cp<r>

CHECK POINT RESEARCH

CYBER ATTACK TRENDS:
2019 MID-YEAR REPORT

Check Point®
SOFTWARE TECHNOLOGIES LTD

TABLE OF CONTENTS

INTRODUCTION

The first half of 2019 demonstrated that no environment is immune to cyber attacks. We have witnessed threat actors developing new tool sets and techniques, targeting corporate assets stored on cloud infrastructure, individuals' mobile devices, trusted third-party suppliers' application and even popular mail platforms.

One of the dominating ongoing trends in 2019 is targeted ransomware attacks. This year collaborations between threat actors allowed even more destructive attacks that paralyzed numerous organizations worldwide. What ends with a ransomware attack usually starts with a more silent sequence of bot infections.

Still highly visible, cryptominers are on the decline this year – only 21% of organizations worldwide were affected by cryptominers' attacks in comparison to 42% during its peak in 2018. This was the outcome after shutting down the 'CoinHive' drive-by mining service.

Software supply chain attacks attracted public and government attention. In such attacks threat actors inject malicious code into components of legitimate applications, victimizing a large number of unsuspecting users. The accumulation of several cases since the beginning of the year led the American government to devote special attention to this evolving threat and will soon publish official recommendations on ways to minimize the impact of such attacks.

To provide organizations with the best level of protection, security experts should be attuned to the ever-changing landscape and the latest threats and attack methods. With data drawn from Check Point's ThreatCloud World Cyber Threat Map between January and June 2019, combined with primary research performed by the company's cyber security experts , the following report holds a comprehensive overview of the trends observed in the various categories of cryptominers, ransomware, botnet, banking Trojans, data breaches, and mobile threats.

SOFTWARE SUPPLY CHAIN ATTACKS ON THE RISE

Growing cyber security awareness and the increasing use of security solutions have made cyber attack attempts more challenging and have pushed motivated threat actors to extend their attacks to new vectors. Focusing on the supply chain of a selected target is such an attempt. In software supply-chain attacks the threat actor typically installs malicious code into legitimate software by modifying and infecting one of the building blocks the software relies upon. As with physical chains, software supply chains are only as strong as their weakest link.

Software supply chain attacks can be divided into two main categories. The first includes targeted attacks aiming to compromise well-defined targets, scanning their suppliers list in search of the weakest link through which they could enter. The ShadowHammer attack on ASUS is a recent example. Attackers implanted malicious code into the ASUS Live Update utility, allowing them to later install backdoors on millions of remote computers. Interestingly, the malicious implant included a hardcoded list of several hundred network adapters' MAC addresses which means second stage backdoors could be surgically delivered to predefined targets.

In the second category, software supply chains are used to compromise as many victims as possible by locating a weak link with a large distribution radius. One such example is the attack on PrismWeb, an e-commerce platform, in which attackers injected a skimming script into the shared JavaScript libraries used by online stores, affecting more than 200 online university campus stores in North America. Many of such MageCart style attacks utilize similar supply chain attack vectors.

The sharp increase in supply chain attacks has brought the US Department of Homeland Security (DHS) to establish the Information and Communications Technology Supply Chain Risk Management Task Force which started its work earlier this year. In addition, on May 15, the White House issued an executive order, declaring foreign supply chain threats as a national emergency and empowering the Secretary of Commerce to prohibit transactions – later leading to a ban of the technology giant Huawei.

The mobile arena is also prone to supply chain attacks. Operation Sheep, as reviewed by Check Point Research, exposed the SWAnalytics infected SDK. Non-suspecting mobile apps developers used this SDK and thus unknowingly assisted in distributing malicious contact-harvesting malware to more than 100 million end-users.

From the hacker's point of view this method has at least two distinct advantages – they rely on the good reputation of third-party vendors and multiply their circulation manifold by using the original vendor's distribution mechanism.

The supply chain attack vector has been a growing trend for a while but the reaction of US and international authorities testify to both its magnitude and severity. This type of attack vector is more than just a dangerous technique; it strikes at the basic trust on which supplier-customer relations are based.

EMAIL SCAMS GEAR UP

It is safe to say there is no organization or individual that is not exposed to multiple malicious email campaigns at any given time. But with the growing attention of security vendors and the public awareness for email attacks, threat actors have introduced improved phishing tactics aimed at establishing credibility among victims, as well as advanced evasion techniques to bypass mail security solutions.

With this shift, Check Point researchers witnessed a surge in the volume of Sextortion scams and business email compromise (BEC), which fraudulently trick victims into making a payment through blackmail or by convincingly impersonating others, respectively. Both scams adopt these elements and do not necessarily contain any malicious attachments or links, which makes them even harder to detect.

Email scammers have started to employ various evasion techniques designed to bypass security solutions and anti-spam filters. The various evasions we detected included encoded emails, images of the message embedded in the email body, as well as complex underlying code that mixes plain text letters with HTML character entities. Social engineering techniques, as well as varying and personalizing the content of the emails, are additional methods allowing the scammers to fly safely under the radar of anti-spam filters and reach their target's inbox.

Determined to convince victims of their credibility, this year saw the Sextortion scammers doing everything possible to make their victims worried enough to pay up and avoid the publication of the alleged sexual materials. This mainly includes providing the victim's personal credentials as evidence, which were usually leaked in previous data breaches or purchased in underground forums. Other tactics, mainly common in BEC attacks, are domain and display-name spoofing as well as sending the emails from valid high-reputation entities such as compromised Microsoft Office 365 or Gmail accounts. In April, one sextortion campaign went as far as pretending to be from the CIA and warned victims they were suspected of distributing and storing child pornography, while demanding $10,000 in Bitcoin.

In a world where email scams have become a business in which professional cyber criminals are hired to run email campaigns, it is also safe to say that this industry is definitely here to stay. Spammers will continue to improve their capabilities and techniques to ensure their scams' profitability, just as security vendors will continue to improve their products to protect against such threats.

ATTACKS AGAINST CLOUD ENVIRONMENTS

The growing popularity of public cloud environments has led to an increase of cyber attacks targeting resources and sensitive data residing within these platforms.

Following the 2018 trend, practices such as misconfiguration and poor management of cloud resources remained the most prominent threat to the cloud ecosystem in 2019 and, as a result, subjected cloud assets to a wide array of attacks. This year, misconfiguring cloud environments was one of the main causes for a vast number of data theft incidents experienced by organizations worldwide.

In April, more than half a billion records of Facebook's users were exposed by a third party on unprotected Amazon cloud servers. Misconfigured Box.com accounts leaked terabytes of extremely sensitive data from many companies, and in another case sensitive financial information of 80 million Americans hosted on a Microsoft cloud server was exposed online.

Besides information theft, threat actors intentionally abuse the different cloud technologies for their computing power. So far this year, cloud cryptomining campaigns stepped up, upgraded their technique set and were capable of evading basic cloud security products, abusing hundreds of vulnerable exposed Docker hosts and even shutting down competitors' cryptomining campaigns operating in the cloud.

In addition, in 2019 Check Point researchers witnessed an increase in the number of exploitations against public cloud infrastructures. A vulnerability in SoftNAS Cloud platform discovered in March may have allowed attackers to bypass authentication and gain access to a company's web-based admin interface and then run arbitrary commands. Furthermore, a new type of attack vector, dubbed Cloudborne, demonstrated that hardware re-provisioned to new customers could retain backdoors that can be used to attack future users of the compromised system.

With the number of enterprises that migrate their storage and computing infrastructure to the cloud environment increasing, best security practices must be followed and proper solutions implemented in order to prevent the next massive data breach.

THE EVOLVING MOBILE LANDSCAPE

Since all of our personal and business lives are managed and stored within mobile devices, threat actors are today extremely motivated to launch a wide range of attacks: profitable advertising campaigns, sensitive credential theft through fake apps, and surveillance operations are just some of the exploits conducted. So far this year we have seen more and more malicious actors adapting techniques and methods from the general threat landscape to the mobile world.

As one of the most popular malware types, banking malware has successfully infiltrated the mobile cyber arena with a sharp rise of more than 50% compared to 2018. In correlation to the growing use of banks' mobile applications, malware capable of stealing payment data, credentials and funds from victims' bank accounts have been pushed from the general threat landscape and became a very common mobile threat too.

The methodology used to distribute banking malware has also been borrowed from the general threat landscape – malware builders available for purchase in underground forums. In this way the builders of mobile bankers, such as Asacub and Anubis, can allow the creation of new versions of these malware, ready for massive distribution, by anyone willing to pay.

Another interesting element observed so far this year and inspired by the general threat landscape, is the dawn of the evasions era for the mobile arena. From a delayed execution to avoid sandboxes, through using transparent icons with empty application labels, to encrypting the malicious payload – it is quite evident that cyber criminals have boosted their skill sets and creativity for mobile attacks, determined to evade detection while keeping their malware persistent and effective.

This year, two fake applications were discovered on Google Play capable of monitoring devices' motion sensors to evade security emulators. Furthermore, in March, a new Android Trojan dubbed Gustuff was introduced to be capable of targeting customers of leading international banks and features various evasion techniques, including turning off Google Protect, the built-in anti-malware protection on Android.

So after probing the mobile field, threat actors are stepping up their efforts and as a result we can expect to see mobile attacks rise in the months and years ahead.

ONGOING TRENDS

In addition to the above major trends, there are three other cyber trends of 2018 that are still very relevant in 2019.

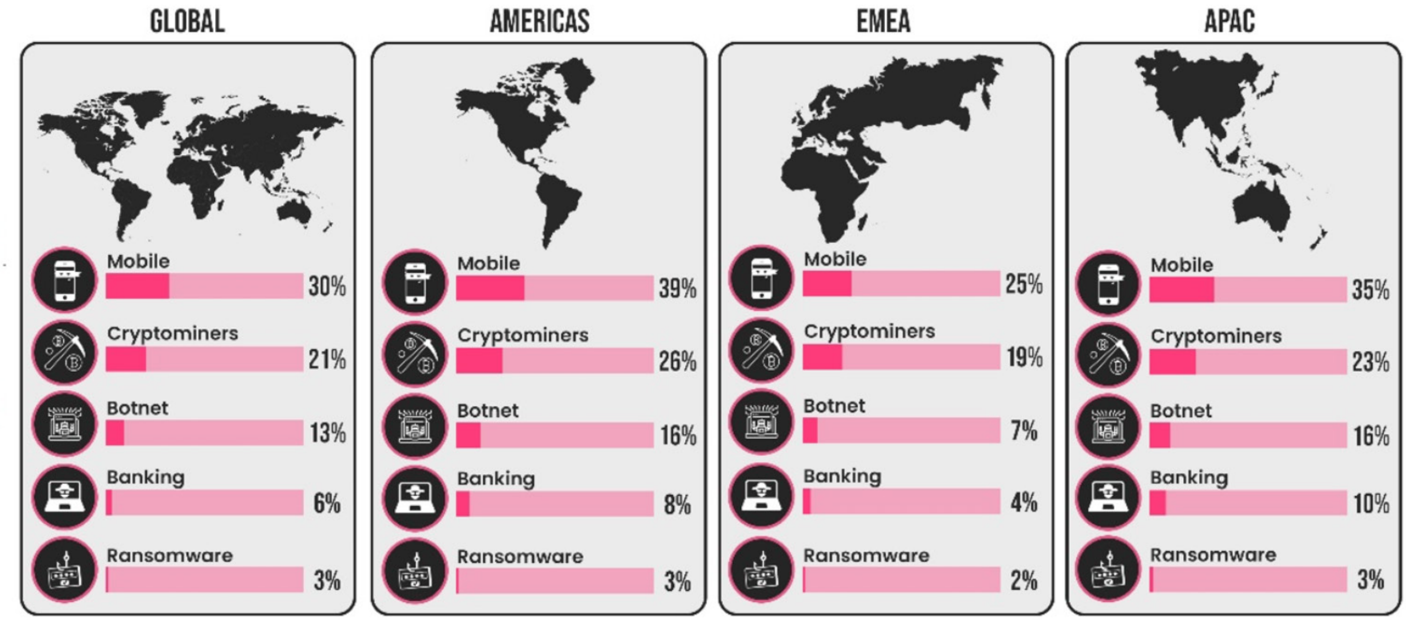
- **The targeted ransomware approach** which gained popularity during 2018 has proven effective in 2019; not a week goes by without some kind of tailored destructive ransomware attack hitting the headlines. One such prominent attack vector utilizes Emotet's vast distribution and victim base to select lucrative targets. Emotet is used to spread TrickBot within the compromised corporate network which, in turn, deploys Ryuk or other ransomware as the final payload. From countless local government entities through a cloud hosting provider, industrial corporations and airports, this year every organization is a potential target to the catastrophe of targeted ransomware, led by Ryuk and LockerGoga.

- The infamous **cryptominers** remained a prevalent malware type in the first half of 2019's threat landscape. This is despite the shutdown of the notorious drive-by mining service 'CoinHive' this March, which led to a decrease in the popularity of cryptominers among threat actors. As a result, and in order to remain prevalent in 2019, threat actors have been adopting a new approach regarding cryptominers, aiming at more rewarding targets than consumer PC's and designing more robust operations. Among the new victims one can find corporations, factories, powerful servers and even cloud resources. And if that was not enough, we have even seen them integrating cryptominers as part of a DDoS botnet for side-profits.

- **DNS Attacks** target one of the most important mechanisms that govern the internet – the Domain Name System (DNS). The DNS is in charge of resolving domain names into their corresponding IP addresses and it is a crucial part of the internet's trust chain. Such attacks target DNS providers, name registrars, and local DNS servers belonging to the targeted organization and are based on the manipulation of DNS records. DNS takeovers can compromise the whole network and enable multiple attack vectors: control of email communications, redirection of victims to a phishing site, and more. One of the biggest advantages DNS attacks provide is the option to issue legitimate looking certificates by Certificate Authorities which rely on DNS to verify that you are the legitimate holder of the domain in question.

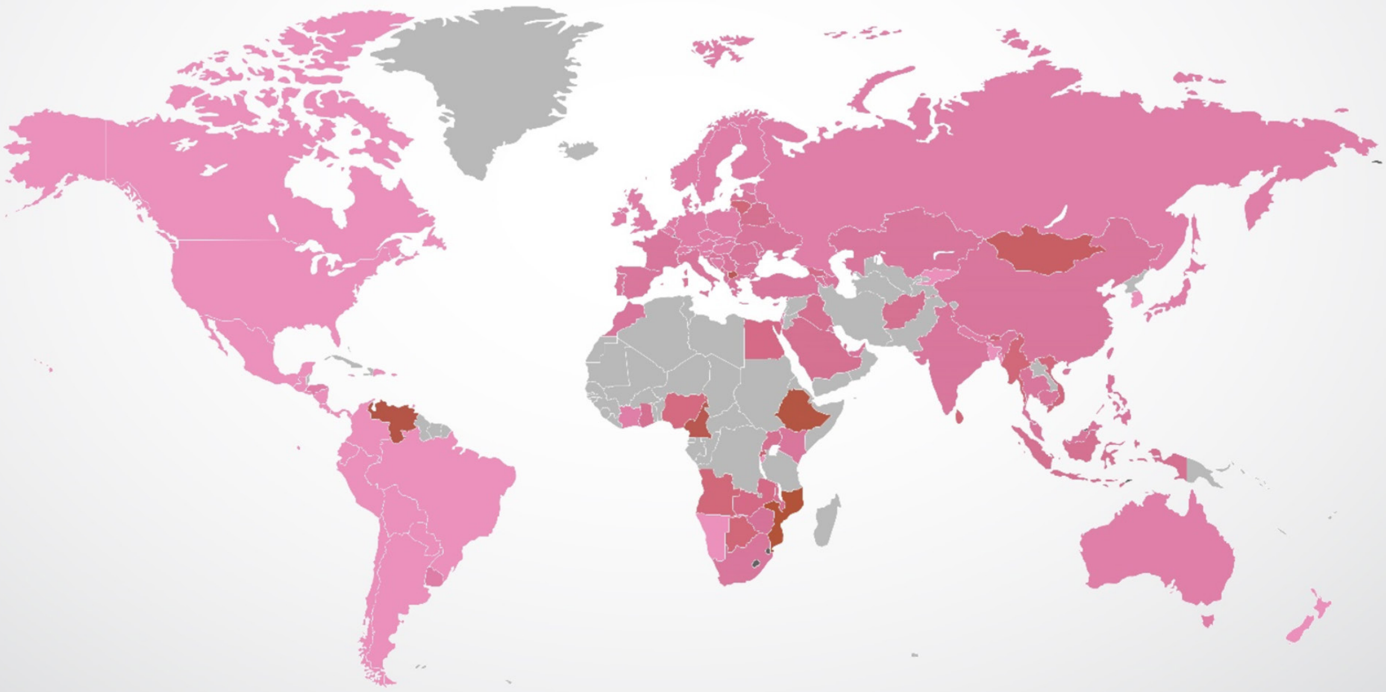
  The growing popularity of DNS attacks pushed the Department of Homeland Security and the Internet Corporation for Assigned Names and Numbers (ICANN) to issue official warnings of a significant risk to this key component of the Internet infrastructure. Large incidents involving DNS attacks include attacks on government and internet and telecommunications infrastructure, as depicted in the recent DNSpionage and SeaTurtle campaigns.

CYBER ATTACK CATEGORIES BY REGION

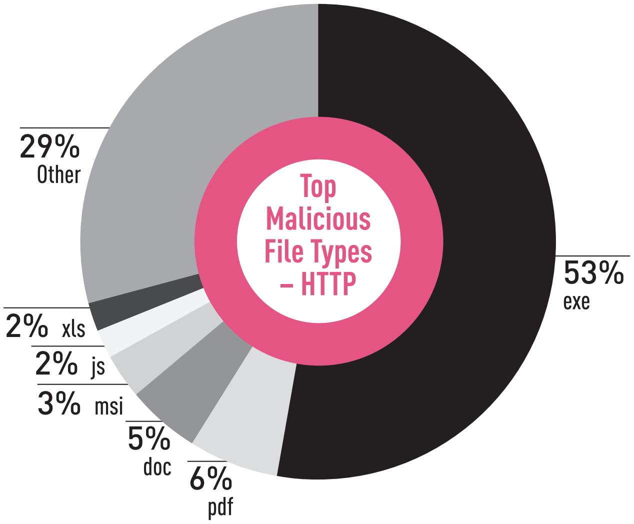


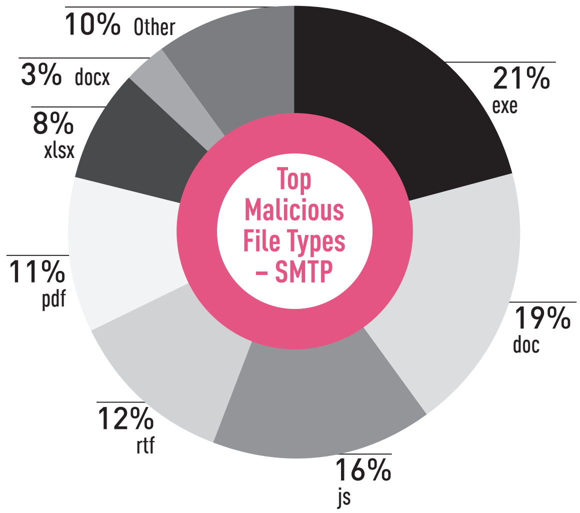
GLOBAL THREAT INDEX MAP

Check Point's Threat Index is based on the probability that a machine in a certain country will be attacked by malware. This is derived from the ThreatCloud World Cyber Threat Map, which tracks how and where cyberattacks are taking place worldwide in real time.

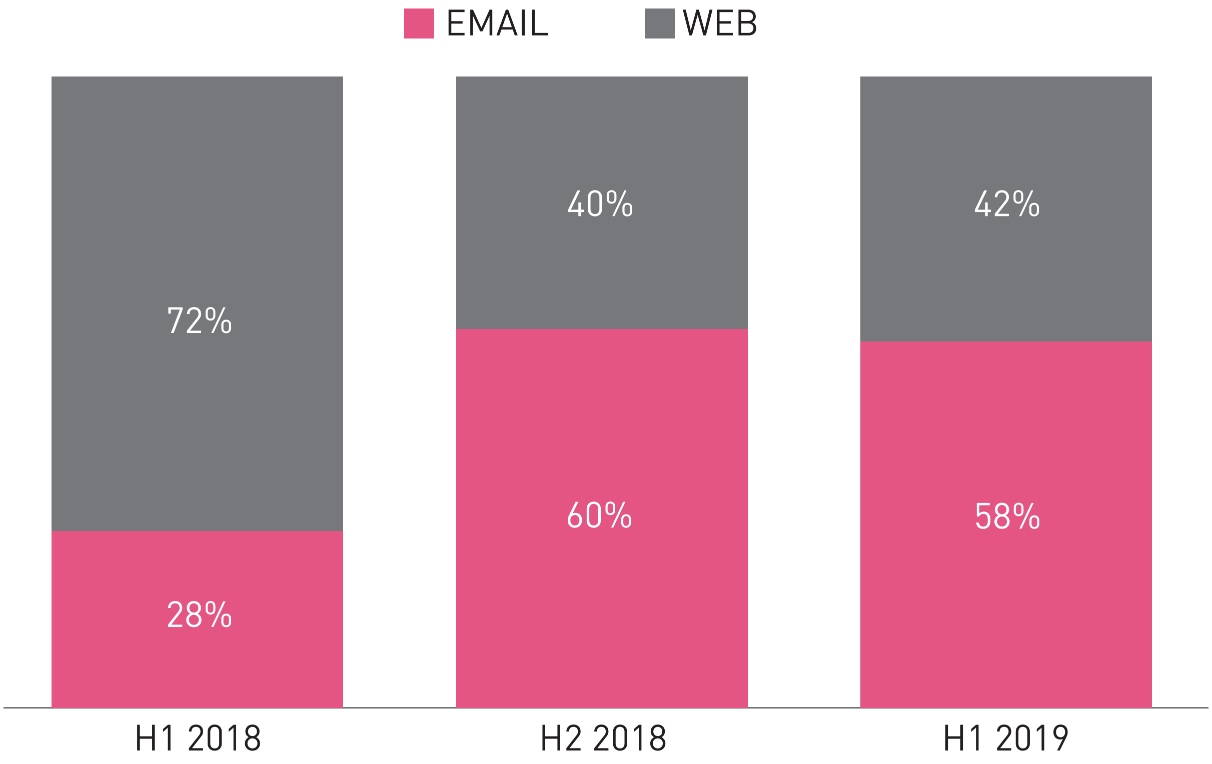


TOP MALICIOUS FILE TYPES – H1 2019





FILE DISTRIBUTION METHOD – MAIL VS. WEB ATTACK VECTORS (2018-2019)



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 2019.

TOP MALWARE FAMILIES

Global

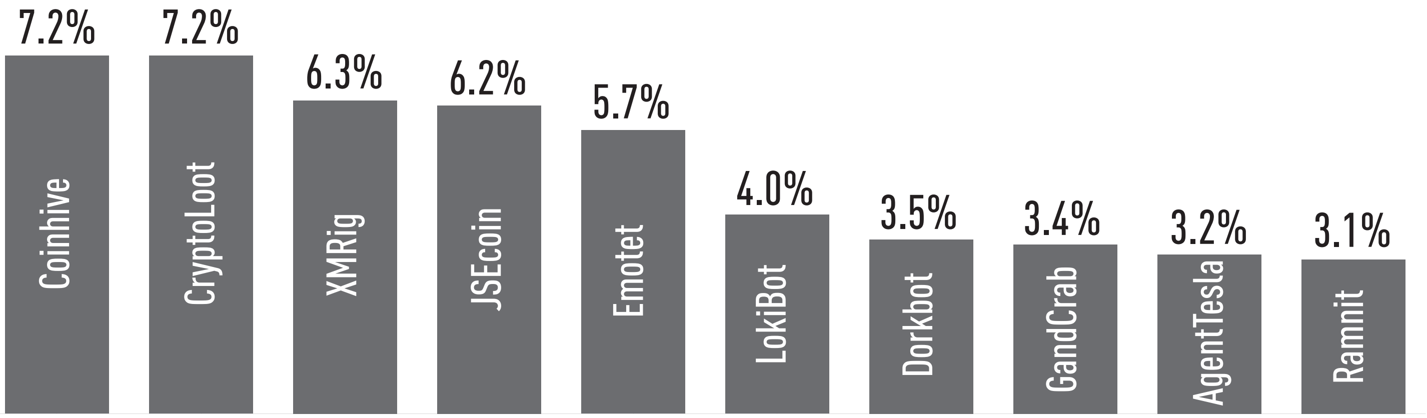


Figure 1: Most Prevalent Malware Globally: Percentage of corporate networks impacted by each malware family

Americas

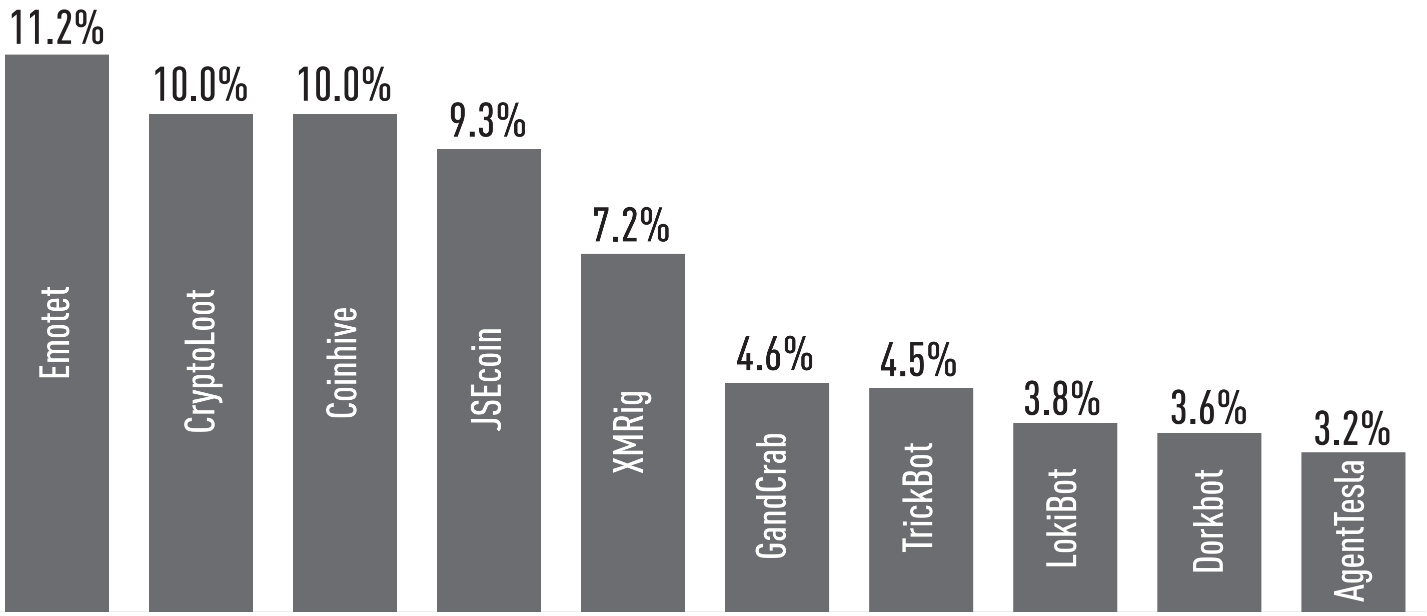


Figure 2: Most Prevalent Malware in the Americas

Europe, Middle East and Africa (EMEA)

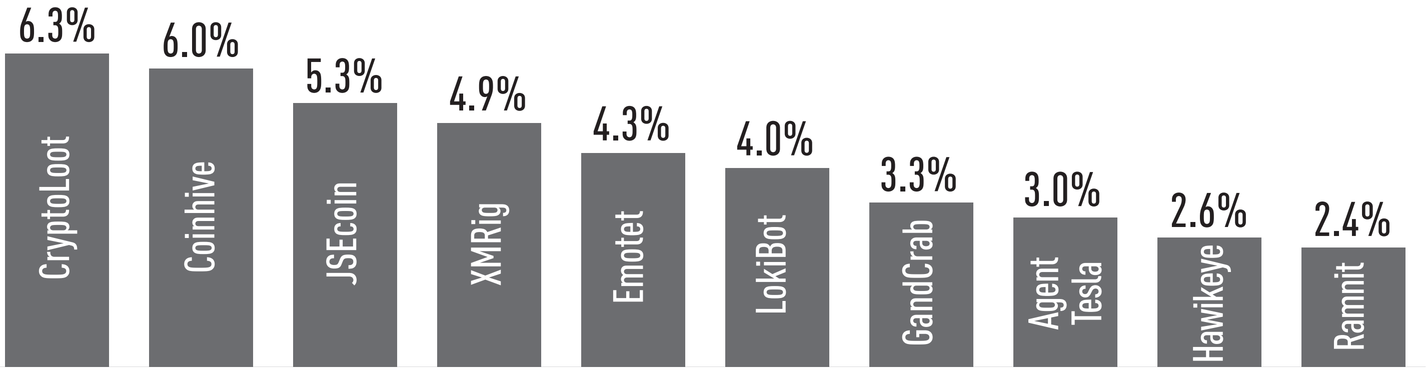


Figure 3: Most Prevalent Malware in the EMEA

Asia Pacific (APAC)

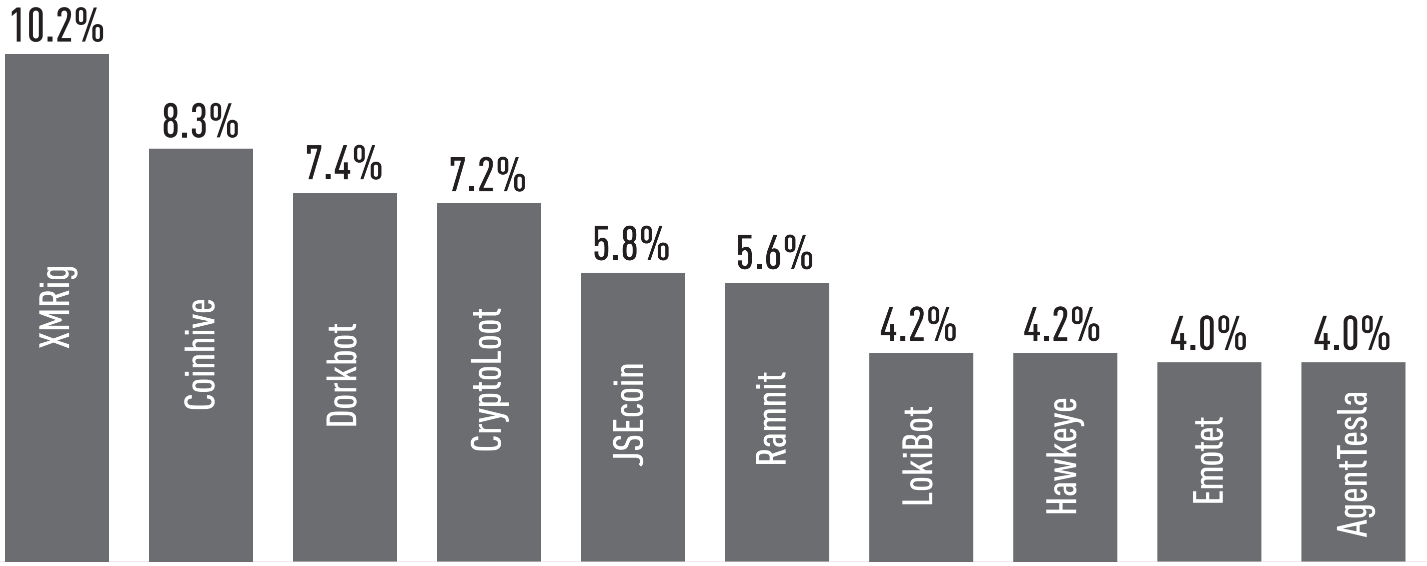


Figure 4: Most Prevalent Malware in the APAC

Global Analysis of Top Malware

In 2019 cryptominers continue to dominate the malware rankings, keeping their place at the top of the global and regional ranks. Our charts show cryptomining malware are undoubtedly still a preferred tool in the arsenal of malicious actors, despite the Coinhive shutdown that occurred this March. We do, however, see a decrease in the impact of the Cryptomining squad, with only 26% of organizations affected by them in comparison to 42% of the organizations in 2018.

GandCrab, the infamous Ransomware-as-a-Service, has entered our top global charts after being highly active in the first half of 2019. Exploiting a recently patched critical Oracle WebLogic Server vulnerability, as well as aiming at multiple targets including Managed Service Providers (MSPs), Manufacturing Firm and Windows servers running MySQL databases, are only few of this year's GandCrab victims. However, despite the meteoric success, in May the ransomware's authors announced the service's shutdown and prompted their affiliates to terminate their ongoing operations and stop distributing GandCrab.

TOP CRYPTOMINING MALWARE

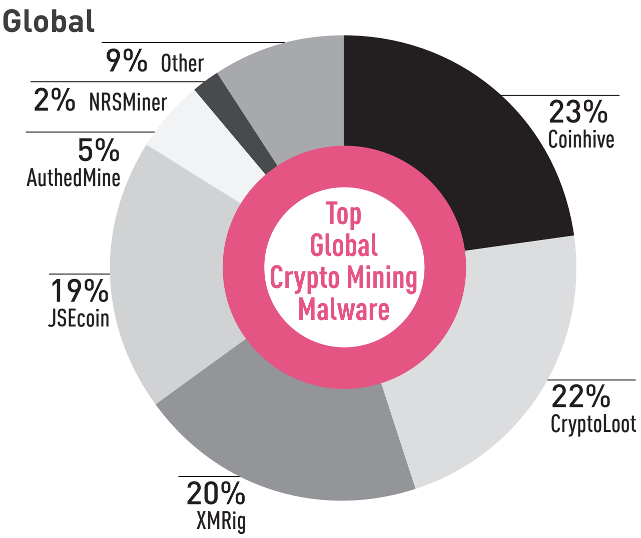


Figure 5: Top Cryptomining Malware Globally

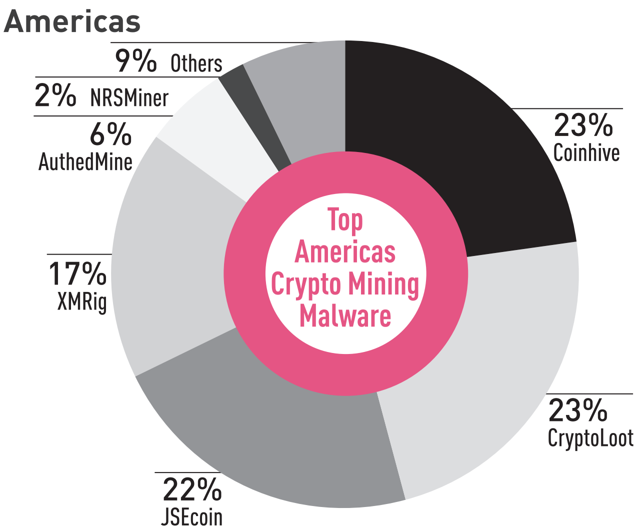


Figure 6: Top Cryptomining Malware in the Americas

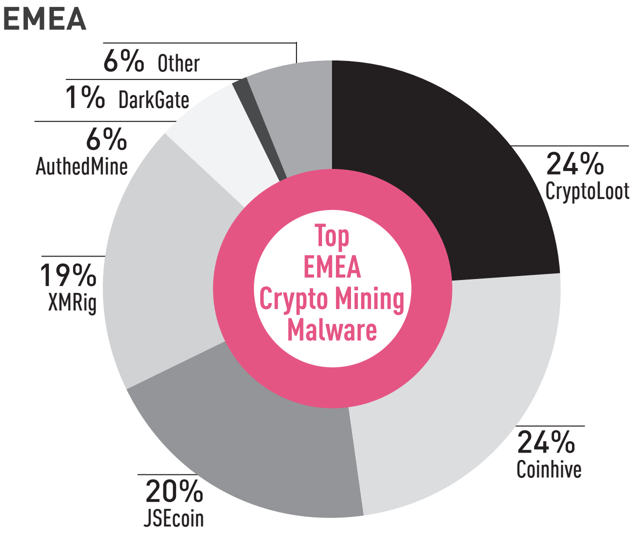


Figure 7: Top Cryptomining Malware in EMEA

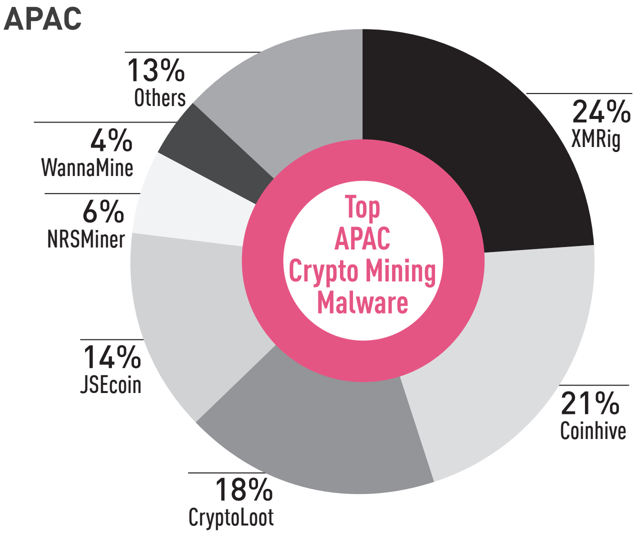


Figure 81: Top Cryptomining Malware in APAC

Cryptomining Malware Global Analysis

Ranking first in EMEA and second or third in all other regions, **CryptoLoot**, the CPU/GPU-based Javascript web miner for Monero, is getting ready to take over CoinHive's position at the top. Furthermore, for the first time **DarkGate** has entered our top list. Capable of performing multiple additional activities besides cryptomining, such as credential stealing, file encryption and remote-access takeovers, DarkGate represents a generation of malware which integrates mining capabilities into their existing tool set.

TOP BANKING MALWARE

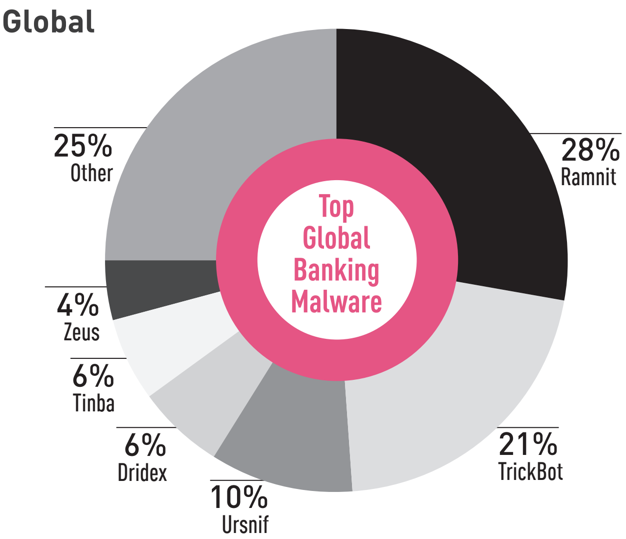


Figure 9: Most Prevalent Banking Malware Globally

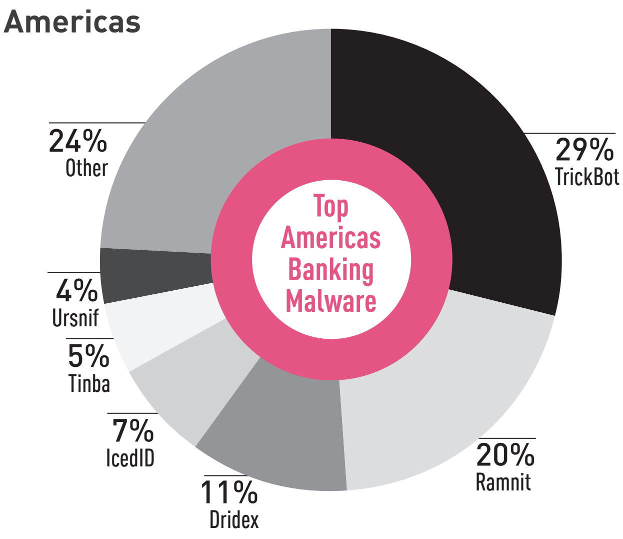


Figure 10: Most Prevalent Banking Malware in the Americas

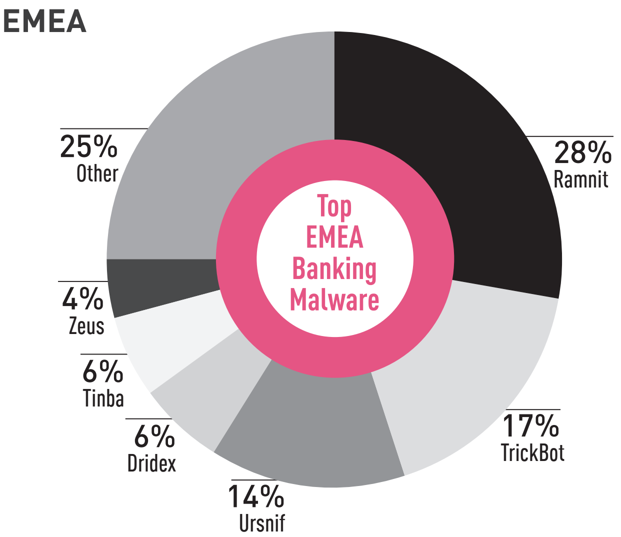


Figure 11: Most Prevalent Banking Malware in EMEA

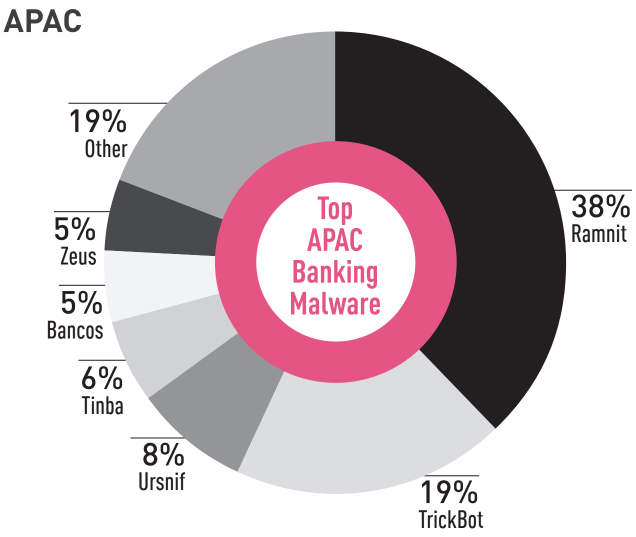


Figure 12: Most Prevalent Banking Malware in APAC

Banking Malware Global Analysis

Ramnit, the prolific Banking Trojan, has kept its place as the most prevalent banker of 2019 so far. Over the years, Ramnit has expanded its target array to include online advertising, web services, social networking sites and e-commerce sites. This year Ramnit has returned to its roots and was spotted largely targeting financial services websites to coincide with tax return activity, primarily in Italy.

Ursnif, which is also known as "Gozi ISFB," has climbed its way to the top of the Banking Trojans list. The leak of its source code in underground forums has made Ursnif one of the most popular Banking Trojans, which evolves and integrates new features and capabilities. This year, Ursnif variants have constantly hit the headlines; distributers adopted new techniques to avoid detection, targeted entities in Japan and Italy, massively distributed it alongside GandCrab ransomware and added new modules of stealing not only financial information but also email user accounts, content of inboxes and cryptocurrencies wallets, as well as user credentials for local webmail, cloud storage, and e-commerce sites.

TOP BOTNET MALWARE

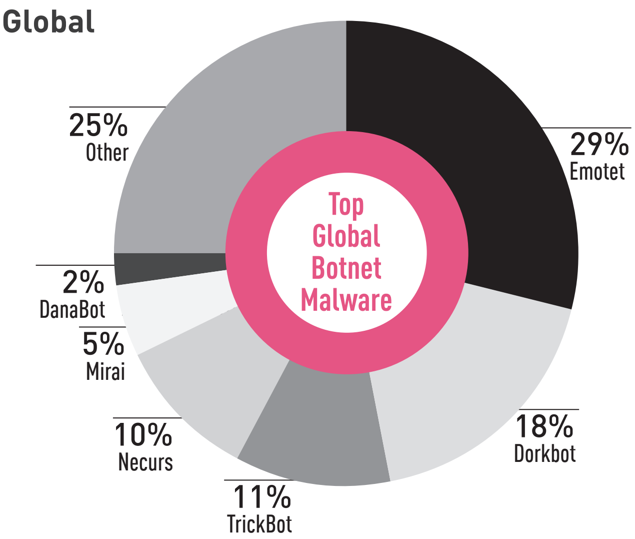


Figure 13: Most Prevalent Botnet Malware Globally

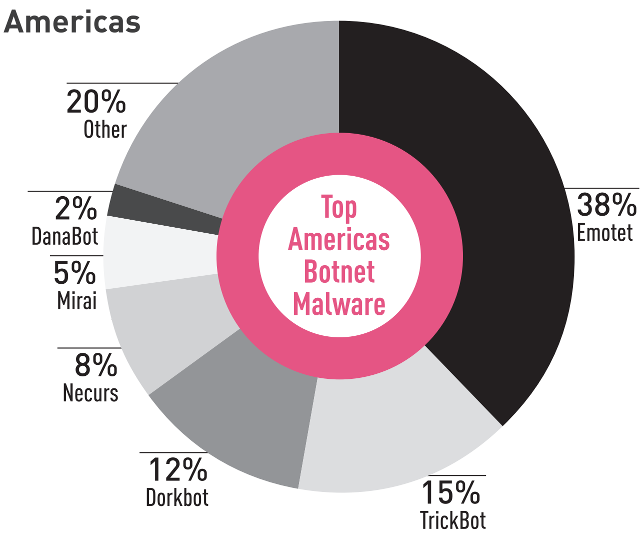


Figure 14: Most Prevalent Botnet Malware in the Americas

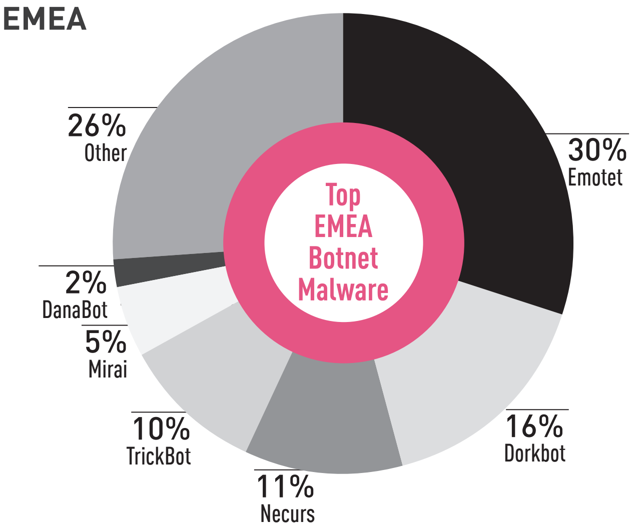


Figure 15: Most Prevalent Botnet Malware in EMEA

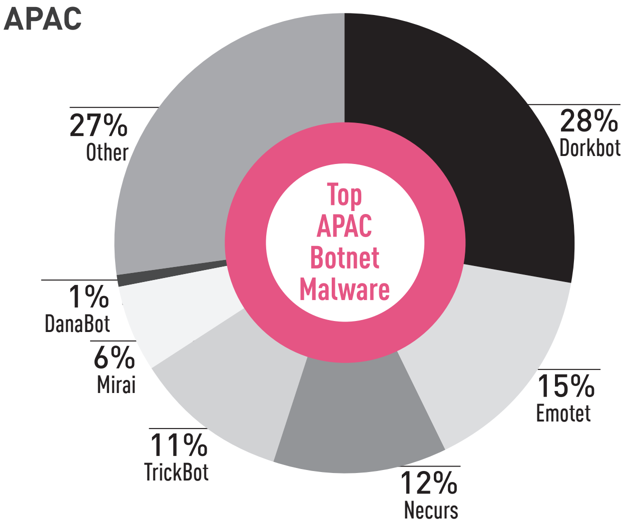


Figure 16: Most Prevalent Botnet Malware in APAC

Botnet Malware Global Analysis

Emotet, once employed as a Banking Trojan, is nowadays an advanced, self-propagating and modular Trojan which also distributes spam emails and malware strains. Emotet leads the top Global, Americas and EMEA ranks as one of the most prevalent Botnets of the first half of 2019. This year, it seems Emotet became attackers' favorite, massively delivering multiple other variants of malware as well as extending its capabilities with multiple novel evasion techniques. In mid-June Emotet stopped propagating itself, and as of this writing hasn't generated new infections. Another prominent Botnet dominating the charts is **TrickBot**, which has made fast-paced evolution from Banking Trojan to a multi-purpose Trojan with a high level of flexibility and customization. This year TrickBot is taking a leading part in the Ryuk distribution as well as in devious campaigns leveraging Tax Day in the USA to steal bank account details and confidential tax documents for fraudulent use.

TOP MOBILE MALWARE

Global

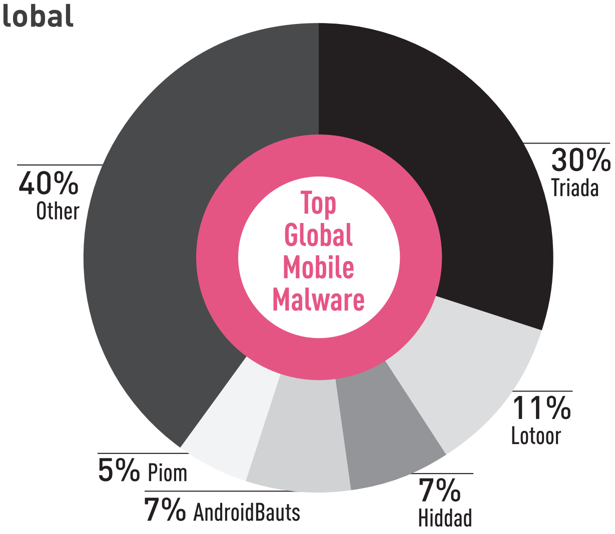


Figure 17: Top Mobile Malware Globally

Americas

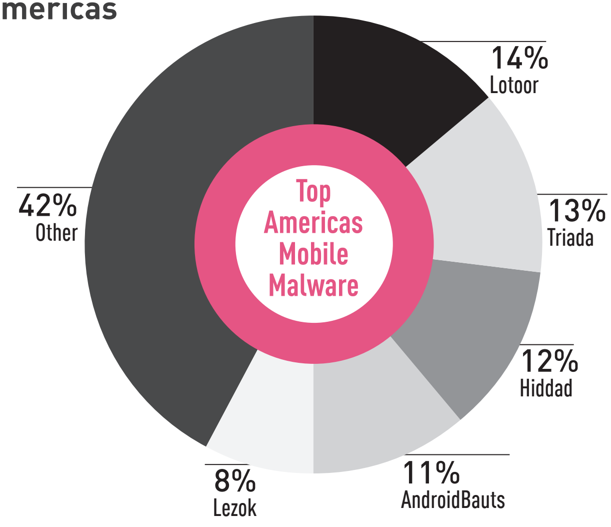


Figure 18: Top Mobile Malware in the Americas

EMEA

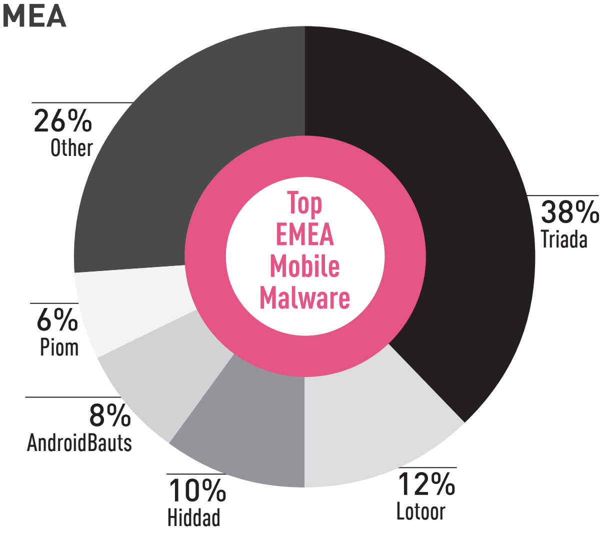


Figure 19: Top Mobile Malware in EMEA

APAC

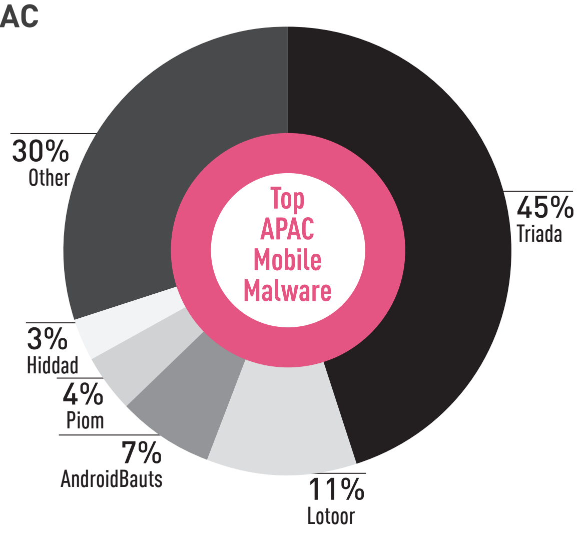


Figure 20: Top Mobile Malware in APAC

Mobile Malware Global Analysis

Triada, the powerful Android modular Trojan, is once again starring in our charts, ranked first in the Global, EMEA and APAC regions. Considered one of the most advanced mobile malware, last year Triada was found pre-installed on Android smartphones, infecting hundreds of thousands of victims. In June, Google published a report stressing that Triada was injected into the system image of mobile devices through a third party during the production process. Another leading mobile malware throughout the first half of 2019 is **Lotoor**, a malware that is capable of exploiting numerous vulnerabilities on the Android operating system, allowing it to gain root privileges on compromised mobile devices.

MAJOR CYBER BREACHES (H1 2019)

In the first half of 2019 cyber breaches continued to be one of the major threats to organizations in all sectors and all regions, putting at risk sensitive information of billions of people. What characterizes 2019 is not the number of reported breaches but rather their magnitude. Below is a recap of the major attacks in each region.

Americas

- **January:** Over 770 million email addresses and 21 million unique passwords were exposed in a popular hacking forum after being hosted in the cloud service MEGA, and became the single largest collection of breached personal credentials in history, named "Collection #1". Later this year, Collection #1 was discovered as a minor slice of a bigger one terabyte data leak, split into seven parts and distributed through data-trading.
- **February:** 620 million account details were stolen from 16 hacked websites and offered for sale on the popular Dark Web marketplace, Dream Market. Later on, the same threat actor under the alias "gnosticplayers", published another trove of 127 million accounts for sale from eight more hacked websites.
- **March:** The world's largest email validation company, Verifications.io, fell victim to a major data breach due to an unprotected MongoDB database, exposing online data from over 800 million emails. The leaked emails contained sensitive information including personally identifiable information (PII).
- **April:** More than half a billion records of Facebook's users were found exposed on unprotected Amazon cloud servers. The exposed data sets were collected and not securely stored online by third-party Facebook app developers.
- **April:** Eight unsecured databases containing scraped data and email addresses of nearly 60 million LinkedIn users were found online. A LinkedIn investigation yielded that the exposed databases belonged to a third-party company that aggregated data from multiple sources, including LinkedIn.
- **May:** A Russian hacking group offered for sale access to networks of anti-virus vendors and the source code of their software. The group, called Fxmsp, claimed to breach the networks of McAfee, Symantec and Trend Micro, and steal 30 terabytes of data that they are offering for sale.
- **June:** American Medical Collection Agency (AMCA) suffered a major data breach exposing personal and payment information of almost 20 million patients after attackers infiltrated their web payment portal. The information included names, date of birth, address, phone, date of service, provider, balance information, and credit card or bank account. AMCA has filed for bankruptcy as the breach has led to both financial and legal consequences for the organization.

Europe, the Middle East and Africa (EMEA)

- **January:** Highly sensitive personal data of over 100 German politicians, celebrities and journalists, including German Chancellor Angela Merkel, was leaked. The leaked data appears to have been collected from their personal smartphones, and included mobile phone numbers, addresses, private conversations with families, holiday pictures, bills, and communications between politicians.

- **January:** Airbus, the world's second-largest manufacturers of commercial airplanes, was subject to a data breach exposing personal data of some of its employees as unauthorized attackers breached its "Commercial Aircraft business" information system.

- **February:** The South African state-owned energy supplier "Eskom" experienced two security breaches. An unsecured database containing customer information was exposed to the internet and a corporate computer was infected with the AZORult information-stealing Trojan after an employee downloaded a cracked Sims 4 game.

- **April:** The Georgia Institute of Technology suffered a data breach that exposed the personal information of 1.3 million current and former faculty members, students, staff and student applicants. By exploiting a vulnerability in its web app, an unauthorized entity gained access to the university's central database.

Asia-Pacific (APAC)

- **January:** A massive online database was revealed to contain sensitive and personal records of more than 202 million Chinese citizens. The data is believed to have been collected from job seekers' resumes from various Chinese websites using a scraping tool called "data-import".

- **February:** Indian state-owned LPG Gas Company had online personal and sensitive data belonging to 7 million customers and distributors leaked following vulnerabilities in their iOS applications. The compromised information included names, addresses and personal identity numbers (Aadhaar numbers), as well as distributors' bank details such as bank name, account number, IFSC code, and more.

- **April:** Personal data of 100 million users of the Indian search service JustDial was exposed after an unprotected database was found online. The leaked data was collected in real-time from every customer who accessed the service via its website, mobile app, or even by calling, and included usernames, email addresses, mobile numbers, addresses, occupation and even photos.

- **April:** A misconfigured Elasticsearch DB on the Tommy Hilfiger Japan website led to the exposure of hundreds of thousands of customers' personal information; full names, addresses, phone numbers, email addresses, date of birth, and transaction information were accessible in unencrypted plaintext format.

- **June:** FMC Consulting, a Chinese headhunting company, was responsible for a major data leak of millions of records due to a misconfigured and publicly accessible ElasticSearch. The leaked information included resumes and company records, as well as customers' and employees' PII data and internal emails.

HIGH PROFILE GLOBAL VULNERABILITIES

The following list of top attacks is based on data collected by the Check Point Intrusion Prevention System (IPS) sensor net and details some of the most popular and interesting attack techniques and exploits observed by Check Point researchers in the first half of 2019.

- **BlueKeep Microsoft RDP (Remote Desktop Protocol) Vulnerability (CVE-2019-0708)** – Exploiting Remote Desktop Protocol (RDP) is already an established, popular attack vector which could allow cyber criminals to access targeted machines and even install a backdoor for further malicious activities. The recently patched critical, wormable, Windows RDP vulnerability, dubbed **BlueKeep**, took the cyber security community by storm as it is capable of spreading automatically on unprotected networks, potentially leading to a Wannacry-scale attack. Shortly after Microsoft released its patch, actors started scanning the internet for vulnerable devices revealing that over 1 million machines are vulnerable to it. However, there are as yet no known cases of the flaw being exploited by threat actors as part of an attack in the wild.

- **Oracle WebLogic Server Vulnerabilities (CVE-2017-10271, CVE-2019-2725)** – The various critical remote code execution vulnerabilities that reside in Oracle WebLogic Servers allow an unauthorized attacker to remotely execute arbitrary code and affect numerous applications and web enterprise portals using the servers. This year alone cyber criminals have exploited Oracle WebLogic Server vulnerabilities, including a newly discovered one patched this April, to deliver Sodinokibi ransomware, Satan ransomware and install Monero Cryptomining malware.

- **DoS Vulnerabilities in Linux and FreeBSD – TCP SACK Panic (CVE-2019-11477, CVE-2019-11478, CVE-2019-5599, CVE-2019-11479)** – A critical set of vulnerabilities was unveiled in 2019 that affected FreeBSD and Linux operating systems. The three flaws were found in the Linux kernel's handling of TCP networking. Successful exploitation of one of the vulnerabilities is capable of remotely crashing servers and disrupting communications. The most severe vulnerability could allow a remote attacker to trigger a kernel panic in systems running the affected software and, as a result, impact the system's availability.

Interestingly, according to Check Point global attack sensors, throughout the first half of 2019, 90% of the attacks observed leveraged vulnerabilities registered in 2017 and earlier and over 20% of attacks used vulnerabilities that are at least seven years old.

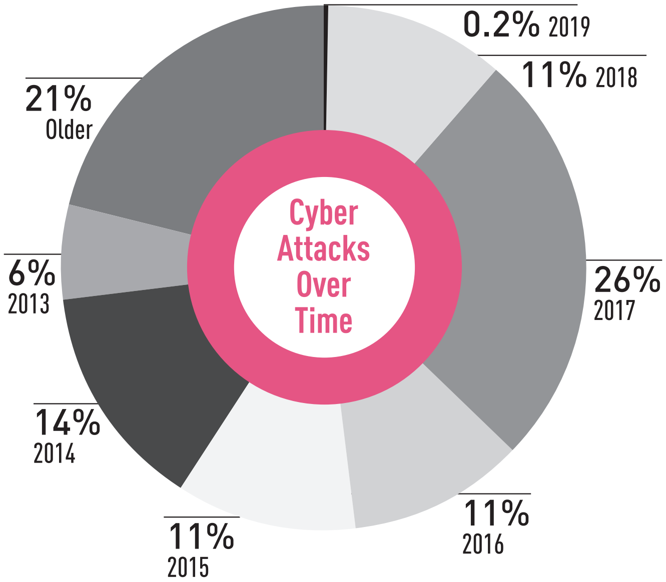


Figure 20: Percentage of attacks leveraging vulnerabilities found since 2012 and earlier

APPENDIX – MALWARE FAMILY DESCRIPTIONS

- **AdvisorsBot –** AdvisorsBot is a sophisticated downloader first spotted in the wild in May 2018. Once AdvisorsBot has been downloaded and executed, the malware uses HTTPS to communicate with the C&C server. AdvisorsBot has significant anti-analysis features including using "junk code" to slow down reverse engineering and Windows API function hashing to make it harder to identify the malware's functionality.
- **AgentTesla –** AgentTesla is an advanced RAT which functions as a keylogger and password stealer and has been active since 2014. AgentTesla can monitor and collect the victim's keyboard input, system clipboard, and can record screenshots and exfiltrate credentials belonging to a variety of software installed on a victim's machine (including Google Chrome, Mozilla Firefox and Microsoft Outlook email client). AgentTesla is openly sold as a legitimate RAT with customers paying between $15-$69 for user licenses.
- **AmmyyRat –** FlawedAmmyy is a remote access Trojan (RAT) that has been developed from the leaked source code of the remote administration software called Ammyy Admin. FlawedAmmyy has been used in both highly targeted email attacks as well as massive spam campaigns and implements common backdoor features, allowing the attackers to manage files, capture the screen, remote control the machine, establish RDP SessionsService and much more.
- **AndroidBauts –** AndroidBauts is an adware targeting Android users that exfiltrates IMEI, IMSI, GPS Location and other device information and allows the installation of third party apps and shortcuts on mobile devices.
- **Anubis –** Anubis is a banking Trojan malware designed for Android mobile phones. Since its initial detection, it has gained additional functions including Remote Access Trojan (RAT) functionality, keylogger, audio recording capabilities and various ransomware features. It has been detected on hundreds of different applications on the Google Store.
- **Asacub –** Asacub Mobile Banker was first introduced in 2015 as a spyware. Nowadays Asacub functions as a banker aiming at the victim's bank account information, and also capable of siphoned incoming SMS messages, browser history, and contacts, as well as execute commands, intercept messages, turn off the phone or its screen. Asacub spread via phishing SMS containing a link which leads to downloading the APK file of the Trojan to the infected device.
- **AuthedMine –** AuthedMine is a version of the infamous JavaScript miner Coinhive. Similarly to Coinhive, AuthedMine is a web-based cryptominer 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.
- **AZORult –** AZORult is a Trojan that gathers and exfiltrates data from the infected system. Once the malware is installed on a system (typically delivered by an exploit kit such as RIG), it can send saved passwords, local files, crypto-wallets, and computer profile information to a remote C&C server. The Gazorp builder, available on the Dark Web, allows anyone to host an AZORult C&C server with moderately low effort.
- **Bancos –** Bancos 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.
- **Coinhive –** 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.
- **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.
- **DanaBot –** DanaBot is a Trickler that targets the Windows platform. The malware sends out information to its control server, downloads and decrypts files to execute on the infected computer. It is reported the downloaded module can download other malicious files on the system. Moreover, the malware creates a shortcut in the user's startup folder to achieve persistence on the infected system.
- **DarkGate –** DarkGate is a multifunction malware active since December 2017 combining ransomware, credential stealing, RAT and cryptomining abilities. Targeting mostly windows OS, DarkGate employs a variety of evasion techniques.

- **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.
- **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.
- **Emotet –** Emotet is an advanced, self-propagating and modular Trojan. Emotet was once employed as a banking Trojan, and recently was used as a distributer to other malware or malicious campaigns. It uses multiple methods for maintaining persistence and evasion techniques to avoid detection. In addition, it can also be spread through phishing spam emails containing malicious attachments or links.
- **Gandcrab –** GandCrab is a RaaS malware (Ransomware-as-a-Service). First discovered in January 2018, it operated an "affiliates" program, with those joining paying 30%-40% of the ransom revenue to GandCrab and in return getting a full-featured web panel and technical support. Estimates are that it affected over 1.5 million Windows users before retiring and halting its activities in mid-2019. Decryption tools exist for all GandCrab versions.
- **Guerilla –** Guerrilla is an Android Trojan found embedded in multiple legitimate apps and is capable of downloading additional malicious payloads. Guerrilla generates fraudulent ad revenue for the app developers.
- **Gustuff –** Gustuff is an Android banking Trojan introduced in 2019, and capable of targeting customers of over 100 leading international banks, users of cryptocurrency services, and popular ecommerce websites and marketplaces. In addition, Gustuff can also phish credentials for various other Android payment and messaging apps, such as PayPal, Western Union, eBay, Walmart, Skype and others. Gustuff employs various evasion techniques including using the Android Accessibility Service mechanism to bypass security measures used by banks to protect against older generations of mobile Trojans.
- **Hawkeye –** Hawkeye is an info stealer malware, designed primarily to steal users' credentials from infected Windows platforms and deliver them to a C&C server. In past years, Hawkeye has gained the ability to take screenshots, spread via USB and more in addition to its original functions of email and web browser password stealing and keylogging. Hawkeye is often sold as a MaaS (Malware-as-a-Service).
- **Hiddad –** Android malware that 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.
- **IcedID–** IcedID is a banking Trojan which first emerged in September 2017, and usually uses other well-known banking Trojans to empower its spread potential, including Emotet, Ursnif and TrickBot. IcedID steals user financial data via both redirection attacks (installs local proxy to redirect users to fake-clone sites) and web injection attacks (injects browser process to present fake content overlaid on top of the original page).
- **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.
- **Lezok –** Lezok is an Android Trojan capable of downloading additional malware to victim's computer without user's consent, as well as generating pop-up advertisements when the user is surfing the Internet.
- **LockerGoga –** LockerGoga ransomware was first seen in the wild towards the end of January 2018, while targeting heavy industry companies. It appears that the threat actors behind the attack invest time and efforts in choosing the victims and are working to launch the attack in perfect timing and against critical assets. The attack usually involves encryption of Active Directory server and endpoints, in order to leave no alternative other than paying the ransom. Using a combination of AES-256 and RSA makes the encryption very solid. However, a poor code design makes the encryption process very slow.

- **LokiBot –** LokiBot is an info stealer with versions for both Windows and Android OS. It harvests credentials from a variety of applications, web browsers, email clients, IT administration tools such as PuTTY and more. LokiBot has been sold on hacking forums and believed to have had its source code leaked, allowing for a range of variants to appear. It was first identified in February 2016. Since late 2017 some Android versions of LokiBot include ransomware functionality in addition to their infostealing capabilities.
- **Lotoor –** Lotoor is a hack tool that exploits vulnerabilities on Android operating systems in order to gain root privileges on compromised mobile devices.
- **MageCart –** MageCart is a type of attack in which malicious JavaScript code is injected into e-commerce websites and third-party suppliers of such systems in order to steal payment details.
- **Mirai –** Mirai is a famous Internet-of-Things (IoT) malware that tracks vulnerable IoT devices, such as web cameras, modems and routers, and turns them into bots. The botnet is used by its operators to conduct massive Distributed Denial of Service (DDoS). Mirai botnet first surfaced on September 2016 and quickly made headlines due to some large-scale attacks. Among them were a massive DDoS attack used to knock the entire country of Liberia offline, and a DDoS attack against the Internet infrastructure firm Dyn, which provides a significant portion of the United States internet's backbone.
- **Necurs –** Necurs is a 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.
- **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.
- **Piom –** Piom is an Adware which monitors the user's browsing behaviour and delivers unwanted advertisements based on the users web activities.
- **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 worm operators the ability to steal account credentials for all services used by the victim, including bank accounts, corporate, and social networks accounts.
- **Retadup –** Retadup is a Trojan that targets Windows platform. It is reported that this malware is used for targeted attacks and some variants of the malware comes with Keylogger, screen capture and password stealing capabilities. The malware is used to mine cryptocurrency on the infected system. It communicates with its remote control server and accept commands to execute on the infected system.
- **Ryuk –** A ransomware used in targeted and well-planned attacks against several organizations worldwide. The ransomware's technical capabilities are relatively low, and include a basic dropper and a straightforward encryption scheme. Nevertheless, the ransomware was able to cause severe damage to the attacked organizations, and led them to pay extremely high ransom payments of up to 320,000 USD in Bitcoin. Unlike common ransomware, systematically distributed via massive spam campaigns and exploit kits, Ryuk is used exclusively for tailored attacks. Its encryption scheme is intentionally built for small-scale operations, such that only crucial assets and resources are infected in each targeted network with its infection and distribution carried out manually by the attackers. The malware encrypts files stored on PCs, storage servers and data centers.
- **Satan –** Satan is a Ransomware-as-a-Service (RaaS) which first emerged in January 2017. Its developers offer a user-friendly web portal with customization options, allowing anyone who buys it to create custom versions of Satan ransomware and distribute it to victims. New versions of Satan were observed using the EternalBlue exploit to spread across compromised environments, as well as performing lateral movement using other exploits.
- **Sodinokibi –** Sodinokibi is a Ransomware-as-a-Service which operates an "affiliates" program which was first spotted in the wild in 2019. Sodinokibi encrypts data in the user's directory and deletes shadow copy backups in order to make data recovery more difficult. Moreover, Sodinokibi affiliates use various tactics to spread it through spam and server exploits, as well as hacking into managed service providers (MSP) backends, and through malvertising campaigns redirected to the RIG exploit kit.

- **TheTruthSpy –** An Android spyware that first emerged in May 2017. TheTruthSpy is capable of monitoring WhatsApp messages, Facebook chats, and internet browsing history.
- **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.
- **Ursnif –** Ursnif is a Trojan that targets the Windows platform. It is usually spread through exploit kits – Angler and RIG, each at its time. It has the capability to steal information related to Verifone Point-of-Sale (POS) payment software. It contacts a remote server to upload collected information and receive instructions. Moreover, it downloads files on the infected system and executes them.
- **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.
- **WannaMine –** WannaMine is a sophisticated Monero cryptomining worm that spreads by exploiting the EternalBlue exploit. WannaMine implements a spreading mechanism and persistence techniques by leveraging Windows Management Instrumentation (WMI) permanent event subscriptions.
- **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.

Check Point
SOFTWARE TECHNOLOGIES LTD

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