cp<r>
CHECK POINT RESEARCH

2023 CYBER SECURITY REPORT

CHECK POINT™


YOU
DESERVE
THE BEST
SECURITY

CONTENTS

01 INTRODUCTION TO THE CHECK POINT 2023 SECURITY REPORT

CHAPTER 1

MAYA HOROWITZ

VP Research, Check Point

In 1976, Queen Elizabeth II sent the first royal email. It was sent over ARPANET, 7 years before the internet was invented, and a long 13 years before the first recorded internet hack.

Almost 50 years later, email has evolved into a popular communication method, and the most popular vehicle for threat actors to initiate their attacks. In fact, the Check Point Research (cp<r>) annual Security Report shows that in 2022, the proportion of email-delivered-attacks has increased, reaching a staggering record of 86% of all file-based attacks in-the-wild.

In our Security Report, we discuss a few more trends observed by cp<r> throughout the year. The Russia-Ukraine war demonstrated how the traditional, kinetic, war can be augmented by a cybernetic war. It has also influenced the broader threat landscape in the rapid changes of hacktivism and how independent threat actors choose to work for state-affiliated missions. The war has also seen enhanced usage of wiper malware, and this trend has been adopted by several actors, reaching a point where 2022 has seen more wiper attacks globally, than in the previous decade altogether. Traditional cybercrime has also changed—in 2022, threat actors started using more legitimate tools in their operations, including native operating system files, IT software and penetration testing tools, all helping them in their efforts to stay under the radar. In their ransomware attacks, threat actors are starting to skip the encryption process, realizing that the financial rewards comes mostly from data breaches and the threat to publish victim data. In attacks on mobile devices, attackers make a habit out of mimicking legitimate applications, and in the cloud threat landscape—companies' data is at risk mostly when hosted by third parties, and susceptible to attacks due to misconfigurations, over-permissive roles and permissions, and access keys stored publicly.

In the last days of 2022, we witnessed a dramatic advancement in the field of generative artificial intelligence, now widely available to the public, and which is able to generate highly professional text (code included) on demand in seconds. As we step into 2023, we should keep in mind that this technology may quickly be adopted by threat actors, to craft even more malicious emails, in even better quality than those typically authored by threat actors, and with endless variations of malware and malicious code in general. This comes to prove, yet again, the importance of zero day prevention of attacks, across the entire IT infrastructure, including email, endpoint, network, cloud, and everything in between.

Check Point Software is committed to ensuring our customers are provided the best and prevention-first security across all these vectors. At Check Point Research, we are happy to provide this annual Security Report to help in raising awareness and vigilance, so that we can all join hands in preventing the next cyberattack.

Maya Horowitz

VP Research at Check Point Software Technologies

02

TIMELINE OF 2022'S KEY CYBER EVENTS

JANUARY

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.

Television channels and a radio station run by Iran's state broadcaster were hacked in a complex attack by an exiled opposition group. Hacktivist group Edalat-e Ali (Ali's Justice) hacked the television website and broadcasted a video with a strong opposition message. The video started with footage of people in Tehran's Azadi stadium shouting "death to dictator" referring to Supreme Leader Ali Kamenei, then it cut into a close up of a masked man similar to the protagonist of the movie V for Vendetta, who said "Khamenei is scared, the regime's foundation is rattling". Check Point Research provided in-depth technical analysis of one of the attacks. CPR was able to discover part of the tools that were utilized in this operation, including the evidence of the usage of a destructive wiper malware.

UKRAINE

IRAN

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.

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.

State-sponsored Attack Groups Capitalise on Russia-Ukraine War for Cyber Espionage

CPR has observed advanced persistent threat (APT) groups around the world launching new campaigns, or quickly adapting ongoing ones to target victims with spear-phishing emails using the war as a lure.

https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/

Check Point Research has released data on cyberattacks observed around the Russia/ Ukraine conflict. Cyberattacks on Ukraine's government and military sector **surged by 196% in the first three days of combat**. Cyberattacks on Russian organizations increased by 4%. Phishing emails in the East Slavic languages increased 7-fold.

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.


BELGIUM


GERMANY


NETHERLANDS


UKRAINE

OpenSea

MARCH

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.

As part of the NVIDIA leak by the Lapsus$ ransomware gang were 2 stolen code signing certificates used by to sign their drivers and executables. Attackers have already started using these certificates to sign malware, hoping to evade security solutions. Ransomware gang Lapsus$, which took responsibility for the breach on the giant chip firm NVIDIA, claims it also managed to breach the Korean manufacturer Samsung, and published 190GB of sensitive data online.

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.

RUSSIA

NVIDIA

МИРАТОРГ

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.

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 areas. 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.

Check Point Research identified "ALHACK", a set of vulnerabilities in the ALAC audio format that could have been used for remote code execution on two-thirds of the world's mobile devices. The vulnerabilities affected Android smartphones powered by chips from MediaTek and Qualcomm, the two largest mobile chipset manufacturers.

Check Point Research identified a vulnerability in the Everscale blockchain wallet. If exploited, the vulnerability would have given an attacker full control over a victim's wallet and subsequent funds. The vulnerability was discovered in the web version of Everscale's wallet, known as Ever Surf. Available on Google Play Store and Apple's App Store, Ever Surf is a cross-platform messenger, blockchain browser, and crypto wallet for the Everscale blockchain network.

SINGAPORE

android

Everscale

Blockchain Security 101

Every year, ordinary people lose money in blockchain hacks. Could it be that this technology is simply insecure by nature? Or is there something we're all missing—something that can save this industry, and the millions of people who've invested their hard-earned money into it, from squandering billions of dollars every year?

Tune in to CP<RADIO> our Podcast channel for this insightful podcast

https://research.checkpoint.com/2022/blockchain-security-101/

MAY

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. The Conti Ransomware gang has allegedly taken its infrastructure offline after its leaders announced they were reorganizing their operation. The news comes a few days after Conti extorted Costa Rica. Conti members are believed to be currently migrating and rebranding into smaller ransomware operations.

Lincoln College, a 157-year-old institution in Illinois, has announced it will indefinitely close after a significant ransomware attack that occurred in December 2021 took a toll on the school operations.

Sberbank, a Russian banking services organization, has been the target of continuous attacks in the past month by Pro-Ukraine hackers. The bank recently suffered the **largest distributed denial-of-service (DDoS) attack ever recorded**, measured at 450GB/sec.

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.

How the Evolution of Ransomware Changed the Threat Landscape From WannaCry to Conti: A 5 Year Perspective

https://www.checkpoint.com/ransomware-hub/

JUNE

CERT Ukraine has issued a warning concerning Russian hackers, possibly the state-sponsored APT group Sandworm, launching attacks exploiting the Follina critical vulnerability (CVE-2022-30190) in Microsoft Windows Support Diagnostic Tool. The campaign leverages malicious emails with DOCX attachments targeting media and news outlets in Ukraine.

The largest ever-recorded HTTPS DDoS attack has recently been mitigated, with 26 million request per second. The attack targeted a Cloudflare customer and originated from cloud service providers rather than residential internet service providers, indicating the use of hacked virtual machines.

Microsoft has issued a fix to address the critical Follina vulnerability (tracked CVE-2022-30190) which has been exploited in the wild, recommending users to urgently update and patch.

Russian intelligence services have reportedly increased attacks against governments and NGOs supporting Ukraine in 42 different countries, with the goal to obtain sensitive information from NATO countries' agencies.

Check Point customers among the first to be protected from Follina Vulnerability

Check Point customers were protected on the same day Follina was discovered (May 30th). Utilizing Harmony Endpoint and Threat Emulation behavioral protections

https://blog.checkpoint.com/2022/05/31/follina-zero-day-vulnerability-in-microsoft-office-check-point-customers-remain-protected/

JULY

Both Norway and Lithuania were victims of large-scale DDoS. The attacks are assumed to have been carried out by separate pro-Russian hacker groups, with the goal of discouraging the nations' support of Ukraine.

Twitter has suffered a data breach after threat actors used a vulnerability to build a database of phone numbers and email addresses belonging to 5.4 million accounts, with the data now up for sale on a hacker forum for $30,000. It has been reported on a stolen data market that the database contains info about various accounts, including celebrities, companies, and random users.


NORWAY


LITHUANIA

Data Breaches. Is your Business Protected?

Download our guide to learn more about data breaches and the best practices you must follow to prevent them.

https://pages.checkpoint.com/prevent-cyber-attack-data-breach.html

The New Era of Hacktivism—State-Mobilized Hacktivism Proliferates to the West and Beyond

In the past year, things have changed. As one of the multiple fallouts of conflicts in Eastern Europe and the Middle East, some hacktivism groups stepped up their activities in form and focus to a new era; Hacktivism is no longer just about social groups with fluid agendas.

https://research.checkpoint.com/2022/the-new-era-of-hacktivism/

AUGUST

Atlassian Confluence critical vulnerability tracked CVE-2022-26138 has been exploited in the wild. Unauthenticated actors could leverage the flaw remotely to gain unrestricted access to all pages in confluence. In addition, CISA issued a warning and ordered US federal agencies to address the vulnerability.

Cisco confirms it has been breached by the Yanluowang ransomware group. The initial access was gained after the threat actor gained an employee's Google account credentials, saved in their browser, and after getting an MFA push accepted by the user. The company says that while there have also been signs of pre-ransomware activity, no ransomware has been deployed on Cisco's systems.

The pro-Russian hacker group Killnet publicly targeted Lockheed Martin, calling other hacker groups to join in on attacks. At this point Killnet claims to be responsible for a recent DDoS attack on the company, and tells they have obtained personal data of the company's employees; claims were denied by the American corporation.

South Staffordshire Water, UK's largest water company supplying 330M liters of drinking water to 1.6M consumers daily, has been a victim of ransomware attack launched by Cl0p, a Russian-speaking ransomware gang. The group caused disruption of the company's IT systems, allowing them access to more than 5TB of data including passports, screenshots from water treatment SCADA systems, driver's licenses, and more.

Apple has issued an urgent patch for two zero-day flaws actively exploited by attackers to hack iPhones, iPads, or Macs. Among them is CVE-2022-32893, an out-of-bounds write vulnerability in WebKit that would allow an attacker to perform arbitrary code execution, and CVE-2022-32894, an out-of-bounds write vulnerability in the operating system's kernel that would allow an attacker to execute code with kernel privileges.

Check Point Research has discovered an active cryptocurrency mining campaign imitating "Google Translate Desktop" and other free software to infect PCs. Created by a Turkish speaking entity called Nitrokod, the campaign counts 111,000 downloads in 11 countries since 2019.

SEPTEMBER

A traffic jam was generated in Moscow in a kind of physical DDoS attack, as attackers hacked Russian taxi service Yandex, and ordered dozens of cars to a specific location. The Anonymous collective claims to be behind this attack.

Multiple cyberattacks linked to Iran have been disrupting Albania's government systems since July, forcing them to shut down some online services. In response, Albania's government halted its diplomatic ties with Iran, ordering staff to leave within 24 hours. The latest attack which occurred over the weekend, allegedly by the same actor, targeted the Albanian Police's computer system, forcing officials to take its TIMS system, used for immigration data tracking, offline.

Uber has suffered a data breach, allegedly by an 18-year-old hacker who managed to gain access using social engineering tactics on an employee. The hacker claims to have access to Uber's internal IT systems and to the company's HackerOne bug bounty account, which contains vulnerabilities in Uber's systems and apps, disclosed privately by security researchers. Uber claims that the users' private information was not compromised.

A new record-breaking DDoS attack in has been recorded this week, peaking at 704.8 Mpps, about 7% higher than the previous attack recorded on the same European organization last July.

OCTOBER

Hacktivist groups around the world have taken aim at the Iranian regime, as protests throughout the country continue. The groups have been leaking information relating to Iranian government officials, and offering support to the protesters in sharing information and evading censorship.

Personal information of 10 million Australians has been stolen in a breach of telecom company Optus. The data includes sensitive information, such as passport and healthcare details. While the hackers initially demanded a 1M USD ransom, they later retracted their demand due to the high attention drawn to the hack and the law enforcement operation initiated to identify the attackers.

Check Point Research published a report studying the rising trend of state-mobilized Hacktivism. While in the past Hacktivist groups tended not to affiliate themselves with national interests, groups nowadays take part in state-directed efforts, driven by geopolitical conflicts.

Russian-speaking threat group Killnet claims responsibility for attacks taking down different US state government websites, including those of Colorado, Kentucky, Mississippi and others.

Online shopping company Woolworths has reported a data breach impacting over two million Australian users of its MyDeal subsidiary. The company said the breach was due to a compromised user credential that was used to gain unauthorized access to MyDeal's customer relationship management system. Several Australian companies have been breached during October—The country's largest health insurance firm, Medibank, froze trading on the Australian stock exchange after confirming a 200GB data breach; In a breach of wine retailer Vinomofo's network data of over 500,000 customers was leaked; an attack on energy company EnergyAustralia exposed payment data of hundreds of the company's customers.

Pulling the Curtains on Azov Ransomware: Not a Skidsware but Polymorphic Wiper

CPR provides under-the-hood details of its analysis of the infamous Azov Ransomware

https://research.checkpoint.com/2022/pulling-the-curtains-on-azov-ransomware-not-a-skidsware-but-polymorphic-wiper/

Russian-affiliated hacktivist group 'Killnet' has launched a DDoS attack against government websites in Bulgaria, causing them to become inaccessible. Killnet said that Bulgaria was targeted due to its "betrayal to Russia" and the supply of weapons to Ukraine.

The Largest copper manufacturer in Europe—Aurubis—has been the victim of a cyberattack that targeted its IT systems and forced the company to shut down many of its sites' systems.

OpenSSL, used widely for secure communications, gave heads-up for a critical vulnerability in versions 3.0 and above that will be published on Tuesday, November 1st. eventually the vulnerabilities published were downgraded to 'high' severity

Check Point Research found that global attacks increased by 28% in the third quarter of 2022, with education/research as the most attacked industry overall, and the healthcare sector the most targeted industry in ransomware attacks.

NOVEMBER

IT Army of Ukraine claim to have gained access to Russia's Central Bank. They published 27K of the leaked files, containing personal, legal, and financial data.

Check Point Research identified a new and unique malicious package on PyPI, the leading package index used by developers for the Python programming language. The package was designed to hide code in images and infect through open-source projects on Github.

The Azov ransomware is being distributed worldwide to encrypt victim files, while in fact an analysis by Check Point Research proves that Azov ransomware is a data wiper aimed at destroying data with no way to recover the files.

Meta has fired dozens of employees, after the employees had received thousands of dollars in bribes by outside hackers in return for granting access to users' Facebook or Instagram profiles. The employees used the company's internal support tool, which allows full access to any user account.

The European Parliament website has been attacked following a vote declaring Russia a state sponsor of terrorism. The pro-Russian hacktivist groups Anonymous Russia and Killnet, have claimed responsibility for the attack, causing an ongoing DDoS (Distributed Denial of Service).

Black Basta ransomware group is running a campaign targeting organizations in the United States, Canada, United Kingdom, Australia, and New Zealand. The group uses QakBot (AKA QBot, Pinkslipbot) banking Trojan to infect an environment and install a backdoor allowing it to drop the ransomware.

Банк России

python Package Index

Meta

DECEMBER

Cyber criminals who breached Australian Medibank's systems have released another batch of data onto the dark web, claiming that the files contain all data harvested in the former heist that impacted 9.7 million customers in October 2022. Medibank has confirmed the data breach.

Researchers found that over 300,000 users across 71 countries were effected by an Android campaign meant to steal Facebook credentials. This is by using Schoolyard Bully Mobile Trojan, deployed in legitimate education-themed applications, which were available in the official Google Play Store.

Check Point Research has analyzed the activity of cyber-espionage group Cloud Atlas. Since its discovery in 2014, the group has launched multiple, highly targeted attacks on critical infrastructure across geographical zones and political conflicts, however its scope has narrowed significantly in the last year, with a clear focus on Russia, Belarus and conflicted areas in Ukraine and Moldova.

As artificial intelligence (AI) models grow more and more popular, Check Point Research discusses the risks and upsides of the technology. CPR demonstrates how AI technologies, like ChatGPT and Codex, can easily be used to create a full infection flow, from spear-phishing to running a reverse shell, and provides examples of the positive impact of AI on the defenders' side.

medibank For Better Health

Google Play

03

2022'S CYBER SECURITY TRENDS

RUSSO-UKRAINIAN CONFLICT

The ongoing Russian-Ukrainian war has had a profound effect on cyberspace and caused a significant increase in cyber-attacks in 2022. Hacktivism has been transformed, and the use of destructive malware by state-sponsored groups and independent entities has become more prevalent globally.

The role of cyberwarfare has been well documented in this first full-blown hybrid conflict, where battles are fought online as well as on physical ground. The Russians revealed new cyber tools and achieved tactical objectives that affected military and civil communications, including blocking public media transmissions. While cyber activity cannot win the war on its own, it does play a significant part in tactical operations and has an indisputable psychological and economic effect.

For cyber-operations to be effective, is not just a matter of employing malware. Much like conventional warfare, cyberwarfare also requires meticulous and thorough preparations. Reconnaissance, intelligence gathering and assessment, target-bank compilation and prioritization, dedicated-payload development and network infiltration are all prerequisites for a successful campaign.

As was the case on the physical battleground, the Russians apparently did not prepare for a long cyber campaign. Their cyber operations, which in the early stages included carefully planned precise attacks, have all but ceased. Multiple new tools and wipers, that were characteristic of the initial stages, have been replaced with a different operational mode. Current offensive cyberattacks are mostly rapid exploitations of opportunities as they arise and use already known attack tools. These are not intended to assist tactical combat efforts but rather create a psychological effect by damaging the Ukrainian civil infrastructure.

The recruitment of cyber professionals, criminals, and other civilians to the military cyber effort—on both sides of the conflict—has further blurred the distinction between nation-state actors, cyber criminals, and hacktivists. The Ukrainian government has established an army of hacktivists whose management is very different from anything we have seen before. Previously characterized by loose cooperation between individuals in an ad hoc fashion, new-hacktivist organizations conduct recruitment, training, intelligence-gathering and allocation of targets and

battlefield status compilation in a military manner. Attacks on Russian entities, which were once considered off-limits by many cybercrime entities, have now increased and Russia is struggling under an unprecedented hacking wave that combines state-sponsored activity, political cyber warriors and criminal action. On the other side, multiple Russian-affiliated hacktivist groups were established that target not only Ukraine but also Europe, North America and Japan. For more details, see our section on Hacktivism.

The extensive use of destructive malware has already resulted in an increase in similar activities in other regions and by other geopolitical groups. Can cyberattacks be considered a hostile act? What type of proof, and how extensive must the damage be to be considered a *casus belli*? Are modifications to existing treaties required? We address these questions in another chapter of the report entitled "Wipers".

Eight years of continuous cyber hostility between Russia and Ukraine have served as a training period for both sides. Ukraine's cyber defense organizations are praised as "the most effective defensive cyber activity in history". Knowing adversaries tools and modus operandi has an increased importance in cyber warfare. The impact of a first-time deployment of a particular wiper may be devastating, but the impact of the second one is often much smaller. For example, the effect of the Industroyer2 attack on the energy sector in Ukraine in March 2022 was limited in comparison to Industroyer's first deployment in 2016.

The full scope of changes brought on by this conflict is yet to be seen, but we have already learned some valuable lessons.

SERGEY SHYKEVICH

Threat Intelligence Group Manager, Check Point Software Technologies

"The role of cyberwarfare has been well documented in this first full-blown hybrid conflict, where battles are fought online as well as on physical ground. The Russians revealed new cyber tools and achieved tactical objectives that affected military and civil communications, including blocking public media transmissions. While cyber activity cannot win the war on its own, it does play a significant part in tactical operations and has an indisputable psychological and economic effect.

THE YEAR OF UNRESTRAINED WIPER DISRUPTION

Wipers and other types of destructive malware are carefully designed to cause irreversible damage, and if tightly woven into cyberwarfare, the effect can be catastrophic. This is probably why we have only seen limited use of wipers over the years, and they were usually associated with nation states. Until recently, countries primarily used cyberattacks for the purpose of espionage and intelligence gathering, and only rarely resorted to destructive cyber tools. In 2022 we have seen a change in the appearance of multiple new wiper families that are used to destroy thousands of machines.

Wipers are destructive malware, designed to inflict damage with limited potential for financial gain for attackers. Early use of wipers to showcase attackers' capabilities was thus limited and short-lived. But in all the cases, the main purpose of the wipers is to interrupt operations or to irreversibly destruct data. While the process of data destruction has several technological implementations.

Stuxnet, arguably the most famous destructive malware, was used in 2010 to sabotage the centrifuges in the Iranian nuclear project. At the time, Stuxnet was unique in many respects but mostly because its immediate impact was the physical destruction of mechanical hardware. In 2012, Shamoon was deployed to disrupt oil companies in the Middle East, targeting Saudi and Qatari facilities. In 2013, DarkSeoul, attributed to North Korea, was used to destroy more than 30,000 computers related to the banking and broadcasting sectors in South Korea. This attack took place during a period of heightened tensions between the two countries following nuclear testing by the North.

In the ensuing years we witnessed the Black Energy attack in 2015 on the Ukrainian energy infrastructure (KillDisk) and another attack on Saudi targets by dubbed Shamoon2 in 2016. NotPetya was distributed against Ukrainian targets in 2017 in a supply chain attack which caused significant collateral damage globally. In 2018 Olympic Destroyer, purportedly produced by North Korea, was used by the Russian-affiliated Sandworm to disrupt the

opening ceremonies of the Winter Olympic Games. In 2019 Dustman and ZeroCleare were used in Iranian attacks on targets in the Middle East related to oil production. On average, there was one attack by a wiper family per year.

During 2022, there has been a noticeable shift in the tactics of destructive malware deployment. Cyberespionage continued, as it was previously, but this activity has been supplemented by destructive cyber operations, instigated by nations whose goal appears to be to inflict as much damage as possible. The start of the Russian-Ukrainian war in February saw a massive uptick in disruptive cyberattacks carried out by Russia against Ukraine. Russia has a long history of cyber assaults against its neighbor. In January 2022, WhisperGate was used to attack government and financial organizations in Ukraine, overwriting systems' MBR (Master Boot Record) to prevent system reboot and file recovery. Attackers left a ransom note but did not offer a recovery mechanism, leading to speculation that the demand for payment was only intended to mislead victims. The files were further corrupted using a second stage payload that was hosted on a Discord channel.

On the eve of the ground invasion in February, three additional wipers were deployed: Hermetic wiper, HermeticWizard and HermeticRansom. The tools were named after their certificate which was issued to 'Hermetica Digital Ltd'. Additional wipers were reported later that month. Another attack was directed at the Ukrainian power grid in April, using a new version of Industroyer, the malware that was used in a similar attack in 2016.

ELI SMADJA

Security Research Group Manager, Check Point Software Technologies

> **Wipers and other types of destructive malware are carefully designed to cause irreversible damage, and if tightly woven into cyberwarfare, the effect can be catastrophic. This is probably why we have only seen limited use of wipers over the years, and they were usually associated with nation states. Until recently, countries primarily used cyberattacks for the purpose of espionage and intelligence gathering, and only rarely resorted to destructive cyber tools. In 2022 we have seen a change in the appearance of multiple new wiper families that are used to destroy thousands of machines.**

In total, there were at least nine different wipers deployed in Ukraine in less than a year. Many of them were most likely separately developed by different Russian intelligence services and employed different wiping and evasion mechanisms.

One of the attacks, enacted hours before the ground invasion of Ukraine, was intended to interfere with Viasat, satellite communications company that provided services to Ukraine. The attack used a wiper called AcidRain that was designed to wipe modems and routers and cut off internet access for tens of thousands of systems. There was also significant collateral damage, including thousands of wind turbines in Germany.

The attacks were clearly the result of detailed planning. Some of the tools were designed specifically to fit their intended targets, with attackers breaching security measures and gaining access months earlier and then using GPOs (Group Policy Objects) to deploy their wipers at the time of the actual attack.

Cyber destructive activity was not restricted to Russia-Ukraine. In the Middle East, Iran has suffered a series of destructive attacks since the middle of 2021. In July 2021, a hacktivist group identifying itself as Predatory Sparrow attacked Iran's railway system, causing delays and general panic. An investigation by Check Point Research (cp<r>) revealed that older versions of the wipers were used in attacks against multiple targets in Syria.

In January 2022, the Iranian state broadcasting service IRIB was attacked by destructive malware. The attack, investigated by cp<r>, caused damage to computers at dozens of TV and radio stations throughout Iran. Images of the leaders of the Iranian opposition, the anti-regime organization Mojahedin-e-Khalq (MEK), were aired on TV screens across the country, calling for "Death to Ayatolla Khamenei!" MEK, which conducts much of its activity from exile in Albania, denied responsibility. In June, the Chaplin wiper, a revised version of Meteor, previously used by Predatory Sparrow, hit steel plants in Iran. Other wiper attacks were reported in Iran that employed the Dilemma and Forsaken families but attracted less attention due to the general unrest in the country.

On July 18, just a few days before MEK's conference titled "the World Summit of Free Iran", the Albanian government stated it had to "temporarily close access to online public services and other government websites" due to disruptive cyber activity. The Homeland Justice hacktivist group that was behind the incident (later attributed to Iran) used various images and articles suggesting it was carried out in retaliation for attacks on the Islamic Republic. Researchers found that the wiper used in this instance, ZeroClear, is related to destructive attacks previously directed at energy-sector targets in the Middle East.

The MEK summit was cancelled, but this did not prevent a second cyberattack from hitting Albanian government systems in September. While this was an unprecedented attack on a NATO member state, the defense alliance did not consider it to be an "armed attack" as defined by Article 5 of the NATO treaty. However the organization has in the past reaffirmed that cyberspace is part of NATO'S core task of collective defense. Iran has consistently invested in extending its foothold on western countries' IT infrastructure. This bold act of deploying destructive malware against a NATO member without retaliation could have serious ramifications.

The destructive cyber activity continued throughout 2022. Somnia, a new wiper-turned-ransomware was deployed by the FRwL (From Russia with Love) hacktivist group against Ukrainian targets. The attacks resemble techniques practiced by ransomware groups, but no ransom demand was submitted, and the intent was clearly only to inflict maximum disruption on the victim. Similar attacks that deploy the CryWiper malware have recently been targeting municipalities and courts in Russia, leaving ransom notes and Bitcoin wallet addresses. However, in reality the damage is irreversible.

Azov is a new widespread wiper that falsely links itself to various security researchers and blames multiple nations and political entities for the current state of warfare. Azov has not been officially linked to any of the fighting sides and has been causing damage indiscriminately since November 2022, as detailed in a recent investigation by cp<r>.

More wipers have been used this year than were probably recorded in the past 30 years, and they have evolved both in the way they are deployed and in their impact. Some actors in this area are willing to take actions that could justify a war, modelling the definition of endured cyber hostility. It has become increasingly difficult to tell the difference between nation-state APT activity and hacktivist groups. Many countries are involved to a degree in the activities of non-governmental entities, ranging from providing inspiration, tools and target allocation, to direct management and financing of attacks disguised as private initiatives. This ambiguity further extends the degree to which threat actors can operate without the likelihood of retaliation. This will lead to more widespread destructive cyber operations and in turn ever higher levels of collateral damage.

HACKTIVISM GRADUATES TO MAJOR PLAYER ON GEOPOLITICAL STAGE

Hacktivism, the act of carrying out politically or socially motivated cyberattacks, was traditionally associated with loosely managed entities such as Anonymous. These previously decentralized and unstructured groups were made up of individuals cooperating ad hoc for a variety of agendas. Over the last year, following developments in the Russian-Ukrainian conflict, the hacktivist ecosystem has matured. Hacktivist groups have tightened up their level of organization and control, and now conduct military-like operations including recruitment and training, sharing tools, intelligence and allocation of targets. Most of the new hacktivist groups have a clear and consistent political ideology that is affiliated with governmental narratives. Others are less politically driven but have nonetheless made their operations more professional and organized.

The rise of politically motivated Middle Eastern groups in the past couple of years, such as the Iranian-associated "Hackers of Savior" or anti-Iranian regime "Predatory Sparrow", marked the beginning of the change, as groups began focusing on a single agenda. Early this year, following Russian attacks on Ukrainian IT infrastructure at the beginning of the war, Ukrainian government set up an unprecedented arrangement called the "IT Army of Ukraine". Through a dedicated Telegram channel, its operators manage more than 350,000 international volunteers in their campaign against Russian targets. On the other side of the battlefield, Killnet, Russia-affiliated group, was established with a military-like organizational structure and a clear top-down hierarchy. Killnet consists of multiple specialized squads that perform attacks and answer to the main commanders. These groups are led by a hacker called KillMilk.

Unlike Anonymous, who have an open-door policy, regardless of skill or specific agenda, the new era hacktivists screen out applicants who fail to meet specific requirements. This reduces the risk of exposing the inner workings of their operation. XakNet, a pro-Russian group, declared that they will not recruit hackers, pentesters, or OSINT specialists without proven experience and skills. Other groups, like the pro-Russian NoName057(16), offer training through e-learning platforms, tutorials, courses or mentoring.

Organized operations invest in and develop their members' technical proficiency and tools. Although most of the activity is focused on defacement and DDoS attacks using botnets, in some cases, groups use more sophisticated destructive tools. TeamOneFist, a Ukraine affiliated group, has been linked to destructive activities against SCADA systems in Russia. The Belarusian Cyber Partisans group, in an attempt to prevent the movement of Russian troops to Ukraine, encrypted internal databases of the Belarusian Railways to disrupt its operation just before the invasion started. The pro-Russian group 'From Russia with Love' (FRwL) was observed using a data wiper called 'Somnia' to encrypt the data of Ukrainian organizations and disrupt their operations.

The battle is not only about inflicting damage. All active groups are aware of the importance of media coverage. They use their communication channels to collect reports of successful attacks and publish them to maximize the effect. For example, Killnet has more than 89,000 subscribers on their Telegram channel, where they publish attacks, recruit team members and share attack tools. There is also extensive coverage of the group's activity in major Russian media outlets to promote their achievements in cyber space and validate the impact of their successful attacks.

Well organized and coordinated groups also use their resources to cooperate with other entities. Killnet's success has put them in a position where other groups want to collaborate with them or officially join forces. On October 24, Zarya (Killnet's squad) allegedly conducted a joint operation with two Russian-speaking groups, Xaknet and Beregini, to breach and leak data from the Ukrainian Security Service (SBU). In addition, Killnet recently announced the launch of a Killnet collective which has become an umbrella organization for 14 pro-Russian hacktivist groups.

The transformation in the hacktivism arena is not limited to specific national conflicts or geographical zones. Now major corporations and governments in Europe and the US are targeted by this new type of hacktivism. For example, in November 2022 the European Parliament was targeted with a DDoS attack launched by Killnet. In recent months, the US, Germany, Estonia and Lithuania, Italy, Norway, Finland, Poland and Japan suffered severe attacks from state-mobilized groups, with significant impact in some cases. New hacktivist groups are being mobilized based on political narratives and are achieving strategic and broad-based goals with higher success levels, and a much wider public impact than ever before.

Several groups in the Middle East, the most prominent being Predatory Sparrow, have been observed attacking high profile targets associated with the Iranian regime. The latest large-scale hacktivist attack was inflicted on Albania by "HomelandJustice", a hacktivists group affiliated with Iran's Ministry of Intelligence and Security. The group served Iranian interests by attacking the Albanian government who sheltered the "Mujahedin-e-Khalq" (MEK), an Iranian dissident group. Between October 2021 and January 2022 the group used a unique email exfiltration tool to collect emails. Then on July 15, they temporarily shut down multiple Albanian government digital services and websites using ransomware file encryption and disk wiping malware. These operations resulted in Albania's termination of diplomatic ties with Iran on September 6.

The increased level of organization and specialization among hacktivist groups is not limited to political agendas. The Guacamaya hacktivist group targets entities in Latin America for their role in the region's environmental degradation and repression of native populations. Since March 2022, the group has focused on infiltrating mining and oil companies, the police and several Latin American regulatory agencies. On September 19, Guacamaya leaked 10 terabytes of documents belonging to several entities in Mexico, Guatemala, Chile, Peru, Colombia and El Salvador. They also accused the United States and Western corporations of over-exploiting the region's natural resources.

Hacktivist operations, which until recently were marked by a spirit of anarchy and loose cooperation, have been inspired by state-run cyber campaigns to improve their level of organization and management. This enhanced orchestration resulted in improved infrastructure, manpower, tools, and capabilities which in turn led to more effective and destructive operations. This began in specific conflict zones but quickly spread globally. In turn, this is expected to inspire hacktivist groups with more diverse agendas. The boundaries between state cyber-operations and hacktivism are blurred, which allows nation states to act with a degree of anonymity without fear of retaliation. Non-state affiliated hacktivist groups are better organized and more effective than ever before, and this is expected to increase in the future.

ALEXANDRA GOFMAN

Threat Intelligence Analysis Team Leader, Check Point Software Technologies

> **The boundaries between state-sponsored cyber operations and hacktivism have become increasingly blurred, which allows nation-states to act with a degree of anonymity without feat of retaliation. This also provides hacktivists with the opportunity to publicly claim responsibility for cyber attacks and draw significant attention to their cause, which can be just as significant as the actual damage caused. Non-state affiliated hacktivist groups are better organized and more effective than ever before, and this is expected to increase in the future.**

WEAPONIZATION OF LEGITIMATE TOOLS

The basic layer of cyber protection is recognizing malicious tools and behaviors before they can strike. Security vendors invest substantial resources in the research and mapping of malware types and families, and their attribution to specific threat actors and the associated campaigns, while also identifying TTPs (Techniques, Tactics and Procedures) that inform the correct security cycles and security policy.

To combat sophisticated cybersecurity solutions, threat actors are developing and perfecting their attack techniques, which increasingly rely less on the use of custom malware and shift instead to utilizing non-signature tools. They use built-in operating system capabilities and tools, which are already installed on target systems, and exploit popular IT management tools that are less likely to raise suspicion when detected. Commercial off-the-shelf pentesting and Red Team tools are often used as well. Although this is not a new phenomenon, what was once rare and exclusive to sophisticated actors has now become a widespread technique adopted by threat actors of all types.

There are several reasons why the use of legitimate tools is an attractive option for cybercriminals. First, as these tools are not inherently malicious, they often evade detection and are difficult to distinguish from regular users or IT operations. Second, many of these tools are open-source or available for purchase, so threat actors have easy access to them. In addition, when threat actors share tools, it makes it harder to identify who is responsible for a particular attack.

LIVING OFF THE LAND (LOTL)

LotL or LOLBin attacks, which have been around for several years, leverage utilities already available within the targeted system. Attackers use them to download and execute malicious files, conduct lateral movement, and for general command execution. On Windows OS these utilities often involve command shell, Windows Management Instrumentation, and native Windows scripting platforms such as PowerShell, mshta, wscript or cscript. This technique allows attackers to remain under the radar, as legitimate software and native OS binaries are less likely to raise suspicion and are typically whitelisted by default. Attackers often use these utilities for fileless attacks.

This leaves fewer traces as no malicious artifacts are written to hard drives, and it makes incident response and remediation work even more complex.

OFFENSIVE FRAMEWORKS

A tight and robust security policy involves constant testing to find vulnerabilities and weaknesses within the network and systems deployed in it. Organizations often rely on the expertise of Red Team professionals to mimic every step of a cyberattack. Red Teams deploy multiple tools to test the resilience of the environment. Many of these tools are free or available for use or purchase in criminal circles and they are often spotted in the wild, in the hands of threat actors.

Cobalt Strike is the most widespread penetration testing tool to be exploited by threat actors, particularly since its source code was leaked in 2020. Brute Ratel is another legitimate offensive framework that uses a licensing process and is currently priced at $2,500. Customers must pass a vetting process before being issued a license to verify that the software will not be used with malicious intent. As cybersecurity solutions are increasingly focused on Cobalt Strike detections, some threat actors quietly switched to Brute Ratel for their 2022 attacks. This includes creating fake US companies to pass the licensing verification system. In an overview report on this tool, techniques associated with APT29 were identified, suggesting it has been adopted by APT-level actors. Researchers also identified the use of the tool by the BlackCat ransomware gang since at least March 2022, which implies that threat actors were able to circumvent the developer's verification procedure.

LOTEM FINKELSTEEN

Director, Threat Intelligence & Research, Check Point Software Technologies

> **There are several reasons why the use of legitimate tools is an attractive option for cybercriminals. First, as these tools are not inherently malicious, they often evade detection and are difficult to distinguish from regular users or IT operations. Second, many of these tools are open-source or available for purchase, so threat actors have easy access to them. In addition, when threat actors share tools, it makes it harder to identify who is responsible for a particular attack.**

As with Cobalt Strike, a cracked version of Brute Ratel was shared in underground cyber-criminal forums in September 2022, leading to predictions that this tool will be widely adopted by threat actors. This is a concerning expansion of the criminal use of Red Team tools, as Brute Ratel was developed by a former Red Teamer with extensive knowledge of EDR (Endpoint Detection and Response) technologies and is specifically designed to evade detection by EDR products.

Another emerging offensive framework detected in 2022 is Manjusaka, the Chinese counterpart of Cobalt Strike which is freely available on GitHub. The tool was observed in campaigns targeting the Haixi Mongolian and Tibetan Autonomous Prefecture region in China. Additional tools include the Sliver framework, which was seen in multiple campaigns during 2022 and continues to gain popularity at the year's end.

Earlier this year, Check Point Research uncovered a two year-long campaign targeting financial organizations in French-speaking regions of Africa. Attackers deployed several of these tools, including Metasploit as well as PoshC2, another offensive framework available on GitHub. DWservice is another interesting tool found in this campaign. DWservice is a legitimate remote access service and, while it is subscription-based, it also has a free plan. These are all easy-to-use tools, exploited by actors with varying levels of technical expertise, and we expect to see their use increase at different stages of offensive operations.

LEGITIMATE IT AND SECURITY SOFTWARE

Remote Management and Monitoring (RMM) software is used daily for legitimate purposes. Given its destructive potential when used in malicious campaigns, it is crucial to keep a close eye on its use and implement intelligent security policies.

In 2022, multiple ransomware gangs made use of legitimate IT software in successful campaigns. One of the developments was the rise of BazarCall-style social engineering campaigns now employed by multiple ransomware groups. First seen in 2021 when used by the Ryuk/Conti ransomware gang, a BazarCall attack starts with a phishing email that urges the victim to call an actor-controlled call center. The operator instructs the victim to install a potent management tool to be used as malware. This not only allows threat actors to target specific entities based on targeted industry, revenue or other factors. It also leverages social engineering techniques to control the malware delivery process. In multiple campaigns reported in 2022, three separate groups—Silent Ransom, Quantum, and Roy/Zeon—used this method to initiate Zoho Assist sessions, a legitimate remote support tool, which allowed them to gain initial access to corporate networks.

The Conti ransomware group and their affiliates often relied on legitimate remote management solutions such as **Splashtop**, **AnyDesk** or **ScreenConnect**, as well as one-month trial-versions of the **Atera** agent to regain and establish persistence in cases where Cobalt Strike was previously detected. This is now used repeatedly by their successors. In a cp<r> publication earlier this year, researchers found that Atera remote management tool was used also to deploy the Zloader banker.

In a case investigated by the Check Point Incident Response Team (CPIRT) of a Hello ransomware incident, attackers used Desktop Central, a unified endpoint management solution, together with **Atera** and Wazuh. Desktop Central was installed prior to the investigated breach, which indicates that it was either utilized legitimately by the IT department—although they did not recognize it as a tool in their use—or was part of a previous breach.

Wazuh is another legitimate software often used by IT personnel. It is not a remote access tool, but rather a security platform used for network asset discovery and vulnerability management. This allows attackers to disguise their activity as legitimate scans for network assets and vulnerabilities.

Other security tools adopted by threat actors include Impacket and BloodHound. **BloodHound** is a powerful tool for security assessments of Active Directory (AD) environments used in the analysis of AD rights and relations, which can easily be abused by attackers. **Impacket** is designed for IT administration and penetration testing of network protocols and services. Both tools were exploited by APT groups in high-profile campaigns, such as the WhisperGate destructive operation against Ukrainian organizations, Sandworm attacks against Ukrainian energy facilities together with Industroyer2 malware, and in a Russian state-sponsored campaign targeting defense contractor networks in the US.

Before deploying the Somnia wiper, the FRwL (From Russia with Love) hacktivist group used a toolset consisting of AnyDesk, Ngrok reverse proxy, Netscan network reconnaissance tool, and open-source Rclone for data exfiltration —tools that were previously used in financially-motivated campaigns.

Instead of developing their own malware, threat actors are now using legitimate tools developed and made available by tech companies. This trend sets new challenges for detection, protection, attribution and further mapping of the cyber arena. To meet these challenges, defense systems must employ holistic protection approaches. This emphasizes the operational need for Extended Detection and Response systems (XDR), which provide context-based anomalies-detection and are precisely designed to track down the malicious use of otherwise legitimate tools.

CHAPTER 3

RANSOMWARE EXTORTION— SHIFTING FOCUS FROM ENCRYPTION TO DATA EXTORTION

Seeking to maximize the pressure on their victims, ransomware actors employ multiple-extortion tactics. Data on the victims' systems is encrypted, with decryption keys released only after the ransom payment. Unless they pay, companies know their data could be openly published, sold or even used to extort their employees and customers directly. Some ransomware affiliates, which have now become more dominant in the ransomware crime scene, and better skilled at identifying sensitive information in victims' networks, even skip the encryption phase altogether and rely solely on data publication threats to generate ransom payments. This may have serious implications for defense mechanisms, attribution, and future analysis of the ransomware ecosystem.

In the early days, ransomware attacks were conducted by single entities who developed and distributed massive numbers of automated payloads to randomly selected victims, collecting small sums from each "successful" attack. Fast forward to 2022 and these attacks have evolved to become mostly human-operated processes, carried out by multiple entities over several weeks. The attackers carefully select their victims according to a desired profile, and implement a series of pressure measures to extort significant sums of money. Threats of exposing sensitive data have proven to be very effective. This is because the victims fear the consequences of large fines, lawsuits on behalf of employees and customers, and the resulting negative effect on stock prices and reputation.

Ransomware attack-management has also evolved with an increase in threat actors that operate a Ransomware-as-a-Service model (RaaS) through affiliates. Affiliates, who may participate in multiple RaaS programs simultaneously and choose between various encryption tools have become the "producers", initiating attacks and paying part of the revenue back to the RaaS operator. Affiliates further outsource operations by purchasing stolen credentials or network access from access-brokers. The fragmented nature of this operation complicates the attribution of attacks and the tracking of criminal entities. Tactics, techniques, and procedures (TTPs) used to gain initial access to a system are no longer necessarily connected to the affiliate or to the RaaS payload later deployed.

Current Ransomware-as-a-Service (RaaS) actors are competing for the attention of affiliates, and typically charge 10% - 20% of the ransom payment as a fee for their services. The speed of the encryption module is one of the main "selling points", allowing the attacker to reduce the encryption time and probability of detection. RaaS actors' attempts to shorten encryption time include allowing affiliates to choose from various encryption modes or even offering partial file encryption ("intermittent encryption").

Some groups now skip the encryption phase altogether, relying on threats of data exposure alone to extort money. In September 2021, a group named Karakurt Team started to employ extortion without encryption. Attacking mostly North American and European victims, Karakurt operators typically contact their victims, provide screenshots and copies of the stolen data, and threaten to auction the information or release it unless their demands are met. They often contact the victims' employees, business partners and clients to ramp up the pressure. This new behavior, involving direct contact with the victims' clients, was first observed in 2020, and is referred to as Triple Extortion. Many different types of information are considered sensitive, from corporate financial and proprietary data to personal data relating to physical or mental health, financial data or any other personal identifiable information (PII), which makes the threat of data exposure even more potent.

Negotiation with the victims is often conducted over relatively secure mediums, using proprietary access codes. This is typically done to prevent uncontrolled publication which would result in reduced potential leverage. At least in theory, victims who pay can emerge from an attack relatively unscathed, without their details posted on Karakurt's shame-site, and thereby stopping their customers or the authorities from finding out they have been attacked.

An example of the effectiveness of the threat of personal data exposure was demonstrated in a recent attack on Medibank, an Australian health insurer, in October 2022. When the company refused to pay ransom demands of $10M, the attackers (possibly connected to the REvil group) dumped massive amounts of personal information relating to pregnancy termination, drug and alcohol abuse, mental health issues and other confidential and highly sensitive medical data relating to millions of Australian and international customers.

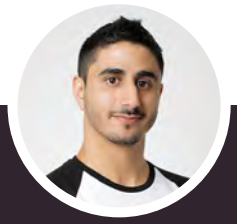
The Lapsus$ group also received a lot of public attention following a series of data breaches of large tech companies, including Microsoft, Nvidia and Samsung. Since its first recorded attack in December 2021 on the Brazilian health ministry, in which they stole and threatened to publish medical information regarding COVID-19 vaccinations, the group has focused on data exfiltration rather than encryption. Headed by young criminals of British and Brazilian nationality, Lapusus$ uses various methods to gain initial access to their victims, including payments to employees, purchasing credentials and social engineering. The group focuses on locating and exfiltrating the proprietary source code of their victims' products. The ensuing threat of publication is estimated to have generated $14M in revenue after only a few months of activity.

Some RaaS actors even recommend their affiliates to avoid encrypting critical areas such as data belonging to healthcare patients. They permit attacking and exfiltrating data from hospitals but not encrypting them, suggesting some twisted version of a moral code among hackers. Hive RaaS, which focuses on healthcare, sometimes makes an effort to not disable the systems. Publishing stolen data has proven effective and threat actors have developed elaborate extortion mechanisms. BlackCat and Lockbit ransomware groups added searchable data mechanisms, allowing employees, customers and other potential victims to search repositories of stolen data. Also, valuable stolen data is often monetized by selling it on Darknet markets.

Other threat actors have turned to destroying data instead of encrypting it. The Onyx ransomware group, active since April 2022, destroys files larger than 2MB instead of encrypting them. Others have followed suit. A new sample of the ExMatter exfiltration tool now includes dedicated wiping functionality. Although it was initially detected as part of the BlackMatter RaaS in late 2021, ExMatter development is attributed to an affiliate and not the RaaS entity. This marks the possible independence of ransomware affiliates from their RaaS partners.

Choosing to base their extortion solely on data publication is understandably attractive to attackers. It offers the option of quick deployment, without a prolonged and messy encryption process, thereby reducing the possibility of detection. Victim management becomes simpler. There is no need to supply individual decryption keys to different victims and operate a logistically complicated "customer support" mechanism. Above all, it frees affiliates from their dependence on large RaaS actors who demand their share of the income.

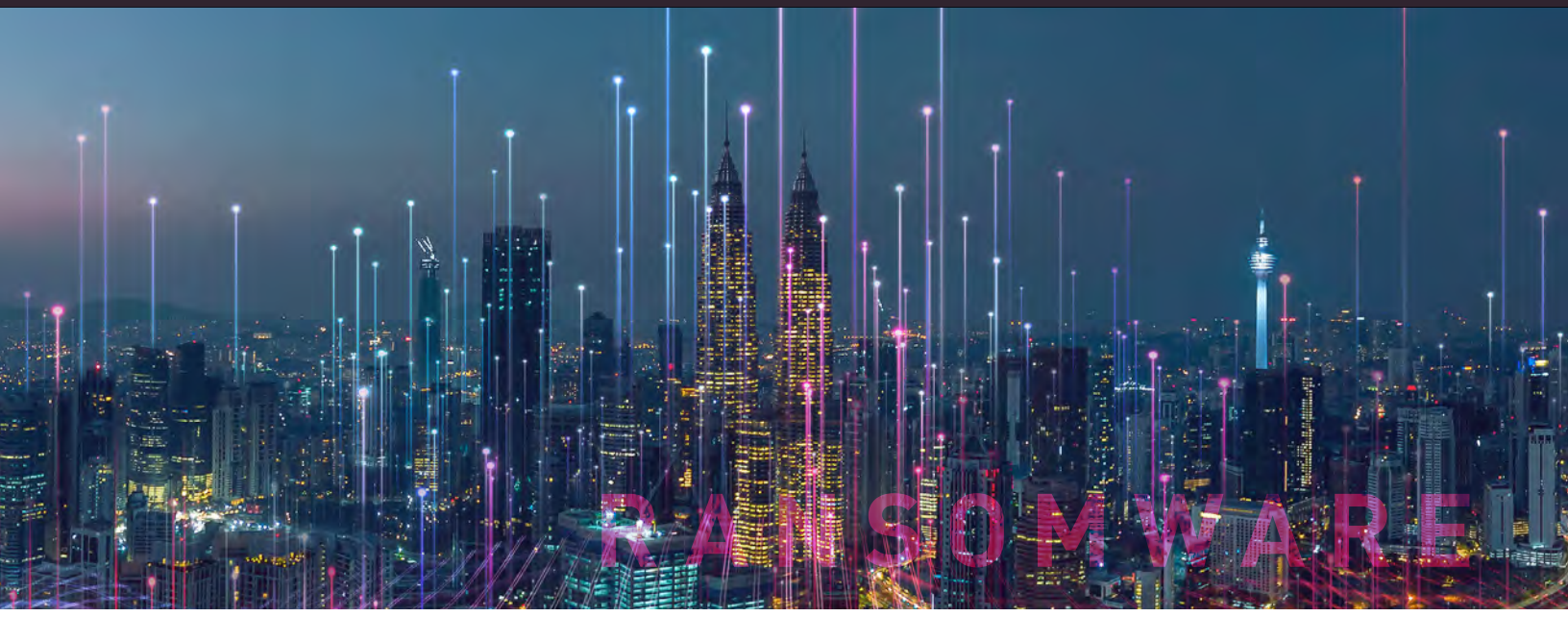
As this data extortion model becomes prevalent, possible ramifications include increased fragmentation of the ransomware ecosystem. Attribution of ransomware operations and tracking threat actors may become even harder and existing protection mechanisms which are based on detecting encryption activity could prove less effective. In its place, cyber security providers will need to focus more on data wiping and exfiltration detection.



ITAY COHEN

Technology Leader,
Check Point Software
Technologies

“As this data extortion model becomes prevalent, possible ramifications include increased fragmentation of the ransomware ecosystem. Attribution of ransomware operations and tracking threat actors may become even harder and existing protection mechanisms which are based on detecting encryption activity could prove less effective. In its place, cyber security providers will need to focus more on data wiping and exfiltration detection.



MOBILE MALWARE LANDSCAPE— THE RISK OF TRUSTING THE FAMILIAR

In our 2022 mid-year report we reviewed some major events in the mobile threat landscape, including the vast increase in the number of malicious applications infiltrating Google and Apple stores. Often disguised as innocent applications like QR readers, external Bluetooth apps, flashlights or games, they are designed to attract as little attention as possible. In our latest analysis, we focus on attempts to hide mobile malware in "unofficial" versions of well-known applications. Mostly, these are malicious modified versions (aka Mods), typically distributed through third-party app stores and downloaded by users who prefer an unofficial version for a variety of reasons. This is not a completely unheard of threat, but 2022 has seen multiple attacks using apps that are well known, trusted, and widely used.

Mod APKs (Android Package Kits; applications for Android devices) are reworked copies of well-known applications, designed to provide users with extended functionalities or access that are not available in the original version. In the past few years, we have seen modified versions of a variety of applications, from instant messaging and social media apps, to live streaming, VPN services and more. The apps are usually distributed through unofficial channels to users looking for free versions of known apps, or for additional features that do not exist in the original versions. In some cases, users are targeted and offered direct links to the modified APKs. In others, users seek them out voluntarily due to limited access to official applications. For example, FMWhatsApp allows users to redesign their WhatsApp interface and edit the "last seen" and "blue tick" functionalities. These Mods are not scrutinized as carefully as the official version, which makes them a natural exploitation target for threat actors. Often the infection is achieved through advertisement SDKs, used by the Mods' developers. This was the case with HMWhatsApp infection with the Triada Trojan in August 2021, and APKPure later that year.

When made aware of these threats, WhatsApp issued an alert in July 2022, warning users not to use modified versions of the app, and described its joint efforts with Google to eradicate previous malicious versions. Despite this warning, another modified build of WhatsApp was reported in October 2022. Once again, the YoWhatsApp Mod was found to contain the Triada malware. When it is implemented in a fully functioning version of the popular messenger app, the malware is granted extensive permissions, including access to SMS messages, similar to the permissions the official WhatsApp app receives. This can allow threat actors to bypass Multi Factor Authentication mechanisms and take over a wide range of applications and accounts, from email to banking and corporate accounts, as well as the WhatsApp account itself. The latest campaign deploying Triada malware through modified applications, which was reported by Check Point Research, weaponized copies of the Telegram messaging app to steal personal information from multiple users.

In most cases, Mods are not distributed through official app stores. However, sometimes unsuspecting users can obtain them through official channels. In October, WhatsApp's parent company Meta, filed a lawsuit against three companies based in China and Taiwan for developing unofficial versions of the application, and selling them on their websites and in the Google Play Store. Once installed, the modified application was used to hijack accounts and steal sensitive information from more than one million Android users.

Mods have also been used by nation-state actors. In August, researchers exposed the Dracarys Android spyware deployed in a modified version of the Signal messaging application. Despite reports of attacks against its users, Signal is considered a secured messenger, but its modified version provided attackers with extensive spying capabilities along with its regular functions. The operation was attributed to Bitter APT, a group known to operate in South Asia, which is reportedly also producing similar Mods for Facebook,

Telegram, YouTube and WhatsApp. The attack was deployed using phishing sites that mimicked the genuine Signal site, and most likely targeted users through phishing emails and social media. Meta also accused Transparent Tribe (APT-36), a Pakistan affiliated state-sponsored threat actor, of creating and using fake versions of WhatsApp, WeChat and YouTube, and identified more than 10,000 potentially affected users.

Malicious modified versions of two mobile VPN applications, SoftVPN and OpenVPN, were used to spy on users by the mercenary Bahamut APT group, which offers hacking services to a wide range of clients.

Populations of totalitarian regimes often have limited access to applications in the official app stores and must seek other alternatives. This makes them more susceptible to attacks by financially or politically motivated actors. This was the case in 2018 and 2019 when the Iranian government blocked secure instant messaging (IM) apps, resulting in an increase in cloned unofficial versions of Telegram, Instagram and other IM applications. Many of the unofficial applications were later revealed as part of a government program to spy on and control opposition and minority groups.

Mobile devices are targeted by hostile entities for a variety of reasons and motivations. Attackers often target the most popular, well- known and widely used applications which users would consider safe. Exploits can come in either the form of modified or fake applications, or through the exploitation of vulnerabilities in the original versions. We should take this as a reminder of the need to stay vigilant, especially when using the most popular and widely used applications.

SHANI SHPRINGER

Data Research Analysis Team Leader, Check Point Software Technologies

Mobile devices are targeted by hostile entities for a variety of reasons and motivations. Attackers often target the most popular, well- known and widely used applications which users would consider safe. Exploits can come in either the form of modified or fake applications, or through the exploitation of vulnerabilities in the original versions. We should take this as a reminder of the need to stay vigilant, especially when using the most popular and widely used applications.

CLOUD: THIRD PARTY THREAT

Over the past few years, Check Point Research (cp<r>) has been tracking the increasing adoption of cloud infrastructure in corporate environments, as well as the evolution of the cloud threat landscape. Currently, around 98% of organizations use cloud-based services, and 76% of them have multi-cloud environments that incorporate services from two or more cloud providers.

When comparing the past two years, we have seen a significant increase in the number of attacks on cloud-based networks per organization, which shot up by 48% in 2022 compared with 2021. Although the overall number of attacks on cloud-based networks is 17% lower than non-cloud networks, a closer examination of the types of attacks shows that newly disclosed vulnerabilities (2020-2022) are exploited more frequently on cloud-based than on-premise environments. This might indicate a shift that some threat actors now prefer to scan the IP range of cloud providers. This might enable to gain easier access to sensitive information or critical services.

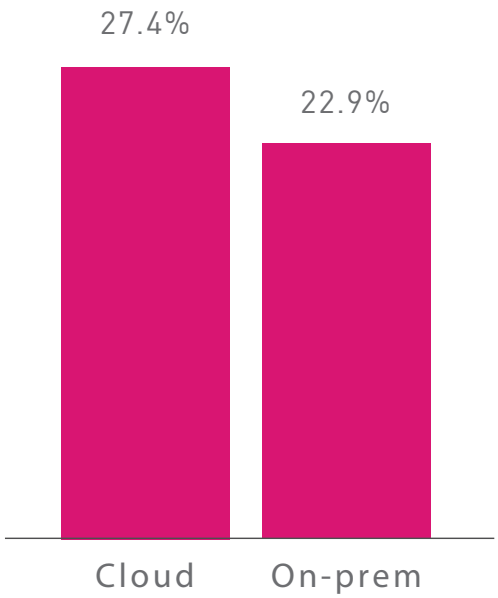


Figure 1 - Percentage of attacks leveraging recent vulnerabilities (disclosed 2020-2022)

In addition to vulnerability exploitation attempts, cloud environments have become both a source and target of security incidents and breaches that involve improper access management, sometimes combined with the use of compromised credentials. In March 2022, the ransomware gang Lapsus$ announced in a statement on its Telegram channel that it had gained access to Okta, an identity management platform. Lapsus$ has a history of publishing

sensitive information, often source code, stolen from high-profile tech companies such as Microsoft, NVIDIA, and Samsung. However, this time, the actors claimed their target was not Okta itself, but rather its customers.

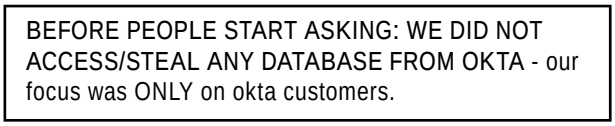


Figure 2 - LAPSUS$ announcement about OKTA on their telegram channel

Following the breach, Okta released an official statement revealing that approximately 2.5% of their customers were affected by the Lapsus$ breach—around 375 companies, according to independent estimates. Okta, is used by thousands of companies to manage and secure user authentication processes, as well as by developers to build identity controls. This effectively means that hundreds of thousands of users worldwide could potentially be compromised by the company responsible for their security.

On its Telegram channel, Lapsus$ claimed that Okta was storing AWS keys in Slack and that Okta's third-party support engineers had access to all the company's 8,600 Slack channels. It is possible that Lapsus$ gained initial access to Okta via Slack using stolen cookies and/or social engineering. cp<r> suggested that Lapsus$'s access to Okta clients could explain the cybercrime gang's modus operandi and impressive record of successes, all thanks to excessive permissions granted to a third-party within the corporate cloud environment. Identity and Access Management (IAM) role abuse attacks were thoroughly discussed by cp<r> in 2021, and while this is still an ongoing issue, there are other risks of which businesses need to be aware.

On September 16, 2022, Uber stated that they were responding to a security incident which they later attributed to a hacker connected to the very same Lapsus$ group. The company explained that the attacker used stolen credentials of an Uber contractor in a Multi Factor Authentication fatigue attack, where the contractor was flooded with two-factor authentication (2FA) login requests until one of them was accepted. These credentials were then used for lateral movement and privilege escalation that resulted in the intruder gaining administrator access to Uber's AWS cloud account and its resources.

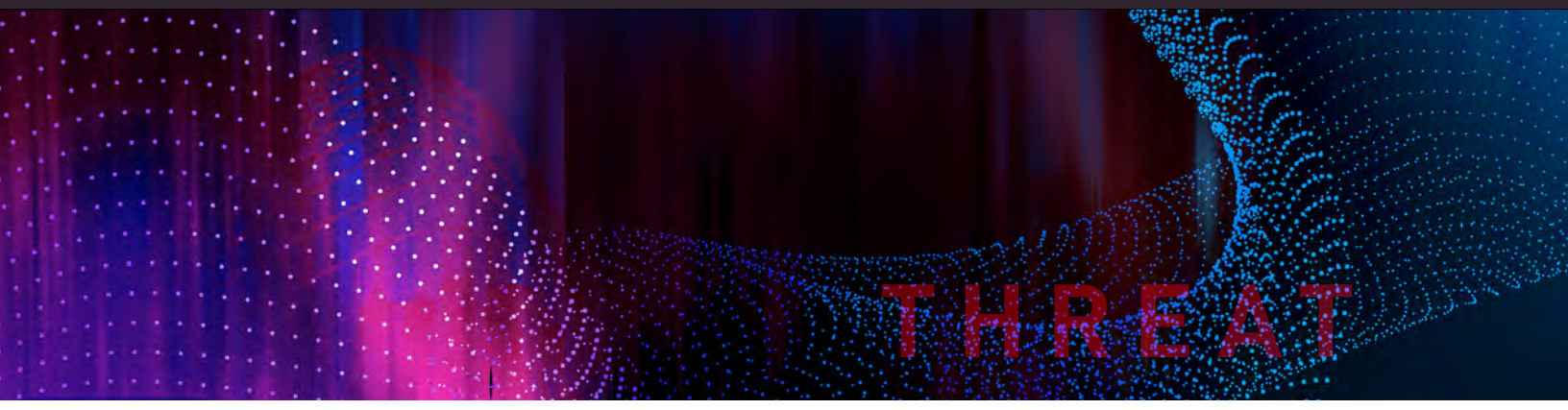
Towards the end of the year, Uber suffered another high-profile data leak that exposed sensitive employee and company data. This time, attackers breached the company by compromising an AWS cloud server used by Tequivity, which provides Uber with asset management and tracking services. It is not clear if the unauthorized access was due to misconfiguration or stolen credentials, but it's evident that we need to adapt our methods of assessing third-party risk to the world of cloud infrastructure.

From basic rules like not storing cloud access keys publicly or not ignoring 2FA bypass attempts, to more complicated but essential ones such as prevention of cloud misconfigurations and using proper IAM, the events of 2022 show that any violations of these rules puts cloud environments at risk.

OMER DEMBINSKY

Data Research Group Manager, Check Point Software Technologies

> **When comparing the past two years, we have seen a significant increase in the number of attacks on cloud-based networks per organization, which shot up by 48% in 2022 compared with 2021. Although the overall number of attacks on cloud-based networks is 17% lower than non-cloud networks, a closer examination of the types of attacks shows that newly disclosed vulnerabilities (2020-2022) are exploited more frequently on cloud-based than on-premise environments. This might indicate a shift that some threat actors now prefer to scan the IP range of cloud providers. This might enable to gain easier access to sensitive information or critical services.**



CHAPTER 4

04 GLOBAL ANALYSIS

CYBER ATTACK CATEGORIES BY REGION

GLOBAL

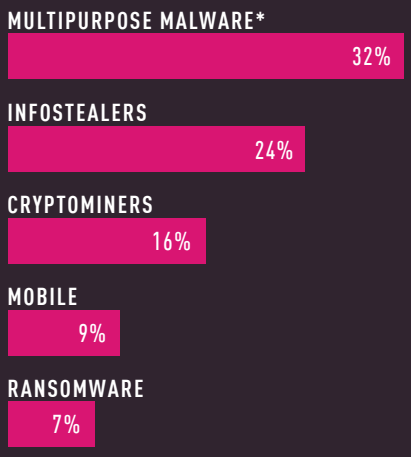


Figure 3: Percentage of organizations affected by malware type globally in 2022.

* 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.

AMERICAS

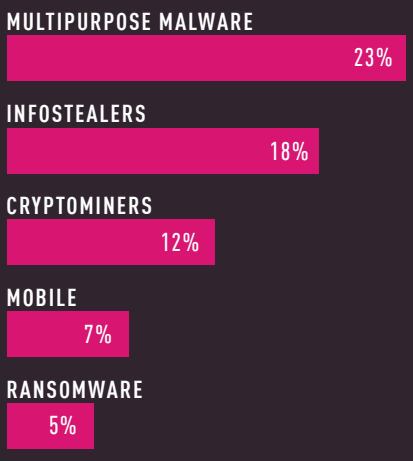


Figure 4: Percentage of organizations affected by malware type in the Americas in 2022.

CYBER ATTACK CATEGORIES BY REGION

EMEA

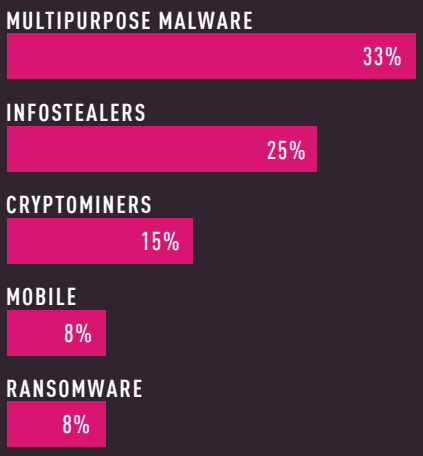


Figure 5: Percentage of organizations affected by malware type in EMEA in 2022.

APAC

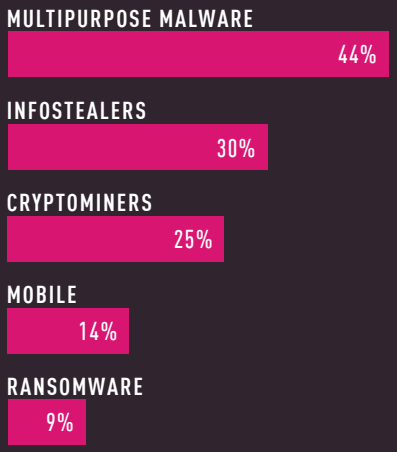
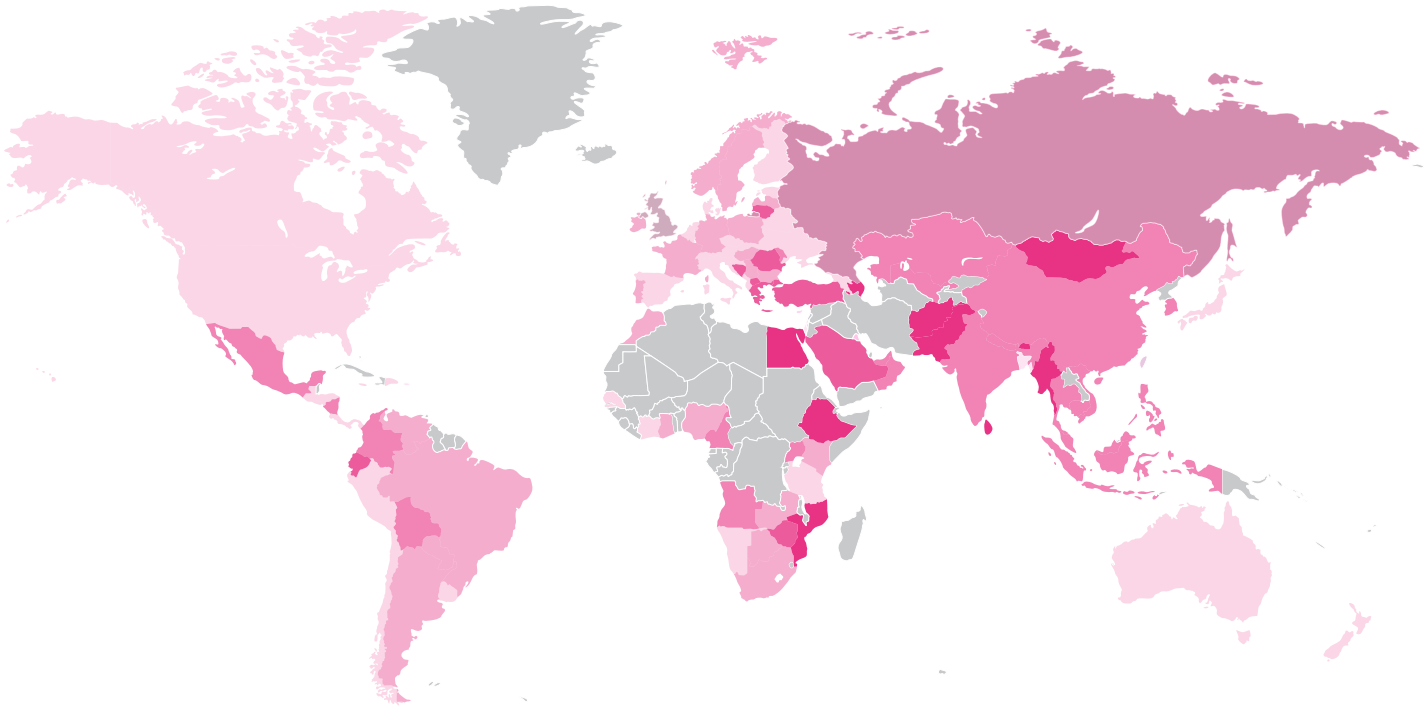


Figure 6: Percentage of organizations affected by malware type in APAC in 2022.

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 7. Global Threat Index Map

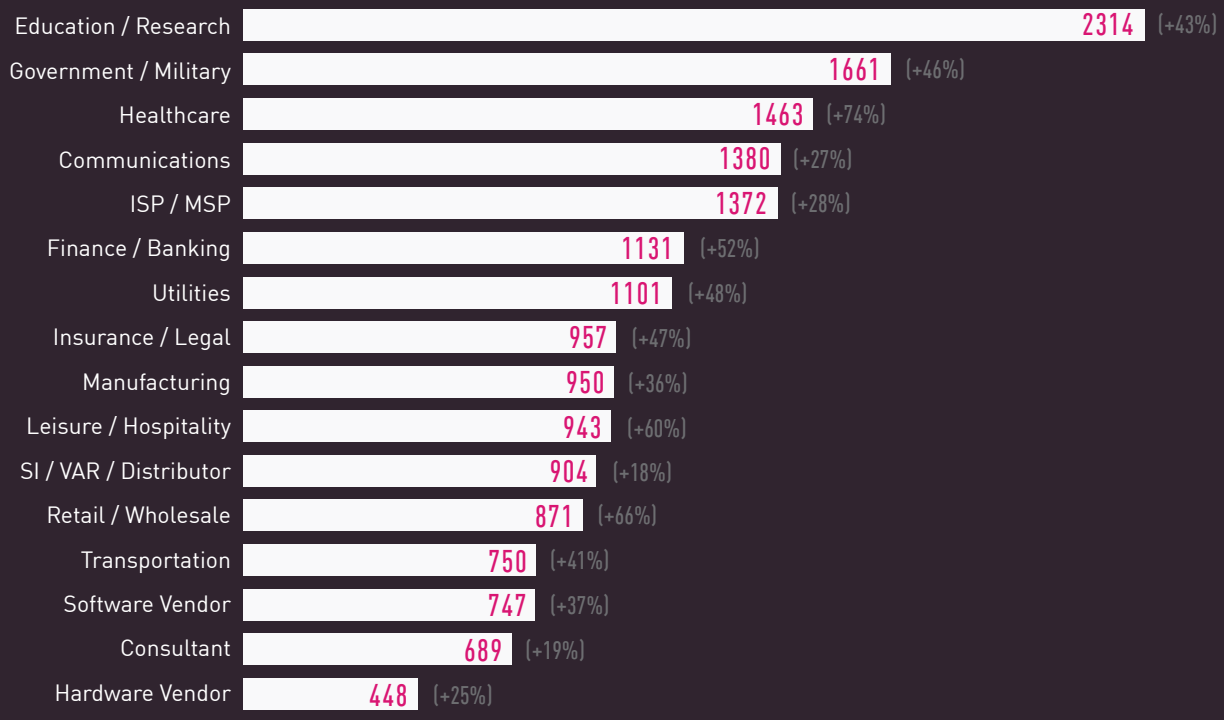


Figure 8 - Global Average of weekly attacks per organization by Industry in 2022 [% of change from 2021]

Data collected in 2022 shows a continued rise in attacks against all industries. Most targeted are the educational and research institutions, with an average of 2,314 attacks per week per organization, an increase of more than 40% from 2021. Attacks on the healthcare sector registered the highest surge, 74% more attacks than last year, placing it as the third most targeted industry in this index. From hospitals and clinics to research facilities, attackers have been focusing on the healthcare industry since the beginning of the COVID-19 pandemic, seeking financial gain. 89% of healthcare organizations reported cyberattacks within the last year with an average total cost reaching $4.4M. Reported attacks included the CommonSpirit Health, the second largest non-profit hospital chain in the US. CommonSpirit, which operates 140 hospitals, has reported data of more than 600K patients stolen, the attack resulting in medical damage to patients. Hospitals in New York were hit by ransomware in November leaving medical systems down for weeks after the attack. An attack on the Dallas-based Tenet health care cooperation, operating hundreds of medical sites, caused disruption to acute care operations. Among ransomware groups reported to target healthcare organizations are Lockbit, BlackCat, Cuba, Zeppelin and more.

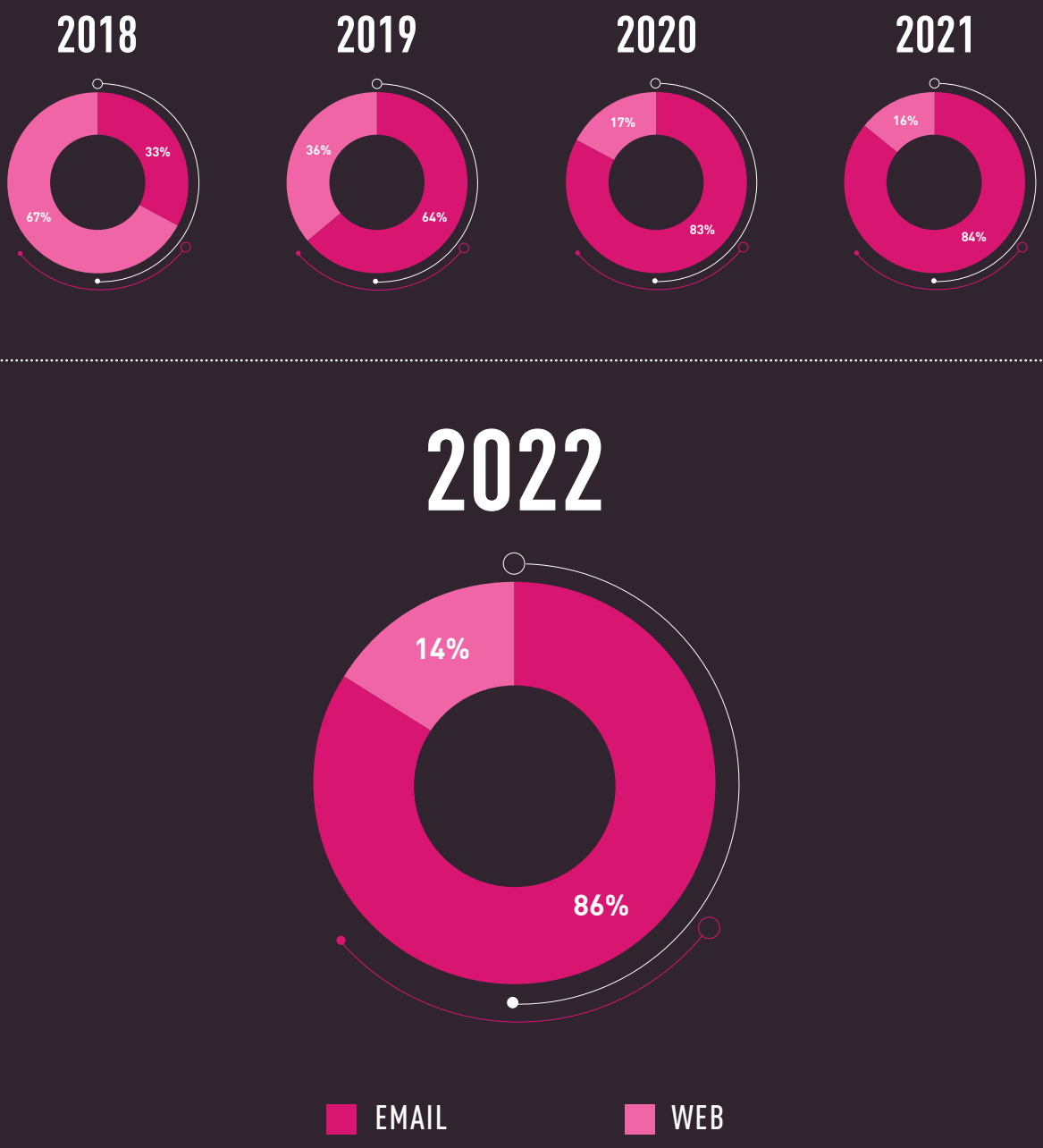


Figure 9: Delivery Protocols—Email vs. Web Attack Vectors in 2018-2022.

TOP MALICIOUS FILE TYPES—WEB VS. EMAIL

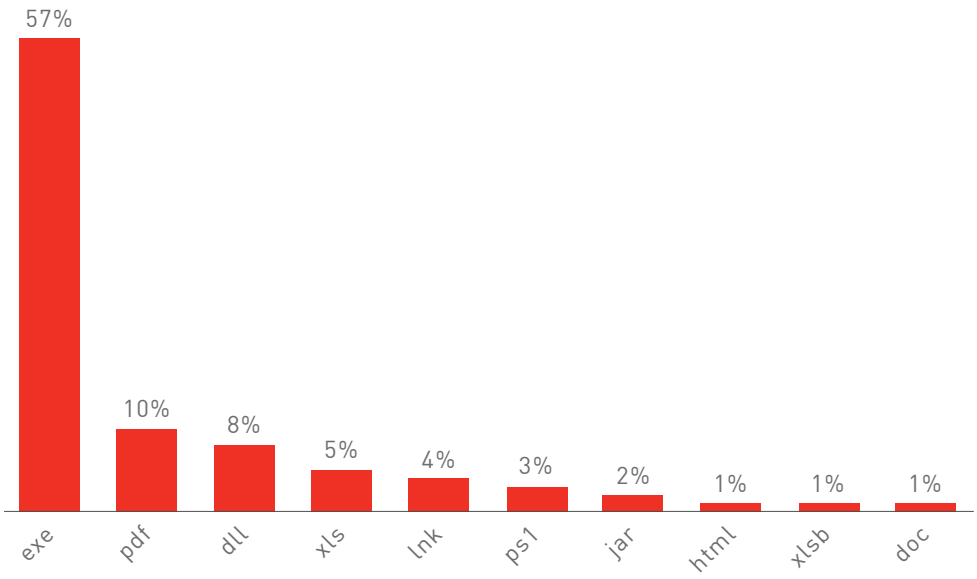


Figure 10: Web—Top malicious file types in 2022.

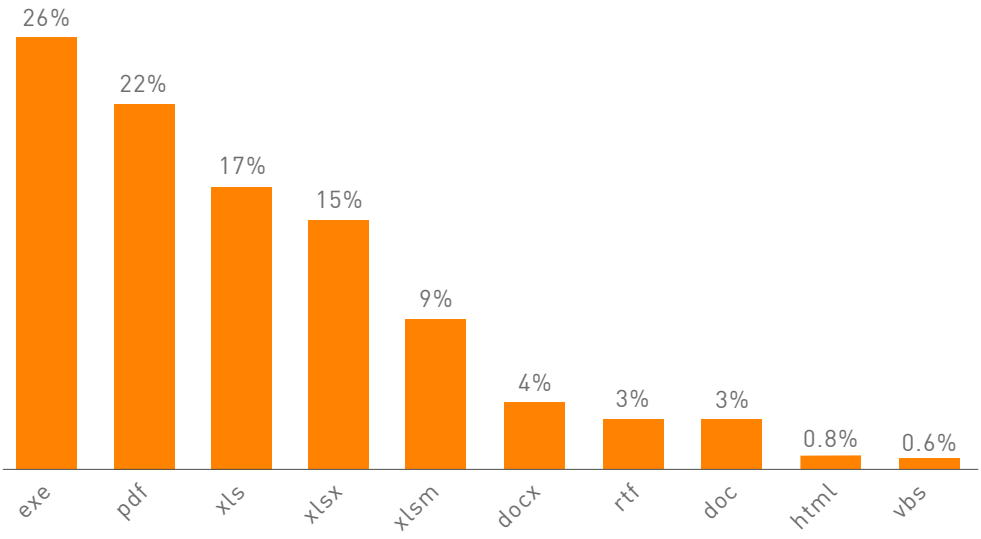


Figure 11: Email—Top malicious file types in 2022.

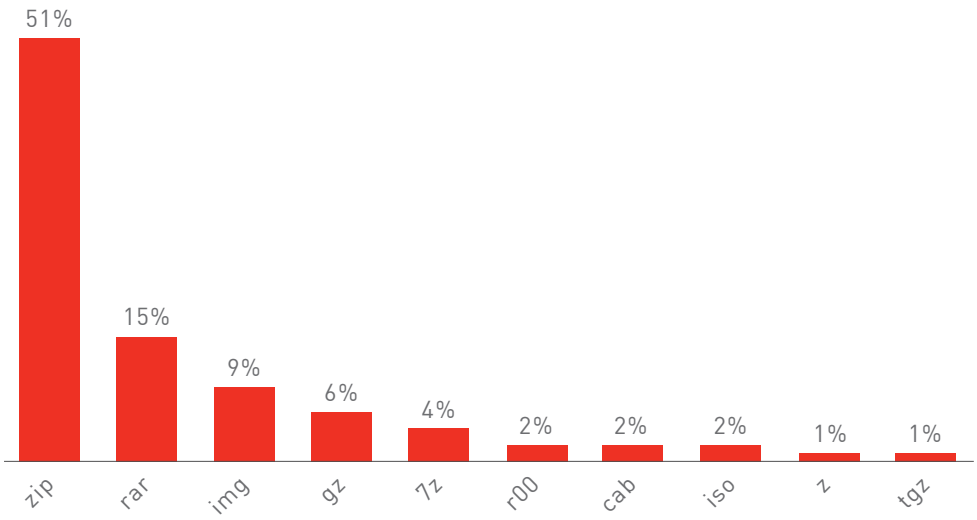


Figure 12: Top malicious archive files delivered by both Web and Email in 2022.

The proportion of email-delivered-attacks has increased, reaching a staggering record of 86% of all file based in-the-wild attacks. Data shows an increase in the utilization of various types of archive file formats, as threat-actors attempt to conceal malicious payloads. Included in password protected archives, the functionality of malware is hidden until they are extracted, making their identification as malicious by security products especially challenging. Zip files are the most commonly used format for this purpose, while in the top malicious archives types we observe also .img and .iso files, since their extraction functionality is integrated in Windows or with very popular tools. Archive files are often used to bypass the mark-of-the-web based protection mechanism.

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 December 2022.

For each of the regions below, we present the percentage of corporate networks impacted by each malware family, for the most prevalent malware in 2022.

GLOBAL

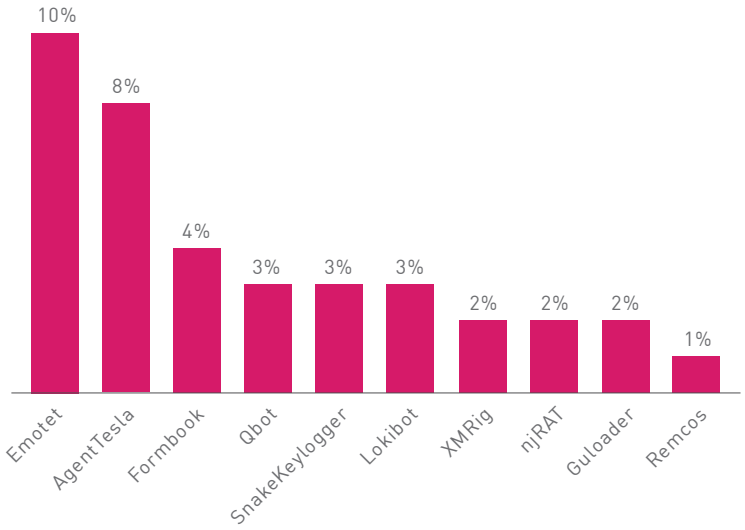


Figure 13: Most prevalent malware globally—2022

AMERICAS

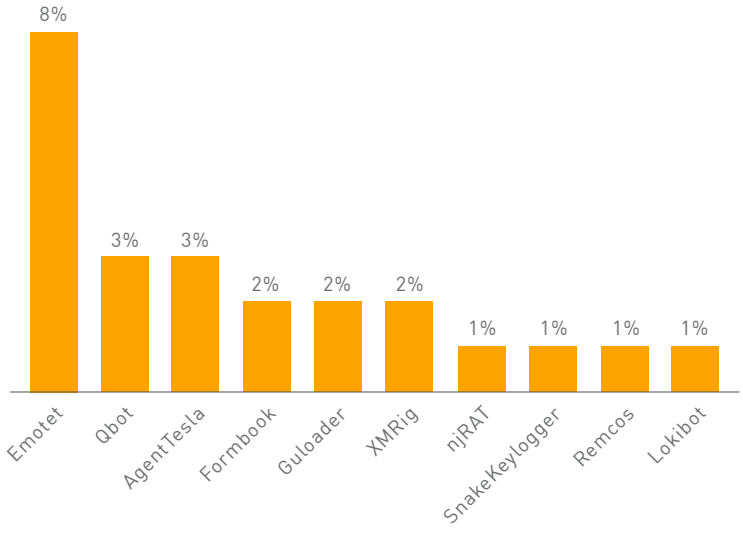


Figure 14: Most prevalent malware in the Americas—2022

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

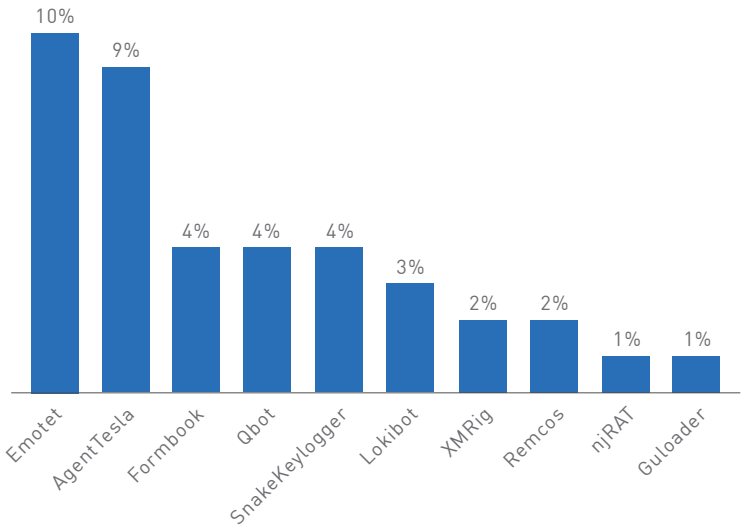


Figure 15: Most prevalent malware in EMEA—2022

ASIA PACIFIC (APAC)

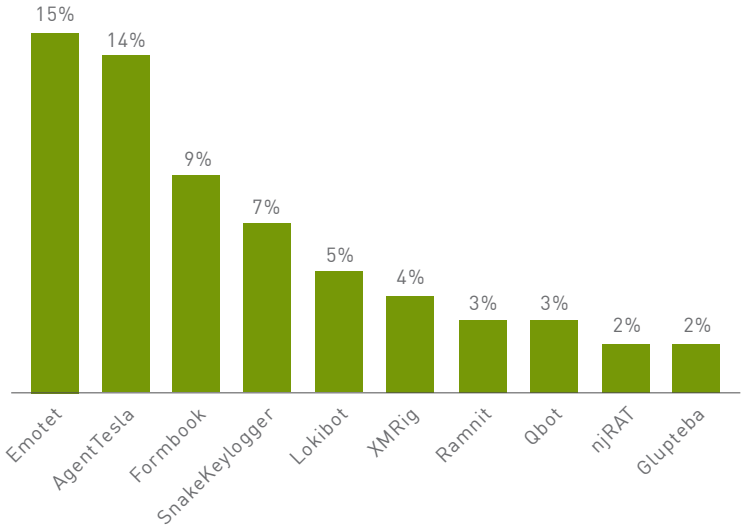


Figure 16: Most prevalent malware in APAC—2022

GLOBAL ANALYSIS OF TOP MALWARE

Rising back from its fourth place in Check Point's 2021 most prevalent malware list, Emotet has regained its position at the top of 2022 table, affecting 10% of all corporate networks. Initially discovered in 2014 as a banking Trojan, Emotet has developed into a significant multipurpose malware, serving as an initial access malware and used by sophisticated Eastern European cyber criminals. Identified as one of the major cyber threats, Emotet was taken down in January 2021, on a global law enforcement operation, only to resurge by the end of that year. On its return Emotet was distributed with Trickbot's assistance and later deployed large scale spam campaigns with malicious Office documents. Relying heavily on Office macros' exploitations, Microsoft's intension to disable VBA macros in documents obtained from the internet was expected to affect Emotet's distribution. Emotet's operators prepared for the change, experimenting with alternative file types including .lnk, .xll zip and .iso files. In November, Emotet returned from one of its routine breaks, and went back to its previous weapon of choice—Excel files with malicious macros. To bypass the Mark-of-the-Web limitations, the attached maldocs displayed detailed instructions directing users to copy the files into the trusted "Templates" folder. Emotet continues to use email threads hijacking technique and customizes email content according to the targeted country. Emotet was observed deploying other malware families like IcedID and XMRig on victim system. Other Emotet campaigns in 2022 include a campaign targeting IKEA employees; a US phishing campaign impersonating the IRS during the 2022 tax season and many more.

Infostealers occupied a central place in this year's table, with four of the most commonly used stealers, AgentTesla, Formbook, SnakeKeylogger and LokiBot occupying the top six places in our top malware list. The popularity of infostealers is connected to the growing market for stolen credentials and their availability to threat actors for relatively low prices. One of the emerging techniques of cyber cybercriminals is using infostealers for widely spread infections that are not specifically focused on corporate networks. After the initial infection, cybercriminals mine the data to identify corporate VPN credentials, which will allow them to get an initial access to corporate networks.

TOP MULTIPURPOSE MALWARE

GLOBAL

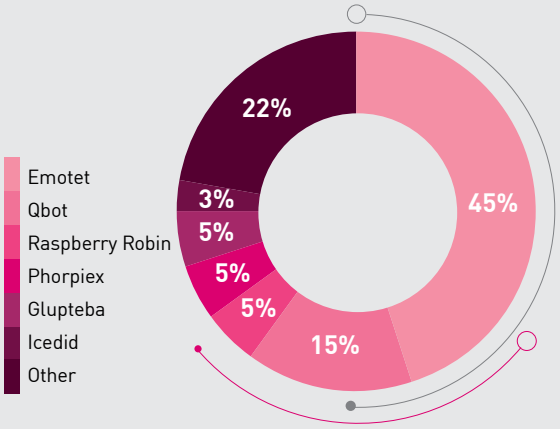


Figure 17: Most prevalent multipurpose malware globally

AMERICAS

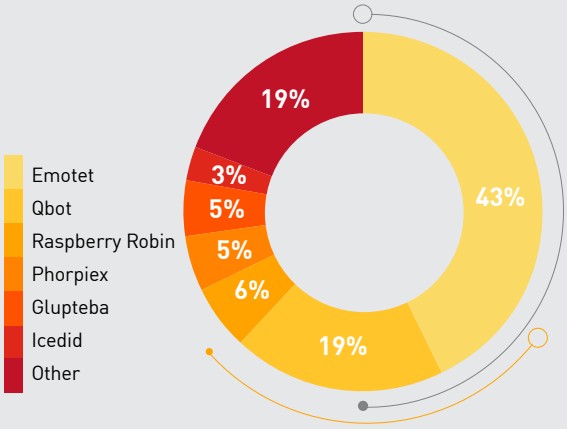


Figure 18: Most prevalent multipurpose malware in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

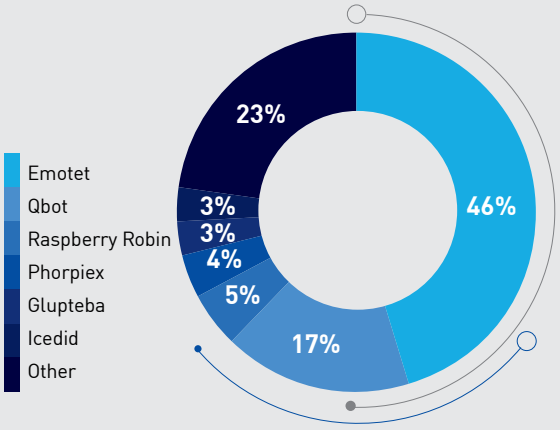


Figure 19: Most prevalent multipurpose malware in EMEA

ASIA PACIFIC (APAC)

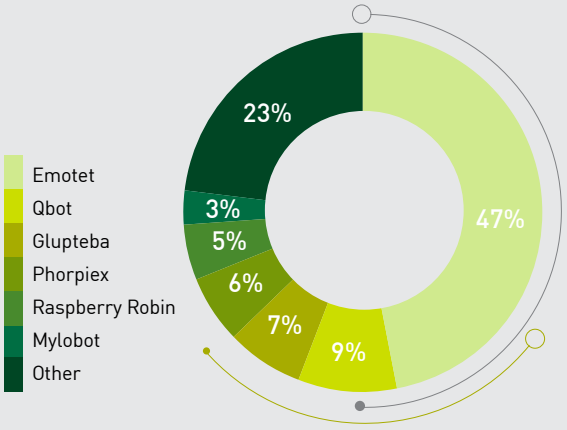


Figure 20: Most prevalent multipurpose malware in APAC

MULTIPURPOSE MALWARE GLOBAL ANALYSIS

As in our last midyear report, two malware categories, banking Trojans and botnets, which were previously classified as distinct types, have been merged. As many banking Trojans received additional functionalities, that make the differentiation between the two categories less distinct, we introduce the unified category, "multipurpose malware". Comparisons in this category therefore relate to the last midyear report rather than to older annual data.

Emotet and **Qbot** have increased their relative activity and now comprise of more than 60% of infection attempts in this category. **Raspberry Robin** is a new entrant to the multipurpose list. First detected in September 2021 using infected USB devices and wormable capabilities to spread, Raspberry Robin has become one of the largest active malware distribution platforms within a year. It was reported to deploy various other malware families, including IcedID, Bumblebee and ransomware brands like Clop and LockBit. With possible relations to Evil Corp this malware constitutes a serious new threat.

The **Phorpiex** botnet, which has been known for distributing other malware families via spam campaigns, as well as for fueling large-scale spam, sextortion campaigns and ransomware spread, started 2022 with crypto-transaction hijacking and continues its expansion, occupying the fourth place in the multipurpose table.

Glupteba has fully returned from the 2021 takedown operation carried out by Google. This malware features a variety of capabilities including a credential stealer, crypto miner, router exploiter and more. However, Glupteba is best known for its use of the bitcoin blockchain technology as its C&C infrastructure to receive configuration information. Glupteba's use of bitcoin records improves its resilience against takedowns, since the blockchain transactions cannot be deleted, however they remain exposed for public inspection. Tracking Glupteba's activity through the blockchain has exposed a large ongoing campaign which started in June 2022.

TOP INFOSTEALER MALWARE

GLOBAL

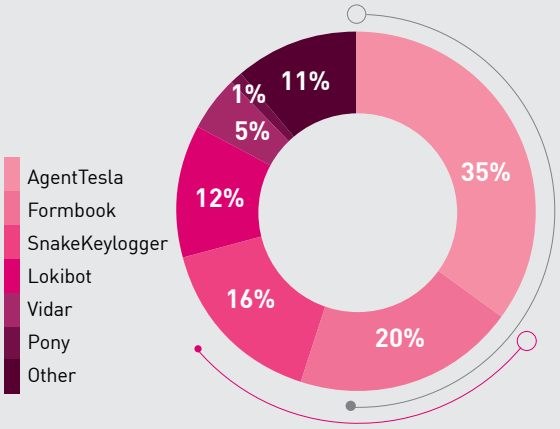


Figure 21: Top infostealer malware globally

AMERICAS

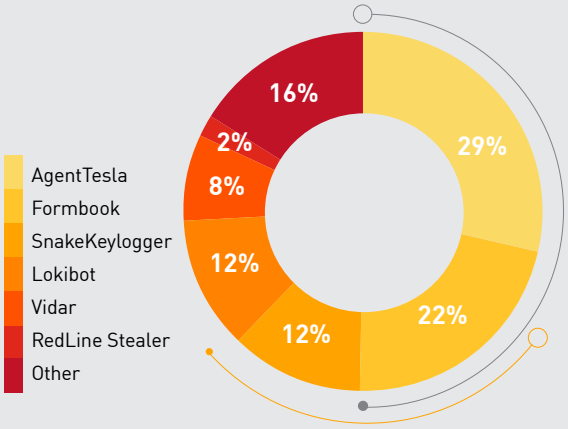


Figure 22: Top infostealer malware in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

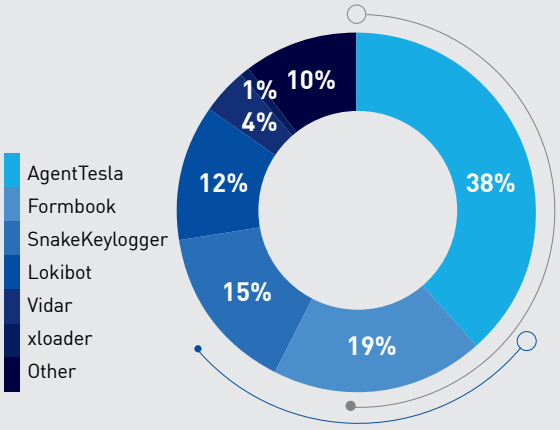


Figure 23: Top infostealer malware in EMEA

ASIA PACIFIC (APAC)

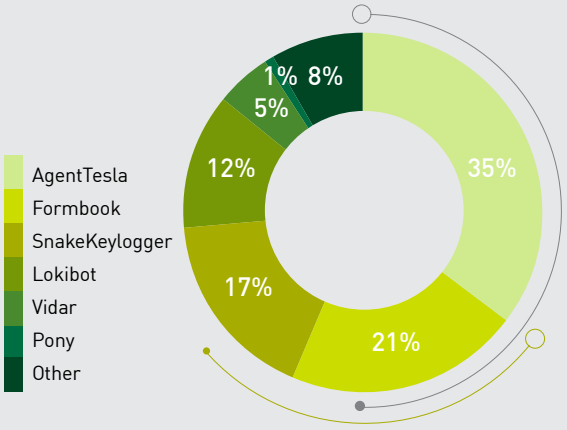


Figure 24: Top infostealer malware in APAC

INFOSTEALER MALWARE GLOBAL ANALYSIS

The growing market for stolen credentials and cookies, which are later used in the evolving life cycle of access-brokers, ransomware affiliates and RaaS suppliers, has contributed to the growing popularity of infostealers. Check Point data reveals a steady increase in infostealers use, affecting 18% of corporate networks in 2020, 21% in 2021 and reaching as much as 24% of all organizations in 2022. Infostealers are sold on underground forums for a monthly subscription fee that ranges between $60 to $1,000, to threat actors of varying levels of technical knowledge. This market, which was previously divided between multiple smaller malware families, has consolidated and this year three brands, AgentTesla, Formbook and SnakeKeylogger are responsible for 71% of Check Point monitored infostealers attacks.

Formbook, detected in 20% of infostealer cases is a commodity malware sold as-a-service on underground forums since 2016. It is designed to collect keystrokes, search and access files, take screenshots, harvest browser credentials and download and deploy additional payloads. It has been used by multiple actors, often distributed using email attachments including pdf, doc, RTF document, exe, zip, rar etc. Formbook has been deployed this year targeting Ukraine and in numerous other campaigns.

The **SnakeKeylogger** modular .NET infostealer has tripled its rank compared to our 2021 top malware statistics. 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. In August, researchers observed SnakeKeylogger in malspam campaign spreading via phishing emails to target IT firms located in the US.

TOP CRYPTOMINING MALWARE

GLOBAL

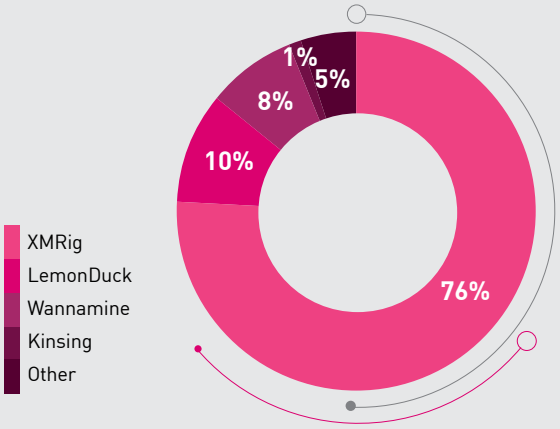


Figure 25: Top cryptomining malware globally

AMERICAS

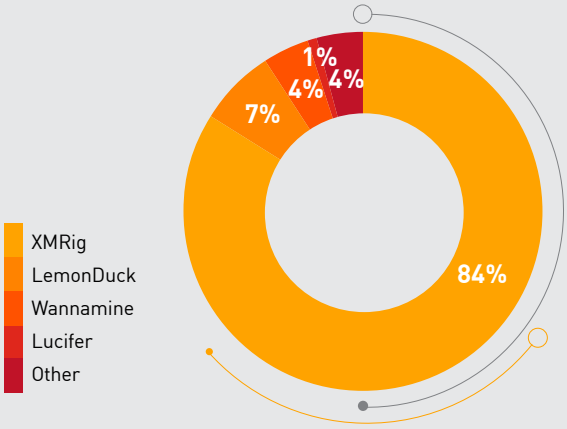


Figure 26: Top cryptomining malware in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

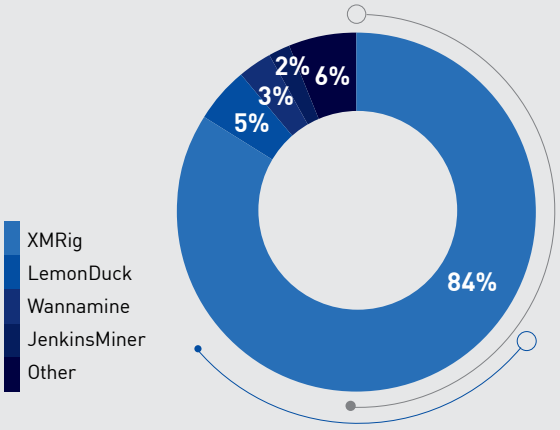


Figure 27: Top cryptomining malware in EMEA

ASIA PACIFIC (APAC)

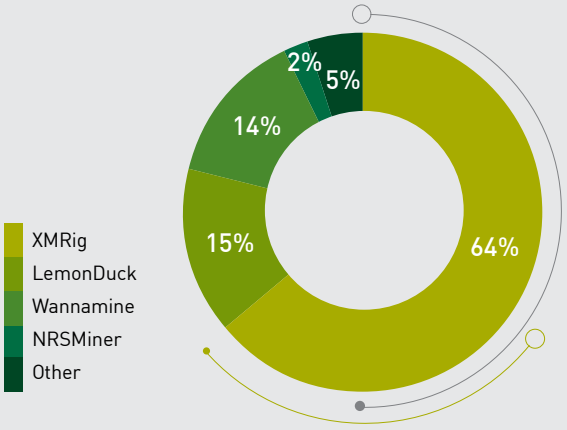


Figure 28: Top cryptomining malware in APAC

CRYPTOMINERS GLOBAL ANALYSIS

The crypto market cap has fallen dramatically in 2022, losing nearly $2 Trillion, from a record $2.9T in November 2021. Low crypto rates combined with increased mining costs affect mining profitability and with it the motivation for cryptomining. This explains cryptominers' visibility decreasing from 21% in 2021 to 16% globally in 2022. This decline has left XMRig, a legitimate open-source mining tool, as the most dominant tool used by attackers for malicious purposes. XMRig has been used in 76% of cryptomining attacks in 2022 and as reported in the CPIRT chapter often marks a breach which could later lead to the deployment of other malware.

LemonDuck, a relatively new cryptomining malware has no legitimate use, and since its initial detection in 2019 added 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 possible precursor for severe attacks.

TOP MOBILE MALWARE

GLOBAL

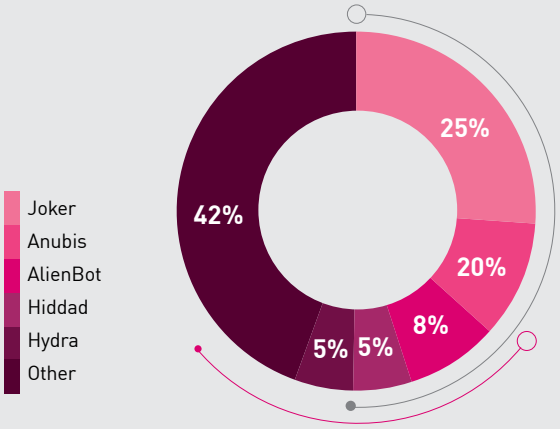


Figure 29: Most prevalent banking Trojans globally

AMERICAS

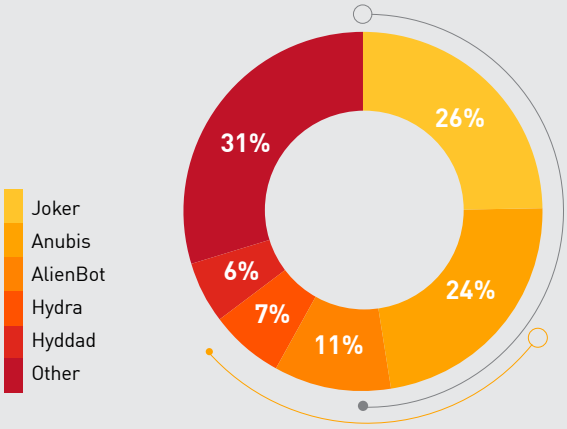


Figure 30: Most prevalent banking Trojans in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

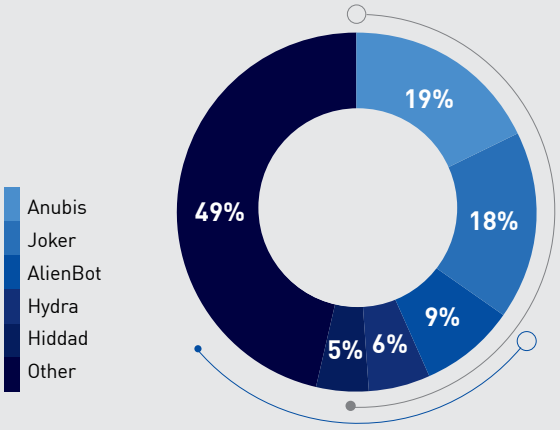


Figure 31: Most prevalent banking Trojans in EMEA

ASIA PACIFIC (APAC)

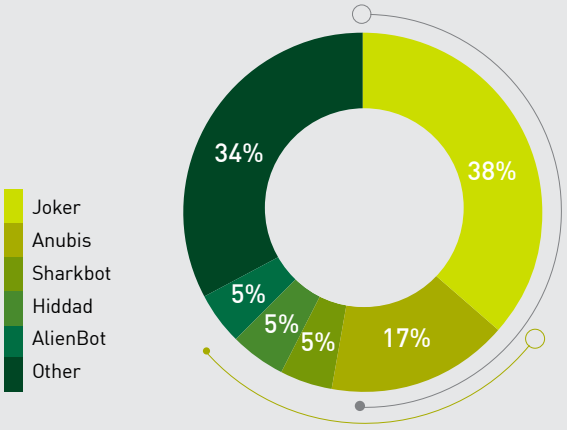


Figure 32: Most prevalent banking Trojans in APAC

MOBILE MALWARE GLOBAL ANALYSIS

Joker, an Android mobile malware, is a stealer capable of accessing SMS messages, contact lists and device information but mostly generates income through unauthorized subscriptions to paid premium services. Joker uses its access to SMS messages to authenticate requests and authorize payments. Joker (aka Bread) was first identified in 2017 concealed in more than 1,700 benign looking applications offered on Google Play Store. The malware has resurged this year, hiding in at least 8 applications on Google Store with more than 3 million downloads in 2022, climbing to the top of Check Point's global mobile malware list.

Anubis is a banking Trojan malware designed for Android mobile phones. Since it was initially detected in 2017, it has gained additional functions including Remote Access Trojan (RAT) functionality, keylogging, and audio recording capabilities. It has been detected on hundreds of different applications available in the Google Store reaching Check Points top mobile malware list earlier this year.

CHAPTER 5

05

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 cp<r> in 2022.

PROXYSHELL VULNERABILITIES (CVE-2021-34473, CVE-2021-34523 AND CVE-2021-31207)

This is the name given to an attack-chain which exploits three vulnerabilities in Microsoft's Exchange Server. Combining these vulnerabilities allows unauthenticated attackers to perform Remote Code Execution (RCE) on vulnerable servers. All three vulnerabilities have been reported and patched in 2021 they remain at the top of the most exploited vulnerabilities list even in 2022. Some of the reasons for their popularity with attackers are their simple exploitation, the prevalence of MS Exchange servers with government and large businesses and the fact they were thoroughly analyzed, and discussed by researchers. Check Point data shows that 21% of our customers have been impacted with ProxyShell attempts in 2022. ProxyShell vulnerabilities have been exploited for a variety of motivations including by financially motivated threat actors to deploy ransomware, for espionage in the Middle East and Africa and by Iranian APT entities to gain access to American, Australian, Canadian and UK entities. Check Point Incident Response Team (CPIRT) investigations found ProxyShell exploitations in one in every six attack cases. Together with ProxyLogon and the recently reported ProxyNotShell, these MS Exchange vulnerabilities constitute a significant attack surface, frequently exploited in the wild, often resulting in major breaches.

FOLLINA IN MICROSOFT OFFICE (CVE-2022-30190)

Reported in May 2022, this vulnerability in Microsoft Support Diagnostic Tool (MSDT) is exploited using Microsoft Office documents. Microsoft has gone a long way in their effort to reduce attacks utilizing office documents by disabling macros in documents from external sources. Exploiting the new Follina vulnerability, attackers are now using specially crafted .docx and .rtf documents to download and execute malicious code even in Protected Mode and when macros are disabled. Despite Microsoft's mitigation efforts, threat actors have exploited Follina in unpatched systems to deploy Qbot, and other RATs, making Follina one the most frequently used vulnerability discovered in 2022 contributing to the popularity of malicious office docs.

FORTINET CVE-2022-40684 AND CVE-2022-42475

Two critical bugs reported in October (CVSS score: 9.6) and December (CVSS score: 9.3) in Fortinet products allow unauthenticated attackers to execute arbitrary code via specially crafted requests. The company notified of in-the-wild exploitations and issued updates while CISA warned of significant risk to the federal enterprise. Exploitation attempts of CVE-2022-40684 in the last 3 month impacted 18% of organizations.

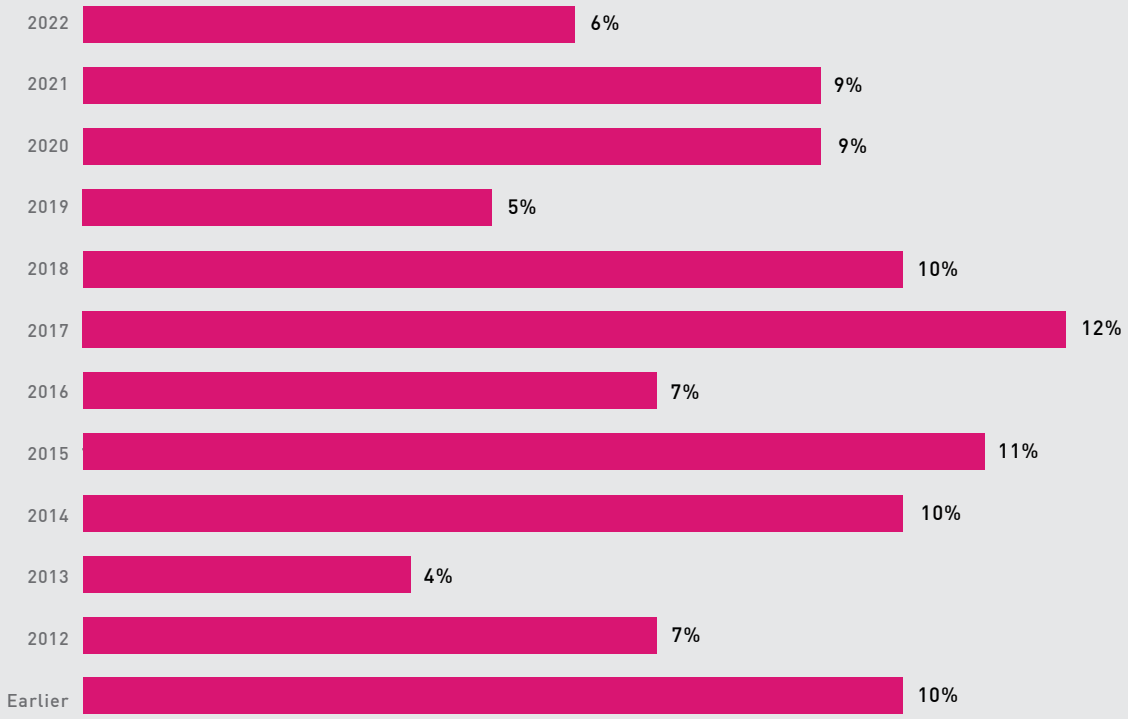


Figure 33: Percentage of attacks leveraging vulnerabilities by Disclosure Year in 2022.

New vulnerabilities discovered and reported in 2022 have been quickly weaponized and used by threat actors this year. Compared to only 2% of attacks in 2021 using same-year vulnerabilities, this year they were observed in 6% of the attacks monitored by Check Point. In addition to the vulnerabilities reviewed above, the Atlassian Confluence RCE (CVE-2022-26134) and F5 BIG IP (CVE-2022-1388) reviewed in our midyear report contributed their share to new exploitation attempts. Our data shows that vulnerabilities reported in the last three years made up 24% percent of exploitation attempts compared to only 18% in 2021. This indicates an upgrade in threat actors' competence and integration ability, especially manifested in cloud based attacks, with 27% of the attacks leveraging new vulnerabilities (2020-2022). Exploitation of older vulnerabilities continued with widely used 2017 CVEs including, Apache Struts2

Remote Code Execution (CVE-2017-5638) which is used by botnets and the PHPUnit remote code execution (CVE-2017-9841), still used to exploit vulnerable WordPress plugins. Information collected by the CPIRT (Check Point Incident Response Team) shows the proportion of newly reported vulnerabilities in successful attacks is even higher, with the ProxyShell vulnerabilities alone used in 17% of investigated cases. This demonstrates that while 4-5 year old vulnerabilities' exploitation attempts are widespread, successful attacks more often rely on newly discovered flaws, exploited before patched. The "long tail" phenomenon of vulnerability exploitation persists, with 50% of attacks in the wild targeting vulnerabilities reported before 2017. These are mostly less effective and used by less advanced attackers. These findings once again highlight the importance of timely system patching.

06 INCIDENT RESPONSE PERSPECTIVE

(A specific case investigated by CPIRT in 2022 is highlighted in the boxed text. Other text includes observations and data referring to all cases handled in 2022. Certain details have been modified to ensure customer confidentiality)

On a Monday morning in March 2022, the Check Point Incident Response Team (CPIRT) received a call from a medium-sized European technology company which had been the victim of a Quantum Locker ransomware attack deployed early in the morning the day before. Robert, the company's CISO, was on the line. Thus began a typical workday in the life of an IR analyst, which is often one of the worst days of the customers' (professional) life.

Unlike the analysis 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 perspective of the Check Point Incident Response Team who provide attack mitigation services in response to various types of active breaches, and not specific to Check Point customers.

Robert reported that most of their data center servers, including the Domain Controllers and File Servers, had been encrypted and rendered non-functional. With no backups, their entire operation came to a halt and they were in need of assistance to investigate and mitigate this attack. CPIRT's mission was to look for ongoing vulnerabilities and malicious activity, resume network functionality, and perform root cause analysis to identify the initial attack vector and prevent future attacks.

CPIRT involvement usually follows the discovery of visible malicious activity, such as encrypted files (ransomware), detection of spoofed or forged emails (email compromise), or the presence of malware files or unknown processes on a computer system. CPIRT's breakdown of the initial threat indication provides a different perspective of the threat landscape than the one routinely provided by our product data.

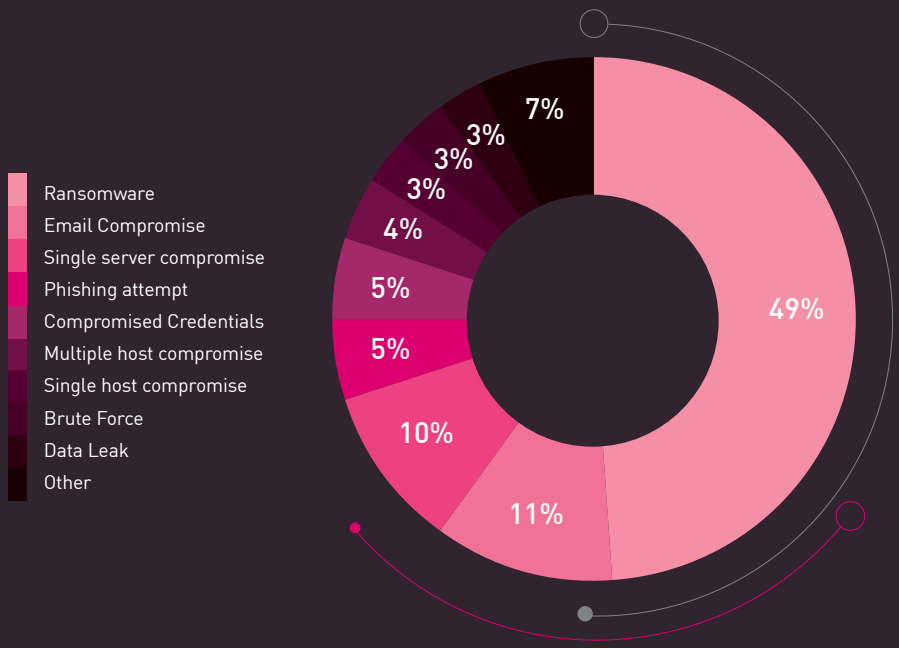


Figure 34: Breakdown of CPIRT cases by initial threat indication in 2022

DANIEL WILEY
Head of Threat Management and Chief Security Advisor, Check Point Software Technologies

"Analysis of the initial threat indications as seen by CPIRT in 2022 indicates that almost 50% of investigations involve ransomware infections. The threat breakdown above is different from what we see in our product data, which places multipurpose malware and infostealers at the top of the threat list. However, CPIRT data shows that the biggest risks that are visible from a large corporate perspective—are full-blown ransomware attacks and full network compromises. Product telemetry that records multipurpose malware activity often just shows the initial incursion which if prevented, blocks much larger damage.

After the initial CPIRT forensic investigation, it became clear that the entry point to the organization was the company's exchange server. The server had not been patched and was vulnerable to two very popular exploits used by threat actors since 2021: the same group of vulnerabilities used by Hafnium (CVE-2021-26855 and CVE-2021-26855, CVE-2021-26857 or CVE-2021-26858) and the ProxyShell vulnerabilities (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207).

In almost half of CPIRT cases, the initial foothold is achieved by exploiting a vulnerable server with an unpatched RCE vulnerability and open ports to the internet. In fact, ProxyShell vulnerabilities specifically were the cause of one in every six incidents CPIRT investigated in 2022, despite those vulnerabilities being disclosed and patched in 2021.

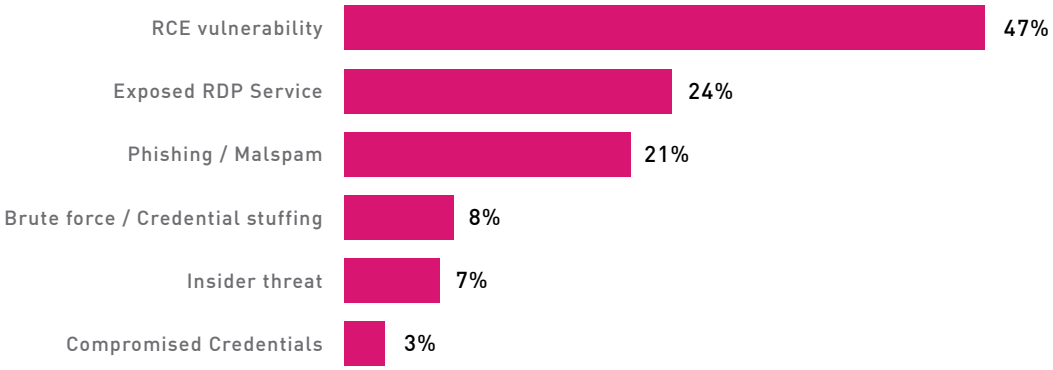


Figure 35: Breakdown of the initial entry vector in CPIRT cases in 2022

An exposed RDP service is often used by attackers in combination with an RCE vulnerability or password attacks such as brute force or credential stuffing attack to gain a foothold in the network. Mail servers are often the weak link in a network and are a common initial entry point for attackers and more easily encrypted. That is because, due to performance considerations, endpoint security and anti-ransomware products are frequently not installed on servers. Combined with the high number of vulnerabilities, network exposure and poor patch management, in many organizations, it's the servers and not the peripheral endpoints that are the weakest point and are therefore exploited in many attacks.

> *Further analysis revealed that the same vulnerable Exchange server had been exploited twice, in incidents nine months apart. The first exploitation of the server occurred in June 2021. Initially, "only" a cryptominer was installed, utilizing multiple assets across the network.*

This emphasizes the need to treat every breach as seriously as a full-blown ransomware attack. As in this case, cryptominers and other "minor" malware types are often initial indicators of possible exploitation that could lead to cyber disasters later on.

> *Persistence in this attack was achieved by changing a registry key to periodically connect and download an external resource. Initially, this was a cryptominer installed on dozens of machines, but the resource could easily have been changed to another payload. By the end of the initial attack in mid-2021, the attackers leaked a list of network assets in the network, and used Mimikatz to harvest credentials from the infected network. Some of the harvested passwords were NTLM hashes which, due to the practice of simple passwords, were easily reverse-engineered to the plain text version.*

CPIRT case statistics reveal extensive utilization by attackers of non-signature tools. The top tools used this year were Cobalt Strike and Mimikatz. However, for the first time, the third most popular tool in this list, AnyDesk, is a legitimate admin tool. As threat actors have started using more legitimate admin tools in their attacks, the use of customized malware built by the same threat actors has declined, and we are seeing an increase in attacks that might not include any malware at all. This shift in the tools deployed by attackers is detailed in a dedicated chapter in this report.

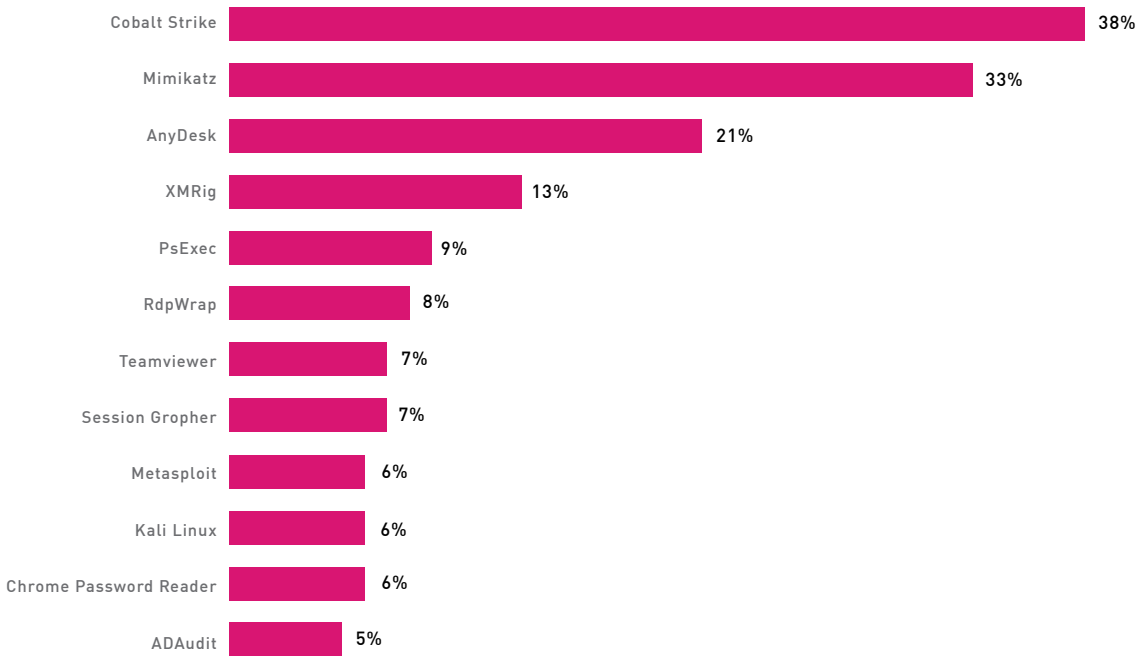


Figure 36: Tools used on compromised systems in 2022 CPIRT cases.

During the second breach in March 2022, the attackers used the data retrieved nine months earlier. The asset list and credential dump stolen during the first attack were now used to enable and direct the ransomware deployment.

Stolen credentials and initial access to corporate networks are now often traded between threat actors or sold by "initial access brokers". The outsourcing of more and more parts of the attack process, and the further fragmentation of the threat landscape, complicates attribution efforts. For these reasons, in many of CPIRT cases in 2022, the attack attribution was *not* to a very well-known or common threat group. We have also seen multiple malware families used in a single attack, for example, the use of IceID to deliver RansomEXX.

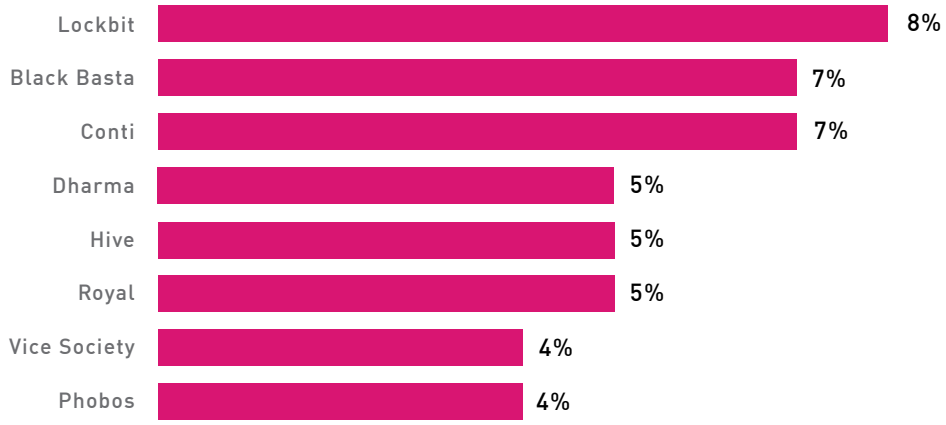


Figure 37: Top Ransomware Families seen in IR cases in 2022

> *While the first attack went relatively unnoticed, the second attack resulted in the encryption of critical servers and ensuing serious damage. But there is a happy ending: at the end of a long, nerve-wracking process, thanks to CPIRT assistance, Robert was able to recover his company's data and resume normal business activity.*

This case is one of many dozens handled by CPIRT in 2022 that emphasizes the critical importance of the following:

- Patch immediately when an update is available.
- Impose a complex password policy with frequent updates.
- Use endpoint security and anti-ransomware on critical systems.

As Robert can attest, these actions prevent corporate catastrophes.

CHAPTER 7

07

2023 INSIGHTS FOR CISOS: DISRUPTION AND DESTRUCTION

EXPECT INCREASED GLOBAL ATTACKS ON BUSINESSES, STRICTER GOVERNMENT REGULATIONS AND MORE

CISOs had to deal with a lot in 2022. Global attacks increased by 28% in the third quarter of 2022 compared to same period in 2021, and the average weekly attacks per organization worldwide reached over 1,130. As we look ahead to 2023, that trend shows no signs of slowing down with increases in ransomware exploits and state-mobilized hacktivism driven by international conflicts. At the same time, organizations' security teams and CISOs will face growing pressure as the global cyber workforce gap of 3.4 million employees widens further, and governments introduce stricter cyber regulations to protect citizens against breaches.

In 2022, cyber criminals and state-linked threat actors continued to exploit organizations' hybrid working practices as businesses shifted to decentralized workforces, and the increase in these attacks is showing no signs of slowing down as the Russia—Ukraine conflict continues to have a profound impact globally. Organizations need to consolidate and automate their security infrastructure to enable them to better monitor and manage their attack surfaces and prevent all types of threat with less complexity and less demand on staff resources.

2023 INSIGHTS: WHAT SHOULD CISOS BE LOOKING OUT FOR, AND WHAT DOES IT MEAN FOR YOUR ORGANISATION?

Hikes in destructive malware and impactful hacking exploits

- No respite from ransomware: this was the leading threat to organizations in the first half of 2022, and the ransomware ecosystem will continue to evolve and grow with smaller, more agile criminal groups forming to evade law enforcement.
- Compromising collaboration tools: while phishing attempts against business and personal email accounts are an everyday threat, in 2023 criminals will widen their aim to target business collaboration tools such as Slack, Teams, OneDrive and Google Drive with phishing exploits. These are a rich source of sensitive data given most organizations' employees often continue to work remotely.

MAYA HOROWITZ

Vice President, Research, Check Point Software Technologies

> Ransomware threat actors will continue to carry out double extortions—encrypting network and sending out the data—as big money comes from the data breach. But we will also start to see more attacks where extortion is only related to a data breach with no encryption taking place, meaning that whilst the data is stolen, it can still be used.

JEREMY FUCHS

Researcher/Analyst, Avanan (a Check Point Software Company)

> When looking at compromised collaboration tools, there will be more sophisticated attacks within multiple domains, known as 5th Gen attacks, as the attack may start with email but move to the network, firewall and more. This can all take months to unfold. We are also seeing a rise in "static expressway" where you can create static 'allow lists' so everything from Google is allowed. This is common because it is hard to go through all domains. For example, we can create something malicious on a popular site and know that the receiving party will get it, with a good proportion clicking on it because it is a real Paypal/Quickbook invoice, but with a virus attached. This could expand to other trusted brands. With phishing, attackers use a fake email but in these cases, it seems legitimate, so both the user and security system are at a loss.
>
> With the move to collaboration tools such as Slack and Teams over the pandemic period, there will be an increase of attacks using these platforms. Most attacks so far have been via email, but it could happen through any application or via services that use the same logins. There is a perception that Teams is impervious to attack, which means users are loose with sharing data and personal information, but this is not the case. Business Email compromise has resulted in $2.4B in losses, but in reality, perhaps it should be renamed **business collaboration compromise.**

HACKTIVISM AND DEEPFAKES EVOLVE WITH ATTACKS ON NATIONAL ORGANISATIONS AND GOVERNMENT AGENCIES

- **State-mobilized hacktivism:** In the past year, hacktivism has evolved from social groups with fluid agendas (such as Anonymous) to state affiliated groups that are more organized, structured and sophisticated. Such groups have attacked targets in the US, Germany, Italy, Norway, Finland, Poland and Japan recently, and these ideological attacks will continue to grow in 2023.

- **Weaponizing deepfakes:** In October 2022, a deepfake of U.S. President Joe Biden singing 'Baby Shark' instead of the national anthem was circulated widely. Was this a joke, or an attempt to influence the important U.S. mid-term elections? Deepfakes technology will be increasingly used to target and manipulate opinions, or to trick employees into giving up access credentials.

SERGEY SHYKEVICH

Threat Intelligence Group Manager, Check Point Software Technologies

"The lines between nation state actors, cybercriminals and hacktivists will continue to blur. We will see more hacktivists groups in support of nation-state narratives, and nation-state actors learning techniques from veteran cybercriminals. All of this makes it harder to attribute attacks to any one group, so organizations will have to build proper cyber protections against all types of threat actors.

CLOUD-BASED AND IOT SOLUTIONS— "VULNERABLE BY DESIGN" AFFECTS BUSINESS ATTACK VECTORS

- Cloud gets more complicated: It is clear that the increased use of cloud based and IoT solutions has presented new challenges for security professionals. With less control and visibility over where data is stored and how it is accessed, it can be difficult to ensure that access to sensitive information is properly secured. This is especially true in industries like healthcare and manufacturing, where IoT-based sensors and devices are becoming more prevalent. Additionally, the use of devices such as cameras, printers, and smart TVs for video conferencing have introduced new vulnerabilities. Overall, it is important for organizations to take steps to ensure the security of their cloud based and IoT systems as they will continue to be central and trendier pieces of any IT environment, including implementing proper access controls and regularly monitoring for potential vulnerabilities.

MUHAMMAD YAHYA PATEL

Global Cybersecurity Evangelist, Check Point Software Technologies

"Vulnerability exploitation is prevalent as attackers are exceptionally quick at finding holes in well-known products widely used by organizations. That is why it is important to patch, patch, patch and keep up with updates as a minimum, as these simple security measures are usually overlooked.

> I expect to see cloud transformation slow down due to cost and complexity, with many companies considering the action of bringing workloads back in-house, or at least to private data centers. This could help in reducing the overall threat surface.

DERYCK MITCHELSON

Field CISO EMEA,
Check Point Software
Technologies

GOVERNMENTS STEP UP MEASURES TO PROTECT CITIZENS AND ORGANIZATIONS

- **New laws around data breaches:** the breach at Australian telco Optus has driven the country's government to introduce new data breach regulations to protect customers against subsequent fraud, with new laws introduced lifting maximum penalties for serious or repeated breaches from the current A$2.22million to the greater of A$50 million. Similar measures by the British Government were introduced with a new mandatory reporting obligation on MSPs (Managed Service Providers) to disclose cyber incidents or be fined £17 million for non-compliance. In Australia, the government is also considering imposing a ban on ransoms to cybercriminals leading other national governments to possibly follow this example in 2023, in addition to existing measures such as GDPR.

- **New national cybercrime task forces:** More governments will follow Singapore's example of setting up inter-agency task forces to counter ransomware and cybercrime, bringing businesses, state departments and law enforcement together to combat the growing threat to commerce and consumers. These efforts are partially a result of questions over whether the cyber-insurance sector can be relied upon as a safety net for cyber incidents. The EU has also strengthened its cybersecurity and resilience with its new directive, NIS2. NIS2 will set the baseline for risk management and reporting across all sectors including energy, health and critical infrastructure.

- **Mandating security and privacy by design:** The automotive industry has already moved to introduce measures to protect the data of vehicle owners. This example will be followed in other areas of consumer goods that store and process data, holding manufacturers accountable for vulnerabilities in their products.

ASHWIN RAM

Cybersecurity Evangelist, Check Point Software Technologies

"To prevent highly sensitive data from falling into the wrong hands, CISOs must focus on understanding where the organizations' crown jewels are stored, including within 3rd party systems. CISOs should take into consideration who and what has access to their data, think APIs, and prioritize Zero Trust implementation. This means enforcing the principle of least privilege so that users and systems are granted the bare minimum access to resources, to do their job.

"Attacks on critical infrastructure will continue to increase with threat actors becoming more shameless, though they will be more difficult to conduct and require special tools. Key sectors such as energy, telecommunications and healthcare are targeted because they have so much to lose, and are more likely to pay. Though attacks on the education sector is random, attacks will continue because of how the networks are built.

MAYA HOROWITZ

Vice President, Research, Check Point Software Technologies

ZERO-DAY VULNERABILITIES IN SUPPLY CHAIN AND SOFTWARE CODE CAN BE EXPLOITED, DESTROYING DAY-TO-DAY BUSINESS OPERATIONS

- **Zero-day vulnerabilities continue to plague businesses:** While these vulnerabilities are typically discovered and patched by white hat hackers before they are made public, they can be easily exploited once they are found. This has not happened yet, as most threat actors are more interested in exploiting vulnerabilities that are easier to access. The proxy logon vulnerability, which was discovered last year, is still the most exploited vulnerability simply because it is effective. However, if a threat actor were to find and exploit a zero-day vulnerability before it was patched, the damage could be devastating and destructive. Until recently, there have not been many threat actors with the motivation to take down as many networks as possible, but the current climate of chaos and changing motivations may lead to more attempts to exploit such zero-day vulnerabilities. Patching and keeping software up to date is a critical mission.

PETE NICOLETTI

Field CISO, Americas, Check Point Software Technologies

> **Supply Chain Attacks and breaches will continue accelerating over the next year. Most companies do not do a good enough job with managing the risk of the components they are using and do not have visibility into their SBOM nor a complete strategy, much less an understanding of where the gaps are.**

CONSOLIDATION AS A SOLUTION TO EVOLVING CORPORATE CYBER CHALLENGES

Cutting complexity to reduce risks: Organizations have more complex, distributed networks and cloud deployments than ever before because of the pandemic. With so many elements to consider, security teams need to consolidate their IT and security infrastructures to improve their defenses and reduce their workload to help them stay ahead of threats. The statistics speak for themselves, where over two-thirds of CISOs stated that working with fewer vendors' solutions would increase their company's security. Security teams need to consolidate their IT and security infrastructures to improve their defenses and reduce their workload to help them stay ahead of threats.

JONATHAN 'JONY' FISCHBEIN

CISO,
Check Point Software Technologies

> The industry as a whole has made great strides in decreasing the number of solutions to reduce the complexity. Historically companies were using 15-17 solutions. Now CISOs are trying to cut down the number of solutions to reduce complexity, leading the industry to turn to consolidation as an answer. We suggest a management dashboard that allows security professionals to reduce the level of complexity when dealing with security issues.

DERYCK MITCHELSON

Field CISO EMEA,
Check Point Software
Technologies

> Consolidation will become a "real" priority in 2023, especially as businesses look to remove cost, heightened with the much talked about recession, and more importantly, complexity from entire digital and security stack.

ANTOINETTE HODES

Solutions Architect
& Evangelist, EMEA,
Check Point Software
Technologies

> Organizations need to consider the new 'work from home' realm and how to address security challenges from the hybrid and remote workforce as they may not have as strong a security posture as the organizations they belong to. With these workers leveraging the network, preventing such attacks through these new vector needs to be considered. Consolidating the entire cybersecurity posture would be a step in the right direction.

CHAPTER 8

08

PREVENTION IS AT REACH

BECOMING A VICTIM IS NOT PREDESTINED—PREVENTION IS AT REACH

Zero-day attacks are unknown cyber risks that easily circumvent signature-based security solutions and therefore pose an exceptionally dangerous risk to businesses. **Ransomware** attacks became a central cyber threat and oppose a disruptive factor globally to organizations, corporates and even governments. **Phishing** attacks can have several different goals, including malware delivery, stealing money, and credential theft. However, most phishing scams designed to steal your personal information can be detected and their sometime enormous damage can be prevented. **A Data breach** can ravage an organization. A data breach often results in expensive security audits, fines and stakeholders often lose trust in the organization as a result. The rapid rise of high-profile data breaches shows it is critical for security professionals to reexamine their current security strategies and implement unified security across network, cloud, and mobile environments in an effort to prevent the next breach. **Modern Cloud Applications** brings new security challenges to developers which needs to make sure thery are preventing code leaks and other potential breaches that can be disastrous.

In this section, we provide security professionals practical recommendations that can mean the difference between joining the growing statistics of cyber victims and preventing the next one.

HOW TO PREVENT RANSOMWARE ATTACKS

There are several actions that a company can take to minimize their exposure to and the potential impacts of a ransomware attack.

1. Robust Data Backup

The goal of ransomware is to force the victim to pay a ransom in order to regain access to their encrypted data. However, this is only effective if the target actually loses access to their data. A robust, secure data backup solution is an effective way to mitigate the impact of a ransomware attack. If systems are backed up regularly, then the data lost to a ransomware attack should be minimal or non-existent. However, it is important to ensure that the data backup solution cannot be encrypted as well. Data should be stored in a read-only format to prevent the spread of ransomware to drives containing recovery data.

2. Cyber Awareness Training

Phishing emails are one of the most popular ways to spread ransom malware. By tricking a user into clicking on a link or opening a malicious attachment, cybercriminals can gain access to the employee's computer and begin the process of installing and executing the ransomware program on it. With the global gap in cybersecurity talent impacting organisations around the world, frequent cybersecurity awareness training is crucial to protecting the organization against ransomware, leveraging their own staff as the first line of defence in ensuring a protected environment. This training should instruct employees to do the following:

- Not click on malicious links
- Never open unexpected or untrusted attachments
- Avoid revealing personal or sensitive data to phishers
- Verify software legitimacy before downloading it
- Never plug an unknown USB into their computer
- Use a VPN when connecting via untrusted or public Wi-Fi

3. Up-to-Date Patches

WannaCry, one of the most famous ransomware variants in existence, is an example of a ransomware worm. Rather than relying upon phishing emails or Remote Desktop Protocol (RDP) to gain access to target systems, WannaCry spread itself by exploiting a vulnerability in the Windows Server Message Block (SMB) protocol. At the time of the famous WannaCry attack in May 2017, a patch existed for the EternalBlue vulnerability used by WannaCry. This patch was available a month before the attack and labeled as "critical" due to its high potential for exploitation. However, many organizations and individuals did not apply the patch in time, resulting in a ransomware outbreak that infected 200,000 computers within three days. Keeping computers up-to-date and applying security patches, especially those labeled as critical, can help to limit an organization's vulnerability to ransomware attacks as such patches are usually overlooked or delayed too long to offer the required protection.

4. Strengthening User Authentication

Cybercriminals commonly use the Remote Desktop Protocol (RDP) and similar tools to gain remote access to an organization's systems using guessed or stolen login credentials. Once inside, the attacker can drop ransomware on the machine and execute it, encrypting the files stored there. This potential attack vector can be closed through the use of strong user authentication. Enforcing a strong password policy, requiring the use of multi-factor authentication, and educating employees about phishing attacks designed to steal login credentials are all critical components of an organization's cybersecurity strategy.

5. Anti-Ransomware Solutions

While the previous ransomware prevention steps can help to mitigate an organization's exposure to ransomware threats, they do not provide perfect protection. Some ransomware operators use well-researched and highly targeted spear phishing emails as their attack vector. These emails may trick even the most diligent employee, resulting in ransomware gaining access to an organization's internal systems. Protecting against this ransomware that "slips through the cracks" requires a specialized security solution. To achieve its objective, ransomware must perform certain anomalous actions, such as opening

and encrypting large numbers of files. Anti-ransomware solutions monitor programs running on a computer for suspicious behaviors commonly exhibited by ransomware, and if these behaviors are detected, the program can take action to stop encryption before further damage can be done.

6. Utilize better threat prevention

Most ransomware attacks can be detected and resolved before it is too late. You need to have automated threat detection and prevention in place in your organization to maximize your chances of protection.

- **Scan and monitor emails.** Emails are a common choice of cybercriminals executing phishing schemes, so take the time to scan and monitor emails on an ongoing basis, and consider deploying an automated email security solution to block malicious emails from ever reaching users.
- **Scan and monitor file activity.** It is also a good idea to scan and monitor file activity. You should be notified whenever there is a suspicious file in play—before it becomes a threat.

HOW TO PREVENT PHISHING ATTACKS

1. Always note the language in the email

Social engineering techniques are designed to take advantage of human nature. This includes the fact that people are more likely to make mistakes when they are in a hurry and are inclined to follow the orders of people in positions of authority. Phishing attacks commonly use these techniques to convince their targets to ignore their potential suspicions about an email and click on a link or open an attachment. Some common phishing techniques include:

- **Fake Order/Delivery:** A phishing email will impersonate a trusted brand (Amazon, FedEx, etc.) stating that you have made an order or have an incoming delivery. When you click to cancel the unauthorized order or delivery, the website (which belongs to a cybercriminal) will require authentication, enabling the attacker to steal login credentials.

- **Business Email Compromise (BEC):** BEC scams take advantage of hierarchy and authority within a company. An attacker will impersonate the CEO or other high-level executive and order the recipient of the email to take some action, such as sending money to a certain bank account (that belongs to the scammer).

- **Fake Invoice:** The phisher will pretend to be a legitimate vendor requesting payment of an outstanding invoice. The end goal of this scam is to have money transferred to the attacker's account or to deliver malware via a malicious document.

2. Never share your credentials

Credential theft is a common goal of cyberattacks. Many people reuse the same usernames and passwords across many different accounts, so stealing the credentials for a single account is likely to give an attacker access to a number of the user's online accounts.

As a result, phishing attacks are designed to steal login credentials in various ways, such as:

- **Phishing Sites:** Attackers will create lookalike sites that require user authentication and point to these sites in their phishing emails. Beware of links that don't go where you expect them to.

- **Credential-Stealing Malware:** Not all attacks against your credentials are direct. Some phishing emails carry malware, such as keyloggers or trojans, that are designed to eavesdrop when you type passwords into your computer.

- **Support Scams:** Cybercriminals may pose as customer support specialists from Microsoft, Apple, and similar companies and ask for your login credentials while they "help" you with your computer.

3. Always be suspicious of password reset emails

Password reset emails are designed to help when you can't recall the password for your account. By clicking on a link, you can reset the password to that account to something new. Not knowing your password is, of course, also the problem that cybercriminals face when trying to gain access to your online accounts.
By sending a fake password reset email that directs you to a lookalike phishing site, they can convince you to type in your account credentials and send those to them. If you receive an unsolicited password reset email, always visit the website directly (don't click on embedded links) and change your password to something different on that site (and any other sites with the same password).

4. Educate Employees About Current Phishing Threats

Phishing attacks use human nature to trick people into doing something that the attacker wants. Common techniques include creating a sense of urgency and offering the recipient of the email something that they desire, which increases the probability that the target will take action without properly validating the email.

Phishers will often take advantage of current events or impersonate trusted brands in their emails to make them more realistic. By offering information, goods, or opportunities related to a current event or creating a situation where the recipient believes that something has gone wrong (like a fake package delivery notification), these emails increase their probability of getting clicks.

Phishing techniques and the pretexts used by cybercriminals to make their attacks seem realistic change regularly. Employees should be trained on current phishing trends to increase the probability that they can identify and properly respond to phishing attacks.

5. Deploy an Automated Anti-Phishing Solution

Despite an organization's best efforts, employee cybersecurity education will not provide perfect protection against phishing attacks. These attacks are growing increasingly sophisticated and can even trick cybersecurity experts in some cases. While phishing education can help to reduce the number of successful phishing attacks against the organization, some emails are likely to sneak through.

Minimizing the risk of phishing attacks to the organization requires AI-based anti-phishing software capable of identifying and blocking phishing content across all of the organization's communication services (email, productivity applications, etc.) and platforms (employee workstations, mobile devices, etc.). This comprehensive coverage is necessary since phishing content can come over any medium, and employees may be more vulnerable to attacks when using mobile devices.

To learn more about protecting against phishing attacks and schedule a private demo to see for yourself how Check Point's email security solutions can help you to identify and block phishing attacks against your organization.

HOW TO PREVENT ZERO DAY ATTACKS

Threat Prevention across your organization

- Threat intelligence provides the information required to effectively detect zero day attacks. Protecting against them requires solutions that can translate this intelligence into actions that prevent the attack from succeeding.

Check Point has developed over sixty threat prevention engines that leverage ThreatCloud's threat intelligence for zero day prevention. Some key threat prevention capabilities include:

- **CPU Level Inspection:** Cyberattackers commonly use return oriented programming (ROP) to bypass defenses built into CPUs. CPU level inspection identifies attempts to overcome executable space protection and code signing, blocking the attack before malicious code can be downloaded and executed.

- **Threat Emulation and Extraction:** Analysis of suspicious content within a sandboxed environment can help to detect malware before it is delivered to a target system. This enables the malware to be blocked or malicious content to be excised from a document before delivery.

- **Malware DNA Analysis:** Malware authors commonly build on, borrow from, and tweak their existing code to develop new attack campaigns. This means that novel exploits often include behavior and code from previous campaigns, which can be used to detect the newest variation of the attack.

- **Anti-Bot and Anti-Exploit:** Modern cyberattacks often rely heavily upon compromised machines being used as part of a botnet. After identifying a compromised machine, an organization can isolate it and block bot-related traffic to stop the spread of the malware.

- **Campaign Hunting:** Malware is reliant upon the attacker's backend infrastructure for command and control. Using threat emulation and extraction, Check Point can identify new command and control domains used by malware and leverage this information to detect other instances of the attack campaign.

- **ID Guard:** Account takeover attacks have become increasingly common with the growing use of Software as a Service (SaaS) applications. Behavioral analysis and anomaly detection can identify and block attempted attacks even if the attacker has the correct credentials.

Security Consolidation works

Many organizations are reliant upon a wide array of standalone and disconnected security solutions. While these solutions may be effective at protecting against a particular threat, they decrease the effectiveness of an organization's security team by overwhelming them with data and forcing them to configure, monitor, and manage many different solutions. As a result, overworked security personnel overlook critical alerts.

A unified security platform is essential to preventing zero-day attacks. A single solution with visibility and control across an organization's entire IT ecosystem has the context and insight required to identify a distributed cyberattack. Additionally, the ability to perform coordinated, automated responses across an organization's entire infrastructure is essential to preventing fast-paced zero-day attack campaigns.

Threat Intelligence must be kept up to date

Modern cyberattacks are widespread and automated. A zero-day attack will target many different organizations, taking advantage of the narrow window between vulnerability discovery and patch release.

Protecting against this type of large-scale attack requires access to high-quality threat intelligence. As one organization experiences an attack, the data that it collects can be invaluable for other organizations attempting to detect and block the attack. However, the speed and volume of modern attack campaigns makes manual threat intelligence sharing too slow to be effective.

Check Point's ThreatCloud is the world's largest cyber threat intelligence database. ThreatCloud leverages artificial intelligence (AI) to distill the data provided to it into valuable insights regarding potential attacks and unknown vulnerabilities. Analysis of over 86 billion daily transactions from more than 100,000 Check Point customers provides the visibility required to identify zero-day attack campaigns.

DATA BREACHES CAN BE PREVENTED

1 EDUCATE AND TRAIN

First and foremost, educating and training your work force to take security precautions in order to prevent a breach from occurring.

2 SECURE PASSWORDS

Creating a secure password and frequently changing it to prevent access.

3 REDUCE DATA ACCESS

Reducing the ability to transfer data from one device to another decreases the risk of data getting into the wrong hands.

4 SCREEN THIRD PARTY VENDORS

Screening third party vendors to make sure that they have proper security protocols enabled to prevent hackers accessing via their network.

5 ENCRYPT PCS AND DEVICES

Regulating employee computers and devices in which they have access to company data can be significantly reduced by using only encrypted PCs and devices.

6 CREATE AND INTERNAL CLOUD

One way to prevent open access to sensitive data from being accessed is by creating and internal cloud where only those who need access to it, can access it.

7 UPDATE PASSWORDS

Implementing password updates and two-step authentication also mitigates this issue. Additional security measures such as limiting website access from work devices, frequent password changes, updating security software, and monitoring access to data can significantly reduce the risk of a data breach.

8 UPDATE SOFTWARE

Frequent security software updates can prevent room for gaps in your security. Updating in crucial.

Supply chain attacks are designed to exploit trust relationships between an organization and external parties. These relationships could include partnerships, vendor relationships, or the use of third-party software. Cyber threat actors will compromise one organization and then move up the supply chain, taking advantage of these trusted relationships to gain access to other organizations' environments.

Such attacks became more frequent and grew in impact in recent years, therefore it is essential developers make sure they are keeping their actions safe, double checking every software ingredient in use and especially such that are being downloaded from different repositories, especially ones which were not self-created.

Best Security From Code To Cloud, Check Point CloudGuard offers unified cloud native security across your applications, workloads, and network-giving you the confidence to automate security, prevent threats, and manage posture-at cloud speed and scale. CloudGuard Spectral is a developer-centric code security platform that seamlessly monitors, classifies, and protects codes, assets, and infrastructure; simply.

In order to scale this process, automation is a necessity.

PREVENT COSTLY MISTAKES

Mitigate secret leaks caused by bad credentials hygiene and human error that can have devastating results.

INTEGRATE WITH YOUR CLOUD INFRASTRUCTURE

CloudGuard Spectral integrates with all leading CI systems with built-in support for Jenkins, Azure and others.

DETECT AS EARLY AS A PRE-COMMIT

When working with Git, employ our pre-commit, Husky and custom hooks to automate early issue detection.

INSTALL YOUR BUILD SYSTEMS PLUGIN

Scan during your static builds with native plugins for JAMStack, Webpack, Gatsby, Netlify and more.

CloudGuard Spectral's automated tools integrate with developers' tools to detect code vulnerabilities and to identify secrets and misconfigurations in the code before deployment, preventing unauthorized use to nefarious ends.

With CloudGuard Spectral, organizations can prevent exposing API keys, tokens and credentials, as well remediating security misconfigurations.

09 MALWARE FAMILY DESCRIPTIONS

AcidRain

AcidRain is a destructive malware reported on 24 February 2022 targeting Viasat modems. Coinciding with the Russian ground invasion of Ukraine, AcidRain attack on satellite communication systems caused widespread disruption to communication systems providing services to Ukraine.

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.

Azov

Azov is a data wiper first reported in November 2022 and mostly being spread via SmokeLoader malware. The ransom note left on victim systems blames security researchers and political entities for the fighting in Ukraine.

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.

BlackMatter

BlackMatter is a ransomware operated in a RaaS model. The malware has been active since 2021 with victims including multiple US critical infrastructure entities. BlackMatter is possibly a rebranding of the DarkSide ransomware.

Bumblebee

BumbleBee is a new loader that is active since the beginning of 2022 and is used to deliver other payloads. Bumblebee payloads vary greatly based on the type of victim. Infected standalone computers will likely be hit with banking trojans or infostealers, whereas organizational networks can expect to be hit with more advanced post-exploitation tools such as CobaltStrike.

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.

CryWiper

CryWiper is a data-wiping malware disguised as ransomware used in 2022 to attack Russian public sector entities. Despite payment demands displayed in a ransom note, files encrypted by CryWiper cannot be restored.

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.

Dracarys

Dracarys is an Android infostealer discovered in 2022, used by the Bitter APT group to steal contacts, messages, call logs, screenshots, and more.

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.

Dustman / ZeroCleare

Dustman is a wiper, first detected in December 2019, targeting Middle Eastern entities. Dustman is a variant of the ZeroCleare wiper and has code similarities with Shamoon malware.

Emotet

Emotet is an advanced, self-propagating and modular Trojan. Emotet was once used to employ as a banking Trojan, and now is used as a distributer for other malware or malicious campaigns. It uses multiple methods for maintaining persistence and evasion techniques to avoid detection. In addition, Emotet can also be spread through phishing spam emails containing malicious attachments or links.

FormBook

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.

GuLoader

GuLoader is a downloader first reported in 2019. Since then it was used to distribute various malware including Lokibot, NanoCore, Formbook, Azorult, Remcos and more.

HermeticRansom

In early 2022, HermeticRansom malware was utilized to distract victims while HermeticWiper attacks were launched against organizations in Ukraine. These attacks rendered devices inoperable and as such were destructive in nature and not financially motivated.

HermeticWiper

HermeticWiper is a destructive malware first reported in January 2022 and used to target organizations in Ukraine. The malware is one of a series of wiping malware targeting Ukrainian organizations during the Russian-Ukrainian war and has similarities to WhisperGate

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 2021 and 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.

Hydra

Hydra in an Android banking Trojan discovered in 2019 distributed through infected applications on Google Play Store.

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.

Joker

Joker, an Android mobile malware known since 2017, is a stealer capable of accessing SMS messages, contact lists and device information. Joker generates income mostly through unauthorized subscriptions to paid premium services.

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.

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.

LockBit

LockBit is a ransomware, operating in a RaaS model, first reported in September 2019. LockBit targets large enterprises and government entities from various countries, abstaining from Russian or other Commonwealth of Independent States victims.

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.

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.

njRAT

njRAT, aka Bladabindi, is a RAT developed by the M38dHhM hacking group. First reported in 2012 it has been used primarily against targets in the Middle East.

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.

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 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.

Ponystealer

PonyStealer is an infostealer used for stealing passwords from a large number of applications including VPNs, FTP clients, email programs, instant messaging tools, and web browsers.

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.

Quantum

Quantum is a rasnomware operated in a RaaS model. The malware has been discovered in 2021 with victims including multiple healthcare entities. Investigators link Quantoum to ex-Conti actors.

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.

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.

RansomEXX

RansomEXX is a ransomware operated in a RaaS model with both Windows and Linux variants. The malware has been active since 2020 targeting mostly large corporations.

Raspberry Robin

Raspberry Robin is a multipurpose malware initially distributed through infected USB devices with worm capabilities.

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 Windows UAC security and execute malware with high-level privileges.

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.

Somnia

Somnia is a type of ransomware that was deployed by the FRwL (From Russia with Love) group against Ukrainian entities in November 2022. Victims of Somnia were not asked to pay for decryption. The goal of the attackers was to disrupt systems, rather than to achieve financial gain.

Stuxnet

Stuxnet is a malicious computer worm discovered in 2010 that targeted and disrupted the Iranian nuclear program. It caused physical damage to equipment by manipulating industrial control systems and was the first publicly known example of nation-state cyberattacks.

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.

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.

Whispergate

WhisperGate is a destructive malware first reported in January 2022 and used to target organizations in Ukraine. The malware is one of a series of wiping malware targeting Ukrainian organizations during the Russian-Ukrainian war. WhisperGate damages the system's MBR while displaying a false ransom message.

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.

ZeroCleare

ZeroCleare is a destructive wiper malware that was first identified in December 2020. It has been used in targeted attacks against organizations in the Middle East, and is notable for its ability to evade detection and wipe both hard drives and backup systems. ZeroCleare is believed to be the work of a state-sponsored hacking group.

10 CONCLUSION

As we navigate our way through a new year, it is important to re-evaluate the cybersecurity processes you have in place to ensure they stand up against the emerging threats outlined by our experts in this report.

There will undoubtedly be an increase in ideological motivated attacks in response to geopolitical conflicts as seen between Russian and Ukraine. Known threats such as ransomware will continue to evolve, and new vulnerabilities will be exploited, especially given the huge leaps made in generative AI, making it easier for malicious actors to craft attacks, leading to newer strains of cyberattack modes and breaches. Governments worldwide will tighten up regulations around cybercrime to protect their citizens, and organizations will have to consolidate and automate their IT and security infrastructure to plug the cyber skills gap, which is set to grow even wider this year.

While we are seeing a rise in cyberattacks overall, given the growth of 5th Generation cyberattacks in the last year, the maturing of cyber defense solutions today means that organisations and the wider society can adopt prevention-first solutions to block threats from ever reaching us. Businesses and governments are addressing today's sophisticated threats and increasing investment in their security strategies, which bodes well as the world faces even greater challenges, with the upcoming recession and expected evolution of new malicious software and nefarious practices. Only time will tell how this upward of attacks will continue in 2023.

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™

© 1994-2023 Check Point Software Technologies Ltd. All Rights Reserved.