CHECK POINT
RESEARCH

2017

Global Cyber Attack Trends Report

Check Point®
SOFTWARE TECHNOLOGIES LTD

The Check Point 2017 Global Threat Intelligence Trends Report

Introduction

2017 has been an incredible year for the cyber security industry. With attacks reaching ever higher scales and increasing levels of innovation there seems to be no stop to the cat and mouse game taking place between threat actors and security experts.

Threat actors look to stay ahead in this chase in order not to be caught, and so far they are succeeding. There is a lot that organizations still need to do to prevent from being attacked. Indeed, the trends we observed in the first half of 2017, and even 2016, continued through the second half of the year too, as well as some more new and surprising ones.

One of the top continuous trends is ransomware. This is still a leading attack vector, used for both global attacks such as the WannaCry cyber-attack, seen earlier in the year, and targeted attacks against specific organizations.

Another old, yet powerful attack vector is Malspam-based campaigns. Aggressive spam email distribution and devious scam operations are still flooding consumers worldwide, and have recently taken over market share previously occupied by exploit kits.

The Shadow Brokers leak of alleged NSA cyber tools has also cast a long shadow over the global InfoSec ecosystem during the second half of 2017. Due to this leak, implementation of the EternalBlue and EternalRomance SMB exploits has led to a significant increase in the use of lateral movement to spread throughout infected networks, causing dramatic damage in massive attacks.

Lastly, a few of the most sophisticated malware observed during the last couple of years, such as Mirai IoT botnet and WannaCry ransomware, have made some unwanted comebacks. This is due many attackers choose to utilizing certain elements of them to create a new and improved versions, instead of developing a new malware from scratch.

The second half of 2017 has also featured some new and interesting trends. Crypto-miners have taken the world by storm and became a favorite monetizing attack vector. While this is not an entirely new malware type, the increasing popularity and value of cryptocurrency has led to a significant increase in the distribution of crypto-mining malware. The crypto-mining frenzy has also given birth to a new type of crypto-mining malware, web-based crypto miners. Along with feasting on a victim's computational resources, this malware has also nibbled away a respectful share of the online advertisement market.

The Check Point Global Threat Intelligence Trends Report provides a comprehensive overview of the malware landscape during the past few years, as well as predictions of the trends that will stand out during 2018. The report is based on threat intelligence data drawn from the ThreatCloud World Cyber Threat Map between January and December 2017.

Global Trends

Cryptocurrency Miners Frenzy

One of the most significant trends of the last few months which took the world by storm is the incredibly rapid rise of cryptocurrency miners, especially the web-based type. While crypto miners are common tools used by individuals to mine their own coins, the rising public interest in virtual currencies has slowed the mining process, which depends directly on the number of currency holders.

This slowdown has increased the computational power needed to mine crypto-coins, which led cyber criminals to think of creative ways to channel the computation resources of the general public in their favor. Over the years, and especially during 2017, we have witnessed a number of campaigns that spread crypto miners via malspam and exploit kits; nowadays though, a new method is taking over the internet – online cryptocurrency miners are injected, both knowingly and unknowingly, to some top websites, without notifying the user and without limiting the CPU power consumed. While website owners may choose to replace ads with cryptocurrency miners in order to improve the customer's experience, it poses a great danger to the consumers. The miners have a

clear interest to increase the percentage of the computer resources consumed, and perhaps even leverage access and elevate their privileges over the user's machine. The increase in the number of organizations infected by crypto-miners was observed by Check Point global sensors as well, and reached its peak in December 2017, with 20.5% of organizations hit by crypto-miners.

Decrease in Exploit Kits

Up until a year ago, Exploit kits used to be a prime attack vector. They could be purchased in various Darknet and clear web forums, easily managed by unskilled actors via a comprehensive panel, and the prominent ones, such as Nuclear and Angler, were always up-to-date with newly-found vulnerabilities.

During 2017 however, the use of exploit kits has significantly decreased, and here is why.

The exploited platforms have become more secure. Common web browsers, such as Internet Explorer for example, have implemented new security measures, making it hard for even the more skilled attackers, to discover new vulnerabilities and develop new exploits. Moreover, the rapid response to new vulnerabilities exposed in these products by security vendors and leading browser developers, along with automatic updates of newer versions, have significantly shortened the shelf life of new exploits.

As zero-day vulnerabilities in web browsers are harder to find today, those that are, are rarely published. Instead, they are sold to the highest bidder on one of many Bug Bounty frameworks. This may be either to the platform owner, to an exploit acquisition platform such as Zerodium, or sold even to powerful nation-state agencies.

Another important cause is the decline in the number of zero-day Flash vulnerabilities exposed throughout the past year. Less than 70 Flash vulnerabilities were exposed during 2017, whereas some 266 vulnerabilities were exposed the year before. Exploit kits cannot usually afford to purchase zero-day exploits. This means they are left with older exploits, which are blocked by most web browsers. While there are still active exploit kits, the detailed process has led to a gradual decrease in the infection rate of drive-by attacks, and, as a result, to a reduction in the actual use

and development of new kits. We must note that while drive-by attacks are decreasing however, malvertising campaigns are still a prominent part of the infection chain, used as redirectors to the landing page in which an infection takes place.

Increase in Scam Operations and Malspam

The infection landscape, once heavily occupied by drive-by attacks such as exploit kits, now clearly relies on malspam. This includes various phishing techniques, scam operations and aggressive spam email distribution.

2017 was a particularly interesting year in the malicious email distribution market in its various forms, as some distributers were taken down but others once again reared their heads.

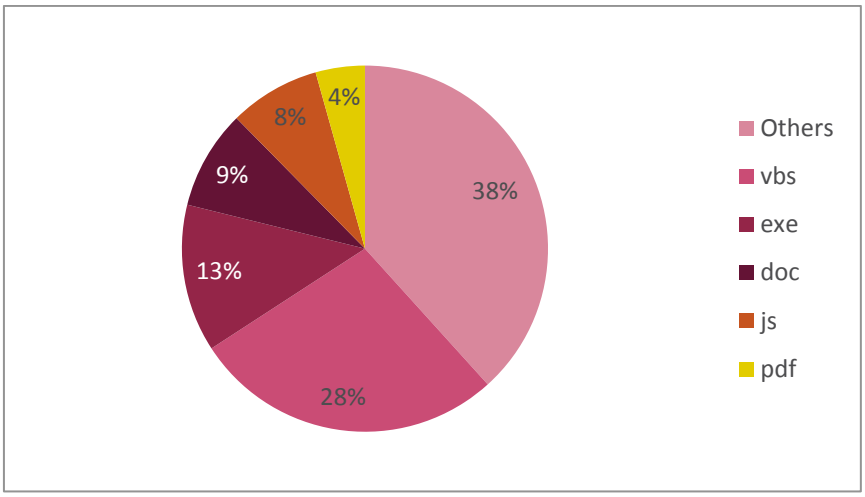
Throughout 2017, the ratio between infections based on HTTP and STMP shifted in favor of SMTP, from 55% in the first half of 2017 to 62% in the second. The increase in the popularity of these distribution methods attracted skilled threat actors who brought with them an advanced practice that included various exploitations of vulnerabilities in documents, especially in Microsoft Office.

Thus, unlike before, high-quality scam operations are adopted by serious attackers in order to carry out massive rather than minor targeted attacks, spreading unsophisticated malware.

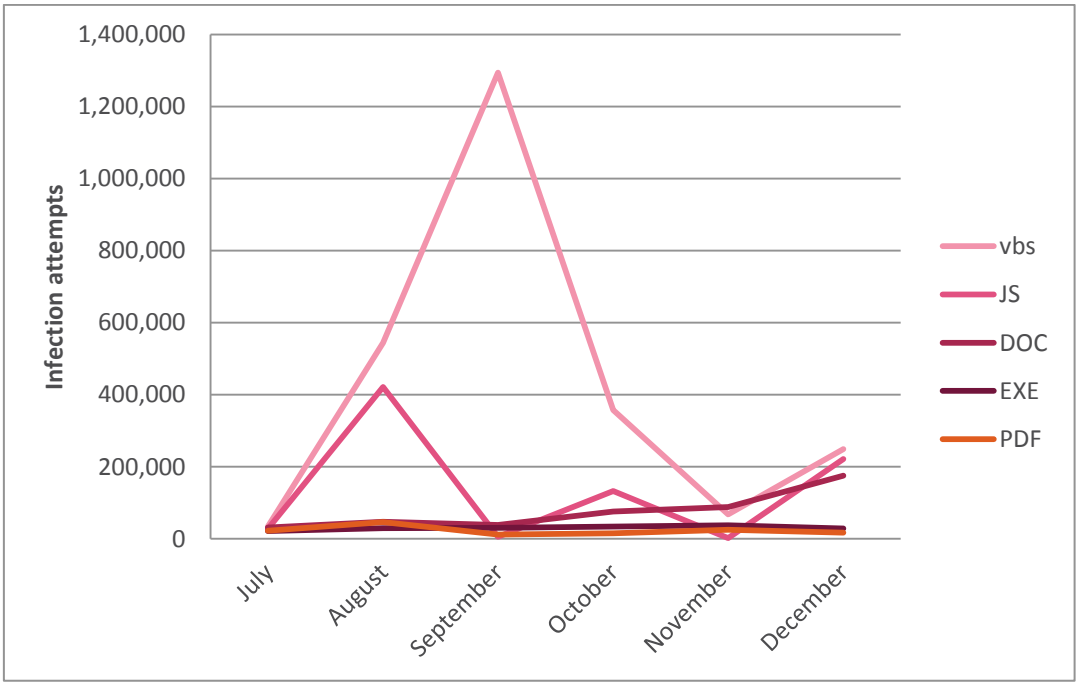
The growth of this market has encouraged the exploitation and utilization of vulnerabilities, especially in Microsoft Office. We have coped with new vulnerabilities time and again, from the RTF CVE-2017-0199 vulnerability, to mouse hovering and the famous DDE exploitation. We have also seen usage of a wide variety of file types, many times of esoteric versions of key products, especially in Microsoft Office and Adobe.

New file types such as .xlam and .xlb have also been observed in the last year, used to pull and execute second stage malware. Some of the campaigns were well-accustomed to the targets on the other side of the internet, and some used broader themes, hoping to take advantage of anyone who is not aware of them.

Top Malicious File Types – H2 2017



File Type Activity Rate Over Time – H2 2017



Lateral Movement Prominence

The term lateral movement represents an attacker's ability to spread throughout an organization's infrastructure based on a single gate to the network.

While a shift in the common infection method used by attackers these days has been observed, we have witnessed both an increase in the use lateral movement techniques and some new, interesting lateral movement methods.

Wannacry, NotPetya and BadRabbit are a few examples of prominent malware families that used lateral movement during the past year. All three families were used in large-scale campaigns targeting enterprises, civil companies or government-related organizations. Examples in the IoT arena include IoTroop botnet, and a botnet targeting Huawei home routers which delivers the Satori payload, both revealed by Check Point researchers.

The greatest contribution to the significant rise in the use of this technique came from the release of alleged NSA tools by the Shadow Brokers group last April. Two of which, EternalBlue and EternalRomance, exploit vulnerabilities in Microsoft's implementation of the Server Message Block (SMB) protocol.

Both tools are used to gain access to a vulnerable system, and then seek additional vulnerable systems within its network. The vulnerable machines found would then be infected in the same way.

A great advantage of infection via lateral movement is the ability of this technique to influence an entire organization, via a single entry point. In this way, unpatched or unprotected systems can be taken down in no time, leaving an entire organization paralyzed.

Mix and Match Malware

While hundreds of new malware families are discovered every year, many of those share close ties to an old yet successful malware family. These versions use pieces of code originating in the old malware, and sometimes are even a hybrid product of mixing code fragments from several older payloads. The aim is to form an improved model.

In August 2016, one of the most significant botnets of recent years, Mirai, made headlines when it recruited vulnerable Internet of Things (IoT) devices to its botnet, and used them to launch multiple high-volume Distributed Denial of Service (DDoS) attacks.

Over a year later, two additional significant IoT botnets, IoTroop and Satori, were revealed by Check Point researchers. Both rapidly recruited hundreds of thousands of bots. Both botnets demonstrated better infection and C&C communication capabilities. This is not a great surprise given that they were both improved versions of Mirai.

For example, IoTroop shares an extensive code base with Mirai, but while Mirai botnet uses brute force password cracking to access the infected device, IoTroop utilizes a vulnerability scanning functionality, which requires fewer resources and reduces the detection rate.

Additional infamous examples are Wannacry and NotPetya, two ransomware-worms that utilize alleged leaked NSA tools, DoublePulsar backdoor and EternalBlue exploit.

Malware code reuse saves time and enables attackers to focus on tailoring a successful campaign, improving evasion techniques and of course, initiating a campaign as quickly and effectively as possible. This trend also opens 'career' options for hackers to those who are less technically-advanced, as they can simply copy and paste code for their own usage. Importantly, more hackers directly leads to more hacking.

Mobile Botnets Now Used In DDoS Attacks

Ever since we found Viking Horde, the first widespread Android botnet on Google Play, we have long foreseen that the use of Android botnets for DDoS attack is just around the corner.

This year, a new mobile botnet called Wirex spread through Google Play. It was used to conduct volumetric DDoS attack at the application layer, shutting down websites globally. As it is easy to reach a widespread infection by imbedding malicious code in apps on Google Play, mobile botnets are the perfect weapon for mass DDoS attack, and will continue to trouble us in the future.

Mobile Malware Reaches the Enterprise Level

In the last year, we have witnessed several attacks directed at enterprises originating from mobile devices. Of these attacks, two types stand out.

The first is mobile devices acting as a proxy used to collect internal data from the enterprise's corporate network, like the MilkyDoor malware. The second type is mobile malware, such as the Switcher malware, that attempts to attack network elements (e.g. routers) to redirect a network's traffic to a malicious server under the attacker's control. This elaborate piece of code tries to guess the router's password, and then reconfigure its settings, thereby rerouting traffic from the internal network to the cybercriminal's servers.

Global Malware Statistics

Data comparisons presented in the following sections of this report are based on data drawn from the Check Point ThreatCloud Cyber Threat Map between July and December 2017.

Top Malware Families

Global

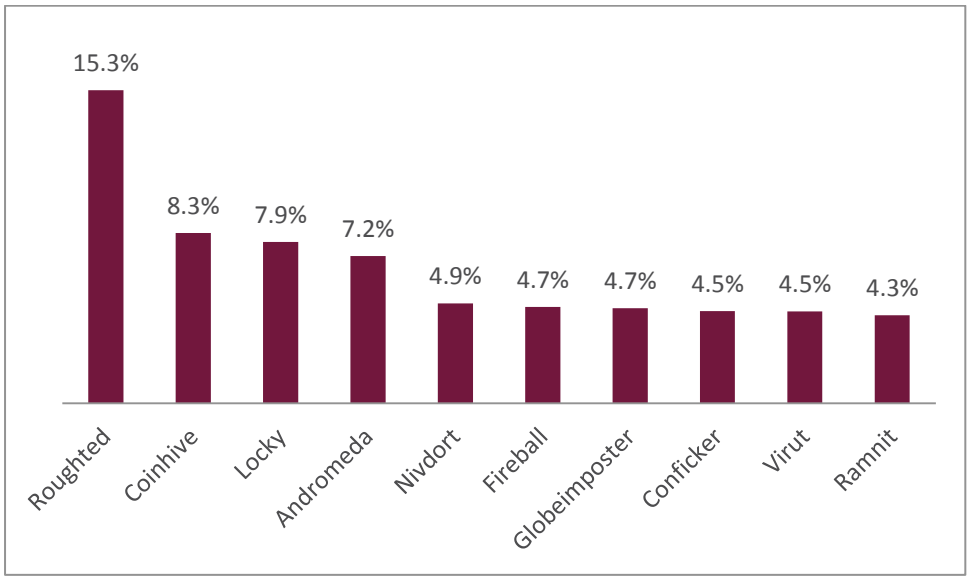


Figure 1: Most Prevalent Malware Globally: Percentage of corporate networks experiencing each malware type

For each of the regions below we present two graphs. The first details the most prevalent malware in that region, followed by a second graph that details the malware families with the highest presence in that region compared to others.

Americas

Figure 2: Most Prevalent Malware in the Americas

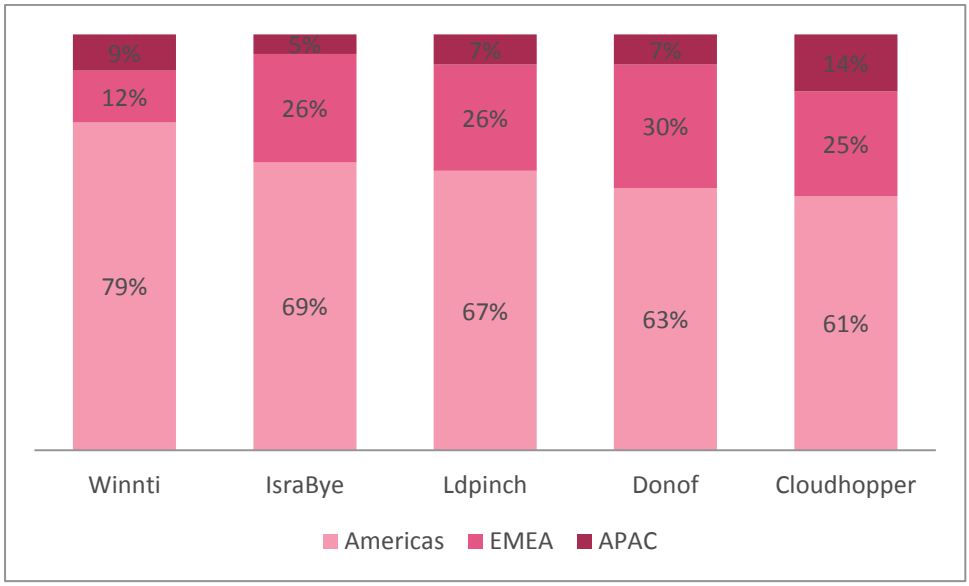


Figure 3: Top Targeted Malware in the Americas

Europe, Middle East and Africa (EMEA)

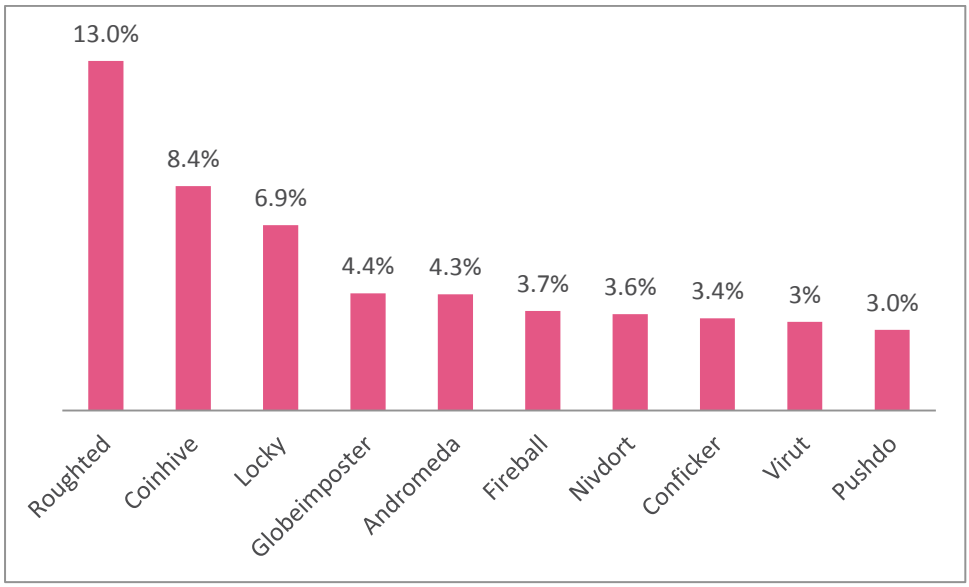


Figure 4: Most Prevalent Malware in EMEA

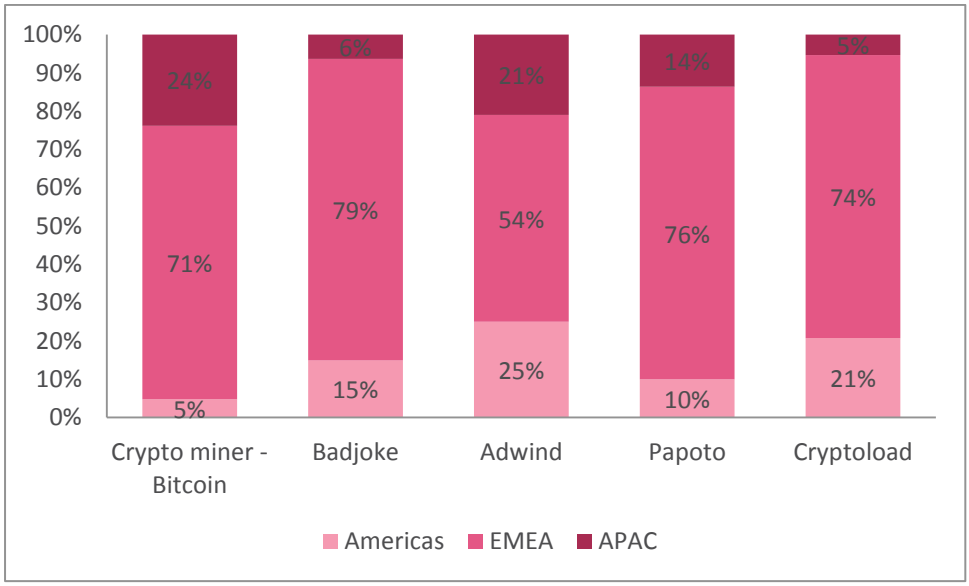


Figure 5: Top Targeted Malware in EMEA

Asia Pacific (APAC)

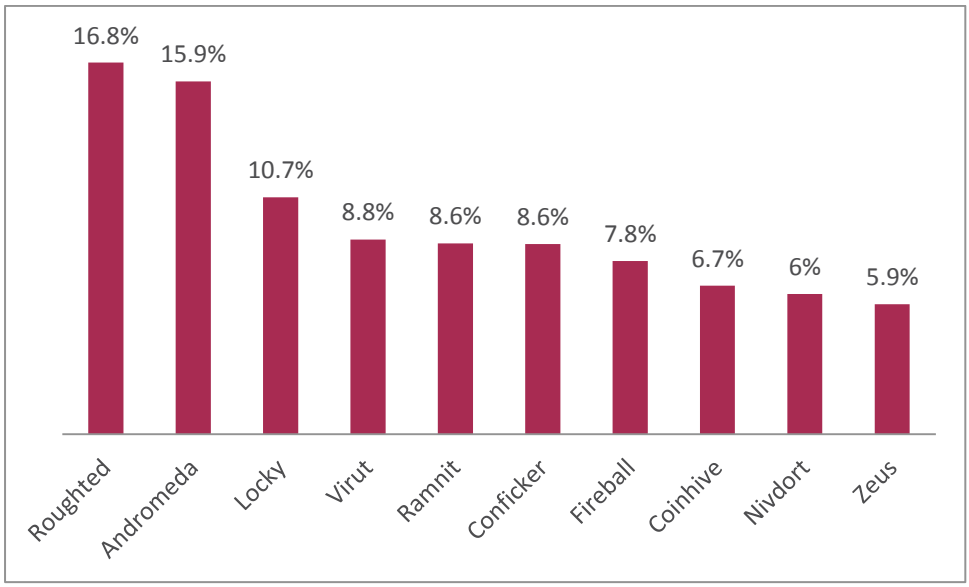


Figure 6: Most Prevalent Malware in APAC

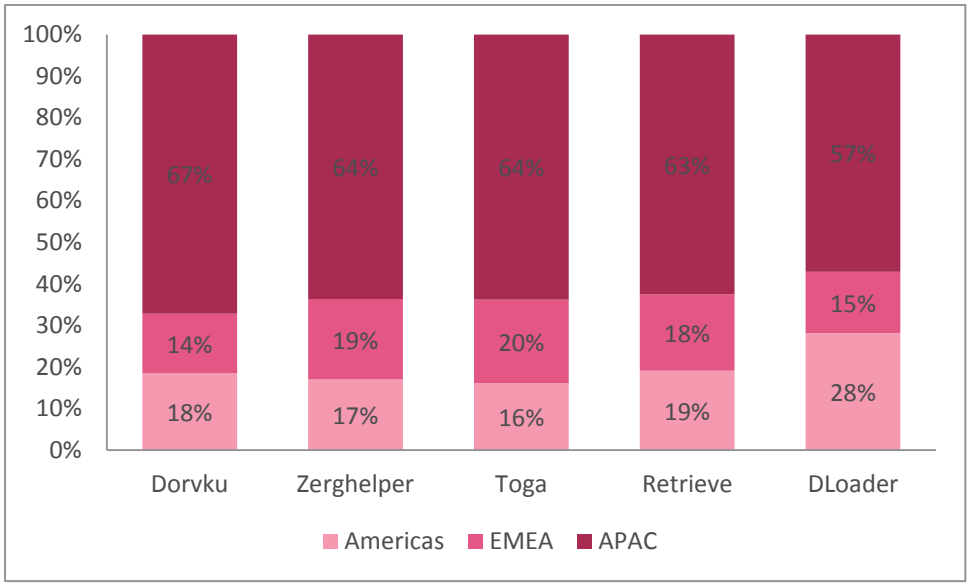


Figure 7: Top Targeted Malware in APAC

Global Analysis of Top Malware

- **CoinHive**, a web-based Crypto miner which mines the Monero cryptocurrency, was only launched last September and yet is already the second most popular malware globally, with 12% of the organizations worldwide hit by it. The reason for such a quick spread of the malware is most likely due to many websites, among them leading streaming and media portal, having integrated the CoinHive JavaScript as a possible replacement for online

advertisements, often without notifying the users and without limiting the amount of resources consumers by the miner. Notably, its classification as malware is subjective, as while most websites use it without their users' knowledge or consent, some might use it with full agreement by their users.

- **RoughTed**, a large-scale malvertising campaign used to serve malicious websites and payloads, maintained its fourth place position in the malware rankings of 2017. RoughTed began to spike in late May and at its peak in June had affected organizations in 150 different countries, mostly in the education, communications and retails & wholesale sector. In July, the campaign fell by over a third, from 28% of all corporate networks to 18%. RoughTed infection rates spiked throughout the year as attackers do not need to maintain a heavy distribution infrastructure. Instead, they only have to compromise one online ad provider to reach a wide range of infections.

- Although **Necurs** is currently one of the largest spam botnets in the world it did not land on the global top malware list, and only made it to the top malware rank of APAC. In September, Locky ransomware made a comeback to our monthly 'Most Wanted Malware' rankings thanks to Necurs spreading the ransomware. During the US Thanksgiving holiday in November, Necurs was used to distribute a relatively new ransomware, dubbed Scarab, in an aggressive spam email campaign.

Top Ransomware

Graphs in this section of the report represent the percentage of organizations that were affected by each ransomware. The graphs present a global view and also regional insights into the top ransomware.

Global

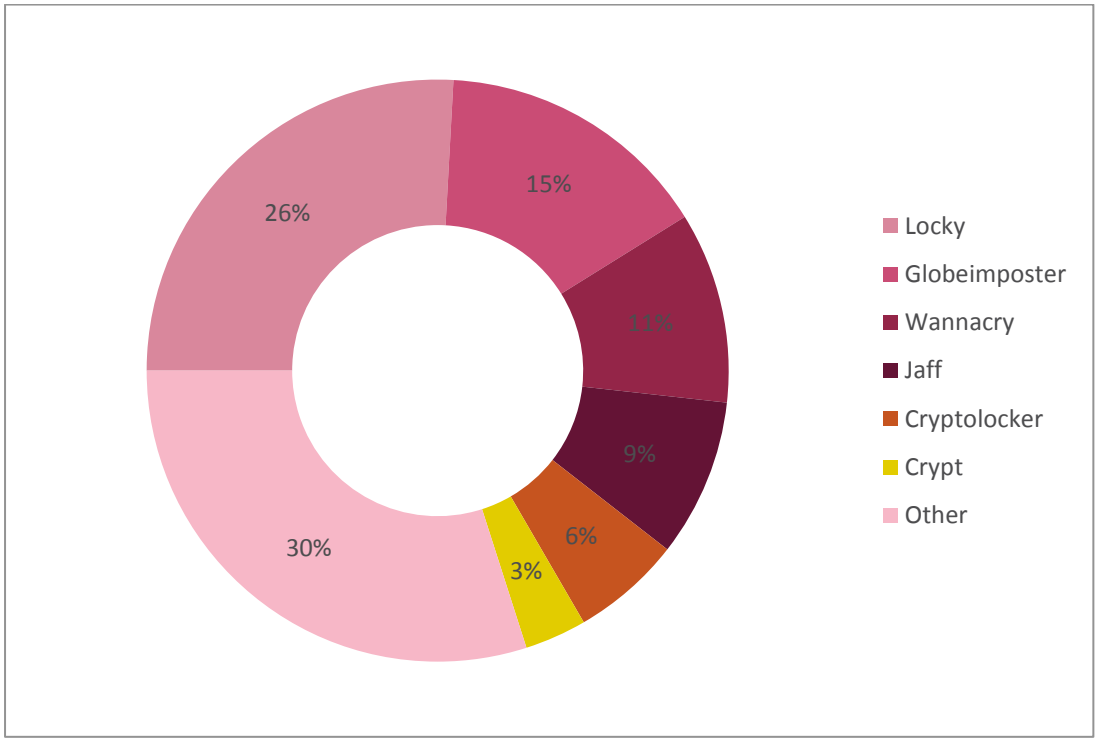


Figure 8: Most Prevalent Ransomware Globally

Americas

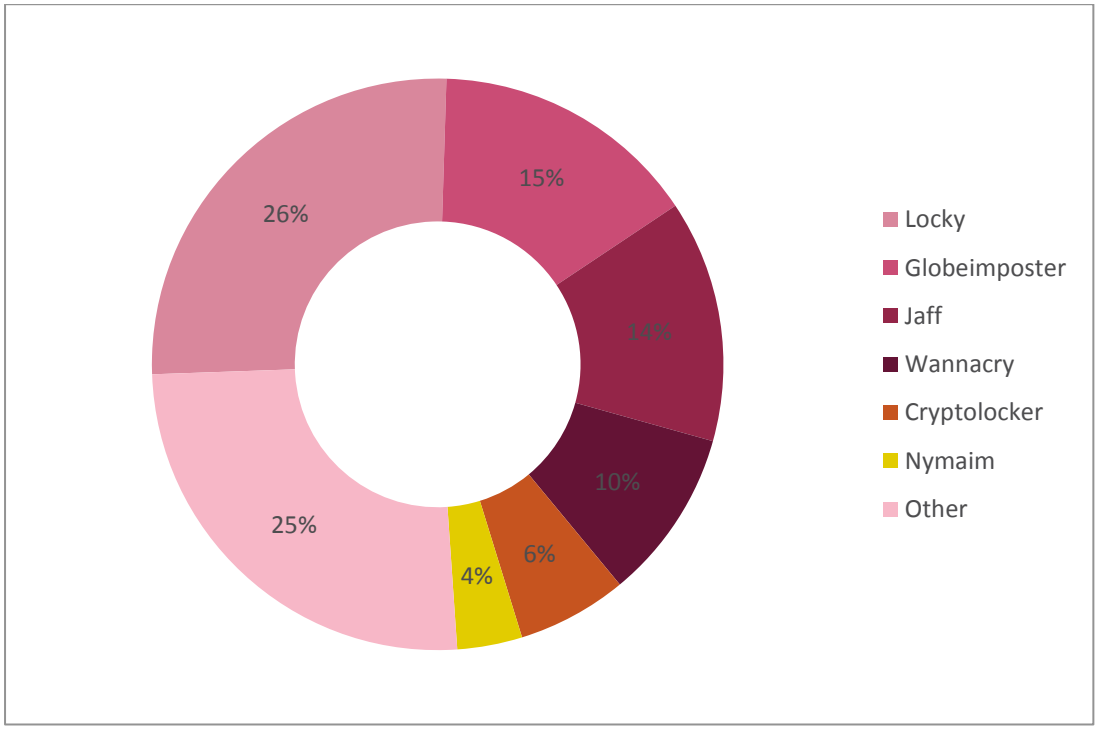


Figure 9: Most Prevalent Ransomware in the Americas

EMEA

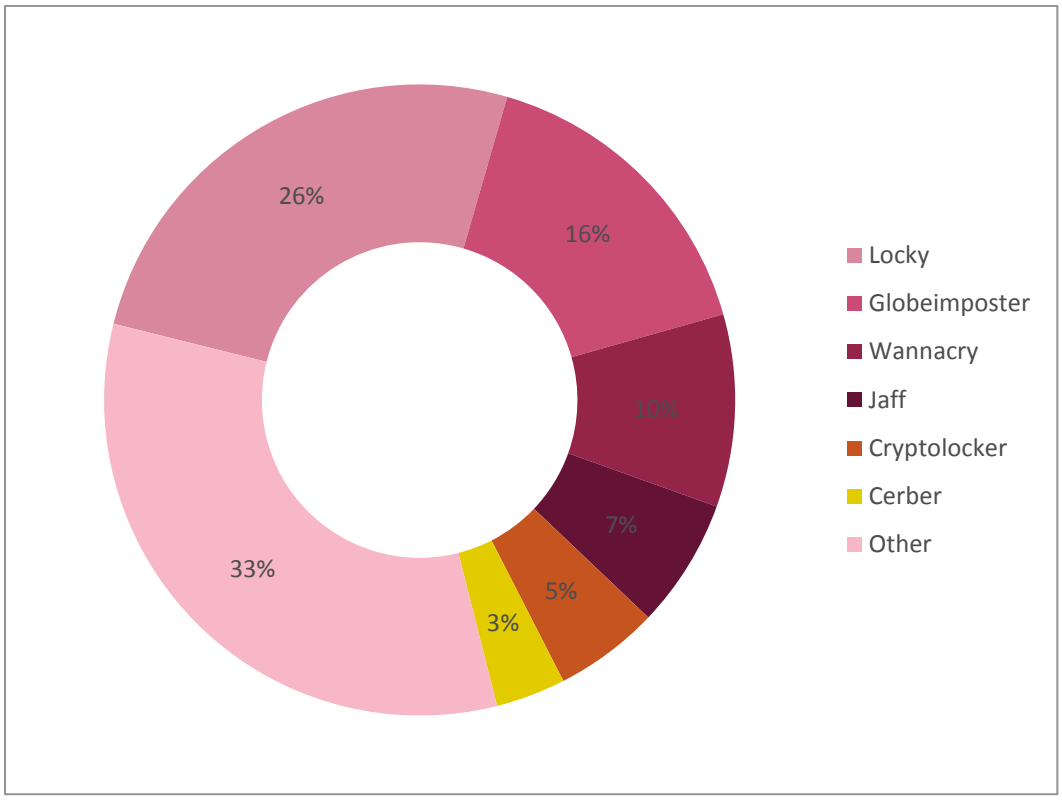


Figure 10: Most Prevalent Ransomware in EMEA

APAC

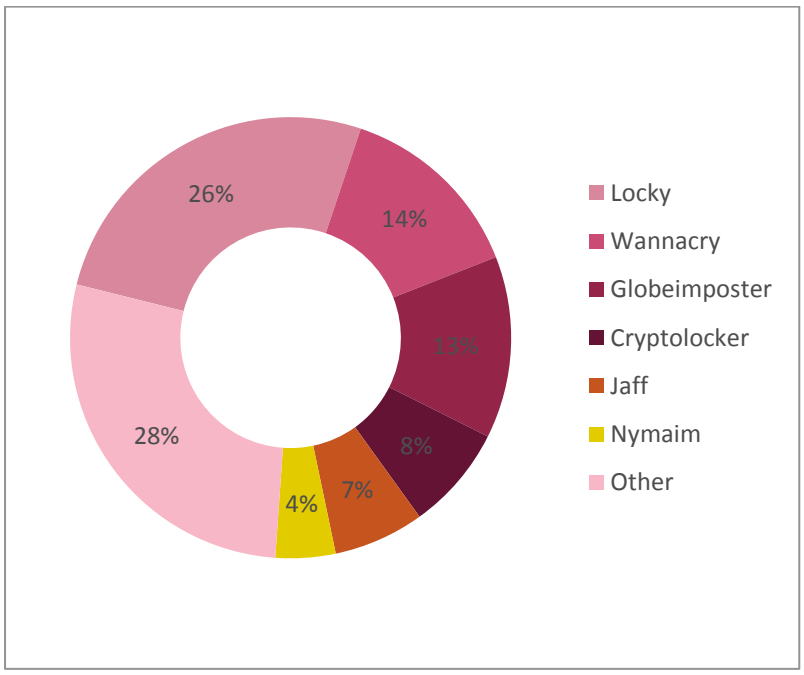


Figure 11: Most Prevalent Ransomware in APAC

Ransomware Global Analysis

- **Locky** ransomware, which first emerged in February 2016, has climbed back to the top global and regional ranks after starring in the ranks in the second half of 2016 and dropping in the first half of 2017. One of the most prominent ransomware in these rankings is **Globeimposter**, a variant of the Globe ransomware which is spread by spam and malvertising campaigns including the Necurs botnet. The ransomware only emerged in May 2017 and is already ranked third in the world, and second in EMEA and APAC.

Top Banking Malware

In this section of the report the graphs illustrate the percentage of organizations that were affected by each banking malware. The graphs provide global views and also regional insights into the top banking malware.

Global

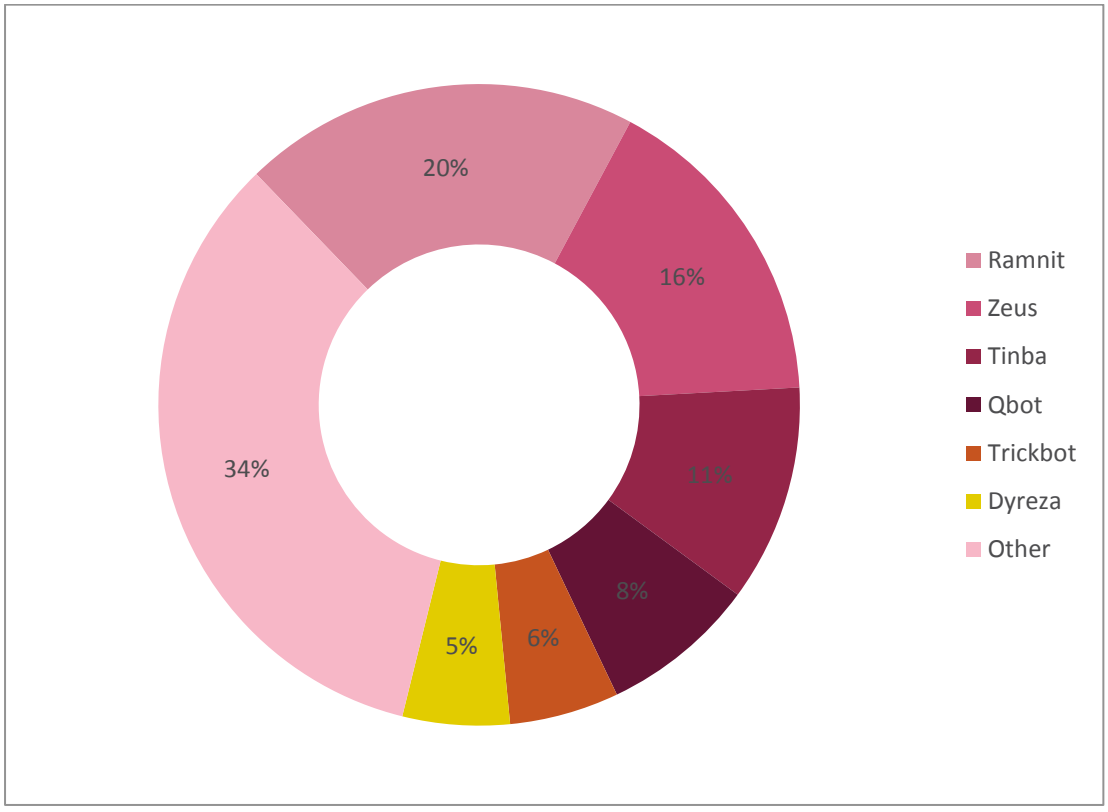


Figure 12: The Most Prevalent Banking Malware Globally

Americas

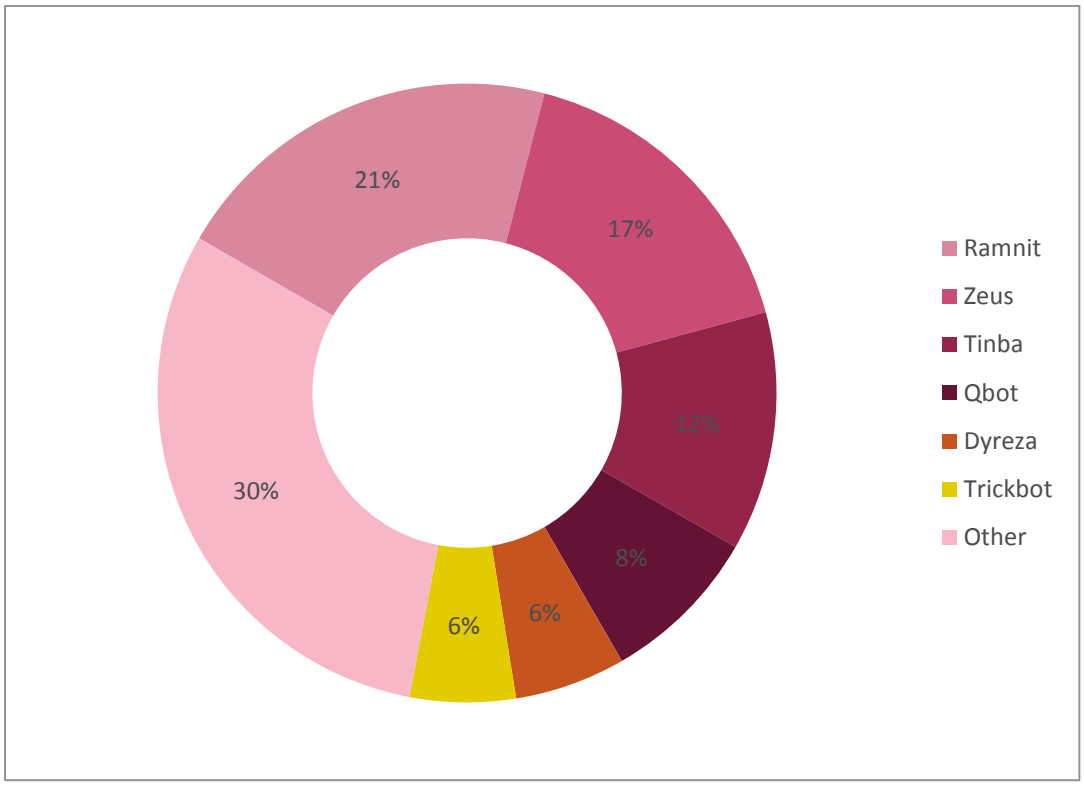


Figure 13: Most Prevalent Banking Malware in the Americas

EMEA

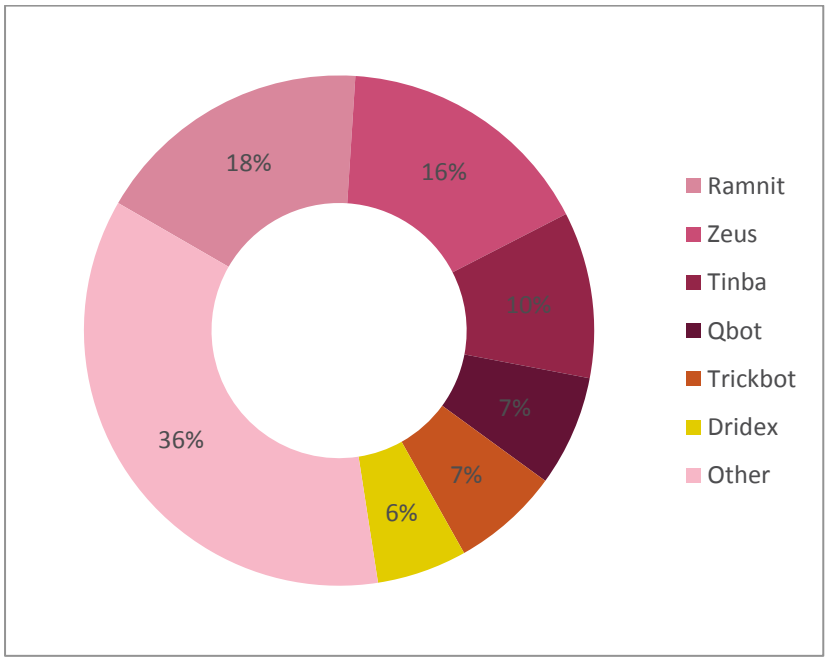


Figure 14: Most Prevalent Banking Malware in EMEA

APAC

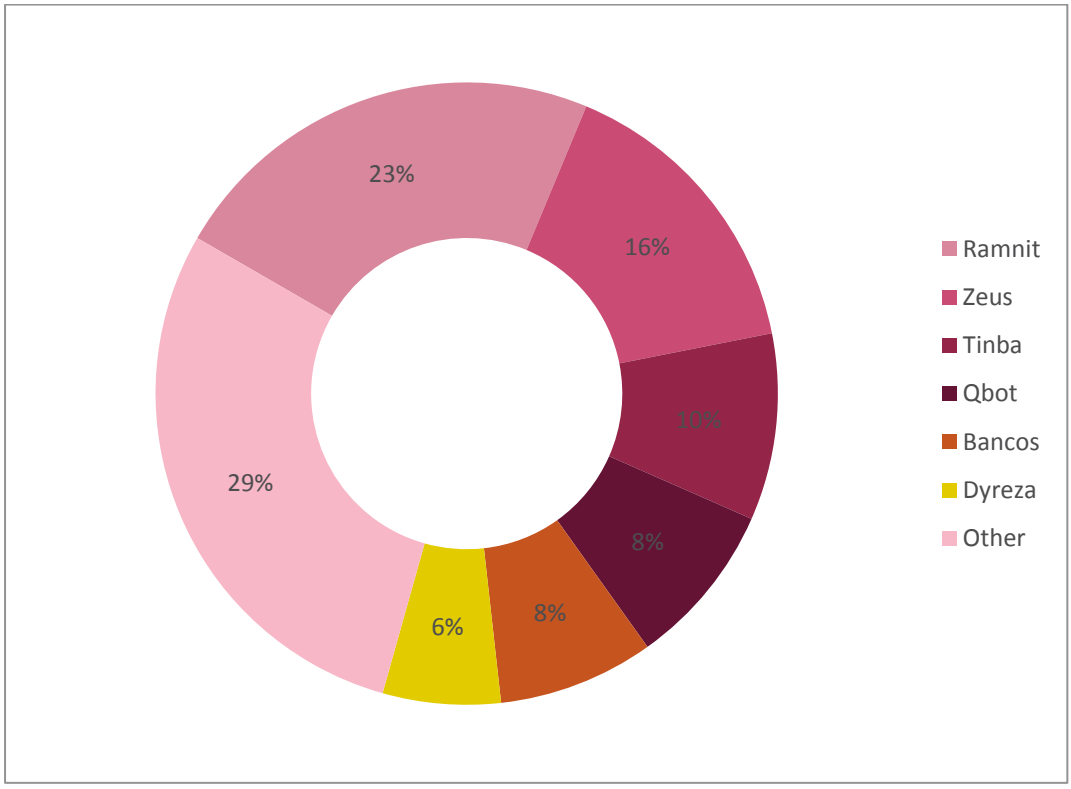


Figure 15: Most Prevalent Banking Malware in APAC

Banking Malware Global Analysis

One of the most prominent banking malware of the second half of 2017 is **Trickbot**. Similarly to Zeus and Ramnit, Trickbot recognizes that the victim is visiting a banking website, and then utilizes keylogging or web injects to harvest login credentials or more sensitive information such as PIN numbers. Trickbot emerged in 2016 but only made it to the top ranks in the second half of 2017, and has been heavily distributed by massive spam campaigns carrying malicious .docx files, especially during the middle of the year, but it is known for its use in SMB exploits for lateral movement among infected networks.

Top Mobile Malware

In this section of the report the graphs illustrate the percentage of organizations that were affected by each mobile malware. The graphs provide global views and also regional insights into the top mobile malware.

Global

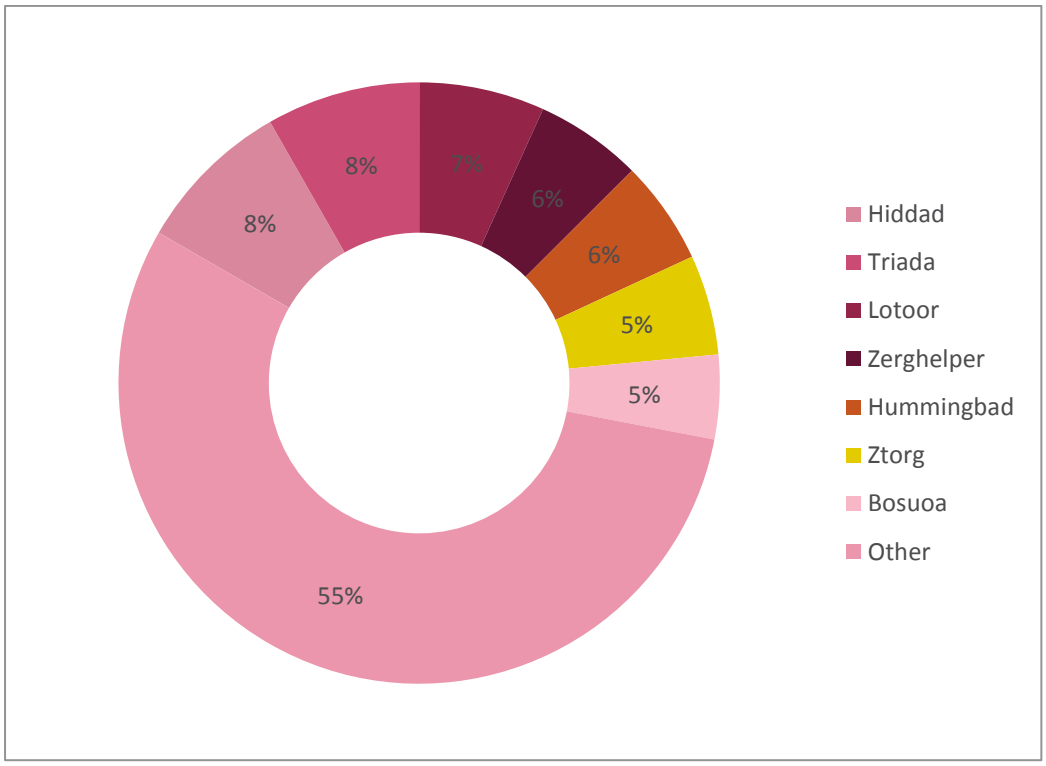


Figure 16: Top Mobile Malware Globally

Americas

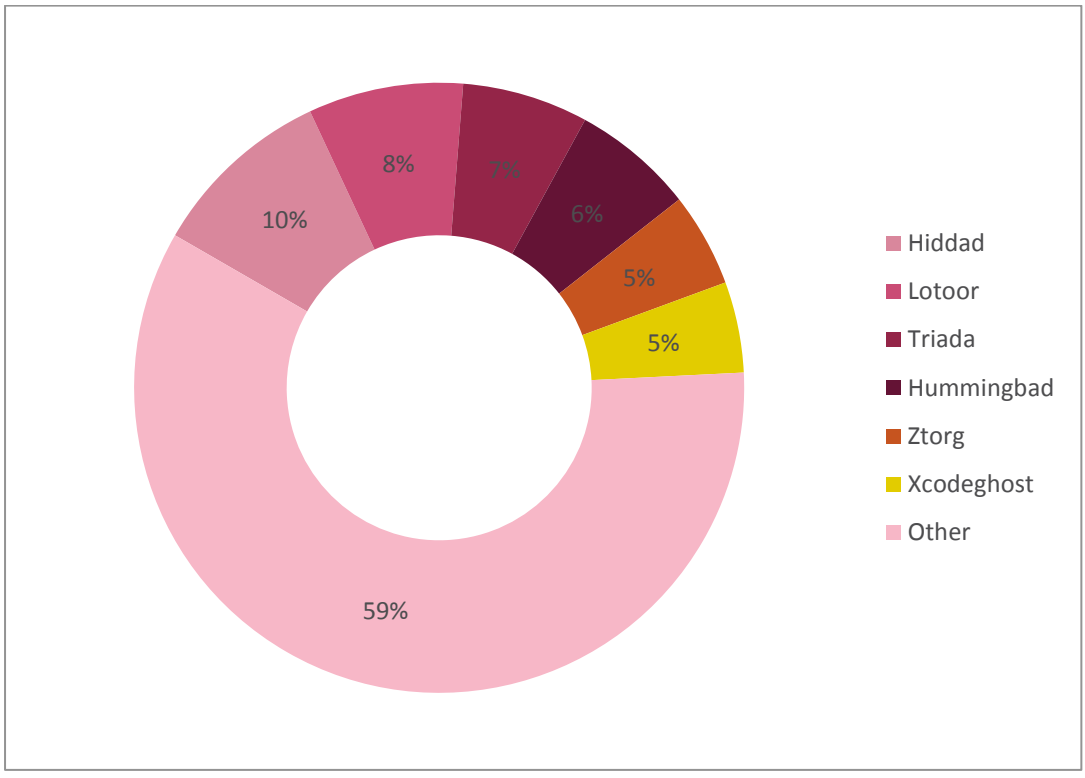


Figure 17: Top Mobile Malware in the Americas

EMEA

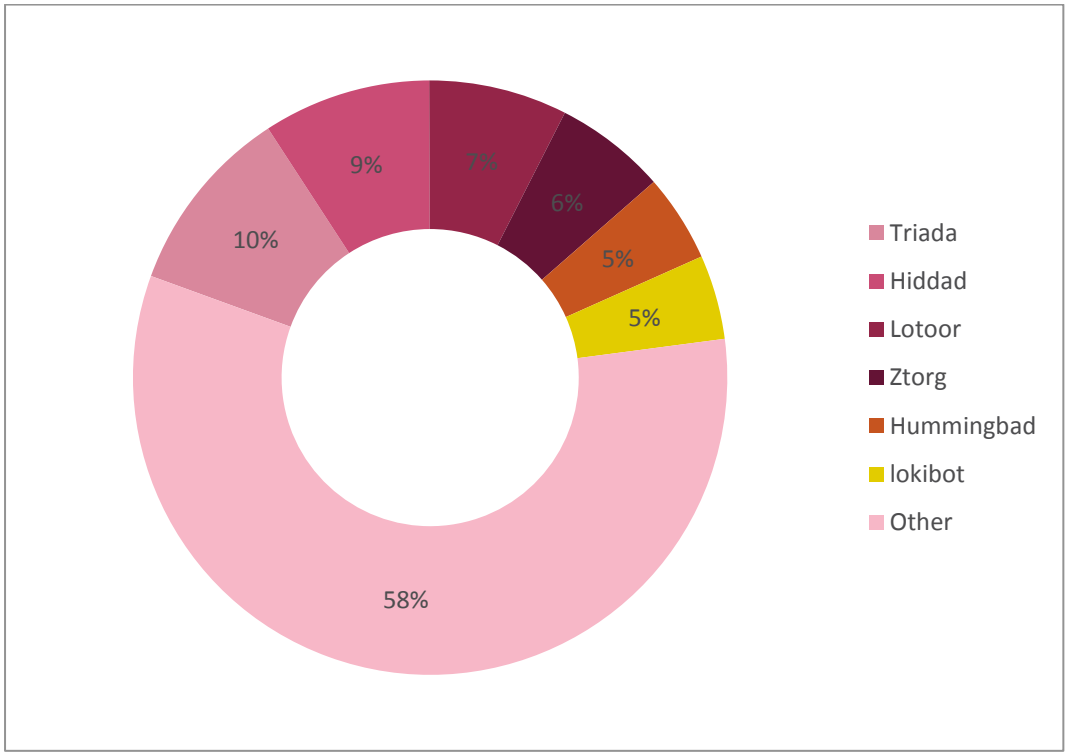


Figure 18: Top Mobile Malware in EMEA

APAC

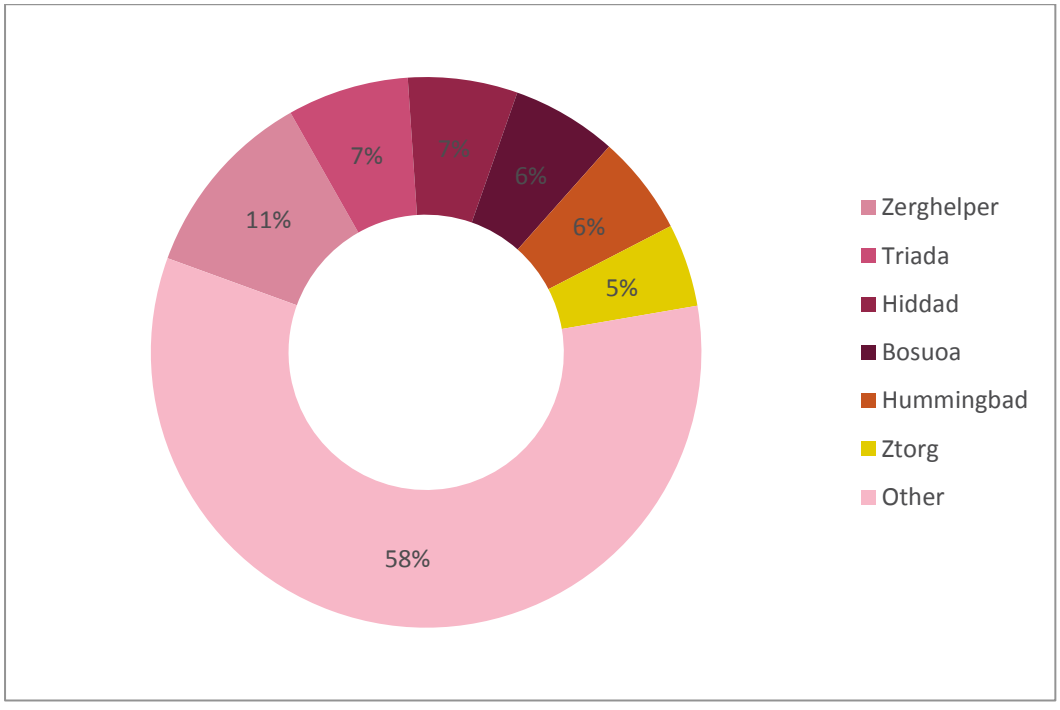


Figure 19: Top Mobile Malware in APAC

Mobile Malware Global Analysis

- **Hiddad**, an Android malware used mainly to display ads, first appeared in the top mobile ranks on the first half of the year, and has kept its place at the top of the global rankings and in the Americas. In parallel, two new mobile malware families entered the top ranks. First, **ZergHelper**, a malware which targets Chinese iOS users and managed to penetrate the App Store, is starring in the APAC top mobile malware rankings. Second, **Lokibot**, an Android banking malware and info-stealer which can turn into a ransomware, has entered the EMEA top rankings with 5% of the overall attacks.

Top Crypto Mining Malware

In this section of the report the graphs illustrate the percentage of organizations that were affected by each crypto mining malware. The graphs provide global views and also regional insight into the top crypto mining malware.

Global

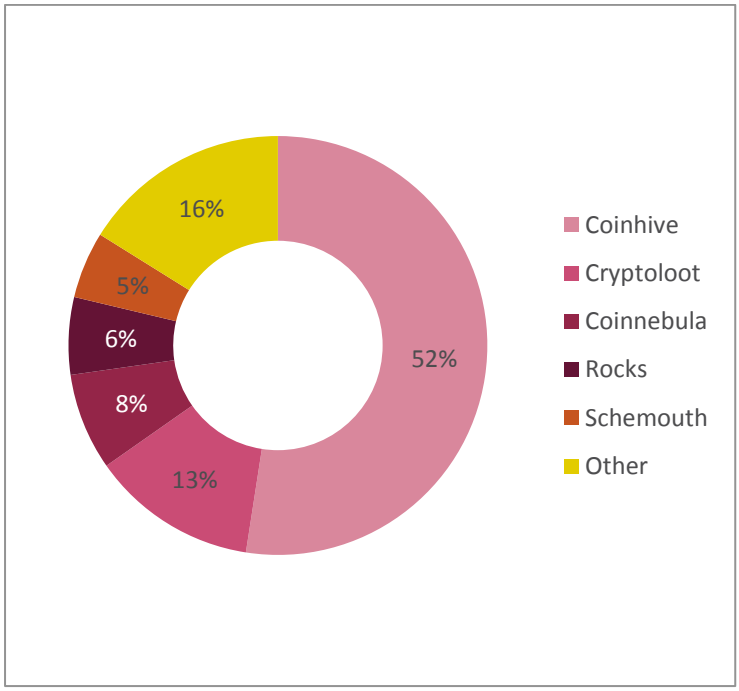


Figure 20: Top Crypto Mining Malware Globally

Americas

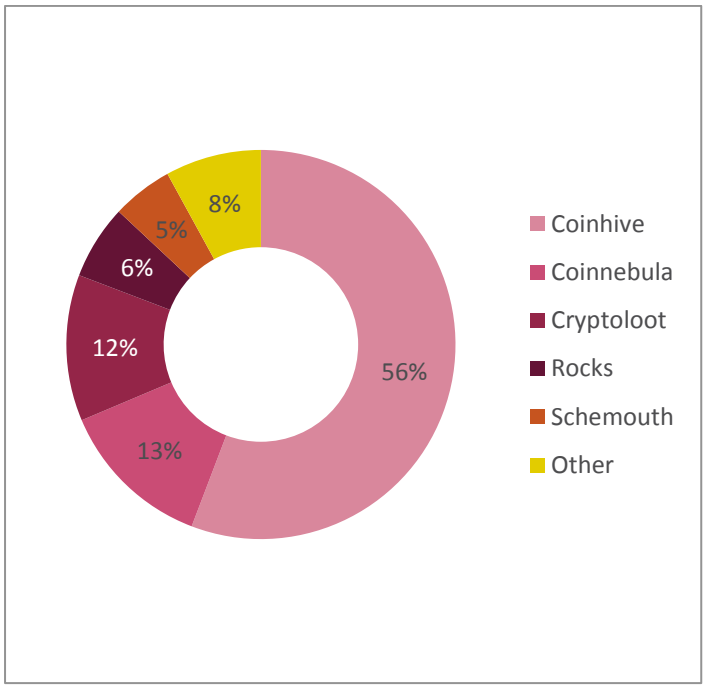


Figure 21: Top Crypto Mining Malware in the Americas

EMEA

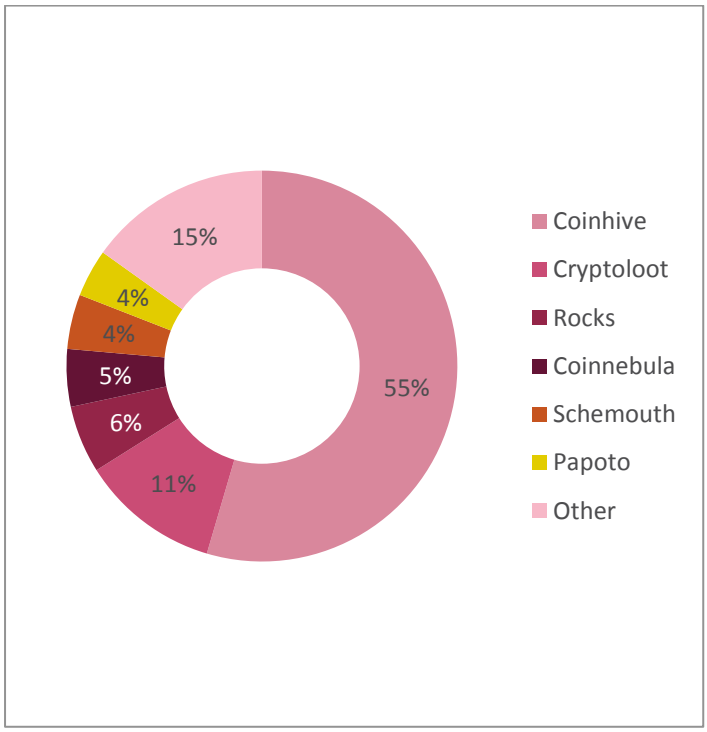


Figure 22: Top Crypto Mining Malware in EMEA

APAC

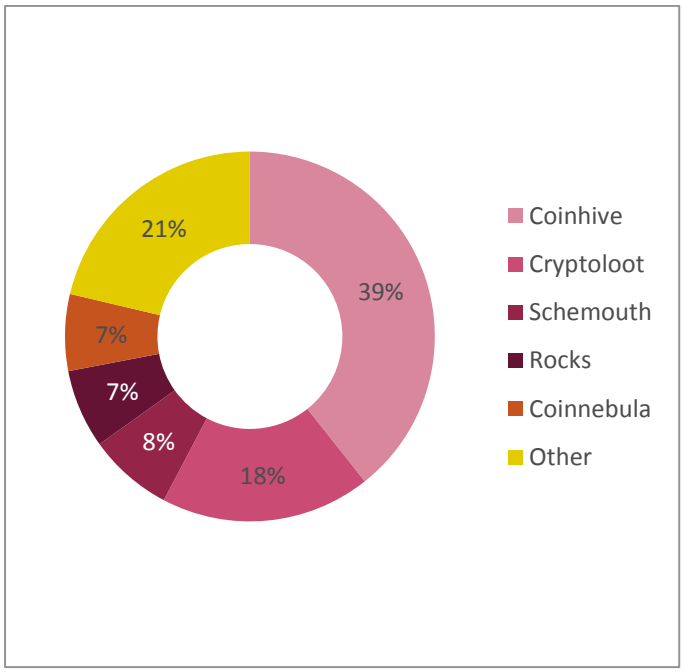


Figure 23: Top Crypto Mining Malware in APAC

Crypto Mining Malware Global Analysis

- **Crypto Loot**, the second most popular crypto-mining malware globally is a Javascript miner for Monero which functions very similarly to CoinHive and is even marketed as a CoinHive alternative. The malware only emerged in October, and its creators promise that running the miner on a website will go 'unnoticed by users' under certain conditions. Interestingly, while in the past crypto-miners were aimed at mining BitCoin, all miners that made it to our top list are mining for Monero.

Cyber Attack Categories by Region

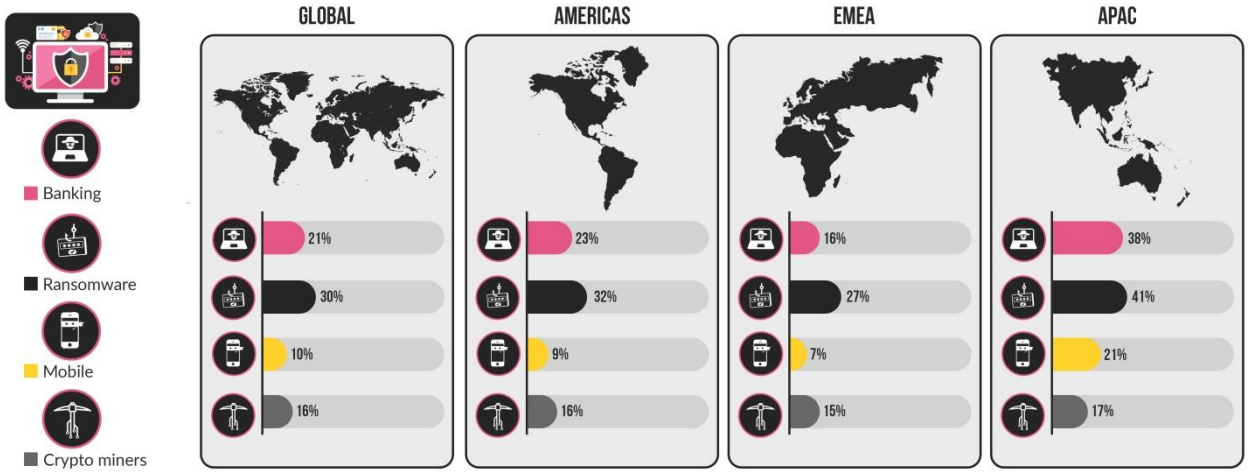


Figure 24: Attack Categories by Region

Global Threat Index Map

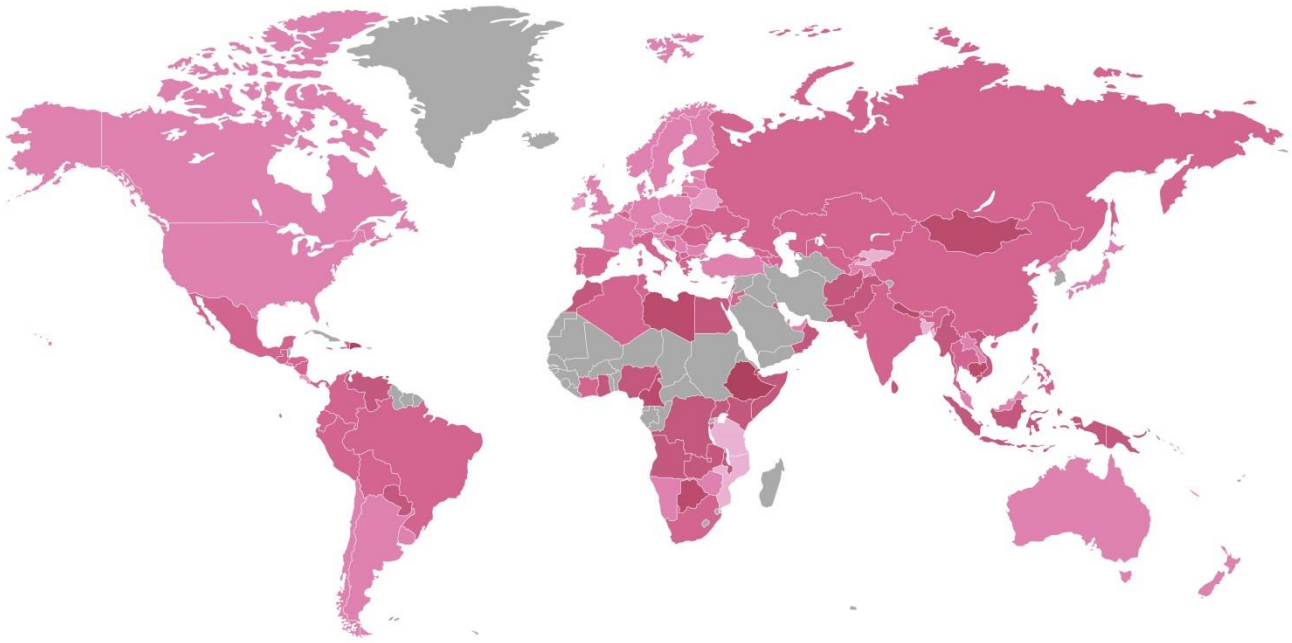


Figure 25: The 2017 H2 World Cyber Threat Index Map

Global Top Exploited Vulnerabilities

The top attacks list presented below is based on data collected by Check Point's IPS solution, and details the most popular attack techniques and exploits observed by Check Point researchers between July and December 2017.

- **SMB propagation (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145)** – several SMB vulnerabilities, EternalBlue, EternalRomance and more, which were allegedly discovered and exploited by the NSA, were leaked online last April by the Shadow Brokers group. When exploited, these vulnerabilities allow attackers to spread laterally between connected machines and take complete control over entire networks. The vulnerabilities were leveraged in massive attacks, such as WannaCry, NotPetya and BadRabbit, causing major damage worldwide.

- **Apache Struts 2 (CVE 2017-5638)** - a few vulnerabilities that were revealed in Apache Struts 2 had a significant impact on the threat landscape as of their exposure. The vulnerabilities gained a lot of attention during the Equifax breach, in which threat actors exploited an unpatched Apache Struts in the company's network. The breach resulted in the leak of over 200,000 credit card numbers and 143 million US customers' data, and is one of the most harmful targeted attacks in recent years. The vulnerability lies in the file upload request with successful exploitation potentially resulting in execution of arbitrary code on the affected machine.

- **IoT vulnerabilities (CVE 2017-8225)** – Several IoT vulnerabilities hit the headlines throughout the past year, with multiple attacks and campaigns targeting them. One of the most prominent operations based on these vulnerabilities is IoTroop, a major IoT botnet that emerged in 2017. The botnet features a vulnerability scanning functionality instead of the original brute forcing password functionality, and scans potential devices such as WIFICAM IP cameras and DLINK routers for several vulnerabilities.

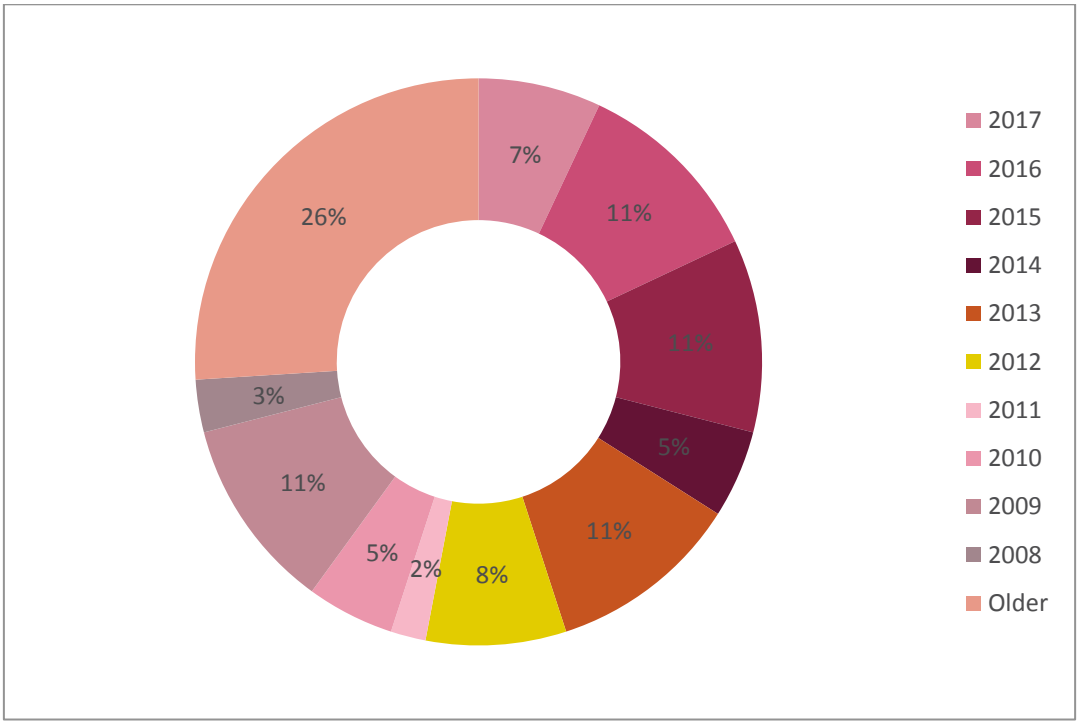
- **RTF (CVE 2017-0199, CVE 2017-11882)** – Security flaws in Microsoft Office Rich Text Format (RTF) were widely abused by threat actors throughout 2017. These security flaws

allow attackers to download and execute malicious scripts containing PowerShell commands on target machines depending only on the end-user's decision to open malicious documents. These vulnerabilities were used mainly in malspam campaigns, within documents that serve as downloaders for various malware types.

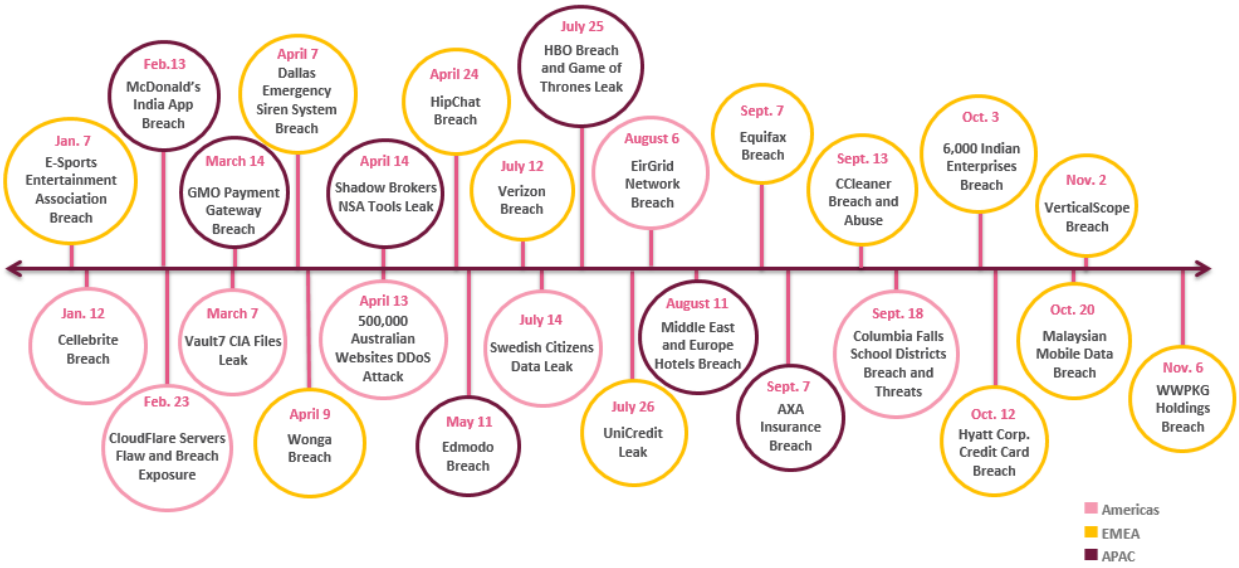
- **DDE – Marco-less code execution** – Microsoft Dynamic Data (DDE) Exchange is a legitimate feature that has been widely abused into an attack vector as of late 2017. Its purpose is in allowing Office files to load data from other Office applications. The feature has been widely leveraged by threat actors in order to deliver malicious payloads to target machines, as unlike many other methods it does not require the user to enable macros or actively run the malicious code. When trying to open a file which includes a DDE field, a warning pops up stating that the document contains link to other files; for this reason, Microsoft claims that this is not vulnerability.

  However, following the surge of malware campaigns leveraging this feature, the company has released an update that disables the DDE feature in Word applications as part of December's Patch Tuesday. DDE attacks were observed during the 1990's, and made a comeback this year, leveraged by threat actors such as the FIN7 hacking group which specializes in attacks against financial organizations.

Interestingly, according to Check Point global sensors, throughout the second half of 2017 some 93% of the attacks observed by our sensors leveraged vulnerabilities registered in 2016 and earlier. Over a quarter used vulnerabilities that are more than 10 years old.



Yearly Data Breaches Timeline



Top Predictions for 2018

Blockchain Attacks – The Crypto Miner's Evolution

While web-based crypto miners are the most common Blockchain-based attack vector currently observed in the wild, we estimate that in the upcoming year we will witness a variety of new attack methods, leveraging the potential that lies in the cryptocurrency mining and trading systems.

Major Cryptocurrency exchanges have already been victims of remarkable thefts. One of which is Bitfinex, one of the biggest exchanges, which lost millions of customers' funds in two hacking operations. The first incident was revealed in August 2016 when 120,000 BitCoin units, then worth a sum of $66 million, were stolen due to a vulnerability in Bitfinex's account structure.

In the second breach, in November 2017, $30 million worth of USDT, a cryptocurrency issued by Tether Limited which is pegged to the US dollar, were stolen from the company's treasury wallet.

Additional attack methods and malware types which may become common in the upcoming year include virtual wallet and credential theft, cryptocurrency transaction theft, and banking Trojans collecting virtual wallet credentials.

Last June, a user reported on Raddit that some 13 BTC had been stolen by a malware that replaced the destination BitCoin address with a different one during the transaction. Recently, in October 2017, a malware dubbed CryptoShuffler, which monitors the victim machine's clipboard and replaces any cryptocurrency wallet ID with the attacker's address, was revealed after successfully stealing $140,000 in BTC.

The mobile arena will not be left unaffected by this trend either. It is likely we will begin to see mobile botnets used to mine crypto-currencies illicitly, as a sufficient mass of mobile zombies can amount to a significant computing power.

Cloud Attacks Will Make Headlines

Last June, a security researcher discovered that some 198 million US voter records (1.1 terabytes of data) collected during the last three presidential campaigns, were found accessible to the public via a database on an Amazon S3 server which was misconfigured.

Indeed, in 2017 we witnessed many such cases, in which improper security configurations left sensitive data unprotected.

Granted, Microsoft has recently reported it witnessed some 300% increase in attacks against its cloud-based accounts during the past year. The company's Security and Protection team claims that most of the attacks observed are the result of poor password management, or guessable passwords. We estimate that in 2018 we will witness an increase in the amount of attacks against cloud-based storage centers, databases and cloud-based accounts.
However, more importantly, while in 2017 most of the attacks relied on faulty or lacking security configurations, we believe that in 2018 attackers will take cloud attacks to the next level. We will witness designated exploits against global storage services, well-orchestrated targeted attacks against cloud infrastructure of specific companies, and data compromise operations, which can cause severe damage to any company just by altering a small piece of data on the company's databases.

As the trust in the cloud increases, more sensitive data is migrated into cloud infrastructures, and the cloud is becoming an attractive target for attackers. This accelerates the development of new, sophisticated offensive tools and techniques. However, many companies are still struggling to adapt their security procedures and solutions to the new infrastructure, and so, as a result, sensitive data will become increasingly vulnerable to attacks.

IoT Attacks Escalation

Mirai malware, the largest IoT attack observed at that time, enslaved vulnerable IoT devices and channeled them to carry out DDoS attacks against some top global internet services. Mirai recruited its bots using factory-set or hardcoded passwords. IoTroops, a new botnet which relies on Mirai's

code, scans its potential bots and leverages nine known vulnerabilities across various devices for infection.

While an increase in the level of sophistication was definitely noted, we estimate that in 2018 the amount of IoT devices integrated into our everyday life will increase, security measures will improve and devices will no longer sustain such basic attack techniques. These factors would lead to the development of far more sophisticated forms of attacks against such devices.

IoT zero-day vulnerability research will become a thriving arena and may even lead to a new, profitable market in underground forums. New attack techniques will also lead to new ways to leverage the infected devices and the data they collect. Nowadays the biggest attack operations which involve IoT devices are DDoS attacks; but as each device records certain types of personal data, we believe that designated attack methods against specific devices will be developed, and will lead to an increased number of data breaches and extortions, and have a greater impact on home users.

Cross-Platform Attacks

Tailored ransomware attacks against hospitals, enterprises and major service providers have been witnessed throughout the last two years, taking entire networks offline and in many cases, putting patients' lives at risk. What could possibly be worse than this?

Well, imagine a scenario in which not only the hospital's network is shut down, but also the employees' mobile phones and all of the web-connected medical equipment.

Such a scenario can be the result of a cross-platform attack. An operation like this relies on malware which moves laterally within the targeted network, but also that can 'jump' from one platform to another. This kind of maneuvering would deprive an entire organization from all sources of communication.

Cross-platform malware have been witnessed in only a handful of occasions in recent years. A notable cross-platform malware observed several times though is Adwind, a remote access Trojan

(RAT) sold as a service, which is capable of infecting any machine installed with Java, including Windows, Mac OSX, Linux, and Android.

However, with the rise in the number of every day devices which require connectivity, and the increasing popularity of well-managed ransomware attacks, we estimate that cross-platform attacks will take on new and varied forms.

Multi-platform attacks enable end-to-end attacks covering all of the resources of the targeted organization, such as a company's corporate network and its cloud-based company resource data center; from a home network and IoT devices such as the house alarm, a hospital's patient data and medical equipment, and more.
In addition, the level of mobile malware targeting enterprises has increased during 2017. From its employees' personal devices to its financial and customer data repositories, such attacks are clearly a great starting point to infect an entire company.

Android Patching Will Continue To Be Patchy

While Google has released its latest Android version 8.0, 'Oreo', with a low adoption rate of just 0.3%, the world is still lagging behind.

We will continue to see archaic exploits and malware successfully targeting old Android versions and reaching a wide spread as a large portion of Android users never receive a security update. This should concern not only the owners of the devices, but any network which has such a device in its midst. After all, it only takes one entry point to infect an entire network.

Additional Observations / Conclusions

2017 introduced us to some significant new malware and attack vectors, which only recently have emerged and yet already generated great impact over the threat landscape and internet in general.

Adware, which was hardly considered as a threat and operated under the radar of the security community, has been in the spotlight in the passing year with the exposure of the Fireball malware global operation.

The great growth of the cryptocurrency market and the development of new coins produced a new kind of tool to generate easy revenue too. This is now in a prominent part of the cyber arena. Web-based Crypto miners, which are embedded inside leading websites and leverage the visitors' computer resources to mine cryptocurrency, often without notifying the users or limiting the percentage of CPU consumed, have indeed become a major player in the world of malware.

The Shadow Brokers leak of alleged NSA tools continued to make waves throughout the year too. From massive attack campaigns, including WannaCry and IoTroops, which rely on these leaked tools and exploits, to a general increase in the use of lateral movement techniques by various malware, the damage the leak caused cannot be overstated.

As for the infection arena, in 2017 a shift has also been observed. While the use of exploit kits has gradually decreased thanks to some new security measures and a decline in the rate of new zero-day flash vulnerabilities, users are still being flooded with aggressive scam campaigns. Serious threat actors are shifting to malspam and are bringing advanced exploit techniques with them, especially in Microsoft Office.

In 2016, several older malware families such as the Conficker botnet, Cryptowall ransomware and Zeus banking malware maintained their place in the top of our global malware rank. While we can still see some of those malware families in our charts, both in this report and in the 2017 Mid-Year Report, their prominence has decreased and their place as market dominators has been taken by newer dominant malware, such as Locky ransomware, Jaff ransomware and RoughTed malvertising campaign. Some of these malware families owe their distribution to Necurs, one of the world's largest spam botnets.
Ries

Ransomware has maintained its place as the most popular malware type among all three regions, but this year, banking malware has accelerated as well. Among the top banking malware list one family, which emerged in late 2016 but spiked in the middle of 2017, stands out - Trickbot banking malware, the malware that spreads via massive spam campaigns and SMB-based lateral movement.

The Check Point ThreatCloud is the largest collaborative network dedicated to exposing and fighting cybercrime. It uses a global network of threat sensors to deliver the most up-to-date threat data and cyber-attack trends. The ThreatCloud database identifies millions of malware types daily, and contains more than 250 million addresses analyzed for bot discovery, as well as over 11 million malware signatures and 5.5 million infected websites.

Appendix 1 – Major Cyber Breaches (H2 2017)

Americas

- **July.** Verizon, a multinational telecommunications provider, suffered a data breach as part of which over 14 million records of US customers were made available on the internet. The records were found on an unprotected server controlled by Nice Systems. As the server was used for customer engagement, the records include customer names, phone numbers, and account PIN codes.

- **July-August**. Threat actors breached HBO's servers and leaked the latest script and full episode of Game of Thrones. According to the threat actors, they stole over 1.5TB of data in their attack. Television network HBO attempted to gather $250,000 in Bitcoins to pay the hackers who breached the company's network, in what HBO prefers to call a 'bug bounty payment'. Some claim this was a delay tactic. The hackers demanded millions of dollars and leaked episodes of many HBO shows, the script of the 5th episode of the popular HBO series Game of Thrones, and personal information of the show's stars.

- **September.** The FBI and Montana's security forces investigated a threat operation in which an attacker breached Columbia Falls Schools District servers. The attacker gained phone numbers and contact information of students, parents and staff members, and sent them threatening messages.

  Following the attack, classes were cancelled for a couple of days in all 30 schools of the district. The school district officials received a related ransom note demanding between $75k and $150k. The ransom note was signed after TheDarkOverlord threat group, which is considered to be responsible for the HBO and Netflix breaches earlier this year.

- **September-October.** The popular financial services provider Equifax suffered a security breach which led to the theft of personal information of over 145 million of its US customers, 15.2 million UK customers and tens of thousands Canadian customers. Approximately 209,000 credit card numbers and an additional 182,000 dispute documents with personal details were compromised by the threat actors.

  The files acquired in the attack contained client information from the years 2011 to 2016, including passwords and answers to security questions. Following the incident, the company announced that the Chief Information Officer and Chief Security Officer had departed their positions. Visa and Mastercard are reportedly taking measures to prevent misuse of the 200,000 credit cards leaked in the breach.

  At a hearing in front of U.S regulators, the company's former CEO took full responsibility for the breach and said the company did not identify the Apache Struts vulnerability which led to it until as late as March 2017.

- **November.** Canadian company VerticalScope, which manages hundreds of forum sites totaling over 40 million users, was breached, with information of at least 2.7 million user accounts stolen and sold on the dark net. This was the second time in the last two years that the company was breached, following a 45-million user account theft in June 2016.

EMEA

- **July.** Italian banking company UniCredit announced that information of 400,000 of its customers had been disclosed following a breach of one of the company's partners. According to UniCredit, passwords were not leaked in the breach.

- **July**. Following the discovery that a government contract had led to a massive leak of nearly all of the country's citizens' personal information, the Swedish government was in turmoil, and saw two ministers resigning.

  In 2015, the Swedish Transport Agency had outsourced database management to Intel Sweden, which in turn outsourced it to companies in Eastern Europe, whose employees had access to the information but without security clearance. The leaked database contained information of all vehicles, including some military vehicles; license information (including

photos) of all citizens, including protected individuals (undercover law enforcement officers, persons in witness protection programs); and information about national infrastructure in the country.

- **August**. Reports claimed that a nation-state actor had breached EirGrid, Ireland's electricity transmission company, and gained complete access to the company's network. It is not yet clear what the attacker's goal was in this breach, but one aim could have been to cause blackouts across Ireland.

- **August**. The Russian hacker group APT28 (Fancy Bear), famous for breaching and leaking the contents of the DNC in the 2016 American elections, was likely behind breaches into several hotels in the Middle East and Europe. The group used their access to the hotels' networks to steal credentials and gain control of visitors using the hotels' Wi-fi. APT28 utilized EternalBlue, an SMB 0-day vulnerability attributed to the NSA.

- **September**. CCleaner, an anti-potentially-unwanted-programs (PUP) freeware, was breached and abused. The program, developed by Avast-owned Piriform, was modified by the attacker so it would insert a backdoor into infected machines, allowing the attacker to run any code. In response to the attack, Piriform pushed an automatic update for CCleaner in order to disarm the threat and remove the backdoor.

APAC

- **September**. The personal data of 5,400 customers of AXA Insurance, a Singaporean life insurance company, was stolen as part of an attack against the company's health portal. Customers' e-mail address, mobile number and date of birth were exposed.

- **October**. Hackers gained access to servers belonging to over 6,000 Indian enterprises, and offered the data, as well as a network takedown of affected organizations, up for sale on the dark net. It is estimated that the compromised organization, based on which access to the others was obtained, is India's National Internet Registry (IRINN). The hacker also claimed to have manipulated the IP address allocation pool, which could trigger a severe outage.

Affected organizations included Internet Service Providers, government agencies and private organizations. The stolen data included credentials, business documents and PII data.

- **October**. Hyatt Corp., an international hotel chain, notified its customers about yet another credit card breach. As part of the incident, payment card information from cards entered or swiped manually at the front desk of 41 properties across 11 countries had been collected. The largest number of Hyatt properties impacted was located in China. Hyatt suffered a breach in late 2015, as part of which credit card systems at 250 locations in 50 different countries were affected.

- **November**. Information of over 45 million mobile phone accounts in Malaysia was stolen and sold on the dark net. The accounts were from multiple companies, and it was unclear what the source of the breach was. As Malaysia has a population of 32 million, it was assumed that every mobile phone account in the country was affected by this breach.

- **November**. WWPKG Holdings, a prominent travel agency in Hong Kong, was the subject of a breach, part of which some 200,000 records from the company's customer database had been accessed and the database encrypted. The compromised data included customer names, ID number, passport numbers, credit card details and more. The company refused to pay the demanded ransom and the police helped WWPKG decrypt the database.

Appendix 2 – Malware Family Descriptions

Nuclear	Nuclear Exploit Kit has been around since 2009, but first gained prominence in 2013. Nuclear is one of the first exploit kits that implemented evasion techniques such as storing cookies, checking referrer headers and blocking IPs, in an attempt to prevent detection. As in all exploit kits, the attack begins with a redirection to a Nuclear landing page. The landing page contains obfuscated JavaScript that checks for vulnerable plug-ins and delivers the exploit. Nuclear has exploits for Flash, Silverlight, PDF, and Internet Explorer.

Angler	Angler first appeared in late 2013. By early 2015, it was the widest spread exploit kit in the wild, a description which is still valid in 2016. Angler is known for its early adoption of zero day exploits, sometimes using them within a few days of the first disclosure. The infection starts when a browser is redirected to a landing page that contains heavily obfuscated JavaScript. The Angler landing page identifies the plug-in versions found on the infected machine so the exploit can target vulnerabilities. It also tries to identify if the vulnerable system is a virtual machine. Flash is the primary exploited program. There are also active exploits for Java, Silverlight, Acrobat and even old versions of Internet Explorer.
WannaCry	Ransomware which was spread in a large scale attack in May 2017 utilizing a Windows SMB exploit called EternalBlue in order to propagate within and between networks. WannaCry's infection vector appears to be direct infection utilizing SMB as delivery method. The ransomware's code is loosely written, and it features a component called 'kill-switch' - before encryption, Wannacry attempts to contact a certain pre-defined domain - if it is active, the malware shuts down and encryption is prevented.
NotPetya	Ransomware which was spread in a worldwide attack that erupted on June 27 with a high concentration of hits in Ukraine including the Ukrainian central bank, government offices and private companies. It was an MBR ransomware, similarly to the Petya ransomware, with worm capabilities such as abusing active sessions and stealing credentials. Additionally, NotPetya used the 'EternalBlue' SMB exploit. Once the malware infiltrates into a network, it makes lateral movement in order to infect the entire network. It is estimated that the source of the attack was M.E.Doc, a Ukrainian accounting software provider whose systems were abused to distribute the attack via its software update mechanism.
BadRabbit	Worm.Win32.BadRabbit is a Worm that targets Windows platform. It is reported that the malware has been used in attacks. The malware has a list of usernames/passwords that it could use to access and spread to SMB shares on other systems in the network. It is also capable to spread via the EternalRomance exploit. The malware encrypts files with the specific extensions on the infected system. It then demands the infected user to pay a ransom in order to get the files decrypted. It overwrites the original MBR with the malicious one. Furthermore, it adds a task in the Task Scheduler to survive system reboots.
IoTroop	An IoT botnet that emerged worldwide during October 2017. It's code is based on the Mirai botnet, but whereas Mirai enumerated on default credentials for lateral movement, IoTroop exploits several vulnerabilities in IoT devices.
Viking Horde	Viking Horde is a mobile malware that targets Android devices and first emerged on May 2016. On all devices, Viking Horde creates a botnet that uses proxy IP addresses to disguise ad clicks, generating revenue for the attacker. On rooted devices, Viking Horde delivers additional payloads that can execute code remotely and also takes advantage of root access privileges to make itself difficult to remove manually.

WireX	Also known as 'Android Clicker', Wirex is a botnet that consists of tens of thousands of Android smartphones. The botnet collects its bots via more than 300 malicious apps installed from Google Play Store and is designed to carry out massive application layer DDoS attacks. The botnet has been used to conduct DDoS attacks as of early August 2017, and in late August an increase in the scale of the attacks has been observed. At its peak in late August, some 120,000 Android smartphones were infected.
MilkyDoor	MilkyDoor is an Android malware, disguised as a proxy that collects internal data from an enterprise's corporate network, in order to infiltrate into the network. MilkyDoor uses Socket Secure (SOCKS) protocol to communicate with its command-and-control servers and exfiltrate the stolen data, and in addition uses the SSH protocol in order to blend in the normal network traffic.
RoughTed	Large scale Malvertising used to deliver various malicious websites and payloads such as scams, adware, exploit kits and ransomware. It can be used to attack any type of platform and operating system, and utilizes ad-blocker bypassing and fingerprinting in order to make sure it delivers the most relevant attack.
CoinHive	Web-based Crypto miner designed to perform online mining of Monero cryptocurrency when a user visits a web page without the user's approval. The implanted JavaScript uses great computational resources of the end users' machines to mine coins, thus impacting the performance of the system.
Locky	Locky is a ransomware Trojan that targets the Windows platform. This malware sends out system information to a remote server and receives an encryption key to encrypt files on the infected system. The malware demands that the payment to be made in the form of Bitcoins digital currency. To survive a system reboot, it adds a Run key Registry entry.
Andromeda	Andromeda is a modular bot for malicious activity, and was first spotted in 2011. It is used mainly as a backdoor to deliver additional malware on infected hosts, but can be modified to create different types of botnets. Andromeda utilizes various anti-sandboxing and anti-AV capabilities, such as injecting its code into legitimate processes, and is not visible in the task manager.
Nivdort	Nivdort is a Trojan family which targets the Windows platform. It gathers passwords and system information or settings such as the Windows version, IP address, software configuration and approximate location. Some versions of this malware collect keystrokes and modify DNS settings. Nivdort deploys its files in the Windows system files folder. The malware is spread via spam mail attachments or malicious websites.
Fireball	Fireball is an adware vastly distributed by the Chinese digital marketing company Rafotech. It acts as a browser-hijacker which changes the default search engine and installs tracking pixels, but can be turned into a full-functioning malware downloader. Fireball is capable of executing any code on the victim machines, resulting in a wide range of actions from stealing credentials to dropping additional malware. Fireball is spread mostly via bundling; being installed on victim machines alongside a wanted program, often without user consent.
Globeimposter	GlobeImposter is a ransomware disguised as a variant of the Globe ransomware. It was discovered in

	May 2017, and is distributed by spam campaigns, malvertising and Exploit kits. Upon encryption, the ransomware appends the .crypt extension to each encrypted file.
Conficker	Conficker is a computer worm that targets the Windows OS. It exploits vulnerabilities in the OS and uses dictionary attacks on the admin passwords to enable propagation while forming a botnet. This infection allows an attacker to access users' personal data such as banking information, credit card numbers, or passwords. The worm originally targeted users of networking websites such as Facebook, Skype and email websites.
Virut	Virut is one of the major botnets and malware distributors in the Internet. It is used in DDoS attacks, spam distribution, data theft and fraud. The malware is spread through executables originating from infected devices such as USB sticks as well as compromised websites and attempts to infect any file accessed with the extensions .exe or .scr. Virut alters the local host files and opens a backdoor by joining an IRC channel controlled by a remote attacker.
Ramnit	Ramnit is a worm that infects and spreads mostly through removable drives and files uploaded to public FTP services. The malware creates a copy of itself to infect removable and permanent drivers. The malware also functions as a backdoor, allowing the attacker to connect to the infected machine and communicating via C&C servers. The first variant, discovered in 2010, didn't have many capabilities beyond a basic ability to integrate itself into an infected machine. In 2011 it was modified by malicious actors to have the ability to steal web session information, giving the worm operators the ability to steal account credentials for all services used by the victim, including bank accounts, corporate and social networks accounts.
Cloudhopper	Malware campaign associated to a Chinese APT group known as APT10 and aimed to gain network access and persistence for sensitive information gathering, in many cases using managed IT service providers as an access point.
Winnti	Winnti is a Backdoor that targets the Windows platform. This malware installs a rootkit on victim's system, hooks critical functions and system driver of the infected Windows system. It contacts a remote server for further instruction. It collects system information and sends it to a remote server. It might inject malicious payload into various processes. It has been reported that some variants (32 or 64 bit) of this Backdoor might be signed with a legitimate certificate.
IsraBye	IsraBye is an anti-Israeli data wiper malware targeting Israel-based entities in the wild. The malware poses as ransomware, but the files cannot be recovered once encrypted.
Ldpinch	Ldpinch is a Trojan-type program that targets the Windows platform. The malware is designed to delete, block, modify, or copy data and disrupt computer or network performance. The malware masquerades as a legitimate file or software.
Donoff	Donoff is a malware downloader which uses macros to exploit Microsoft Word and download the malicious payload to the victim machine. Donoff features evasion techniques to prevent execution on a virtual machine and analysis by security analysis tools. Additionally, the macro's commands are obfuscated.

Pushdo	Pushdo is a Trojan that enables unauthorized access and control of an infected computer, allowing an attacker to perform different actions. These actions include delete files, download and execute arbitrary files, keystrokes logging, system settings modifications, private data theft, propagation of the malware to other computers and more. Pushdo is the dropper of the Cutwail spam botnet
Badjoke	Badjoke is a joke program that runs on Microsoft Windows operating systems. Its main purpose is to annoy or entertain the user.
Adwind	Adwind is a Backdoor that targets systems supporting the Java runtime environment. This malware sends out system information and accept commands from a remote attacker. Commands can be used to display messages on the system, open URLs, update the malware, download/execute files, and download/load plugins, among other actions. Downloadable plugins for the malware can provide considerable additional functionality including remote control options and shell command execution.
Papoto	Web-based Crypto miner designed to perform online mining of Monero cryptocurrency when a user visits a web page without the user's approval. The implanted JavaScript uses great computational resources of the end users' machines to mine coins, thus impacting the performance of the system. Papoto miner is known for its fast and well obfuscated script.
Cryptoload	Cryptoload is a generic name for scripts designed to download malware (mainly ransomware), usually sent within archive files as attachments in spam campaigns. They have been seen used for downloading Cryptowall, TeslaCrypt and Locky, as well as Fareit Info-stealer.
Zeus	Zeus is a widely distributed Windows Trojan which is mostly used to steal banking information. When a machine is compromised, the malware sends information such as the account credentials to the attackers using a chain of C&C servers. The Trojan is also used to distribute ransomware. Zeus was first identified in July 2007 when it was used to steal information from the United States Department of Transportation. Over the next few years the malware compromised hundreds of thousands of machines, becoming one of the world's largest botnets. The malware was distributed mostly by email, using phishing attacks.
Dorvku	Dorvku is Trojan that targets the Windows platform. The malware collects system information and sends it to a remote server. It also collects sensitive information from targeted web browsers. Moreover, it accepts commands to perform malicious activities on the infected system.
ZergHelper	iOS malware which targets Chinese users, and therefore displays different behaviors according to the device's location in the world. The malware was able to bypass Apple's security. Once installed on a device in China, the app uses social engineering to install two configuration profiles, based on which applications that did not go through Apple's review, and may contain malicious code, can be downloaded to the infected device.
Toga	Toga is a worm that targets the Windows platform. The malware replicates itself and relies on network or user based security flaws to spread to other computers.
Retrieve	Retrieve is a Trojan that carries out various damaging actions on an infected host. It usually

	originates from adware, pornographic websites, and attachments in spam mail. Once installed, this malware triggers a range of actions that gradually degrades the operating system performance until it can't be used anymore. Such damages include modifying browser settings, DNS settings, crucial system files and registry keys. Retrieve can also collect a user's personal data and send it to a remote server belonging to an attacker.
DLoader	DLoader is a Trojan that can infect all versions of Microsoft Windows. The malware can download and run any software and typically exploits vulnerabilities in outdated software or in the operating system. The infection often goes unnoticed, as it begins when the user clicks a malicious link on a website or email, or installs some dubious free software. The Trojan maintains persistency, and changes both its name and location frequently to avoid detection.
Jaff	Ransomware which began being distributed by the Necrus botnet in May 2017, via spam emails containing a PDF attachment which contains an embedded DOCM file. As the malware first emerged, it was massively spread at an infection rate of approximately 10,000 emails sent per hour.
Cryptolocker	Cryptolocker is a ransomware Trojan family first detected in 2013 which targets the Windows platform. It runs in the background and encrypts various files and documents found on compromised hosts. The user is then contacted with a ransom demand to decrypt the files. Cryptolocker is primarily spread through infected websites or spam campaigns. There is currently no known alternative method for restoring access to the encrypted files. On May 2015, Cryptolocker was taken down along Game over Zeus botnet, in a multi-national law enforcement operation called 'Operation Tovar'. The operation led to the arrest of the creators and the end of Cryptolocker infections.
Crypt	Crypt is a downloader Trojan that downloads and installs malicious files and unwanted content from remote servers onto the victim’s machine without their consent.
Nymaim	Nymaim is a malware dropper and downloader first observed in 2013. Originally, the dropper infected its victims with ransomware and was spread by Black Hole Exploit Kit. Later, Nymain was responsible for the distribution of additional types of malware such as Vawtrak, Miuref, Pony, and Ursnif. The malware's distribution dropped at 2014, and increased again in 2015.
Cerber	First introduced in February 2016, Cerber is an offline ransomware, meaning that it does not need to communicate with its C2 server before encrypting files on an infected machine. It is spread mostly via malvertising campaigns which leverage exploit kits, but also through spam campaigns. The threat actors behind Cerber ask for a 1-bitcoin ransom for decrypting one's files, and according to some reports. Its business model is ransomware as-a-service, meaning that the author recruits affiliates to spread the malware for a share of the ransom payment.
Tinba	Tinba is a banking Trojan which targets mainly European banking customers and uses the BlackHole exploit kit. Tinba steals the victim's credentials using web-injects, which are activated as the user tries to connect to his account on one of the targeted banks' websites. When that occurs, a fake webpage appears on the screen with a message asking the user to fill in his personal information.

	The Trojan has been observed since 2015 and its targets are mostly in Europe, specifically in Poland and Italy. Nevertheless, machines infected with Tinba have been spotted in various countries all over the world. Tinba is also referred to as Tiny Banker or Zusy, due to the fact that at the time of its discovery in 2012, it was the smallest banking Trojan (by file size) seen in the wild.
Qbot	Qbot is a backdoor belonging to the Qakbot family. It is capable of dropping and downloading other malware. It also establishes a connection with a remote HTTP server without user consent and may steal important user information.
Trickbot	Trickbot is a Dyre variant that emerged in October 2016. Since its appearance, it has targeted banking users mostly in Australia and the U.K, and lately it started focusing also on India, Singapore and Malesia. It seems that a professional group of threat actors is behind Trickbot, as it is evolving rapidly. Interestingly, Trickbot banker can pull web-injection instructions from its C&C servers online when the victim tries to reach a website. This is in contrast to most banking Trojans that update their Man-in-the-Browser (MitB) configurations periodically. This feature also helps Trickbot to avoid mistakes caused by an out-of-date configuration that may lead to its discovery.
Dyreza	Dyre is a banking Trojan which targets the Windows operating system. It steals banking credentials and passwords from the top three major browsers: Chrome, Firefox and Internet Explorer. Dyre differs from other banking Trojans by infecting its victims with additional malware such as Fareit. Dyre is usually spread via email which contains a file camouflaged as an invoice, banking document or fax. This file installs the Upatre downloader on the infected machine. Upatre disables the security software and downloads Dyre. After recent takedowns against major banking Trojan such as Game Over Zeus, Ramnit and Shylock, Dyre took their place as one of the major threats to consumers. The malware targets mostly English speaking countries.
Dridex	Dridex is a Trojan that targets the Windows platform. This malware is reportedly downloaded by an attachment found in spam emails. This malware identifies itself with a remote server by sending out information about the infected system. Furthermore, it can download and execute arbitrary modules received from the remote server.
Bancos	Bancos malware steals financial information, using keylogging to record the victim's credentials as they are entered on a targeted bank webpage. Bancos can also supplement or replace a legitimate bank login page with a fake webpage. The Trojan was first spotted in 2006, and is active primarily in Latin America, particularly in Brazil. It is spread mostly via phishing.
Hiddad	Android malware which repackages legitimate apps and then released them to a third-party store. Its main function is displaying ads, however it is also able to gain access to key security details built into the OS, allowing an attacker to obtain sensitive user data.
Triada	Modular Backdoor for Android which grants superuser privileges to downloaded malware, as helps it to get embedded into system processes. Triada has also been seen spoofing URLs loaded in the browser.
Lotoor	Lotoor is a hack tool that exploits vulnerabilities on Android operating system in order to gain root

	privileges on compromised mobile devices.
Hummingbad	Android malware that establishes a persistent rootkit on the device, installs fraudulent applications, and with slight modifications could enable additional malicious activity such as installing a key-logger, stealing credentials and bypassing encrypted email containers used by enterprises
Ztorg	Trojans in the Ztorg family obtain escalated privileges on Android devices and install themselves in the system directory. The malware is able to install any other application on the device.
Bosuoa	Android malware, which disguise itself as a legitimate mobile application, but instead sends multiple premium SMS messages to certain predefined numbers, which lead to significant costs.
Xcodeghost	XcodeGhost is a compromised version of the iOS developer platform, Xcode. This unofficial version of Xcode was altered so that it injects malicious code into any app that was developed and compiled using it. The injected code sends app info to a C&C server, allowing the infected app to read the device clipboard (meaning, any information copied by the user from any of the device interfaces or apps), to change browser info (create phishing websites) and more.
Lokibot	A mobile banking trojan which targets Android smartphones and turns into a ransomware upon an attempt of the victim to remove its admin privileges. LokiBot is primarily a banking trojan - it displays fake login screens on top of popular banking applications. The banker targets mobile banking apps by their design, but also other popular apps such as WhatsApp, Outlook and Skype.
Cryptoloot	Web-based Crypto miner designed to perform online mining of Monero cryptocurrency when a user visits a web page without the user's approval. The implanted JavaScript uses great computational resources of the end users' machines to mine coins, thus impacting the performance of the system.
CoinNebula	Web-based Crypto miner designed to perform online mining of cryptocurrency when a user visits a web page without the user's approval. The implanted JavaScript uses great computational resources of the end users' machines to mine coins, thus impacting the performance of the system. The miner is configured in such a way that disables report of abuse by users.
Rocks	Web-based Crypto miner designed to perform online mining of cryptocurrency when a user visits a web page without the user's approval. The implanted JavaScript uses great computational resources of the end users' machines to mine coins, thus impacting the performance of the system.
Schemouth	Web-based Crypto miner designed to perform online mining of Monero cryptocurrency when a user visits a web page without the user's approval. The implanted JavaScript uses great computational resources of the end users' machines to mine coins, thus impacting the performance of the system.
CryptoShuffler	CryptoShuffler is a malware that first seen in the wild on November 2017. CryptoShuffler monitors the victim machine’s clipboard and replaces any cryptocurrency wallet ID with the attacker’s address, successfully stealing 140,000 USD in BTC. Besides Bitcoin, CryptoShuffler also targeted, Dogecoin, Litecoin, Dash, Ethereum, Monero, and Zcash.

