Blueliv.

ANNUAL CYBERTHREAT LANDSCAPE REPORT

MARCH 2018

TABLE OF CONTENTS

Blueliv.

INTRODUCTION

00

2017: A GOOD YEAR?

There were massive data breaches making the news, more and more powerful threat actors on the scene, successful global ransomware attacks and huge disruption to commercial organizations, public infrastructure and governments around the world. So, if you are a cybercriminal, you might say it was your best year yet. Though the likes of Uber and Equifax won't be looking back at 2017 with particular fondness, it was also a good year for cybersecurity.

WHEN CYBERATTACKS MAKE THE HEADLINES, ORGANIZATIONS IMPROVE THEIR SECURITY POSTURE

When cyberattacks make headlines, other organizations in other industries start to take notice. And when other organizations take notice and start taking proactive steps to strengthen their security posture, that is good news for us all: the fight against cybercrime is a collaborative effort.

Guided by Threat Compass, the Blueliv's Annual Cyberthreat Landscape Report takes a birds-eye view of the major events and trends of last year. The Threat Intelligence analysts at Blueliv then offer their insight into an ever-more sophisticated cybercrime industry for 2018.

> The fight against cybercrime is a collaborative effort

PURPOSE OF THIS REPORT

- A reference document for some of the main cybercrime events of 2017, including intelligence on specific malware advances and threat actor profiles
- Analysis of high profile breaches and prevention techniques to improve your organization's resilience
- Guidance on how to combat attack techniques and bolster your security posture

Day by day, adversaries are getting smarter and coming up with innovative methods to threaten and penetrate organizations. Eliminating blind spots in the threat landscape using this report will enable organizations to protect themselves from the outside in.

> *There are only two safe predictions about cybersecurity in 2018: There will be more spectacular data breaches and the EU General Data Protection Regulation (GDPR) will go into effect on May 25. But as the continuing digital transformation of our lives entails the ongoing digital transformation of crime, vandalism and warfare, 2018 could also bring a lot of new takes on old vulnerabilities, some completely new types of cyberattacks, and successful new defenses.*
>
> ***Gil Press, Forbes, November 2017*** [1]

SUMMARY OVERVIEW

The timeline below illustrates some of the key incidents which defined the cybersecurity landscape in 2017. This is not exhaustive, simply due to the sheer volume of activity that took place.

Instead, we zoom in on some of what we judge to be the most important moments of the year. Most of these are covered in greater detail later in the report.

MALWARE ADVANCES

The sophistication of malware has continued to increase in 2017, with improved complexity, encryption and obfuscation techniques employed by cybercriminals. Stealth and lateral movement has become significantly more common. From attacks on companies of all sizes to stopping critical infrastructure in its tracks, we explore malware advances that made headlines, in addition to providing insight into new techniques used by adversaries.

HIGH PROFILE BREACHES

We take a look at major data breaches and their implications, for the companies themselves and the world at large. Internally, there is still a great need for training programs for all levels, with improvements required in IT security skills and opsec capabilities.

HIGH IMPACT ATTACK VECTORS

An explosion in the number of IoT devices in the past year (being used to perform DDoS attacks, for example) is just partly responsible for an uptick in vulnerabilities identified in 2017. We have also observed other stand-out attack techniques and offer guidance around what companies should be doing to protect themselves.

THREAT ACTOR PROFILES

Many new and dangerous threat actors emerged last year, including a number of state-sponsored actors who are, according to ENISA, "the most omnipresent malicious agents in cyberspace."[2] We profile some actors among them, examine successes so far and dangers they may pose in the future.

LAW ENFORCEMENT ACTIVITY

There were some spectacular takedowns in the past year, but the fight against cybercrime is never-ending. The timeline contains some key moments.

TIMELINE OF NOTABLE CYBERSECURITY INCIDENTS

2017

In the first half of the year, APT33 targets interests in the US, South Korea and Saudi Arabia, including commercial and military aviation companies and organizations in the energy sector

JANUARY

Cerber accounts for 1/4 of ransomware activity

FEBRUARY

New Zeus derivative Zloader detected

Windows Trojan designed to help hackers spread Mirai detected

MARCH

Laptops containing 3.7 million Hong Kong voters' data stolen after chief executive election

APRIL

Lazarus Group launches spear phishing campaign against US defense contractors

Peter Levashov a.k.a. Peter Severa, arrested. His Kelihos botnet infected 100,000 computers worldwide

Shadow Brokers leak a critical arsenal of major exploits called 'Lost in Translation'

MAY

EQUIFAX breached, affecting 143 million people

Peter Levashov a.k.a. Peter Severa, arrested. His Kelihos botnet infected 100,000 computers worldwide

JUNE

NotPetya appears, hitting organizations around the globe

APT28 targets multiple hospitality organizations, including hotels across Europe and the Middle East

Alphabay taken down by FBI. Meanwhile Europol coordinated a secret takeover of Hansa in June – a sting operation to log the massive influx of Alphabay refugees

JULY

New Emotet and Trickbot variants showed worm-like propagation techniques

AUGUST

HBO compromised, with attackers stealing unpublished material and threatening to release it illegally

SEPTEMBER

DELOITTE breach reported

A massive botnet called IoTroop or Reaper is detected. It recruits IoT devices in order to create an army of sleepers

OCTOBER

Bad Rabbit emerges, infecting computers through legitimate compromised websites

NOVEMBER

VERTICALSCOPE breach reported, with 2.7 million user accounts compromised

UBER discloses data breach from previous year

DECEMBER

NECURS variant makes a comeback

Sergey Jarets, a.k.a. Ar3s, arrested. He was responsible for the Andromeda botnet, which spanned over 2 million PCs and distributed over 80 types of malware

In the second half of the year, Lazarus Group carried out various campaigns targeting cryptocurrency

Law enforcement

Ransomware

Data leakage

Threat actor

Trojan banker

Malware

GLOBAL INCIDENT HIGHLIGHTS

93% of breaches could have been prevented (OTA)

$5 BILLION
Global Financial Impact of ransomware (CV)

159,700
total cyber incidents in 2017 (OTA)

18% increase in reported breach incidents (RBS)

$5.3 BILLION
in global BEC losses (FBI)

rise in business targeted ransomware (Symantec) **90%**

Worldwide estimates.
Sources: OTA (Online Trust Alliance); RBS (Risk Based Security); Cybersecurity Ventures (CV)
Source: CSIS

2017 SNAPSHOT

DETECTING COMPROMISED CREDENTIALS

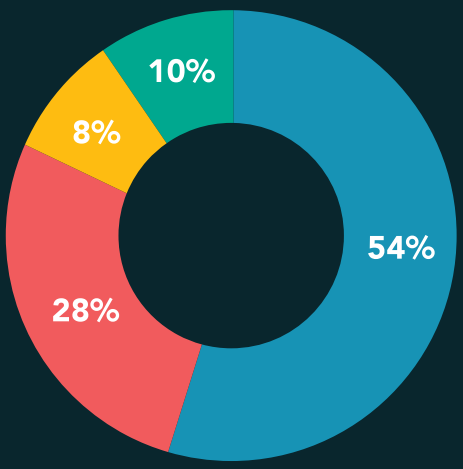
Almost

2 BILLION

exposed credentials detected by **Blueliv** in 2017

Industries highly impacted by credential theft

- Media, Social Networking & Advertising
- Gambling & Gaming
- Retail
- Technology and Telcos
- Banking and Financial Services
- Services & Consulting
- Insurance



PONY, AZORULT and HAWKEYE make up

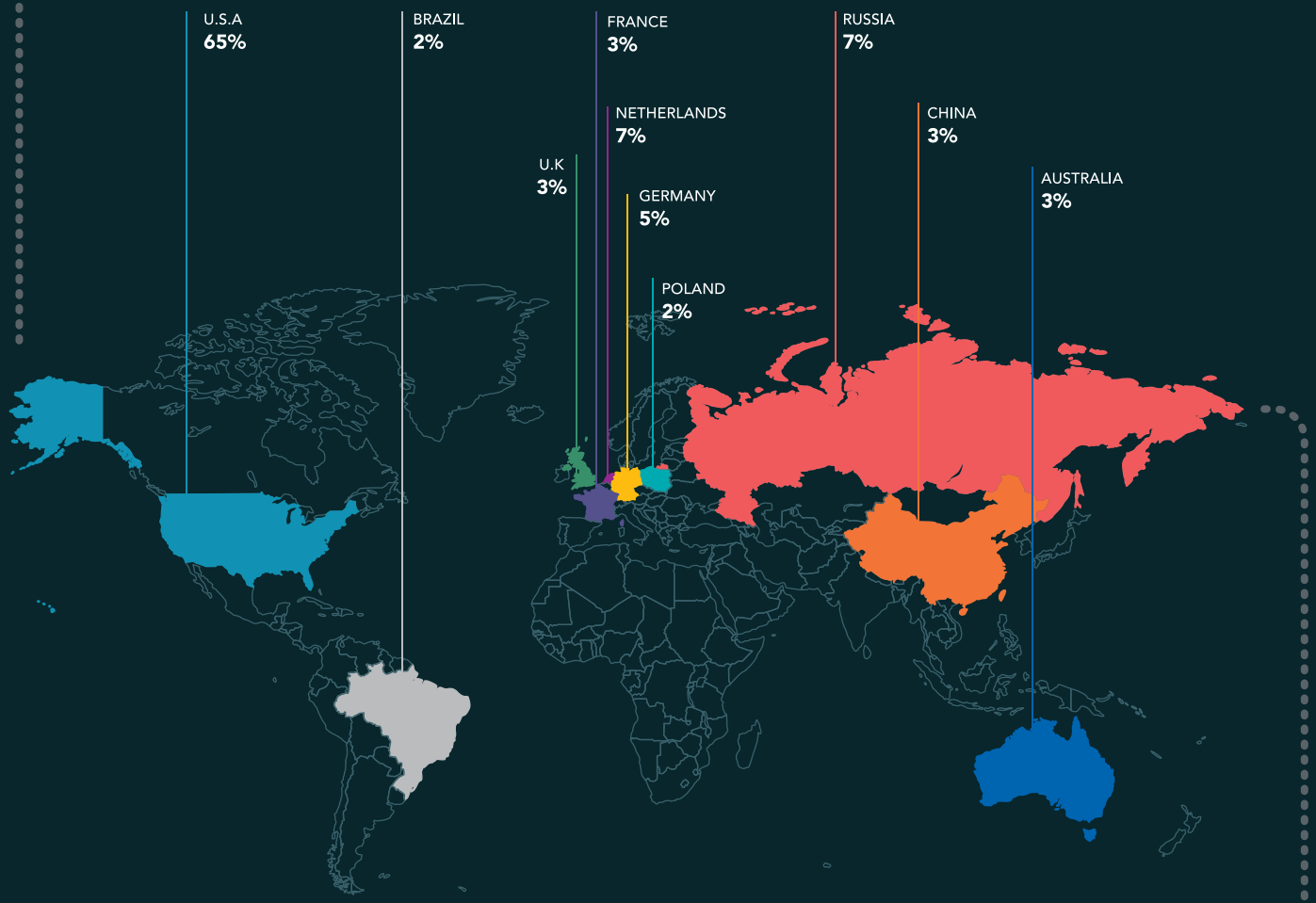
90% of all credential-stealing botnets analyzed in 2017

Pony Azorult Hawkeye Other

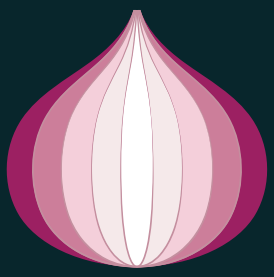
USA boasts the **MOST INFECTED USERS** by country

MONITORING CRIMESERVERS

We geolocated almost 2/3 of malicious crimeservers for phishing, C2 & exploit kits in the USA



These were picked up by our live cyberthreat map throughout the year



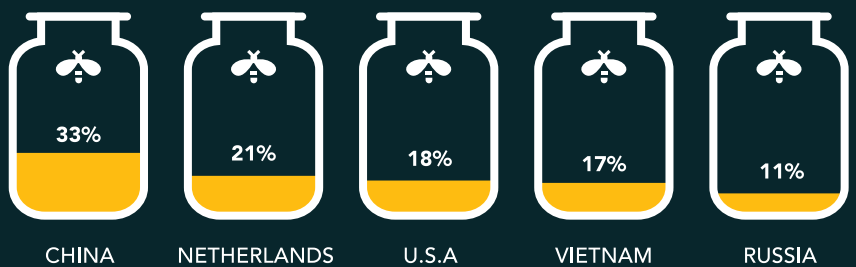
From 2016 - 2017

140%

increase in TOR domains used as crimeservers

PREVENTING ATTACKS

Unsurprisingly the greatest proportion of attacks on our honeypot infrastructure last year in China



CREDIT CARD FRAUD

We discovered

2 MILLION

stolen credit card details in 2017

Around **40%**
of these details come from
FOUR MAJOR BANKS within
the Fortune500 top 30

Lack of EMV makes it easier for the bad guys to copy data using PoS malware

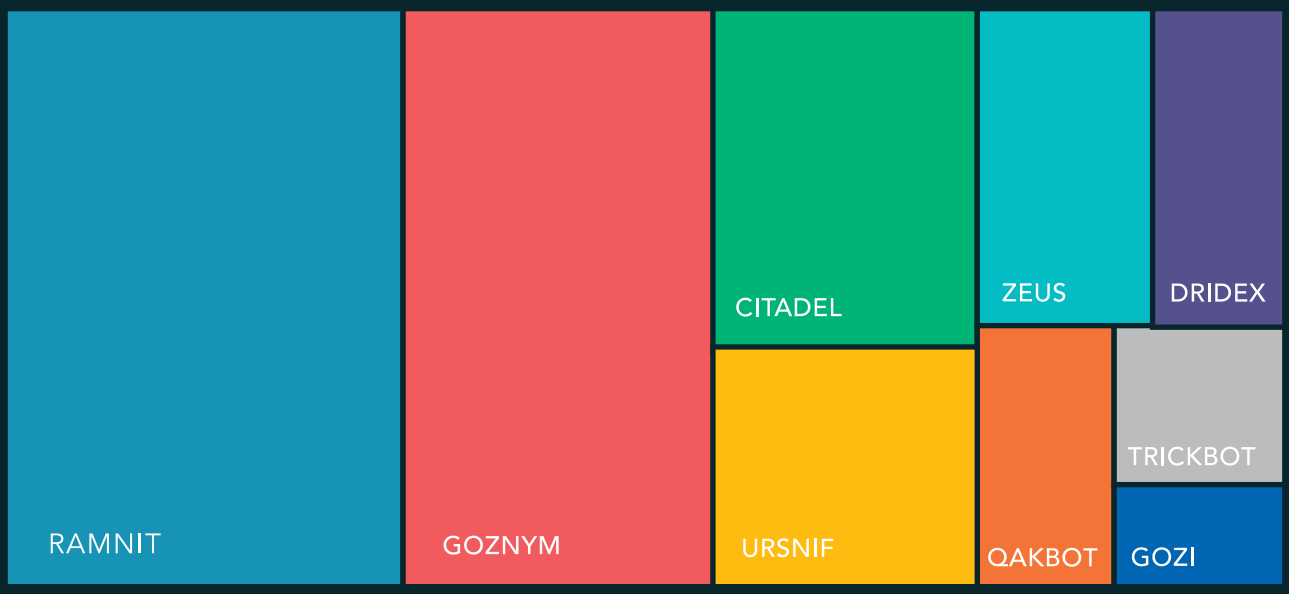
In fact, almost

95%

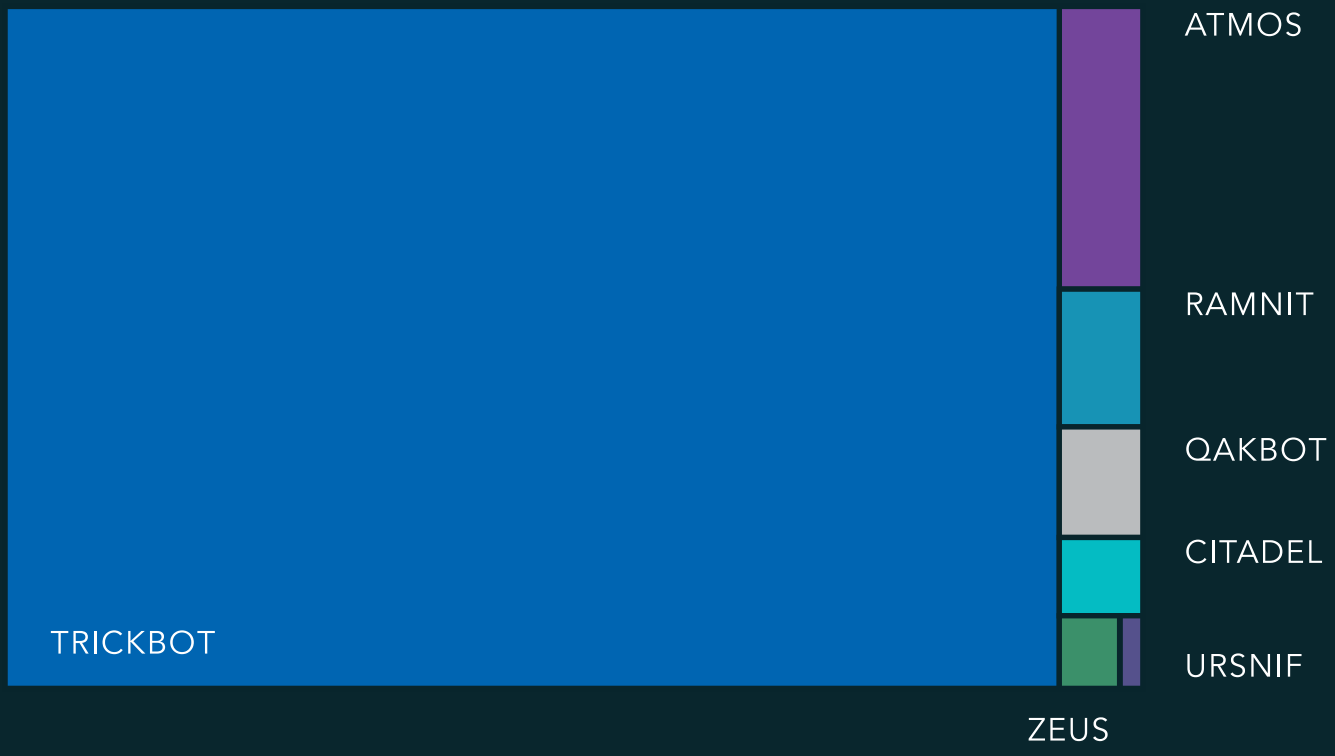
of all cards stolen belonged to American banks

MALWARE

Top 10 malware types affecting financial services and insurance were...



Trickbot was overwhelmingly the most-used web-injected malware in 2017



Top 5 malware techniques used

1. Malicious code injected into another process
2. Malicious code executed from memory regions
3. Detects the presence of a debugger
4. Attempts to delay the analysis task
5. Uses packer protection

Blueliv.

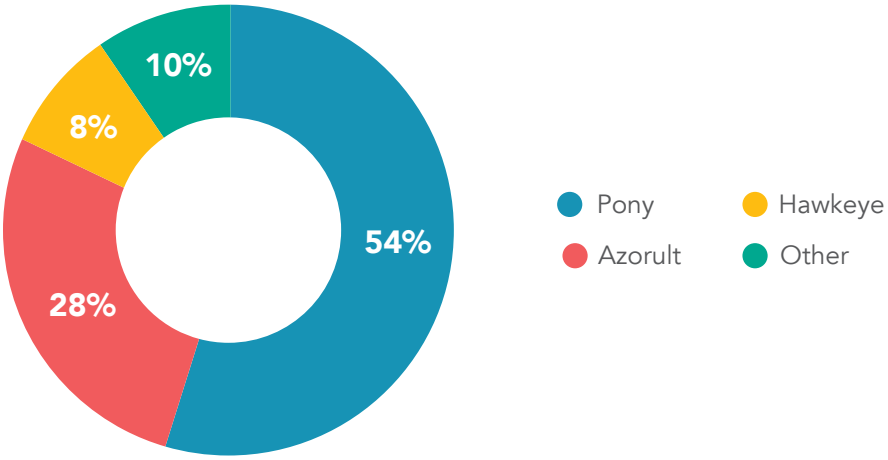
MALWARE ADVANCES

01

In 2017, we examined millions of samples using our proprietary elastic sandbox. Through a combination of automation and machine learning, supported by reverse engineers working in our analyst team, we were able to gain insight into some of the latest malware trends. We outline these in this section.

MALWARE VARIANTS: STEALERS

We analyzed a huge number of botnets that were being utilized to steal credentials in 2017. We highlight the following three, which make up almost 90% of those analyzed.



PONY

PONY, which has been around since at least 2013, continued to dominate the landscape last year. With over 1,000 associated C&Cs, the trojan/downloader not only leads to credential theft but can be used to drop other new malware variants too. [3]

While the malware is hidden in an executable file, the spam messages typically use an overdue invoice/payment notice to manipulate the user. It then uses obfuscation techniques and delay tactics to evade detection. Currently there is no sign that the number of cyberthreats associated with PONY will decrease due to its multifunctional usage as a stealer.

AZORULT

Another stealer which continued to see success last year was AZORult. It was originally discovered in 2016, when the Chthonic Zeus variant was pushed out via legitimate emails from PayPal. After the trojan infected the computer, Cthonic would download another module: AZORult. This same technique was deployed using the Seamless and Ramnit malware too.

It looks for sensitive credentials to submit to a C2, including saved passwords, cookies, wallet.dat files from popular cryptocurrency clients, running processes and several others. Version 2 added support for bit-domains. Though popular, it has been observed that it needs other malware to get into a computer in the first place.

HAWKEYE

Unlike traditional Word document-based attacks, HawkEye does not rely on macros, but rather on whether the user has patched their version of Word recently, or if they blindly trust any documents. When opened, the HawkEye document crashes but retains operational control over the system and downloads further malware to steal from its victim.

Its versatility meant that it was deployed last year across multiple new phishing campaigns, with the aim of stealing email and browser passwords. It also featured keylogger and screenshotting capabilities and sent a number of other credentials back to its C2 server.

MALWARE VARIANTS: TROJAN BANKERS AND WEBINJECTS

CYBERCRIMINALS USE WEBINJECTS TO INTERCEPT AND MODIFY DATA AFTER A WEB SERVER SENDS IT TO THE USER, BUT PRIOR TO ITS DISPLAY IN THE BROWSER

TARGETS: BANKS, ONLINE RETAILERS, INSURANCE, JOBSITES, CRYPTOEXCHANGES

Trojan malware has multiple functionalities which enable cybercriminals to defraud and steal from their victims. These include man-in-the-browser techniques, keystroke logging and form grabbing, webfilters, webfakes and webinjects, amongst others.

Cybercriminals use webinjects to intercept and modify data after a web server sends it to the user's computer, but prior to its display in the browser. Consequently, it gives the trojan the ability to modify the response of a webpage's server. This response is leveraged by banking trojans to request further information from the user, and forces them to perform fraudulent transactions, among other activities. Our report 'Chasing cybercrime: network insights of Dyre and Dridex trojan bankers' details this technique in greater depth.

The main targets of this type of attack are financial institutions, followed by a broad variety of targets including online retailers, insurance organizations, job websites and crypto exchanges. The perpetrators attempt to get hold of users' credentials through tampered login panels and perform fraudulent activities in their name.

RAMNIT

RAMNIT IS MUCH MORE SOPHISTICATED WITH INCLUSION OF ZEUS SOURCE CODE

Discovered in 2010, Ramnit was originally a worm distributed through removable drives, also functioning as a backdoor which allows remote access to the compromised computer. Since its discovery, it has become considerably more sophisticated with the inclusion of Zeus source code. It infects the system through a variety of methods, including exploit kits via advertisements on legitimate websites, and is able to utilize a number of malicious activities such as man-in-the-broswer attacks, FTP credential theft and privilege escalation to grant access to administration rights. Besides stealing credentials for online banking portals, the Ramnit trojan also works like a stealer, with an ability to dump browser passwords.

In March last year, Ramnit was utilizing pop-under adverts on adult websites in Canada and the UK. In late 2017, it was noticed that Ramnit had started popping up on mobile devices, despite its servers being shut down by Europol in 2015. Up to 100 infected apps appeared on Google Play, despite the fact that the trojan doesn't run on Android [4]. Last year a new variant was also discovered that uses DGA to find the C2, and uses new TLDs like .com, .bid and .eu.

PANDA BANKER

PANDA BANKER IS A ZEUS VARIANT AFFECTING FINANCIAL INSTITUTIONS AS WELL AS NON-BANKING TARGETS

Another Zeus variant which propagates itself via email attachments and the Angle, Neutrino and Nuclear exploit kits. Using an automatic transfer system webinject, Panda Banker primarily affected UK and Australian banks, spread through fake Word documents which required their macros to be enabled to launch PowerShell script. It was detected with its binary protected by an obfuscation layer, which when deobfuscated revealed a modular architecture which downloads plug-ins from its C2 server.[5]

A similar technique was used to spread Panda Banker at the end of the year with a campaign that successfully targeted non-banking targets, somewhat unusually for a webinject. Online payment sites, retailers and gambling entities were targeted to take advantage of the holiday shopping period. Once a computer is infected, the man-in-the-middle quietly harvests credentials including credit card details, social security numbers and answers to security questions.

TRICKBOT

TRICKBOT IS THE SUCCESSOR TO DYRE

The Necurs botnet made a comeback at the end of last year, delivering an updated, sophisticated Trickbot trojan many more capabilities than man-in-the-browser alone. Previously, Trickbot only seemed to target banks and financial institutions outside of the US, though via Necurs the threat broadened its scope. Its 2017 configuration delivered its payload through Zip-archived obfuscated JavaScript code and macro-based Word documents.

TRICKBOT CONTINUES TO EXPAND ITS GLOBAL REACH, AND NOW TARGETS BITCOIN SERVICES TOO.

It has been suggested the Trickbot trojan is Dyre's successor, both in terms of effect and attributes. While Dyre ceased operations in 2015 after Russian law enforcement took down the syndicate, there are certain code similarities between the two trojans that suggest a relationship. Furthermore, as Trickbot expanded its global reach (with new campaigns targeting Latin America over the summer, for example), the threat actors responsible added worm-like modules to the malware, as if inspired by WannaCry and NotPetya.

Trickbot has recently been seen targeting bitcoin services. We have seen hundreds of configurations performing man-in-the-browser attacks and stealing credentials on the likes of blockchain.info, coinbase.com, bitcoin.com, bancoinbursa.com, coin.z.com, coincheck.com.

URSNIF

NEW URSNIF/ GOZI-ISFB VARIANT EMERGED WITH NEW ANTI-DETECTION CAPABILITIES AND STEALTH TECHNIQUES

Though a widespread threat since 2007, Ursnif picked up again towards the end of the year with some Gozi-ISFB variants. The recent variant is capable of several malicious activities, including script-based browser manipulation, web injects, man-in-the-browser capabilities amongst many others. Its delivery methods in 2017 were malspam and exploit kits, including emails with attachments from fake financial services companies (especially in Japan).

Most curious about Ursnif/Gozi-ISFB variants is their anti-detection capabilities and stealth techniques. For example, one strain started to employ malicious TLS (Threat Local Storage) techniques when injecting itself into processes, essentially allowing the malware to manipulate the entry point timing. Ursnif has also been known to use the Tor network to hide command-and-control communications, and also booby-trapping itself if it detected – via movements of the mouse – that it was in a research/ sandbox environment.

NUKEBOT

The source code of the original Nukebot was leaked in March, ostensibly by its author Gosya. A Zeus-like banking trojan, Nukebot had man-in-the-browser and webinject capabilities, as well as other features including reverse SOCKS 4 and 32kb binary with obfuscated strings, enabling the theft of bankcard data with some success.

SOURCE CODE FOR NUKEBOT WAS LEAKED BUT VARIANTS HAVE BROADER MALICIOUS CAPABILITIES

Towards the end of 2017, a variant called Jimmy Nukebot emerged, with malicious capabilities including downloading payloads for web-injects, cryptocurrency mining and remote screenshotting. It was noted that one of the troubles with the new variant was that it has become much more difficult to perform static analysis, due to the huge list of strings from which to calculate the checksums.[6] Furthermore, its tasks are no longer to steal credit card data, but rather modules from a remote node.

ZLOADER/TERBOT

ZLOADER USES LEGITIMATE APPLICATIONS TO CARRY OUT MAN-IN-THE-MIDDLE ATTACKS

Another Zeus variant emerged at the beginning of the year, reappearing as malware containing legitimate applications so it can effectively carry out man-in-the-middle attacks. Operating via web browsers, the main module of the bot downloads and drops new elements in a temp folder. These new elements assure persistence in the system, using legitimate PHP BINARIES, as well as obfuscated PHP code. The use of legitimate applications reduces the change of detection, but likely can still be stopped since it uses similar patterns as known malware already. The key is remaining vigilant for 'old' code and its mutations, as well as defending against new code.

MALWARE VARIANTS: RANSOMWARE

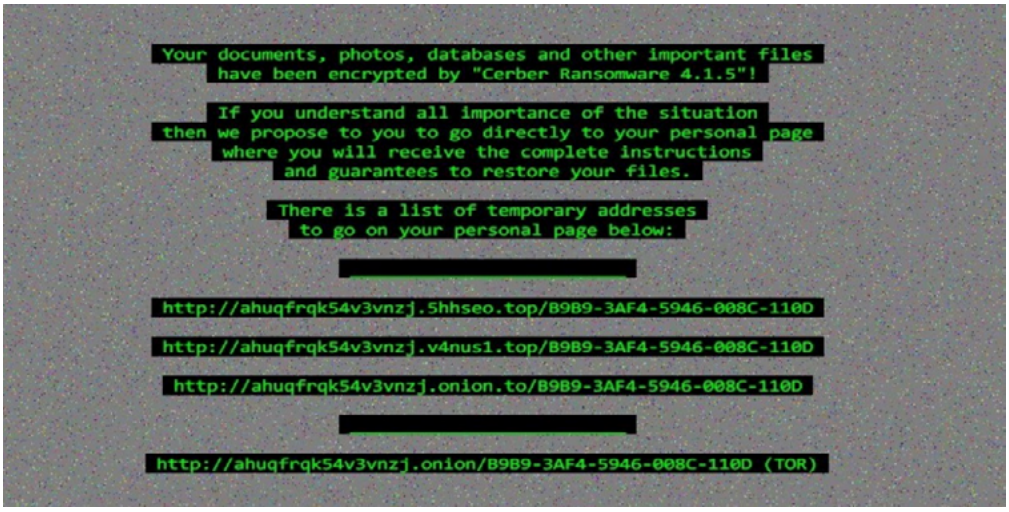
While 2016 saw considerable activity among ransomware families such as Locky and Cerber, 2017 saw the appearance of new ransomware families shifting to other operating systems, and the marquee WannaCry and NotPetya attacks. These are outlined below.

NEW RANSOMWARE EXPLOITS CVE VULNERABILITIES TO SELF-PROPAGATE

Attack patterns changed from common spear phishing attacks to a combination of this plus capabilities that exploit CVE vulnerabilities, in order to self-propagate and exponentially infect more devices. We have observed that bricking healthcare devices is already a handicap experienced by many hospitals, and ransomware attacks affect these devices in a similar way.

CERBER

- One of the most rapidly evolving ransomware families
- Continues to add more extortion techniques to its armoury
- Speaks to you from your computer



2016's Cerber ransomware retained the majority of market share in the first quarter of the year, with certain new functionalities that complemented its 'ransomware-as-a-service' model. The latter meant that non-technical cybercriminals could purchase a customized version of the ransomware, just as they might do for legal SaaS products. New features focused on evasion and obfuscation, employing certain anti-sandbox measures to allow the malware to propagate.

Throughout 2017, Cerber remained dangerous and generated millions of dollars in revenue for cybercriminals. Indeed, it was found on a US government website as late as September, having already evolved to v6 by May.[7] The latest iterations have added cryptocurrency theft to its processes (explained in greater detail later in the report), offering the cybercriminals another way to profit from an infection.[8]

WANNACRY

- First 'cryptoworm' ransomware attack, unprecedented in scale
- In 24 hours, 300,000 computers were affected in 150 countries
- Estimated 1 billion USD cost to business in first four days

10 FEBRUARY – WANNACRY DISCOVERED

14 APRIL – SHADOW BROKERS RELEASE 'LOST IN TRANSLATION'

12 MAY – WANNACRY OUTBREAK, CHAOS ENSUES

In April the 'Shadow Brokers' threat actor group leaked a critical arsenal of major exploits called 'Lost in Translation' which targeted Windows. Most notably, the EternalBlue and EternalRomance exploits took advantage of previously unknown zero-day vulnerabilities in Microsoft's SMBv1 protocol, which allowed attackers to execute arbitrary code on the targeted computer via specially crafted packets.

On 12 May, the ransomware known as WannaCry emerged in an aggressive campaign. The initial attack was unprecedented, infecting more than 300,000 computers in over 150 countries in less than 24 hours.

MORE DETAILED INFORMATION IS AVAILABLE ON OUR BLOG: 'WHAT OUR HONEYPOTS TAUGHT US ABOUT WANNACRY RANSOMWARE.'

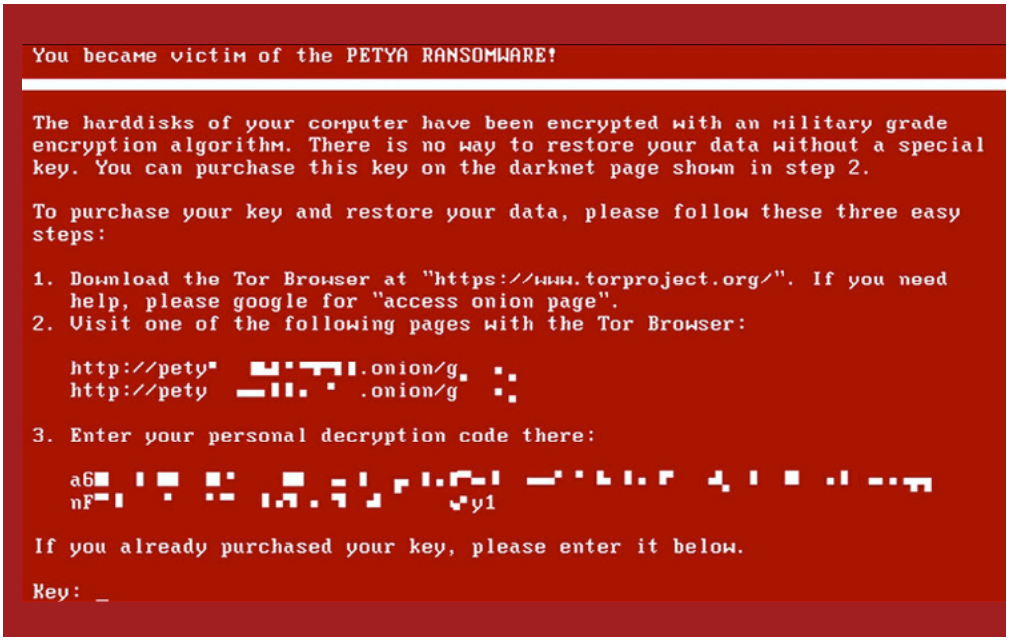
Such large-scale distribution and speed of propagation was due to its worm capabilities, making it the first of its kind and coining the term 'cryptoworm.' WannaCry required no user interaction, using EternalBlue to exploit the CVE-2017-0144 vulnerability with port 445 open, used by the SMB protocol. Moreover, WannaCry forced infected devices to search for other vulnerable computers to propagate the malware.

Our honeypot infrastructure experienced an upsurge of 540% on network traffic directed to the SMB port in the first 24 hours. These connections originated from various countries, but mainly from Russia, China and the United States. We also learned that the most affected operating systems were Windows 7/8 rather than Windows XP. Organizations affected included the United Kingdom's NHS, Deutsche Bank, Telefónica, Nissan and FedEx, with an estimated total cost to business in the first four days reaching over 1 billion USD.

It is surprising how many unprotected devices there remain in the wild with port 445 still open – it is one of the most attacked ports within internal networks and indeed it is common to see it open in a LAN. We believe it remains open perhaps due to discontinuation of services that security teams no longer want to touch. It is clearly unwise to have this port open to Internet too.

NOTPETYA

- Exhibited similar worm-like behavior to WannaCry
- Used lateral movement techniques
- Closer to a wiper than ransomware

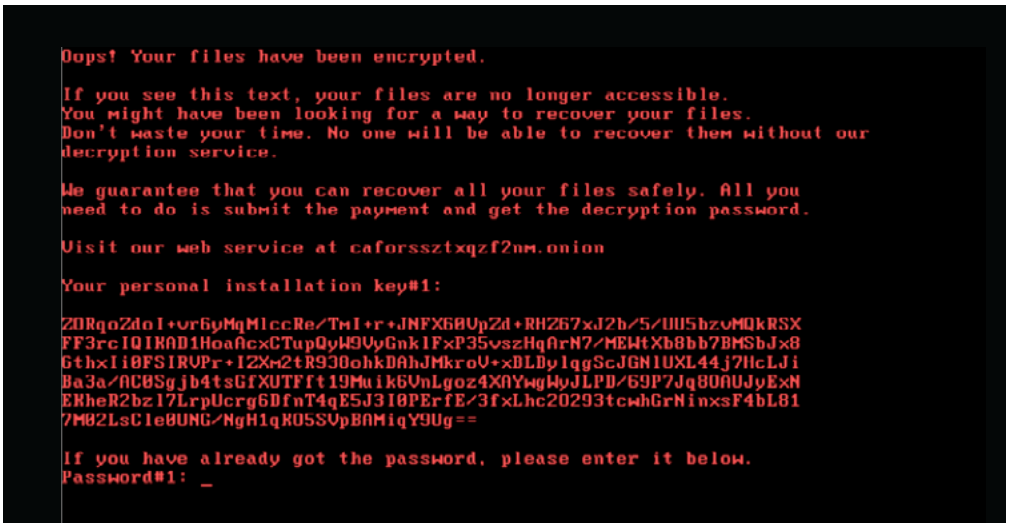


Even after the shocking success rate of WannaCry, many individuals and enterprises failed to install the recommended security patches. NotPetya (also known as ExPetr, EternalPetya or Petya) appeared in late June, and there was another global pandemic. It is believed that the outbreak originated from a compromised update of M.E. Doc, a popular tax preparation software in Ukraine. NotPetya shared a similar worm-like behavior with WannaCry; it used the EternalBlue exploit, supplemented by EternalRomance to propagate itself. However, whereas WannaCry attempted to infect all IPs on a network, NotPetya was more precise and generated less network traffic by checking whether it was on a workstation or a domain controller and altering its attempt accordingly. NotPetya's developers also went a step further to include lateral movement techniques, outlined later in this report.

Subsequent analysis showed that NotPetya didn't possess the capacity to send unique identification for each victim, which would have allowed developers to verify ransom payments. Instead it just provided fake IDs instead, so victims were unable to decrypt files even after they had paid the ransom. This suggests that NotPetya was designed to spread quickly and to cause as much damage as possible, effectively making it closer to a wiper than ransomware. The list of affected organizations was huge, including Ukrainian government agencies, Mondelez International, Merck, Beiersdorf, Saint-Gobain, Reckitt Benckiser, TNT Express and AP Moller-Maersk. Costs were extremely high for those affected; it was estimated that FedEx (parent company to TNT express) lost over 300 million USD during the last quarter of their financial year.

BAD RABBIT

- Used EternalRomance and lateral movement techniques
- Financially motivated, rather than sabotage
- Heavily affected mainly Russian and Ukrainian entities, including Interfax



October's Bad Rabbit outbreak started infecting computers through legitimate compromised websites, offering a fake update download for Adobe Flash Player.

The ransomware used the EternalRomance exploit and lateral movement techniques to spread further, while deeper analysis showed it was equipped with a module to spread itself in local networks using the SMB protocol, as with NotPetya. Unlike NotPetya, however, Bad Rabbit generated a unique key for each infected computer, as well as its own Bitcoin wallet, suggesting that its authors had some financial incentive.

The main targets of the ransomware were state organizations in Russia and Ukraine, but affected a number of strategic organizations in Germany, Japan, Bulgaria, United States, Turkey, South Korea and Poland too. Among the victims were Russian media groups Interfax and Fontanka, the Ukrainian Ministry for Infrastructure, Kiev's metro and Odessa International Airport. It was also reported that these major companies were all hit at the same time, which suggests that it was possible that the attackers had already compromised networks and used the compromised websites as a decoy.

MALWARE VARIANTS: ANDROID RANSOMWARE

The cyberfraud potential in the Android ecosystem can't be understated; in 2017 malware creators sought to replicate successful Windows malware distribution strategies to extort users, depending on the resources it tries to hijack.

CRYPTO-RANSOMWARE HIJACKS THE USER'S FILES

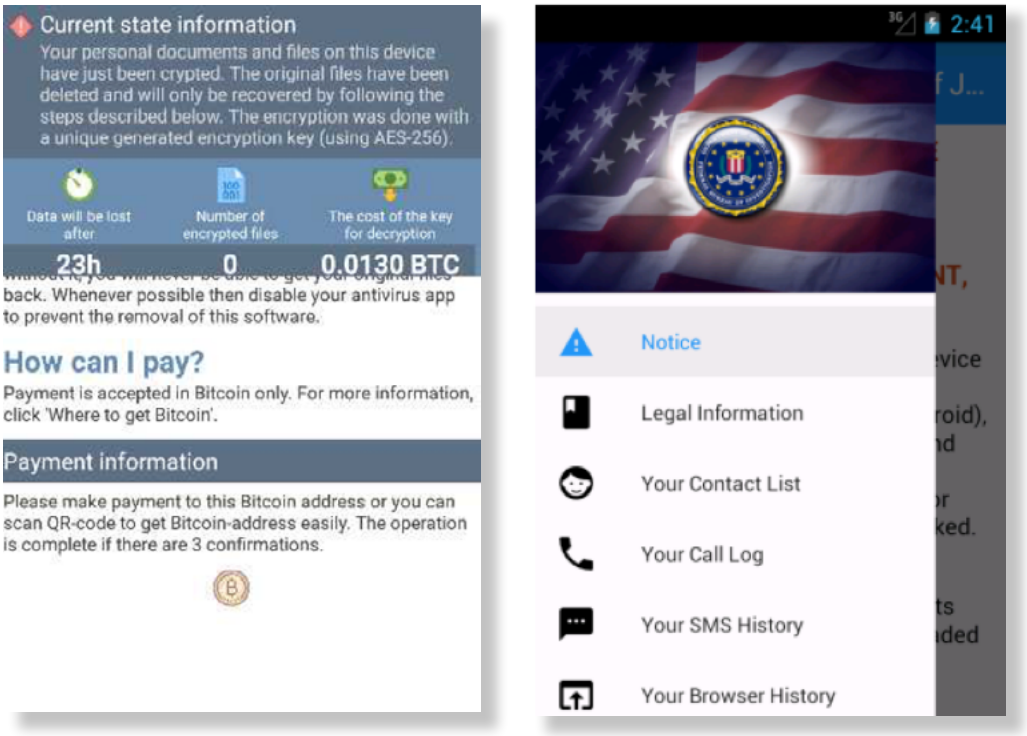
LOCKSCREEN RANSOMWARE HIJACKS ACCESS TO THE SYSTEM

Ransomware on Android tends to use two main strategies to extort users:

1. Crypto-ransomware hijacks the user's files, encrypting them with strong cryptographical algorithms

2. Lockscreen ransomware hijacks access to the system itself

In both cases, cybercriminals demand a ransom to release the resource. Multiple variants of ransomware target Android, disguised as fake utilities or imitating legitimate applications. The most noticeably affected applications are Android Defender, Simplelocker, Lockerpin, Jisut, Koler/Locker and Charger. Recent variants such as Lockdroid use fake package installations to attempt to trick users into providing device administrator privileges.



DoubleLocker seemed to be based on a previously-observed trojan that harvested banking credentials from a device. However, its functions were substituted by two mechanisms to extort money from its victims.

It was distributed similarly to its banking trojan predecessor – a fake Adobe Flash Player installation through compromised websites. Once installed, it requested permissions of accessibility services and once granted, it uses them to activate device administrator rights and sets itself as the default home application, neither with the user's consent.

It then changed the device's security PIN code into a random value, blocking the user, with this new PIN neither stored nor sent to the ransomware's authors, which makes it virtually impossible to be recovered. If the ransom was paid, the attacker could remotely reset the PIN and unlock the device. It also encrypted all files on the device's primary storage using the AES encryption algorithm. The ransom note demands a payment of 0.0130 Bitcoin and highlights the necessity of making the payment within 24 hours, however, there is no evidence of the data being deleted after the deadline is crossed.

Blueliv.

ATTACK TECHNIQUES

02

LATERAL MOVEMENT

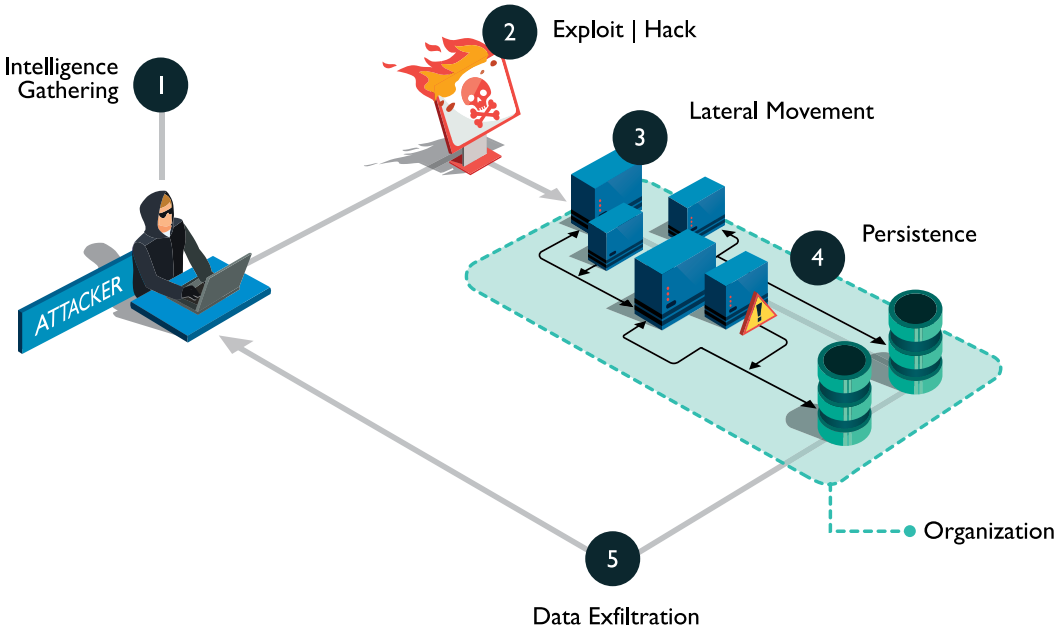


Fig. 1 Lateral movement technique

LATERAL MOVEMENT REFERS TO THE VARIETY OF TECHNIQUES AND PROCEDURES THAT ALLOWS AN ATTACK TO PROPAGATE FURTHER INTO AN INTERNAL NETWORK AFTER THE INITIAL INTRUSION POINT

One of the main trends we observed in 2017 was the proliferation of network lateral movement techniques. Lateral movement refers to the variety of techniques and procedures that allows an attack to propagate further into an internal network after the initial intrusion point.

Thought the concept was already common practice among advanced persistent threats (APTs), it usually implied manual procedures. In 2017, we observed an increased usage of lateral movement techniques, particularly among ransomware strains, which boosts and automates malware propagation.

MALWARE SUCCESSFULLY USING LATERAL MOVEMENT TECHNIQUES INCLUDE EMOTET AND TRICKBOT

For example, NotPetya tried to gather credentials from infected computers using a module like Mimikatz, a tool capable of extracting passwords, hashes, PINs and other useful information from memory in Windows OS. It then used those credentials to connect to other targets through PsExec, a lightweight remote access program, and Windows Management Instrumentation Commandline (WMIC), a command-line and scripting interface – both developed by Microsoft. Such was NotPetya's success that other malware sought to replicate these capabilities.

In July, updated versions of banking trojans Emotet and Trickbot showed worm-like propagation techniques under development. The new version of Emotet had a bare self-extracting RAR file containing a component which scanned for other computers in the network and tries to login using brute-force. This should not be confused with the propagation module of Emotet, which accesses the victim's email contacts to send out infection-driven spam. The new version of Trickbot spreads through SMB, exploiting the Windows API to enumerate domains for lists of servers and LDAP (Lightweight Directory Access Protocol), and identify other computers that might serve as targets.

It is important to note that though lateral movement is not a new malware technique, these do constitute an interesting trend observed in banking trojans. In fact, this might be a growing trend among malware targeted at the financial and insurance sectors. It massively widens the number of possible targets and simplifies distribution methods because it doesn't require victim interaction. However, this kind of lateral movement is clearly more noisy then the usual stealthy lateral movement performed during targeted attacks. In this regard, there has been an increase of compromised companies which usually start with a single infection or stolen credentials, and from there the bad guys move laterally across the organization's network until they find something to monetize the intrusion.

SOCIAL ENGINEERING AND BUSINESS EMAIL COMPROMISE

Many threats still rely on emails as the initial attack vector, either to distribute malware or to make contact with their targets. Malware that infects computers by taking advantage of system vulnerabilities are not uncommon, but this method usually requires quite advanced technical knowledge and tends to be more expensive, as vulnerabilities need to be discovered or bought as zero-days.

Instead, deceiving users to manually execute malware does not require such level of technical expertise nor is it as expensive. With the proliferation of malware-as-a-service, where malware creators adopt commercial distribution of their tools, and in combination of social engineering techniques, virtually anyone can set up his own cybercriminal business.

Manipulating individuals and organizations in order that they give up confidential engineering remained a highly successful attack vector in 2017, and will continue to be as education continues. Cybercriminals take advantage of a natural inclination to trust, with varying degrees of success but attacking the weakest link in the security chain – the person that accepts a scenario at face value.

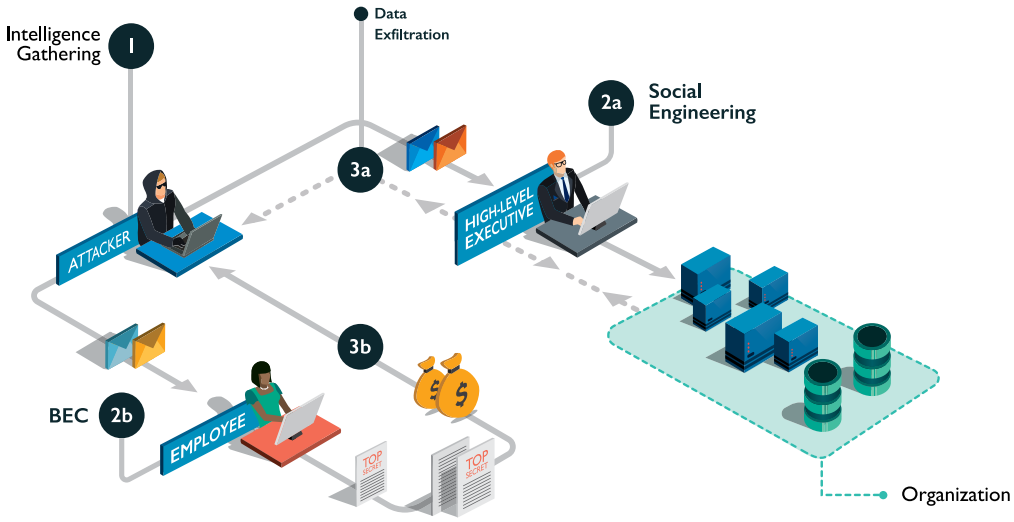
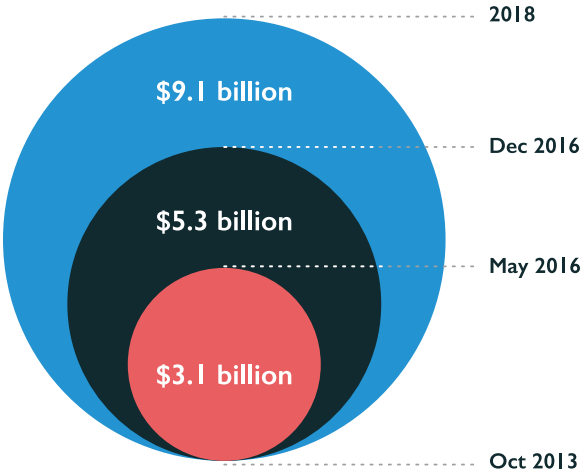


Fig. 2 BEC technique

Initial attacks (pre-BEC) are specially targeted against high-level executives (CEO, CTO, CFO, etc.) with crafted malware or spear-phishing techniques to get hold of financial data, sensitive information or authentication credentials. In the era of social media, these high-value targets are easily identifiable with a few searches online. Moreover, these types of attacks are often as simple as impersonating the email service provider and alerting the user to problems which require some action. Email providers can be identified from the MX records of the DNS, which should point to the email server.

EMPLOYEES ARE TARGETED BY FAKE EMAILS PRETENDING TO BE EXECUTIVES DEMANDING PAYMENT OR INFO

For the BEC attack itself, targets are often financial or administrative departments, to which an impersonated high-level executive or external partner/provider makes contact demanding a payment or asking for sensitive information. These types of attack are referred as Business Email Compromise (BEC) and rely on deception, pressure and fear. Estimations by the Internet Crime Complaint Center (IC3) indicate that losses generated by BEC between October 2013 and May 2016 were approximately $3.1 billion, rising to $5.3 billion by December 2016. These losses are predicted to be around $9.1 billion in 2018. In both cases, attackers seek to keep a low profile to avoid detection or being flagged as spam, rather than the mass-email tactics of common phishing attacks.



Source: TrendMicro [9]

Blueliv.

HIGH PROFILE BREACHES

03

Several major organizations suffered huge financial, business and reputational costs as the result of breaches that either took place or were revealed in 2017. C-level executives were forced to resign, customers left in their droves and public images devastated because of cyberattack.

This section covers some of the most high-profile breaches that took place throughout the year, and lessons that ought to be learned by organizations large and small.

EQUIFAX

143 MILLION
PII STOLEN

APACHE STRUTS VULNERABILITY EXPLOITED

IMMEDIATE 35% STOCK CRASH

$6BN MARKET CAPITAL LOSS

FALLOUT CONTINUES

Probably the most important data breach of the year, both in terms of severity and publicity, was suffered by the consumer credit rating firm Equifax; immediately after the breach, Equifax' stock fell 35%, representing a loss of $6 billion in market capital for its shareholders at the time, and it is still unclear whether it will ever recover from the reputational damage incurred.

The personal information of 143 million people was stolen, including names, addresses, birth dates, social security numbers and driver's license numbers.

Though announced in September, it is believed the breach occurred in mid-May. The attackers entered via a known vulnerability of Apache Struts software, a platform that acts as server for web applications. This vulnerability was disclosed and fixed in March by the Apache Software Foundation, which let Equifax know almost two months before the breach that it should update its servers.

A first group initially exploited the vulnerability and intruded into Equifax's network but, as the attack escalated, handed off to a second group of more sophisticated hackers. The attackers managed to install over 30 web shells among different web addresses. This action guaranteed persistence in the event that Equifax finally fixed the Apache Struts vulnerability.

Since the attack, there have been several claims on underground forums that the data was available. However, all of them have since been proven to be scams to earn some fast cash. The eventual intended use of the data is still unknown, but common sense indicates it will probably be sold to other criminal groups.

UBER

MILLIONS OF PII STOLEN

EXECUTIVES PAID A RANSOM BUT WERE CAUGHT OUT

INVESTIGATIONS ONGOING

In November, it was disclosed that Uber suffered a severe data breach back in October 2016, which was concealed by former chief executives of the company as a result of a $100,000 payout to the attackers.

The data breach happened as two hackers accessed a private GitHub coding site used by Uber software engineers and obtained login credentials. These allowed them to access data stored on an Amazon Web Services account with resources that handled computing tasks of the company. From this point, the attackers obtained email addresses and phone numbers for 50 million Uber riders and the personal information of 7 million drivers around the world. The information also included 600,000 U.S. drivers' license numbers. Later, the hackers contacted Uber by email demanding a ransom.

At the time of the incident, Uber was already under investigations of separate claims of privacy violations and was trying to negotiate with regulators for a settlement. As the company has now recognized, it was under the legal obligation to report the hack both to regulators and affected drivers, rather of paying the hackers to keep the breach quiet.

The breach resulted on the chief security officer being fired, as well as the legal director of security and law enforcement. Currently, the company is being investigated in multiple states, starting with the New York Attorney General, and is also facing class-action lawsuit for negligence over the data breach by a customer.

DELOITTE

LIED ABOUT EXTENT OF ATTACK

REPUTATION SEVERELY DAMAGED

One of the 'Big Four' accountancy firms reported a breach in September, where its internal email systems and critical data around high-value clients were compromised. The Guardian first reported the true scale of the breach, which went against Deloitte's original account, claiming to have only affected a few clients.[10] Cybersecurity heavyweight Brian Krebs reported that internal sources of the company corroborated that the breach affected administration accounts and, therefore, all of the company's emails and potentially the data of many more clients than Deloitte claimed.[11] It is still unknown how the attackers intruded into Deloitte's systems, as internal investigations are ongoing and details have not yet been disclosed by the company.

HBO

SUFFERED EXTORTION

CONTENT LEAKED ANYWAY

The American cable channel HBO was also targeted and breached in Q3. Attackers compromised unpublished material in the form of scripts and entire unaired episodes of the popular series Game of Thrones. Besides causing reputational damage to the company, attackers also extorted the network out of payments in order not to publish the stolen content. Although it impacted the company itself rather than clients or consumers, its relevance should not be understated. HBO is known to have suffered multiple hacks and breaches, both on its social networks and business systems, which set a precedent and likely made them more attractive to further attacks.

VERTICALSCOPE

November also saw the website of Verticalscope, a company that manages discussion forums, compromised for the second time in recent years. It was believed that details of 2.7 million user accounts were stolen. Evidence of the breach was discovered as hackers tried to sell the information. At first, it seemed like a resell of the data obtained in a first breach that happened on 2016, but hackers provided screenshots to prove that the websites were indeed compromised again. The discovery was made just before the hackers launched a commercial service indexing consumer information exposed in corporate data breaches.

Blueliv.

THREAT ACTOR PROFILES

04

This section of the report provides a topline overview of some key threat actors which were active in 2017, and whose activity is worth noting for the coming year.

LAZARUS GROUP

BELIEVED TO BE NORTH KOREAN

RESPONSIBLE FOR POWERRATANKBA, RATANKBAPOS

Lazarus Group is one of the most successful state-sponsored groups and believed to be acting on behalf of North Korea. In February, the group appeared to be using compromised banking websites in Poland, Uruguay and Mexico to redirect visitors, using a custom exploit kit similar to Ratankba. In April, it was found to be involved in a spear phishing campaign against US defense contractors. Towards the end of the year, it turned its sights onto cryptocurrency. Its latest implant, dubbed PowerRatankba, is a PowerShell-based malware that is used like its predecessor Ratankba as a reconnaissance tool ahead of deploying the next stages of its attack.

Once executed, PowerRatankba sends information about the infected machine to C2 server and retrieves a command to execute. The malware is typically delivered via a spear-phishing campaign, and following the implant, it can steal cryptocoin wallets and infiltrate cryptocurrency operations. Once a user is infected, PowerRatankba deploys its next process – GH0STRAT – if it finds cryptocurrency-related software, in order to start siphoning off cash.

Besides stealing cryptocurrency, the group also started operations intended on stealing point-of-sale data from businesses operating in South Korea using a tool code-named RatankbaPOS. The tool searches for strings related to credit cards in the system, then exfiltrates the data to the C2 server.

It is believed that Lazarus is stockpiling financial resources that it will later use to purchase, develop, and launch more dangerous and intrusive campaigns. Stand by for more details…

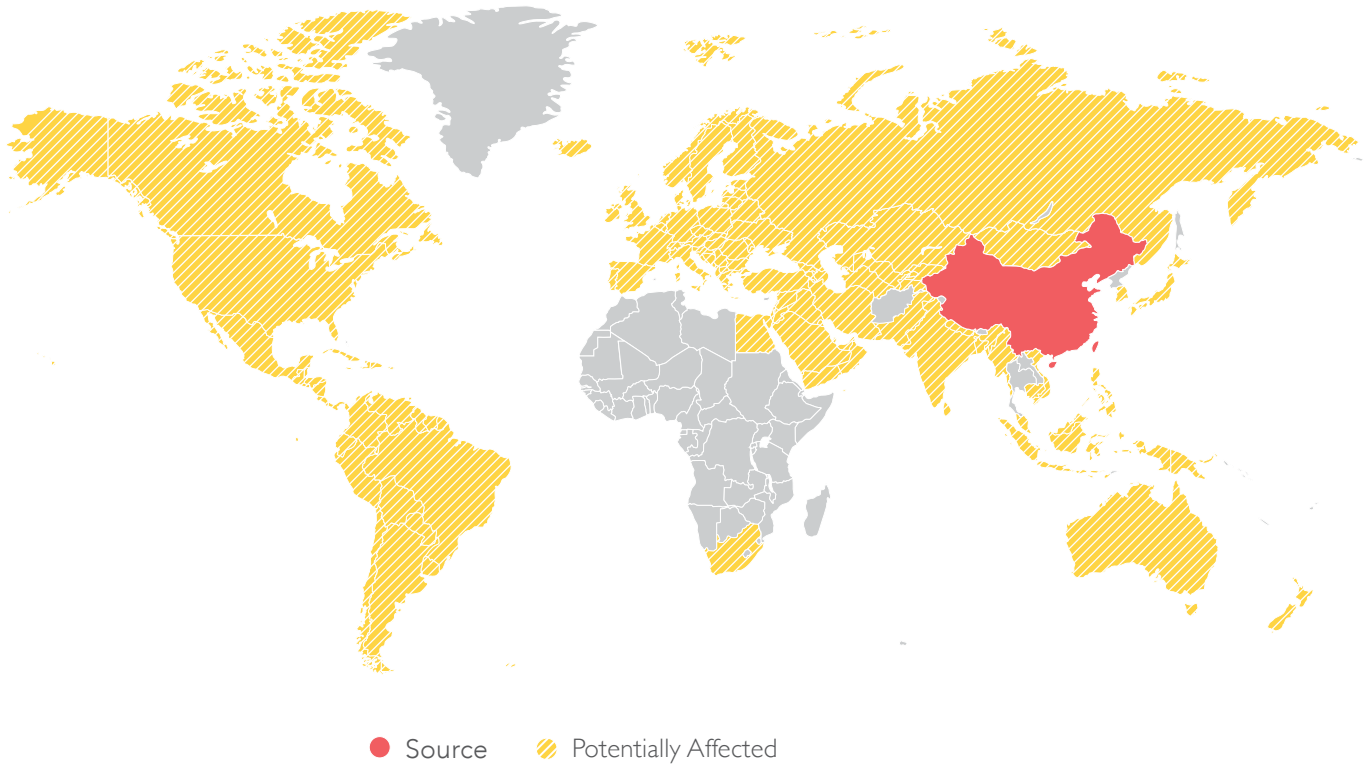
SHADOW BROKERS

BELIEVED TO BE NORTH KOREAN RESPONSIBLE FOR POWERRATANKBA, RATANKBAPOS

First coming onto the scene in the summer of 2016, Shadow Brokers have achieved a great deal, from embarrassing the NSA to dumping sophisticated malware and exploits in the public domain. As mentioned above, ShadowBrokers were responsible for the Lost in Translation dump of critical exploits in April 2017, which included EternalBlue and EternalRomance.

This was in fact the fifth leak, all of which targeted enterprise firewalls and antivirus software. There has been much speculation about the identity of the group – possibly linked to the NSA itself, possibly to Russia. The jury is still out, even though the group is currently quiet.

APT17

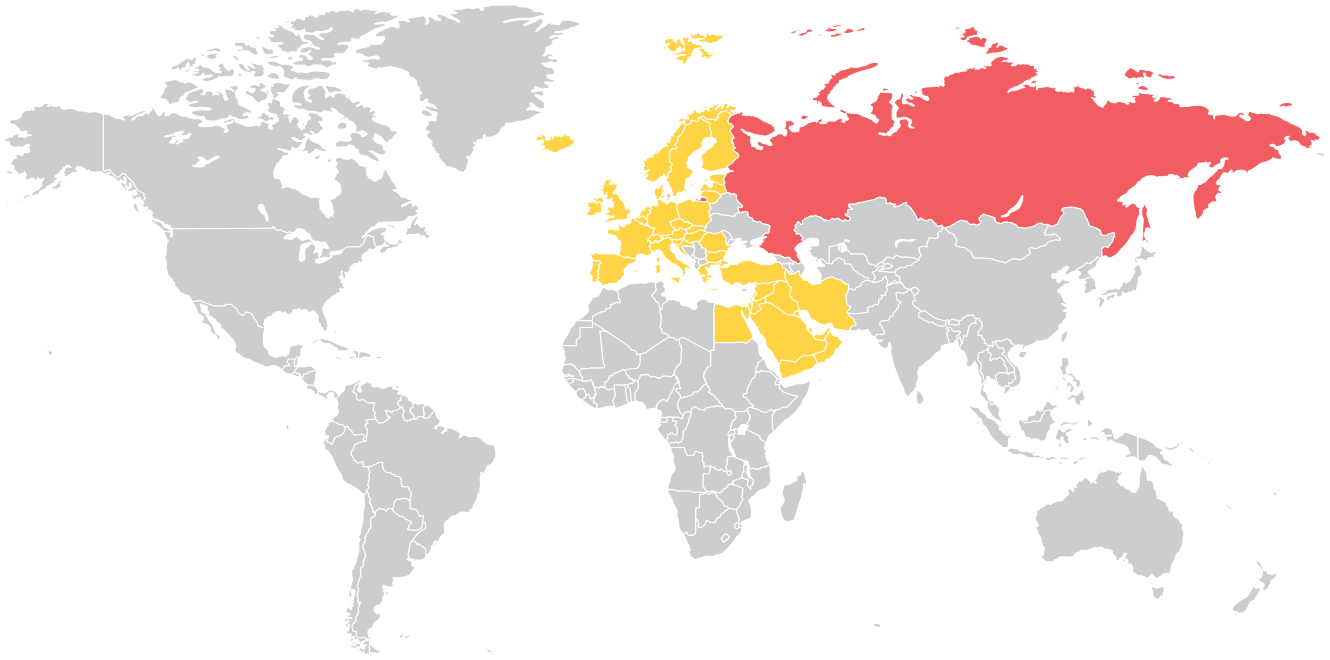


APT17, or Deputy Dog or Axiom, sought to take advantage of the HBO data breach outlined above. Their campaign centered around falsely claiming it had details about series' plots, as well as unpublished video footage. Emails with subject lines such as 'Wanna see the Game of Thrones in advance?' were sent to lure victims into downloading an attached Microsoft Word document, titled 'game of thrones preview.docx.' The attachment embedded a .LNK (an OLE packer shell object) that executed a malicious PowerShell script, installing the diskless 9002 remote access trojan (or RAT).

A similar campaign in 2014 exhibited similar techniques using ZIP compressed files akin to LNK downloaders. Familiarities in the script, payload, file names, images and themes suggest that the Chinese state-sponsored actor APT17 was behind both campaigns.

September's CCleaner hack has also been linked to the group, which affected 2.2 million people. The intrusion contained a backdoor which was capable of installing additional malware.

APT28



APT28, also known as Fancy Bear, Pawn Storm, Sofancy Group, Sednit or STRONTIUM, is a cyberespionage group likely sponsored by the Russian government. In July, it targeted multiple hospitality organizations, including hotels across Europe and the Middle East.

APT28 IS LIKELY SPONSORED BY RUSSIA

ALLEGEDLY PARTICIPATED IN DNC BREACH

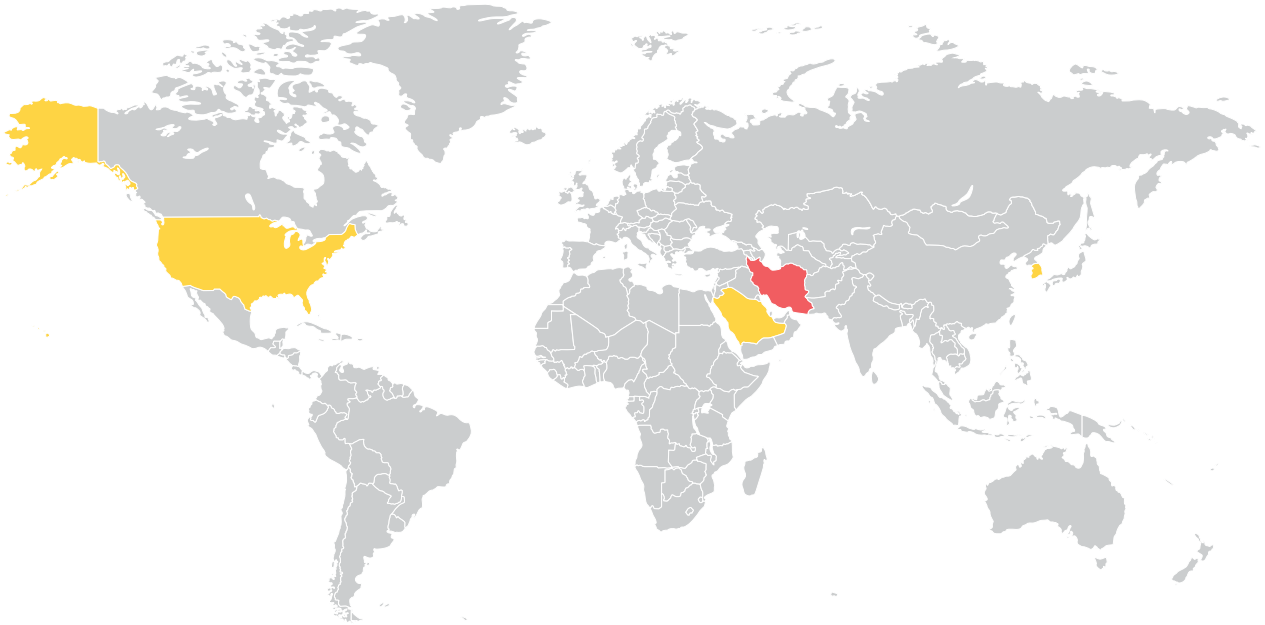
RESPONSIBLE FOR ATTACKS ON HOSPITALITY SECTOR

The group was believed to have close ties with the Russian intelligence agencies and their interests, and allegedly also participated in the data breach of the US DNC (Democratic National Committee) in 2016, interfered in the German and French elections in 2017, and conducted a number of other politically-motivated campaigns aimed at destabilizing NATO-aligned governments.

The modus operandi of the hospitality attack used the EternalBlue exploit and open source tool Responder, where the malware was able to achieve lateral movement into the hotel's network and reach travelers. Once a system was infected, the malware monitored both the guest and internal WiFi networks of the hotel and deploys Responder.

We believe APT28 was conducting this campaign to explore new attack vectors designed to reach VIP enterprise targets. Acquiring these high-value authentication credentials meant that APT28 could infiltrate corporate systems with the aim of compromising services and data for state-led espionage.

APT33



● Source ● Target

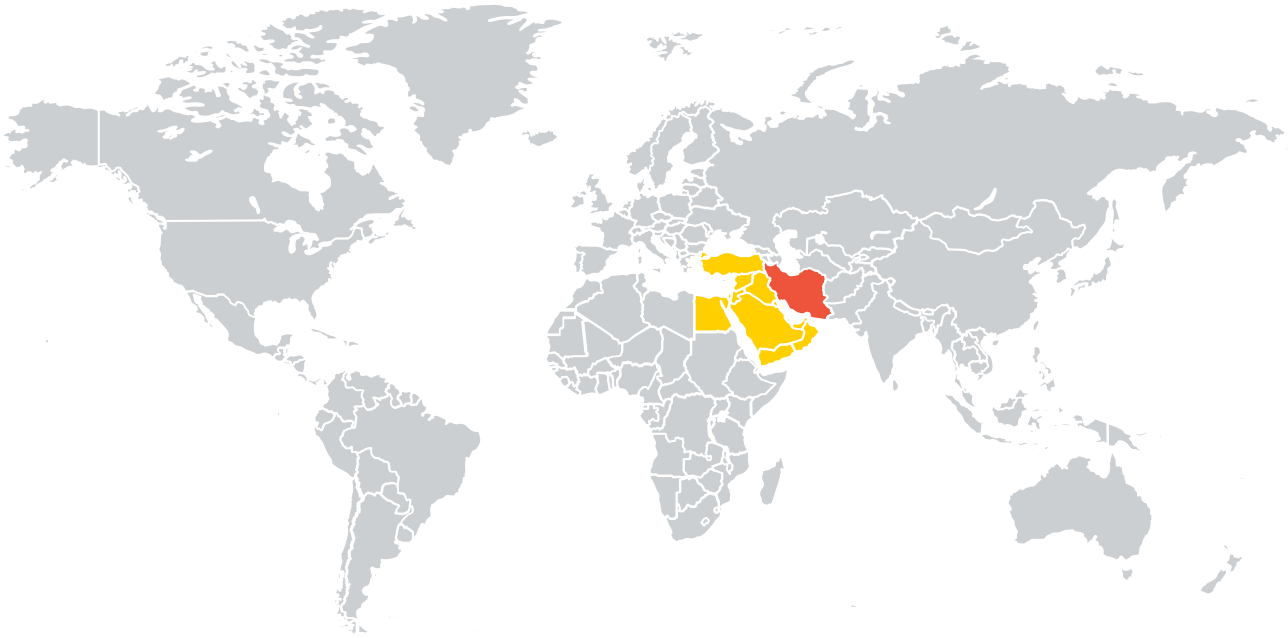
APT33 is believed to be another state-sponsored threat actor, targeting interests in the US, South Korea and Saudi Arabia, including commercial and military aviation companies and organizations in the energy sector.

Its primary identified campaign was distributed through spear phishing, using specially-crafted emails to simulate recruitment.

They contained links to malicious HTML application (.hta) files. These malicious files did indeed contain details of real job offers extracted from employment websites and infected the recipient after a legitimate redirection. Interestingly, the .hta file contained embedded code for a custom backdoor developed by the group.

APT33's targets seemed to align with the national interests of Iran. Additionally, the timings of its campaigns suggested the attackers were operating during Iranian office hours. APT33 has also been observed using tools popular among Iranian hacking communities and DNS servers also suspected to be used by other Iranian threat actors. All this evidence may seem circumstantial but points towards Iran, which lately has bolstered its cyberspace capabilities. We have observed enough evidence to suspect that the Iranian threat will continue to increase in the foreseeable future.

APT34



Source Target

APT34 IS BELIEVED TO BE SPONSORED BY THE IRANIAN GOVERNMENT

APT34, a group believed to be nation-sponsored and working for the Iranian government, used the Microsoft Office vulnerability CVE-2017-11882 in a campaign targeting government organizations in the Middle East.

EXPLOITS CVE-2017-11882 VULNERABILITY

The vulnerability affected multiple versions of Microsoft Office, and when exploited allowed the attacker to execute arbitrary code in the machine. The flaw resides in an old component called Equation Editor, used by the Office products to evaluate mathematical formulas. APT34 leveraged this vulnerability using spear-phishing campaigns that contained the malicious Office document as an attachment.

The group showed itself to be a considerable threat. Just days after Microsoft's disclosure of the vulnerability, they were able to incorporate an exploit in a new campaign. APT34 is currently a major threat actor and is likely to pose an even greater threat in the future if they continue to improve exploitation techniques and methodologies at this pace.

COBALT GROUP

The cybercriminal operation known as Cobalt Group is an outfit that was targeting banks, ATMs and financial institutions in 2017. Back in November, it was reported that Cobalt Group was sending emails containing a malicious RTF file using the CVE-2017-11882 exploit – another example of the group weaponizing Microsoft bugs as soon as they are disclosed.[12] Typical Cobalt Group attacks establish fake domains then send phishing emails with malicious files attached.

TYPICAL COBALT GROUP ATTACKS ESTABLISH FAKE DOMAINS THEN SEND MALICIOUS EMAILS

Allegedly a gang with roots in Russia, Cobalt Group first came on to the scene in the previous year, seemingly trialing their techniques against weaker ex-Soviet and Russian financial institutions before moving towards wealthier targets in the rest of the world. According to Trustwave, carried out a series of ingenious bank heists whose techniques we are likely to see in the English-speaking world more and more this year[13] The attacks combined both cyber and physical activities – mules using rogue identities set up new bank accounts and requested debit cards, manipulated the overdraft limits then involved other mules to withdraw funds abroad later down the line. The group was named Cobalt Group due to the use of Cobalt Strike to carry out their operations. However, several groups are using this tool to perform attacks nowadays, so the name could cause confusion.

OCEANLOTUS GROUP

OceanLotus, also known as APT32, was identified in summer 2017 as a Vietnamese cyberespionage group conducting attacks targeting ASEAN, nation states, corporations and civil society in the region. Throughout 2017 OceanLotus has become increasingly sophisticated in its attack techniques, using a variety of signature malware types (for example, WINDSHIELD, KOMPROGO, SOUNDBITE, and PHOREAL.), which were often deployed with the commercially-available Cobalt Strike BEACON backdoor.[14] Other custom-built malware included a backdoor targeting Outlook and another that uses DLL hijacking attacks against legitimate Microsoft, Google and Kaspersky applications.

OceanLotus also carried out several complex spear phishing campaigns against several targets, in addition to a number of campaigns tricking victims via social engineering to give up their Gmail credentials.[15] The group used customer Google app popups which redirect to an OAuth page, where the user must authorizing their account – emphasizing the importance of education and 2-step verification in the fight against cybercrime

Blueliv.

2018 TRENDS

05

Blueliv.

RANSOMWARE TO BE OVERTAKEN BY CRYPTOJACKING

Though the major caveat here is based on the monetary value of certain cryptocurrencies, it is likely that ransomware attacks will be overtaken by cryptomining – particularly among less-skilled criminals, who would seek to make a fast buck with minimal effort. Indeed, towards the end of last year, we found evidence to suggest that many cybercriminal gangs had shifted resources from ransomware to cryptomining already, where exploitation of computers' processing capacity to mine for cryptocurrency takes place.

CRYPTOCURRENCY IS GOING MAINSTREAM – THE BAD GUYS WILL EXPLOIT IT FURTHER

WEAKER BLOCKCHAIN ALGORITHMS WILL BE COMPROMISED

INFRASTRUCTURE WILL BE HIJACKED TO MINE CURRENCY

This growing trend can be explained in two ways. Firstly, it is due to the recent increase in value of many cryptocurrencies, such as Bitcoin and Ethereum (followed by a spectacular bubble burst for one). Cryptocurrency has always played an important role in black market trading and cybercriminal activities, but with such an explosive increase in monetary value it has become even more desirable. As blockchain technology goes mainstream more generally, with many legitimate financial institutions starting to take notice too, we expect to see an increase in attempted exploitation of the technology. Cryptographic attacks on some of the more secure technologies (powering the likes of Bitcoin, for example) may be relatively few and far between, but weaker algorithms are likely to be exploited. Those blocks which do not have such secure coding will sooner or later be cracked and exploited.

The second way in which the trend appears to be growing is that ransomware is limited by its target's capacity to pay the ransom. In many less developed countries, the expenses associated with retrieving personal files tend to be too high, victims resign themselves to not retrieving their files and therefore offering no income for cybercriminals. On the other hand, cryptominers are able to extract value from a population who simply need to be connected to the Internet. They do not discriminate between targets as they often do not require any payment direct from the victim, just processing power.

Since it takes vast amounts of this to solve cryptographical problems, we are likely to see criminals take advantage of large-scale networks more and more. The temptation to breach networks – from public WiFi to infrastructure systems – to hijack their power is likely to increase exponentially. Cryptominer malware can illegally use up to 65% of the infected system's CPU resources, without the user's approval. A notable example would be CoinHive, designed to mine the Monero cryptocurrency when the user visits a web page where it is installed.

In sum, the cryptocurrency boom, bubble or otherwise, has led to great leaps forward in cybercrime. Threat actors are already taking advantage of the anonymity offered by digital currency to monetize their illicit activities, and we expect this trend to grow.

AI-POWERED ATTACKS

The uses for artificial intelligence at both the consumer and enterprise level are boundless. Indeed, artificial intelligence and automation contributes to the targeted threat intelligence we provide our clients. It allows us to better prepare for attacks using neural networks and models which previously would have been impossible to measure as effectively as we do today.

However, due to the advances in this area on the legitimate side, it was simply a matter of time until adversaries started to exploit vulnerabilities for profit and disruption.

AI-POWERED BRUTE FORCE ATTACKS WILL BE MORE TARGETED IN 2018

For a start, AI-powered brute force attacks could be more targeted in 2018. Using the same principles of big data analysis for legal activities, artificial intelligence can be used to process swathes of password information that can be found on the open, deep and dark webs in order to reduce the time it takes to find out the correct identifiers.

AI CAN FOOL SANDBOXES WITH A HIGHER SUCCESS RATE

Additionally, AI can be used to fool sandboxes and increase obfuscation capabilities. Though AI-powered behavioral analytics used for defense are increasingly powerful, on the flipside, AI can be used to observe these defense patterns – gathering intelligence harvested from sandboxes and implementing it effectively in future attack operations, potentially leading to higher success rates. The cybersecurity industry will therefore need to keep pace in this regard, constantly improving sandboxes for example, to stay ahead of the bad guys.

AI CAN HARVEST DATA FOR USE IN AN ATTACK

Automation may also be used to harvest relevant data from support forms, code repositories and other legitimate internet sources in advance of an attack. In much the same way as actionable threat intelligence can provide organizations with a higher level of protection, actionable information may also be used to enhance and simplify the job for cybercriminals when it is used to find weaknesses in the armor for fraud and phishing attacks.[16]

INTERNET OF THINGS

20 BILLION CONNECTED DEVICES BY 2020

Gartner predicts that by 2020, there will be over 20 billion connected devices - and many of them are currently comparatively easy to compromise.[17] Indeed, the growth in devices will very likely mirror the growth in IoT-based malware and has already been evidenced by the likes of the spillover from 2016 of Mirai and IoTroop/Reaper in 2017. Simply put, the pace of innovation and deployment of network-connected systems has outstripped the necessary safeguarding measures. Last year we identified four key concerns that should be under consideration:

4 KEY VULNERABILITIES TO CONSIDER: FIRMWARE, SOFTWARE, HARDWARE, RADIO

1. **Firmware**, which can contain vulnerable hardcoded critical information and suffer from a lack of integrity in updates.

2. **Software**, vulnerable due to insecure authentication/authorization, and command injection vulnerabilities particularly found in TVs, Smart Home Security systems and more. There are additional problems with mobile apps, whereby if the app is not binary protected, it can be decompiled. Moreover, mobile app updates are often carried out using HTTP without integrity and signature checks.

3. **Hardware**, particularly with regards to personal IoT devices. Even if their intention is not malicious, most personal devices do not have built-in security sufficient for enterprise use, which may allow them to be used to infiltrate or take down corporate networks if connected.

4. **Radio**, from typical frequencies to ZigBee, Bluetooth and WiFi, remain relatively easily decoded, and LTK and STK can be extracted.

IOTROOP / REAPER CONTINUES TO RECRUIT DEVICES TO CREATE ARMY OF 'SLEEPERS'

When enterprises invest in IoT systems, they should seek to incorporate security at the design phase, and plan vulnerability management measures and regular security updates even before connecting to the network. When they do carefully connect to a system, ongoing threat intelligence services can detect and mitigate exploits and malware before they can infiltrate a network. Overall, a higher level of security education for stakeholders – both consumers and businesses – will be the most effective way to remove the 'fear factor' from new technologies. For example, many embedded IoT devices retain default credentials, making them an easy target from the outset if they are not suitably reconfigured. The answer? Education. From intelligence services available at the enterprise level, to tips for consumers on how best to protect themselves and their devices, the best defense we have against threats against IoT is knowledge.

ATTACKS ON UNPROTECTED CONSUMER, HEALTHCARE AND INDUSTRIAL DEVICES COULD HAVE SIGNIFICANT REAL-WORLD IMPACT

In October 2017, researchers identified IoTroop or Reaper, a massive botnet that continues to recruit IoT devices in order to create an army of sleepers. Almost a million organizations were scanned, but the number of potentially infected devices was simply too large and uncertain to be identified.[18] It was also believed that the attack was being spread by the IoT devices themselves, and likely will result in a massive botnet DDoS attack unless fixes have been implemented in time. A key differentiator for this strain of malware was that it appeared to be exploiting multiple device vulnerabilities to infect them, instead of attempting to bruteforce their way in like 2016's Mirai botnet.

Clearly, this is potentially a huge concern for 2018. Attackers that infiltrate unprotected devices will be able to perform more DDoS attacks or brick the devices, as we have seen this year. Should these affect industrial or healthcare systems then the human impact will be considerable – a significant real-world effect from a digital crime.

CREDENTIAL THEFT

Credentials will continue to be stolen at a very high rate this year, since it remains an extremely profitable source of revenue for cybercriminals. Though high-profile ransomware attacks may have stolen some of the headlines in 2017, it is clear that both the actual sale of information on black markets and simply public exposure of a breach can have a catastrophic effect on a company's bottom line.

THE RISE OF THE CRIMINAL DATA-BROKER WILL TRADE IN COMPROMISED CREDENTIALS

NEITHER ORGANIZATIONS NOR INDIVIDUALS ARE SAFE

Given the success of the Equifax and Deloitte breaches, for example, we expect that companies who might be considered 'data brokers' will continue to be highly targeted. Those companies that hold PII information – think real-world information such as addresses and ID numbers, as well digital information that could potentially be damaging, like consumer's personal browsing histories – will likely be popular targets. In a similar vein, cybercriminals are harvesting the data gathered by botnets to carry out more targeted attacks – finding stolen credentials for an interesting target could lead to further compromise using data gathered by these botnets.

Indeed, many companies that hold this information are dangerously lacking in the appropriate cyberdefense tools, and this complacency may be their downfall in 2018. Corporate intrusion can be detected and prevented more effectively using targeted threat intelligence. By finding out where the holes are in advance of an attack, or at the very least identifying where the data has gone in real-time when a breach happens, can mitigate potential damage.

GDPR COMPLIANCE

REAL-TIME THREAT INTELLIGENCE CAN PREVENT, DETECT AND MITIGATE THREATS, PROTECTING YOU FROM THE WORST OF GDPR FINES

GDPR comes into force in May 2018, and will be a fundamental shift in how businesses of all shapes and sizes approach cybersecurity. Indeed, Article 25 of the regulation states that security measures must be baked into products from the outset, rather than sprinkled over the top after going to market. This sort of integration should minimize the financial and reputational costs in the event of a breach, and perhaps even encourage a step-change for the way in which businesses view cybersecurity more generally.

Under GDPR, data breaches will be among the most serious issues a company can face. An organization in breach of GDPR can be fined up to 4 percent of its annual global turnover, or €20 million – whichever is greater. This is the maximum fine that can be levied against the most serious infringements (when a high-risk breach happens, and it is also found that the corporation had no appropriate measures in place, such as real-time intelligence gathering). Unfortunately, data breaches happen continuously and can have a negative financial, operational and reputational effect, often simultaneously. GDPR adds a regulatory impact. When it comes to Data Intrusion, it is a simple fact that is it not if you get breached, but rather when.

Cyberthreat intelligence technology can help in the prevention, detection and remediation of data breaches under GDPR by reducing the chances of a personal data breach occurring, mitigating the effects of a breach and lowering costs incurred. In fact, we see the goal of GDPR to ensure that companies become more committed to the protection of their personal data assets through clear requirements and obligations, and harsh penalties for non-compliance. However, Blueliv foresees a side effect of GDPR. Given the magnitude of potential fines, the threat of a reported data breach will become even more lucrative to cybercriminals. We expect an increased in frequency of data breaches by those who seek to exploit this fear and capitalize on financial opportunities.

Our GDPR whitepaper examines the impact of the legislation in depth.

EDUCATION AND INTELLIGENCE SHARING – WE'RE ALL IN THIS TOGETHER!

Addressing the cyberskills gap is a crucial issue to be addressed this year. Under no circumstances should an opsec team be the only group within a company that knows how to identify a malicious email, for example. Encouragingly, many companies are becoming increasingly conscious that security awareness at all levels is key to protecting their perimeters. Indeed, you are only as strong as your weakest link, so practicing cyber hygiene at all levels, combined with awareness-promotion on a continuous basis will help organizations defend themselves better. Moreover, we know from our 2017 landscaping that cybercriminals are not resting on their laurels after successful attacks. They are constantly seeking to improve and innovate, which means the defenders need to keep up too. Measuring the progress and maturity of cyberdefense systems on a regular basis, and complementing it with services such as threat intelligence will help you protect your organization from the outside in, and maintain a robust security posture to prevent attacks.

ADDRESS THE CYBERSKILLS GAP

EDUCATE EMPLOYEES AND EXECUTIVES

REGULARLY ASSESS AND MEASURE YOUR CYBERDEFENSES

SHARE, SHARE, SHARE INTELLIGENCE

As the landscape evolves, automation will help us respond and scale quicker. However, as in all industries, this relies on the quality of data that you start off with. In order to build the most effective defenses, organizations must share intelligence as openly as possible – a hivemind of cybersecurity professionals fighting the bad guys is infinitely better than siloing ourselves. While intel sharing has been around for a long time, driven by researchers, professionals and governments alike, it has been a relatively slow process. Indeed, a reluctance to share certain data has been founded on fear of reputational damage, legal action or publicizing vulnerabilities. However, it is our opinion that the positives outweigh the negatives here. **Blueliv's** Threat Exchange Network, for example, is a global community of thousands of cybersecurity experts sharing the latest news, views, IOCs and more – united in the fight against cybercrime. A final point to note: it is clear that the bad guys collaborate between themselves, sharing code, handing over infections, even sharing stolen credentials in exchange for other servers. If we don't collaborate on our side, then we'll lose the war.

Blueliv.

AFTERWORD

06

Blueliv.

Despite cybersecurity companies repeating the mantra since their inception, security must be baked in from the outset, not simply an afterthought. It would not be surprising, given the events of 2017, that a previously unforeseen attack caused a meltdown like we've never seen. All of us need to prepare for the worst by using the tools we have at our disposal.

Modular, scalable threat intelligence from Blueliv is a good start. We scour the open, deep and dark web to deliver fresh, automated and actionable threat intelligence to organizations, helping to protect their networks from the outside in. Our scalable cloud-based platform – Threat Compass – turns global threat data into sophisticated and relevant intelligence, enabling organizations to reduce their risk, save time and maximize resource by improving their incident response performance with real-time intelligence. Our solution is bespoke to each customer, highly modular and has the fastest deployment on the market. Threat Compass delivers threat intelligence through ten targeted modules with more to be added in 2018.

Join us in the fight against cybercrime

REFERENCES

1 https://www.forbes.com/sites/gilpress/2017/11/26/60-cybersecurity-predictions-for-2018/

2 https://enisa.europa.eu/publications/enisa-threat-landscape-report-2017

3 https://www.bleepingcomputer.com/news/security/the-number-of-iot-botnet-candc-servers-doubled-in-2017/

4 https://www.scmagazine.com/ramnit-botnet-spotted-in-google-play-but-poses-limited-threat/article/703854/

5 https://vms.drweb.com/search/?q=Trojan.PWS.Sphinx.2

6 https://threatpost.com/revamped-nukebot-malware-changes-targets-adds-functions/127707/

7 https://threatpost.com/us-government-site-removes-link-to-cerber-ransomware-downloader/127767/

8 https://www.scmagazine.com/cerber-most-prolific-ransomware-family-spawns-new-iteration/article/654788/

9 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/delving-into-the-world-of-business-email-compromise-bec

10 https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails

11 https://krebsonsecurity.com/2017/09/source-deloitte-breach-affected-all-company-email-admin-accounts/

12 https://www.bleepingcomputer.com/news/security/a-hacking-group-is-already-exploiting-the-office-equation-editor-bug/

13 https://www.trustwave.com/Resources/SpiderLabs-Blog/Post-Soviet-Bank-Heists---A-Hybrid-Cybercrime-Study/

14 https://www.wired.com/2017/05/close-look-notorious-apt32-hacking-group-action/

15 https://www.volexity.com/blog/2017/11/06/oceanlotus-blossoms-mass-digital-surveillance-and-exploitation-of-asean-nations-the-media-human-rights-and-civil-society/

16 https://www.csoonline.com/article/3244924/data-protection/2018-cybersecurity-trends-and-predictions.html

17 https://www.gartner.com/newsroom/id/3598917

18 https://www.infosecurity-magazine.com/news/reaper-botnet-has-come-for-the/

About Blueliv.

Blueliv is a leading cyberthreat intelligence provider with a world-class in-house threat Intelligence team. We scour the web to deliver fresh, automated and actionable threat intelligence to organizations across multiple industries to protect their networks from the outside in.

Our scalable cloud-based platform turns global threat data into actionable intelligence, enabling organizations to save time and resource by improving their incident response performance and empowering their Security Operations team with real-time intelligence.

Quantify and qualify malicious attack vectors with our plug and play MRTI feed; delivered in STIX/TAXII standard, integration is easy. Start detecting external threats and join the fight against cybercrime today.

Follow Us

twitter.com/blueliv

linkedin.com/company/blueliv

CYBERSECURITY BREAKTHROUGH AWARD 2018

GO IGNITE 2016

Gartner 2015 CoolVendor