Check Point
SOFTWARE TECHNOLOGIES LTD

CYBER ATTACK TRENDS

Mid Year Report 2021

CONTENTS

EXECUTIVE SUMMARY

CHECK POINT SOFTWARE'S MID-YEAR SECURITY REPORT REVEALS A 29% INCREASE IN CYBERATTACKS AGAINST ORGANIZATIONS GLOBALLY

'Cyber Attack Trends: 2021 Mid-Year Report' uncovers how cybercriminals have continued to exploit the Covid-19 pandemic and highlights a dramatic global 93% increase in the number of ransomware attacks

- **EMEA**: organizations experienced a **36%** increase in cyber-attacks since the beginning of the year, with 777 weekly attacks per organization
- **USA: 17%** increase in cyber-attacks since the beginning of the year, with 443 weekly attacks per organization
- **APAC: 13%** increase in cyber-attacks on organizations since the beginning of the year, with 1338 weekly attacks per organization

In the first six months of 2021, the global rollout of COVID-19 vaccines gave hope that we will be able to live without restrictions at some point—but for a majority of organizations internationally, a return to pre-pandemic 'norms' is still some way off. The enforced shift to remote working in March 2020 undoubtedly fast-forwarded 'digital transformation' and brought with it many benefits to our working lives. As such, the first half of 2021 has seen organizations commit to a continuous hybrid model. However, cyber criminals have continued to adapt their working practices in order to exploit this shift, targeting organizations' supply chains and network links to partners in order to achieve maximum disruption. This year, we have seen a huge global increase in the number of ransomware attacks, with high-profile incidents such as the attacks on Colonial Pipeline and JBS making world headlines. And while the 'Double Extortion' ransomware strategy proved popular in 2020, this year's surge in attacks has brought to light a worrying new threat—that of Triple Extortion.

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

Highlights of the 'Check Point Cyber Attack Trends: Mid-Year report 2021' include:

GLOBAL INCREASE IN CYBER-ATTACKS

In 2021, US organizations saw an average of 443 weekly attacks, marking a **17%** increase compared to earlier this year. In EMEA, the weekly average of attacks per organization was 777, a **36%** increase. APAC organizations saw 1338 weekly attacks, a **13%** increase.

THE EMERGENCE OF TRIPLE EXTORTION RANSOMWARE

In a year that has seen a **93%** increase in ransomware attacks, ransomware actors have adopted a new strategy, adding a third step to the Double Extortion technique. In addition to stealing sensitive data from organizations and threatening to release it publicly unless a payment is made, attackers are now targeting organizations' customers and/or business partners and demanding ransoms from them too.

THE SOLARWINDS FALL-OUT

More than **18,000** companies and government offices downloaded what seemed to be a regular software update on their computers, but it was actually a Trojan. By leveraging a common IT practice of software updates, the attackers utilized the backdoor to compromise the organization's assets, both in the cloud and on premise, enabling them to spy on the organization and access its data.

COLONIAL PIPELINE ATTACK

In May 2021 a major US fuel company fell victim to a ransomware attack which led to its entire fuel distribution pipeline being shutdown while it investigated the problem, causing shortages across the East Coast of the United States and influencing oil prices globally.

THE KASEYA INCIDENT – COMBINING SUPPLY-CHAIN AND RANSOMWARE EXPLOITS

Occurring over the US Independence Day weekend, the attack on IT management software firm, Kaseya, combined two of 2021's most notorious cyber attack trends—supply chain attacks and ransomware. At least **1,000** businesses are said to have been affected by the attack, with victims identified in at least 17 countries.

PREDICTIONS FOR H2 2021

Ransomware will grow, despite law enforcement stepping up. Increased use of penetration tools to give live hackers ability to customize attacks on the fly and a trend towards collateral damage well beyond the initial target victim calls for a collateral damage strategy.

TRIPLE EXTORTION RANSOMWARE— THE THIRD-PARTY THREAT

The double extortion strategy in ransomware is now well-established: threat actors steal data from organizations in addition to encrypting the files. It was extremely successful throughout 2020. While not all incidents and their outcomes are disclosed and published, statistics collected during 2020-2021 reflect the prominence of this attack vector. The average ransom payment increased by 171% during the past year, and is now approximately $310,000. Over 1,000 companies suffered data leakage after not giving in to ransomware demands during 2020, and approximately 40% of all newly discovered ransomware families incorporated data exfiltration into their attack process. It is daunting that attackers are still seeking methods to improve their ransom payment statistics, and their threat efficiency.

However, prominent attacks that took place at the end of 2020 and the beginning of 2021 point to a new attack chain which is essentially an expansion of the double extortion ransomware technique, integrating a third, unique threat to the process—we call it Triple Extortion.

The first notable case was the Vastaamo clinic attack, which took place in October 2020. In this innovative attack, the 40,000-patient Finnish psychotherapy clinic suffered a year-long breach that culminated in extensive patient data theft and a ransomware attack. In addition to the ransom demanded from the healthcare provider, the attackers sent smaller ransom demands by email to individual patients. In those emails, the attackers threatened to publish their therapist session notes. For a short while though, it seemed like an outlier within the cyber landscape.

In April 2021, REvil demonstrated another implementation of the technique. The attackers successfully breached Quanta Computer, a prominent Taiwan-based notebook original design manufacturer (ODM) and a business partner to Apple. The company is involved in manufacturing Apple Watch, Apple Macbook Pro, and more. Following the ransomware attack, a payment of approximately

50 million US dollars was demanded from Quanta, along with a warning that the sum would be doubled unless paid on time. Quanta refused to communicate with the threat actors, who then went on to extort Apple directly, requesting Apple pay to "buy back" blueprints of their products found on Quanta's network. Approximately one week later, REvil removed Apple's drawings from their official data leak website, leading to speculation that the ransom was paid.

On a wider scale, the REvil ransomware group, which operates in a Ransomware-as-a-Service business model, announced in March 2021 that they added two more stages to their double extortion scheme: distributed denial-of-service (DDoS) attacks, and phone calls to the victim's business partners and the media. The group now offers its affiliates a free service of DDoS attacks and voice-scrambled voice-over-IP (VoIP) calls to journalists and colleagues, with the aim of applying further pressure on the victim company to meet the ransom demands within the designated timeframe. Ransomware attacks have increased by 93% in 2021 with notable examples including Colonial Pipeline attacked by DarkSide and both JBS Foods and Kaseya targeted by REvil. In fact, the attack on IT management software company Kaseya was the biggest supply chain attack to happen since SolarWinds.

Clop ransomware, which wreaked havoc in Europe and the Americas since it first emerged in March 2020, has not lagged behind—and adopted this trending triple extortion tactic as well. In April 2021, customers of RaceTrac Petroleum, a gas station chain with 650 branches in south east USA, received emails from the Clop gang—encouraging them to convince RaceTrac Petroleum to pay the ransom and threatening to leak their personal data, which was found in RaceTrac Petroleum's network, to a "name-and-shame" darknet website if they didn't comply. And they weren't alone; the same tactic was also reported in a chain of attacks on US universities.

When analyzing the triple extortion technique, certain questions arise. Can customers call on the targeted company, whose actions led to the exposure of their data, to pay the ransom demanded from them individually? Can business partners claim the same? What happens if customers receive extortion emails prior to learning that a breach occurred? Can they demand that the company pay the entire ransom?

It appears that the business development of ransomware pushes the cybercrime groups involved to constantly find more innovative and fruitful models. Third-party victims, such as a targeted company's clients, external colleagues and service providers, are heavily affected by data breaches caused by these ransomware attacks, even if their network resources remain unscathed. Whether a further ransom is demanded from them or not, they have a lot to lose should the ransom incident take a wrong turn. Third-parties make a natural target for extortion, and may continue to be on ransomware groups' radars from this point on.

Ransomware attacks surged 93% in the last 6 months, fueled by innovation in attack technique called Triple Extortion. Every week, more than 1,200 organizations worldwide fall victim to a ransomware attack, and all enterprises are at risk.

SOLARWINDS AND WILDFIRES

Several major events in the final months of last year marked the entrance of new, innovative approaches to network and cloud attacks and introduced us to some sophisticated offensive techniques. The first event was the well-known SolarWinds supply-chain attack. Already thoroughly discussed and analyzed, the SolarWinds incident stands out due to its scale and influence. Approximately 18,000 customers downloaded the compromised Orion software update, including 425 companies on the Fortune 500 list. Due to its innovative attack vector, in which access to Office365 resources was achieved via on-premise servers and the use of forged tokens to move laterally within cloud environments, the attackers were able to proceed without raising red flags.

Sophisticated software supply-chain attacks occurred in the first half of 2021 as well. Codecov, one the world's leading code coverage services which is responsible for optimizing the code delivered by thousands of companies, suffered a security incident which allowed an unauthorized modification of the official Codecov's Bash Uploader script. During the several time-frames of compromise, any customer who used Codecov's Bash Uploader script was unknowingly uploading their development environment's data to a server controlled by the attacker. In this attack scenario, sensitive information, which is often stored in a development environment (or CI/CD), such as tokens or secret keys to various services, was sent to the attacker. As a result, hundreds of companies are reported to have uploaded sensitive data to the attacker's

With supply chain attacks piquing Check Point Researchers' (CPR) interests, in June they decided to take a look at Atlassian, a platform used by 180,000 customers worldwide to engineer software and manage projects. CPR identified security flaws that would have allowed an attacker to get access to the Atlassian Jira bug system, with just one click, and get sensitive information, such as security issues on Atlassian cloud, Bitbucket and on premise products.

server, and several of the affected companies already reported a breach in their own network as a direct result of the Codecov incident. The affected companies included Monday.com, Twilio, Rapid7 and more.

Other events have also showcased examples of advanced persistent threat (APT) groups leveraging sophisticated attacks for mass-compromise operations. The first was fueled by the exposure of a vulnerability known as ProxyLogon, together with three other zero-day vulnerabilities in Microsoft Exchange on-premise servers. When combined together, they allowed for Remote Code Execution (RCE) on any mainstream Exchange server. The flaws were originally revealed in late 2020, but it wasn't until March 2021 that a global attack wave exploiting these flaws was observed worldwide. Microsoft subsequently released critical security updates for four of the flaws, but in the meantime, hundreds of thousands of companies were impacted by the vulnerabilities worldwide, among them at least 30,000 US organizations. More than 10 APT groups leveraged the ProxyLogon flaw, including Hafnium, a Chinese-affiliated group with an established focus on Office 365 resources and an interest in medical research facilities, law firms, education institutes, and more. Another large-scale campaign distributed the DearCry ransomware.

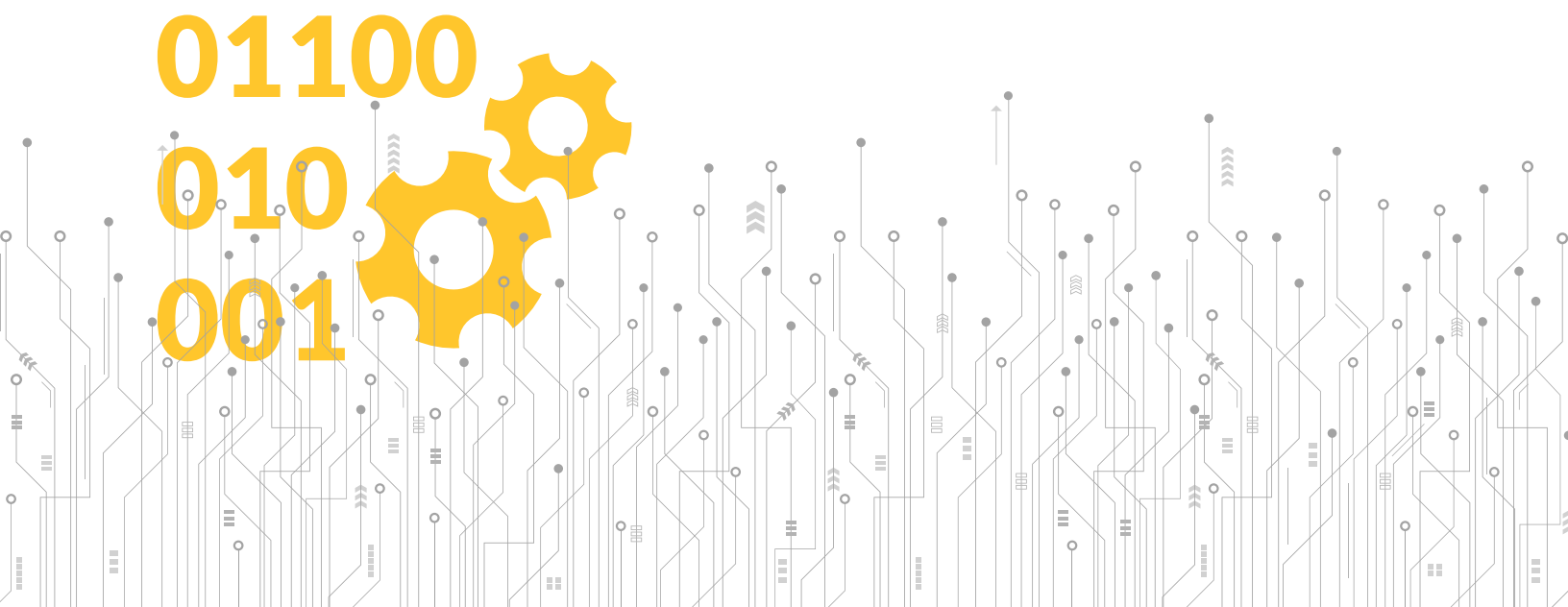
Before the ProxyLogon storm faded from the public view, another large scale attack started making headlines. Accellion, a secure file sharing company, patched a zero-day vulnerability in its File Transfer Appliance (FTA) in December 2020. Accellion's FTA is a 20-year-old legacy product still in broad use. Even though one of the flaws was patched, in January 2021, a ransomware double extortion attack campaign began exploiting them to

access Accellion customers worldwide, among them, telecom giant Singtel. Researchers linked the attacks to a set of threat groups tied to FIN11 and the Clop ransomware gang, after victims began receiving emails demanding a ransom payment and threatening to release their stolen data on Clop's leaks webpage. The Accellion breach alone, which peaked in February, led to an increase in the average ransom payment in the first quarter of 2021.

These large-scale attacks share some basic similarities: the products affected by the exposed flaws are highly common, are developed by top global tech brands, and are used by companies from all sectors and industries. The scale of each of these attacks is colossal, with thousands of organizations potentially affected, and hundreds of organizations actively attacked. It is therefore not surprising that the perception of supply-chain attacks among organizations has changed drastically since the start of 2021.

Companies are looking for better prevention measures to ensure they are unharmed by the next incident, and as a result, the way they integrate, or at an earlier stage, inspect third-party products, is rapidly evolving. We can now expect to see new third-party product evaluation procedures spreading among companies.

From the opposite perspective, service providers, even small-scale ones providing level-one tech support, may become lucrative targets without even realizing it, let alone taking the time to set up adequate security measures to protect their clients. Such companies might believe that they would not be targeted as they don't have sensitive data of their own. However, today's targets are not selected solely based on their resources, but may be selected based on their network connections. In the wake of these events, organizations must adopt adequate security measures, including carefully constructing network connection to third-party components, and patching zero-day flaws as quickly as possible.



THE FALL OF AN EMPIRE— EMOTET'S FALL AND SUCCESSORS

A lot has been written about Emotet in the past few years. This malware debuted in 2014 as an elite banking malware targeting European banking users, and was the top most-distributed botnet in 2019 and 2020, after a years-long evolution into a large-scale botnet with over one million bots at its disposal. Emotet was also involved in the distribution of the most prominent malware at any given moment, including Qbot and TrickBot banking Trojans. According to Check Point Research statistics, the botnet was ranked number one in the global top most-distributed malware lists throughout 2020, with 9% of mentions in the mid-year statistics and 19% of organizations globally in 2020 affected by its infection attempts.

Emotet ceased its attack activities for a five-month period between February and July 2020, yet was still able to surpass all other malware families in terms of global reach.

As early as January 27, 2021, however, Emotet's fortunes took a sharp downward turn as a global operation conducted by law enforcement and judicial authorities worldwide disrupted the botnet's activities and attempted to take control of its infrastructure. Emotet's botnet featured hundreds of servers worldwide with varied functionalities and was used to create new bots, manage infected devices, develop new distribution techniques, drop malware as-a-service and provide additional services to threat groups. The primary success of the multi-stage takedown operation was gaining control over the botnet servers and redirecting active bots to servers controlled by the authorities, using a specially-crafted Emotet module deployed to all victims. In the second phase, which took place on April 25, the new Emotet module initiated a scheduled self-destruct sequence, which then uninstalled Emotet from the infected machines.

MONTHLY EMOTET RELATED MALICIOUS EVENTS

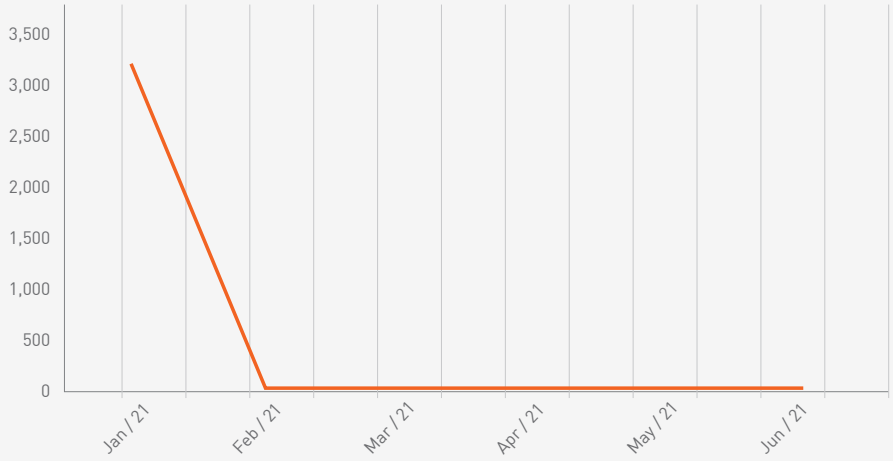


Figure 1: Extension of Emotet botnet distribution since February 2021

In recent years, Emotet has played a crucial role in the global threat landscape, both in large-scale distributed attacks and manually-operated targeted corporate attacks. The botnet, with its quality business model, functioned as the first-phase malware, gaining the initial foothold into the organization, in many cases via an email campaign, and dropping an additional payload of the client's choice. Emotet stood out in the botnet arena due to its modular ecosystem, which includes multiple modules with a wide range of capabilities such as downloading malware, harvesting Outlook email, and self-propagating between machines on the same network.

To measure the success of the takedown operation, Check Point Research examined Emotet's distribution rate throughout the first half of 2021, as well as the distribution of its prospective successors. In February 2021, the first month after the shutdown operation, Emotet fell from the top 10 global most wanted malware ranking. Its place at the top was inherited by one of its potential successors, Trickbot, a botnet and banking malware with enhanced information stealing capabilities. Trickbot was the fourth most prevalent malware globally during 2020, impacting 8% of organizations.

Due to its scale, presence and possibly its former collaboration with Emotet, Trickbot is probably the most prominent successor on the list. Similar to Emotet, Trickbot comprises an estimated one million bots. Unlike Emotet, Trickbot successfully survived a well-planned takedown attempt, led by Microsoft, that took place in October 2020.

The Trickbot botnet was also perceived as a vital threat to the 2020 US presidential elections.

In the preceding months, Dridex, another prominent banker-turned-botnet, made headlines with large-scale campaigns. In March 2021, Dridex made the highest amount of attack attempts against organizations worldwide. The malware first rose to prominence in 2015 as banking trojan, and is characterized by its multi-module structure. The modules are responsible for information theft, ransomware deployment and incorporating an infected machine into a botnet. Other prominent malwares taking over Emotet's turf include Qbot and IcedID. Qbot was already known as a prominent malware, and as a botnet, utilized Emotet's novel phishing technique 'thread hijacking' since July 2020. IcedID, a banking malware, was first revealed in 2017, and was ranked the second-most prominent malware in March 2021. The banker targets banks, credit card companies, payroll services and e-commerce websites primarily in the Americas region.

Trickbot, Dridex, Qbot and IcedID all show signs of continuing to increase in prominence over the next few months. Together, they make up for the loss of Emotet and keep the ransomware distribution rates steady. These malwares resemble Emotet in their infection tactics as well, not only in the adoption of 'thread hijacking' by Qbot. They also use phishing campaigns to distribute documents, mostly Microsoft Office files, which contain malicious macros. We can expect all of these malware families to continue stepping up and improving their distribution techniques, business models and, of course, detection evasion mechanisms.

MOBILE ARENA DEVELOPMENTS

The prominence of mobile devices within the threat landscape continues to grow over time as our personal devices become a more integral part of our professional toolset. Corporate applications have now replaced designated corporate devices as part of the 'Bring-Your-Own-Device' (BYOD) concept, to allow for greater operational flexibility in today's hybrid work model. As a result, a greater amount of professional information is stored or accessible from personal phones. Threat actors are working tirelessly to develop new designated mobile attack techniques aimed at exfiltrating personal and corporate information from mobile phones, and leveraging these devices to obtain access to organizations' networks.

In the field of malware distribution, we saw various malware families adopt a technique that relies on instant messaging. FluBot, a rising Android malware, began spreading among European and UK users in April 2021 via SMS messages impersonating global delivery brands such as FedEx and DHL. The victim is lured to download the service's application to access the package information but the malware, capable of accessing all mobile resources and collecting credentials and bank account information, is embedded within the malicious app. In a similar attack vector, threat actors even integrated two instant messaging platforms in a single attack chain. In a recent scam, the victims received a code via an SMS message, followed by a WhatsApp message from an alleged contact which asked them to share the code, thereby granting the attacker access to the device.

Check Point Research recently uncovered a campaign that distributes an Android malware disguised as a Netflix content enabler app called 'FlixOnline', available on the Google Play Store. The wormable malware is spread via auto-replies to incoming WhatsApp messages, and is capable of extensive data theft.

Apple was in the mobile arena spotlight in the first half of 2021 with a notable increase in the exposure of system vulnerabilities. As early as January 2021, Apple published an iOS update to address three flaws that may have already been exploited in the wild. In late March, the company released an update for a zero-day vulnerability affecting iPhones, iPads and watches that may have already been leveraged for cyber-attacks as well. Finally, in early May, Apple issued an out-of-band patch for critical zero-day vulnerabilities in iPhones, among other devices, that could enable remote code execution. As with the other flaws, this may have already led to active attacks. Overall, seven zero-day vulnerabilities were exposed since the start of 2021. All of them are zero-day flaws, and were probably exploited by threat actors in-the-wild prior to their disclosure and patching.

In 2020, we saw an array of vulnerabilities in the hardware of popular vendors such as the Achilles family of vulnerabilities in Qualcomm chips. In 2021, we saw a new kind of flaw that is drawn from the general threat landscape climate, including misconfiguration of third-party cloud-based services such as real-time databases, storage, and analytic applications. Similar to network environments, third-party services are integrated into complex applications, with a direct impact on their user data security level. For example, improper authentication configuration of cloud real-time databases could easily enable unauthorized access to private customer data. Fortunately, as those are developer issues, mobile malware developers might repeat those mistakes and allow researchers to access their infrastructure.

COBALT STRIKE STANDARDIZATION

Check Point Research thoroughly discussed and analyzed the implications of the SolarWinds supply chain attack on network structure and security, as well as cloud resource management. We are certain that the incident will continue to impact the threat landscape of 2021, as detailed in a separate section in this report. However, one aspect of the attack remained outside the spotlight—how were the attackers behind one of the world's biggest breaches able to remain undetected long enough to move laterally from the on-premise network to the cloud environment and facilitate persistent access to sensitive data? How were the attackers able to remain under the radar of security admins from top technology, consultancy and government networks, such as Microsoft, Cisco, the Department of Homeland Security (DHS) and the National Institute of Health (NIH)?

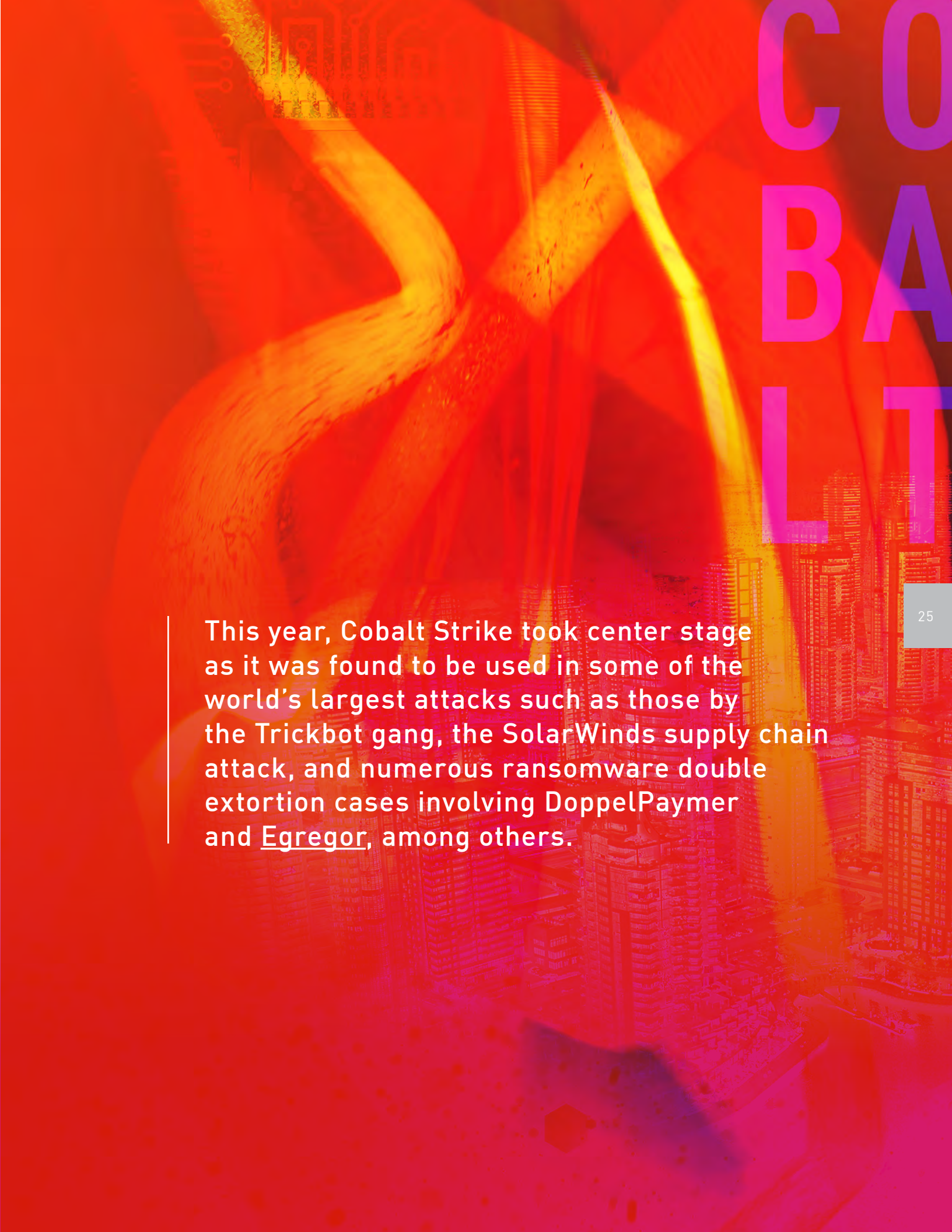
It is estimated that the Sunburst malware was deployed via the compromised Orion update starting on February 20, 2020. Furthermore, researchers recently discovered that a previously undetected piece of malware, called Sunspot, was delivered around October 2019 via an earlier test update to the platform. One of the tools that made this long-lasting breach possible is the Cobalt Strike penetration testing tool, originally developed by 'White Hat' hackers. In the past few years, the commercially available tool became a prominent member of the attack landscape, and somewhat of a post-exploitation standard.

In the SolarWinds chain, two sophisticated loaders were used to deliver Cobalt Strike beacons called Raindrop and Teardrop. The attackers attempted to separate the beacons from the Sunburst backdoor, the DLL deployed via the compromised update for initial access, to evade detection. Unique Cobalt Strike beacons, tailored to the selected victims, were then used to carry out data exfiltration operations. As the tool is commonly used by threat actors, attackers conveniently use it for a wide array of tasks, based on a preference to have it exposed instead of custom tools.

One reason Cobalt Strike beacons are popular among cybercriminals is the versatile toolkit, with its agent called 'Beacon', which provides a platform for the execution of unauthorized access, privilege escalation, code execution and data exfiltration. It is easy to modify, and custom tools as well as other commodity products, can be used to enhance the capabilities of Cobalt Strike even further. Cracked versions of the tool are widely available on underground forums, and in late 2020, the source code of the tool's version 4.0 was leaked online. In fact, researchers reported that in 2020, Cobalt Strike Server was utilized in 13.5% of all malicious C&C servers online.

Cobalt Strike was observed in campaigns of some of the top most popular threat groups of recent years, for both financial and espionage motives. This includes formerly prominent APT groups Cozy Bear, Carbanak, Hancitor group as well as highly influential botnets such as the Emotet runner-up Trickbot. Trickbot has been dropping Cobalt Strike, as a tool for reconnaissance and lateral movement, since at least 2019. In 2020, Trickbot leveraged Cobalt Strike to deploy the Anchor malware and the notorious ransomware Ryuk. Bazar, an additional malware linked to Trickbot, also often distributes Cobalt Strike instead of its tailored malware loader. Qbot also utilizes the tool as one of its plugins after the primary infection phase. Recently, prominent ransomware DoppelPaymer used multiple Cobalt Strike beacons extensively, in a campaign involving Dridex as the initial malware. The beacons are also used for various activities such as data exfiltration, lateral movement and detection evasion.

Cobalt Strike beacons act as the silent partners of a vast array of cyber-attacks. After the initial infection phase, the beacons can be used for multiple purposes including gathering system information, collecting sensitive data, escalating privileges and moving laterally within the target network. The tool is both comprehensive and modular, and widely accessible in various cracked versions. The customization options make it difficult to detect and its popularity also creates attribution difficulties as attacks tend to blend in with all other Cobalt Strike attacks, making attribution to a specific threat group difficult.



This year, Cobalt Strike took center stage as it was found to be used in some of the world's largest attacks such as those by the Trickbot gang, the SolarWinds supply chain attack, and numerous ransomware double extortion cases involving DoppelPaymer and Egregor, among others.

CYBER ATTACK CATEGORIES BY REGION

GLOBAL

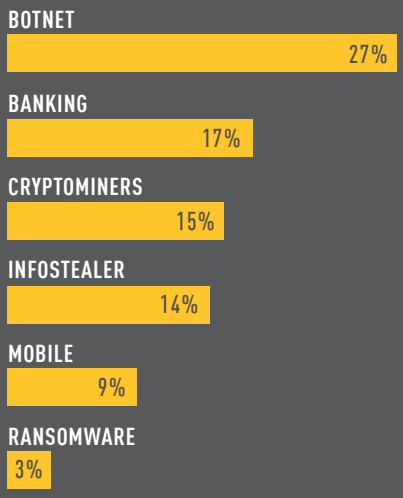


Figure 2: Percentage of corporate networks attacked by each malware type.

AMERICAS

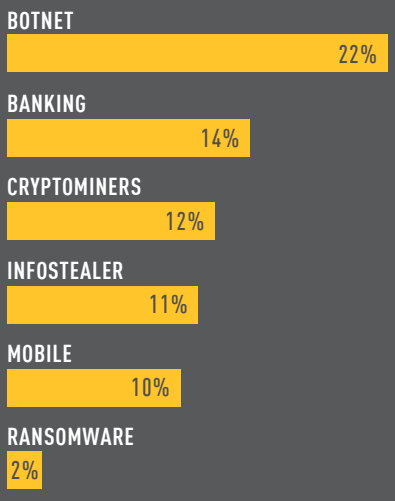


Figure 3: Percentage of corporate networks attacked by each malware type.

CYBER ATTACK CATEGORIES BY REGION

EMEA

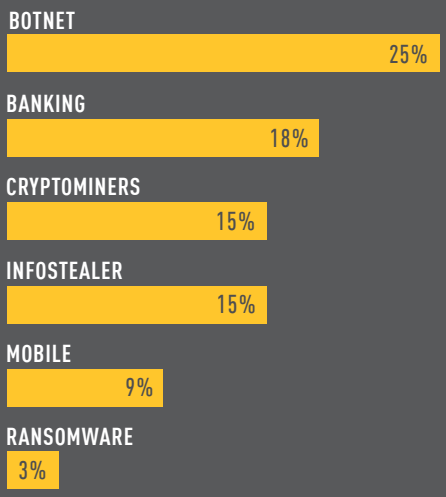


Figure 4: Percentage of corporate networks attacked by each malware type.

APAC

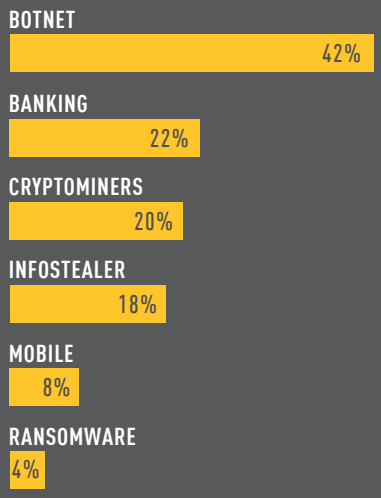
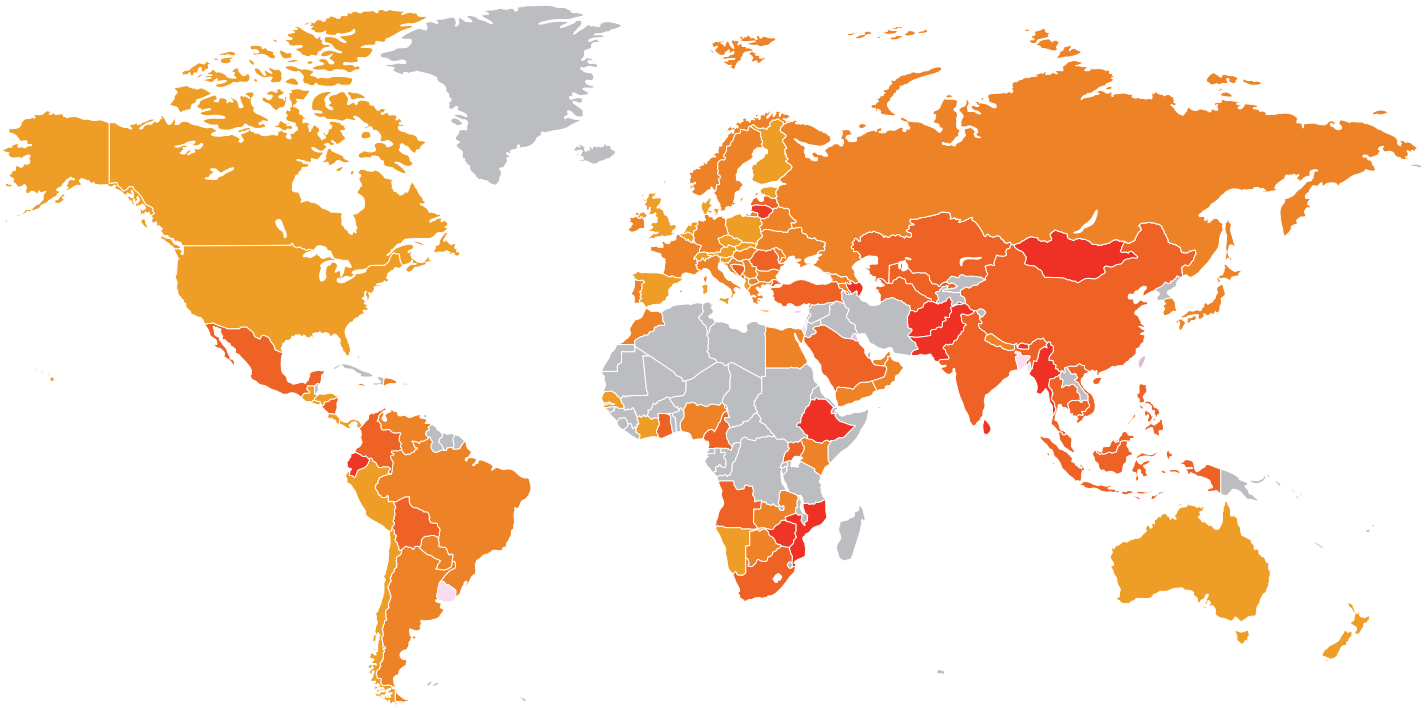


Figure 5: Percentage of corporate networks attacked by each malware type.

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. The map displays the cyber threat risk index globally, demonstrating the main risk areas around the world.



* Darker = Higher Risk
Grey = Insufficient Data

Figure 6.

TOP MALICIOUS FILE TYPES—WEB VS. EMAIL

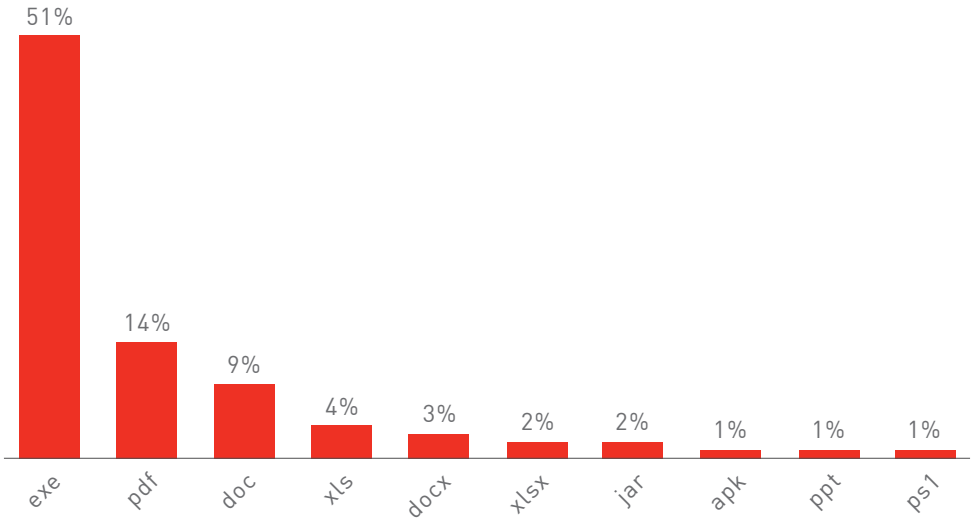


Figure 7: Web —Top Malicious File Types.

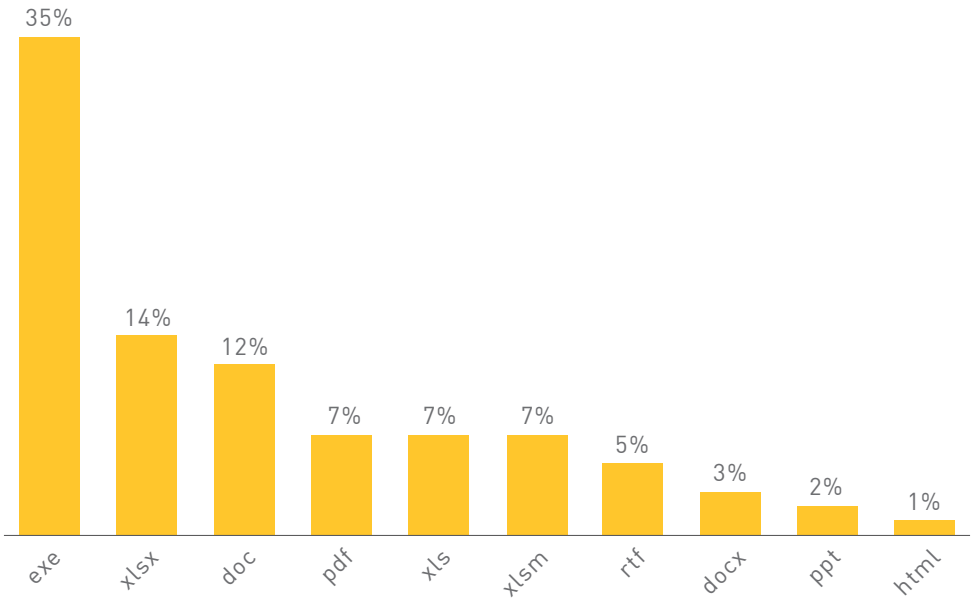


Figure 8: Email—Top Malicious File Types.

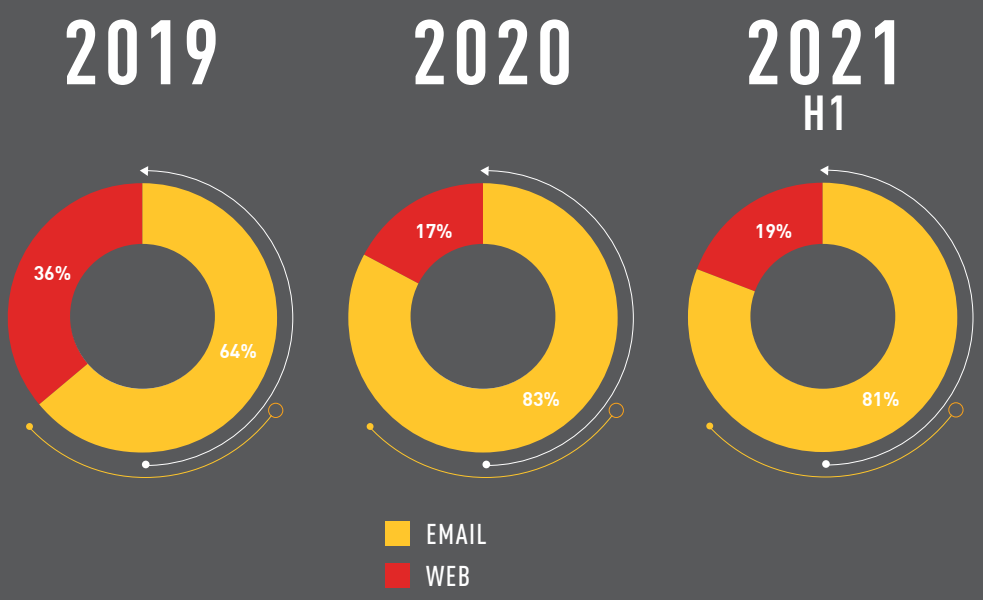


Figure 9: Distribution Protocols—Email vs. Web Attack Vectors in 2019-2021.

The chart above shows that going into 2021, email has become a favorite attack vector. Compared to the diminishing use of web downloads to distribute malware, email leads by nearly a 4 to 1 ratio. Email use had a major spike during 2020 (by almost 20%) but has been steadily increasing for the last few years, and we expect it to continue in the foreseeable future.

Whether used in a targeted attack, or "spray and pray" campaigns by a novice attacker, email-based attacks allow for an easy distribution of malware to a wide array of targets and corporations.

One of the reasons for the rise in email-based attacks is the massive number of large-scale campaigns sponsored and run by large crime groups, who distribute the most prominent malware families today, such as Trickbot, Dridex, Qbot, IcedID, and the now defunct Emotet.

Once these groups realized the effectiveness of a spam campaign with malicious Office document attachments, they have used it almost exclusively as their main infection vector for new networks.

GLOBAL MALWARE STATISTICS

Data comparisons presented in the following sections of this report are based on data drawn from the Check Point ThreatCloud Cyber Threat Map between January and June 2021.

For each of the regions below, we present the most prevalent malware. For readablity reasons we decided not to overwhelm with decimal fractions, and yet the graphs below reflect even minor differences between the mentioned malware families.

TOP MALWARE FAMILIES

GLOBAL

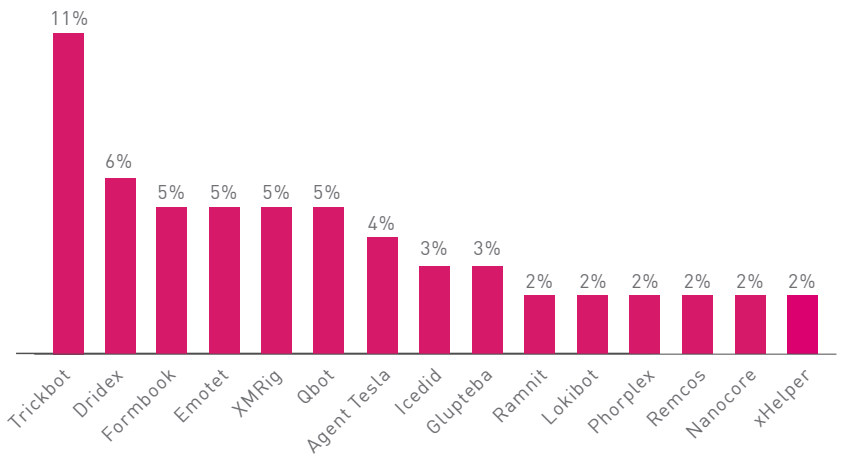


Figure 10: Most Prevalent Malware Globally.
Percentage of corporate networks impacted by each malware family.

AMERICAS

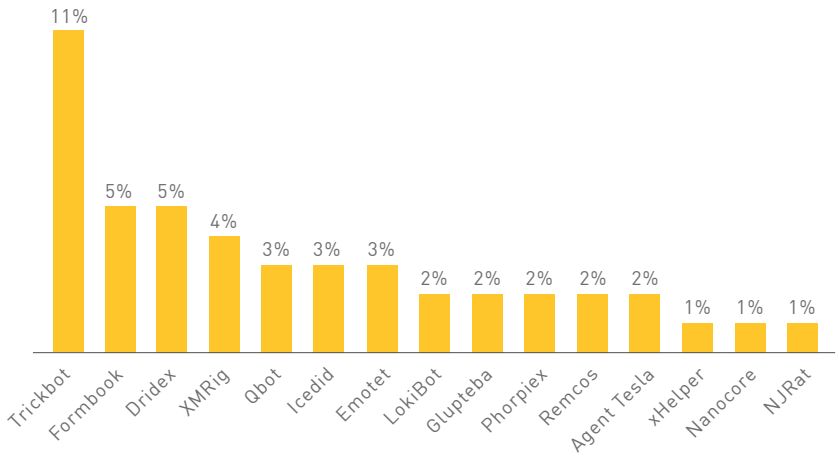


Figure 11: Most Prevalent Malware in the Americas.

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

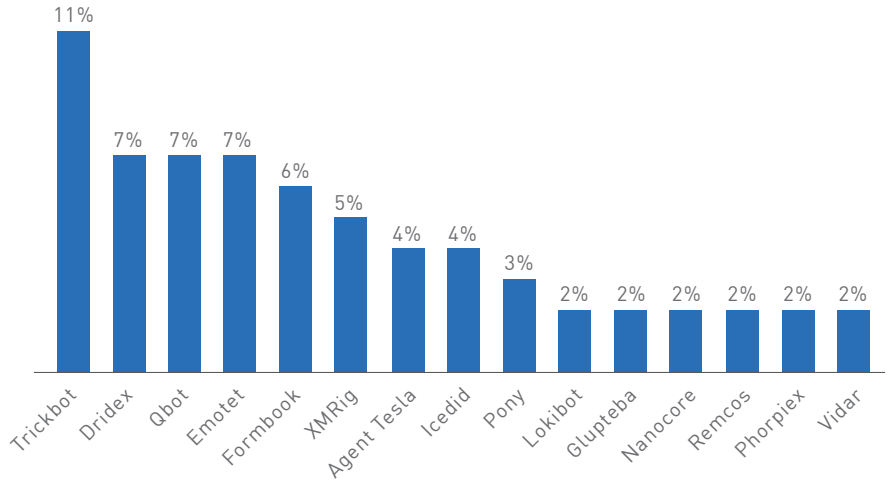


Figure 12: Most Prevalent Malware in EMEA.

ASIA PACIFIC (APAC)

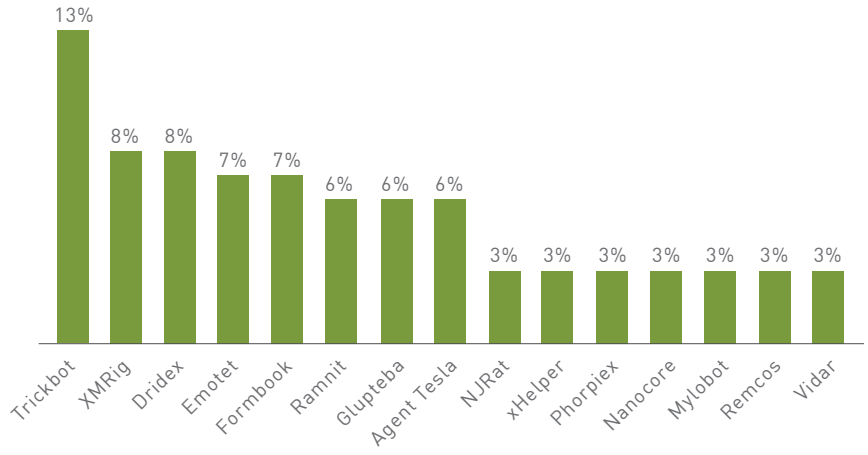


Figure 13: Most Prevalent Malware in APAC.

GLOBAL ANALYSIS OF TOP MALWARE

Not much has changed since our 2020 global malware ranking, just some slight movements up or down. However, the top 10 for the first half of 2021 is missing two whole categories of drive-by attacks, which have been with us for several years. For the first time since Coinhive premiered in the top charts, we no longer have a drive-by crypto-mining service in our top malware ranks. This is due to the decline in profitability of drive-by cryptomining, as well as last year's shutdown of JSECoin. Second, RigEK, one of the longest running and successful Exploit Kit services in operation, can no longer compete with other types of attack surfaces, and dropped from our top global charts as well.

Emotet, a botnet responsible for the distribution of Trickbot, Qbot and more, was the most heavily distributed malware family in 2019 and 2020. With its shutdown in January 2021 after a global law enforcement operation, one might not expect it to feature in our top malware families category for H1. However, during its 27 days of operation in January, Emotet was still able to reach the fourth place in our global ranking, a true testimony to the scale of this long-running operation.

In the rising malware category, the most notable addition to our top 10 ranks is the IcedID banking Trojan, which also operates as a botnet and a dropper. Though available since 2017, during March and April this year, the threat group behind the malware family really stepped up its distribution with several large scale spam campaigns, putting it in the race to be one of Emotet's successors.

TOP CRYPTOMINING MALWARE

GLOBAL

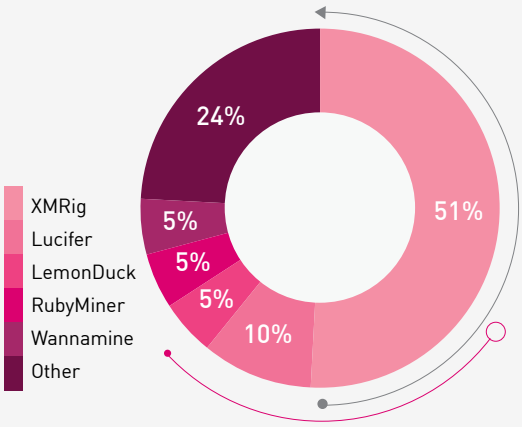


Figure 14: Top Cryptomining Malware Globally

AMERICAS

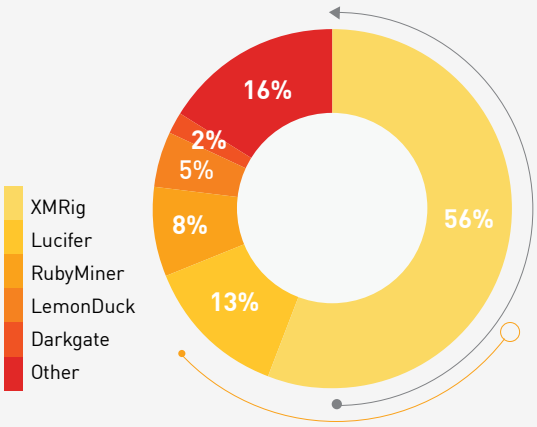


Figure 15: Top Cryptomining Malware in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

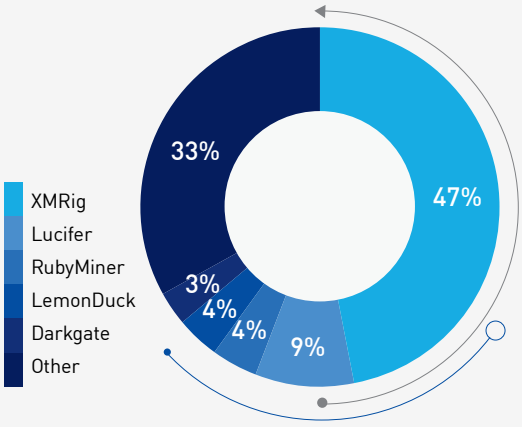


Figure 16: Top Cryptomining Malware in EMEA

ASIA PACIFIC (APAC)

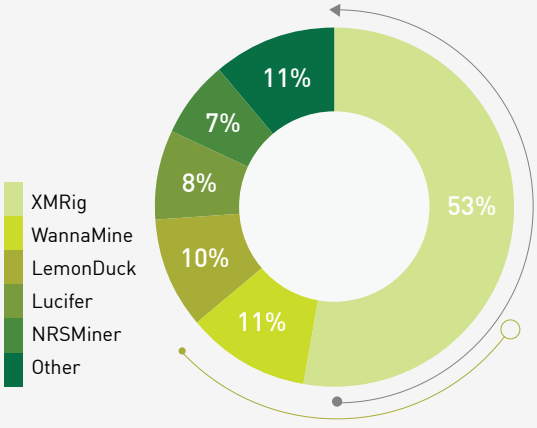


Figure 17: Top Cryptomining Malware in APAC

CRYPTOMINERS GLOBAL ANALYSIS

XMRig, originally a legitimate open-source mining tool that was leveraged by attackers for malicious purposes, continues to top the crypto-miner chart, with a 5% increase compared to last year's first half. Since 2019, we have been witnessing a steady decline in drive-by crypto-miners, which was the dominant cryptomining type in the past years. The decline, together with the diminishing value of drive-by mining profitability, was hastened by the shutdown of Coinhive in March 2019 and JSECoin in April 2020.

A rising crypto-miner making its first appearance on the chart is the LemonDuck family. LemonDuck is a self-propagating cryptomining malware that has been active since at least late 2018, targeting both Windows and Linux machines. LemonDuck utilizes XMRig for its cryptomining tasks and a large variety of techniques for propagation, from exploits like Eternal Blue and SMBGhost, to spreading via Covid-19 themed emails that are sent to the victim's Outlook contacts. During May 2021, the attackers continued to show their resourcefulness and were one of the first to exploit the ProxyLogon vulnerability to deliver LemonDuck to unpatched Exchange servers.

TOP MOBILE MALWARE

GLOBAL

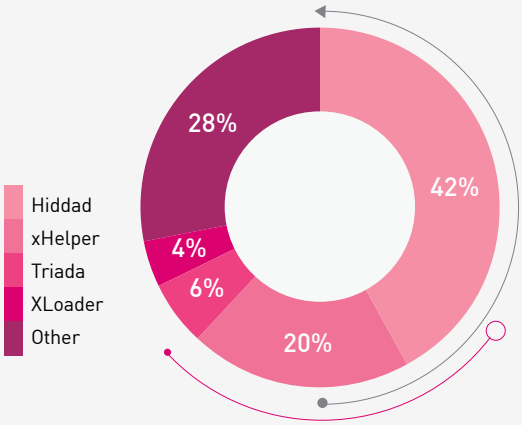


Figure 18: Top Mobile Malware Globally

AMERICAS

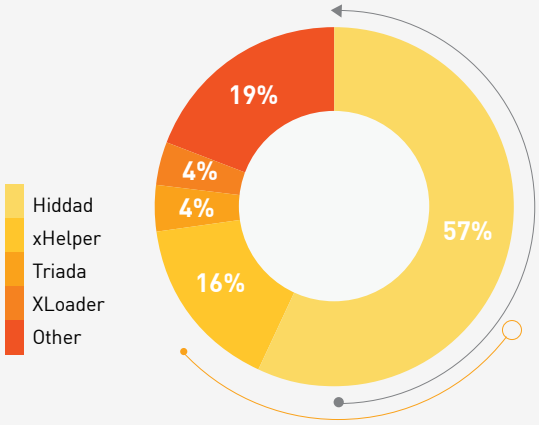


Figure 19: Top Mobile Malware in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

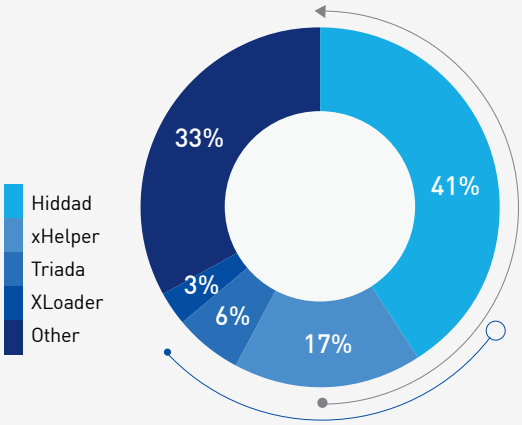


Figure 20: Top Mobile Malware in EMEA

ASIA PACIFIC (APAC)

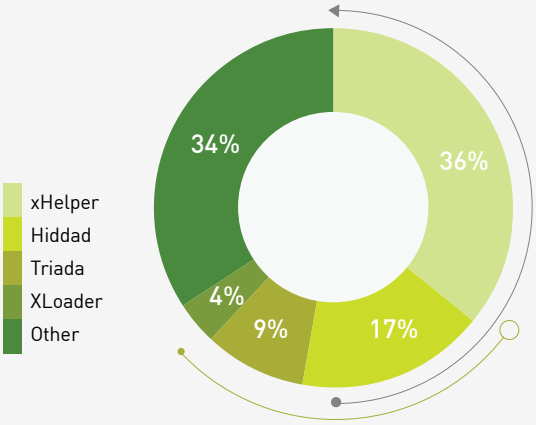


Figure 21: Top Mobile Malware in APAC

MOBILE MALWARE GLOBAL ANALYSIS

Hiddad, short for 'Hidden Ad', continues to dominate as the most prominent mobile threat. This family of Trojans is designed to display ads and collect system information, and features simple yet clever ways to keep itself on the victim's device. It hides its icon from the app launcher, and masquerades as other apps post-installation, such as Google Play Service and Google Play Store.

xHelper for Android, which first appeared in mid-2019, maintained its position in second place this year. xHelper is a mobile malware dropper which perplexed researchers when it was first discovered, as it can survive a factory reset, something which is usually successful at getting rid of any installed applications and malware. Further research showed that there was a connection between xHelper and number 3 on our list: the **Triada** backdoor. When xHelper is used to gain the initial persistence on a target, the Triada backdoor is often downloaded and executed in the later stages of the infection.

TOP BOTNETS

GLOBAL

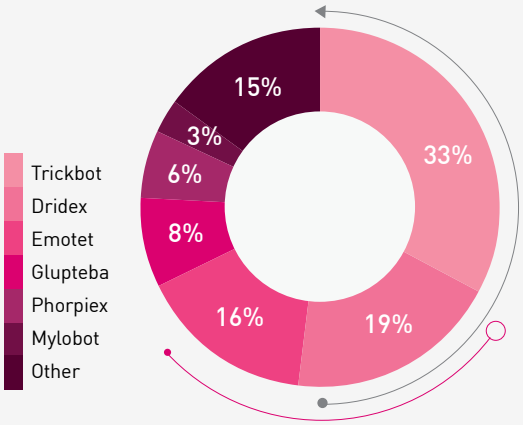


Figure 22: Most Prevalent Botnets Globally

AMERICAS

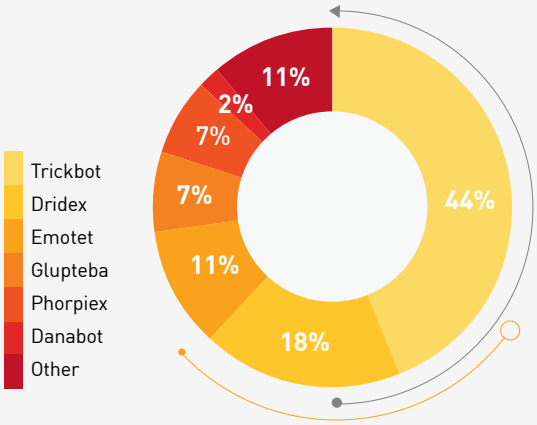


Figure 23: Most Prevalent Botnets in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

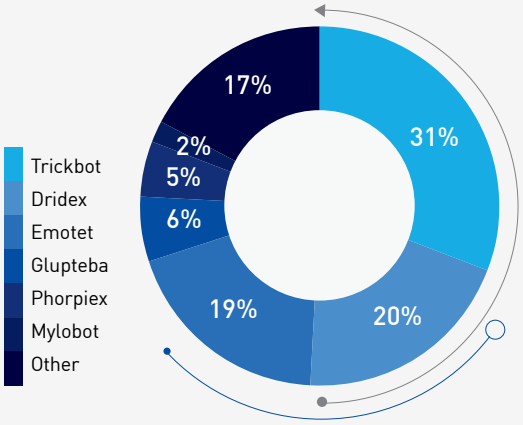


Figure 24: Most Prevalent Botnets in EMEA

ASIA PACIFIC (APAC)

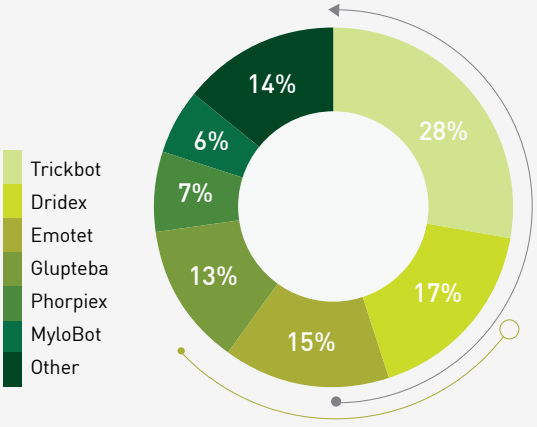


Figure 25: Most Prevalent Botnets in APAC

BOTNET GLOBAL ANALYSIS

The botnet arena remains in control of several prominent botnets, including **Emotet** and **Trickbot**, as it was last year. Emotet, third in the chart, was one of the largest PC botnet operations. It provided installation services for other attackers, and enabled backdoor access to thousands upon thousands of organizations worldwide, until it was successfully disrupted by a law enforcement operation in January 2021.

Trickbot, which started as a banking Trojan, evolved into a botnet operation, as the Trickbot gang expanded their business model with every new opportunity on the market, from cryptocurrency mining, to selling access to corporate networks. Trickbot, like Emotet, experienced a takedown attempt last year, but unlike Emotet, it managed to survive, and has now become one of Emotet's probable successors at the top of the botnet charts. While Emotet was one of the major Trickbot distributers, luckily for the Trickbot operators, they were never entirely reliant on Emotet's installation services alone, and had additional spam operations for its distribution. Today, Trickbot leads the way for destructive cyber operations, by either providing services for other threat actors using their Anchor module, or by delivering devastating double extortion attacks via Ryuk and Conti ransomware.

TOP INFOSTEALER MALWARE

GLOBAL

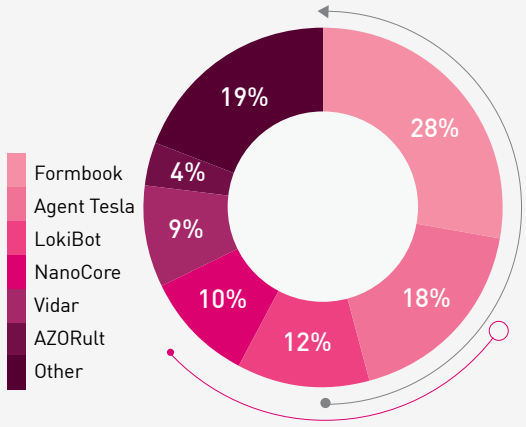


Figure 26: Top Infostealer Malware Globally

AMERICAS

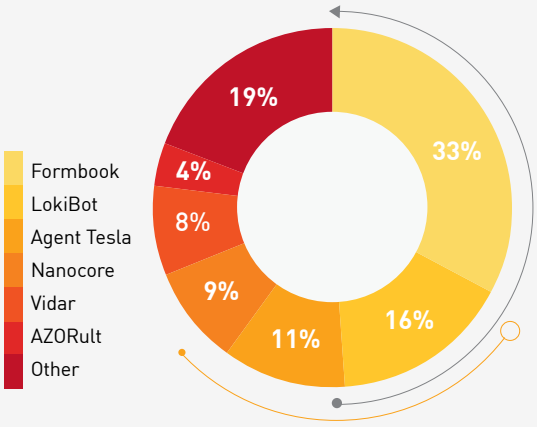


Figure 27: Top Infostealer Malware in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

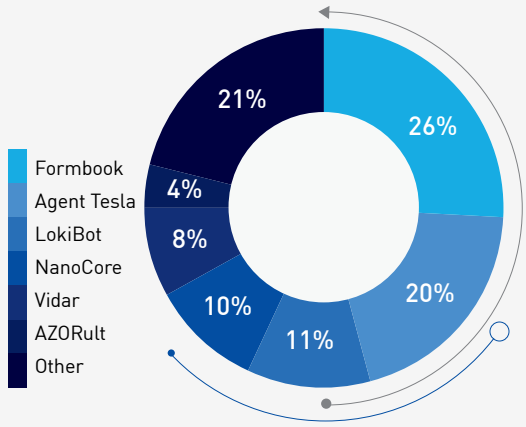


Figure 28: Top Infostealer Malware in EMEA

ASIA PACIFIC (APAC)

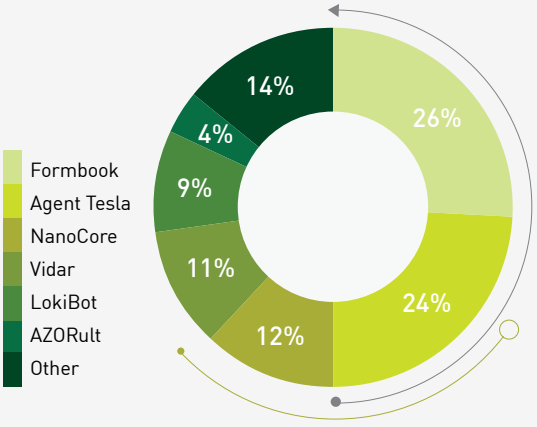


Figure 29: Top Infostealer Malware in APAC

INFOSTEALER MALWARE GLOBAL ANALYSIS

The infostealer top ranks did not see significant changes in the last year. The infostealer arena continues to be dominated by three prominent commodity malware families: **Formbook**, **Lokibot** and **Agent Tesla**.

These commodity malware families are available for purchase and/or download, whether as Malware-as-a-Service (MaaS) or in the form of free cracked malware distributed in underground forums. The availability and ease of use allow the malware to be operated by attackers with lesser technical skills, and the malware is often observed in both spearphishing and large-scale spam campaigns.

While each infostealer is unique, most share the same core capabilities which allow the attacker to easily control the target device and intercept important data. The capabilities often include keylogging, taking screenshots, file theft, and harvesting credentials from popular applications.

TOP BANKING TROJANS

GLOBAL

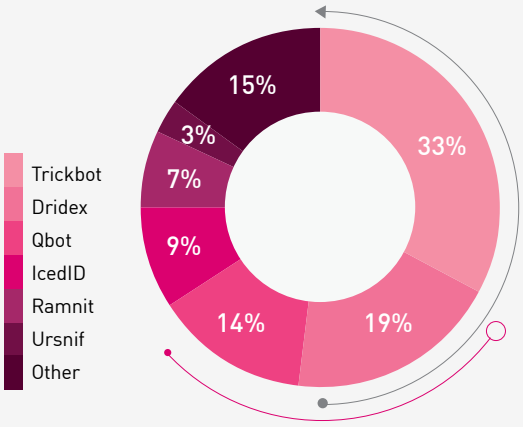


Figure 30: Most Prevalent Banking Trojans Globally

AMERICAS

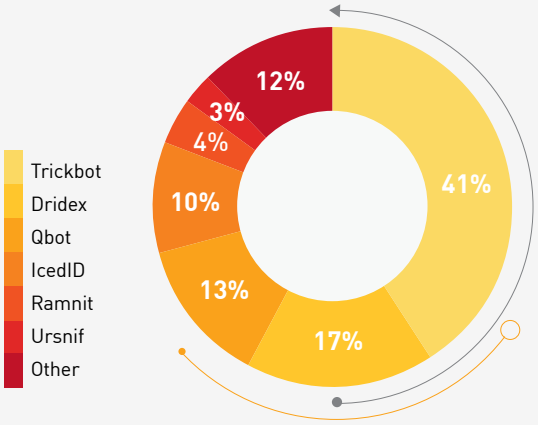


Figure 31: Top Most Prevalent Banking Trojans in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

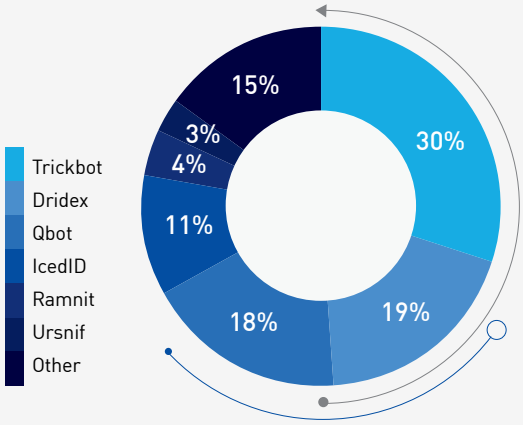


Figure 32: Most Prevalent Banking Trojans in EMEA

ASIA PACIFIC (APAC)

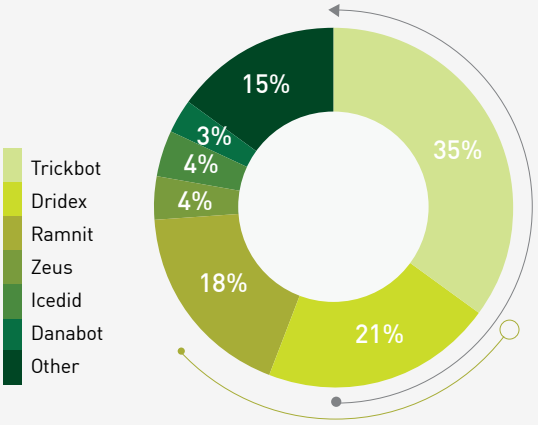


Figure 33: Most Prevalent Banking Trojans in APAC

BANKING TROJAN GLOBAL ANALYSIS

In the past few years, we have seen a steady trend of banking Trojan operators shifting their business models from vanilla banking Trojan operations to newer ventures. They no longer settle for the profits that can be made from transferring relatively small sums of money from a compromised bank account. Instead, they now try to monetize every machine and network they compromise. Our top four banking Trojans, **Trickbot**, **Dridex**, **Qbot** and **IcedID**, are all proof of this constant evolution. These banking-Trojans-turned-botnets have become major platforms for launching devastating ransomware and double extortion attacks, which are much more profitable. They also make it easier to execute cyber-attacks, compared to the complex operations required by banking Trojan operations, which often involve additional steps of covert money transfers.

Ursnif (aka Gozi), is one of the last true banking Trojans in our top ranks. Unlike most of the other banking Trojans, Ursnif is a product of a leaked source code, followed by numerous versions and code forks. As a result, it is operated behind the scenes by several threat actors, all whom continue to develop their versions even further, each with a different focus and geographical targeting.

In the past year, Italy became one of the main subjects of such targeted, geofenced Ursnif attacks. Spam campaigns delivering malicious documents are the first stage of the attack, using various themes ranging from economic support campaigns, to parcel shipping information and Social Security information campaigns. The success of these operations was recently showcased when security researchers located a database full of stolen credentials and banking information belonging to 1700 victims from over 100 Italian banks, all of which were stolen with the help of the Ursnif banking Trojan.

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 2021.

DRAYTEK VIGOR COMMAND INJECTION (CVE-2020-8515)

Draytek is a Taiwan-based manufacturer of networking equipment and management systems such as firewalls, VPN devices, and routers. Draytek Vigor is a series of VPN routers designed to build site-to-site VPN with other routers and fit into an organization's network infrastructure. In January 2020, the Draytek Vigor router product line was found to be vulnerable to a critical remote code execution vulnerability that allows an unauthenticated attacker to execute arbitrary code as root via shell metacharacters. This high-profile vulnerability was listed in the NSA's top 25 vulnerabilities exploited in the wild by Chinese state-sponsored threat actors during 2020. This year, it was one of the most heavily leveraged vulnerabilities by cyber attackers. According to Check Point Research, approximately 30% of organizations were affected by exploitation attempts of the Draytek Vigor vulnerability in the first half of 2021.

PROXYLOGON—MICROSOFT EXCHANGE SERVER AUTHENTICATION BYPASS (CVE-2021-26855)

ProxyLogon is the name given by researchers from DEVCORE to an authentication bypass vulnerability (CVE-2021-26855) they first discovered and reported in late 2020. When chained together with other vulnerabilities (CVE-2021-26857, CVE-2021-26858, CVE-2021-27065), this infection chain can lead to remote code execution on any unpatched mainstream Exchange Server.

During March 2021, researchers discovered that this vulnerability had already been used in-the-wild as a zero-day since at least January 2021, by a Chinese based threat group named HAFNIUM.

Microsoft subsequently released critical security updates for all four flaws, but in the meantime, hundreds of thousands of companies worldwide were impacted by the vulnerabilities, including at least 30,000 US organizations. This triggered a race between sysadmins' global patching frenzy and various threat groups, including financially motivated ones, deploying Black Kingdom and DearCry ransomware families on unpatched servers.

F5 BIG-IP iCONTROL UNAUTHENTICATED REMOTE COMMAND EXECUTION VULNERABILITY (CVE-2021-22986)

F5's BIG-IP is a popular multi-purpose networking device designed around application availability, access control, and security solutions. In May of this year, a critical flaw was discovered in BIG-IP's iControl REST API which allows attackers to execute arbitrary system commands, create or delete files, and disable services. Researchers were quick to release POC codes demonstrating the vulnerability, as well as a Metasploit exploitation module. Various attackers quickly adapted, including integrating their malware into the Mirai botnet variant that scans the internet for vulnerable devices. According to Shodan and BinaryEdge, at least ten thousand such F5 devices were exposed at the time the vulnerability was disclosed.

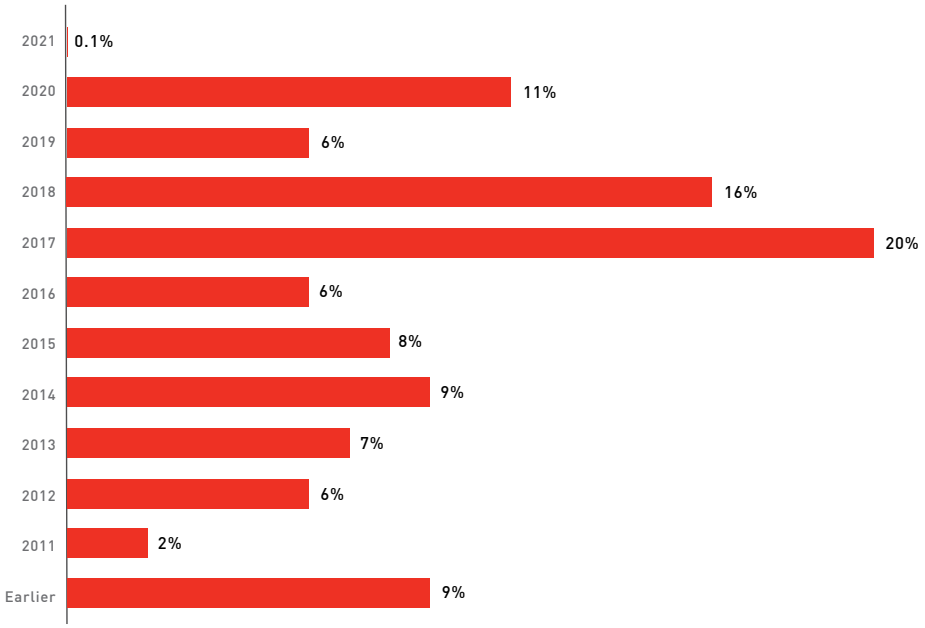


Figure 32: Percentage of Attacks Leveraging Vulnerabilities by Disclosure Year in 2021 H1.

In the first half of 2021, the exploitation of vulnerabilities that were first discovered in 2020 rose to 11%, compared to 5% last year, showing increasing adoption. Approximately 67% of all exploitation attempts utilized exploits from 2017 and earlier. The most prominent year of origin for vulnerabilities, in which 20% of the vulnerabilities exploited this year were revealed, is 2017. This leads us to conclude that exploits are not aging but rather remain effective or die. While many exploits are developed by skilled actors or threat groups for personal use, the most heavily exploited vulnerabilities are the ones who have easily available POC codes or were integrated into botnets or popular toolkits.

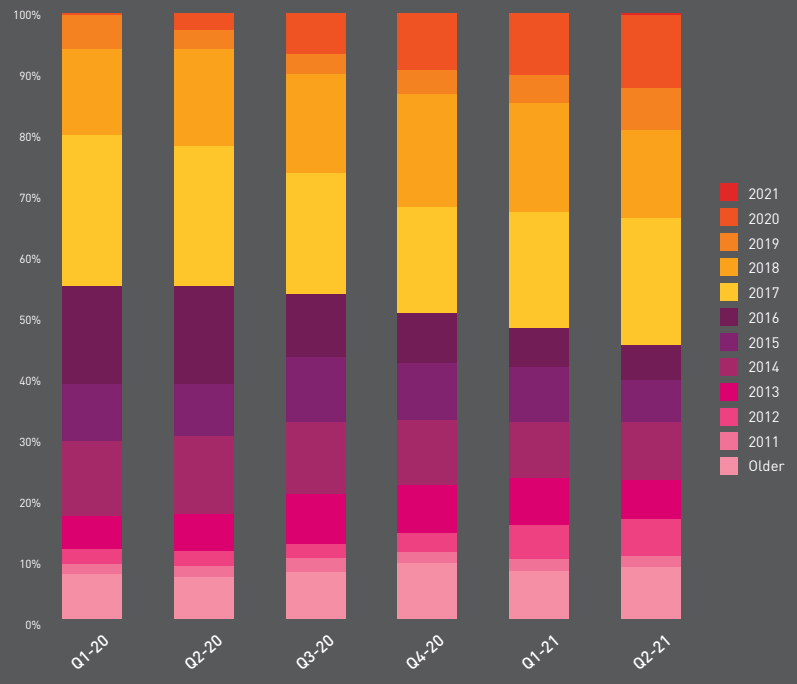


Figure 35: Percentage of Attacks Leveraging Vulnerabilities by Disclosure Year per Quarter.

The chart above shows the integration of new vulnerabilities in exploit chains during the year, and reveals how CVEs from 2020 were increasingly exploited by attackers throughout the last year and a half, ultimately comprising 12% of all exploited vulnerabilities.

MAJOR CYBER BREACHES (H1 2021)

In the first half of 2021, 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

- Microsoft internal investigation of the recent SolarWinds supply-chain attack revealed that the threat actors managed to move laterally in their network and gain access to Microsoft source-code repositories. The US Department of Justice confirmed that it had been affected by the Solarwinds supply-chain attack, and that 3% of its employee email boxes were accessed in order to steal sensitive data.
- Multiple source code repositories belonging to Nissan North America, comprising 20 gigabytes of data, were exposed due to a misconfigured Git server in which default credentials were not replaced. Mobile applications, internal analysis tools and NissanConnect services were among the exposed tools.
- Threat actors leaked 28 million user records from MeetMindful dating site. The data included real names, Facebook account tokens, email addresses, and geolocation information.

FEBRUARY

- UScellular, the fourth-largest wireless carrier in the United States, disclosed a data breach that led to the exposure of personal customer information. The attackers managed to gain access to the provider's CRM via phishing scams targeting several employees who were logged-in to the database.
- Hackers suspected to be of Chinese origin exploited a bug in Solarwinds to access the National Finance Center, a federal payroll agency inside the US Department of Agriculture, among other organizations. The flaw utilized by the actor is separate from the one exploited in the infamous Solarwinds supply-chain attack.
- Popular music streaming platform Spotify was hit by a credential-stuffing attack, only three months after a similar incident. The attack used stolen credentials from some 100,000 user accounts and leveraged a malicious Spotify login database.
- Threat actors gained access to the industrial control system at a US drinking water treatment facility and leveraged the software to sabotage the water treatment process and increase the amount of sodium hydroxide. According to the FBI, the attackers' vector of access is still unknown.

- Threat actors associated with Clop ransomware gang and the FIN11 group combined multiple zero-day vulnerabilities and a new web shell to breach up to 100 companies using Accellion's legacy File Transfer Appliance and steal sensitive files. Recent victims included supermarket giant Kroger and law firm Jones Day, among others.
- Kia Motors America was hit with a double-extortion ransomware attack executed by the "DoppelPaymer" group. The group demanded $20 million for a decryptor and a guarantee to not publish sensitive data.
- Sequoia Capital, one of Silicon Valley's oldest Venture Capital firms, suffered a data breach as a result of a successful phishing attack allowing an unauthorized third-party actor to access personal and financial information.

MARCH

- Cybercrime group dubbed 'Hotarus Corp' breached Ecuador's Ministry of Finance, as well as the country's largest private bank, Banco Pichincha. The group claimed they had stolen data from the bank's network, and recently posted online some 6,500 records, allegedly taken from the Ministry of Finance.
- American Telecom provider T-Mobile disclosed it suffered a breach, after multiple customers fell victim to SIM swapping attacks, in which a hacker ports the victim's number using social engineering to gain control over their account. Personal information and identification information were stolen.
- SITA, a communications and IT vendor for 90 percent of the world's airlines, was breached in a massive supply-chain attack, compromising frequent-flyer data across many carriers such as United, Singapore Airlines, Lufthansa, and more.
- Spirit Airlines suffered a data breach by "Nefilim" ransomware. A first batch of customer data was released on the dark web, exposing over 40GB of data including credit card numbers and personal information.
- CompuCom, a US managed service provider, was hit by malware, potentially DarkSide ransomware. The attack led to service outages and to customers disconnecting from the MSP's network to prevent the spread of malware.
- Qualys, a Cybersecurity firm, was the latest victim to have suffered a data breach published by Clop ransomware gang after a zero-day vulnerability in Accellion FTA server was exploited to steal hosted files.
- Security footage and live feed data of some 150,000 surveillance cameras was accessed by a hacker collective. The data was managed by Verkada, a Silicon Valley startup. Breached cameras were located in hospitals, schools, state departments and companies including Tesla and Cloudflare.
- Web shells deployed by the Black Kingdom ransomware operation group were discovered on approximately 1,500 Exchange servers vulnerable to ProxyLogon attacks, mostly in the US. In some cases, the web shells were later used to install the ransomware.

APRIL

- The Clop ransomware gang leaked personal and financial information stolen from users in Stanford Medicine, the University of California, and the University of Maryland Baltimore. The actor leveraged flaws in the Accellion File Transfer Appliance, in use by the universities for knowledge sharing.
- The U.S National Security Agency (NSA), the Cybersecurity and infrastructure security agency (CISA), and the Federal Bureau of Investigation (FBI) published a joint advisory warning that a Russia-linked APT group, APT25, is exploiting five vulnerabilities in an ongoing attack against U.S targets.

EUROPE, THE MIDDLE EAST AND AFRICA (EMEA)

JANUARY

- The European Medicines Agency (EMA), responsible for the approval of medicine for the European Union, was hacked, leading to the exposure of third-party documents related to the Covid-19 vaccines online.
- The Scottish Environment Protection Agency (SEPA), a public regulator with 1,200 employees, suffered a ransomware attack by the Conti ransomware. The attackers managed to steal company data and begun leaking information online.
- One of Germany's largest newspaper publishers, Funke Media Group, was attacked by ransomware, impacting over 6,000 laptops and thousands of additional machines. The attack halted the activities at the company's editorial offices and several printing houses.
- The CHwapi hospital in Belgium was hit by BitLocker, encrypting 40 of its servers and 100 TB of data. The attack caused the hospital to redirect patients and delay surgical procedures.

FEBRUARY

- 250 servers across the United States, United Kingdom, Lebanon, Israel and more were breached by Volatile Cedar, an APT affiliated with Lebanon. The campaign focused on vulnerable Atlassian and Oracle 10g servers and exploited an Oracle vulnerability assigned CVE-2012-3152.
- Stormshield, a French cybersecurity firm, suffered a data breach. The incident affected the firm's technical portal used for support ticket management, possibly enabling access to personal user data. The attackers managed to steal source code for Stormshield Network Security firewall software.
- Russian Internet and e-Commerce giant Yandex suffered a breach that led to the exposure of almost 5,000 customer accounts. The breach was enabled by a system admin that sold unauthorized access to customer mailboxes.
- UAE government agencies were targeted by a campaign most likely carried out by the Iranian espionage group Static Kitten. The campaign featured phishing emails using Israeli geopolitics and Ministry of Foreign Affairs references.

MARCH

- The biochemical systems at an Oxford university research lab studying the Covid-19 pandemic was breached. Clinical research was not affected by the incident. Breached systems included machines used to prepare biochemical samples, and hackers attempted to sell their access to those machines.
- Npower, a British gas and energy supplier, shut down its mobile application following a data breach that leveraged the application to steal sensitive customer information, via a credential stuffing attack.
- Maza, an elite Russian forum where reputable cybercriminals can connect to collaborate in malicious operations, was under attack, leaving members worried that their identities would be revealed.
- Ransomware groups exploited the recently revealed Microsoft Exchange server vulnerabilities to compromise Exchange servers and download a new ransomware called 'DearCry'. The Norway parliament suffered a data breach leveraging those flaws leading to data theft. Check Point Research published statistics of the exploit attempts on organizations by country and vertical.
- Several members of the German Parliament were hit by a targeted spear-phishing attack allegedly launched by the Russia-linked Ghostwriter threat group.

APRIL

- Asteelflash, a French multinational electronics manufacturing company, suffered an attack by the REvil ransomware. The company has not released an official statement yet, and the cybercrime gang is demanding a $24 million ransom.
- The Iranian threat group APT34, also dubbed 'OilRig', recently launched a new campaign according to Check Point Research. The campaign is focused on a Lebanese target and leverages an alleged job opportunity document and a new backdoor called 'SideTwist'.
- Pierre Fabre, a prominent French pharmaceutical and cosmetics company, suffered an attack by the REvil ransomware, leading to a temporary pause in all production processes. The gang demanded a $25 million ransom.
- The University of Hertfordshire, UK, suffered an attack that shut down all of its IT systems including Office 365, Teams and Zoom, local network, Wi-Fi, email, data storage, and VPN. Following the attack, all live online teaching was cancelled for 2 days.
- QNAP NAS storage devices were hit by a new strain of ransomware named "Qlocker". The malware moved all files stored on the device to password-protected 7zip archives and demanded a $550 ransom.

ASIA-PACIFIC (APAC)

JANUARY

- The Reserve Bank of New Zealand announced it suffered a breach via a third-party file sharing service used to store sensitive data. The scope of the information accessed is still being evaluated.
- Buyucoin, an Indian cryptocurrency exchange, suffered a data breach by a threat actor named ShinyHunters, known for stealing and selling website databases. The leaked data included email addresses, country, hashed passwords, mobile numbers and Google sign-in tokens for the exchange's 160,000 users.
- The Taiwanese hardware vendor QNAP warned customers of a new variant of Dovecat, a crypto-mining malware targeting Network-Attached Storage devices exposed online and using weak passwords.
- A new Android malware masqueraded as a Pakistani chat application, stealing users' personal data.

FEBRUARY

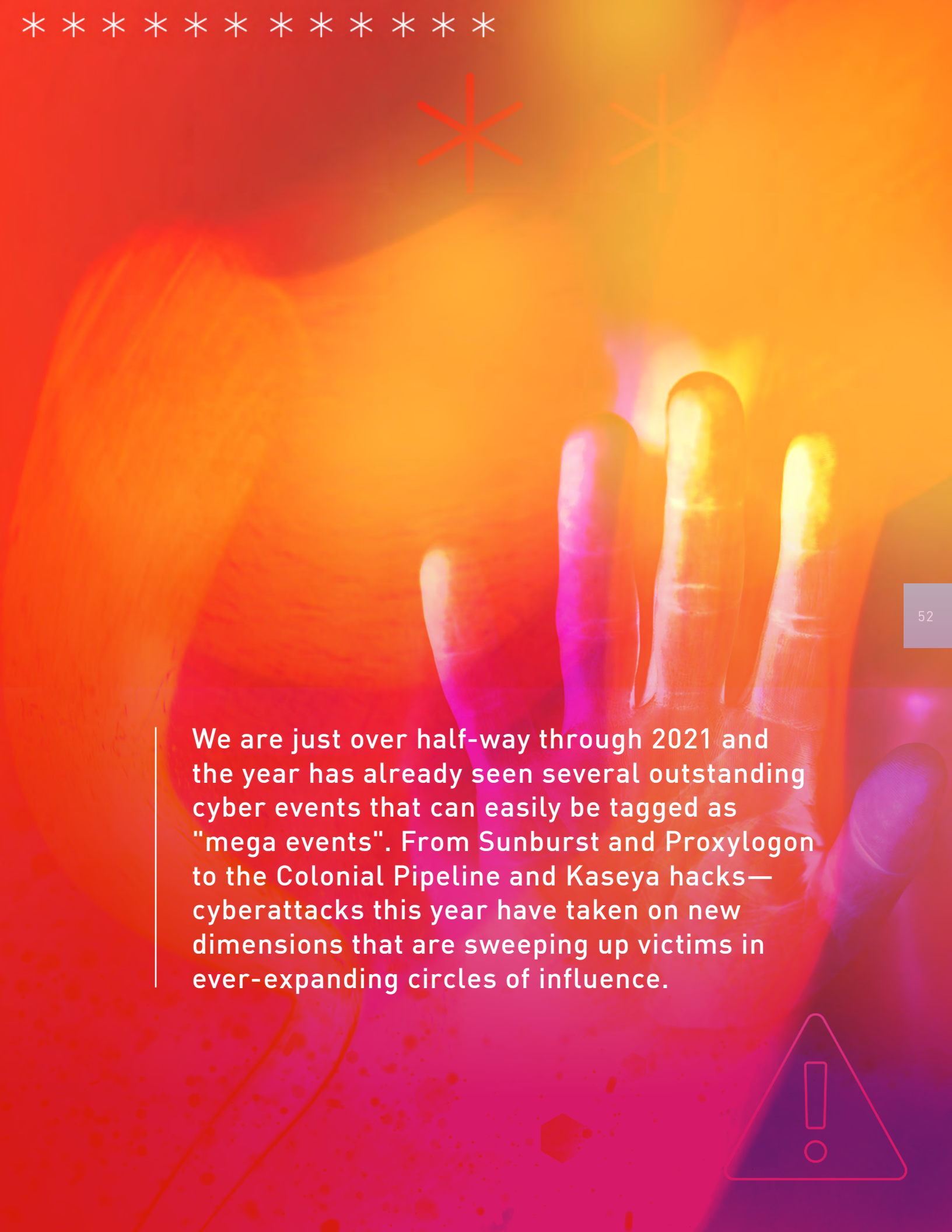
- Researchers suspected that North Korean APT Lazarus is behind a social engineering espionage campaign that was targeting security researchers. The group established several Twitter accounts posting high quality security content in order to gain credibility.
- Singaporean Telecom giant Singtel fell victim to an attack originating from a security flaw in a third-party file-transfer appliance. An Australian medical research institution also suffered a similar attack. The software leveraged for the attack is Accellion, a legacy file-transfer platform.

MARCH

- Gmail accounts of global pro-Tibet organizations were targeted by the Chinese APT TA413, an espionage group known for its operations against civil dissidents. The campaign leveraged a customized malicious Mozilla Firefox browser extension to gain control over the victims' Gmail accounts.
- Taiwanese electronics giant Acer was hit by The REvil ransomware group, demanding a 50 million USD ransom in exchange for their file recovery and data privacy.
- New espionage campaign dubbed 'Operation Diànxùn' targeted telecommunications companies in the US and India. The campaign was most likely run by the Chinese APT group 'Mustang Panda', and the primary attack vector may have been a phishing website disguised as a Huawei company career page.
- Eastern Health, one of Melbourne's largest metropolitan public health services, fell victim to a cyber attack, leaving many of its systems offline and forcing the facilities to postpone less urgent medical procedures.

APRIL

- Click Studio, an Australian software company developing the Passwordstate password manager, suffered a data breach potentially exposing its 29,000 enterprise customers. Any customer who did In-Place Upgrades within the 26-hour attack timeframe had their credentials compromised and would have needed to replace them.



We are just over half-way through 2021 and the year has already seen several outstanding cyber events that can easily be tagged as "mega events". From Sunburst and Proxylogon to the Colonial Pipeline and Kaseya hacks—cyberattacks this year have taken on new dimensions that are sweeping up victims in ever-expanding circles of influence.

H2 2021: WHAT TO EXPECT AND WHAT TO DO

We are just over half-way through 2021 and the year has already seen several outstanding cyber events that can easily be tagged as "mega events". From Sunburst and Proxylogon to the Colonial Pipeline and Kaseya hacks—cyberattacks this year have taken on new dimensions that are sweeping up victims in ever-expanding circles of influence.

WHAT CAN WE EXPECT, LOOKING FORWARD?

Combating Ransomware

The change in policy towards ransomware attacks may redefine the arena as we used to know it. However, this doesn't necessarily indicate an immediate change for the better as far as the victims are concerned.

The Biden Administration has made the fight against ransomware a major priority. Specialist task forces were set up in both the Department of Justice and the FBI. To support the task forces' efforts, the agencies began to invest in the relevant technology and recruit the right talent, equipped with a budget granted by the Senate for this specific purpose.

Although the data shows that ransomware attacks are happening all over the world, the US is undoubtedly a major arena for the attacker groups involved. Recent attacks on Colonial Pipeline and Kaseya broke new records of disruption and destruction; however, the attackers suffered some major setbacks themselves.

The DarkSide group behind the Colonial Pipeline hack announced a few days after the attack that it had shut down its affiliation program due to an "unspecified law enforcement agency" that took down critical parts of its offensive infrastructure. An unexplained activity was also recorded in REvil's infrastructure several days after the attack on Kaseya, when the group's websites disappeared from the network and there was silence among REvil's spokespeople.

At the time of writing, no one has taken official responsibility for this digital retaliation. Whoever they are, they enjoy broad support. However, the Kaseya case teaches us something else about this fight. Both sides stimulate and challenge each other to present capabilities that are ever more advanced. We could assume that after the DarkSide shutdown, the other groups would think twice before disrupting US businesses, but then we had Kaseya. They say it's always darkest before the dawn, but in this case it turned out to be a false dawn.

Man-in-the-Middle becomes the hacker in the network

Over the past two years, we have seen an acceleration in the use of penetration tools, such as Cobalt Strike and Bloodhound among many others. These tools don't just pose a real challenge from a detection point of view, they also grant live hackers access to the compromised networks, allowing them to scan and scroll as they wish.

Why is it so different from what we already know? A live hacker is capable of customizing the attack on the fly, while any other file-based hack is programmed to do one set of things alone. Attacks mentioned in the report will be the inspiration for other threat actors. Nowadays we see even top malwares like Qbot with broad infection bases using penetration tools. And it is only going to get worse, meaning that security professionals will need a whole new set of skills to detect this form of attack and prevent it from happening in the future, and causing major damage.

Collateral Damage

The growing trends of triple extortion, supply chain attacks and even just remote cyberattacks may affect your business now more than ever.

The triple extortion trend in ransomware expanded its impact-circles and now includes not only the original target organization, but also extends to the victim's customers, partners and vendors. This multiplies the actual victims of each attack, and requires a special security strategy.

The same applies to supply chain attacks that proved, once again, it does not matter whether we are on the target list of one specific group or another - but rather more importantly it is a question of whether we use the exploited technology that was their original method of entry. In practice this means that you will be burdened with both the financial cost of recovery and the reputational damage of such an attack, even though you may not initially have been in the crosshairs of the hackers.

SolarWinds, with its 18,000 victims, might only be a promo for an even bigger scale impact. And when a company like Colonial Pipeline shuts down its operations due to a cyberattack, the lives of many millions are affected. What is the lesson here? Organizations need to prepare a Collateral Damage strategy, to be able to respond promptly to minimize the impact on their operation—the supply chain trend is not going anywhere other than to the next attack.

WHAT DO WE RECOMMEND, LOOKING FORWARD?

Install updates and patches regularly.

WannaCry hit organizations around the world hard in May 2017, infecting over 200,000 computers in three days. Yet a patch for the exploited EternalBlue vulnerability had been available for a whole month before the attack. Updates and patches must be installed immediately and have an automatic setting.

Adopt a prevention-first strategy and approach.

A detection-only approach is not enough. Cyberattacks can be targeted and evasive and, if data is stolen, the costs to the organization will be high. Once an attack has penetrated a device or a corporate network in any way, it's too late. It is therefore essential to use advanced threat prevention solutions that stop even the most advanced attacks as well as preventing zero-day and unknown threats.

Install anti-ransomware.

Anti-ransomware protection watches out for any unusual activity such as opening and encrypting large numbers of files, and if any suspicious behavior is detected, it can react immediately and prevent massive damage.

Education is an essential part of protection.

Many cyberattacks start with a targeted email that does not contain malware, but uses social engineering to try to lure the user into clicking on a dangerous link. User education is therefore one of the most important parts of protection.

Ransomware attacks do not start with ransomware.

Be aware of other malicious codes, such as Trickbot or Dridex that infiltrate organizations and set the stage for a subsequent ransomware attack.

Collaborate.

In the fight against cybercrime collaboration is key. Contact law enforcement and national cyber authorities; do not hesitate to contact the dedicated incident response team of a cybersecurity company. Inform employees of the incident, including instructions on how to proceed in the event of any suspicious behavior.

PREVENTING MEGA CYBER ATTACKS

THREAT PREVENTION—PREVENT ATTACKS BEFORE THEY HAPPEN

One of the biggest challenges facing security practitioners is Gen V mega attacks—the combination of a wide breadth of threats, large scale attacks and a broad attack surface. True comprehensive protection requires an architected approach that prevents attacks before they happen. Ultimately, the goal is to defeat all attacks across all possible vectors. A security architecture that enables and facilitates a unified and cohesive protection infrastructure is going to provide more comprehensive and faster protection than an infrastructure comprised of pieces that don't work together. This is the heart of what Check Point Infinity delivers—a security architecture to prevent attacks before they happen.

MAINTAIN SECURITY HYGIENE

- **Patching:** All too often, attacks penetrate by leveraging known vulnerabilities for which a patch exists but has not been applied. At the time of the famous WannaCry attack in May 2017, a patch existed for the EternalBlue vulnerability used by WannaCry. This patch was available a month prior to the attack and labeled as "critical" due to its high potential for exploitation. However, many organizations and individuals did not apply the patch in time, resulting in a ransomware outbreak that infected more than 200,000 computers within three days. Keeping computers up-to-date and applying security patches, especially those labeled as critical, can help limit an organization's vulnerability to attacks. Organizations should strive to make sure up-to-date security patches are maintained across all systems and software.

- **Segmentation:** Networks should be segmented, applying strong firewall and IPS safeguards between the network segments in order to contain infections from propagating across the entire network.

- **Review:** Security products' policies must be carefully reviewed, and incident logs and alerts should be continuously monitored.
- **Audit:** Routine audits and penetration testing should be conducted across all systems.
- **Principle of Least Privilege:** If you want to minimize the impact of a potentially successful attack, it is important to ensure that users only have access to the information and resources they absolutely need to do their jobs. Segmentation minimizes the risk of attacks spreading uncontrollably across the network. Dealing with the aftermath of an attack on one system can be difficult, but repairing the damage after a network-wide attack is much more challenging.

UNIFIED THREAT PREVENTION AND INTELLIGENCE EVERYWHERE

Distributed across the Infinity architecture are more than 60 threat prevention technologies that block both known and unknown attacks, driving protections based on a Zero Trust model throughout the network. These protections determine whether a system, or its applications, are secure and operating within regulatory guidelines. Coping with sophisticated attacks requires that protections are pushed as fast as possible to secure user and system interactions between applications within the network, the cloud, and end user environments. Powering Infinity's threat prevention technologies is Check Point ThreatCloud, the world's largest threat intelligence database. ThreatCloud gathers intelligence from more than 150,000 connected networks, detecting 2,000 zero-day files and emulating 13 million files daily. Discoveries made by Check Point Research further enrich ThreatCloud with additional information about new attacks, and artificial intelligence (AI) engines help predict and ultimately prevent the next generation of attacks.

SECURE YOUR EVERYTHING

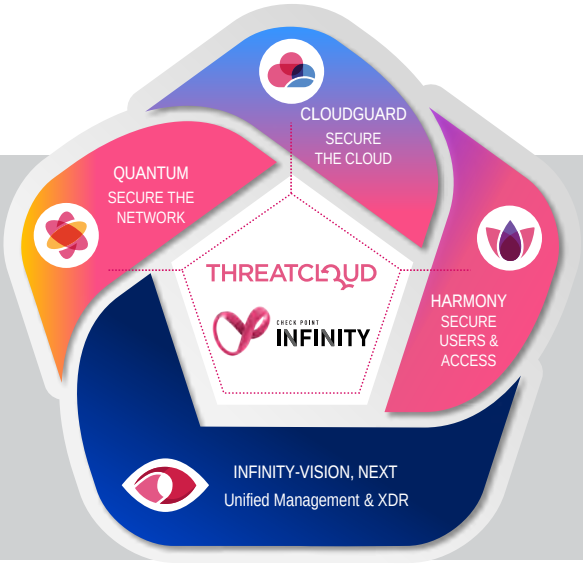
Every part in the chain matters. The new normal introduced during the response to COVID-19 requires that you revisit and check the security level and relevance of all your network's infrastructures and processes, as well as the compliance of connected mobile and endpoint devices, and your growing IoT device estate.

The increased use of the cloud also demands means an increased level of security, especially in technologies that secure workloads, containers, and serverless applications on multi- and hybrid-cloud environments.

DRIVE FOR CONSOLIDATION

The twin forces of the COVID-19 pandemic and the rise in supply chain attacks will transform enterprise security for years to come. Threat actors took advantage of the chaos, stepping-up phishing and ransomware attacks, and even targeting the supply chains responsible for distributing vaccines. Without doubt the most devastating supply chain attack was the breach of the SolarWinds Orion platform. Press reports maintain that the primary targets of the attack were U.S. federal agencies, however the SolarWinds Orion tool is used by some 18,000 public and private organizations around the world.

Slowed economic growth and the push to secure systems from sophisticated new threats presents a conflict for many companies. IT organizations are tasked with implementing new controls and increasing their overall security posture, while at the same time searching for greater efficiency because they have limited buying power. Organizations will seek technology partners that provide security platforms—multifunction systems that address more than one need—because they must consolidate the vendors with whom they work to cope with the challenge of doing more security with less funding. To make consolidation work they will need platform providers to deliver centralized, automated management tools that analyze the overall health and operational efficiency of the systems they maintain, all while securing the move of their IT operations to the cloud.



Check Point Infinity provides a complete security architecture across cloud, network, endpoint, and mobile. Its efficient, easy-to-use management tools enable organizations to implement controls throughout the enterprise.

The Check Point Incident Response Team (IRT) is available 24x7x365 to deliver security incident handling. Organizations that believe they have been exposed to an attack can call Check Point's IRT hotline. Check Point's security experts will help contain the threat, minimize its impact, and keep your business running.

CONCLUSION

The first half of 2021 has seen record numbers of ransomware attacks, both in terms of volume and scale. But why does this trend keep growing? The answer is simple, the technique continues to work, and the hackers behind the attacks keep getting paid. And from ransomware-as-a-service to the triple extortion technique—these threat actors aren't just becoming bigger, they are becoming better at what they do. One of the only ways for organizations to be better prepared is to work under the assumption that something will go wrong, and that their network will be breached at some point. Becoming more resilient, having backups, protecting sensitive data in stronger or different ways. Preventing, detecting and responding to any unusual behavior.

With the Emotet takedown at the beginning of the year, it will be interesting as we progress through 2021 to see whether Trickbot or another type of malware dominates the landscape as much as Emotet once did. Looking ahead, organizations need to be aware that cyberattacks can and will happen to them. They must ensure adequate solutions are in place, but also remember that attacks can be prevented, not just detected, including zero-day attacks and unknown malware. With the right technologies in place, the majority of attacks, even the most advanced ones can be prevented without disrupting the normal business flow.

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: 800-429-4391 | 650-628-2000 | Fax: 650-654-4233

UNDER ATTACK?

Contact our Incident Response Team:
emergency-response@checkpoint.com

CHECK POINT RESEARCH PODCAST

Tune in to cp<radio> to get CPR's latest research,
plus behind the scenes and other exclusive content.
Visit us at https://research.checkpoint.com/category/cpradio/

EXCLUSIVE CYBER SECURITY INSIGHTS FOR EXECUTIVES

Visit: www.cybertalk.org

WWW.CHECKPOINT.COM