CHECK POINT RESEARCH

CYBER ATTACK TRENDS

Check Point's 2022 Mid-Year Report

CHECK POINT™

CONTENTS

CHAPTER 1

01 EXECUTIVE SUMMARY

BY:
MAYA HOROWITZ, VP RESEARCH

MAYA HOROWITZ

VP Research, Check Point

The war in Ukraine has dominated the headlines in the first half of 2022 and we can only hope that it will be brought to a peaceful conclusion soon. However, its impact on the cyber space has been dramatic in both scope and scale, as cyberattacks have become firmly entrenched as a state level weapon. We have identified unprecedented levels of state-sponsored attacks, the growth of hacktivism and even the recruitment of private citizens into an "IT Army." In this report, we take a closer look at how cyber warfare has intensified to become an essential part of the preparation for, and conduct of, actual military conflict. Furthermore, we uncover what the fallout of this will be for governments and enterprises all over the world, even those that are not directly involved in the conflict.

A second major trend in the first half of this year has been the ability of threat actors to disrupt the everyday lives of normal citizens. In this regard there has been crossover with cyber warfare and hacktivism, as we saw a TV station taken down by missiles in Kyiv with a cyberattack launched at the same time for the same purpose, as well as interference with Moscow's smart TV platform to beam live antiwar messages into homes across Russia. The full scale of cyber's ability to cause real harm to citizens, though, is best illustrated by the attack on the entire country of Costa Rica which crippled essential services including healthcare and inland revenue, stopping medical appointments and the collection of taxes. In the US, teachers have been put out of work and student learning disrupted when Lincoln College succumbed to a ransomware attack which resulted in it closing its doors after 157 years. Cyber's theoretical potential for major disruption to civic society just got real in 2022 and in this report, we will look at what organizations can do to avoid becoming the next victim.

The events in Costa Rica also highlighted why ransomware is the number one security threat to enterprises around the world. Imagine an entire country being the victim of cyber extortion by a criminal gang? This was not even an isolated example as Peru became the second victim of 'Country Extortion' not long afterward. The huge potential for financial gain means that ransomware is going to be around for a long time and it's only going to get worse as threat actors invest their ill-gotten gains into better tools and resources. The good news, however, is that we also have new tools and technologies to meet the danger wherever it comes from and however sophisticated the attack.

At the start of the year, we had the continued fallout of Log4j, one of the most serious zero-day vulnerabilities we have ever seen. Any assumptions that it was a one-off event were soon put to bed as just a couple of months later, another huge zero-day vulnerability was found in the open-source Spring Framework—Spring4Shell. We also saw in H1 the demise of a significant malware family, Trickbot, but the good news ended there as the notorious malware Emotet has continued to dominate since its resurgence late last year. In this report, we will unravel 2022's threat landscape and provide examples and statistics of real-world events, so you know exactly what you need to be aware of in your organization.

As we look ahead to the remainder of 2022 and beyond, our global team of experts have provided their predictions, from a tsunami of state-sponsored attacks to the first malicious activity in the Metaverse, so that we can all get prepared now for what's to come.

CHAPTER 2

02 TRENDS

‘CYBER ATTACK TRENDS: 2022 MID-YEAR REPORT’ TAKES A CLOSER LOOK AT HOW CYBERATTACKS HAVE INTENSIFIED IN THE FIRST HALF OF THIS YEAR AND HIGHLIGHTS GLOBAL TRENDS.

RUSSIA UKRAINE WAR— THE FIRST HYBRID WAR THAT FORCED EVERYONE TO TAKE SIDES

On February 24th 2022, Russia launched a full-scale military invasion of Ukraine with attacks on land, at sea and from the air. This was a dramatic escalation of a conflict between the two states that had been going on since 2014.

- **March 2014**—following the Crimean dispute, Russia launched a massive Distributed Denial of Service (DDoS) attack against a large network in Ukraine.
- **December 2015**—as geopolitical tensions continued to rise, Russian state-sponsored Advanced Persistent Threat (APT) group, Sandworm, hacked the power grid of the Ivano-Frankivsk region in Western Ukraine, which distributes power to approximately 230,000 consumers. The attackers also disabled two out of three relevant backup power supplies.
- **April 2022**—two months into the current war, there was another attempt to attack a Ukrainian power grid, which showed similarities to the 2015 incident in terms of the malicious code deployed.

While not as visible as other aspects of the war, the cyber front has silently swept up thousands of 'volunteer troops'—hacktivists, cybercriminals, white hat researchers and even technology companies such as Elon Musk's SpaceX. All these diverse groups chose sides and quickly joined the fight, each with its own targets and toolsets, from DDoS and website defacements to destructive critical infrastructure attacks.

The powerful Conti ransomware group, who claimed hundreds of victims within just a few months, publicly vowed to protect the Kremlin.

SERGEY SHYKEVICH

Group Manager,
Threat Intelligence

> "Cyber warfare is the Hidden Front in the Russo-Ukraine conflict and plays as pivotal a role as tanks and missiles. It has become an essential part of preparations for war as well as playing a role in the conduct or disruption of kinetic military operations. We have also seen that cyberspace is an effective front line in a country's defensive response to military incursion."

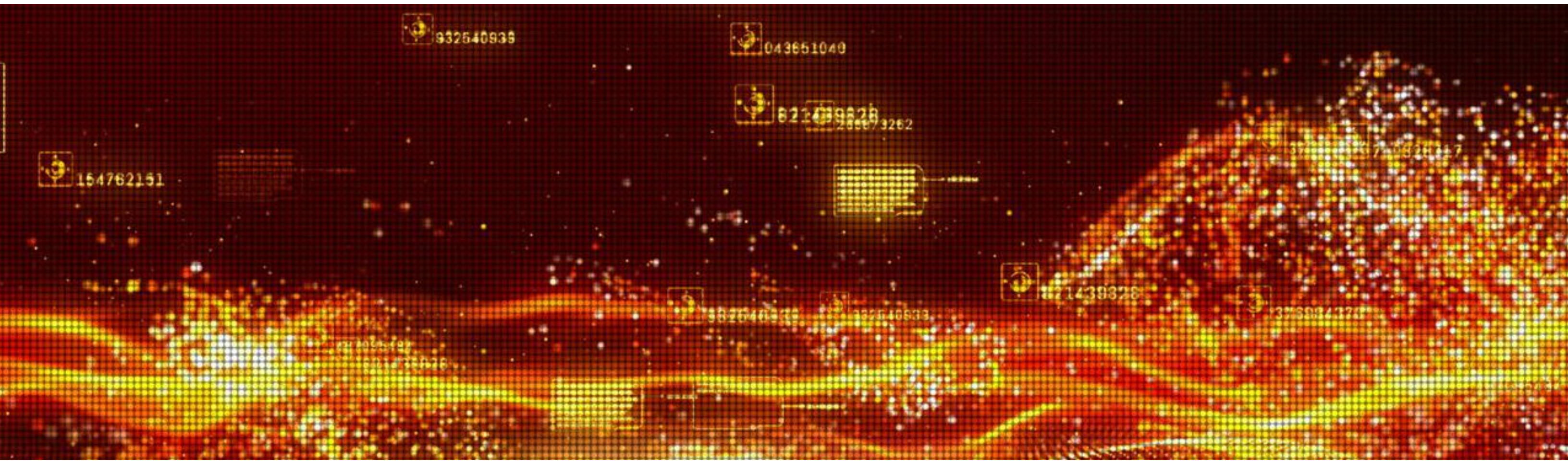
Just three days after the invasion of Ukraine, on February 27th, Check Point Research (CPR) noted a 196% increase in cyber-attacks on Ukraine's government-military sector, and a 4% increase in cyber-attacks per organization in Russia.

Researchers further observed at times that kinetic military and cyberspace actions appeared to be coordinated. For example, on March 1st, a Kyiv TV tower was hit by Russian missiles, resulting in a halt to TV broadcasting in the city. A cyberattack was also launched at the same time for the same purpose. Ukraine in turn took unprecedented steps in the fight in cyberspace by recruiting an international army of motivated hackers to act on its behalf against Russia.

RUSSIAN OPERATIONS AGAINST UKRAINE—DISRUPT AND DESTROY

Even before the full-scale invasion, the Russian government and sophisticated state-sponsored APT groups made an intelligent and coordinated use of both kinetic and cyber-based tools. Top Russian APT groups, widely known for their sophisticated toolsets and global record of attacks, joined the fight as soon as the war started, providing significant cyberspace backup that could potentially tilt the scales in Russia's favor:

- In May, APT28 launched a campaign targeting local state entities, probably with the aim of espionage in order to steal tactical and strategic data.
- In addition to Conti, cybercrime groups such as the 'CoomingProject' announced at an early stage that they would assist the Russian government and protect Russian targets from attacks.
- Killnet, a key pro-Russian hacktivist gang, has consistently targeted NATO members and Ukraine supporters with sophisticated DDoS attacks against critical infrastructure bodies.
- In mid-March 2022, as the war escalated, the Ukrainian CERT reported that critical infrastructure entities were under attack by multiple APT groups. Ukraine stated that 65 critical infrastructure attacks were recorded in a single week.



We estimate these groups started their preparations months earlier, collecting reconnaissance, coordinating targets, gaining access to strategic third-party entities and organizations of interest.

Though some APT groups, such as APT28 and Sandworm, have been associated with the Russian GRU, it is unclear whether coordination procedures are in place, or a general target list is simply shared and pursued. What is clear is that Russian offensive actors are aggressively targeting key national entities in Ukraine to disrupt critical services.

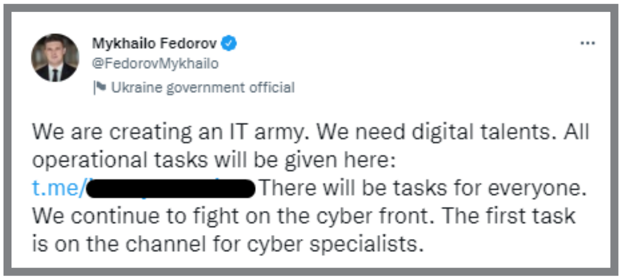
Destructive malware is a significant component of the attacks carried out by the cyberspace actors on the Russian side. Also referred to as a "wiper," destructive malware is used to cause immediate disruption to functionality, destroy data storage systems and harm critical operations. This can have a major impact on public morale as well as unsettle the leadership.

Multiple wipers have been observed since January 2022, with a spike in February, just one day before the invasion when multiple malwares, including HermeticWiper, were deployed against hundreds of Ukrainian government targets, financial, IT and energy institutions. Researchers concluded that eight different wiper malware families were deployed.

UKRAINIAN OPERATIONS AGAINST RUSSIA—CYBER ARMY KICKSTARTER

From recruiting personnel, through to selecting toolsets and coordinating operations between government and individuals, the cyber strategy of the Ukrainian forces has been a major surprise. Until now, Russia had the upper hand in the cyber landscape as it is home to some of the most notorious APT groups and naturally, their loyalty lies with the Russian government and intelligence services. After the war started though, most non-state actors including hacktivist groups, white hat hackers and even the infamous Anonymous Collective, sided with Ukraine, pledging to act against Russia in cyberspace.

The most interesting part of Ukraine's cyber defense strategy centers around the global recruitment of keyboard warriors, proactively inviting recruits from both sides of the law to join the offensive efforts in the cyber arena as part of an organized, government-led initiative. During the first few days of the war, the Ukrainian Minister of Digital Transformation, Mykhailo Fedorov, posted on Twitter calling for "digital talents" to join the newly created IT army, with operational tasks being allocated to them via a designated Telegram channel.



Mykhailo Fedorov
@FedorovMykhailo
Ukraine government official

We are creating an IT army. We need digital talents. All operational tasks will be given here: t.me/[redacted] There will be tasks for everyone. We continue to fight on the cyber front. The first task is on the channel for cyber specialists.

Figure 1: The initiation of IT Army of Ukraine by the Ukrainian government

Just three days after its creation, the Telegram channel had no fewer than 175,000 members. Around that time, Ukraine supporters also started posting requests on underground forums for help in protecting Ukrainian cyberspace. Now, several months into the war, the channel is still active with 262,000 members and is still used to encourage people to help protect Ukrainian critical infrastructure but mostly to promote offensive activities. Attack tools and techniques are shared on a designated website and dozens of Russian targets are published on the channel every day. The channel is also used to publicize successful attacks carried out against Russia, such as replacing the home screen of Russia's smart TV platform with an anti-war message. This attack, which took place on Russian Victory Day, also affected Rutube and Yandex. The Ukrainian government also leveraged its media presence for fundraising via designated ads on underground forums, with over $26 million already collected.

The formation of a state-sponsored cyber army is unprecedented—never before have we seen a government recruiting independents for a global volunteer organization to be used as its personal cyber army. Knowing that its enemy utilizes some of the best attack groups in the world, and that it has the world's sympathies due to its underdog role in the conflict, Ukraine found a way to rapidly enlist powerful players from the global cyber field, helping it regain some advantage.

Anonymous Collective, whose goals overlap somewhat with those of the IT army, has also had successes since it declared cyber war against Russia on Twitter. It appears that the collective launched DDoS attacks against corporate, news and state websites, compromised over 90 databases belonging to telecom, retail and government sector organizations, and leaked hundreds of thousands of documents.

FUTURE IMPLICATIONS

National political agendas have always been a beacon for state-sponsored APT groups. However, cybercrime groups have traditionally sought mostly financial gain, with the goal of monetization clearly guiding them to select their targets. For the first time in a long time, this situation appears to be changing. The Ukraine war has been pushing cybercriminal collectives and lone hackers to back one of the two sides in the conflict. The Ukraine war has set a precedent, moving the fight to cyberspace and blurring the line between the soldiers on the front and the citizens at home. Should cyber offense be a part of every conflict? Should self-motivated hackers take part in national affairs? All we know for sure is that the cyber landscape is continuing to evolve, as it serves more groups and more agendas.

DERYCK MITCHELSON

Field CISO,
EMEA at Check Point

> “If we think at the end of the conflict that the Russian state-sponsored hackers are suddenly going to disappear, then we are absolutely mistaken. I believe they are only going to increase their intensity and we will see a tsunami of cyberattacks on NATO countries.”

When the Russia-Ukraine war does come to an end, it’s likely that we will be in a far worse situation than we are now when it comes to cyber. This is because state-sponsored APT groups, hacktivists and other cybercriminals have been able to ‘hone their craft’ during the conflict. There will be more expertise, more tooling and more groups that have consolidated their efforts and will start to look at attacking NATO countries. And it’s not just government departments in those countries that should be concerned, businesses really need to prepare themselves for what’s coming.

cybercrime groups will continue to target governments in order to cause maximum disruption and to support the goals of their backers, but that’s not where the money is. They need a steady income stream to replenish their cyber warfare coffers to recruit and invest in the latest technology, and that’s why they continue to target enterprises. However, with the right expertise, strategy and cybersecurity solutions in place, organizations are able to prevent attacks from happening.

COUNTRY EXTORTION—RANSOMWARE GROUPS STEP UP TO NATION STATE ACTOR LEVEL

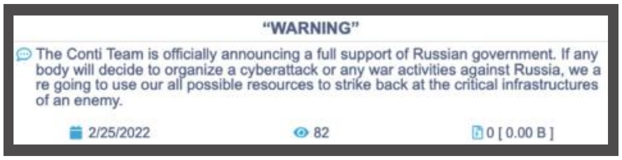
Just like with a new life form we have been tracking the evolution of the ransomware parasite through its evolutionary stages.
In the last six months, we have witnessed ransomware groups actively stepping up to the level of nation state actors, choosing high-level targets and taking sides in global conflicts.
The Conti group, for example, picked fights with entire countries like Costa Rica and Peru, and the newly established Lapsus$ began its malicious activity attacking governmental entities. Not long afterwards, it also successfully went on to target technology giants Microsoft, NVIDIA and Samsung.

Initially, ransomware operations were conducted by individuals or small groups distributing random emails and hoping to collect small amounts of ransom from a large array of victims. As they evolved, the groups expanded to have hundreds of employees, with revenue in the hundreds of millions and sometimes billions of dollars. With their wider scope and scale of operations the groups had to start investing in research and development teams, quality assurance departments, HR people, specialist negotiation teams and sometimes even actual offices.

The larger the operation, though, the more difficult it became to stay under the radar as it is difficult to conceal a multi-billion business employing hundreds of skilled workers with offices in major cities. The larger the business, the more it relies on the cooperation or at least passive consent from local authorities. This dependency forces very large threat actors to identify and align with the geopolitical interests in their home countries. Most ransomware groups are very careful to not attack entities in post-Soviet territories, automatically aborting any operations on machines where Russian is the default language.

In our previous report, we outlined a change in attitude by international law-enforcement agencies, who intensified their war against ransomware groups. Following high-profile attacks, the US government and other law enforcement agencies adopted a more proactive stance. This included internationally coordinated action against ransomware and cryptocurrency money laundering operations, sanctions and more. The Russian authorities 'selectively' cooperated with these moves, detaining some but not others, and releasing them according to their global interests. In January, Russia arrested some members of the REvil ransomware gang, but the group's blog and Tor network returned to full action by April, strangely coinciding with the war in Ukraine and the ending of collaborations between the US and Russia.

Shortly after the war started, Conti expressed its full support for the Russian government and threatened to retaliate with all its resources against "any enemy" that attacks Russian organizations. Conti took the ransomware threat to its highest level, transforming itself into an actor in the geopolitical arena, with cyber offensive weapons capable of causing serious damage to the critical infrastructures of many nation states.



"WARNING"

The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we a re going to use our all possible resources to strike back at the critical infrastructures of an enemy.

2/25/2022 82 0 [0.00 B]

Figure 2: Conti ransomware group announcement from their site.

Conti's declaration had immediate repercussions. Two days later, a new Twitter account called "Conti Leaks" was created by an individual who claimed to be a Ukrainian researcher and who started leaking the group's internal communications. The leak contained nearly 170,000 messages as well as malware source code, which amounted to an unprecedented exposure of the operation and its internal strategies. Check Point Research (CPR) analyzed the Conti leaks and discovered the different layers and hierarchy that you might find in a typical high-tech company with clearly defined roles and departments.

Following its political move, Conti increased the rate of attacks. As reported on its shame blog, the group went from ten victims in January to more than 20 in February, over 50 in March, and nearly 80 in April.

April also signaled a new stage of "country extortion", when Conti attempted to extort the entire country of Costa Rica. The group continued extorting more government entities, continuing with Peru on May 7th. A few days later, on May 12th, Costa Rica's president declared a state of national emergency, later announcing the country was at war with Conti - the first time ever that a country has declared war on a cybercrime group. This extraordinary situation came about after the cybercriminals breached and encrypted the data of at least 27 Costa Rica government agencies, probably the most disruptive cyberattack ever inflicted on any country, including those by another government.

After Costa Rica decided to not pay the ransom, the group publicly declared its intentions to overthrow the government and called for citizens to revolt, stating it would carry out similar operations in the future. In May, the US offered a bounty of ten million dollars for information that would lead to the arrest of Conti's leaders.

While Conti brought about the new method of 'country extortion', Lapsus$ reintroduced an old one and was able to get its hands on proprietary information and source code belonging to the biggest technology companies. Surprisingly, the group's modus operandi excludes the usual encryption element you would expect to see in a ransomware attack, focusing only on data exfiltration and extortion based solely on the threat of publication. This revival of an old phenomenon could be the start of a new trend as the tactics have since been adopted by the RansomHouse group and Karakurt, the data extortion group related to Conti. Apparently, data exfiltration is much easier than encrypting an entire network and then assisting with decryption when the ransom is paid. Threat actors are clearly finding ways to do less work for more money.

LOTEM FINKELSTEEN

Director,
Threat Intelligence and
Research

> “Large threat actors are under a lot of pressure to avoid detection, which could explain their tendency to “rebrand” their ventures. Disbanding an existing operation and later reassembling it under a different name is meant to hinder any investigations. Some observers claimed that Conti's current international actions are a smoke screen, leading up to another rebrand. Regardless of the outcome, these events prove that it is possible to extort an entire country and that a cybercrime organization can evolve into a geopolitical actor. The inclination to rebrand and change operation tactics creates fertile ground for the continued emergence of new groups and new operation methods."

MICROSOFT BLOCKS INTERNET MACROS IN OFFICE—THE DEVELOPMENTS IN THE EMAIL INFECTION CHAINS

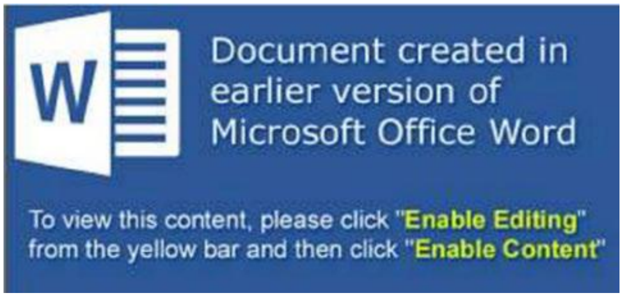
Why do 34% of burglars enter homes through the front door? Because every home has one, and very often, they are left wide open. For many years, MS Office documents have been our digital front doors. Everyone uses them, mostly without questioning their source, which makes them a very widely open door indeed.

The malicious use of Microsoft docs occurs so frequently that they have a name - maldocs. One of the main techniques to create maldocs involves the abuse of Office Macros, which are a highly versatile tool with extensive programing capabilities. Security companies have been fighting this for years, but it was always clear that the key to preventing macro abuse lies in the hands of Microsoft. Indeed, in February 2022 Microsoft announced it would change Office default settings to disable.

Office macros are special purpose programs and, as stated on Microsoft's support page, are often used for malicious purposes:

"Macros automate frequently used tasks to save time... Many were created by using Visual Basic for Applications (VBA) and are written by software developers. However, some macros can pose a potential security risk. Macros are often used by people with malicious intent to quietly install malware, such as a virus, on your computer or into your organization's network."

Although PoC and active exploits using VBA macros appeared as early as 1995, they lacked info-stealing functionality and were mostly used for pranks. These types of attacks died out in 2010 when Microsoft introduced "Protected view", a yellow ribbon warning users not to enable macros' functionality. The use of macros was re-introduced when threat actors realized that, with a bit of social engineering, they could convince users to enable macros and then use them to download and execute other binaries.



Document created in earlier version of Microsoft Office Word

To view this content, please click "Enable Editing" from the yellow bar and then click "Enable Content"

Figure 3: Typical label designed to convince victim to enable macros.

ITAY COHEN

Group Manager,
Cyber Research

> Although Microsoft acknowledged the issue multiple times, the malicious use of Office macros and vulnerabilities increased in popularity throughout the years. By January 2022, our analysis found that as much as 61% percent of all malicious payloads attached to emails sent to our clients were various document types (such as xlsx, xlsm, xls, docx, doc, ppt, pdf, rtf and others). Our current report finds that Excel files alone made up 49% of all malicious files received by email!"

Although Microsoft acknowledged the issue multiple times, the malicious use of Office macros and vulnerabilities increased in popularity throughout the years. By January 2022, our analysis found that as much as 61% percent of all malicious payloads attached to emails sent to our clients were various document types (such as xlsx, xlsm, xls, docx, doc, ppt, pdf, rtf and others). Our current report finds that Excel files alone made up 49% of all malicious files received by email! This trend corresponds with the evident tendency of most actors to use email (SMTP) instead of web-based sites as their initial attack vector. Typically, a carefully socially engineered email carrying an Excel file with a malicious macro is the weapon of choice for non-sophisticated actors as well as top niche APTs.

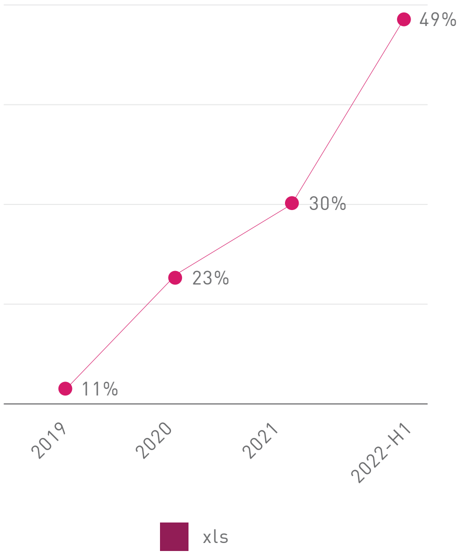


Figure 4: Percentage of Excel files of the total malicious files received by email.

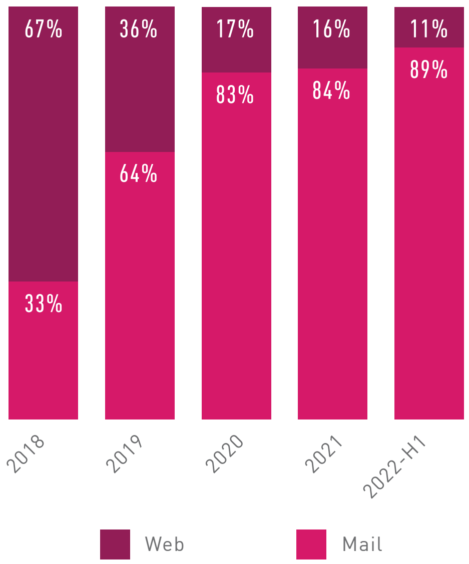


Figure 5: Increase in proportion of malicious files sent by email.

Only recently, CPR reviewed a series of attacks by various APT groups, who socially engineered their attacks using articles on the current Russian war against Ukraine to send weaponized Word documents. Other major malware families using malicious Office documents include TrickBot, Qbot, Dridex and many more. The unofficial king of maldoc usage is Emotet, which routinely sends high volumes of maldocs through email, sometime concealed inside password-protected zip files, to expend its botnet.

In February this year, Microsoft announced its intention to block VBA macros on Office docs. They will present users with a series of alerts and ultimately require them to save files locally and turn off the Mark of the Web (MOTW) protection mechanism. This is in addition to its previous policy change, in which Microsoft restricted the use of Excel 4.0 macros. The policy change is planned to roll out in the coming months.

Following these announcements, threat actors began examining the alternatives for non-executable malicious email attachments. Emotet was reported in April to be testing new TTPs (Tactics, Techniques, and Procedures), emailing OneDrive URL links of Zip files containing malicious xll files. Xll files are .dll libraries designed for Excel, and threat actors typically use an exported *xlAutoOpen* function to download and run malicious payloads. Various existing tools and services, such as Excel-DNA, are already available to build .xll downloaders.

Another possible alternative TTP to maldocs is the use of ISO archives, which bypass the MOTW mechanism. Together with a combination of .hta payload, they can look like documents but run malicious code in the background. We already saw a rise in attacks using these archives. Bumblebee, a new downloader detected in February, delivers various payloads that often result in ransomware attacks, and is reported to initially involve .iso files delivered in email.

Blocking Office internet macros does not eliminate maldoc options. Threat actors continue to exploit vulnerabilities. (CVE-2021-40444) and the newly-discovered Follina, which use HTML template injection, are just recent examples.

Threat actors will continue to find new ways to deliver malware, but this policy update by Microsoft is certainly going to have an effect on current TTPs. Both security providers and users should prepare accordingly.

SCOPE OF THE MOBILE MALWARE LANDSCAPE

In an age when we increasingly rely on third-party applications and connect corporate networks to employees' personal devices, mobile devices have become valuable targets, requiring us to invest resources in mobile protection. The mobile marketplace's exponential growth over the past few years offers a wider range of opportunities for threat actors. This potential is being exploited to its fullest, as we see malicious actors investing efforts in more advanced techniques and innovative social engineering schemes, rivaling the threat landscape for PCs.

Our last security report addressed Pegasus, the notorious NSO group Spyware which made headlines in 2021 after the discovery that the tool was used to gain access to mobile devices belonging to government officials, journalists, human rights activists and business executives worldwide.

Additional Pegasus campaigns were uncovered in the first half of 2022:

- **January**—Pegasus was found to have infected new governmental targets in Finland's Ministry of Foreign Affairs, targeting Finnish diplomats as part of a cyberespionage campaign.
- **April**—Pegasus was revealed to have been detected on multiple official UK networks, including the Prime Minister's office.
- **May**—Pegasus was confirmed to have been found on devices belonging to the Spanish Prime Minister and Defense Minister.

Fortunately, Apple announced in July that it is introducing a 'lockdown mode' for its devices in order to protect against Pegasus hacks. But while Pegasus is one of the most powerful tools currently on the market, the surveillance vendor ecosystem has also become more competitive. Another marketed spyware called Predator, produced by the North Macedonian commercial surveillance company Cytrox, was found to have infected iPhones towards the end of 2021 via single click links sent over WhatsApp. As of today, the reach of these tools, let alone their mechanisms, is not yet fully understood by the cyber community despite extensive research efforts.

In February, researchers found that one of the same vulnerabilities in Apple software exploited by the NSO group in iPhones was simultaneously leveraged by a competing firm called QuaDream. Zero-click vulnerabilities allow a remote intrusion into iPhones without any action needed by the victim, such as clicking a malicious link, to trigger an infection.

Later in April, a new zero-click iMessage exploit leveraged to install Pegasus on iPhones was discovered, running on some early iOS versions prior to 13.2. The exploit named HOMAGE was used in a campaign against Catalan officials, journalists and activists. In this campaign, some victims were also infected with Candiru spyware, from yet another mercenary hacking company. Finally, in May, security researchers found that threat actors used five zero-day vulnerabilities and other known unpatched flaws to install the Predator malware as part of three campaigns that occurred between August and October 2021.

In addition to politically and ideologically driven spyware actors, we have also observed financially motivated operations like Flubot. Since its emergence in December 2020, it has been considered the fastest growing Android botnet ever seen. Flubot's success is partly due to its spreading technique called "Smishing" (SMS Phishing), which uses SMS messages as the attack vector for malware distribution. It sends the same SMS to the initial victim's contacts, resulting in exponential spread.

In May 2022, CPR discovered that MediaTek and Qualcomm, the two largest mobile chipset makers, ported the vulnerable ALAC code into their audio decoders, which are used in more than half of all smartphones worldwide. The ALAC issues found by CPR could be used by an attacker for remote code execution on a mobile device through a malformed audio file. In addition, an unprivileged Android app can use these vulnerabilities to escalate privileges and gain access to media data and user conversations.

The Flubot gang is known to be particularly innovative and continuously seeking to improve its variants, using features that are ordinarily seen in the development of PC malware rather than mobile. Those features include DNS tunneling or Domain Generation Algorithm (DGA), which make detection and shut down more difficult. With its multiple campaigns and tens of thousands of victims, Flubot received so much attention that in June, an international law enforcement operation involving 11 countries led to its infrastructure takedown and rendered the malware inactive. Evidently, Flubot's position could not remain vacant for too long, as a new Android malware operation called MaliBot emerged in the wild soon after. MaliBot is targeting online banking and cryptocurrency wallets in Spain and Italy, using the same smishing distribution method as Flubot.

At the other end of the mobile threat spectrum are application stores, which encapsulate a whole arena of their own for cybercriminals. The most secured stores like the Google Play Store and the Apple App Store have thorough review processes to investigate candidate applications before they are uploaded and are held to high security standards once they are admitted onto the platforms. A recent report stated that throughout 2021, Google blocked 1.2 million suspicious applications from the Google Play Store, and Apple blocked 1.6 million apps from their App Store. Resourceful cybercriminals continually try to bypass these security measures with different tactics such as manipulating their code to pass through the filters or introduce initially benign applications and add the malicious elements at a later stage.

It's not so surprising to still find malicious applications hiding in these stores. In fact, these platforms remain the main infection vectors in mobile threats. For example, CPR recently analyzed suspicious applications on the Google Play Store and found a few of them masquerading as genuine Anti-Virus solutions, while in reality, once downloaded the apps installed an Android Stealer called SharkBot which steals credentials and banking information. SharkBot implements a geofencing feature, Domain Generation Algorithm (DGA), and evasion techniques that make it stand out in the field. SharkBot distribution is not widespread but rather targeted: it selects victims using the geofencing feature to identify and ignore users from China, India, Romania, Russia, Ukraine or Belarus.

In February, a new Android banking Trojan called Xenomorph was spotted lurking behind a fake productivity application on the Google Play Store. There were over 50,000 downloads. The Xenomorph malware has a lot of potential to evolve, as it currently uses classic overlay attacks and has the ability to steal credentials along with intercepting SMS and notification to log and use two-factor authentication (2FA) tokens. It's evident that threat actors will continue to try and leverage official stores.

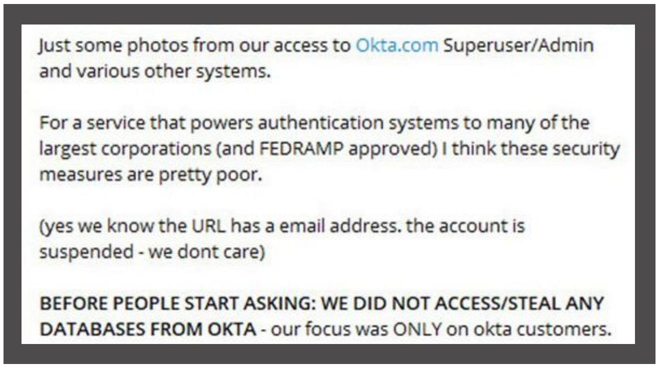
Unfortunately, cybercriminals are well aware of the central role that mobile devices play in many peoples' lives and are always adapting and improving their tactics to match. The threat landscape is evolving rapidly, and mobile malware is a significant danger for both personal and enterprise security.

CLOUD SUPPLY CHAIN ATTACKS

For the past few years, CPR has been following the evolution of the cloud threat landscape, as well as the constant increase in cloud infrastructure adoption by corporate environments. As many as 98% of organizations utilize cloud-based services, and approximately 76% of them have multi-cloud environments, featuring services from two or more cloud providers.

In March 2022, we released a review of the latest cloud trends and attacks on industry-leading cloud service providers. Critical vulnerabilities were exploited by cybercriminals to gain access to the corporate environments of the cloud provider's entire customer list. We also covered the unprecedented progress made by cybercriminals in the field of supply chain attacks, from the SolarWinds Orion software breach—an innovative on-premise-to-cloud incident in which a backdoor embedded in a software update was leveraged to gain access to private cloud environments—to the Log4Shell, a vulnerability in Apache's most popular Java logging library, Log4j, that allows threat actors to easily gain control over Java-based web servers and execute arbitrary code.

It seems we are now gearing up for when supply chain attacks meet the cloud arena. On March 21st, the notorious ransomware gang Lapsus$ released a statement in its Telegram group that said it had gained access to Okta, an identity management platform, by obtaining access to an administrative account. Lapsus$ is known for publishing sensitive information, often source code, stolen from high-profile tech companies such as Microsoft, NVIDIA, and Samsung. However, this time, the target wasn't Okta, but rather its customers. Okta, a cloud-based software, is used by thousands of companies to manage and secure user authentication processes as well as by developers to build identity controls. This means that hundreds of thousands of users worldwide could be potentially compromised by the company responsible for their security.



Just some photos from our access to Okta.com Superuser/Admin and various other systems.

For a service that powers authentication systems to many of the largest corporations (and FEDRAMP approved) I think these security measures are pretty poor.

(yes we know the URL has a email address. the account is suspended - we dont care)

BEFORE PEOPLE START ASKING: WE DID NOT ACCESS/STEAL ANY DATABASES FROM OKTA - our focus was ONLY on okta customers.

Figure 6: Lapsus$ announcement about OKTA, on their Telegram channel.

Curiously, on March 22nd, Okta released an official statement claiming that an investigation concluded that a breach did not occur, although an unsuccessful compromise attempt was observed in January 2022, when a new factor was added to the Okta account of a client's support engineer. At that point, no notification was sent to Okta's customers. However, another statement released in close proximity to the first one, shared that approximately 2.5% of Okta's customers were affected by the Lapsus$ breach—around 375 companies, according to a media report.

Although the statements were probably released to reassure Okta's customers, they only contributed to the general fear caused by the attack. Lapsus$ commented on the statements, or as it called them, *"the lies given by Okta"*, on its popular Telegram channel. Lapsus$ assured its 35,000 followers that the successful breach allowed the attack group to "log in to superuser portal with the ability to reset the password and MFA of ~95% of clients".

CPR suggested that the access Lapsus$ had gained to Okta clients might possibly explain the cybercrime gang's *modus operandi* and impressive record of successes, all thanks to excessive permissions having been granted to a third-party within the corporate cloud environment.

STUART GREEN

Cloud Security Architect
Check Point

"The two biggest concerns I'm seeing in the cloud landscape in 2022 are vulnerabilities within cloud providers themselves and modules in the open-source community that are not properly vetted or managed."

Identity and Access Management (IAM) role abuse attacks were thoroughly discussed by CPR in 2021, and while still an ongoing issue, there are other risks that businesses need to be aware of.

While the Okta breach wasn't necessarily a 'cloud supply chain attack'—this would be when a cloud provider such as Azure or AWS is compromised—it was a significant event from the first half of this year that did affect the supply chain and will hopefully teach businesses some important IAM lessons. Currently, the most prominent supply chain risk we are seeing comes from open-source software.

Many modules and packages are written by individuals who may not have the expertise or budget to make it completely secure. Then when the 'unsecure' code is contributed to the open-source community, who owns it? Who maintains it? As a developer, you might think you're importing one thing, but it actually has dependencies that you aren't aware of. This is how NotPetya came about. It infiltrated computer systems using a popular piece of open-source accounting software.

Unfortunately, when it comes to your chosen cloud provider, you can't control the security of the platform itself. And these platforms do have vulnerabilities. You could have the best will in the world and the highest expertise, but unless you've got a team of analysts constantly researching the platform you're using, it's not going to be enough. This really makes the case for multiple layers of security. You might not be able to prevent a breach of the cloud provider itself, but what you are able to do is mitigate the fallout. Implementing things like zero-trust and least privilege will mean that in the event of a breach, it is contained and cannot spread.

CHAPTER 3

03 CYBER ATTACK CATEGORIES BY REGION

IN THE FIRST HALF OF THE YEAR, THERE WAS A 42% INCREASE IN WEEKLY CYBERATTACKS GLOBALLY WITH EVERY REGION EXPERIENCING A SIGNIFICANT ESCALATION.

CYBER ATTACK CATEGORIES BY REGION

GLOBAL

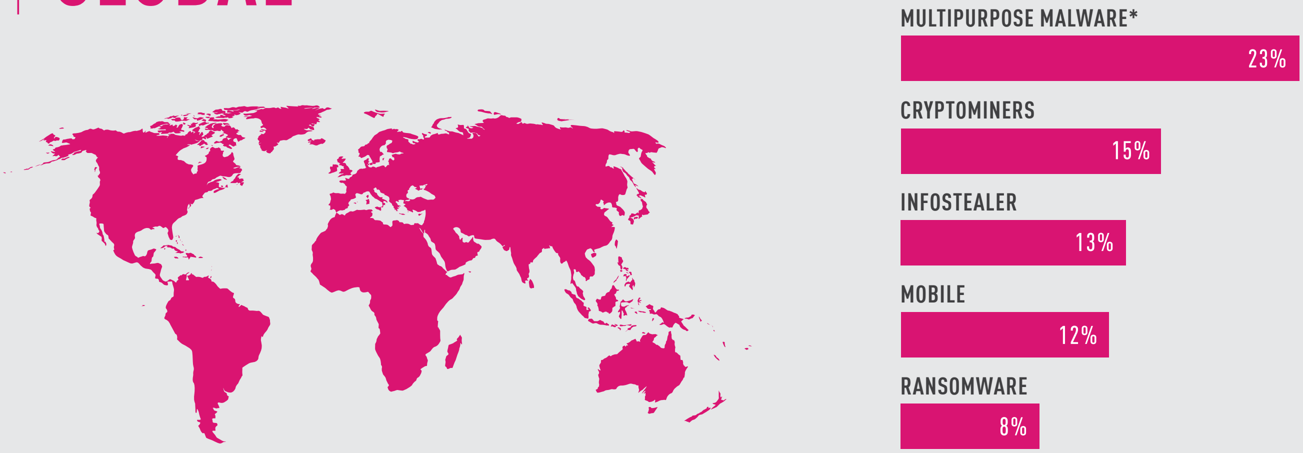


Figure 7: Percentage of corporate networks attacked by each malware type globally.

AMERICAS

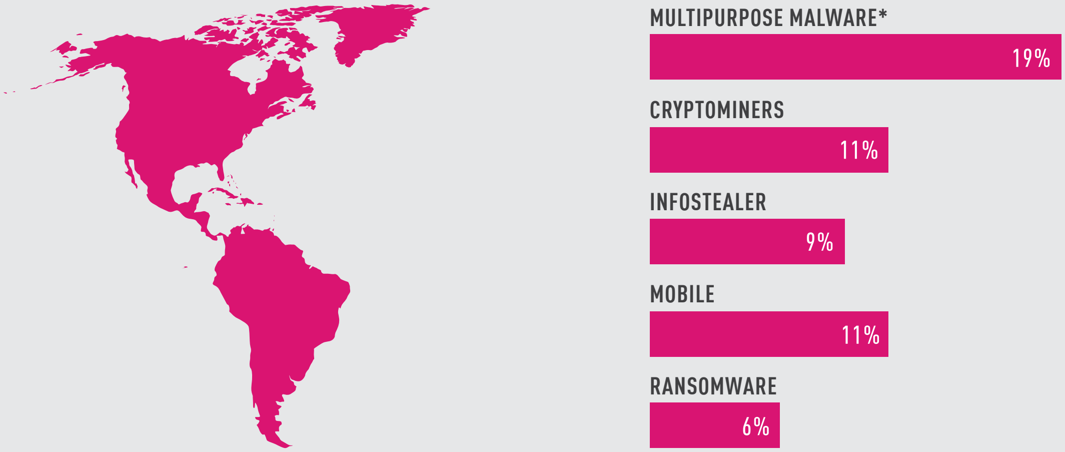


Figure 8: Percentage of corporate networks attacked by each malware type in the Americas.

* Banking Trojans and botnets, previously classified as two distinct types, are combined in a single category. As many banking Trojans received additional functionalities, making the differentiation between the two categories less distinct, we introduce the category "multipurpose malware" to include both genres.

CYBER ATTACK CATEGORIES BY REGION

EMEA

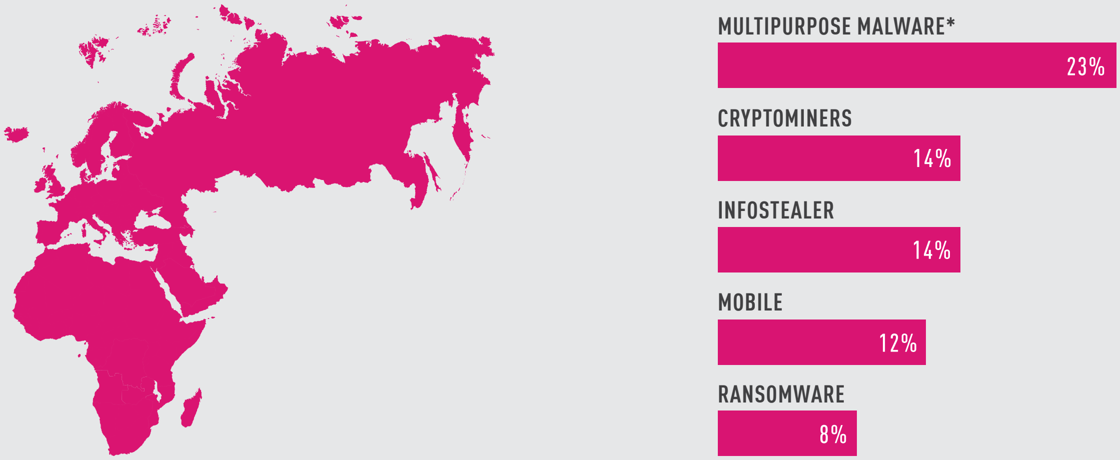


Figure 9: Percentage of corporate networks attacked by each malware type in EMEA.

APAC

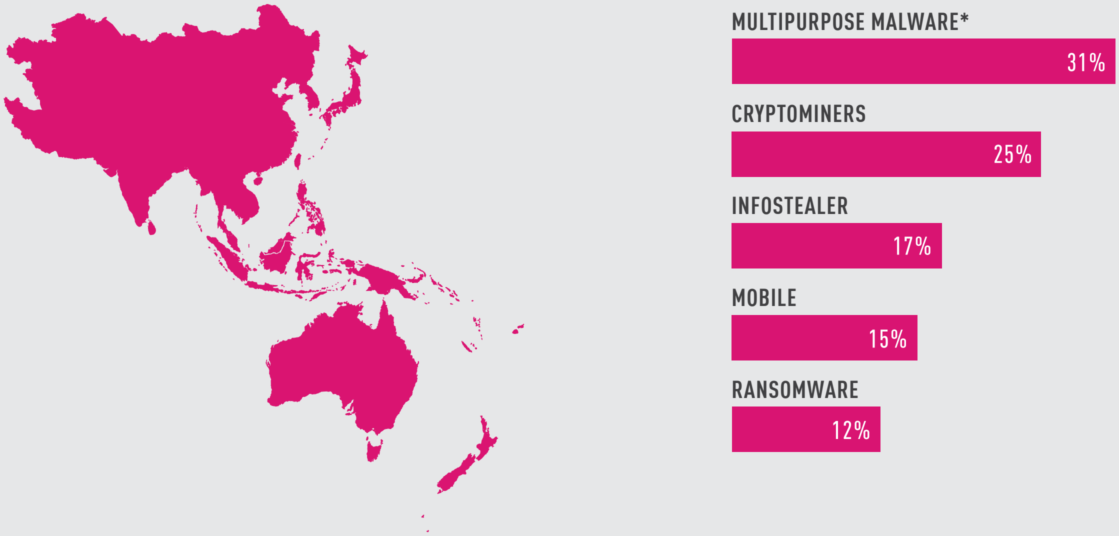


Figure 10: Percentage of corporate networks attacked by each malware type in APAC.

* Banking Trojans and botnets, previously classified as two distinct types, are combined in a single category. As many banking Trojans received additional functionalities, making the differentiation between the two categories less distinct, we introduce the category "multipurpose malware" to include both genres.

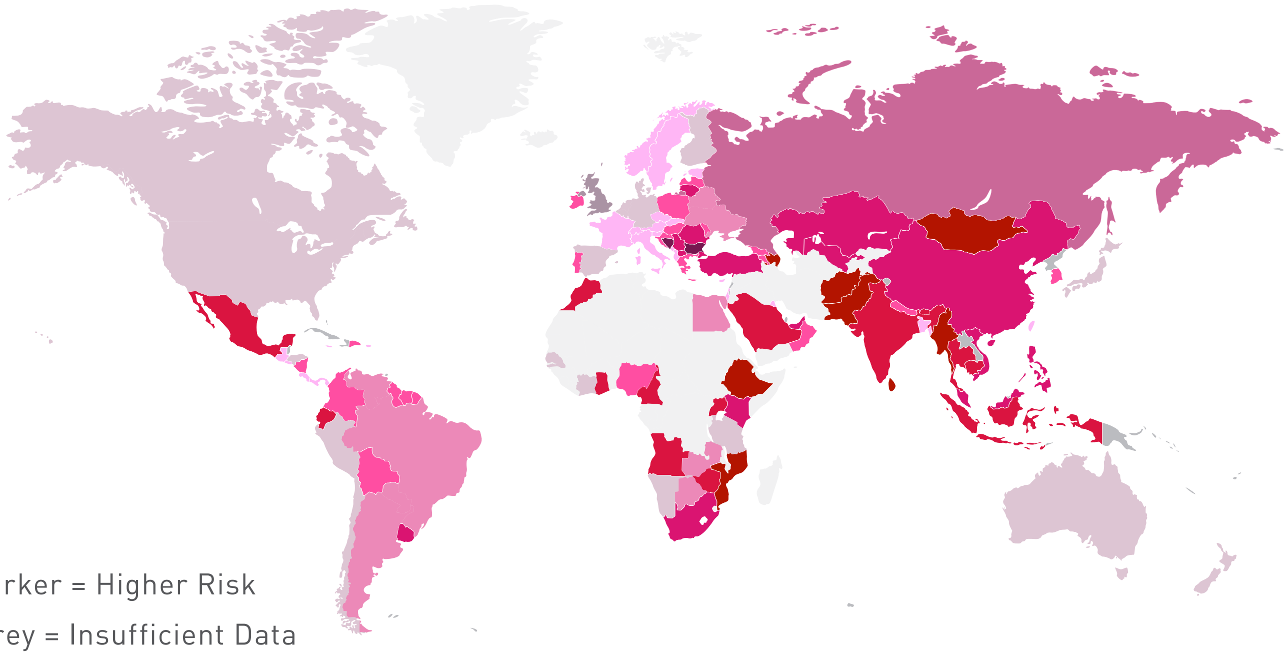
OMER DEMBINSKY

Data Research Group Manager

> The biggest change this year regarding cyberattack categories comes from ransomware. Each region is facing more of these types of attacks, with APAC leading the way (12% of organizations compared to 4% in H1 2021). It is no surprise really when we look at how ransomware actors have evolved this year, and unfortunately it looks set to get worse."

GLOBAL THREAT INDEX MAP

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



* Darker = Higher Risk

* Grey = Insufficient Data

Figure 11: Global Threat Index Map

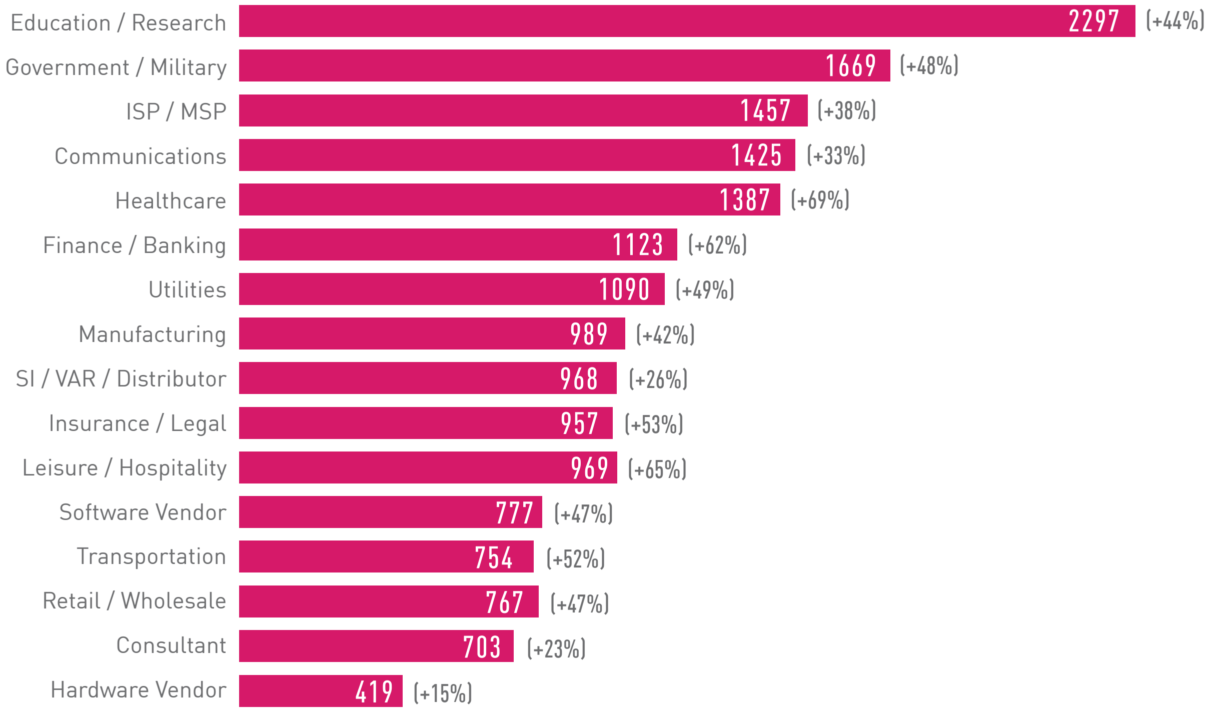


Figure 12: Average weekly attacks per organization by Industry H1 2022 compared to 2021.

Similar to what we saw in our 2021 top industry ranking, the first half of 2022 displays significant rises in attacks against all sectors alike. **Education and Research** still leads as the most targeted industry, with an average of 2,297 attacks against organizations every week showing a 44% increase compared to 2021. In addition, **Healthcare** is still one of the most targeted sectors globally, with a 69% increase compared to 2021. This is the highest increase of all industries, going hand-in-hand with the multiple breaches of different ranges we observed against healthcare organizations during that period.

TOP MALICIOUS FILE TYPES—WEB VS. EMAIL

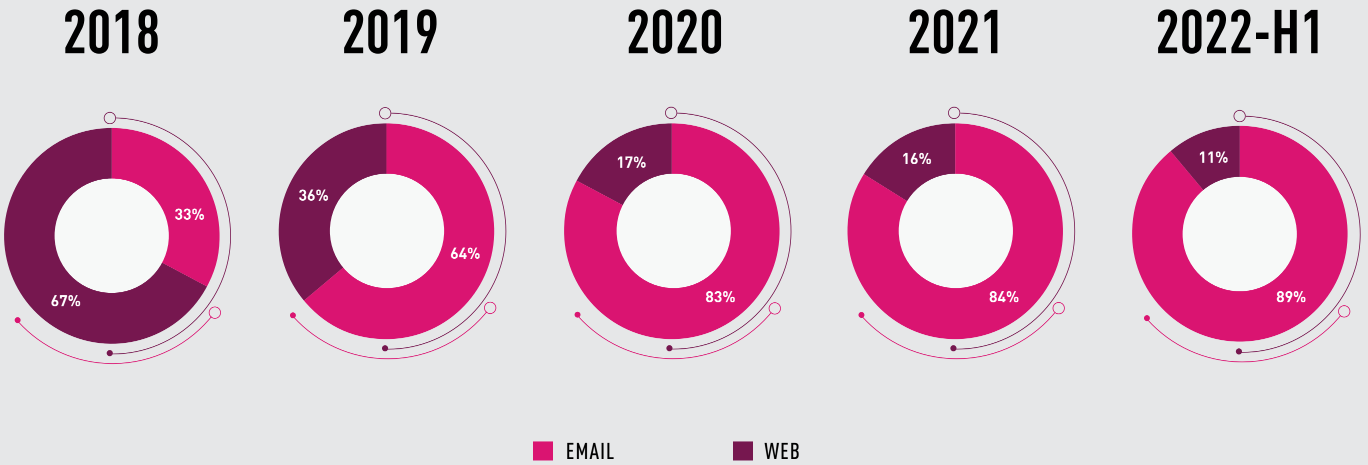


Figure 13: Delivery Protocols—Email vs. Web Attack Vectors in 2018-2022.

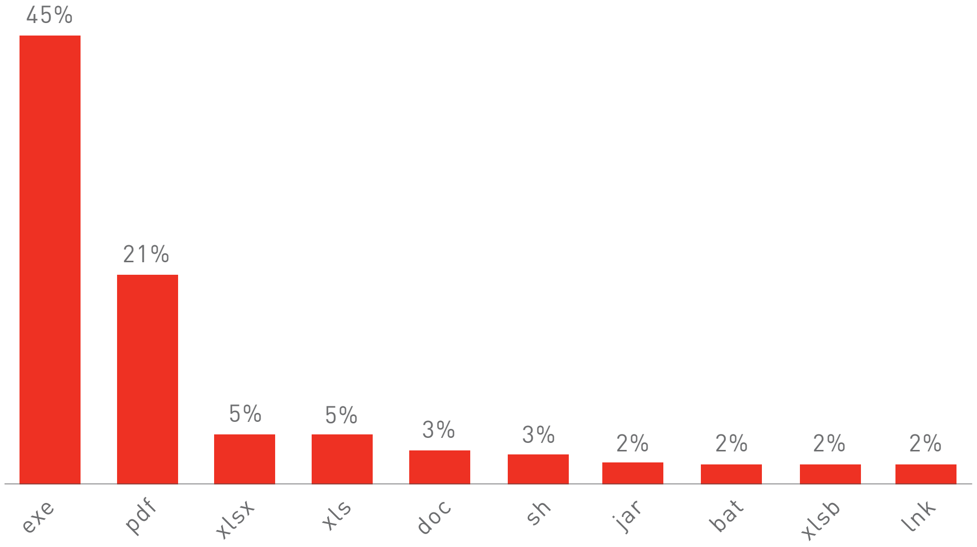


Figure 14: Web—Top malicious file types.

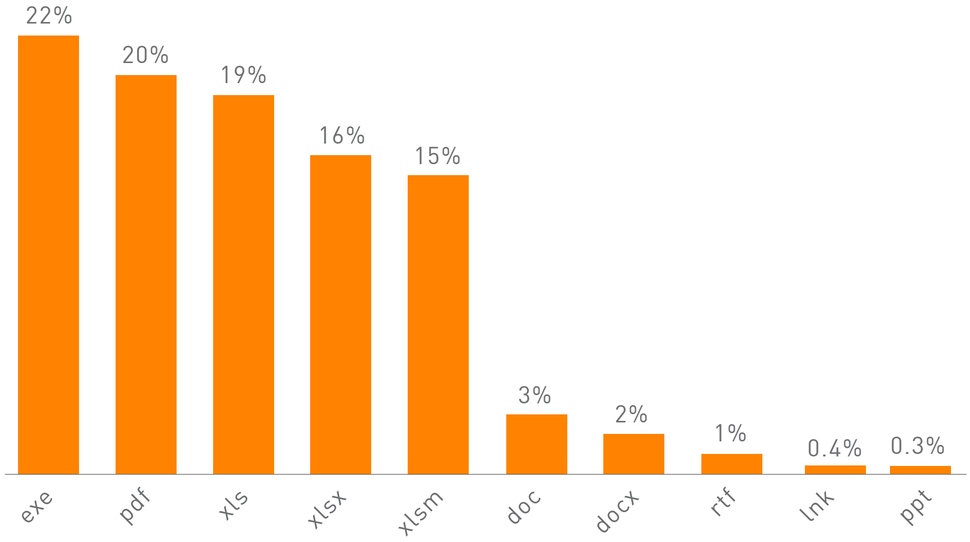


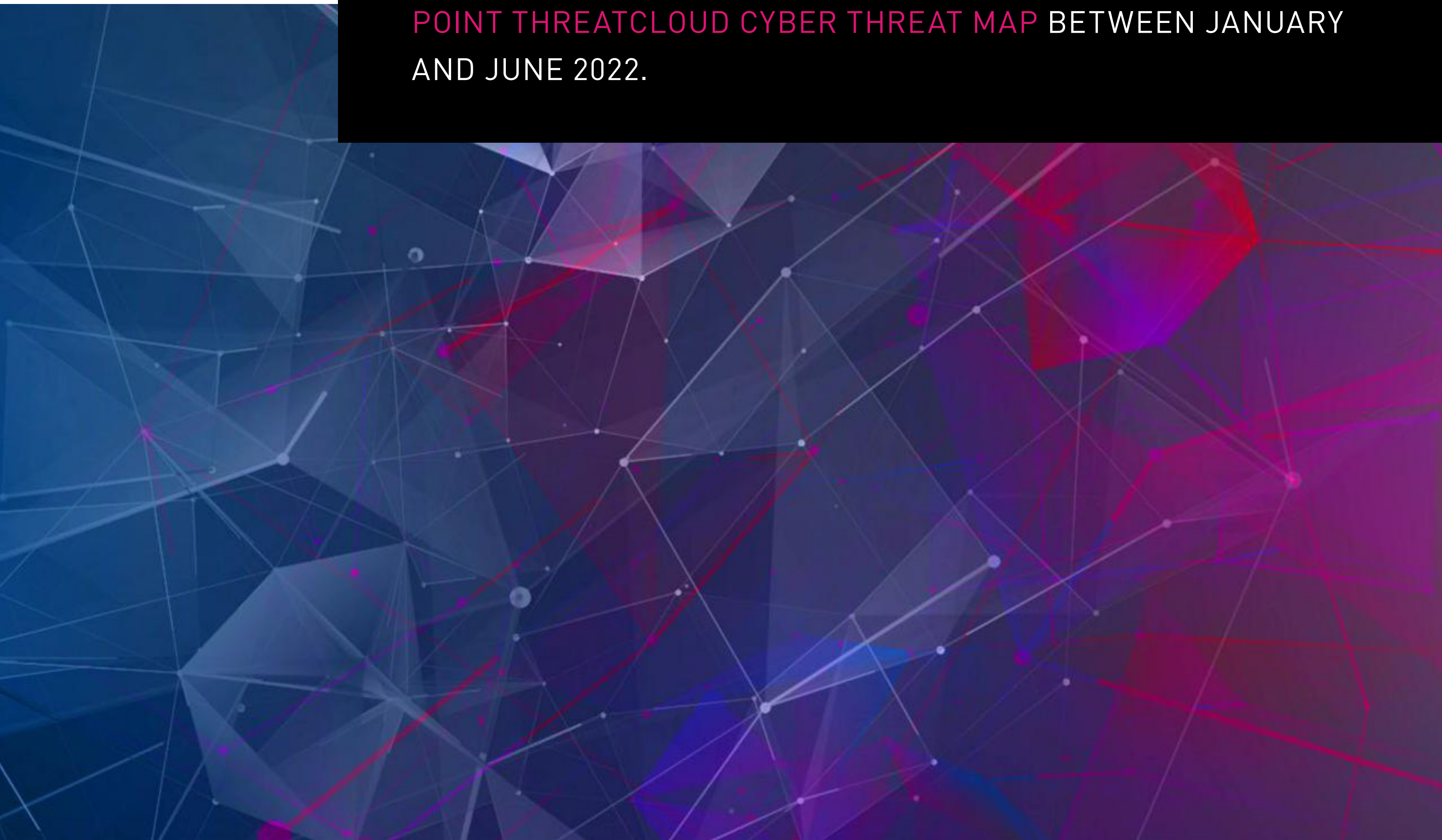
Figure 15: Email—Top malicious file types.

The proportion of email-delivered-attacks has gradually risen to reach a staggering record of 89% of all in-the-wild attacks. Email-delivered attacks typically include socially engineered content, intended to convince recipients to open an attachment, often a PDF or Office file (75% of attachments). Many mass distributed campaigns, with Emotet being the most extensive, use this tactic. However, as important as user awareness and email protection solutions are, it is not enough to ensure full protection. Data collected from the Check Point Incident Response Team (see the last chapter in this report) shows that from cases handled by our IR team, with a known entry point, only 17% of successful breaches originated from SMTP attack. This puts an extra emphasis on alternative attack vectors and the importance of rapid protection publication and vulnerability patching.

CHAPTER 4

04 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 2022.



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 2022.

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

TOP MALWARE FAMILIES

GLOBAL

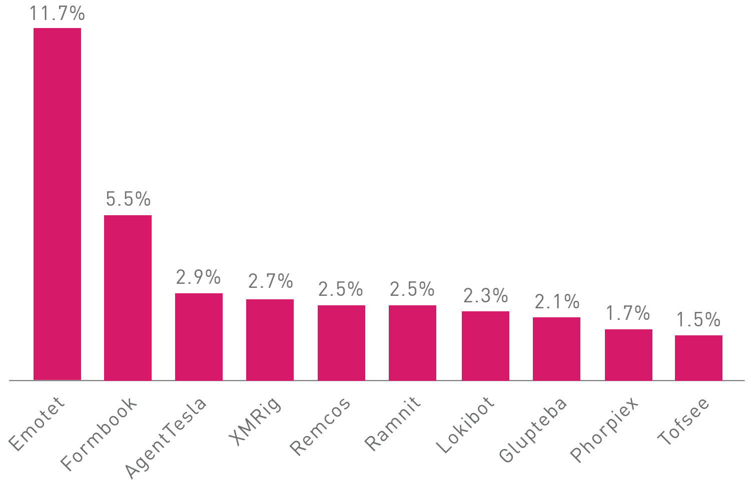


Figure 16: Most prevalent malware globally.
Percentage of corporate networks attacked by each malware family.

AMERICAS

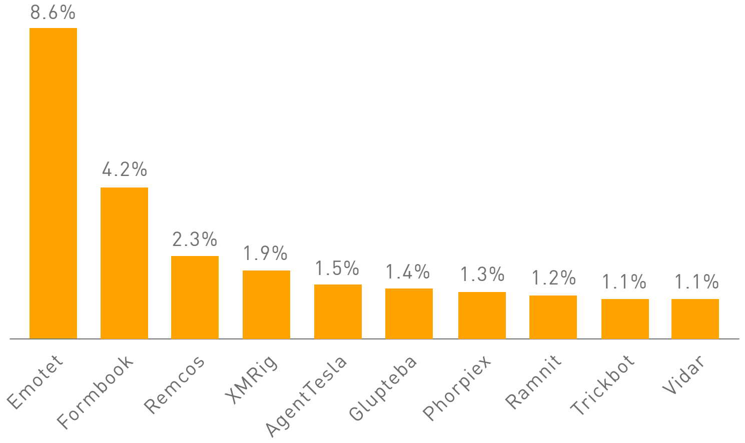


Figure 17: Most prevalent malware in the Americas.

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

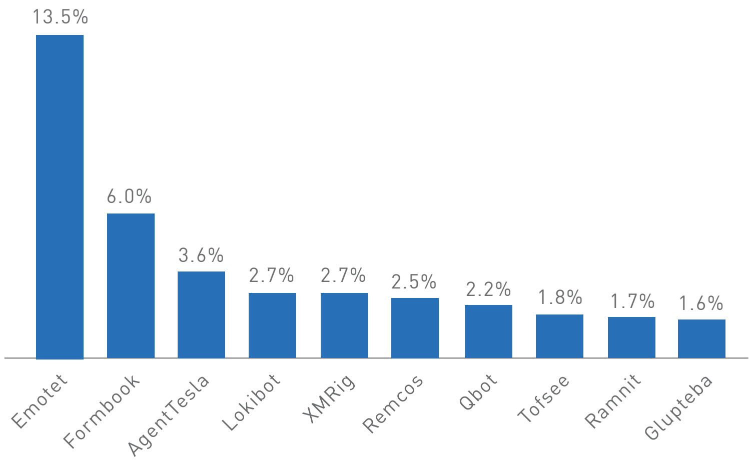


Figure 18: Most prevalent malware in EMEA.

ASIA PACIFIC (APAC)

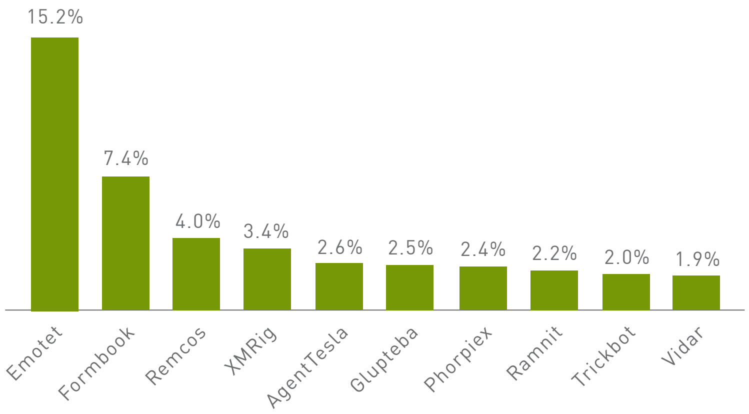


Figure 19: Most prevalent malware in APAC.

CHAPTER 5

05

TOP MALWARE FAMILIES

GLOBAL ANALYSIS OF TOP MALWARE

The Emotet botnet has re-claimed its rightful place at the top of the global top malware chart. In our last yearly report summarizing 2021, Emotet fell to 4th place in the chart, but still impacting approximately 5% of corporate networks worldwide. In the last couple of years, Emotet has been on quite a journey. In early 2021, the malware was taken down in a global operation involving multiple law enforcement agencies and national authorities, in which researchers gained control of its infrastructure. By the end of the year, however, Emotet was back in business. Within two months, the malware resumed operating at approximately 50% of its former attack volume, relying on Trickbot—yet another botnet superpower—as its dropper. Since the end of 2021 and well into 2022, Emotet has been continuously active, carrying out spam campaigns of all kinds. These include a campaign targeting IKEA employees using the thread hijacking technique which relies on legitimate internal corporate emails; a US phishing campaign impersonating the IRS during the 2022 tax season; a financial theft campaign aimed at collecting credit card information stored on Google Chrome; and many more. Emotet operators even managed to recover quickly from the launch a faulty campaign using a broken installer preventing victim infection. It is therefore not surprising that according to data collected by CPR, Emotet has impacted approximately 12% of all corporate networks globally.

In the first half of 2022, we saw the demise of a significant malware family—Trickbot. In our report, summarizing 2021, Trickbot claimed the first place in the global malware chart, with an impact of approximately 11% on all corporate networks. In February, the Banker-turned-Botnet's operators shut down their attack infrastructure, following months of inactivity, with no new campaigns observed by CPR in early 2022 after its delivery of Emotet.

Finally, Dridex, another prominent botnet, left the top chart for the first time in years. The botnet was originally developed as a credential-stealing malware utilizing malicious macros.

TOP MULTIPURPOSE MALWARE

GLOBAL

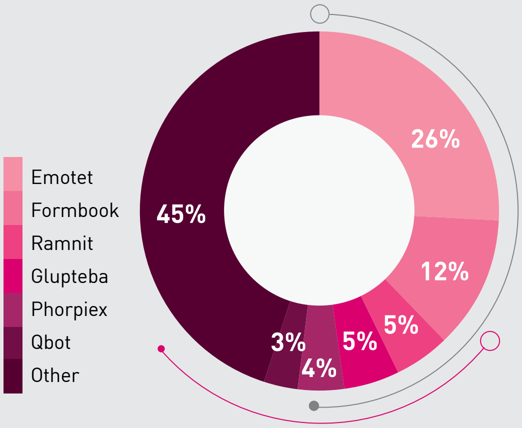


Figure 20: Most prevalent multipurpose malware globally

AMERICAS

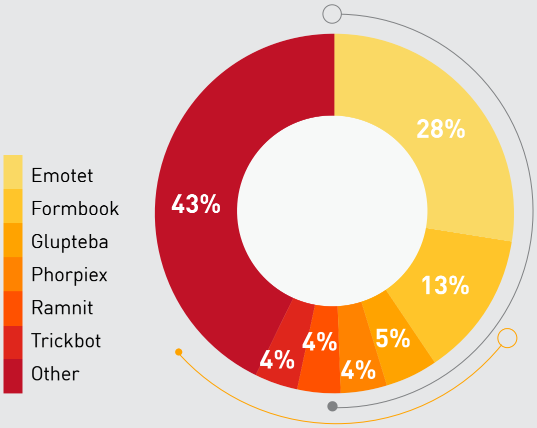


Figure 21: Most prevalent multipurpose malware in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

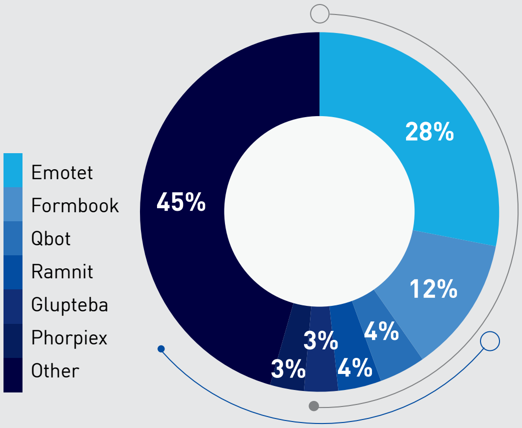


Figure 22: Most prevalent multipurpose malware in EMEA

ASIA PACIFIC (APAC)

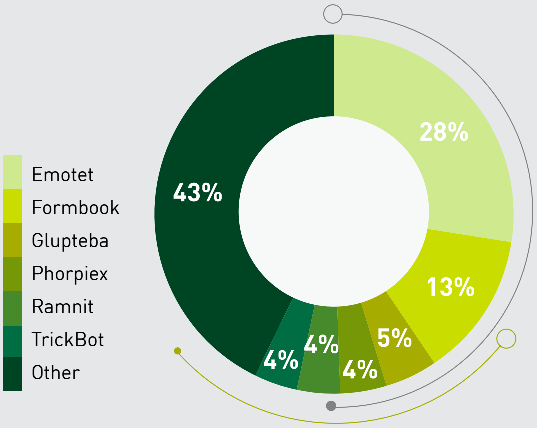


Figure 23: Most prevalent multipurpose malware in APAC

MULTIPURPOSE MALWARE GLOBAL ANALYSIS

We combined banking Trojans and botnets, previously classified as two distinct types into a single category. As many banking Trojans received additional functionalities, which makes the differentiation between the two categories less distinct, we introduce the unified category, "multipurpose malware."

In 2022, Glupteba is one of the most dominant multipurpose malware families in the wild, taking the 3rd place in the chart with involvement in approximately 5% of all corporate networks. This malware features a variety of capabilities including a rootkit, a router attack tool, a credential stealer, a crypto miner and more. However, Glupteba is best known for its unique use of the BitCoin blockchain technology as its C&C infrastructure to receive configuration information. Glupteba's high activity rate in 2022 is curious since in December 2021, Google carried out a takedown operation to put a halt to its attack activities.

The operation involved both legal and technical steps. First, the company, in collaboration with industry partners, disrupted key C&C infrastructure to halt the communications between the botnet operators and its infected bots. Glupteba's innovative C&C technology allows it to swiftly find an alternative C&C server by scanning the blockchain—composed of hundreds of thousands of servers daily taking part in BitCoin transactions—in case its current server is shut down. The technological complexity of the botnet's communication method led Google to incorporate legal steps into the operation. The company took part in a civil lawsuit against the alleged operators of the blockchain-enabled botnet. Despite the large-scale operation, in March 2022 a new massive campaign involving Glupteba and Trickbot was observed by researchers. The campaign targeted MikroTik routers and was designed to form a botnet-as-a-service infrastructure.

TOP INFOSTEALER MALWARE

GLOBAL

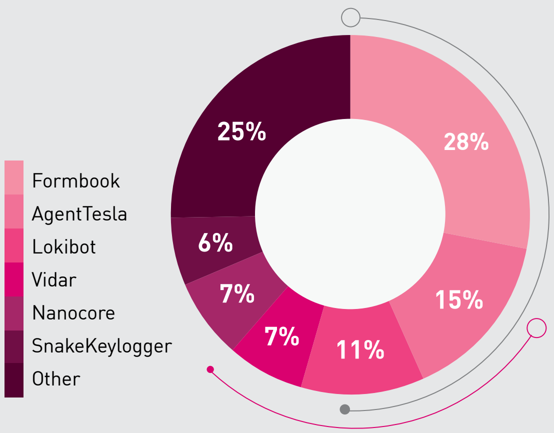


Figure 24: Top infostealer malware globally

AMERICAS

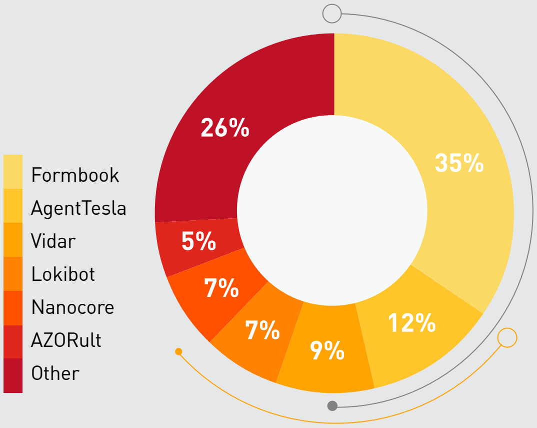


Figure 25: Top infostealer malware in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

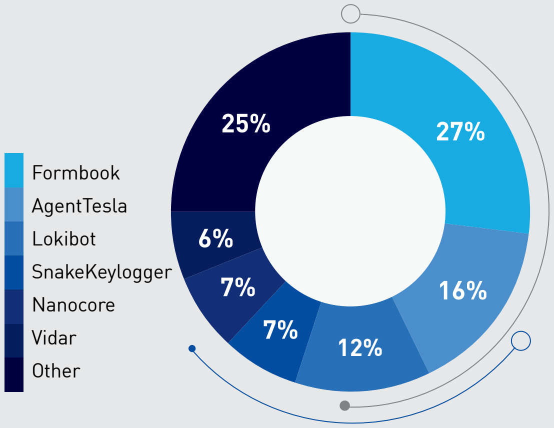


Figure 26: Top infostealer malware in EMEA

ASIA PACIFIC (APAC)

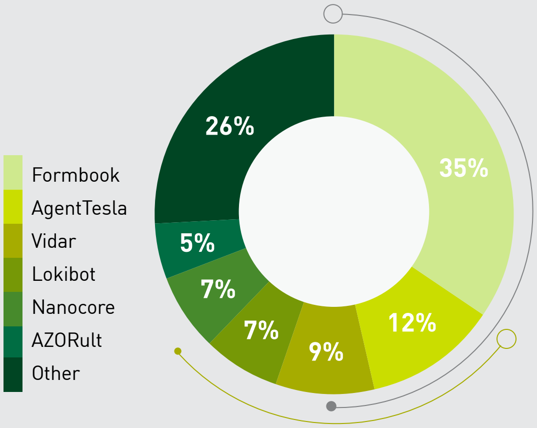


Figure 27: Top infostealer malware in APAC

INFOSTEALER MALWARE GLOBAL ANALYSIS

Still topping the chart is **Formbook**, a commodity infostealing malware sold as-a-service on underground forums since 2016 and is designed to collect information via keylogging. In March, a malicious campaign involving Formbook was found to be targeting Ukrainians with spams, luring victims with fake funding approval letters from the government. Shortly afterwards in April, CPR detected a peak in Formbook's activity.

The **Snake Keylogger** modular .NET keylogger/infostealer is a first-time entrant in our chart. Snake first surfaced around late 2020, and quickly grew in popularity among cyber criminals. Snake's main functionalities include recording keystrokes, taking screenshots, harvesting credentials and clipboard content, in addition to supporting exfiltration of the stolen data by both HTTP and SMTP protocols. It is usually spread through emails that contain DOCX or XLSX attachments with malicious macros. However, in May researchers reported that Snake Keylogger was spreading through PDF files. This could be due in part to Microsoft blocking by default internet macros in Office, compelling cybercriminals to explore new file types such as PDFs.

Finally, we note that the popular **Raccoon** stealer left the ranks. A report in March stated that a key member of the malware as-a-service operation was possibly affected by the conflict in Eastern Europe, and temporarily suspended all activities. Nevertheless, Raccoon resurfaced in June with the newly developed Raccoon Stealer V2 integrating improvements and new features.

TOP CRYPTOMINING MALWARE

GLOBAL

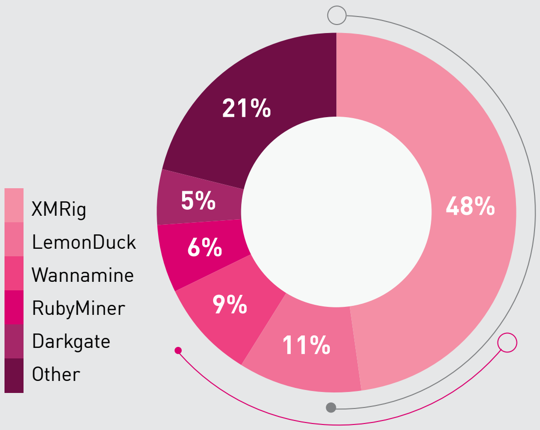


Figure 28: Top cryptomining malware globally

AMERICAS

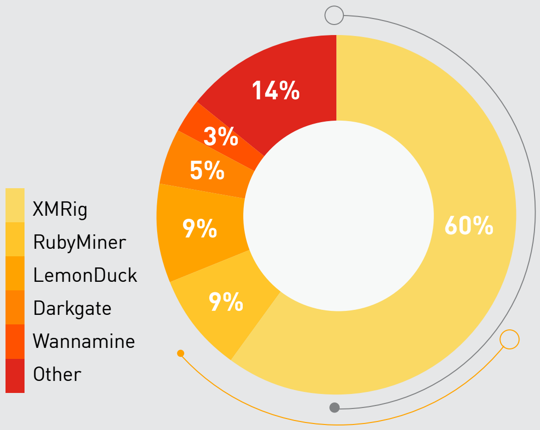


Figure 29: Top cryptomining malware in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

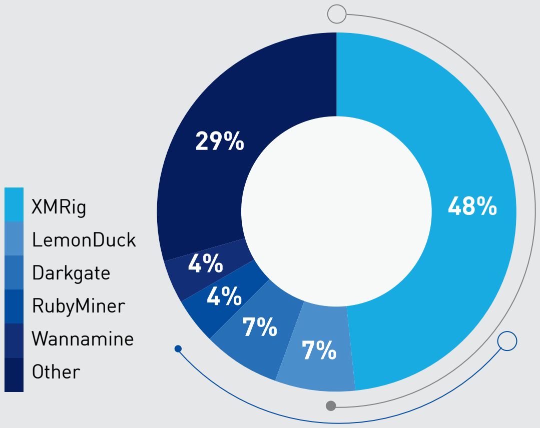


Figure 30: Top cryptomining malware in EMEA

ASIA PACIFIC (APAC)

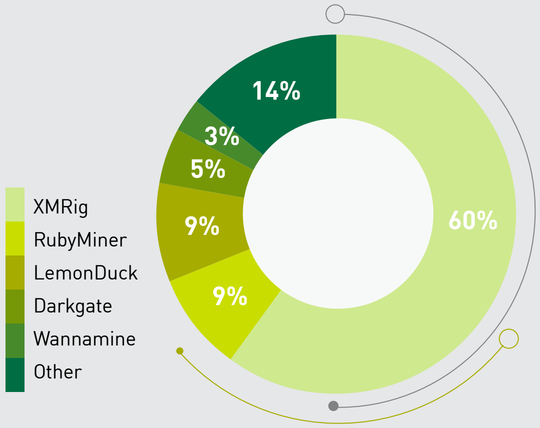


Figure 31: Top cryptomining malware in APAC

CRYPTOMINERS GLOBAL ANALYSIS

The crypto market saw a drastic decrease of value in H1, losing nearly $2 Trillion, from a record $2.9T market cap in November 2021. Low crypto rates affect mining profitability and with it the motivation for cryptomining. This explains cryptominers' visibility decreasing from 21% in 2020, 19% in 2021 globally. However, the hierarchy among the different types remained the same. XMRig, a legitimate open-source mining tool that is used by attackers for malicious purposes, remains the most common tool for unauthorized mining. LemonDuck, a relatively new cryptomining malware which has no legitimate use, also has extensive malicious functionalities including credential stealing and lateral movement. As Lemonduck is equipped with the ability to drop additional tools for human-operated attacks, its detection should be treated seriously as a precursor for severe attacks.

TOP MOBILE MALWARE

GLOBAL

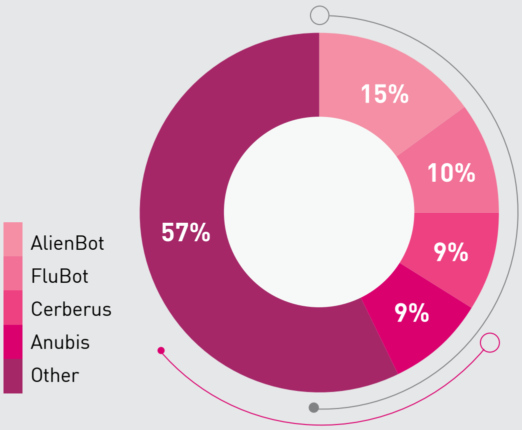


Figure 32: Top mobile malware globally

AMERICAS

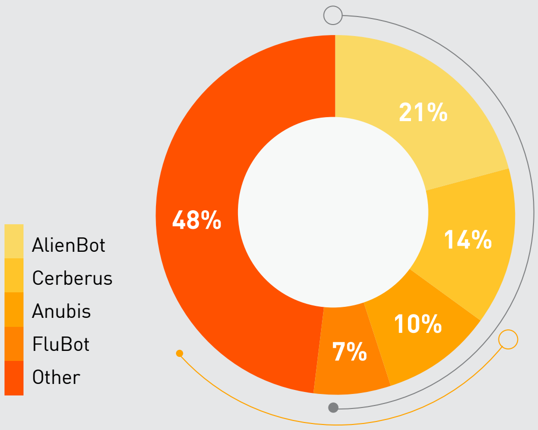


Figure 33: Top mobile malware in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

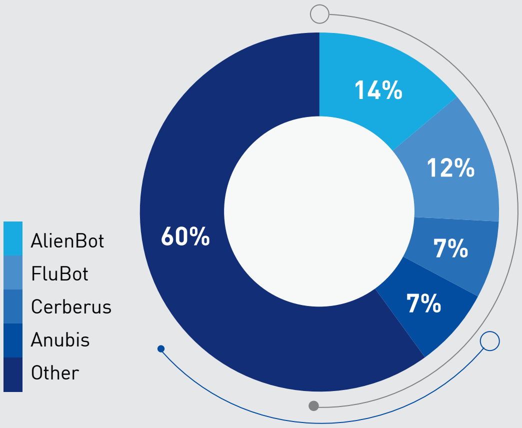


Figure 34: Top mobile malware in EMEA

ASIA PACIFIC (APAC)

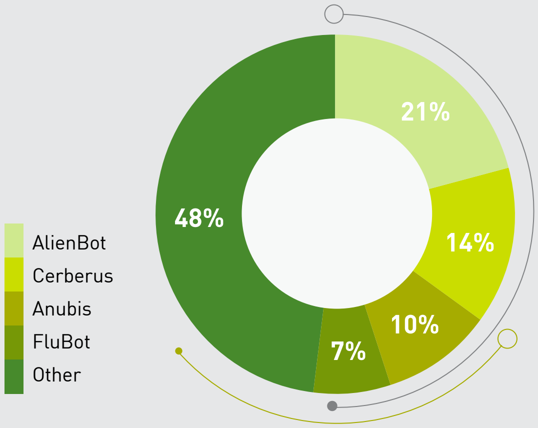


Figure 35: Top mobile malware in APAC

MOBILE MALWARE GLOBAL ANALYSIS

AlienBot, a banking Trojan for Android sold underground as Malware-as-a-Service (MaaS), has taken over the top of the chart. This Trojan supports keylogging and dynamic overlays for credential theft, as well as SMS harvesting for Two-Factor Authentication (2FA) bypass. In addition, AlienBot could gain remote control capabilities by abusing legitimate TeamViewer modules.

FluBot, another Android banking malware, started to emerge in late 2020 spreading via "Smishing" (SMS Phishing). It uses SMS messages as the attack vector for malware distribution and sends the same SMS to all of the initial victim's contacts, generating exponential spread. In January, the malware re-emerged in a new campaign leveraging Adobe Flash Players fake updates to steal banking credentials. FluBot eventually gained a lot of attention, and in June, an international law enforcement operation involving 11 countries led to its infrastructure takedown, rendering the malware inactive.

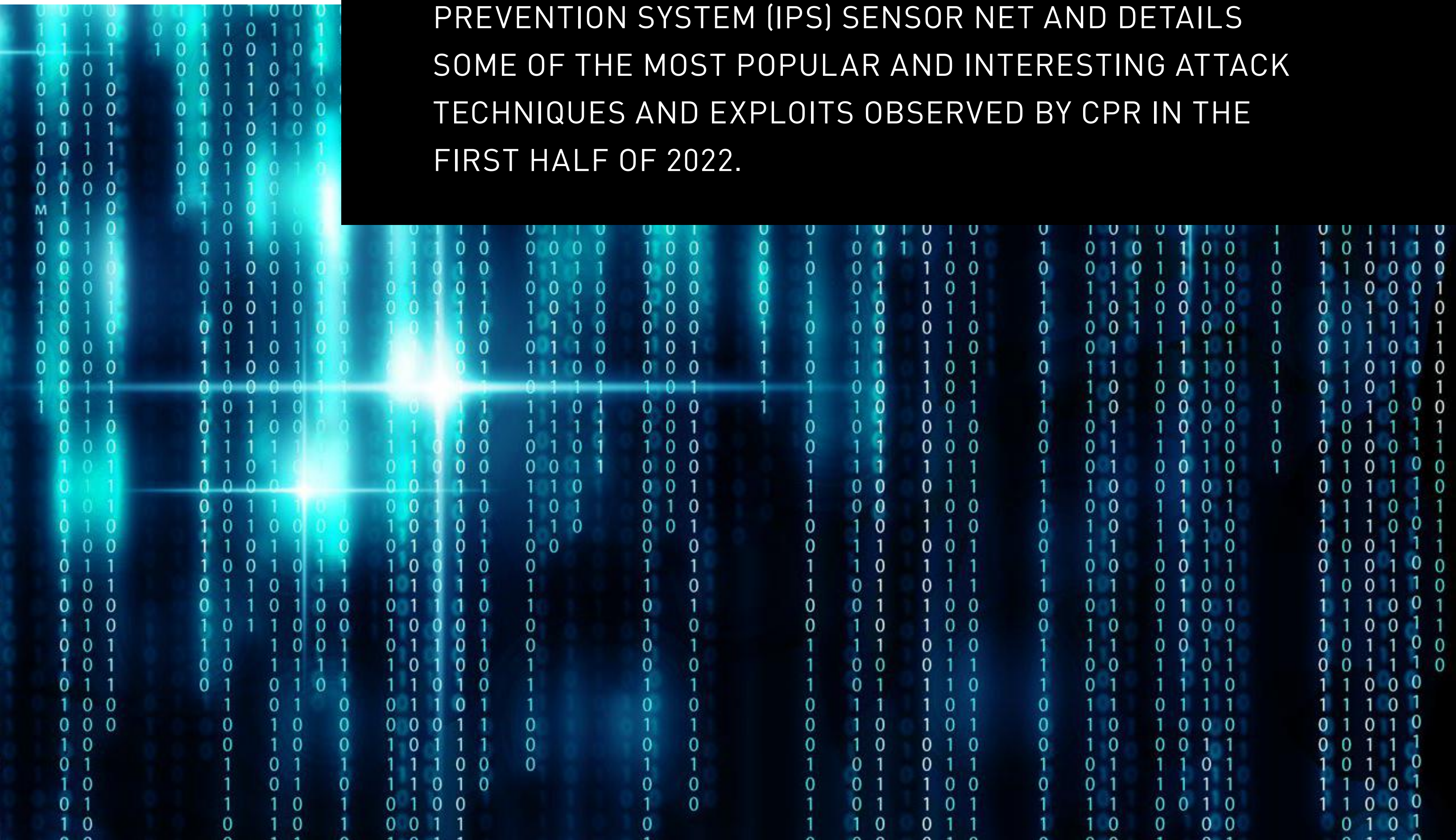
Lastly, **Cerberus**, first seen in the wild in June 2019, is a Remote Access Trojan (RAT) with specific banking screen overlay functions for Android devices. Cerberus has been operating as Malware-as-a-Service (MaaS) and its features include SMS control, key-logging, audio recording, location tracking, and more. This well-known malware is so widespread partly due to the availability of its source code, which was leaked in a failed auction in 2020, offering threat actors the possibility to customize their own versions.

CHAPTER 6

06

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 CPR IN THE FIRST HALF OF 2022.



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 CPR in the first half of 2022.

ATLASSIAN CONFLUENCE—REMOTE CODE EXECUTION (CVE-2022-26134)

The critical remote code execution vulnerability was reported in May 2022 to Atlassian following its in-the-wild discovery as a zero-day. Affecting all supported versions of Confluence Server and Data Center, it was characterized as an Object-Graph Navigation Language (OGNL) injection vulnerability that could lead to execution of arbitrary code by an unauthenticated actor, resulting in the targeted system's takeover. Although Atlassian released fixes in early June, since its discovery the vulnerability has become very popular, and was adapted by a wide range of threat actors to deploy backdoors, ransomware, cryptominers and botnets to vulnerable networks. Volexity, who first discovered the vulnerability, reported that Chinese affiliated attackers were leveraging this exploit on vulnerable servers to deploy web shells, as an initial foothold into targeted organizations. According to CPR, attacks relating to this vulnerability affected approximatively 14% of organizations worldwide.

'LOG4SHELL' APACHE LOG4J REMOTE CODE EXECUTION VULNERABILITY CVE-2021-44228

Apache Log4j is an open-source Java-based logging package provided by the Apache Software Foundation and is used by millions of Java-based applications worldwide to record activities. In late 2021, the Apache Foundation released an emergency Log4j version to address a critical flaw in the logging framework that enables threat actors to compromise a machine by simply sending it a simple string. Called 'Log4Shell', the vulnerability took the security community by storm, due to the magnitude of its influence—millions of companies, including Tesla, Amazon and Apple, use Log4j. Numerous attacks were observed and during 2022 Log4Shell remained one of the most highly exploited vulnerabilities. The vulnerability's simplicity and reach attracted both low-skilled and advanced threat groups. Iranian-aligned APT35 exploited Log4Shell to distribute a new and modular PowerShell toolkit, and China-based threat group Deep Panda used Log4Shell to exploit vulnerable VMware Horizon servers.

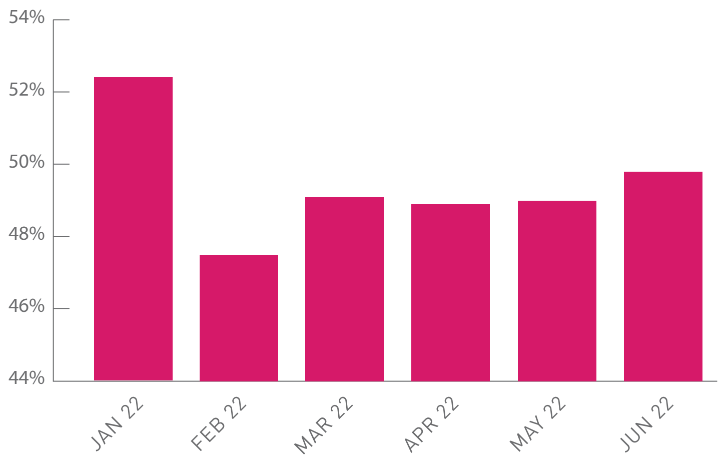


Figure 36: Log4Shell globally affected organizations over time.

F5 BIG IP (CVE-2022-1388)

CVE-2022-1388 is a Remote Code Execution (RCE) vulnerability (9.8 CVSS score) initially published by F5 on May 4. The vulnerability affects the BIG-IP line of products; in less than a week, multiple threat actors began to massively exploit it to drop malicious payloads to thousands of exposed systems. By May 18, CISA published an additional alert, warning that PoC publications enabled "less sophisticated actors" to exploit the vulnerability.

Other attackers refrained from using unpatched F5 BIG-IP devices to gain their initial foothold in organizations, and instead chose a path of destruction, sending the notorious "rm -rf /*" command which erased most of the data on vulnerable devices, including essential configuration data.

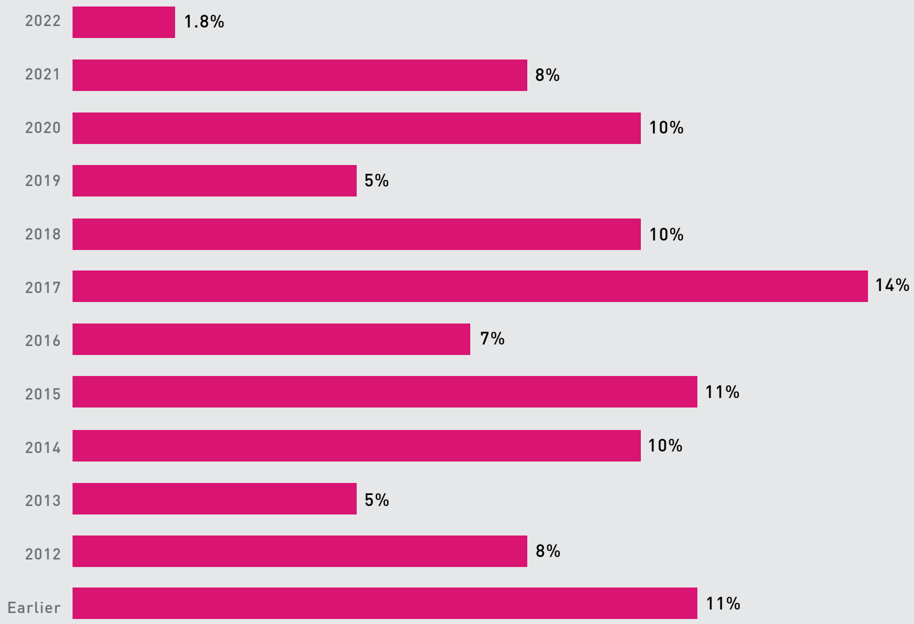


Figure 37: Percentage of attacks leveraging vulnerabilities by disclosure year in the first half of 2022.

Many vulnerabilities discovered in 2017 maintained a strong presence throughout 2022, similar to their behavior in 2021. This is mostly due to popular flaws like the Apache Struts2 Remote Code Execution (CVE-2017-5638) which is used by botnets, or the PHPUnit remote code execution (CVE-2017-9841), often used to exploit vulnerable WordPress plugins. According to the chart above, vulnerabilities disclosed in 2021-2022 were only exploited in 9.8% of the attacks leveraging vulnerabilities observed by CPR. However, information collected by the Check Point Incident Response Team (CPIRT) and shared in the current report allows us to examine the age of vulnerabilities used in **successful** attacks—not only attack attempts prevented by Check Point products—and draw our conclusions.

According to CPIRT, the most common vulnerability observed in the first half of 2022, used in no fewer than 69% of the cases, is the ProxyShell vulnerability chain (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) disclosed in August 2021. This piece of data demonstrates that while attackers heavily exploit 4-5 year old vulnerabilities, successful attacks often rely on newly discovered flaws, probably before the organizations patched its vulnerable servers. The data also shows that older vulnerabilities are constantly exploited – most likely by low-skilled attackers and with much lower success rate. These findings once again highlight the importance of timely system patching.

CHAPTER 7

07 TOP ATTACKS AND CYBER BREACHES H1 2022

IN THE FIRST HALF OF 2022, CYBER ATTACKS AND MAJOR CYBER BREACHES CONTINUED TO BE A MAJOR THREATS TO ORGANIZATIONS IN ALL SECTORS AND ALL REGIONS.

TOP ATTACKS AND CYBER BREACHES H1 2022

In the first half of 2022, cyber attacks and major cyber breaches continued to be a major threats to organizations in all sectors and all regions, putting the sensitive information of billions of people at risk, and disrupting societies worldwide.

Below is a recap of the major attacks and breaches in each region.

AMERICAS

JANUARY

- The Florida based healthcare provider Broward Health has suffered a significant breach impacting over 1.3 million individuals, in which cyber criminals gained access to patients' medical information.
- Albuquerque US Public Schools have had to cancel classes after they were hit by a cyber-attack that compromised the student information system. This event follows a ransomware attack that impacted multiple government services across Bernalillo County on January
- The cryptocurrency exchange platform Crypto.com has announced that 483 user accounts were compromised in a recent hack, resulting in $35 million worth of unauthorized withdrawals.

FEBRUARY

- Check Point Research has discovered a new implementation of the Trickbot banking Trojan. CPR counts over 140,000 machines infected by Trickbot since November 2020, as the threat actors try stealing credentials to financial and other services provided by 60 well-known corporations, including Amazon, Microsoft, Google and PayPal.
- The FBI has announced that the BlackByte ransomware gang successfully broke into US critical infrastructures networks from several organizations in the past three months.
- Following an announcement by OpenSea about a contract migration they are planning, Check Point Research observed that hackers took advantage of the upgrade process and scammed NFT users, leading to theft of millions of dollars.
- US based chipmaker Nvidia has been hit by a cyber-attack impacting their developer tools and email systems. It is claimed that the cyber criminals were hacked back, encrypting the data they had stolen.

MARCH

- State-sponsored APT41 group (aka Wicked Panda) affiliated with China has been successfully breaching into US government networks for the past 6 months by exploiting vulnerable web facing applications. Vulnerabilities included Log4Shell and a zero-day flaw in the USAHerds app tracked CVE-2021-44207.
- Check Point Research reveals how hackers performed flash loan attacks to claim free tokens on ApeCoin Cryptocurrency, fraudulently earning millions of dollars.
- Morgan Stanley customer accounts have been breached in social engineered attacks, which were the result of Vishing schemes. Hackers successfully transferred money to their own bank accounts.

APRIL

- A bug in Palo Alto Networks customer support tickets exposed information belonging to thousands of customers.
- CISA and the US Department of Energy released a joint warning of attacks against internet-connected uninterruptible power supply (UPS) devices utilizing default usernames and passwords. Organizations can mitigate such attacks by removing management interfaces from the internet.

- Check Point Research shows that 16% of the organizations worldwide were impacted with Spring4Shell during the first 4 days after the vulnerability outbreak. VMware has released security updates to address this critical remote code execution flaw within its products.
- The FBI has issued a warning addressed to the Food and Agriculture (FA) organizations on the greater risks of ransomware attacks during the harvest and planting periods.
- CISA, the FBI and the US Treasury Department alert on the North Korean APT group Lazarus targeting companies in the blockchain and cryptocurrency sectors, using social engineering on employees.

MAY

- A 15.3 million request-per-second DDoS attack was recorded by the internet infrastructure company Cloudflare, marking it one of the largest HTTPS DDoS attacks ever.
- FBI warns of BlackCat ransomware after that breached over 60 organizations worldwide.
- Costa Rica has declared a State of Emergency following a devastating ransomware attack by the Conti gang. The attack affected many governmental organizations, including The Finance Ministry, The Costa Rican Social Security Fund, and The Ministry of Science, Innovation, Technology, and Telecommunications. An estimated $200 million was lost due to disruptions related to the tax and customs platforms.
- Check Point Research reported how the Conti ransom group has taken cybercrime to a new, geopolitical level. They intervene in the internal politics of Costa Rica, the relationship between Costa Rica and the US, and basically moved the ransomware gangs to a new business stage of country extortion.

JUNE

- Costa Rica's public health service was attacked by Hive ransomware, which shut off their computer systems. The Hive ransomware group demanded $5 million in Bitcoin to unlock the infected servers. This attack can be related to the Conti ransomware attacks on this and other government-related entities.
- Researchers revealed a zero-day vulnerability in Microsoft Office that might enable remote code execution on a victim's machine. The vulnerability, dubbed "Follina", uses the remote template feature in Word to retrieve an HTML File from a remote server, and can execute a PowerShell by using an ms-msdt MSProtocol URI scheme.
- Researchers have revealed a major phishing scam targeting Facebook users through the company's Messenger app, in which 1M credentials were stolen in 4 months. The campaign peaked in April-May 2022 but has been active since at least September 2021.

CHAPTER 7

EUROPE, THE MIDDLE EAST AND AFRICA (EMEA)

JANUARY

- A series of attacks targeting Russia's Ministry of Foreign Affairs has been attributed to North Korean APT group Konni. Threat actors gained access by leveraging a socially engineered phishing campaign with New Year greetings and stealing credentials, aiming at collecting intelligence.
- Threat actors have been targeting the UK National Health Service (NHS) using the Log4Shell flaw to hack compromised VMWare Horizon servers, likely as a reconnaissance phase.
- Ukraine has been hit by a large scale cyber-attack that took down several of its government and ministries websites. Threat actors defaced the Foreign Affairs website with threatening message reading "Ukrainians!… All information about you has become public, be afraid and expect worse." Researchers additionally found evidence of a significant ongoing operation targeting multiple organizations in Ukraine, leveraging a malware disguised as ransomware that could render a system inoperable.
- A new cyber-espionage campaign by the Arabic-speaking APT group Molerats (aka Gaza Cybergang) has been targeting victims in the Middle East, specifically high-profile targets in the banking, NGOs and political sectors in Palestine and Turkey. The group leverages cloud services like Google Drive or Dropbox to host malicious payloads and for command-and-control.
- Hacktivist group from Belarus called "Belarusian Cyber Partisans" has breached the computers systems of Belarusian Railways. Threat actors claim to have encrypted the network and are extorting the Belarusian government, asking for the release of 50 political prisoners and a pledge from Belarussian Railways to halt transport of Russian soldiers as Russia prepares for a possible invasion of Ukraine.

FEBRUARY

- A significant Ransomware attack has disrupted operations of oil port terminals in Belgium, Germany and in the Netherlands, affecting at least 17 ports and resulting in difficulties loading and unloading refined product cargoes. The BlackCat cybercrime group is suspected to be the group behind the attack.
- Researchers have found a new campaign targeting Turkish private organizations and governmental institutions attributed to Iranian state sponsored group MuddyWater. The group now uses canary tokens to track targets' infection and possibly to evade sandbox-based detection systems.
- 200,000 people have been impacted by a data breach that exposed personal information of users of Croatian phone carrier A1 Hrvatska.
- Ukraine has been at the center of a series of targeted DDoS attacks on its armed forces, defense ministry, public radio and national banks websites. The US Government has officially attributed the attacks to Russia's Main Directorate of the General Staff of the Armed Forces.
- Check Point Research has released data on cyber attacks observed around the current Russia/Ukraine conflict. Cyber attacks on Ukraine's government and military sector surged by 196% in the first three days of combat. Cyber attacks on Russian organizations increased by 4%. Phishing emails in the East Slavic languages increased 7-fold.
- Check Point Research has spotted a new malware, Electron-bot, distributed through gaming applications on Microsoft's official store, with at least 5,000 victims, mostly in Sweden, Bulgaria, Russia, Bermuda and Spain. The malware can control social media accounts of its victims, including Facebook, Google and Sound Cloud. The malware can register new accounts, log in, comment on and "like" other posts

MARCH

- Check Point Research reports on cyber criminals' and hacktivists' increased activity leveraging Telegram amid the Russia-Ukraine war. Anti-Russian cyber-attack groups have been growing, while others claiming to fundraise for Ukraine are suspected to be fraudulent.
- Ukraine "IT army" consisting of cyber-operatives and volunteers worldwide has claimed attacks taking down multiple Russian and Belarusian key websites, including the Kremlin's official site.
- Swedish camera company Axis has had to shut down all its public-facing internet services after a cyber-attack targeted its IT systems.

- TransUnion South Africa has been victim of a breach in which the hacker group named N4aughtysecTU stole 4TB of data. Attackers who claim to be based in Brazil are demanding a $15 million ransom over the sensitive data which includes credit score, banking details and ID numbers.
- One of Russia's largest meat producers Miratorg Agribusiness Holding has suffered a major cyberattack. Threat actors used Windows BitLocker to encrypt the victim's IT systems in full volumes and demanded a ransom. The attack resulted in distribution disruptions for several days.
- German wind turbine company Nordex has been victim of a cyberattack claimed by the Conti ransomware gang. The attack, which occurred on March 30, shut down all the company's internal IT systems and disrupted their remote access to the turbines.

APRIL

- Check Point Research (CPR) revealed a large spike in attacks committed by advanced persistent threat groups (APTs) around the world, using lures utilizing the war between Russia and Ukraine. Most of the attacks started with spear-phishing emails that contained documents with malicious macros dropping malware such as Loki.Rat backdoor.
- Check Point Research discovered six applications spreading banking malware on Google Play Store by masquerading as anti-virus solutions, with over 15,000 downloads. The malware, known as 'Sharkbot', steals credentials and banking information of Android users.

MAY

- The Ukrainian IT army has disrupted Russia's alcohol distribution by performing DDoS attacks to limit access to a portal called State Automated Alcohol Accounting Information System (EGAIS) used by the Russian government.
- The National Health System (NHS) in the UK has been a victim of a phishing campaigns targeting email accounts since at least April 2022. More than a thousand phishing messages were sent from two NHS IP addresses, delivered from hijacked email accounts belonging to 139 employees in England and Scotland.

- Check Point Research has unveiled a targeted cyber-espionage operation against at least two research institutes in Russia, which are part of the Rostec Corporation, a state-owned defense conglomerate. The sophisticated campaign, which CPR dubbed "Twisted Panda", has been attributed to Chinese threat actors, with possible connections to Mustang Panda and Stone Panda (aka APT10). Hackers used new tools, including a multi-layered loader and a backdoor called "SPINNER".
- Russian state-sponsored hacking group, Turla, has been launching a reconnaissance campaign against the Austrian Economic Chamber, a NATO platform, and the Baltic Defense College.

JUNE

- FluBot, the notorious mobile malware threat that spreads globally mainly via SMS-based phishing, has been taken down in a joint law enforcement operation—Europol announced.
- The Italian municipality of Palermo has been victim of a ransomware attack that caused a large-scale service outage affecting over a million people. The attack was claimed by the Vice Society ransomware group, which used the double extortion ransomware.

ASIA-PACIFIC (APAC)

JANUARY

- The Vietnamese trading platform ONUS was victim of a ransomware attack leveraging the Log4j flaw on its payment system. Cyber criminals demanded a $5 million ransom in a double extortion scheme. ONUS refused to pay, so threat actors published for sale records of 2 million ONUS costumers.
- A new password stealing malware dubbed BHUNT has been targeting crypto wallets worldwide, most victims being in India. BHUNT is suspected to be using cracked software installers as an infection vector.
- Delta Electronics, a Taiwanese Apple and Tesla contractor, has been hit by a Conti Ransomware attack. The company stated that only non-critical systems were compromised. Ransomware operators demanded a $15 million ransom payment in exchange for the decryption key.

FEBRUARY

- Researchers have discovered that North Korean APT group Kimsuky has been active in campaigns involving commodity open-source remote access tools dropped with their custom backdoor, Gold Dragon. Their latest campaign is primarily focused on South Korean targets.

MARCH

- Ransomware gang Lapsus$, which took responsibility for last week's breach on the giant chip firm NVIDIA, claims it has now managed to breach the Korean manufacturer Samsung, and published 190GB of sensitive data online.
- Japanese car manufacturer Toyota has halted their operations and productions in its plants across Japan after one of its plastic component suppliers Kojima Press Industries suffered a cyber-attack.

APRIL

- The Pakistan-based threat group APT36 conducted a new campaign against the Indian government. The group used the laced Kavach authentication apps, which are used by the Indian military and other government agencies to access critical IT systems.
- The new Spring4shell vulnerability (CVE-2022-22965) has been actively exploited by threat actors since the beginning of April, leveraging the Mirai botnet. The Singapore region has been one of the most impacted geographic area.
- North Korean state-sponsored APT group Lazarus has been linked to a recent theft of $625 million worth in Ethereum cryptocurrency in the Axie Infinity game.

MAY

- The Japanese financial news outlet Nikkei Group has suffered a ransomware attack that hit its headquarters in Singapore. The company, which is still in the process of determining the scope of the attack, claims that no data was leaked although the affected server may have contained customer data.
- Indian airline SpiceJet has been the victim of a ransomware attack that resulted in delayed flight departures and underlying system failures. The company announced that the attack is also delaying its financial results announcement.

JUNE

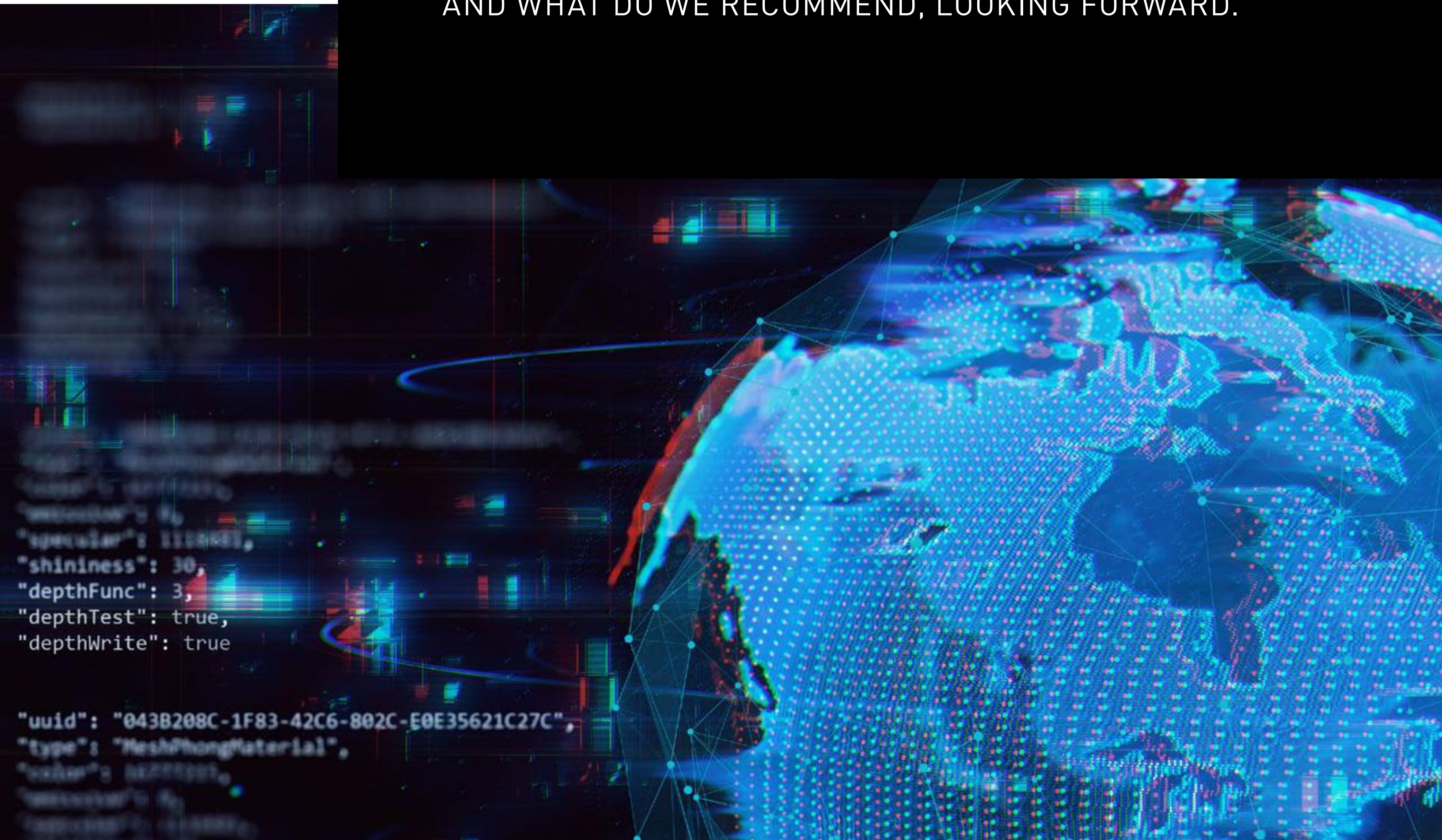
- Check Point Research found a vulnerability within the UNISOC chip firmware used in Android mobile phones, which can allow a remote attacker to disrupt the device's radio communication through a malformed packet.
- A Critical vulnerability affecting Atlassian Confluence and Data Center servers (CVE-2022-26134), exploited in the wild, has been patched. Successful exploitation could allow remote attackers to create new admin accounts, execute commands, and take over the server.

CHAPTER 8

08

H2 2021: WHAT TO EXPECT AND WHAT TO DO

TOP CYBER PREDICTIONS FOR H2 2022 WHAT DO WE SEE AND WHAT DO WE RECOMMEND, LOOKING FORWARD.



PREDICTIONS FOR H2 2022: WHAT TO EXPECT AND WHAT TO DO

We are just over half-way through 2022 and already we have seen huge defining events in the cyber landscape, from the Russia-Ukraine war, state-sponsored attacks and hacktivism to Conti's ransomware attacks on the entire countries of Costa Rica and Peru, not to mention multi-million-dollar incidents, thefts and scams in crypto. So, what can we expect looking forward?

- **Ransomware will become a much more fragmented ecosystem**—there will be a lesson learned from the Conti ransomware group. Its size and power garnered too much attention and became its downfall. Going forward, we believe there will be many small-medium groups instead of a few large ones, so that they can go under the radar more easily.
- **More diverse email infection chains**—due to the implementation of internet macros being blocked by default in Microsoft office, the more sophisticated malware families will accelerate the development of new infection chains, with different file types than just the regular Office files. They will also password protect them to make detection more difficult. It's important that users are well aware of sophisticated social engineering. Cybercriminals will often send a simple email impersonating someone you know just to get into conversation with you and gain trust before then sending a malicious file.
- **Hacktivism will continue to evolve**—hacktivism was really brought to the fore in H1 2022 and we expect hacktivist groups will continue to align their attacks with the agenda of their nation state throughout the rest of the year, particularly as the Russia-Ukraine war is still ongoing.
- **Continued attacks on blockchain and crypto platforms**—so far this year we have found major incidents relating to blockchain platforms, such as vulnerability in the Everscale wallet. With blockchain technology still being so new, cybersecurity is only in the early stages of understanding its full scope and so we expect there to be more vulnerabilities, breaches and crypto attacks in the second half of 2022.
- **The first attacks in the Metaverse**—the Metaverse is built on the blockchain and due to the amount of malicious activity we already see there, we believe it won't be long before we start to see initial attacks in the Metaverse too. It will likely be based on authorization and user accounts will get hijacked.

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.

- **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.

- **Be wary of requests to sign links within any marketplace.** To prevent the theft of crypto keys and wallets, be wary whenever receiving a request to sign links within marketplaces. Prior to approving a request, carefully review what is being requested and consider whether it seems abnormal or suspicious. If there are any doubts, you should reject it. Token approvals can be reviewed and revoked using this link: https://etherscan.io/tokenapprovalchecker.

CHAPTER 09

09 INCIDENT RESPONSE PERSPECTIVE

CYBER-ATTACKS CONTINUE TO GROW GLOBALLY AT AN ALARMING RATE—IN VOLUME, SOPHISTICATION, AND IMPACT.

INCIDENT RESPONSE PERSPECTIVE

Unlike the analyses and trends discussed in previous chapters of this report, which are based on Check Point products anonymized data collected during routine preventative protection, this chapter offers the unique perspective of the Check Point Incident Response Team (CPIRT). CPIRT provides attack mitigation services in response to various types of active breaches and its work is vendor-agnostic, not exclusive to CP customers.

The CPIRT response usually follows the discovery of visible malicious activity, such as encrypted files (ransomware); malicious activity detected on mail servers; emails received without the knowledge of their sender (email compromise), or the presence of malware files or unknown processes on a computer system.

Sometimes the discovery is due to extensive malicious activity, affecting most of the critical assets in the organizational infrastructure (full network compromise). In some cases, the malware is discovered when the victim receives a ransom demand as part of a data leak that is followed by an extortion.

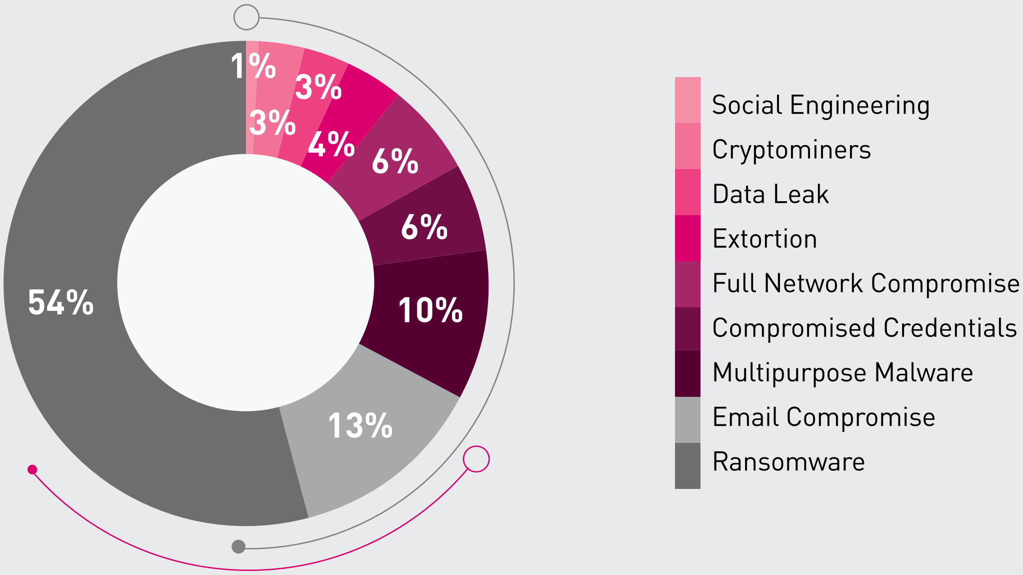


Figure 38: Breakdown of CPIRT cases by initial threat indication.

The threat breakdown above is very different from what we routinely see in our product data. An analysis of cyber-attacks in the wild shows the top threats are multipurpose malware and cryptominers. However, CPIRT data shows that the actual risks—from a large corporate perspective—are full-blown ransomware attacks and full network compromises. Event logs that record multipurpose malware activity often just show the initial incursion. The more significant damage caused by cyber breaches is from extortion following encryption or data exfiltration, and various scams and BECs (business email compromise) conducted through various account takeovers.

Conti, Hive and Phobos are the most common ransomware families we have encountered in the analyzed period, but they are not responsible for the majority of attacks. Seventy-two percent of ransomware cases involved a ransomware family we encountered only once. This suggests that contrary to some assumptions, the ransomware landscape is not dominated by only a few large groups but is actually a fragmented ecosystem with multiple smaller players that are not as well-publicized as the larger groups. Some strategies are shared by different actors; in approximately 40% of ransomware cases, the attackers succeeded in compromising the victim's systems a month or more before they started encrypting the files. The time in between was spent scouting the victims' networks in search of valuable assets.

Judging from our protection sensors, we have witnessed a growing tendency to use SMTP (over Web) as the initial attack vector, which reached a record 89% of **attempted** attacks in the first half of 2022. CPIRT analysis reveals that from **successful** attacks with a known initial entry vector, vulnerable servers are the most common vector leading to compromise.

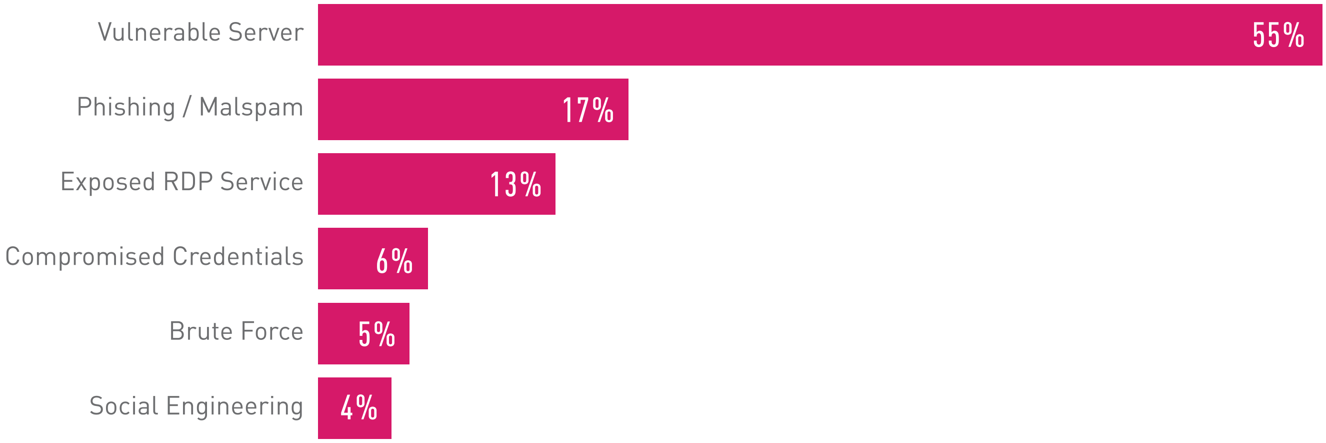


Figure 39: Breakdown of initial entry vector.

The most widespread infection vector observed by CPIRT is the exploitation of vulnerable servers with exposed ports. These are mostly one-day vulnerabilities, which grant the attacker remote code execution options on some of the most valuable servers in the organization. This means that although the most frequent attack vector in the wild is SMTP, often mass-distributed by actors of various sophistication levels, the most effective attacks repeatedly rely on unpatched vulnerabilities.

The most common vulnerability of the first half of 2022, used in 69% of the cases (where the initial infection vector is known), are the ProxyShell vulnerabilities, first reported in August 2021. ProxyShell is the name given to the exploitation of a chain of vulnerabilities (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) in Microsoft Exchange servers.

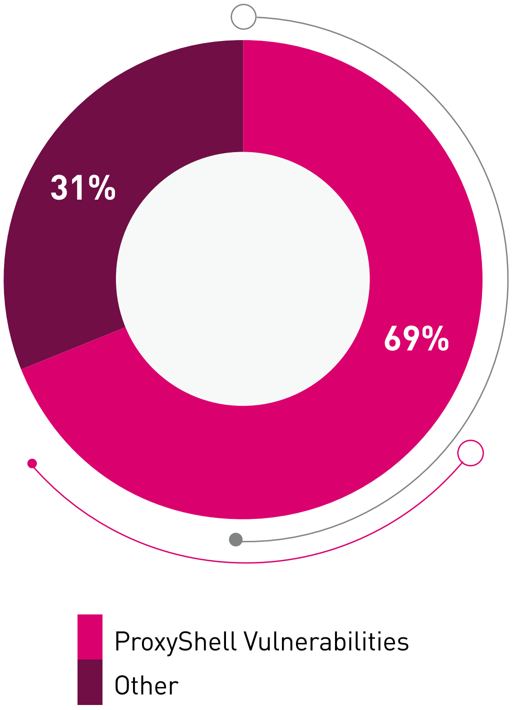


Figure 40: ProxyShell vs other vulnerabilities as infection vectors.

DANIEL WILEY

Head of Threat Management and Chief Security Advisor

> “This finding portrays a different perspective from the one we get by analyzing Check Point product data. Although fewer than 10% of the CVEs used in attacks in the first half of 2022 are new vulnerabilities reported in the past year (see figure 32—Percentage of attacks leveraging vulnerabilities by disclosure year in H1 2022), they make up the majority of effective attacks".

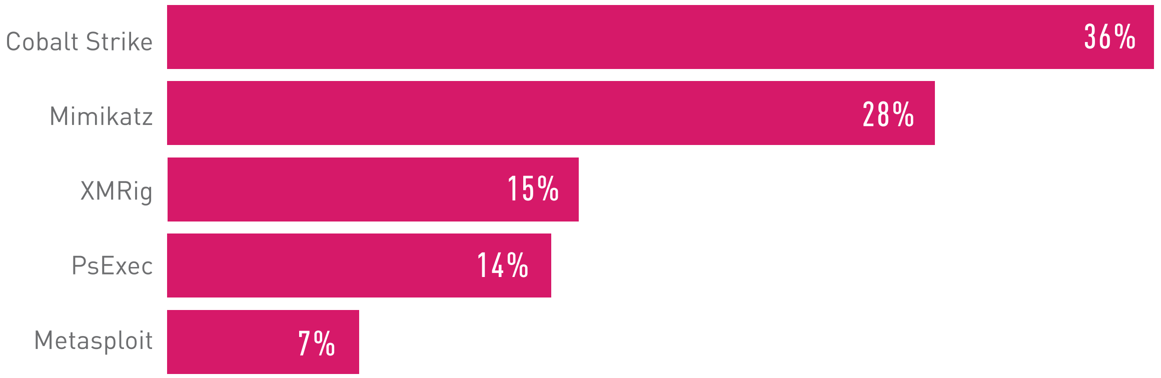


Figure 41: Tools used on compromised systems.

In many cases the exploitations occurred months before they were discovered by the victim. Even though some of the organizations who were attacked have since patched their environment, their systems were already under the control of threat actors by the time the exploit was discovered. Although the majority of attacks attempt to leverage old vulnerabilities, it is crucial to patch and provide up-to-date protections for the most recently discovered CVEs.

Threat actors deploy a wide variety of tools in an attack. Some of these have only illicit uses, such as password stealing tools which serve only as malware. In other cases, hackers abuse otherwise legitimate tools, such as remote-control software.

Cobalt Strike Beacon is the most popular tool used by attackers. Its purpose is to establish a secure C2 communication with the attacker infrastructure. Another common tool is Mimikatz, which is used for password stealing and privilege escalation in the network.

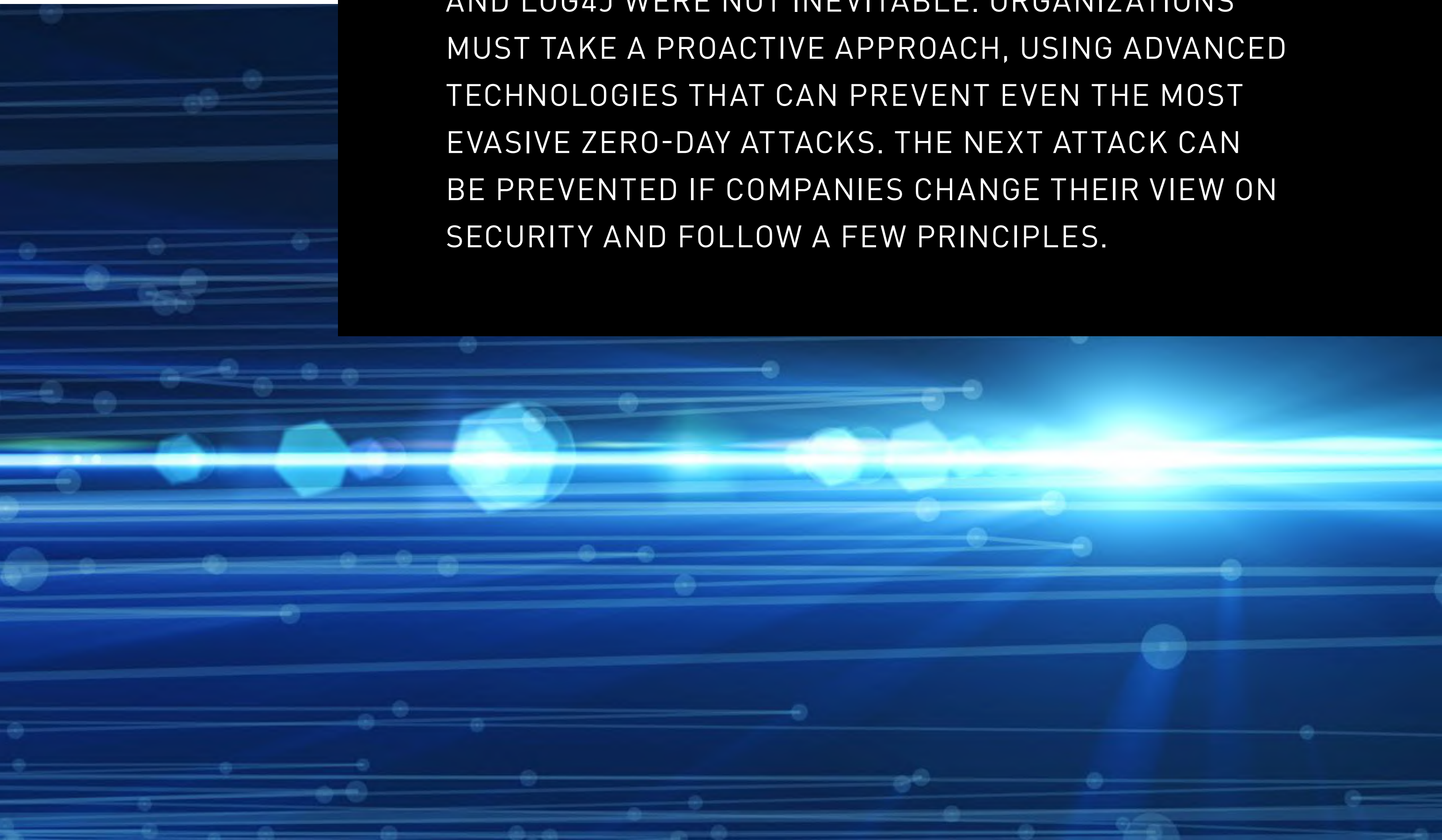
Cryptominers are often installed at an initial stage to start generating profit. Attackers can later leverage their access to the network for other revenue-generating activities. This strategy is often used in non-targeted attacks, where the attacker might put less effort into stealth activity.

CPIRT data, collected from cases of compromised systems, gives a different perspective from our regular product data analyses. It emphasizes the dangers of full-blown cyber-attacks, those that can develop when preliminary incursions like infostealers and cryptominers are disregarded as only minor threats. The importance of regularly updated cyber security systems, that quickly integrate protections for reported vulnerabilities and changing attacks, is evident in light of this data. From the minute a CVE is revealed until a protection is released and deployed, every minute matters.

CHAPTER 10

10
PREVENTION OF THE NEXT ATTACK IS POSSIBLE

THE IMPACTS OF MEGA CYBERATTACKS LIKE SOLARWINDS AND LOG4J WERE NOT INEVITABLE. ORGANIZATIONS MUST TAKE A PROACTIVE APPROACH, USING ADVANCED TECHNOLOGIES THAT CAN PREVENT EVEN THE MOST EVASIVE ZERO-DAY ATTACKS. THE NEXT ATTACK CAN BE PREVENTED IF COMPANIES CHANGE THEIR VIEW ON SECURITY AND FOLLOW A FEW PRINCIPLES.



PREVENTING THE NEXT CYBER ATTACK IS POSSIBLE

Cyber-attacks continue to grow globally at an alarming rate—in volume, sophistication, and impact. In this era of super-powered cybercrime, the need to protect organizations from advanced attacks is more critical than ever before. Companies must use pioneering technologies in order to remain protected. The impacts of mega cyber-attacks like SolarWinds and Log4J were not inevitable. With the correct measures and technologies in place, many organizations could have avoided the impact and devastating effect of such attacks. In order to truly combat the next threats, organizations must take a proactive approach, using advanced technologies that can prevent even the most evasive zero- day attacks.

The next attack can be prevented if companies change their view on security, and follow a few principles.

PREVENTION OVER DETECTION

Traditional cybersecurity vendors often claim that attacks will happen, and there's no way to avoid them, and therefore the only thing left to do is to invest in technologies that detect the attack once it has already breached the network, and mitigate the damages as soon as possible.

This is untrue. Not only can attacks be blocked, but they can be prevented, 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.

KEEP YOUR THREAT INTELLIGENCE UP-TO-DATE

In the constant fight against malware, threat intelligence and rapid response capabilities are vital. Keeping your business up and running with comprehensive intelligence to proactively stop threats, manage security services, to monitor your network and incident response to quickly respond to and resolve attacks.

Malware is constantly evolving, making threat intelligence an essential tool for almost every company to consider. When an organization has financial, personal, intellectual, or national assets, a more comprehensive approach to security is the only way to protect against today's attackers. And one of the most effective proactive security solutions available today is threat intelligence.

MAINTAIN SECURITY HYGIENE

Patching

All too often, attacks are able to penetrate defenses by leveraging known vulnerabilities for which a patch exists but has not been applied. 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.

Educate Employees to Recognize Potential Threats

User education has always been a key element in avoiding malware infections. The basics of knowing where files came from, why the employee is receiving them, and whether or not they can trust the sender continue to be useful tools your employees should use before opening files and emails. The most common infection methods used in ransomware campaigns are still spam and phishing emails. Quite often, user awareness can prevent an attack before it occurs. Take the time to educate your users, and ensure that if they see something unusual, they report it to your security teams immediately.

Audit

Routine audits and penetration testing should be conducted across all systems

Principle of Least Privilege

User and software privileges should be kept to a minimum—is there really a need for all users to have local admin rights on their devices?

Mobile OS should always be updated

We recommend mobile users to always update their phone's OS to the latest version as it may often contain patches and fixes to previously discovered vulnerabilities

KEEP SIGNATURE-BASED PROTECTIONS UP-TO-DATE

From the information security side of things, it is certainly beneficial to keep antivirus and other signature-based protections in place and up-to-date. While signature-based protections alone are not sufficient to detect and prevent sophisticated ttacks designed to evade traditional protections, they are an important component of a comprehensive security posture. Up-to-date antivirus protections can safeguard your organization against known malware that has been seen before and has an existing and recognized signature.

IMPLEMENTING THE MOST ADVANCED SECURITY TECHNOLOGIES

There is no single silver-bullet technology that can protect from all threats and all threat vectors. However, there are many great technologies and ideas available—machine learning, sandboxing, anomaly detection, content disarmament, and numerous more. Each of these technologies can be highly effective in specific scenarios, covering specific file types or attack vectors. Strong solutions integrate a wide range of technologies and innovations in order to effectively combat modern attacks in IT environments. In addition to traditional, signature-based protections like antivirus and IPS, organizations need to incorporate additional layers to prevent against new, unknown malware that has no known signature. Two key components to consider are threat extraction (file sanitization) and threat emulation (advanced sandboxing). Each element provides distinct protection that, when used together, offer a comprehensive solution for protection against unknown malware at the network level and directly on endpoint devices.

CORE THREAT PREVENTION ENGINES

CPU-LEVEL THREAT PREVENTION

- Evasion-resistant, zero-day exploit identification
- Patented CPU-level technology is virtually impenetrable, even by nation states
- Detects and blocks malware before evasion code can execute

THREAT EMULATION

- Highest accuracy scores in industry tests
- Rapid verdicts in milliseconds
- Comprehensive coverage of attack tactics, file-types, and operating systems

THREAT EXTRACTION

- Sanitizes files to prevent threats
- Proactively blocks malware
- Delivers reconstructed and safe files in seconds

AI-POWERED ENGINES

- Artificial intelligence delivers state-of-the-art threat prevention
- Analyzes thousands of threat indicators to produce accurate verdicts
- Provides insights to help expose new malware families

ANTI-RANSOMWARE

- Prevents online extortion attacks
- Automatically restores files encrypted by an attack
- Works in both online and offline mode to automatically restore files

ANTI-PHISHING

- Blocks access to phishing websites
- Alerts when credentials are re-used
- Prevents account takeover
- Covering all attack vectors
- How hackers operate
  - Email or Message: Cyber criminals may send an email or text message with a malicious attachment or a malicious link.
  - Web Browsing: Cyber criminals can compromise the user's browser (typically through exploit kits) or trick a user into downloading and opening a malicious file.
  - Server and Systems Exploitation: Cyber criminals can infect by exploiting unpatched vulnerabilities in any online host.
  - Mobile Apps: One of the most common sources for compromising mobile devices is through mobile apps.
  - External Storage: Physically mounted drives allow malicious files to enter without even traversing the network.
  - Phishing: A fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy person.

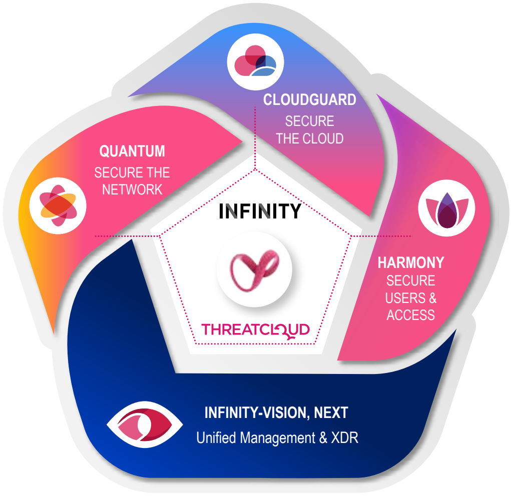
To achieve effective coverage, organizations should seek a single solution that can cover all attack surfaces and vectors. One solution that provides broad prevention across all attack surfaces, including email, web browsing, systems exploitation, external storage, mobile apps and more.

LEVERAGING A COMPLETE UNIFIED ARCHITECTURE

Many companies attempt to build their security using a patchwork of single-purpose products from multiple vendors. This approach usually fails: it results in disjointed technologies that don't collaborate—creating security gaps. Plus, it introduces a huge overhead of working with multiple systems and vendors. As a result of this inefficient approach, many attacks are not prevented, forcing organizations to invest more in post-infection and breach mitigation.

In order to achieve comprehensive security, companies should adopt a unified multi-layer approach that protects all IT elements—networks, endpoint, cloud, and mobile, all sharing the same prevention architecture and the same threat intelligence.

PREVENT THE NEXT ATTACK WITH CHECK POINT INFINITY



In the new normal, we believe our customers deserve to maintain productivity while staying protected in everything they do. Wherever you connect from, whatever you connect to and however you connect—Your home, your devices, your privacy and your organizational data must be secure and protected from any cyber threat.

To make our vision a reality, we have recalibrated our Infinity portfolio of products to focus on those technologies and capabilities that will provide uncompromised security based on our three core principles. Check Point has taken over 80 products and technologies and organized them into three main pillars: Harmony, CloudGuard, and Quantum, with Infinity-Vision as their foundation.

All enriched with Real-time threat intelligence derived from hundreds of millions of sensors worldwide, enriched with AI-based engines and exclusive research data from the Check Point Research Team.

11 CONCLUSION

REGARDLESS OF WHETHER YOUR COMPANY'S INFRASTRUCTURE IS CLOUD-BASED, ON-PREMISE OR BOTH, THE THREAT FROM STATE-SPONSORED CYBERCRIME IS NOW SO SERIOUS, IT IS NO EXAGGERATION TO SAY THAT IT IS TIME FOR ENTERPRISES TO PUT THEIR ENTIRE SECURITY TEAMS ON A WAR FOOTING.

CONCLUSION

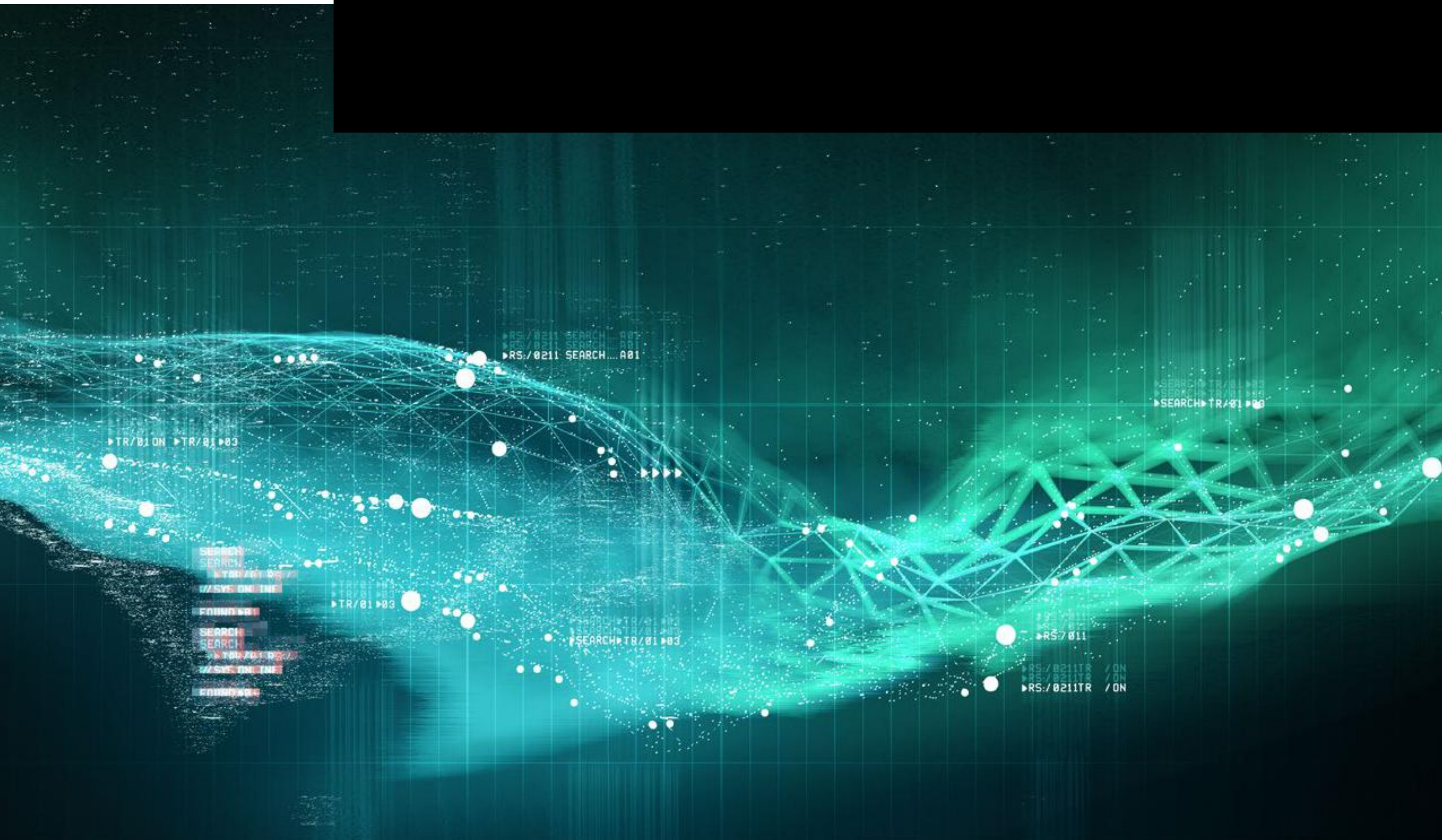
The war in Ukraine has unleashed a tsunami of state-sponsored cyber warfare activity with close coordination of cyber and military campaigns. We have also seen a quantum change of gear from threat actors in attacking entire countries, as was the case in Costa Rica and Peru. Against this backdrop, increasingly, we are seeing cyber activity having a disruptive physical impact in the real-world such as attacks on critical infrastructure. Meanwhile, ransomware has graduated into a sophisticated multi-billion-dollar global industry.

While war and nation state attacks dominate the headlines, ransomware with its potential for enormous financial reward, is now the number one security threat to enterprises. The challenge is made more serious by an increasing reliance on public and private cloud infrastructure and applications. Organizations need to take an integrated, prevent-first, approach to protecting their whole IT estate and not be dependent on the security assurances of public cloud providers. Regardless of whether your company's infrastructure is cloud-based, on-premise or both, the threat from state-sponsored cybercrime is now so serious, it is no exaggeration to say that it is time for enterprises to put their entire security teams on a war footing.

CHAPTER 12

12
ANNEX

MALWARE FAMILY DESCRIPTIONS



AgentTesla

AgentTesla is an advanced RAT which functions as a keylogger and password stealer and has been active since 2014. AgentTesla can monitor and collect the victim's keyboard input 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). AgentTesla is sold on various online markets and hacking forums.

AlienBot

AlienBot is a banking Trojan for Android, sold underground as Malware-as-a-Service (MaaS). It supports keylogging, dynamic overlays for credentials theft, as well as SMS harvesting for 2FA bypass. Additional remote control capabilities are provided using a TeamViewer module.

Anubis

Anubis is a banking Trojan malware designed for Android mobile phones. Since it was initially detected, it has gained additional functions including Remote Access Trojan (RAT) functionality, keylogger, audio recording capabilities and various ransomware features. It has been detected on hundreds of different applications available in the Google Store.

AZORult

AZORult is a Trojan that gathers and exfiltrates data from the infected system. Once the malware is installed on a system, it can send saved passwords, local files, crypto-wallet data, 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.

Bazar

Discovered in 2020, Bazar Loader and Bazar Backdoor are used in the initial stages of infection by the WizardSpider cybercrime gang. The loader is responsible for fetching the next stages, and the backdoor is meant for persistence. The infections are usually followed by a full-scale ransomware deployment, using Conti or Ryuk.

Bumblebee

BumbleBee is a Loader. The malware is likely the latest addition to the Conti gang, designed to replace the BazarLoader backdoor used to deliver ransomware payloads. Attackers drop Bumblebee via ISO and DLL attachemnts in email campaigns, to deploy Cobalt Strike.

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 tracker, and more.

Conti

Conti ransomware emerged in 2020 and has been used since in multiple attacks against organizations worldwide. Conti ransomware is delivered as the final stage after a successful intrusion into the victims' network. Initial intrusion might be performed using spearphishing campaigns, stolen or weak credentials for RDP, or phone-based social engineering campaigns.

Cryptobot

Cryptobot is an advanced cryptominer that collects the victim's wallet and account information upon infection. In December 2021 Cryptobot was observed in a campaign that targeted users with a pirated copy of the Windows operating system.

Cl0p

Cl0p is a ransomware that was first discovered in early 2019 and mostly targets large firms and corporations. During 2020, Cl0p operators 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. In 2021 Cl0p ransomware was used in numerous attacks where the initial access was gained by utilizing zero-day vulnerabilities in the Accellion File Transfer Appliance.

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.

Dridex

Dridex is a Banking Trojan turned botnet, 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.

FluBot

FluBot is an Android malware distributed via phishing SMS messages (Smishing), most often impersonating logistics delivery brands. Once the user clicks the link inside the message, they are redirected to the download of a fake application containing FluBot. Once installed the malware has various capabilities to harvest credentials and support the Smishing operation itself, including uploading of the contacts list, as well as sending SMS messages to other phone numbers.

FormBook

FormBook 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 Windows 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.

HermeticWiper

HermeticWiper is a Wiper that has been targeting hundreds of computers in Ukraine. The Wiper appears to have been compiled in December 2021, which implies that the attack was premeditated for at least a couple of months.

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.

Hive

Hive ransomware emerged in June 2021and uses multiple mechanisms to compromise business networks, including phishing emails with malicious attachments to gain access and Remote Desktop Protocol (RDP) to move laterally once on the network. Hive involves both encryption and data exfiltration and operate a "leak site" over Tor.

IcedID

IcedID is a banking Trojan which first emerged in September 2017. It spreads by mail spam campaigns and often uses other malwares like Emotet to help it proliferate. IcedID uses evasive techniques like process injection and steganography, and steals user financial data via both redirection attacks (installs a local proxy to redirect users to fake-cloned sites) and web injection attacks.

Kinsing

Discovered in 2020, Kinsing is a Golang cryptominer with a rootkit component. Originally designed to exploit Linux systems, Kinsing was installed on compromised servers by abusing vulnerabilities on internet facing services. Later in 2021 a Windows variant of the malware was developed as well, allowing the attackers to increase their attack surface.

LAPSUS$

LAPSUS$ is a data extortion group that specializes in stealing data from big companies and threatening to publish it. The group gains initial access to targets mostly via social engineering, which involves bribing or tricking employees at the target organization or at its partners. LAPSUS$ recent victims include big names such as Samsung, NVIDIA, and Okta.

LemonDuck

LemonDuck is a cryptominer first discovered in 2018, which targets Windows systems. It has advanced propagation modules, including sending malspam, RDP brute-forcing and mass-exploitation via known vulnerabilities such as BlueKeep. Over time it was observed to harvest emails and credentials, as well as to deliver other malware families, like Ramnit.

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.

MaliBot

Malibot is an Android Banking malware that has been spotted targeting users in Spain and Italy. The banker disguises itself as crypto mining applications under different names and focuses on stealing financial information, crypto wallets and more personal data.

Mirai

Mirai is an infamous Internet-of-Things (IoT) malware that tracks vulnerable IoT devices, such as web cameras, modems and routers, and turns them into bots. The botnet is used by its operators to conduct massive Distributed Denial of Service (DDoS) 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.

Nanocore

NanoCore is a Remote Access Trojan that targets Windows operating system users and was first observed in the wild in 2013. All versions of the RAT contain basic plugins and functionalities such as screen capture, crypto currency mining, remote control of the desktop and webcam session theft.

Pegasus

Pegasus is a highly sophisticated spyware which targets Android and iOS mobile devices, developed by the Israeli NSO group. The malware is offered for sale, mostly to government-related organizations and corporates. Pegasus can leverage vulnerabilities which allow it to silently jailbreak the device and install the malware. The malware infects its targets via several means: Spear phishing SMS messages which contains a malicious link or URL redirect, without any action required from the user ("Zero Click"), and more. The app features multiple spying modules such as screenshot taking, call recording, access to messaging applications, keylogging and browser history exfiltration.

Phobos

Phobos is a ransomware first detected in December 2018. It targets windows operating systems and its attack vector often includes exploiting open or poorly secured RDP ports. Phobos bears great resemblance to the Dharma ransomware, both in its ransom note and with much of its code and is thought to have been developed and used by the same group.

Phorpiex

Phorpiex 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.

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.

Raccoon

Raccoon infostealer was first observed in April 2019. This infostealer targets Windows systems and is sold as a MaaS (Malware-as-a-Service) in underground forums. It is a simple infostealer capable of collecting browser cookies, history, login credentials, crypto currency wallets and credit card information.

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.

RedLine Stealer

RedLine Stealer is a trending Infostealer and was first observed in March 2020. Sold as a MaaS (Malware-as-a-Service), and often distributed via malicious email attachments, it has all the capabilities of modern infostealer—web browser information collection (credit card details, session cookies and autocomplete data), harvesting of cryptocurrency wallets, ability to download additional payloads, and more.

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.

REvil

REvil (aka Sodinokibi) is a Ransomware-as-a-service which operates an "affiliates" program and was first spotted in the wild in 2019. REvil encrypts data in the user's directory and deletes shadow copy backups to make data recovery more difficult. In addition, REvil 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.

Sharkbot

Sharkbot steals credentials and banking information on Android mobile devices. Sharkbot lures victims to enter their credentials in windows that mimic benign credential input forms. When the user enters credentials in these windows, the compromised data is sent to a malicious server. The malware implements geofencing feature excluding users from China, India, Romania, Russia, Ukraine or Belarus. Sharkbot has several anti-sandbox evasion techniques.

Snake Keylogger

Snake Keylogger is a modular .NET keylogger/infostealer. Surfaced around late 2020, it grew fast in popularity among cyber criminals. Snake is capable of recording keystrokes, taking screenshots, harvesting credentials and clipboard content. It supports exfiltration of the stolen data by both HTTP and SMTP protocols.

SparrowDoor

SparrowDoor is an advanced backdoor used by the FamousSparrow APT group to spy on hotels, governments and more. It was spotted exploiting the Microsoft Exchange ProxyLogon vulnerability around March 2021. The backdoor is loaded using DLL Hijacking combined with a legitimate binary, to help bypass AV products.

Tofsee

Initially detected in 2013, Tofsee botnet targets Windows machines and has a variety of uses including spam distribution, DDoS attacks, crypto mining and more.

Triada

Triada which was first spotted in 2016, is a modular backdoor for Android which grants admin privileges to download another malware. Its latest version is distributed via adware development kits in WhatsApp for Android.

Trickbot

Trickbot is a modular banking Trojan, attributed to the WizardSpider cybercrime gang. Mostly delivered via spam campaigns or other malware families such as Emotet and BazarLoader. 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 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.

Vidar

Vidar is an infostealer that targets Windows operating systems. First detected at the end of 2018, it is designed to steal passwords, credit card data and other sensitive information from various web browsers and digital wallets. Vidar is sold on various online forums and used as a malware dropper to download GandCrab ransomware as its secondary payload.

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.

Xenomorph

An android banking Trojan, first detected in February 2022 on Google Play. Xenomorph is designed to steal banking credentials, intercept multifactor authentication codes and other user data, heavily relying on an overlay attack mechanism.

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.

Zloader

Zloader is a banking malware which uses webinjects to steal credentials and private information, and can extract passwords and cookies from the victim's web browser. It downloads VNC that allows the threat actors to connect to the victim's system and perform financial transactions from the user's device. First seen in 2016, the Trojan is based on leaked code of the Zeus malware from 2011. In 2020, the malware is very popular among threat actors and includes many new variants.

z0Miner

Z0Miner, first observed in November 2020 is a cryptominer which was found on thousands of servers exploited by Oracle's WebLogic Server Remote Code Execution flaw. The group behind Z0miner has since been taking advantage of the Atlassian Confluence RCE vulnerability (CVE-2021-26084), to infect additional 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: 800-429-4391 | 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/

WWW.CHECKPOINT.COM

CHECK POINT™