Table of Contents

Executive Summary

In the past six months, the way we live and work has changed beyond recognition. To put it simply – life on earth has gone online. The change was not gradual but happened seemingly overnight. Almost everything is different now, from the way we conduct relationships, work or even do our grocery shopping. Changes of the same order of magnitude can be found in the cyber arena.

The new normal has created challenges alongside opportunities. Infrastructure changes made by companies to allow remote access have also required threat actors to adapt to a hybrid world that integrates cloud technologies. In addition, the rapid spread of the corona virus and global research efforts to find a vaccine have created new phishing options and made medical research institutions a sought-after target for criminal and state actors.

We will address these effects and more aspects of the threat landscape, while providing examples and statistics of real world events.

Here are some of the cyber attacks trends we discuss:

Double Extortion

Ransomware actors have adopted a new strategy; in addition to making the victim's files inaccessible, they now exfiltrate large quantities of data prior to its encryption in the final stage of the attack. Victims who refuse payment demands find their most sensitive data publicly displayed on dedicated websites.

Cyber Warfare

Nation-state cyber activity has seen a surge in intensity and escalation in severity. In times when traditional tactics to gather intelligence and knowledge are no longer feasible due to social distancing, the use of offensive cyber weapons to support national missions appears to have expanded. The goal may be better understanding of the Corona virus or securing intelligence operations, and countries and industries are the targets.

Mobile

Threat actors have been seeking new infection vectors in the mobile world, changing and improving their techniques to avoid detection in places such as the official application stores. In one innovative attack, threat actors used a large international corporation's Mobile Device Management (MDM) system to distribute malware to more than 75% of its managed mobile devices.

Cloud

Industries were required to make rapid infrastructure adjustments to secure their production when working remotely. In many cases, this would not have been possible without cloud technologies. However, it also exposed more misconfigured or simply unprotected assets to the internet. In addition, for the first time, alarming vulnerabilities were revealed in Microsoft Azure infrastructure that could enable invaders to escape VM infrastructure and compromise other customers.

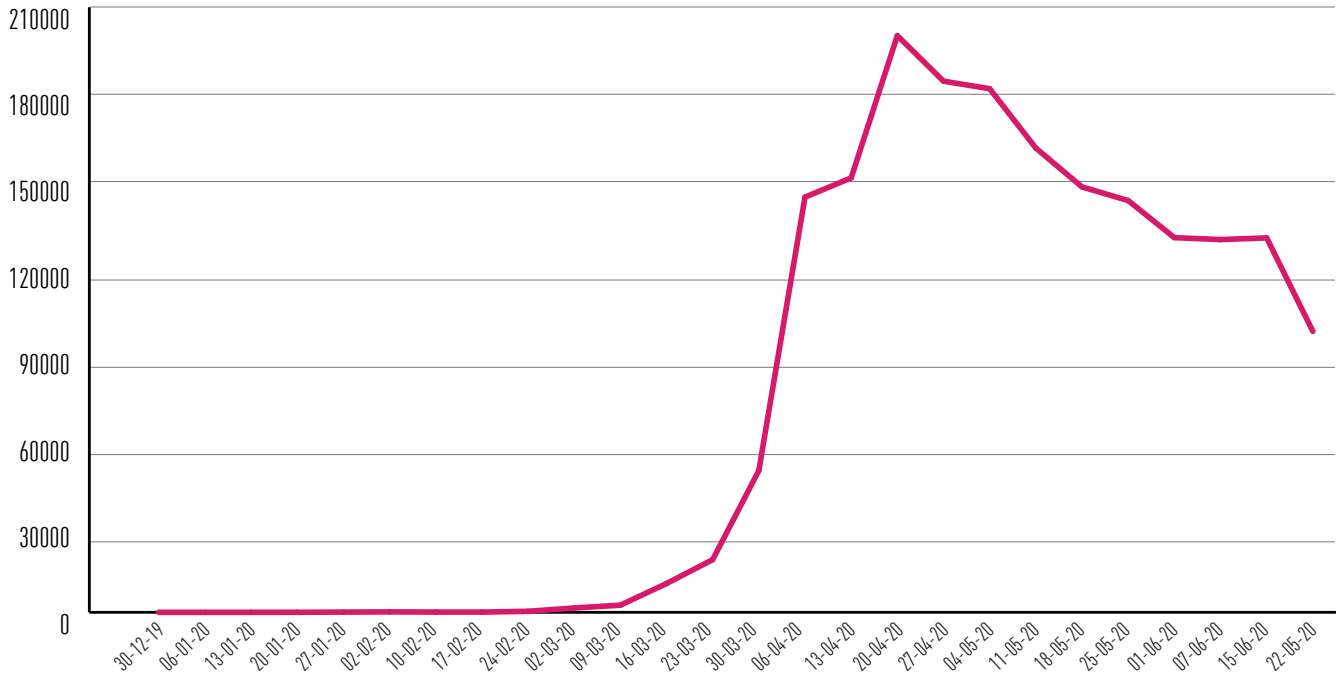
The World Under COVID-19

The COVID-19 pandemic has had a dramatic effect on virtually every aspect of life and was without doubt the most influential event in H1 2020. There were substantial repercussions in the cyber arena as well. A variety of actors with diverse motivations – criminal, political or espionage – used concerns about COVID-19 and related themes to target a whole new set of victims.

The first impact of the pandemic was the proliferation of malware attacks that used social engineering techniques with COVID-19 thematic lures for the delivery stage. As early as January, we reported Emotet using weaponized documents with Coronavirus-related content targeting Japanese users.

Thousands of Coronavirus-related domain names were registered, many of which would later be used for various scams. Some were used to sell fake COVID-19 vaccinations or medication, others for various phishing campaigns, and for distributing malicious mobile applications. Similar to holidays and sales events, scammers offered merchandise in "special coronavirus discounts". Hackers even offered Malware-as-a-Service at special prices.

Weekly Coronavirus Related Cyber Attacks



The graph represents all coronavirus-related attacks, detected by Check Point's Threat Prevention technologies across networks, endpoints and mobile devices

Not only financially motivated groups took advantage of the situation; China-based APT groups composed Corona-related content and used it in malicious RTF documents for a campaign directed at Mongolian public entities. Some estimate that the decline in traditional espionage activities, hampered by travel restrictions and social distancing, has been compensated for by an increased effort in online operations. The European External Action

Service (EEAS) reported increased intentional coordinated disinformation activities, often carried out by state or state-sponsored actors promoting false health information along with continued efforts at deflecting blame for the outbreak of the pandemic.

As the pandemic evolved and social distancing policies were enacted, a substantial portion of businesses adjusted to remote work policies, thus exposing private and public entities to additional attack venues. Video communication platforms became a target as hackers attempted to infiltrate video sessions, and other threat actors registered fake domains and distributed malicious apps impersonating Zoom, Microsoft Teams and other web-conferencing sites. As use of remote access technologies such as RDP and VPN increased, a sharp rise in RDP brute force attacks was also recorded.

The health sector is under extreme pressure to treat patients and advance efforts to produce vaccines and develop medication that are effective against the virus. Despite promises to refrain from attacking health care organizations, ransomware operators like Maze continued ransom attacks, realizing that their victims would be in a poor position to negotiate. Other campaigns impersonated pharmaceutical organizations and attempted to spread ransomware in Italy, specifically targeting the health sector. The WHO (World Health Organization) reported a dramatic increase in the number of cyber-attacks directed at its staff and systems.

Another type of attack took advantage of the worldwide economic stress due to lockdowns and business closures, with large scale fraud against companies and states. Stolen PII (personally identifiable information) was used to submit fraudulent unemployment claims. Corporations operating under emergency transaction authorization procedures fell victim to BEC (Business Email Compromise) attacks. Europol reported that a French pharmaceutical company transferred $7.25 million to a fake supplier for the purchase of hand sanitizer and protective masks.

The coronavirus outbreak amplified several cyber security trends which might outlive the pandemic. Many countries enforced emergency regulations and activated special tracking systems, some of them mandatory, developed to fight the outbreak. India's "Aarogya Setu" contact-tracing application, as an example, had more than 100 million downloads, and its popularity raises issues of privacy and security. Any such system must maintain a delicate balance between privacy and security; poor implementation of security standards may put users' data at risk. The city of Hangzhou in China already announced they intend to continue using their application on a permanent basis. Researchers warn that measures brought in to protect and monitor citizens in exceptional circumstances could outlast the current crisis.

It is unclear when the COVID-19 pandemic will end. Some say that its effects are permanent, and we must adjust to the 'new normal' conditions of a post-COVID-19 World. This new world will require corresponding new cyber protections.

Double Extortion

The latest trend in ransomware attacks combines encryption of the victim's files with threats to publish stolen confidential information unless ransom demands are met. This trend is now practiced by most major ransomware cyber actors, and potentially turns every ransomware attack into a data breach. Payment of the ransom money no longer guarantees the end of the attack, as the victims can never be certain that the stolen information was actually deleted.

Since their emergence in 1989, ransomware attacks have gone from mass deployment of malware through email to precision targeting of carefully chosen victims. Initially, attacks relied on user participation (like clicking a link or opening an attachment) to infect a victim's machine. However, later attacks were performed with "drive-by" methods using wormlike distribution methods or existing botnets to deliver the malware as payloads.

The victims suffer a double blow: the attackers prevent access to their files and data by encrypting it, but prior to its encryption, some of the information is exfiltrated. Unless the ransom is paid, sensitive data can be made publicly available, while at the same time critical company systems remain crippled, disrupting regular operations.

The first published double extortion case occurred in November 2019, when Allied Universal, a large American security staffing company, was hit with Maze ransomware and refused to pay a ransom of 300 Bitcoins. The attackers responded by publishing sensitive information extracted from Allied Universal's systems, including contracts, medical records, encryption certificates and more. TA2101, the group behind the Maze ransomware, has since created a dedicated web page that lists the identities of non-cooperative victims and regularly publishes samples of stolen data. They have published the details of dozens of companies, law firms, medical service providers and insurance companies.

Other cybercriminal groups, including Sodinokibi (aka REvil), Clop, Nemty, and DopplelPaymer, followed suit. Information published on their sites was soon found offered for sale by ransomware groups or by other criminals who collected the data from the dump sites.

Traditional ransomware attacks, as vicious as they are, give victims the option to recover everything from backups or surrender to criminal demands and pay ransom in hopes of receiving decryption keys.

Data breaches, on the other hand, expose their victims to loss of proprietary information as well as hinder their ability to protect clients' and employees' personal information. Regulatory laws like the European Union GDPR and security breach notification laws in the US mandate that victims of such attacks must disclose the details of the attack to both designated authorities and to the corporations and individuals to whom the information belongs. This increases the damage by adding additional costs needed for the protection of employees and customers from fraud and identity theft, as well as possible exposure to lawsuits.

Cyber Warfare During a Pandemic

The COVID-19 pandemic dramatically reshaped the inter-state cyber arena. It challenged intelligence units, redefined goals and created new opportunities for threat actors. In times when traditional intelligence activity is limited due to sustained lockdowns, social distancing and international travel restrictions, the use of offensive cyber tools to carry out national intelligence gathering and espionage operations appears to have expanded. In fact, the new cyber intelligence has become the weapon of choice of many countries.

The World Health Organization (WHO) reported a sharp rise in cyber-attacks including an attack attributed to the DarkHotel APT group in an operation which involved other healthcare and humanitarian organizations. In a joint statement, the US and UK cyber agencies warned of increased APT activity targeting healthcare services, specifically accusing China of an organized large scale campaign. APT-41 group is reported to have carried out one of the broadest campaigns by a Chinese actor in the months since the virus outbreak, mostly exploiting Citrix and Cisco vulnerabilities. Iranian-linked hackers are believed to be behind an attack on US drug manufacturer, Gilead, which is in an advanced stage of developing a COVID-19 treatment.

Other regional APT groups utilized the COVID-19 conversation to disguise their routine operations. APT-36, a Pakistan-based threat group, has been pushing its CrimsonRat against Indian governmental entities using fake COVID-19 advisories. India-related Patchwork APT targeted Chinese entities using malicious Excel documents impersonating the Chinese National Health Commission, while Chinese APT groups attacked Mongolia and APAC countries using infected RTF COVID-19-related documents and sending forged diplomatic emails. The North Korean-affiliated group Kimsuky conducted an operation against South Korean organizations under the cover of COVID-19 related material.

The Russian-linked Gamaredon group targeted Ukrainian entities, impersonating Ukraine's Ministry of Health. Hades, another suspected Russian-affiliated group, targeted Ukrainian entities while disguising themselves as an RIA newspaper journalist in pursuit of COVID-19-related information. This attack was suspected to be connected to a later disinformation campaign when a flood of messages on social media claimed that COVID-19 arrived in Ukraine, resulting in escalating fears and riots.

MILESTONE

Countries often use cyber-attacks to achieve their military and political goals in a stealthy manner, without the regular retaliation and consequences of kinetic military action and provocations. One recent cyber conflict stands out. In an attack directed at the Israeli water infrastructure in April, alleged Iranian threat actors aimed to raise chlorine levels in the county's drinking water. In what is considered a retaliatory act, Israel is believed to be behind the cyber-attack that hit Iran's Shahid Rajaee port on the Strait of Hormuz and halted port activity. Neither country officially took responsibility for the attacks, yet this exchange of cyber blows marks a new level of integration of cyber-warfare into the domain of traditional warfare.

Mobile Trends – Seeking New Infection Vectors

From the threat actors' perspective, gaining a foothold on victims' platforms is perhaps the most challenging stage. This is true even more so with mobile platforms, which have controlled access to the official app stores. Traditionally, attackers relied on third party app stores and user errors for the initial infection stage. However, growing user awareness has driven threat actors to increase their efforts at finding additional infection vectors.

In recent months, we have witnessed a substantial increase in the number of malicious applications in the official Google Play store. We reported applications infected with the Tekya clicker, BearCloud and Haken, and much more malware, all found on the official Google Play store.

One of the methods used to disguise the malicious nature of an application is the use of the native programing languages used for their development. Many threat actors "go native"; instead of using Java for developing malicious applications, they use native Android code, typically C and C++. That makes it much harder to decompile the code and identify it as malicious. It also reduces the effectiveness of malware detection procedures in the Google Store. Tekya, Haken, Joker and Circle are just some of the malware using native implementation to evade detection. And indeed, when researchers examined 150,000 Android apps, they found that almost 7% of the apps on Google Play contained hidden backdoors.

In other cases like Mandrake, threat actors worked in multiple stages, with the first stage delivering a benign application. Only in later stages, after the operators carefully verified they are not running in a controlled (sandbox) environment, do they continue to the next stage, dropping the malicious part of the application.

Other actors try to adopt general desktop malware TTPs (techniques, tactics and procedures) and replicate them on mobile platforms. Trickbot has been detected pushing an Android app called Trickmo to supplement its abilities and bypass 2FA (Two-Factor Authentication) mechanisms. Trickbot is not the only app reading SMS messages. EventBot, an Android infostealer was also designed to intercept SMS authentication messages that are used for more than 200 financial applications in the US and Europe.

MILESTONE

Among all the mobile attacks reported over the past six months, we found one which may indicate a new methodology of malware distribution. In this attack, threat actors infected more than 75% of the mobile platforms belonging to a multinational corporation with the Cerberus banker. To accomplish this, they used the corporate's Mobile Device Management (MDM), often mistaken as a security measure, to centrally install Cerberus on multiple mobile devices. This was the first attack seen in the wild that puts enterprise mobile networks at risk of a coordinated attack that affects operations and endangers digital assets.

Cloud Threats

Cloud technologies and services, with the benefits of scalability, agility and cost effectiveness, are widely recognized as the engine that allowed companies worldwide to make a rapid and sudden transition to working from home. But months after COVID-19 entered our lives and changed the way we work and do business, we must also acknowledge the risks we face and guard against these new threats. The last few months demonstrated that new risks to and malicious utilization of the cloud environment are still unfolding.

MILESTONE

In January, for the first time, a critical vulnerability in a major cloud infrastructure was found and reported by Check Point researchers. The vulnerabilities, with a perfect 10.0 CVE score, could allow threat actors to escape the virtual machine infrastructure of Microsoft Azure and compromise data and apps of other tenants who unknowingly share the same hardware. Unlike in previous cloud breaches, the source of the problem was the infrastructure itself and individual users could do nothing to protect themselves, proving that cloud infrastructure is not without its pitfalls.

Cloud service providers are also vulnerable to flaws in their unpatched equipment, as was demonstrated when a French cloud service provider was hacked through an unpatched Citrix server vulnerability. In this case, 30TB of client information was encrypted using the DoppelPaymer ransomware.

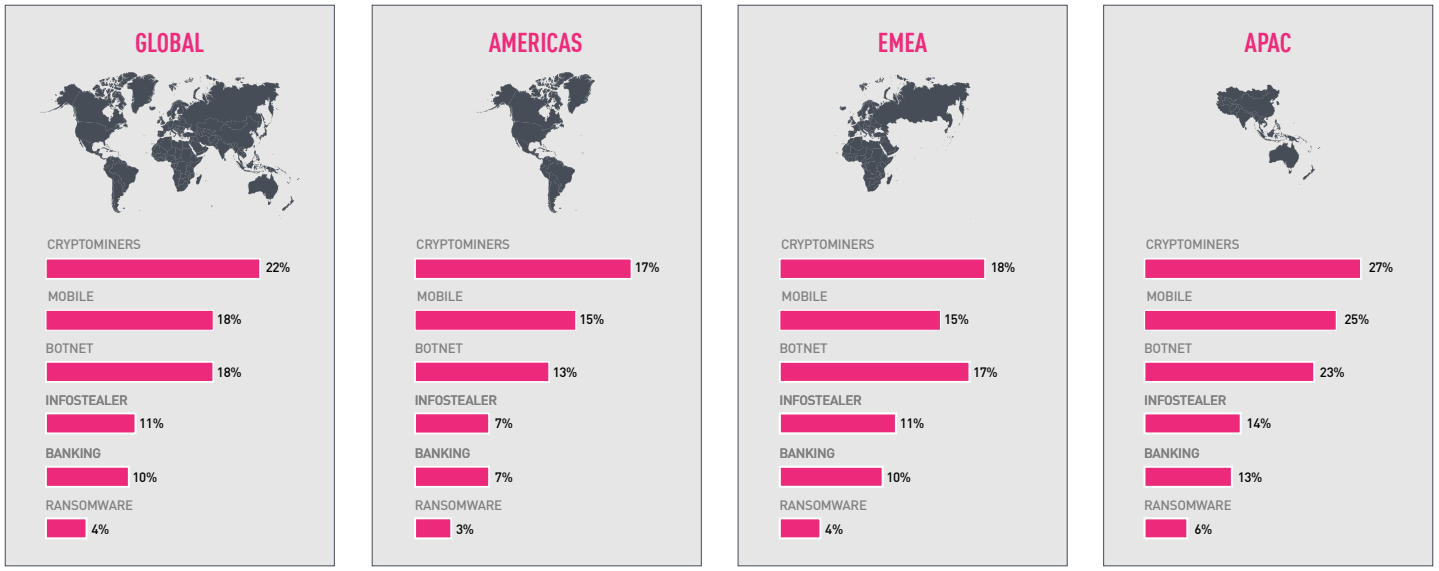
Another growing trend is the use of cloud infrastructure for the benefit of the threat actors. Attackers disguise malicious payloads in cloud infrastructure, storing them on GitHub, Gmail or Alibaba to deliver commands or host configuration files. In other cases, just uploading seemingly benign documents with malicious links to Google Drive can give them the extra touch of legitimacy needed to trick unsuspecting victims. Cloud services are aware of the way these TTPs implement emulation and scanning procedures, but threat actors retaliate with encryptions and camouflage techniques, offering droppers dedicated to placing malware on the cloud.

Cloud-based applications make phishing attacks more effective and facilitate BEC attacks, which are the leading reason for financial loss in cyber-attacks. The extensive control granted to users by Office365 and similar services can give attackers in possession of stolen credentials, obtained from phishing operations, a critical foothold inside the target organization. Attackers have been seen maintaining control of stolen accounts for long periods of time, eventually conducting sophisticated BEC operations utilizing the information they receive.

Misconfigured cloud resources remain one of the top reasons for data breaches in the cloud. Hundreds of gigabytes of a finance company were compromised through an AWS S3 bucket which had not used any form of encryption, authentication or access credentials. Another AWS unprotected storage of a student loan company leaked thousands of recorded calls and personal document scans. Hundreds of millions of US real-estate related records were exposed on an unprotected and unidentified Google Cloud service.

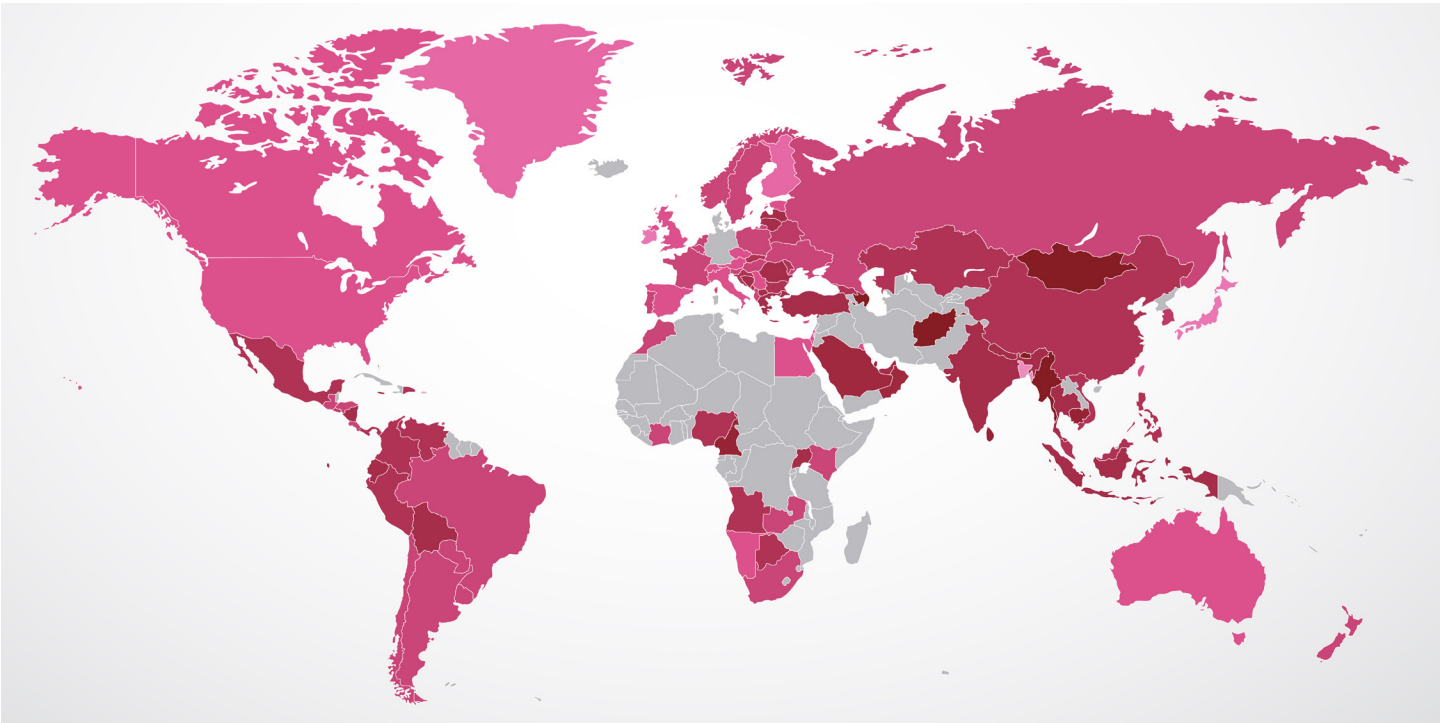
Whether it is through cloud infrastructure vulnerabilities, direct attacks on cloud service providers or by taking advantage of misconfiguration and users errors, the cloud continues to be a lucrative target for threat actors especially in the post-Corona world that day by day becomes the new normal.

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 cyber attacks are taking place worldwide in real time.



Top Malicious File Types – Web vs. Email

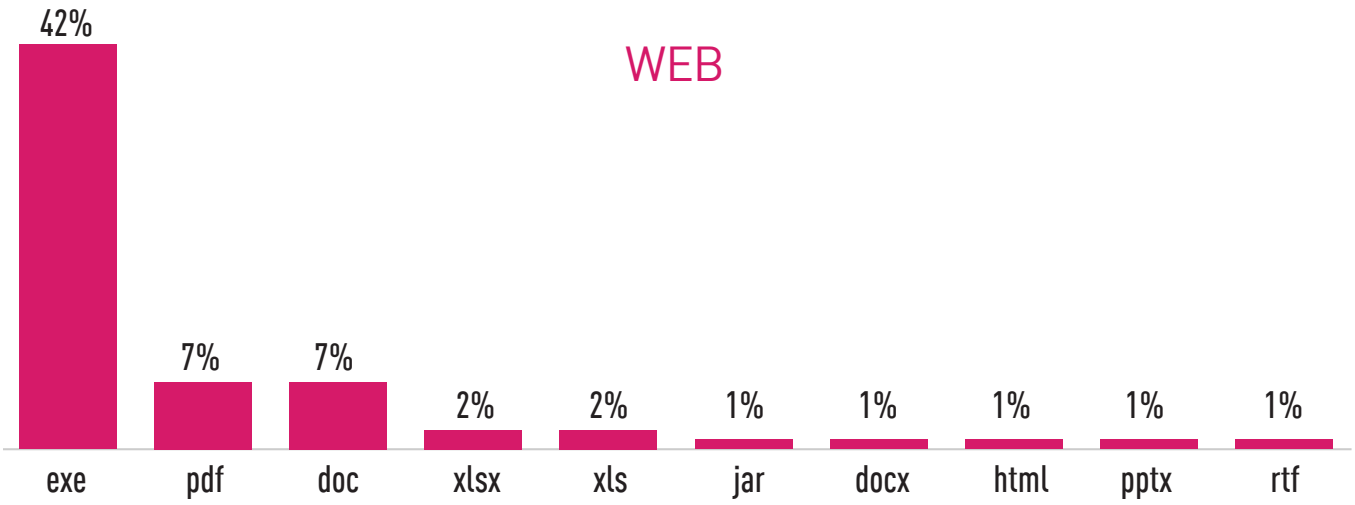


Figure 1: Web – Top malicious file types

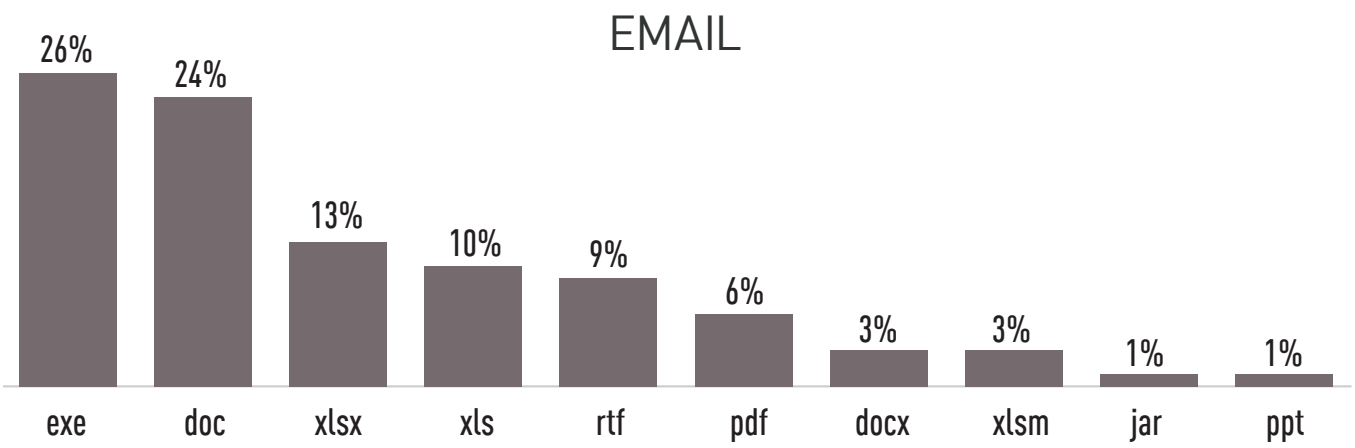


Figure 2: Email – Top malicious file types

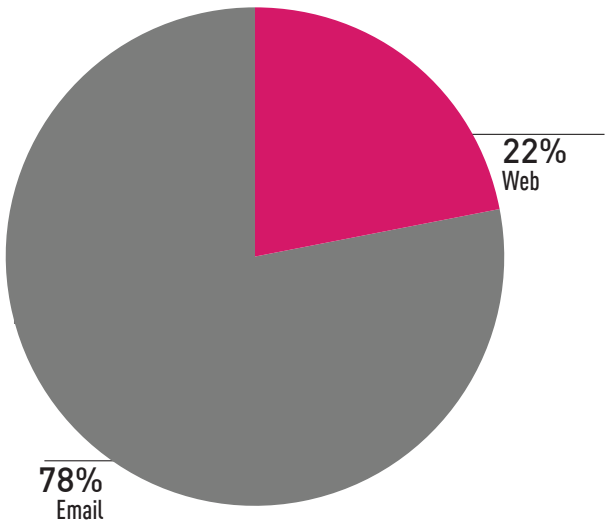


Figure 3: Distribution protocols – email vs. web attack vectors

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 2020. For each of the regions below we present the most prevalent malware.

Top Malware Families

Global

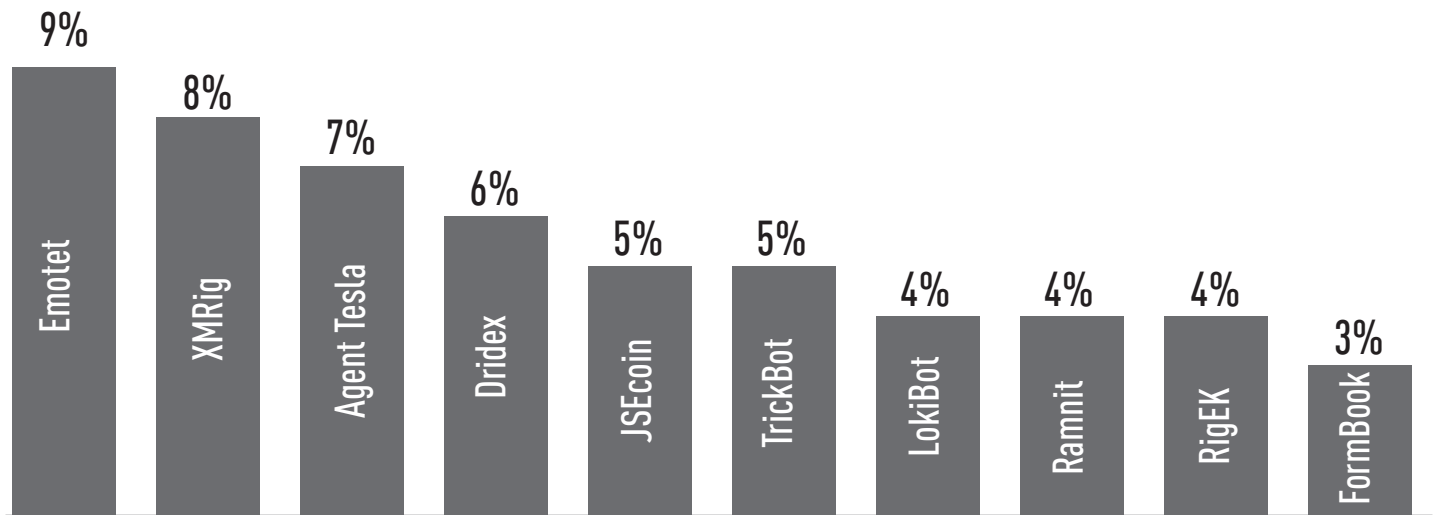


Figure 4: Most Prevalent Malware Globally: Percentage of corporate networks impacted by each malware family

Americas

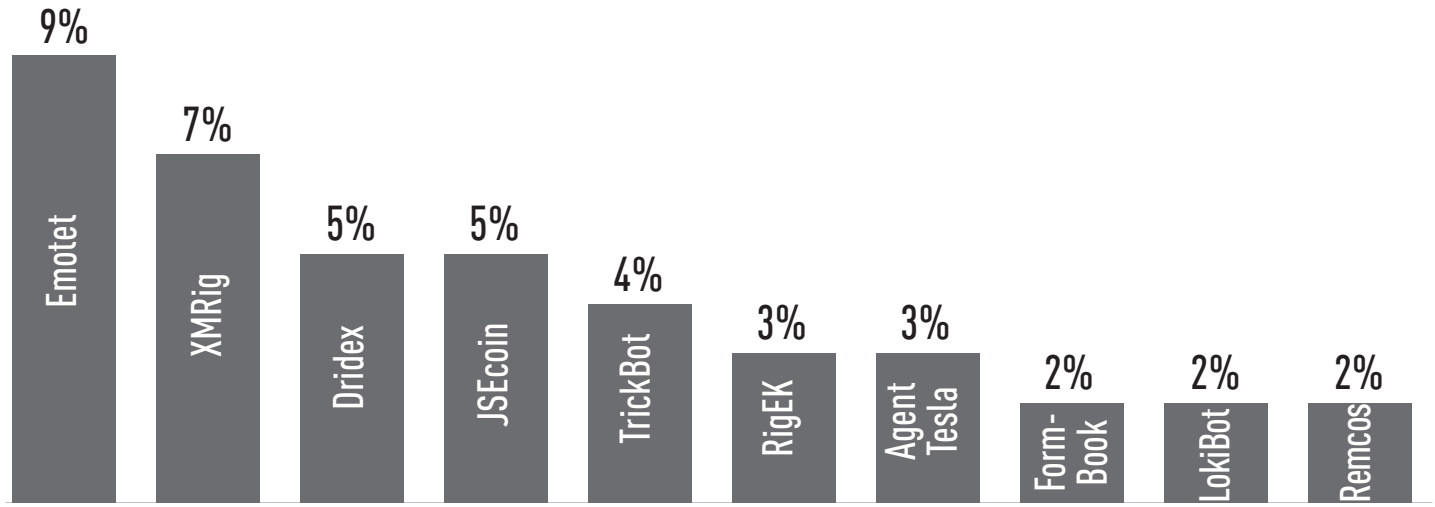


Figure 5: Most Prevalent Malware in the Americas

Europe, Middle East and Africa (EMEA)

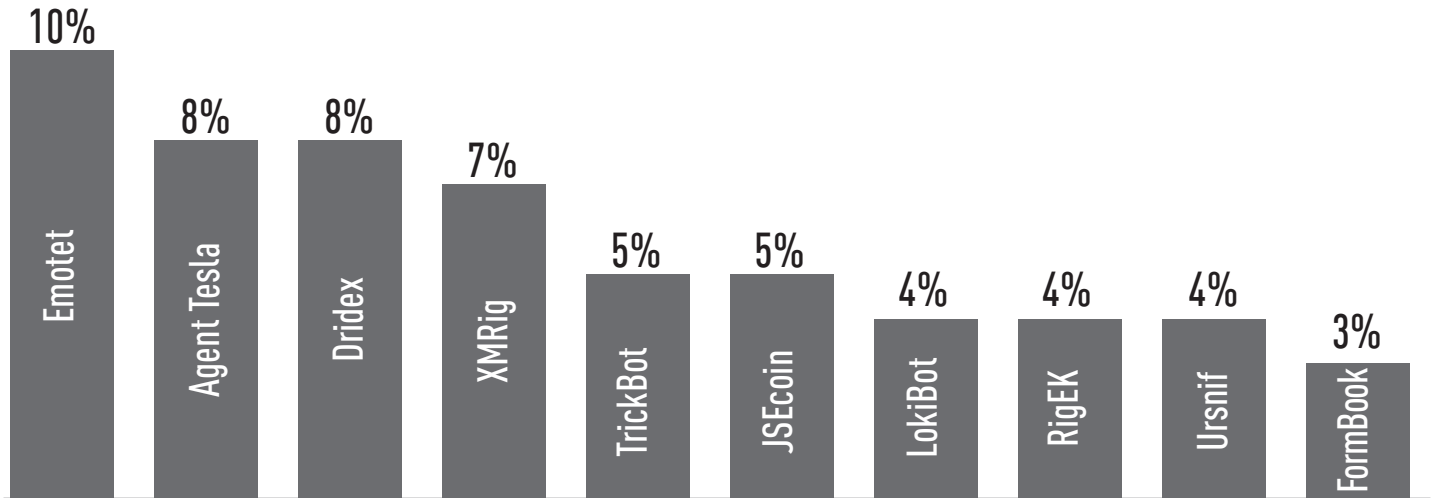


Figure 6: Most Prevalent Malware in the EMEA

Asia Pacific (APAC)

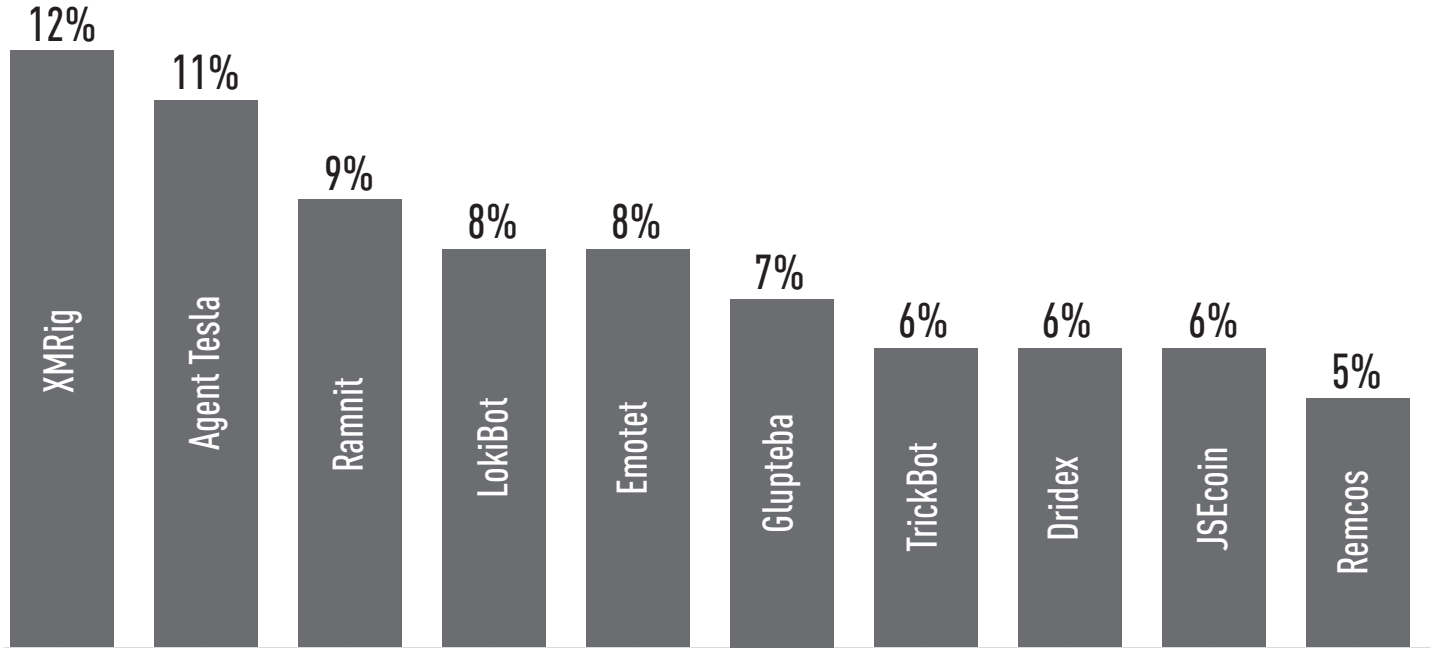


Figure 7 Most Prevalent Malware in the APAC

Global Analysis of Top Malware

Despite Emotet's operators habit to take long breaks in activity, the current pause starting in February 2020, while active, Emotet is so prolific that it still reached the dishonorable first place at the top of the global malware chart. Originally a banking Trojan, Emotet has evolved into a botnet operation, mostly propagating through malicious documents sent by email, leasing its infection-base to ransomware threat actors.

The shutdown of notorious drive-by cryptomining services like Coinhive and JSEcoin left XMRig, as the leading cryptominer. Agent Tesla, Lokibot and Remcos, are popular commodity malware options for the less skilled threat actor. They allow attackers to easily build and deploy a remote access Trojan, without requiring any knowledge in malware development, enabling them to rely on existing, easily available tools and tutorials.

Top Cryptomining Malware

Global

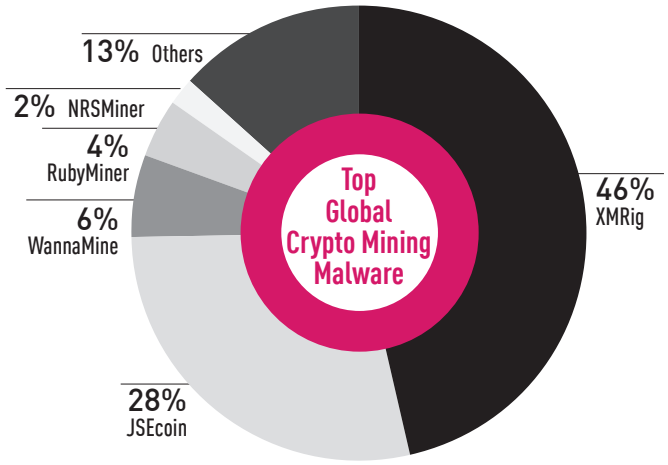


Figure 8: Top Cryptomining Malware Globally

Americas

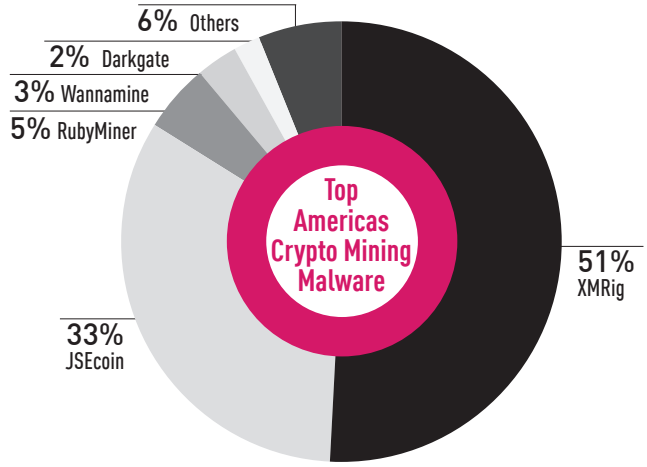


Figure 9: Top Cryptomining Malware in the Americas

EMEA

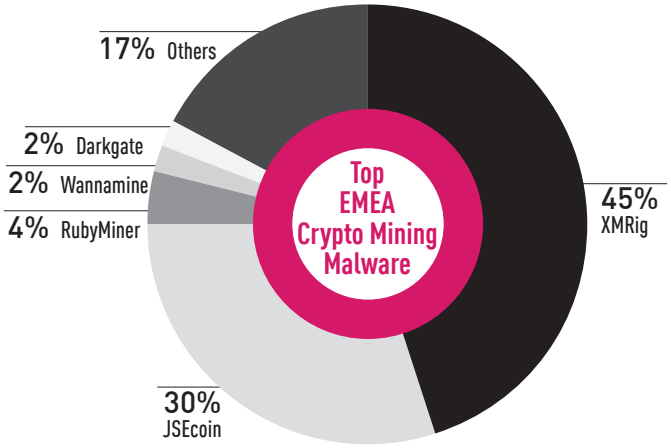


Figure 10: Top Cryptomining Malware in EMEA

APAC

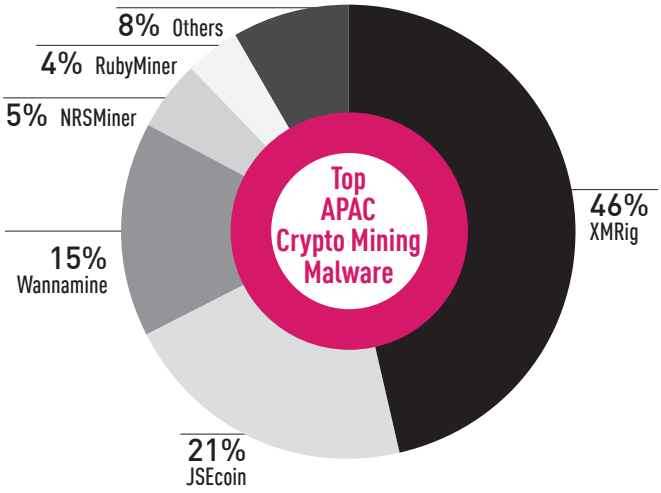


Figure 11: Top Cryptomining Malware in APAC

Cryptominers Global Analysis

The diminishing profitability of drive-by mining caused last year's shutdown of Coinhive, and now JSEcoin's operations. XMRig, a popular open-source mining malware, took their place on the list of top crypromining threats.

XMRig is an open-source tool created for legitimate purposes, but threat actors often use it, or a modified version, as a mining tool for cryptocurrency. Today, XMRig is still actively used in various malicious activities, including in compromised Kubernetes clusters. Together with mining malware like Wannamine and RubyMiner, XMRig is likely the leader in the illegitimate cryptocurrency mining world. With the increasing computational power currently required to mine substantial funds, threat actors are seeking new venues, and in some occasions have even been seen exploiting supercomputers for mining purposes. Another noticeable trend is for other genres of malware to add cryptomining as an additional source of income as we reported regarding the Phorpiex botnet.

Top Mobile Malware

Global

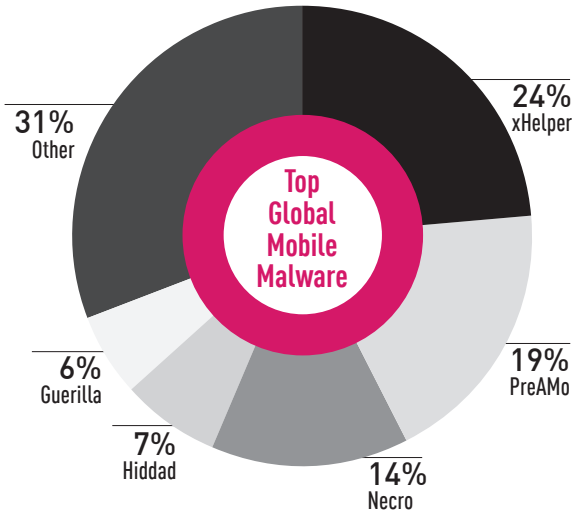


Figure 12: Top Mobile Malware Globally

Americas

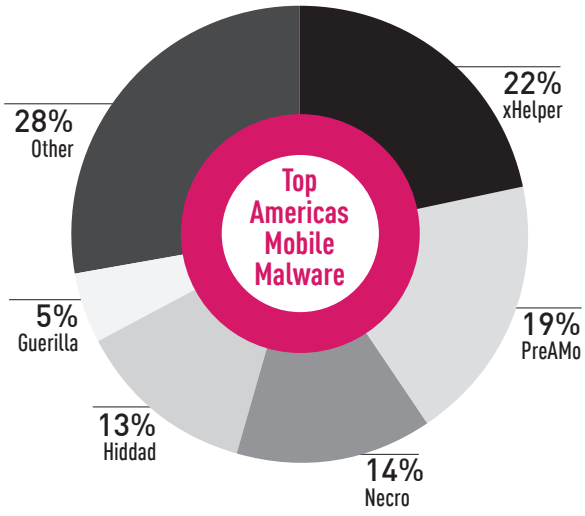


Figure 13: Top Mobile Malware in the Americas

EMEA

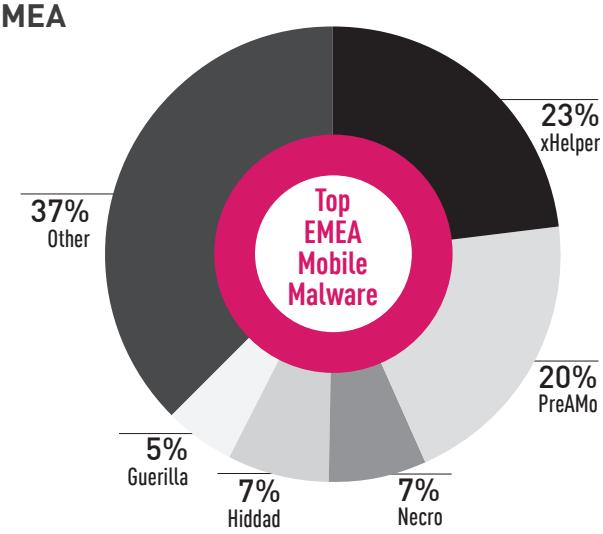


Figure 14: Top Mobile Malware in EMEA

APAC

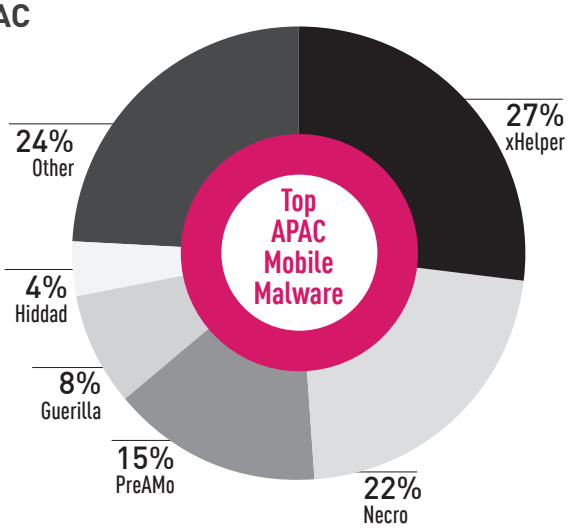


Figure 15: Top Mobile Malware in APAC

Mobile Malware Global Analysis

xHelper for Android, which first appeared in mid-2019, is at the top of the mobile malware list. xHelper perplexed users with its extraordinary persistence that allows it to survive a factory reset. It is followed by PreAMo, Necro, Guerrilla and Hiddad, which are all multifunctional Trojans operating as droppers but mainly monetize by displaying ads and click scams.

Top Botnets

Global

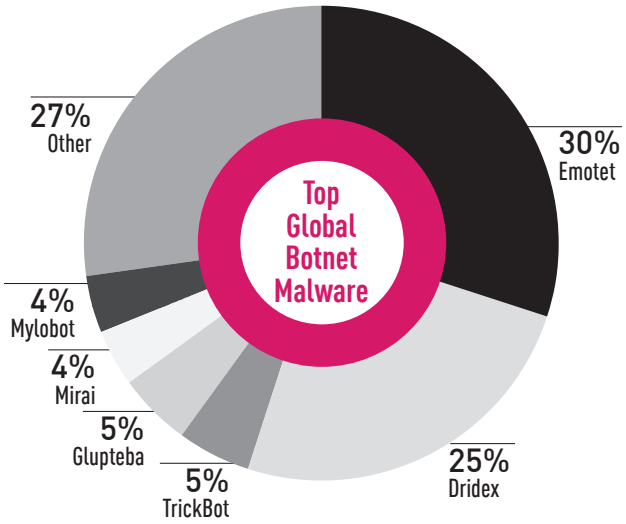


Figure 16: Most Prevalent Botnets Globally

Americas

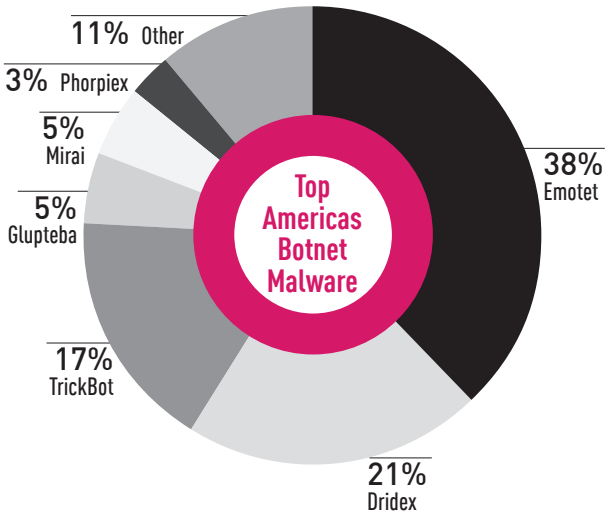


Figure 17: Most Prevalent Botnets in the Americas

EMEA

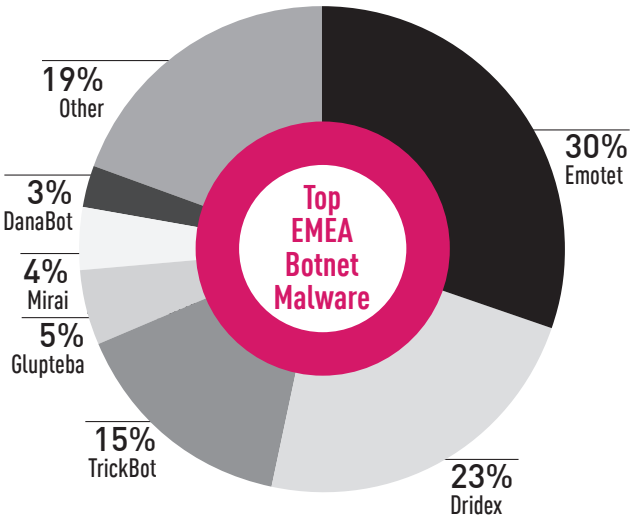


Figure 18: Most Prevalent Botnets in EMEA

APAC

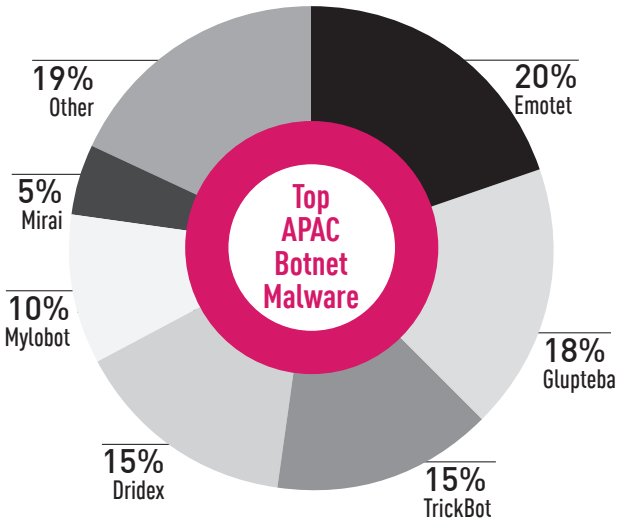


Figure 19: Most Prevalent Botnets in APAC

Botnets Global Analysis

Many malware families started out as specific malware types and then expended to become full-fledged botnets. Emotet followed a similar pattern. Spreading itself through themed malspam campaigns, Emotet holds an extensive infection base. Through sequence of collaborations, Emotet is an important link in malicious supply chain that might start with Emotet infection and end with a ransomware. Most notable is the cooperation between Emotet authors and the TrickBot gang, distributing TrickBot as a second stage malware, often turning into a full blown ransomware attack with the help of the Ryuk ransomware. While Emotet is the most prevalent botnet globally, it occasionally halts its operations for periods. Emotet's most recent disappearance started this February. Having displayed intense activity in January, ending with a COVID-19-related campaign targeting Japan, Emotet ceased its activities and is expected to return later this year.

Top Infostealer Malware

Global

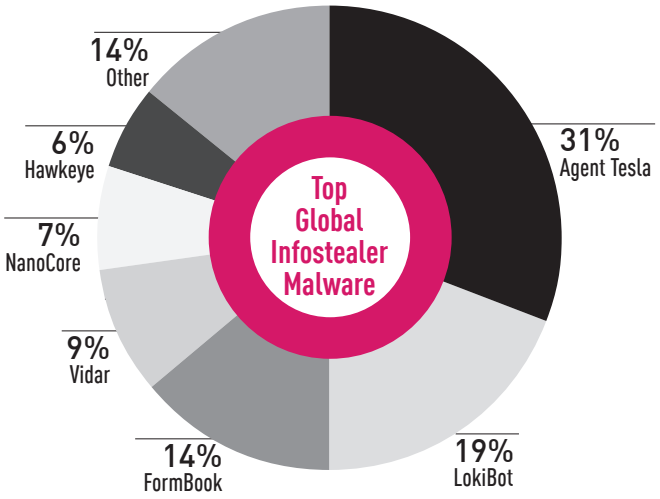


Figure 20: Top Infostealer Malware Globally

Americas

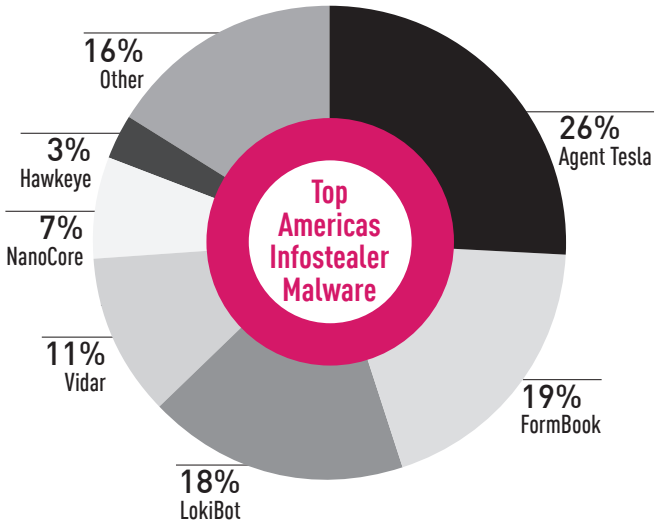


Figure 21: Top Infostealer Malware in the Americas

EMEA

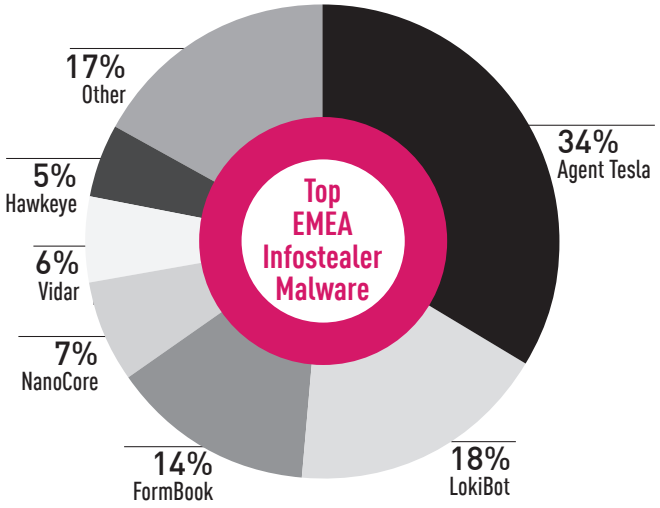


Figure 22: Top Infostealer Malware in EMEA

APAC

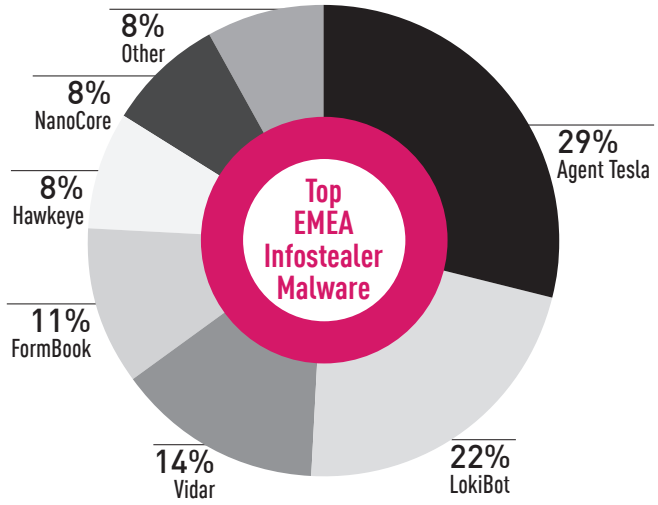


Figure 23: Top Infostealer Malware in APAC

Infostealer Malware Global Analysis

Agent Tesla is a commodity RAT that has been around since 2014, and this year became the most popular infostealer globally. Its functionality includes monitoring keystrokes and the system clipboard. It can also take screenshots and exfiltrate credentials for a variety of software including Google Chrome, Mozilla Firefox and Microsoft Outlook email client. Agent Tesla has been operated as part of a Malware as a Service (MaaS) model with customers paying between $15 - $69 for user licenses. Continuously integrating new functionalities, this year featured a capability to steal Wi-Fi profiles.

Top Banking Trojans

Global

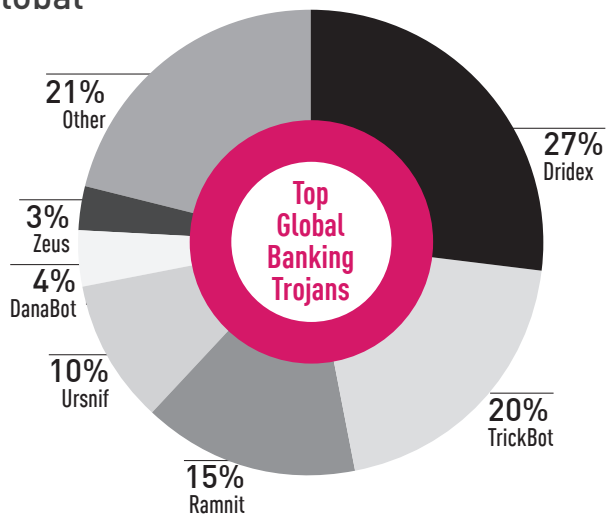


Figure 24: Most Prevalent Banking Trojans Globally

Americas

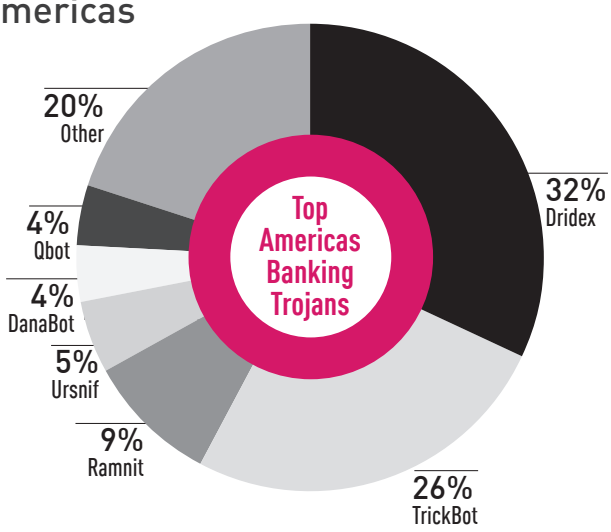


Figure 25: Most Prevalent Banking Trojans in the Americas

EMEA

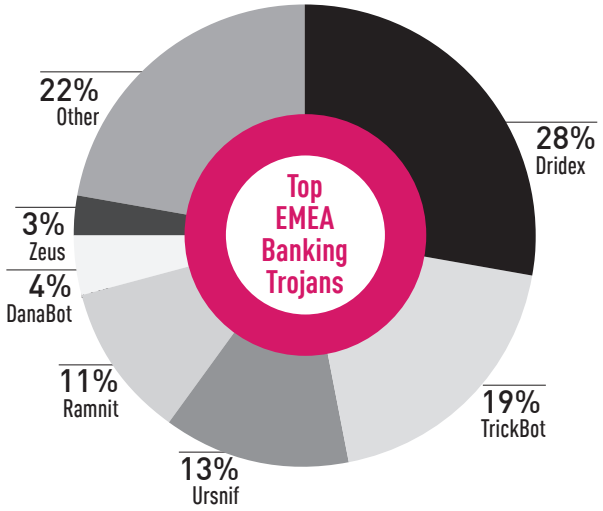


Figure 26: Most Prevalent Banking Trojans in EMEA

APAC

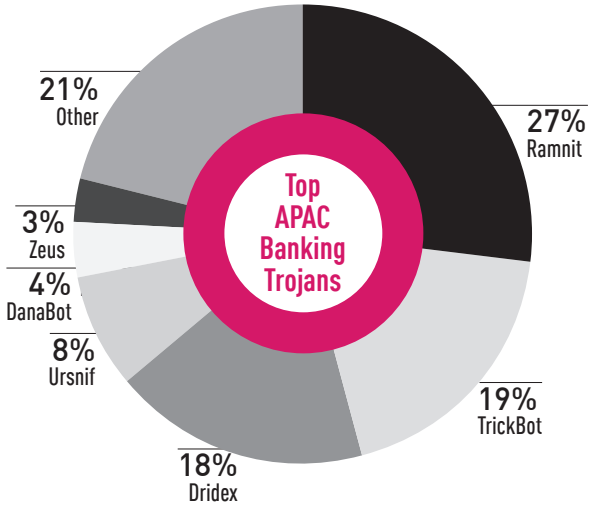


Figure 27: T Most Prevalent Banking Trojans in APAC

Banking Trojans Analysis

The bankers' arena remains dominated by three prominent Trojans – Dridex, TrickBot and Ramnit. The remaining actors engage in a variety of criminal activities in which they operate like botnets, delivering other strands of malware as additional sources of income. As one example, the attack on Maastricht University, conducted by the threat group TA505, used Dridex as its infection vector. Like other malware types, the banking Trojans also leveraged the COVID-19 pandemic to reach new victims.

TrickBot: TrickBot is a Dyre variant, which first emerged in October 2016. Since its initial appearance, it has gradually evolved and extended its functionality from a banking Trojan to a malware collecting the credentials of email accounts, browsers and more, constantly searching for new income sources. TrickBot played a leading role in Ryuk ransomware attacks. This year it continued to develop, adding a new PowerShell backdoor called PowerTrick and a new variant called Anchor. Anchor has been deployed in conjunction with a PowerShell malware attributed to the North Korean Lazarus group. Research suggests a possible collaboration between Lazarus and TrickBot operators. During the COVID-19 pandemic, Trickbot operators targeted Italian users using weaponized fake health warning documents.

High Profile Global Vulnerabilities

The following list of top vulnerabilities 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 2020.

- **Exim Mail Transfer Agent (MTA) software vulnerability (CVE-2019-10149)** – Exim is used to transfer email messages and often comes preinstalled with versions of Linux. The Exim Mail Transfer vulnerability was found and reported in March 2019. An improper handling of recipient address validation on servers with Exim 4.87 through 4.91 could lead to Remote Code Execution and it was therefore ranked as a critical. Although a security update was released by June 2019, there are still almost a million unpatched servers online daily, mostly in the US, Germany and Russia. The flaw is actively exploited and an NSA advisory warned that the Russian Sandworm APT has been abusing it for almost a year.

- **Draytek Vigor Command Injection vulnerability (CVE-2020-8515)** – One interesting vulnerability revealed this year affects routers and VPN gateways of the Taiwanese manufacturer DrayTek. The critical RCE vulnerability, tracked as CVE-2020-8515, was first reported in January 2020 and a PoC soon followed. It now seems that the vulnerability has been exploited since at least December 2019. Although a patch was published, by March 2020, researchers reported evidence of active campaigns exploiting it and attempts to establish a new DDoS botnet. By the end of H1, we saw 24% of organizations have been affected by exploitation attempts of the Draytek Vigor bug.

- **Microsoft Windows SMBGhost RCE Exploit (CVE-2020-0796)** – An alarming wormable flaw in the Microsoft SMB protocol, affecting Windows 10 and Windows Server 2019, was reported publicly in March 2020. Initial PoCs demonstrated only Local Privilege Escalation (LPE) capabilities and Microsoft was quick to publish a patch. By June 2020, researchers published a PoC for RCE, which raised concerns for millions of unpatched computers that could be exploited. US CISA released an advisory warning that "cyber actors are targeting unpatched systems with the new PoC."

Throughout the first half of 2020, 80% of the observed attacks utilized vulnerabilities reported and registered in 2017 and earlier. More than 20% of the attacks used vulnerabilities that are at least seven years old.

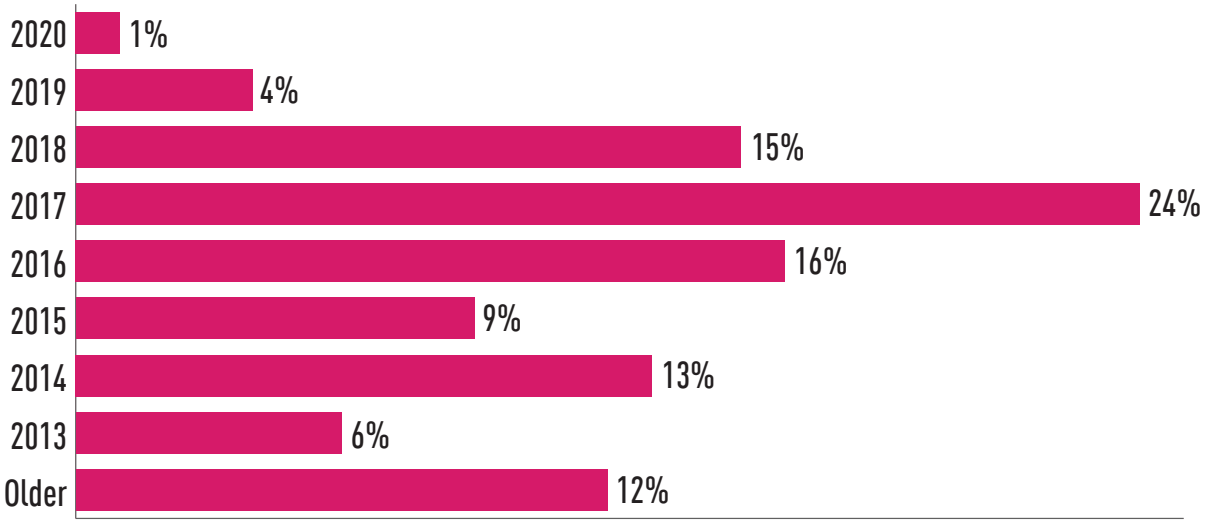


Figure 28: Percentage of attacks leveraging vulnerabilities by disclosure year

Major Cyber Breaches (H1 2020)

In the first half of 2020, cyber breaches continued to be one of the major threats to organizations in all sectors and all regions, putting the sensitive information of billions of people at risk. Below is a recap of the major attacks in each region.

Americas

- **January:** Following the assassination of Iranian Major General Qasem Soleimani, US CISA (Cybersecurity and Infrastructure Agency) issued an official warning regarding a rise in Iranian cyber-attacks directed at US industries and government agencies. In one such incident, hackers identified as "Iran Cyber Security Group Hackers" temporarily defaced the homepage of the U.S. Federal Depository Library Program.
- **January:** Following the refusal of Travelex to pay a ransom demand of $6M in exchange for decryption keys, the group behind the Sodinokibi ransomware (aka REvil) threatened to sell 5GB of customer personal information stolen and exfiltrated prior to the encryption, thus exposing the company to GDPR proceedings.
- **January:** The Albany County (NY) Airport Authority announced it was hit by a Sodinokibi ransomware attack encrypting its servers and backup systemss.
- **February:** The US Federal Trade Commission issued a warning regarding phishing attacks relating to the fears surrounding the Coronavirus, where emails and text messages asking for donation or offer advice are used for attacks.
- **February:** MGM resorts suffered a data breach exposing over 10.6 million guests' names, addresses, and passport numbers. The data breach stems from a security incident that took place last year. Among people affected were business travelers, reporters attending tech conferences, CEOs, government officials, and celebrities like Justin Bieber and Twitter founder Jack Dorsey.
- **March:** Cybercriminals continue to exploit the fear surrounding the COVID-19 outbreak and are distributing instances of AZORult info stealer using a weaponized application for the Coronavirus heat map. The app displays a legitimate Coronavirus map while the info stealer runs in the background.
- **March:** The operators behind Sodinokibi ransomware claim that they are in possession of 70,000 financial and work documents as well as 60,000 customer data records belonging to the US fashion house Kenneth Cole. The operators published a portion of the data, and threaten to release all of it if the fashion house refuses to pay ransom.
- **April:** Marriott hotels disclosed a security breach affecting 5.2 million guests. The company informed guests via email and provided personal-information-monitoring services to those impacted. Marriott was fined $123 million last year for a 2018 breach of 327 million records.

- **April:** Hammersmith Medicines Research LTD (HMR), a research firm on standby to perform live trials of coronavirus vaccines, suffered a data breach by the Maze ransomware. HMR decided not to pay the ransom, and the stolen data was published a week later on the attackers "News" site. The attack compromised volunteers' identity documents and test results, including positive HIV and drug tests.
- **May:** Check Point Research discovered a targeted attack on a multinational conglomerate. The company's Mobile Device Manager (MDM) server was compromised and used to install Cerberus banking Trojan on employees' mobile devices. This new variant of Cerberus has enhanced RAT capabilities and can exfiltrate extensive data including credentials, SMS messages (along with Two-Factor Authenticaiton SMS codes) and more.
- **June:** The US NSA warned that Russia's Sandworm APT group, an arm of Russian military intelligence, has been exploiting a vulnerability in the Exim mail traffic agent since August of last year, giving it remote code execution abilities. Sandworm is believed to be responsible for the Ukraine grid disruptions in 2015.

Europe, the Middle East and Africa (EMEA)

- **January:** Bretagne Télécom, a French cloud services company, was hit by a DoppelPaymer ransomware attack. The attackers successfully exploited the then-unpatched vulnerability in Citrix (CVE-2019-19781), and managed to encrypt 148 machines. The attackers stole some data during the attack, and published samples of it in DopplePaymer's recently-launched data leak website.
- **February:** Croatia's petrol station chain INA group was hit by "CLOP" ransomware. The attack affected normal operations such as issuing mobile phone vouchers and electronic vignettes, and paying utility bills.
- **March:** Global fear of the Corona virus epidemic continues to be exploited for malicious cyber operations. Check Point Research reports thousands of newly registered coronavirus related domains, which are 50% more likely to be malicious than other domains. CPR also revealed a Trickbot campaign using a fake health warning document to target Italian users.
- **March:** UK based telecom provider Virgin Media reported a year-long data leak exposing the personal information of 900,000 customers, due to the misconfiguration of a marketing database.
- **April:** Travelex opted to pay $2.3 million to release its information. Travelex, a London-based foreign exchange company was crippled for weeks due to a ransomware attack by the Sodinokibi gang. Travelex negotiated with the group for the last few weeks until arriving at a mutually agreed upon payment.
- **April:** The Portugal electric company, Energias de Portugal (EDP), was hit by Ragnar Locker ransomware. The attackers demanded 1,580 Bitcoin, the equivalent of $10.9 million, to retrieve 10 TB of stolen data. To prove they had the company's data, the threat actors leaked data from EDP's KeePass password manager, which contains the employee login credentials, accounts, URLs and notes.

- **April:** Sonatrach, Algeria's national oil company, is the latest victim of the Maze ransomware group. As part of its double-extortion strategy, the attackers posted Sonatrach's investment plans, financials and other details on a dedicated site, threatening to publish additional information unless ransom is paid.
- **May:** A misconfigured Elasticsearch server belonging to the French newspaper Le Figaro exposed over 8TB of data containing 7.4 billion records with PII (Personally Identifiable Information) of reporters, employees and at least 42,000 users.
- **May:** UK National Cyber Security Centre (NCSC) warned of targeted cyber attacks against UK universities and scientific institutions involved in COVID-19 research.
- **June:** Hackers targeted executives of a German task force supplying face masks and medical equipment to use against COVID-19. The hackers launched a spear-phishing campaign to steal Microsoft login credentials, targeting over 100 senior executives in 40 organizations.

Asia-Pacific (APAC)

- **January:** A cyber espionage campaign targeting NGOs, political organizations and government agencies in Asia was uncovered. The operation, attributed to the Chinese APT group Bronze President, has been active since at least mid-2018 and used a variety of tools, both well-known and custom-made. Initial access is probably gained using phishing emails with malicious links.
- **February:** Australian logistics and transportation corporation Toll Group suffered a targeted ransomware attack affecting over 1000 servers and disabling most of the company's services. Toll Group reports the ransomware used in the attack was a variant of Mailto aka Kokoklock.
- **March:** APT36, a Pakistani based threat actor, has been spreading the Crimson RAT via a spear-phishing campaign using a coronavirus-themed document disguised to look like a health advisory email. The RAT steals credentials from the victim's browser, captures screenshots, collects anti-virus software information, lists running processes, and more.
- **March:** A campaign leveraging the COVID-19 pandemic to target the Mongolian public sector was detected by Check Point Research. The campaign, attributed to a China-linked APT group, used spear-phishing and coronavirus-themed documents to install a custom remote-access Trojan.
- **April:** A database containing 400,000 payment card records belonging to South Korean and US banks and financial companies was uploaded to a hacking forum. The source of the data remains unknown.
- **April:** Hackers abused the login system of Nintendo, resulting in the leakage of the data for 160,000 user accounts. The breach was discovered after a number of users complained their accounts were accessed; many of the hacked accounts were abused to purchase game features and virtual coins.

- **April:** Threat actors employed the previously-unknown PoetRAT Trojan in a coronavirus-themed campaign aimed at the Azerbaijan government and utility companies. Delivered via phishing, the malware infected ICS and SCADA systems used to control the wind turbines within the renewable energy sector.
- **May:** Check Point Research discovered an ongoing cyber espionage operation against government entities in the Asia Pacific (APAC) region. The operation is attributed to the Naikon APT group, and uses a backdoor called Aria-body to take control of the victims' networks. One of the attack vectors infected a foreign embassy as a launching pad to propagate the attack to government entities via malicious emails.
- **May:** Unacademy, an India-based online learning platform, suffered a major data breach that exposed the details of 22 million users. The compromised information included usernames, hashed passwords, first and last names, and other account profile details, and was offered for sale on Dark Net forums for $2,000.
- **May:** Thailand's Android users were targeted by a new variant of DenDroid named "WolfRAT", and operated by "Wolf Research" over messaging apps like WhatsApp, Facebook Messenger and Line. The new variant performs spying functions, steals photos, audio, text messages and more.
- **June:** Hackers hijacked a domain belonging to the Japanese cryptocurrency exchange CoinCheck after managing to access their account at the Oname.com domain registrar. The hijacked domain was used to conduct spear-phishing attacks on customers and alter the main DNS entry of the company domain.
- **June:** Delhi-based hack-for-hire group BellTroX allegedly targeted thousands of high-profile individuals and hundreds of organizations worldwide in a seven-year long campaign. The group used phishing kits to steal sensitive data from the victims and conduct commercial espionage on behalf of their clients.
- **June:** Operations of the Australian beverage company Lion were shut down due to a ransomware attack. The attack is the latest in a series of ransomware to hit Australian companies, such as Toll logistics and BlueScope Steel Limited.

Appendix – Malware Family Descriptions

- **Agent Tesla –** Agent Tesla is an advanced RAT which functions as a keylogger and password stealer and has been active since 2014. Agent Tesla can monitor and collect the victim's keyboard input and system clipboard, and can record screenshots and exfiltrate credentials for a variety of software installed on a victim's machine (including Google Chrome, Mozilla Firefox and Microsoft Outlook email client). Agent Tesla is sold on various online markets and hacking forums.
- **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.
- **Cerberus –** First seen in the wild in June 2019, Cerberus is a Remote Access Trojan (RAT) with specific banking screen overlay functions for Android devices. Cerberus operates in a Malware as a Service (MaaS) model, taking the place of discontinued bankers like Anubis and Exobot. Its features include SMS control, key-logging, audio recording, location tracking, and more.
- **Clop –** Clop is a ransomware that was first discovered in early 2019 and mostly targets large firms and corporations. It was used in an attack on the Dutch University of Maastricht which some researchers linked to the Russian cybercrime group TA505. During 2020, Clop began exercising a double-extortion strategy, where in addition to encrypting the victim's data, the attackers also threaten to publish stolen information unless ransom demands are met.
- **Coinhive –** Coinhive is a now defunct, once popular cryptomining service, designed to perform unauthorized online mining of Monero cryptocurrency when a user visits a particular web page. The implanted JavaScript uses a large amount of the end user machines' computational resources, thus impacting performance.
- **DanaBot –** DanaBot is a modular banking Trojan written in Delphi that targets the Windows platform. The malware, which was first observed in 2018, is distributed via malicious spam emails. Once a device is infected, the malware downloads updated configuration code and other modules from the C&C server. Available modules include a "sniffer" to intercept credentials, a "stealer" to steal passwords from popular applications, a "VNC" module for remote control, and more.
- **DarkGate –** DarkGate is a multifunction malware active since December 2017 which combines ransomware, credential stealing, and RAT and cryptomining abilities. Targeting mostly the Windows OS, DarkGate employs a variety of evasion techniques.
- **DopplePaymer –** DopplePaymer is a variant of the BitPaymer ransomware discovered in 2019. It was involved in several high-profile targeted attacks including attacks against the city of Florence, Alabama, and Bretagne Télécom. It is usually delivered as the final stage after a successful intrusion into the victims' network. DoppelPaymer targets mostly middle to large businesses and demands high ransoms. In 2020, the operators of DoppelPaymer began exercising a double-extortion strategy, where in addition to encrypting the victim's data, they also threaten to publish stolen information unless ransom demands are met.
- **Dridex –** Dridex is a Banking Trojan that targets the Windows platform. It is delivered by spam campaigns and Exploit Kits, and relies on WebInjects to intercept and redirect banking credentials to an attacker-controlled server. Dridex contacts a remote server, sends information about the infected system, and can also download and execute additional modules for remote control.
- **Emotet –** Emotet is an advanced, self-propagating and modular Trojan. Emotet was once used to employ as a banking Trojan, and now is used as a distributer for other malware or malicious campaigns. It uses multiple methods for maintaining persistence and evasion techniques to avoid detection. In addition, Emotet can also be spread through phishing spam emails containing malicious attachments or links.
- **FormBook –** FormBooks is an Infostealer targeting the Windows OS and was first detected in 2016. It is marketed as Malware as a Service (MaaS) in underground hacking forums for its strong evasion techniques and relatively low price. FormBook harvests credentials from various web browsers, collects screenshots, monitors and logs keystrokes, and can download and execute files according to orders from its C&C.
- **Glupteba –** Known since 2011, Glupteba is a backdoor which gradually matured into a botnet. By 2019 it included a C&C address update mechanism through public BitCoin lists, an integral browser stealer capability and a router exploiter.

- **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.
- **Hawkeye –** Hawkeye is an infostealer malware for Windows, active since 2013, which is designed primarily to steal users' credentials from infected devices and deliver them to a C&C server. In recent years, Hawkeye 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 which repackages legitimate apps and then releases them to a third-party store. Its main function is displaying ads, but it also can gain access to key security details built into the OS.
- **JSEcoin –** Web-based cryptominer designed to perform unauthorized online mining of Monero cryptocurrency when a user visits a particular web page. The implanted JavaScript uses a large amount of the computational resources of the end users' machines to mine coins, thus impacting the performance of the system. JSEcoin stopped its activity in April 2020.
- **LokiBot –** LokiBot is commodity infostealer for Windows. 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, thus allowing for a range of variants to appear. It was first identified in February 2016.
- **Maze –** Maze is a ransomware first discovered in mid-2019 and was the first ransomware to practice the double-extortion strategy. Maze operators opened a dedicated webpage where, in addition to encrypting victim's data, they started publishing stolen sensitive information from victims who refused to pay the ransom. Many other threat groups followed this strategy.
- **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 Distribute Denial of Service (DDoS) attacks. The Mirai botnet first surfaced in September 2016 and quickly made headlines due to some large-scale attacks including 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 infrastructure.
- **Mylobot –** Mylobot is a sophisticated botnet that first emerged in June 2018 and is equipped with complex evasion techniques including anti-VM, anti-sandbox, and anti-debugging techniques. The botnet allows an attacker to take complete control of the user's system, downloading any additional payload from its C&C.
- **Necro –** Necro is an Android Trojan Dropper. It can download other malware, show intrusive ads and fraudulently charge for paid subscriptions.
- **NRSMiner –** NRSMiner is a cryptominer that surfaced around November 2018, and was mainly spread in Asia, specifically Vietnam, China, Japan and Ecuador. After the initial infection, it uses the famous EternalBlue SMB exploit to propagate to other vulnerable computers in internal networks and eventually starts mining the Monero (XMR) Cryptocurrency.
- **Phorpiex –** Phorpiexecro is a botnet (aka Trik) that has been active since 2010 and at its peak controlled more than a million infected hosts. It is known for distributing other malware families via spam campaigns as well as fueling large-scale spam and sextortion campaigns.
- **PreAMo –** PreAMo is a clicker malware for Android devices, first reported in April 2019. PreAMo generates revenue by mimicking the user and clicking on ads without the user's knowledge. Discovered on Google Play, the malware was downloaded over 90 million times across six different mobile applications.
- **Qbot –** Qbot AKA Qakbot is a banking Trojan that first appeared in 2008. It was designed to steal a user's banking credentials and keystrokes. Often distributed via spam email, Qbot employs several anti-VM, anti-debugging, and anti-sandbox techniques to hinder analysis and evade detection.
- **Ragnar Locker –** Ragnar Locker is a ransomware first discovered in Dec. 2019. It deploys sophisticated evasion techniques including deployment as a virtual machine on targeted systems to hide its activity. Ragnar was used in an attack against Portugal's national electric company in a double-extortion act where the attackers published sensitive data stolen from the victim..
- **Ramnit –** Ramnit is a modular banking Trojan first discovered in 2010. Ramnit steals web session information, giving its operators the ability to steal account credentials for all services used by the victim, including bank accounts, and corporate and social networks accounts. The Trojan uses both hardcoded domains as well as domains generated by a DGA (Domain Generation Algorithm) to contact the C&C server and download additional modules.

- **Remcos –** Remcos is a RAT that first appeared in the wild in 2016. Remcos distributes itself through malicious Microsoft Office documents, which are attached to SPAM emails, and is designed to bypass Microsoft Windowss UAC security and execute malware with high-level privileges..
- **RigEK –** The oldest and best known of the currently operating Exploit Kits, RigEK has been around since mid-2014. Its services are offered for sale on hacking forums and the TOR Network. Some "entrepreneurs" even re-sell low-volume infections for those malware developers not yet big enough to afford the full-fledged service. RigEK has evolved over the years to deliver anything from AZORult and Dridex to little-known ransomware and cryptominers.
- **RubyMiner –** RubyMiner was first seen in the wild in January 2018 and targets both Windows and Linux servers. RubyMiner seeks vulnerable web servers (such as PHP, Microsoft IIS, and Ruby on Rails) to use for cryptomining, using the open source Monero miner XMRig.
- **Ryuk –** Ryuk is a ransomware used by the TrickBot gang in targeted and well-planned attacks against several organizations worldwide. The ransomware was originally derived from the Hermes ransomware, whose technical capabilities are relatively low, and includes a basic dropper and a straight-forward encryption scheme. Nevertheless, Ryuk was able to cause severe damage to targeted organizations, forcing them to pay extremely high ransom payments in Bitcoin. Unlike common ransomware, systematically distributed via massive spam campaigns and Exploit Kits, Ryuk is used exclusively in tailored attacks.
- **Sodinokibi –** Sodinokibi is a Ransomware-as-a-service which operate an "affiliates" program and was first spotted in the wild in 2019. Sodinokibi encrypts data in the user's directory and deletes shadow copy backups to make data recovery more difficult. In addition, Sodinokibi affiliates use various tactics to spread it, including through spam and server exploits, as well as hacking into managed service providers (MSP) backends, and through malvertising campaigns that redirect to the RIG Exploit Kit.
- **TrickBot –** TrickBot is a modular Banking Trojan that targets the Windows platform, and is mostly delivered via spam campaigns or other malware families such as Emotet. Trickbot sends information about the infected system and can also download and execute arbitrary modules from a large array of available modules, including a VNC module for remote control and an SMB module for spreading within a compromised network. Once a machine is infected, the Trickbot gang, the threat actors behind this malware, utilize this wide array of modules not only to steal banking credentials from the target PC, but also for lateral movement and reconnaissance on the targeted organization itself, prior to delivering a company-wide targeted ransomware attack.
- **Ursnif –** Ursnif is a variant of the Gozi banking Trojan for Windows, whose source code has been leaked online. It has man-in-the-browser capabilities to steal banking information and credentials for popular online services. In addition, it can steal information from local email clients, browsers and cryptocurrency wallets. Finally, it can download and execute additional files on the infected system.
- **WannaMine –** WannaMine is a sophisticated Monero crypto-mining worm that spreads the EternalBlue exploit. WannaMine implements a spreading mechanism and persistence techniques by leveraging the Windows Management Instrumentation (WMI) permanent event subscriptions.
- **xHelper –** xHelper is an Android malware which mainly shows intrusive popup ads and notification spam. It is very hard to remove once installed due to its reinstallation capabilities. First observed in March 2019, xHelper has now infected more than 45,000 devices.
- **XMRig –** XMRig is open-source CPU mining software used to mine the Monero cryptocurrency. Threat actors often abuse this open-source software by integrating it into their malware to conduct illegal mining on victims' devices.
- **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.

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