reported on defacement activity claimed by the Saudi Electronic Army, a pro-Saudi hacktivist group that has arisen in the latter half of the year.

ANONYMOUS

Hacktivists Condemn Net Neutrality Repeal

On 14 December 2017, the Federal Communications Commission (FCC) voted to repeal the protections commonly known as Net Neutrality, which has been a focal point for many online activist groups for years. Following the successful action to repeal Net Neutrality, social media accounts associated with Anonymous began to post threatening dialogue against the FCC and the three specific individuals they claim were responsible for the vote.[14]



Anonymous
@LatestAnonNews

The FCC has voted to remove your freedom to information. That said, this will not go unpunished.

Anonymous ensures that @AjitPaiFCC, @brendancarrfcc, and @mikeofcc who voted to repeal #NetNeutrality, understand the mistake of taking away our freedom.

Expect us.

10:18 AM - 14 Dec 2017

Figure 2. Anonymous Tweet Threatening Retaliation for Net Neutrality Repeal

Following through with the threats against the FCC Chairman Ajit PAI, Anonymous released what they purported to be PAI's personal information. The information disclosure (also known as a *dox*) was conducted by the Anonymous affiliated group, *Anonymous Intel Sec*, and posted under the hashtags

[14] CSWR-17048, *GTAC Weekly Wrap-Up: Week of 12/9/17*

#OpNetNeutrality and #OpDefendTheNet. According to industry sources, the information included street addresses, phone numbers, emails, and social media accounts for PAI, as well as the information of 42 family members and associates.[15]

The Anonymous collective claims to fight for personal liberties, and the freedom of the internet is one they hold especially close, as it is the medium in which they perform nearly all their activities. As such, Anonymous-associated groups will likely be outspoken against the Net Neutrality repeal as the issue faces a legislative battle in the new year.

Target: Jerusalem

On 6 December, the Trump administration recognized Jerusalem as the capital of Israel. In reaction to this announcement, on 7 December, hacktivists aligned with the *Anonymous* hacktivist collective in an attempt to launch reiterations of the operations known as #OpUSA and #OpIsrael in an effort to target U.S. and Israeli government assets.[16] Information for hacktivists seeking to join the effort was posted to a Pastebin site and included 15 targets for U.S. and Israeli government websites, defacement code, and instructions that directed "Data Dump, Government Breach, Defacing, DDoSing".

A number of hacktivist groups and actors—many with pro-Palestinian associations—expressed interest in supporting these operations. As part of this opposition, two incidents were claimed by the Palestinian group *Anonymous Arabe*—also referred to as "Anonymous International" in Arabic (الأنونيموس منظمة الدولية). On 15 December, Anonymous Arabe claimed responsibility for a compromise of the website of the United Nations Framework Convention on Climate Change, and for a Distributed Denial of Service (DDoS) attack against the website of the U.S. Department of State.[17] This group is an example of many regional groups that have modeled themselves after the larger Anonymous collective, but have adopted nationalist causes.

GEOPOLITICAL HACKTIVISM ADVERSARY HIGHLIGHTS

Pro-Russia Hacktivist Front Group

Beregini Female Hackers Team

In December 2017, the suspected pro-Russia hacktivist front group known as Beregini Female Hackers Team (@BereginiHackers) claimed to have compromised and defaced the Ukrainian news site Ukraine News (*ukraine-news[.]com*) with anti-Ukrainian language.[18] Their rhetoric specifically threatened Ukraine's 72nd Centre for Information and Psychological Operations, which has been criticized before by pro-Russia groups of creating anti-Russia propaganda.

In addition to this activity, the group claims to have created a database of "[translation] those who are involved in the annihilation of our Ukraine." The database includes personal information, such as private email addresses, phone numbers, and social media accounts for suspected Ukrainians. One of the entries links to Roman BURKO, a well-known anti-Russia journalist who runs the pro-Ukraine volunteer

[15] CSWR-17049, *GTAC Weekly Wrap-Up: Week of 12/16/17*
[16] CSWR-17047, *GTAC Weekly Wrap-Up: Week of 12/2/17*
[17] CSWR-17048, *GTAC Weekly Wrap-Up: Week of 12/9/17*
[18] CSWR-17049, *GTAC Weekly Wrap-Up: Week of 12/16/17*

media platform *InformNapalm*. It is currently unclear what Beregini plans to do with the database, but based on previous behavior, it is possible the entities listed will be targeted by the hacktivist group in the near future.

The Beregini group surfaced in September 2016, with early activity primarily focused on targeting InformNapalm, suggesting the group's creation was designed to counter pro-Ukrainian hacktivist efforts. The group gained notoriety in December 2016 for supporting *Sprut*, another pro-Russia hacktivist group (and suspected front group for state-sponsored adversaries), in the attacks against Ukraine energy provider Ukrenergo directly before the provider was hit by destructive attacks by a suspected Russian targeted intrusion adversary.[19] While Beregini's activity last month did not coincide with a larger attack against Ukrainian entities, the timing of this activity—on the anniversary of last year's destructive attacks—suggests the group aimed to have some kind of psychological effect. Previous 2017 activity from Beregini occurred in June and July. The June activity also featured the defacement of media websites and another apparent collaboration with Sprut.

Pro-Saudi Hacktivism

Saudi Electronic Army

On 25 December, pro-Saudi hacktivist group, Saudi Electronic Army (SEA), claimed responsibility for defacing the website of the Movement for Islamic Reform (للإصلاح الإسلامية لحركة), an organization headed by UK-based Saad Al-FAQIH, and which advocates for the overthrow of the Saudi government.[20] SEA also defaced a related website, Asrar Arabiya (اسرار عربية) ("Arab Secrets"), which frequently purports to leak sensitive information from Gulf Cooperation Council (GCC) governments, namely Saudi Arabia and the UAE.

The SEA was born out of the GCC dispute with Qatar that began in May 2017. Its members comprise both hacktivists and traditional activist actors, who prior to the group's formation, operated as part of a larger, relatively unorganized pro-Saudi activist scene. Tensions between Qatar and other GCC states—namely the United Arab Emirates (UAE) and Saudi Arabia—have not shown significant signs of de-escalation. At the same time, Saudi foreign policy, led by Crown Prince Mohammed bin SALMAN, has increasingly sought to more aggressively counter expanding Iranian influence in the region. These two factors have contributed to an increase in pro-Saudi online activism, and as a result, the formation of and rise in activity by SEA. The December 2017 defacements are part of ongoing operations by SEA in support of the Saudi government and in opposition to Iran, Hezbollah, and Qatar-aligned entities.

RECENT REPORTING ON SAUDI ELECTRONIC ARMY

CSIT-17194 Saudi Electronic Army Operations Target Organizations Perceived as Aligned with Iran; Include Public and Covert Activity

[19] CSA-16419, *Suspected Cyber Attacks Continue Against Ukraine's Critical Infrastructure; Likely Part of a Larger Coordinated Effort by Malicious Actors Targeting Ukraine Interests*

[20] CSWR-17050, *GTAC Weekly Wrap-Up: Week of 12/23/2017*

OUTLOOK FOR HACKTIVIST ACTIVITY

Throughout 2017, groups and actors aligned with the Anonymous collective were vocal about their lack of support for the current U.S. administration. In 2018, these individuals are likely to continue rhetoric and some hacktivist campaigns in protest to President Donald TRUMP's policies and initiatives. The Jerusalem announcement may continue to incite additional pro-Palestinian groups to expand their target scope.

The Saudi Electronic Army will likely continue to remain active as a reflection of developments in the Middle East. The scope of SEA's targeting could expand to private companies, as has been evidenced by the group's October 2017 aspirations to disrupt private firms it perceives as aligned with Iran and its Shi'a allies.

Like Russian targeted intrusion adversaries, pro-Russian hacktivist groups and suspected front (faketivism) groups may be active in January and early February 2018, prior to the 2018 Winter Olympic games.

APPENDIX

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

Targeted Intrusion Adversaries

ADVERSARY	TARGETING		UPDATES, TTPs, and OBSERVED ACTIVITY
	by Region	by Sector	
DEEP PANDA	U.S.	Legal Services	• Spear phishing • Macro-enabled documents to deliver Empire PowerShell
FANCY BEAR	Belarus, Europe (NATO)	Defense, Government, Military,	• Spear phishing • Macro-enabled Word documents delivering malware • Continues use of *Zekapab* • Use of next-stage PowerShell script • Use of a 256-bit prime number to encrypt C2 messages
HAMMER PANDA	Russia	N/A	*ZeroT* malware delivered by self-extracting archive (SFX)
QUILTED TIGER	U.S.	Think Tanks	This actor profile was recently created to track the actor group publicly known as "Patchwork."
VENOMOUS BEAR	N/A	N/A	New dropper for the *Snake* implant identified

Table 6. Summary of Targeted Intrusion Adversary Updates—December 2017

eCrime Adversaries

ADVERSARY	TARGETING		UPDATES, TTPs, and OBSERVED ACTIVITY
	by Region	by Sector	
BAMBOO SPIDER	Italy, U.S.	Financial, Retail	• Use of *Cutwail* spam botnet as a delivery vector • Release of major version 2.6.1
CARBON SPIDER	U.S.	Food & Beverage	New samples of *Sekur* implant observed

DUNGEON SPIDER	N/A	N/A	*Locky* ransomware continues to be distributed via *CraP2P*
GURU SPIDER	N/A	N/A	• Release of version 1.54+ of Quant Loader • Observed instance of Quant Loader downloading *DiamondFox* malware
HOUND SPIDER	N/A	N/A	Affiliates arrested
INDRIK SPIDER	N/A	N/A	A supporter of money laundering operations sentenced
MONTY SPIDER	N/A	N/A	*CraP2P* spam botnet was observed delivering *Globe Imposter* ransomware.
MUMMY SPIDER	N/A	N/A	• Use of invoicing-themed spam • Macro-enabled documents that run encoded PowerShell commands
WIZARD SPIDER	Canada, U.S., Germany, Switzerland	Financial	• Multiple new versions of TrickBot released • Expanded targeting • Use of “Revenue Agency” lure

Table 7. Summary of eCrime Adversary Updates—November 2017