
cp<r>
CHECK POINT RESEARCH
CYBER ATTACK TRENDS
2018 MID-YEAR REPORT
Check Point
SOFTWARE TECHNOLOGIES LTD

TABLE OF CONTENTS

INTRODUCTION

When it comes to the global cyber landscape, threats are ever evolving, keeping organizations as well as the security community constantly challenged. From taking advantage of the Blockchain trading systems to developing new attack methods in the thriving mobile arena, as well as adapting previous attack tools to the cloud environment, there are clear uses of current technological developments and their rising implementation in the 2018 cyber threat landscape.

So far this year, the different strains of malware and their authors have proven to be capable of much more than previously imagined, with more sophistication and with a new level of agility. As seen in our analysis of the GandCrab Ransomware, malware are now rapidly adapting in real-time to security solutions offered by security vendors.

One of the biggest ongoing trends is Cryptominers and crypto-related threats as a whole. Indeed, Cryptominers have taken the world by storm, becoming the leading attack vector used by threat actors this year, overtaking even Ransomware. So far, Cryptominers have greatly improved their capabilities as well as upgraded their targets array: servers, mobile devices, industrial systems and cloud infrastructure – no one is left behind.

The first half of 2018 has also featured some new and interesting trends. The Cloud infrastructure for instance, has become one of the most attractive targets for threat actors; as the vast amount of sensitive data along with the available computing resources reside on the cloud environment, have easily captivated the attackers' attention. Tesla's cloud servers infected with Monero miner earlier this year and a massive leak of sensitive data of FedEx customers are just two examples of what 2018 has brought to us.

To provide organizations with the best level of protection, security experts must be attuned to the ever-changing landscape and the latest threats and attack methods. The Check Point Global Threat Intelligence Trends report provides a comprehensive overview of the malware landscape in the top categories of Cryptominers, Ransomware, banking and mobile threats, based on threat intelligence data drawn from the ThreatCloud World Cyber Threat Map between January and June 2018.

GLOBAL TRENDS

THE EVOLUTION OF CRYPTOMINERS

It's difficult not to notice the incredible surge in Cryptomining attacks. During the first half of 2018, Cryptominers dominate the top cyber-attacks and malware families seen in the wild. Overtaking Ransomware, Cryptominers affected over 42% of organizations worldwide, compared to 20.5% at the end of 2017. Over the past six months, Cryptomining attacks are estimated to have 'earned' their users more than $2.5 billion, and still counting.

Since their creation, Cryptominers have come a long way. Evolving from simple website compromise, Cryptominers have been observed this year spreading through Facebook Messenger, YouTube ads and Google Play, while infecting tens of thousands of websites, personal computers and powerful severs such as Jenkins. In 2018, Cryptominers have upgraded and vastly improved their abilities, becoming more sophisticated and even destructive.

Motivated by a clear interest to increase the percentage of computational resources leveraged, and crafted to be even more profitable, Cryptominers today target anything that could be perceived as being in their way. As a result, we have witnessed Cryptominers targeting SQL Databases, industrial systems, a Russian nuclear plant, and even cloud infrastructure. Cryptominers have also highly evolved recently to exploit high profile vulnerabilities and to evade sandboxes and security products in order to expand their infection rates.

The mobile arena was not deprived of Cryptomining attacks either. Last April, the Android Cryptominer dubbed HiddenMiner targeted numerous devices, continuously mining Monero until the devices' resources were drained. Mobile miners have even managed to breach Apple's garden wall and penetrated the App Store, with a malware trying to steal victims' login credentials to cryptocurrency wallets.

Adding more fuel to the fire, since the beginning of 2018 a variety of new attack methods have surfaced, leveraging the potential that lays in cryptocurrency trading systems. Among others, these methods include virtual wallet and credential theft, cryptocurrency transaction maneuvering, as well as ICO scams (Initial Coin Offering) that lure victims to invest in a fake premature cryptocurrency.

Moreover, other malware families have begun integrating mining capabilities into their arsenal. Ransomware, as well as prominent Banking Trojans including Panda and TrickBot, are now targeting not only bank accounts but also cryptocurrency wallets and trading system accounts, adding features of cryptocurrency credential theft to their arsenal.

As threat actors become more aware of the lucrativeness of the crypto-business, even more than other exploits, there is almost never a day that goes by without some kind of crypto-threat making the headlines.

NEW THREATS FROM TRANSITION TO THE CLOUD

The cloud environment has changed the way companies manage, store and share their data, applications, and workloads. Along with a wide range of benefits, the cloud infrastructure also introduces a new, fertile and attractive environment for attackers who crave the enormous amount of available computing resources and sensitive data it holds.

Indeed, 2018 has brought us various sophisticated techniques and tools exploited against cloud storage services. In the past year alone, 51% of organizations worldwide have experienced cloud-based attacks, including FedEx, Intel, and Honda.

Several cloud-based attacks, mainly those involving data exfiltration and information disclosure, derived from poor security practices. Credentials left available on public source code repositories or the use of weak passwords are just some examples of how threat actors gained access and control over unprotected resources hosted in the cloud.

Another rising threat taking the cloud environment by storm is the infamous Cryptominers, targeting the cloud infrastructure in order to exploit the vast computational power it presents, and generate huge profits for threat actors. In the first half of 2018, we have witnessed cryptominers targeting two of the cloud's core components – Docker and Kubernetes systems. This is how, for example, Tesla's internal cloud servers were infected with a Monero Cryptominer a few months ago.

Application Programming Interfaces (APIs) that are used to manage, interact and extract information from services have also been a target for threat actors. The fact that cloud API's are accessible via the Internet has opened a window for threat actors to take advantage and gain considerable access to cloud applications.

As time passes, it seems that the cloud's threats will continue to evolve. Attackers will continue to develop more and more tools for their cloud playground, pushing the limits of the public cloud services. Indeed, as new cloud exploitations emerge, there is no doubt that the next attack is already taking place.

MULTI-PLATFORM ATTACKS: DESKTOP AND MOBILE

In the beginning of 2018, a new Advanced Persistent Threat (APT) dubbed 'Dark Caracal' was revealed, possibly after five years of under the radar activity. Though APT groups have carried out extensive espionage campaigns in the past few years, this group presents a unique method of operation which marks one of 2018's most prominent trends. It began collecting sensitive data from mobile devices but has recently shifted to a more effective technique of using one piece of malware which infects Windows, Linux and Mac OS. Whether they are based on one malware or not, multi-platform attacks may have a crippling effect on its victims, whether they be private homes in which all desktop machines, mobile devices and consumer devices are attacked at once, or an enterprise whose industrial systems and data centers get attacked simultaneously.

Up until the end of 2017, multi-platform malware was witnessed in only a handful of occasions, but as predicted, the rise in the number of consumer connected devices and the growing market share of operating systems which are not Windows has led to an increase in cross-platform malware. Campaign operators implement various techniques in order to take control over the campaigns' different infected platforms.

In the first half of 2018, we witnessed the Android Banking Trojan "Roaming Mantis" roaming further afield than it ever had before, targeting both iOS users and personal computers' resources for mining operations, allowing its authors to vastly accelerate their infection rate.

With the introduction of new technologies like powerful smartphones and Office 365, potential victims are no longer using single endpoints but rather several fully connected devices and services.

This introduces a whole new environment in which victims are exposed to more attack vectors that could be exploited by threat actors trying to find the weakest link that leads to a person or organization's data.

MOBILE MALWARE THROUGHOUT THE SUPPLY CHAIN

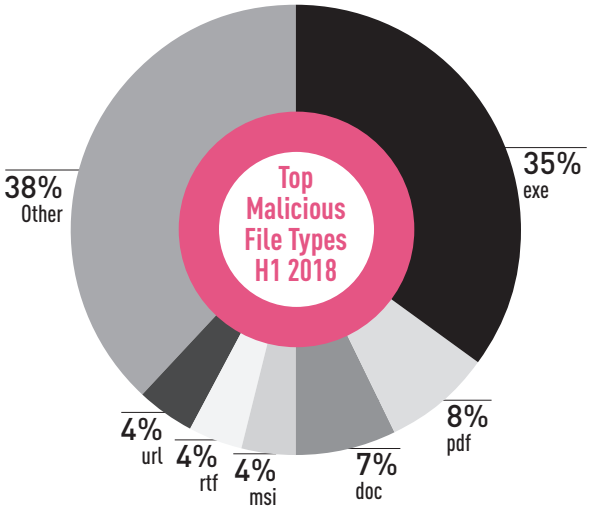
Getting infected with malware on a mobile device is by now nothing new. From being downloaded from a malicious URL or disguised as an innocent looking mobile app, there are various ways a device can be hacked.

In the first half of this year, however, we have witnessed an interesting trend – preinstalled malware. In several incidences malware was not pulled from an app store or downloaded from a malicious URL, but instead arrived already installed within the device. This March, Check Point researchers revealed a widespread mobile botnet dubbed 'RottenSys', infecting nearly five million Android devices. RottenSys, disguised as a legitimate 'System Wi-Fi service' app, came preinstalled on millions of brand new smartphones manufactured by leading brands including Huawei, Xiaomi, Vivo and Samsung. In another case, 42 models of low-cost smartphones were found being sold with the Triada Banking Trojan preinstalled. Threat actors' ability to infiltrate somewhere along the supply chain is concerning and will continue to trouble us in the future.

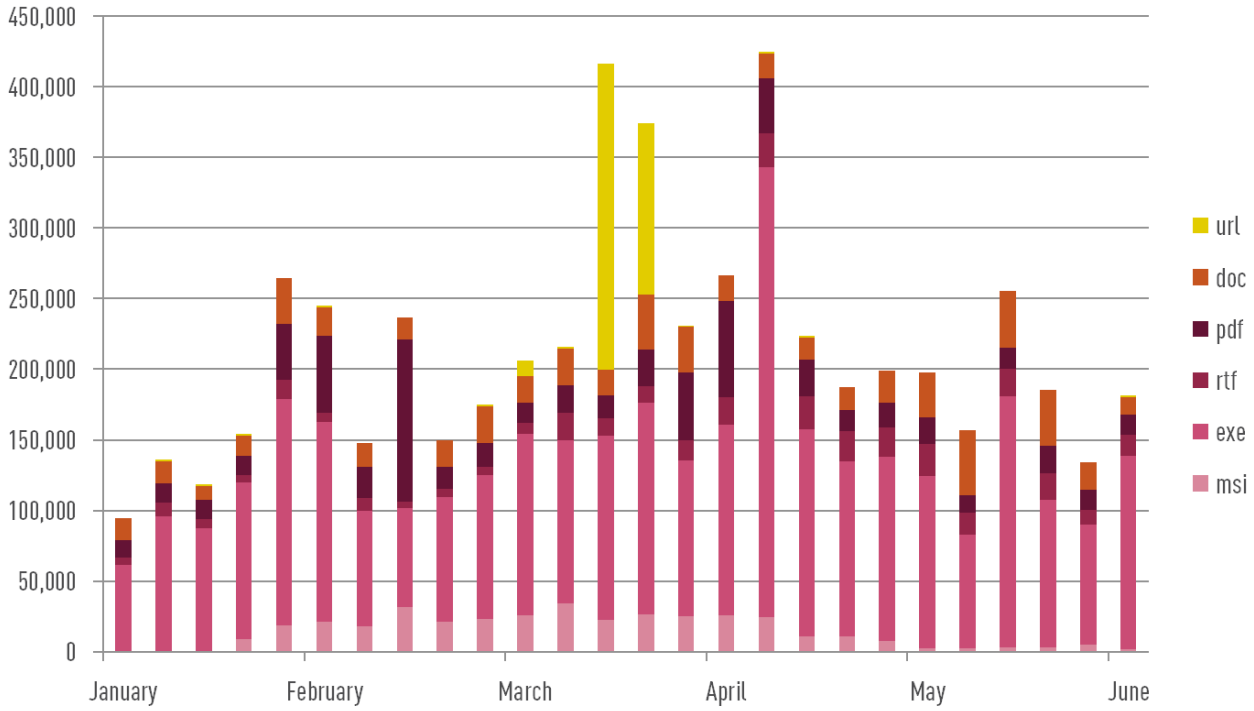
In addition, with the growing dependence on our mobile devices, application markets are flooded with different apps designed to optimize a device's battery performance, allowing users a few more moments of joy with their smartphones. This year, it appears that threat actors have spotted the potential opportunities in this market, as we discovered a vast amount of these allegedly innocent apps were actually malware under disguise. Among them, Banking Trojans, Adware, and even sophisticated RATs such as AndroRAT masqueraded as a utility app named "TrashCleaner" and were capable of stealing mobile network information, storage capacity, calendar events and preforming shell command executions.

Knowing that all of our personal and business life is being managed over some extremely hackable devices, these two phenomena of preinstalled malware and the constant rise of malicious mobile apps reflect how motivated threat actors are to exploit this arena.

TOP MALICIOUS FILE TYPES – H1 2018



FILE TYPE ACTIVITY RATE OVER TIME – H1 2018



GLOBAL MALWARE STATISTICS

Data comparisons presented in the following sections of this report are based on data drawn from the Check Point ThreatCloud World Cyber Threat Map between January and June 2018.

TOP MALWARE FAMILIES

Global

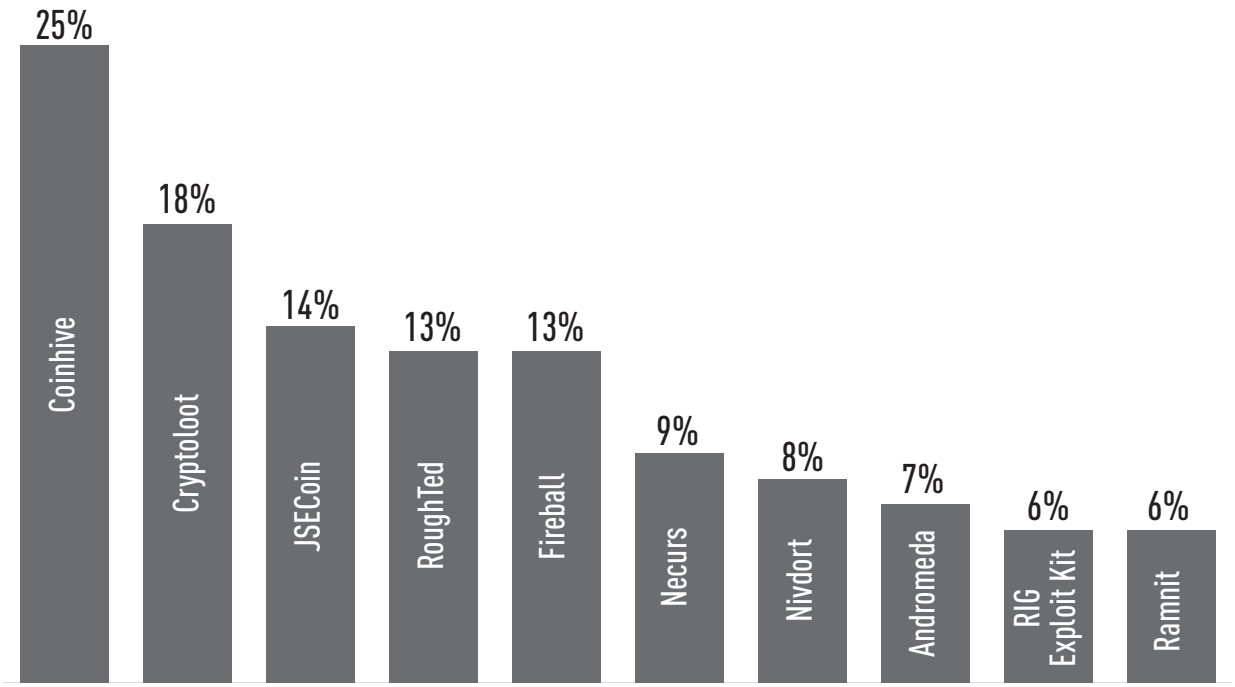


Figure 1: Most Prevalent Malware Globally: Percentage of corporate networks experiencing each malware type

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

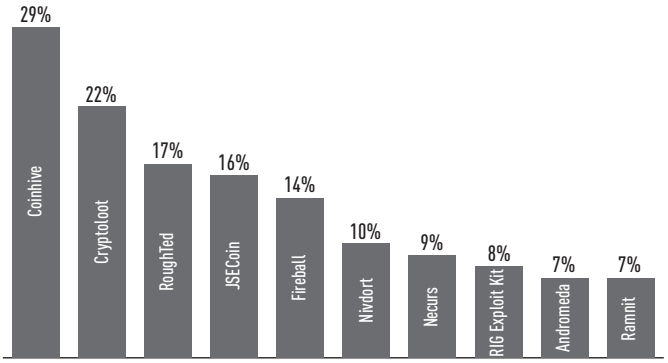


Figure 2: Most Prevalent Malware in the Americas

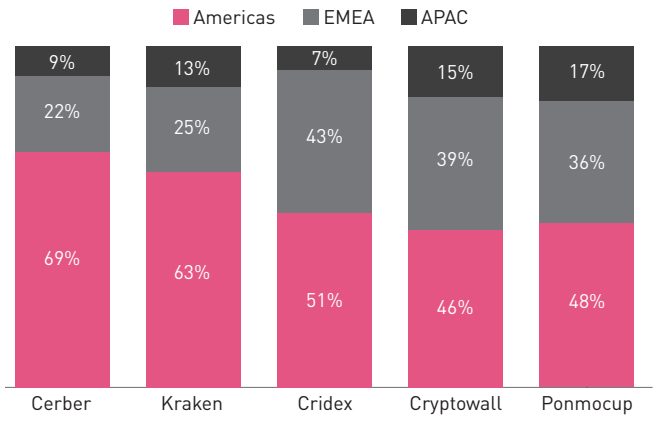


Figure 3: Top Targeted Malware in the Americas

Europe, Middle East and Africa (EMEA)

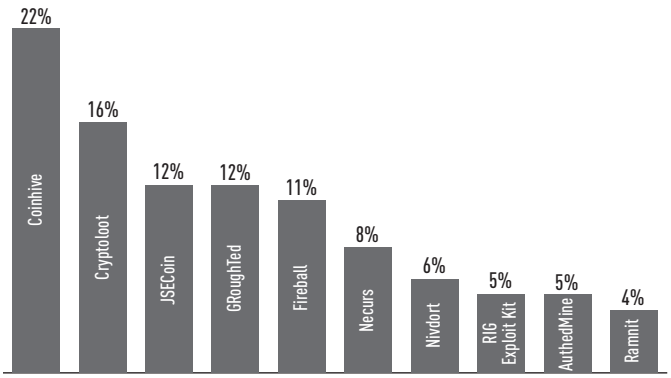


Figure 4: Most Prevalent Malware in EMEA

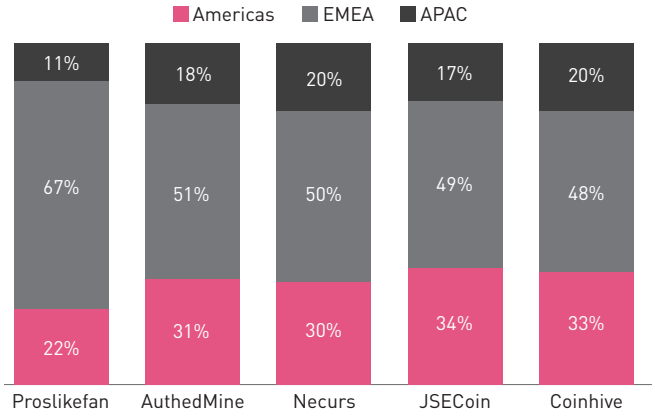


Figure 5: Top Targeted Malware in EMEA

Asia-Pacific

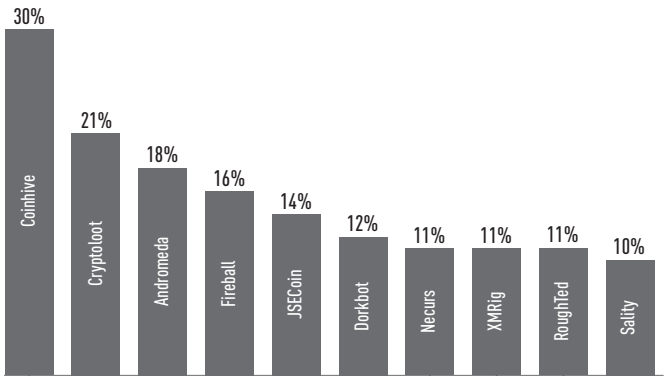


Figure 6: Most Prevalent Malware in APAC

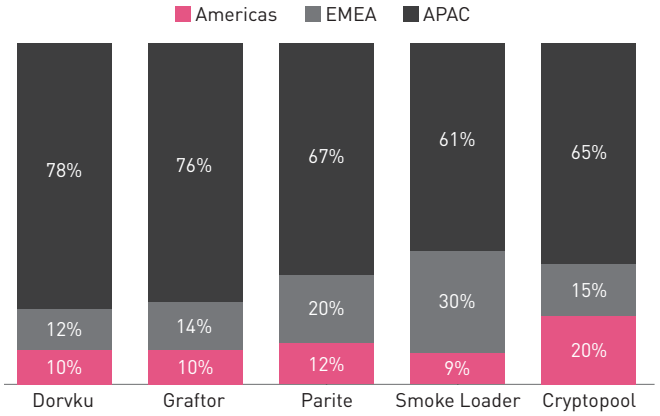


Figure 7: Top Targeted Malware in APAC

Global Analysis of Top Malware

- **Coinhive**, the popular web-based Monero Cryptocurrency miner has maintained its place at the summit of the global and regional rank, with 25% of the organizations worldwide hit by it. Together with Cryptoloot and Jesscoin, the cryptominers squad has shown no signs of slowing its dominance, impacting about 40% of the globe. Ever since Coinhive first released its JavaScript mining code last September, it is being integrated into tens of thousands of websites at any given moment, utilizing visitors' computing resources, and functioning as a lucrative replacement for online advertisements leveraged by threat actors. This year Coinhive was delivered intensively, being found hidden inside YouTube advertisements, distributed via Google's DoubleClick platform and Facebook Messenger, and also embedded in thousands of websites.

- **RIG Exploit Kit**, one of the most prominent exploit kits in the wild with several different campaigns currently in action, has climbed its way up the global and regional ranks. The RIG infection chain starts with a redirection to a landing page that contains JavaScript that checks for vulnerable plug-ins and exploits the browser. RIG delivers Exploits for Flash, Java, Silverlight and Internet Explorer, and was the first one to include the new zero-day vulnerability discovered this year in IE, tracked as CVE-2018-8174. In the first half of 2018 RIG has hit the headlines, pushing various payloads including Bunitu, cryptominers, and the popular Smoke Loader.

TOP CRYPTO MINING MALWARE

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

Global

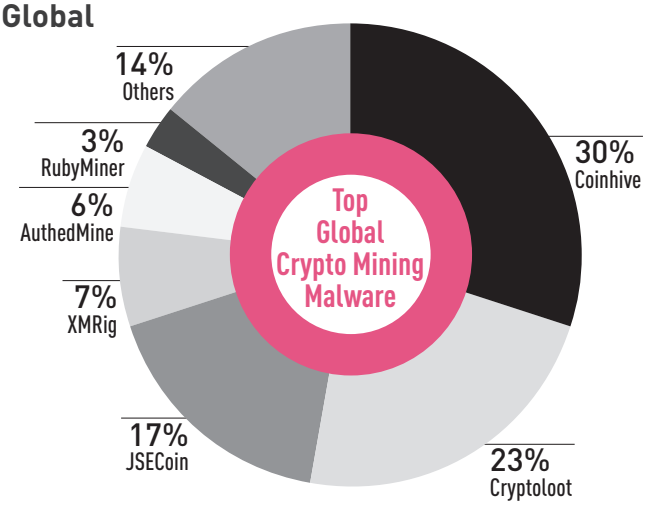


Figure 8: Top Crypto Mining Malware Globally

Americas

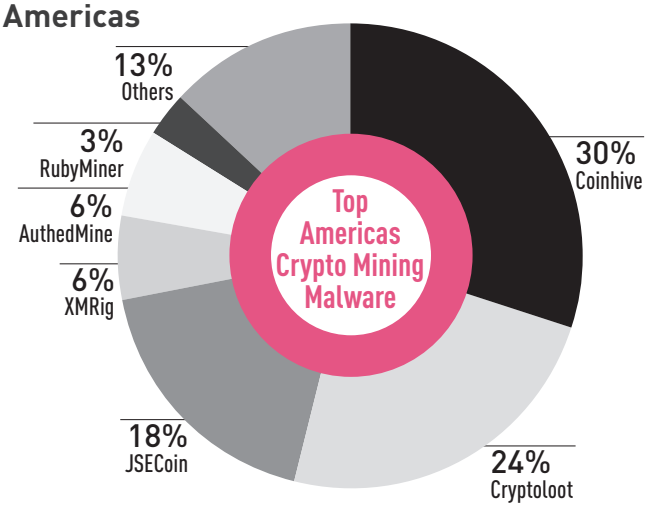


Figure 9: Top Crypto Mining Malware in the Americas

EMEA

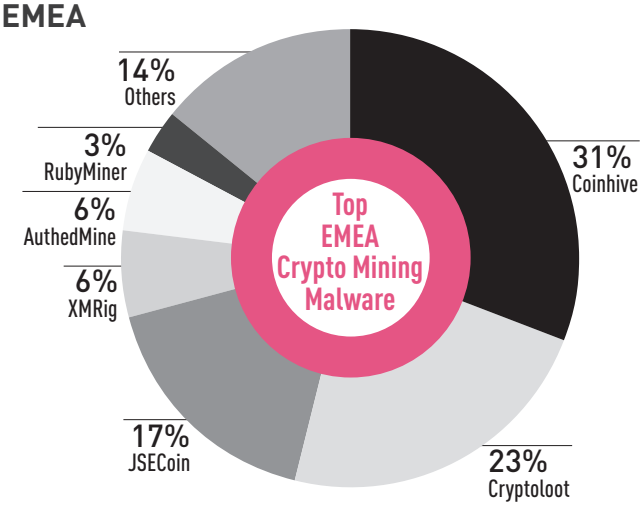


Figure 10: Top Crypto Mining Malware in EMEA

APAC

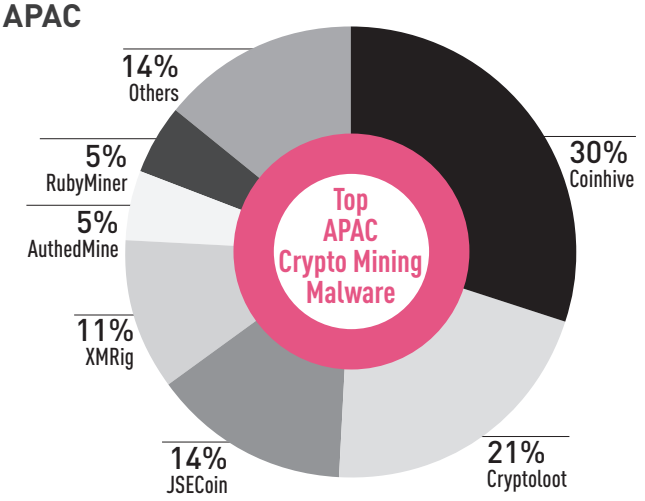


Figure 11: Top Crypto Mining Malware in APAC

Crypto Mining Malware Global Analysis

- First seen in the wild in May 2017, the open-source CPU mining software **XMRig** is ranked third in all of the regions. Being the most popular and exclusive mining code leveraged by threat actors during the first half of 2018, the XMRig mining code has been utilized by wide range of crypto-strains – one of which is RubyMiner. Exclusively detected by Check Point researchers last January, RubyMiner got into the global and regional ranking list. Targeting unpatched Windows and Linux servers, rather than being injected into websites as most of the others in the rank, RubyMiner has attempted to exploit 30% of all corporate networks worldwide in order to mobilize poweful servers into its operator's mining pool.

TOP RANSOMWARE

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

Global

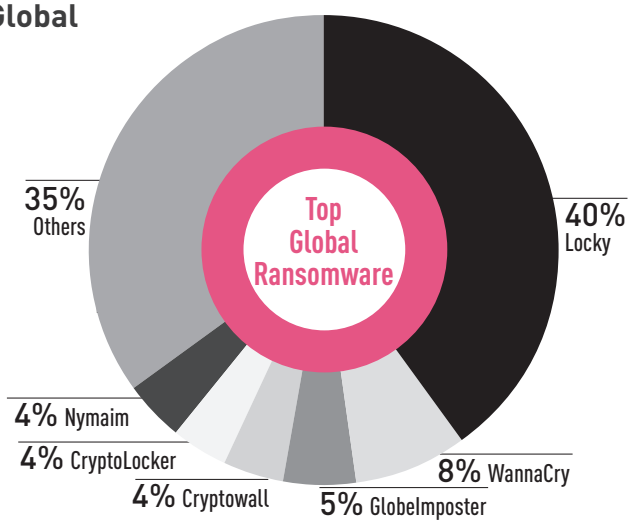


Figure 12: Most Prevalent Ransomware Globally

Americas

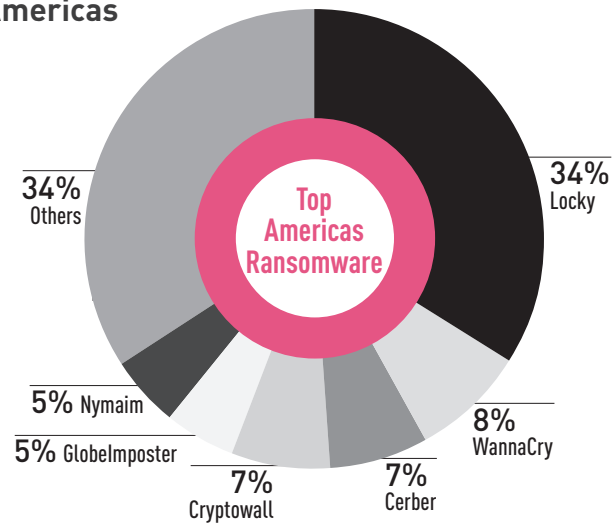


Figure 13: Most Prevalent Ransomware in the Americas

EMEA

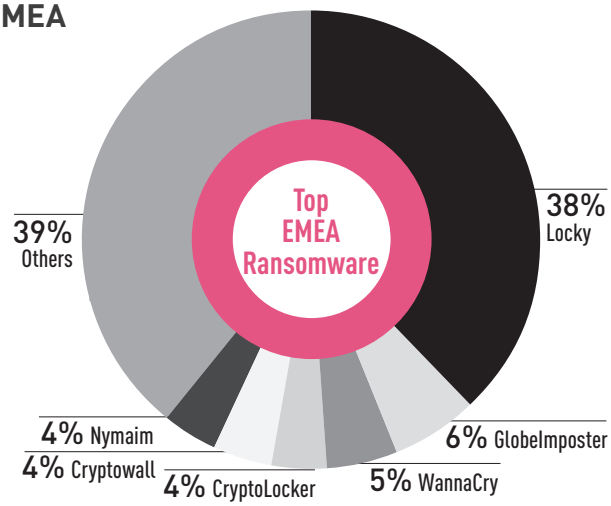


Figure 14: Most Prevalent Ransomware in EMEA

APAC

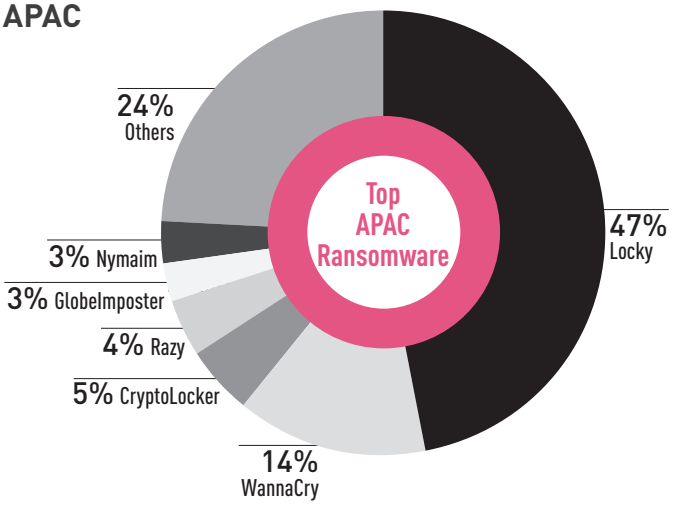


Figure 15: Most Prevalent Ransomware in APAC

Ransomware Global Analysis

- **Locky** Ransomware, which first emerged in February 2016, has kept the crown, leading the top global and regional ranks as one of the most prevalent Ransomwares of 2018. Surprisingly, the infamous **WannaCry** has also maintained its high rank of 2017, although it has been a bit more than a year since it had spread like wildfire to hundreds of thousands of devices. It appears that even a year later there are still machines infected with WannaCry that keep scanning the internet for vulnerable Windows machines.

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

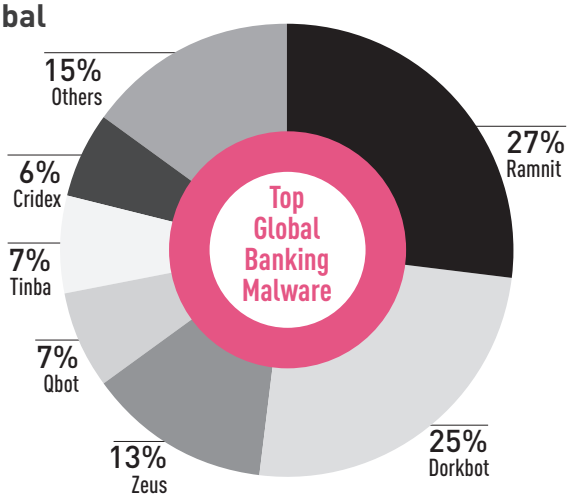


Figure 16: Most Prevalent Banking Malware Globally

Americas

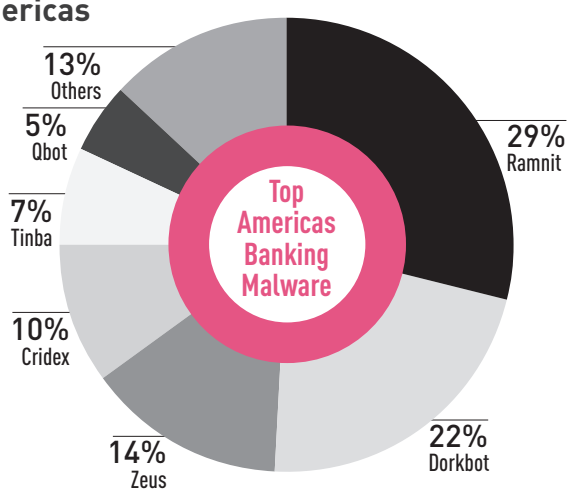


Figure 17: Most Prevalent Banking Malware in the Americas

EMEA

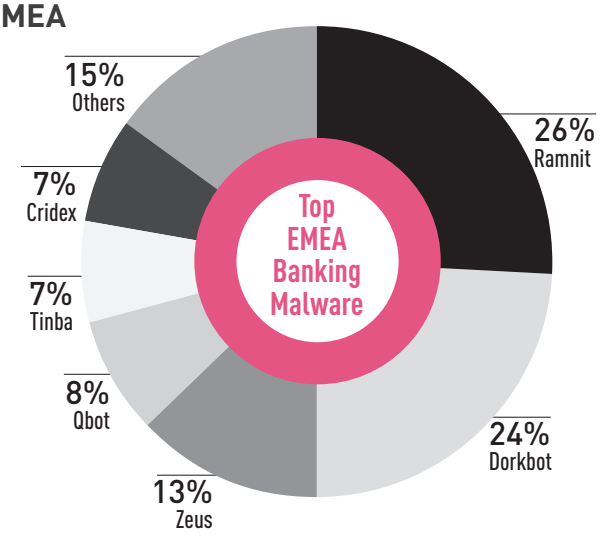


Figure 18: Most Prevalent Banking Malware in EMEA

APAC

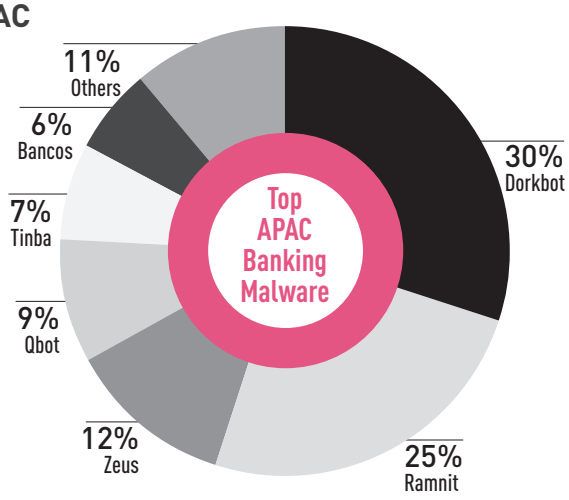


Figure 19: Most Prevalent Banking Malware in APAC

Banking Malware Global Analysis

- The most prominent banking Trojans dominating the Global Top Banking Malware list, **Ramnit** and **Zeus**, have kept their place at the top of the list since the second half of 2017. Both are persistent and evolving banking Trojans capable of recognizing when a victim is visiting a banking website, and then they utilize keylogging or web injects to harvest login credentials or more sensitive information such as PIN numbers. In addition **Dorkbot**, known malware that dates back to 2012, has entered back into the top ranks, starring as the APAC Top Banking Malware and also ranking second in the Americas, in the EMEA and globally. Dorkbot, designed to allow its operators remote code execution capabilities with a primary motivation to steal sensitive banking information, was observed last April using a new code injection technique dubbed "Early bird", allowing it to avoid detection by anti-malware security products.

TOP MOBILE MALWARE

In this section 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

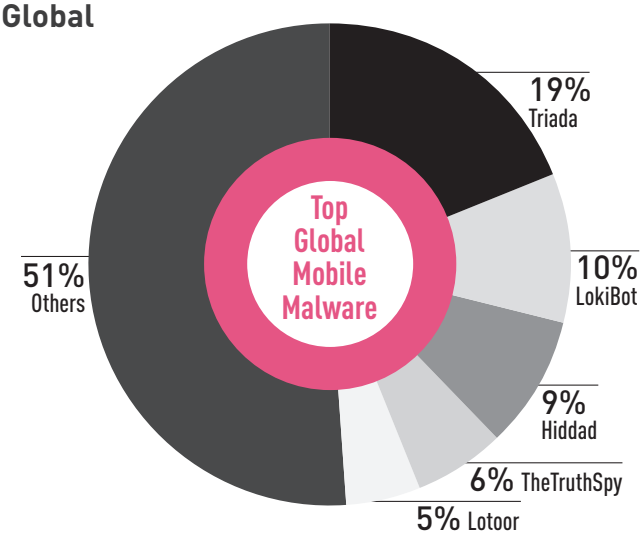


Figure 20: Top Mobile Malware Globally

Americas

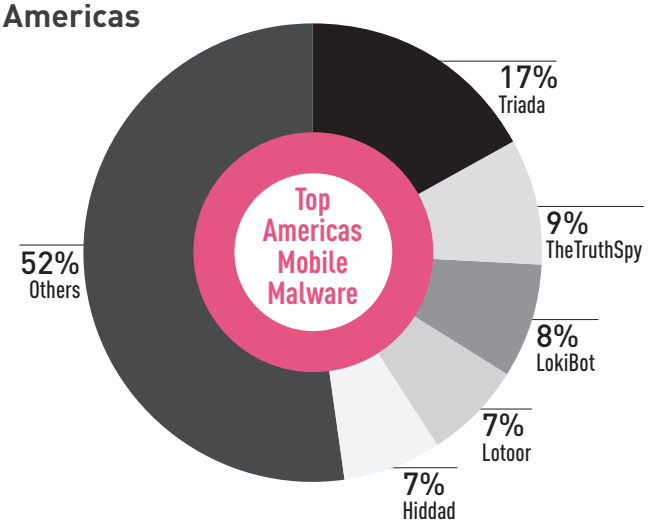


Figure 21: Top Mobile Malware in the Americas

EMEA

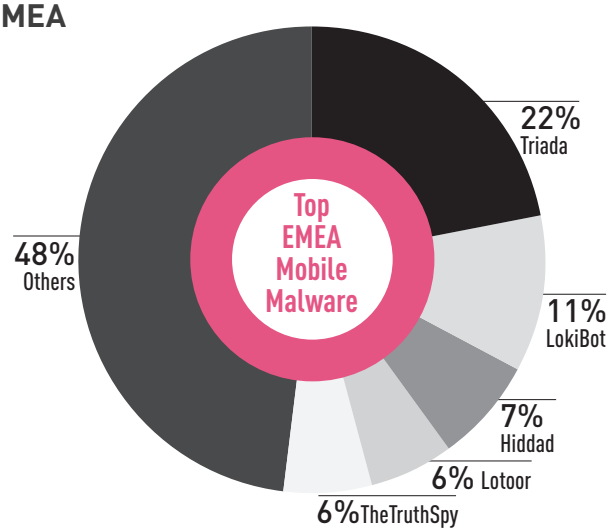


Figure 22: Top Mobile Malware in EMEA

APAC

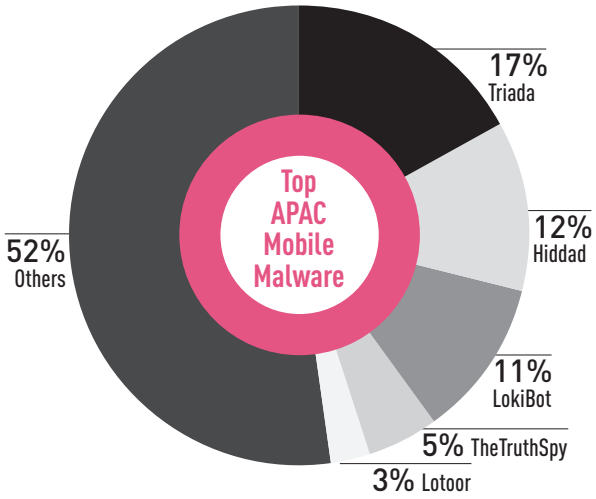


Figure 23: Top Mobile Malware in APAC

Mobile Malware Global Analysis

- **Triada**, a very powerful Android banking Trojan discovered in 2016 and considered to be one of the most advanced mobile threats, has reached the top of the global and regions rankings. Last March Triada was found pre-installed on 42 models of low-cost smartphones, infecting hundreds of thousands of victims and stealing their credit card data. Furthermore, a new Mobile malware family has entered the charts – **TheTruthSpy**, capable of monitoring WhatsApp messages, Facebook chats, and internet browsing history. TheTruthSpy only emerged in May 2018 and is already ranked third in the world, and second in EMEA and APAC.

CYBER ATTACK CATEGORIES BY REGION

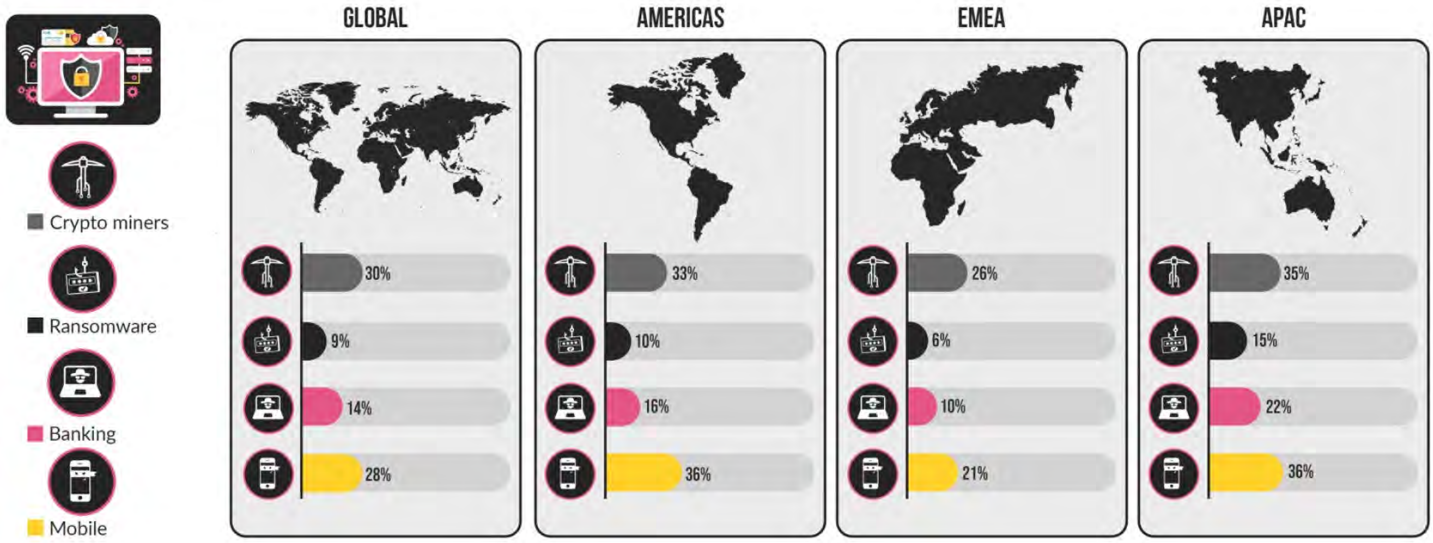


Figure 24: Attack Categories by Region

GLOBAL THREAT INDEX MAP

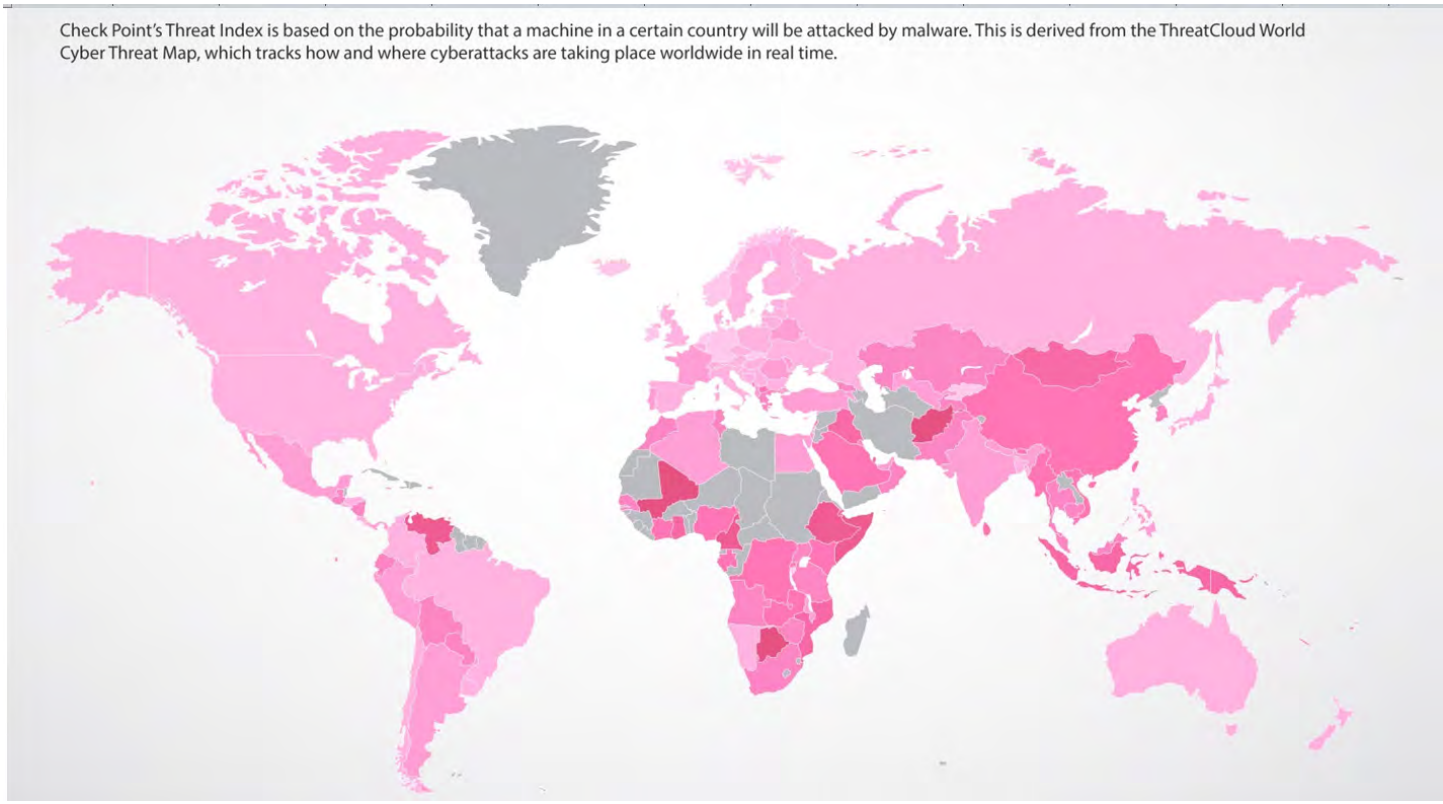


Figure 25: The 2018 H1 World Cyber Threat Index Map

MAJOR CYBER BREACHES (H1 2018)

So far in 2018 cyber breaches continue to affect businesses in all sectors, putting at risk the sensitive information of billions of people. Moreover, threat actors are targeting all geographies as all regions suffered numerous attacks. Below is a recap of the major attacks in each region.

Americas

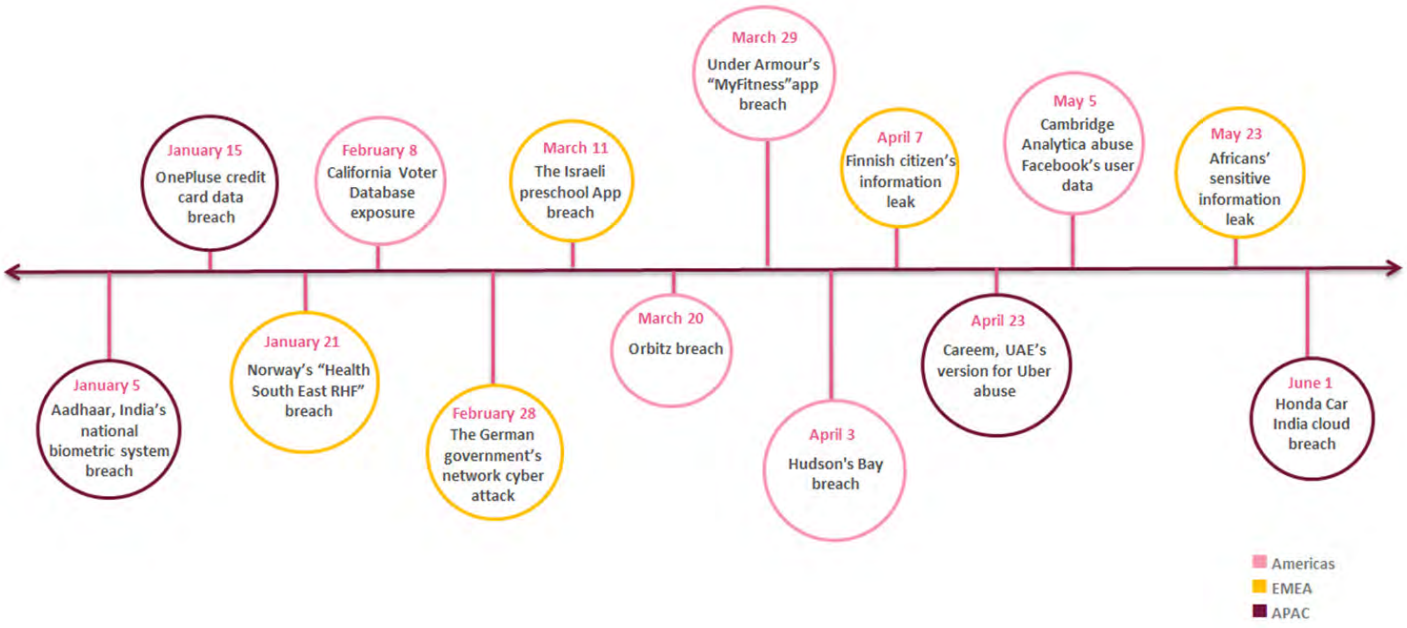
- **February:** Voter registration information of over 19.5 million California residents was leaked online via an unsecured MongoDB database and held for ransom by threat actors. The *Sacramento Bee*, a local Sacramento-area newspaper that announced itself as the source of the breach, refused to pay the ransom and deleted the database.
- **March:** The leading fitness company "Under Armour" suffered a major breach of the company's app, MyFitnessPal. The company announced that the breach had exposed the data of 150 million users of the app including their user names, email addresses and hashed passwords.
- **March:** Orbitz, an Expedia-owned travel site announced a data breach leading to the disclosure of 880,000 payment cards used for online purchasing, along with other personal information belonging to customers. The incident had taken place between October 2016 and December 2017.
- **April:** Hudson's Bay, the parent company of Saks Fifth Avenue and Lord & Taylor, suffered a major breach of the company's payment systems. The breach was attributed to the FIN7 APT group who managed to steal credit and debit card information of about five million consumers who had shopped at both of the retailers.
- **May:** The data-mining company, Cambridge Analytica, was been accused of exploiting Facebook to harvest up to 87 million individuals' personal details in order to target US voters in the 2016 Presidential election. This successful exploitation was achieved by using an app that paid users to take a personality test and give consent for data collection.

Europe, the Middle East and Africa (EMEA)

- **January:** Norway's biggest health authority, Health South East RHF, suffered a data breach, which affected more than half of the nation's population. Cybercriminals stole the personal info and health records of around 2.9 million Norwegians.
- **February:** The German Government announced that it experienced a massive cyber-attack in which several of its networks, including an isolated one, were breached and infected with malware for about a year. The breach was only discovered in December, and included the servers of the Interior Ministry and other unspecified ones. German authorities suspect the Russian hacking group APT28 was behind the attack.
- **March:** A serious security breach in an app named "Remini" left millions of pictures of Israeli children, as well as the personal details of more than 100,000 parents, vulnerable to being leaked to the internet. The app allows preschool teachers to contact the parents and share any relevant information including schedules of classroom activities, pictures, videos and personal information with them.
- **April:** The New Business Center in Helsinki, Finland, fell victim to a major data breach. Threat actors stole over 130,000 users' login usernames and passwords which were stored on the site in plain-text.
- **May:** A database containing the sensitive personal data of nearly one million South Africans were publicly leaked online. The database was discovered on a public web server belonging to a company that handles electronic traffic fine payments in South Africa and included names, ID numbers, e-mail addresses, and passwords.

Asia-Pacific (APAC)

- **January:** Aadhaar, India's national biometric system, fell victim to a major data breach as threat actors gained access to the personal information of more than one billion Indian residents. The threat actors later offered a paid service via WhatsApp to help victims retrieve their information, including names, addresses, postal codes, photos, phone numbers, and email addresses.
- **January:** The Chinese smartphone manufacturer, OnePlus, fell victim to a credit card data breach affecting more than 40,000 customers. A malicious script was injected into its payment page code and was able to capture full credit card information, including credit card numbers, expiry dates and security codes directly from the browser window.
- **April:** Careem, the United Arab Emirates version of Uber was hacked and the private data of 14 million drivers and customers was stolen including names, phone numbers, email addresses and ride data.
- **June:** 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:** Honda Car India left personal data of over 50,000 users exposed on two public unsecured Amazon S3 buckets. The exposed data belonged to the users of the remote car management app Honda Connect App and included names, phone numbers, emails, passwords, Car VIN, Car Connect IDs and more.



GLOBAL TOP EXPLOITED VULNERABILITIES

The top attacks list presented below is based on data collected by Check Point's Intrusion Prevention System (IPS) solution and details some of the most popular and interesting attack techniques and exploits observed by Check Point researchers in the first half of 2018.

- **Drupalgeddon2 and Drupalgeddon3 (CVE-2018-7600, CVE-2018-7602)** – The exposure of highly critical flaws in Drupal, the Content Management System (CMS) giant, had a significant impact on the threat landscape. The vulnerabilities, affecting over a million Drupal websites, may have allowed an unauthenticated attacker to perform remote code executions on Drupal installations, taking full control over the affected website. Proofs of concept that were released put the unpatched Drupal sites under constant attack. These attacks ranged from various kinds of crypto-miners placed both on servers and websites, to delivering RATs and infostealer malware, conducting Tech support scams, and creating massive botnets.

- **RTF (CVE-2017-11882, CVE-2017-0199, CVE-2018-0802)** – Security flaws in Microsoft Office Rich Text Format (RTF) were widely abused by threat actors throughout the first half of 2018. 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. This year we have witnessed these vulnerabilities highly used in malspam campaigns, including several lunched by APT groups, and within documents employed as downloaders for various malware types. Among them are the malware LokiBot, Remcos RAT, KevDroid Android RAT, ThreadKit exploit builder kit and Zyklon.

- **"Double kill" (CVE-2018-8174)** – Double Kill is a remote code execution Internet Explorer (IE) zero-day vulnerability of Windows VBScript engine, affecting the latest versions of IE and any other applications that utilize IE components. When exploited, this vulnerability allows remote attackers to embed malicious VBScript to Office documents or websites and run malicious payloads that are loaded from a remote server. It has been two years since a zero-day vulnerability was found in the browser and the discovery of this one has made many headlines in 2018, leveraged by threat actors such as the APT-C-06 group, and also exploited by the infamous RIG Exploit Kit to deliver a Monero Cryptominer.

- **IoT vulnerabilities (CVE-2018-10561, CVE-2018-10562)** – This year security flaws were found in over one million Dasan GPON home routers, exposing them to a wide range of attacks. These vulnerabilities allow any attacker to access the router's settings by appending a certain string to any URL and gain control over the device. The vulnerabilities were widely leveraged by botnet herders to recruit their armies, among them the Satori, Mirai and TheMoon botnets.

Interestingly, according to Check Point global attack sensors, 99% of the attacks observed throughout the first half of 2018 leveraged vulnerabilities registered in 2017 and earlier and over 40% of attacks used vulnerabilities that are at least seven years old.

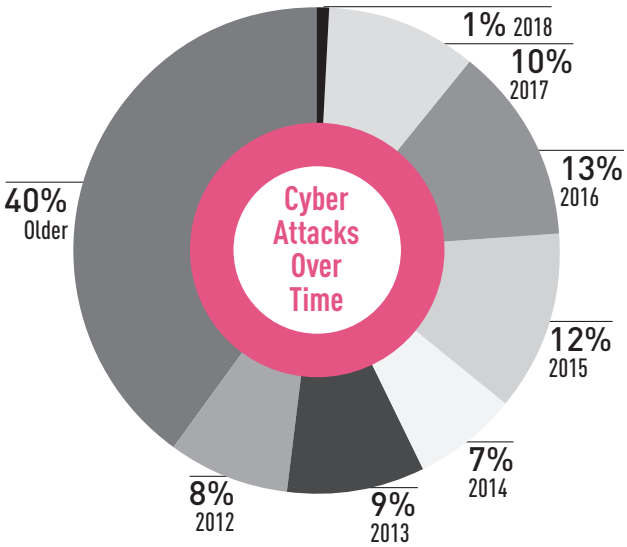


Figure 26: Percentage of attacks leveraging vulnerabilities found since 2012 and earlier

ADDITIONAL OBSERVATIONS/CONCLUSIONS

With the fifth generation of the cyber threat landscape now firmly established, it should come as no surprise that the types of threats seen in 2017 have continued into 2018. Neither do they show any sign of slowing. If anything, they have become more entrenched and are now reaching deeper into organizations' IT infrastructure.

Whether by embedding themselves through preinstalled malware in the mobile supply chain or leveraging cloud platforms' higher computing resources to mine the valuable cryptocurrencies, threat actors are adapting today's technologies to their own financial gain. In addition, large data breaches have not abated either, bringing reputational damage as well as large financial costs to those that experience them.

As a result, it is imperative that organizations worldwide equip themselves with the highest and most advanced protection technologies in order to keep ahead of these trends and prevent themselves from being the next victim to hit the headlines.

RECOMMENDATIONS

What is needed is an advanced protection technology that can give you zero-day prevention from unknown and more sophisticated attacks that may bypass traditional signature-based technologies.

Check Point SandBlast provides that technology by consisting of two main elements: **Threat Emulation** and **Threat Extraction**.

Threat Emulation is an extremely powerful evasion resistant sandbox technology which is proactively combined with Threat Extraction to deliver clean files to users. By combining these two elements, a proactive approach means only clean files are allowed to enter the organization, and with threat emulation that can identify zero-day and unknown malware attempting to enter your network, you can ensure very strong coverage for the unknown element of cyber attacks in general and crypto mining attacks in particular.

SandBlast also includes a family of products designed to cover your entire IT infrastructure.

Check Point SandBlast NETWORK

SandBlast is available across all Check Point gateways to protect your mail, users browsing the web within your network, and your data centers.

Check Point SandBlast AGENT

SandBlast Agent on the endpoint will give you direct advanced protections on all of your endpoints and integrated protections for the browsers within the endpoint, for as we have seen, web browsing is a fundamental way of being attacked.

CHECK POINT CloudGuard

SandBlast is also a core part of CloudGuard, which covers both SaaS and IaaS so that all of your cloud assets can also be covered by this advanced technology.

Check Point SandBlast MOBILE

SandBlast Mobile gives you coverage for iOS and Android against all forms of known and unknown mobile attacks, including Man-in the-Middle attacks over Wi-Fi networks, malicious links sent over SMS, and OS exploits.

Check Point SandBlast <API>

SandBlast also comes with an API which means you can integrate the capabilities of SandBlast with any business process or business logic that you have that is not strictly covered by the other products in the SandBlast family.

APPENDIX – MALWARE FAMILY DESCRIPTIONS

- **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.
- **AndroRAT –** AndroRAT is an open-source tool that first emerged in November 2012, targeting Android devices. AndroRAT allows a remote attacker to take control over the victim's machine, make phone calls and send SMS messages of infected devices, access victim's GPS coordinates, and use the microphone and camera.
- **AuthedMine –** AuthedMine is a version of the infamous JavaScript miner Coinhive. Similarly to Coinhive, Authedmine is a web-based crypto miner used to perform online mining of Monero cryptocurrency when a user visits a web page without the user's knowledge or approval the profits with the user. However, unlike Coinhive, Authedmine is designed to require the website user's explicit consent before running the mining script.
- **Bancos –** Bancos steals financial information, using keylogging to record the victim's credentials as they are entered on a targeted bank web page. Bancos can also supplement or replace a legitimate bank login page with a fake web page.
- **Cerber –** Cerber, also known as Zerber, which was first introduced in February 2016, is an offline Ransomware, meaning that it does not need to communicate with its C2 server before encrypting files on an infected machine.
- **Coinhive –** Crypto Miner designed to perform online mining of Monero cryptocurrency when a user visits a web page without the user's approval. The implanted JS uses great computational resources of the end users' machines to mine coins, thus impacting its performance.
- **Cridex –** Cridex is a worm for the Windows platform. It attempts to steal victims' credentials, such as credit card information. It can download and execute other malicious files on to the infected system. It may spread itself via removable drives and network shares.
- **CryptoLocker –** Cryptolocker is a Ransomware, first detected in 2013, which targets the Windows platform. It runs in the background and encrypts various files and documents found on compromised hosts.
- **Cryptoloot –** A JavaScript Cryptominer, designed to perform online mining of Monero cryptocurrency when a user visits a web page without the user's approval. The implanted JS uses great computational resources of the end users machines to mine coins, thus impacting its performance. It is a competitor of Coinhive.
- **CryptoPool –** Web-based Cryptominer 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.
- **Cryptowall –** Cryptowall is a leading Ransomware Trojan which encrypts files on an infected machine and then asks users to pay for them to be decrypted. It spreads through malvertising and phishing campaigns. Cryptowall first appeared in 2014.
- **Dorkbot –** IRC-based Worm designed to allow remote code execution by its operator, as well as the download of additional malware to the infected system, with the primary motivation being to steal sensitive information and launch denial-of-service attacks.
- **Dorvku –** Dorvku is a 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.
- **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.
- **Gamarue –** Gamarue is a modular bot with a loader, which downloads additional modules from its C&C server. The loader has both anti-VM and anti-debug features. It injects into trusted processes to hide itself and then deletes the original bot.
- **GandCrab –** GandCrab is a Ransomware which targets mainly Scandinavia and the English-speaking countries. GandCrab is distributed via the RIG and GrandSoft exploit kits, as well as email spam. The Ransomware is operated in an affiliates program, with those joining the program paying 30%-40% of the ransom revenues to the GandCrab author. In return affiliates get a full-featured web panel and technical support.

- **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.
- **Graftor –** Graftor is an adware and browser-hijacker that has Trojan-like capabilities. It can be used as an attack vector for other malicious software. It is also known for hiding executables and DLLs in PNG files to avoid detection.
- **Hacker Defender –** Hacker Defender is a rootkit for Windows 2000 and Windows XP, and may also work on later Windows NT based systems. The rootkit modifies several Windows and native API functions to remain undetected by security softwares.
- **Hiddad –** Android malware which repackages legitimate apps and then releases 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.
- **HiddenMiner –** A strain of Android Cryptominer that was spotted in April 2018. The HiddenMiner is delivered through a fake Google Play update app, exhausting the devices resources in mining Monero.
- **JSECoin –** Web-based Cryptominer 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.
- **Kraken –** Kraken is a Ransomware Trojan that targets the Windows platform. The malware collects system information and sends it to a remote attacker via Discord chat service. The malware encrypts files with the specific extensions on the infected system. It downloads and executes the decryptor on the infected system and demands the infected user to pay a ransom in order to get the files decrypted. It also can kill processes.
- **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.
- **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.
- **Lotoor –** Lotoor is a hack tool that exploits vulnerabilities on the Android operating system in order to gain root privileges on compromised mobile devices.
- **Necurs –** Necurs is one of the largest spam botnets currently active in the wild, and it is estimated that in 2016 it consisted of some 6 million bots. The botnet is used to distribute many malware variants, mostly banking Trojans and Ransomware.
- **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.
- **Nymaim –** Nymaim is a malware dropper and downloader, first observed in 2013. Originally, Nymaim dropped Ransomware, after being distributed by the 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.
- **Panda –** Panda is a Zeus variant that was first observed in the wild at the beginning of 2016, and is distributed via Exploit Kits. Since its initial appearance, Panda has targeted financial services in Europe and North America. Before the Olympic Games of 2016, it also ran a special campaign against Brazilian banks.
- **Parite –** Parite is a polymorphic virus which infects executable files (EXE and SCR) on the infected host and on network drive. It drops a malicious DLL file into the Windows temporary directory which is injected into the explorer.exe process.
- **Ponmocup –** Ponmocup is a Botnet which has been active as of 2006 and reached its peak in 2011, with approximately 2.4 million controlled machines. Its infrastructure is complex and includes dedicated servers for various tasks.
- **Proslikefan –** Proslikefan is a Worm that targets Windows systems supporting JavaScript. This malware attempts to spread through network shares, removable drives, and peer-to-peer programs. It attempts to send system information to a remote server.
- **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.

- **Ramnit –** Ramnit is a banking Trojan which incorporates lateral movement capabilities. Ramnit steals 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.
- **RIG Exploit Kit –** RIG EK was first introduced in April 2014. It has since received several large updates and continues to be active to this day. RIG serves many threat actors while distributing their malware among the victims it succeeded in exploiting.
- **Roaming Mantis –** Roaming Mantis is an Android banking Trojan that first emerged on March 2018. It is capable of stealing users' sensitive information, login credentials and the secret code for two-factor authentication. Roaming Mantis is being distributed using DNS hijacking attacks, disguised as Chrome browser or Facebook apps. An evolved version of Roaming Mantis is also targeting iOS devices with phishing attacks, and desktops and laptops with the Coinhive cryptomining script.
- **RottenSys –** RottenSys is a widespread Android-oriented Trojan that has targeted nearly 5 million Android devices. RottenSys came preinstalled on the devices disguised as a legitimate 'System Wi-Fi service' app. RottenSys malware was originally used to aggressively display ads on users' devices, but it also has extensive capabilities, including silently installing additional apps and UI automation.
- **RoughTed –** Large scale Malvertising campaign used to serve various malicious websites and payloads such as scams, adware, and Ransomware. It can be used to attack any type of platform and operating system, and utilizes ad-blocker bypassing and fingerprinting.
- **RubyMiner –** RubyMiner is a Monero miner targeting both Windows and Linux servers trying to find vulnerable versions (such as PHP, Microsoft IIS, and Ruby on Rails) in order to mobilize them to its mining pool, and to install the open source Monero miner named XMRig.
- **Sality –** Sality is a virus which spreads itself by infecting .exe and .scr files as well as via removable drives and network shares. Systems infected with Sality can communicate over a peer-to-peer (P2P) network for spamming purposes.
- **Smoke Loader –** Smoke Loader is a Trojan that enables an attacker to remotely control an infected computer and perform a range of malicious activities including downloading and installing other malware based on the geo-location of the victim, and stealing passwords.
- **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 their account.
- **Triada –** Modular Backdoor for Android which grants super-user privileges to download a malware. Triada has also been seen spoofing URLs loaded in the browser.
- **Trickbot –** Trickbot is a Dyre variant that emerged in October 2016. Since its first appearance, it has been targeting banks, mostly in Australia and the U.K, and lately it has also started appearing in India, Singapore and Malesia.
- **WannaCry –** Ransomware which was spread in a large-scale attack on May 2017, utilizing a Windows SMB exploit called EternalBlue in order to propagate within and between networks.
- **XMRig –** XMRig is open-source CPU mining software used for the mining process of the Monero cryptocurrency, and first seen in-the-wild on May 2017.
- **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.

ABOUT CHECK POINT RESEARCH

Check Point Research provides leading cyber threat intelligence to Check Point Software customers and the greater intelligence community. The research team collects and analyzes global cyber attack data stored on ThreatCloud to keep hackers at bay, while ensuring all Check Point products are updated with the latest protections. From the moment a breach is initiated, ThreatCloud begins sharing data across the entire network, providing researchers with the intelligence they need to deeply analyze and report on attacks. Check Point Research publications and intelligence sharing fuel the discovery of new cyber threats and the development of the international threat intelligence community to keep you secure.

LEADING THE THREAT INTELLIGENCE COMMUNITY

The research team consists of over 100 analysts and researchers currently cooperating with other security vendors, law enforcement, and different CERTs. Their data sources also include open sources, the ThreatCloud customer sharing network, and dark web intelligence. Internally, the team has developed their own machine learning modules, anomaly detection, reverse engineering, and campaign hunting techniques that all assist in staying ahead of hackers and the latest cyber threats.

CONTACT US

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 |
Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070
Tel: 800-429-439 | 650-628-2000 | Fax: 650-654-4233

checkpoint.com