cp<r>
CHECK POINT RESEARCH

CHECK POINT™

2023 MID-YEAR CYBER SECURITY REPORT

CONTENTS

01 INTRODUCTION

CHAPTER 1

MAYA HOROWITZ

VP Research, Check Point

Technology has continued its rapid and transformative march in the first half of 2023, revolutionizing various aspects of our lives. The proliferation of 5G networks has laid the groundwork for unprecedented connectivity and communication speeds, making it possible for smart cities and the Internet of Things (IoT) to flourish. Artificial Intelligence (AI) has become deeply engrained into daily existence, enhancing everything from virtual assistants and automated vehicles to personalized healthcare and predictive analytics. Quantum computing has taken significant strides, promising breakthroughs in solving complex problems that were once deemed insurmountable and augmented and virtual reality have become more immersive and mainstream, enhancing entertainment, education, and industrial applications.

However, amidst these marvels, concerns about data privacy, cybersecurity, and ethical implications have also escalated, underscoring the need for responsible innovation. Criminal activities have continued to escalate in the first half of the year, with an 8% surge in global weekly cyberattacks in the second quarter marking the highest volume in two years. Familiar threats such as ransomware and hacktivism have evolved further with criminals gangs modifying their methods and tools to infect and affect organizations worldwide. Even legacy technology such as USB storage devices, which have long been gathering dust in desk drawers, have gained popularity as a malware messenger.

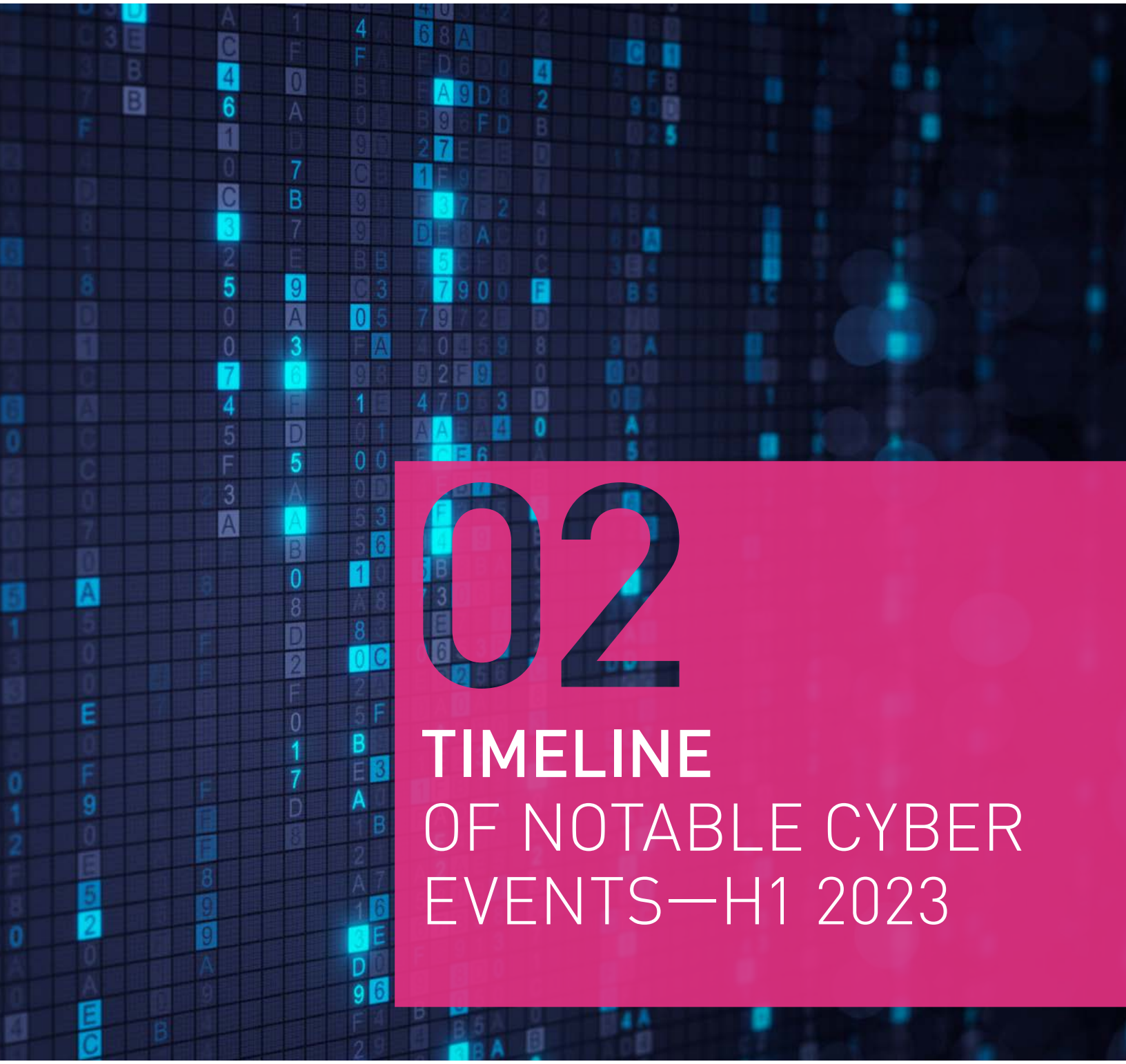
It is not just the known quantities keeping CISOs up at night. New tools such as Generative AI, which hold so much promise for good, have been manipulated by the bad guys to create code and phishing emails that can deceive even the trained eye.

Despite these challenges, there have been moments of glory for the cyber defenders. The takedown of the prominent Hive ransomware group, which prevented potential ransom payments of $130 million, was just one of the notable successes against cybercriminals in the first half of this year and governments across the globe are discussing and implementing more stringent regulations and penalties that will support the drive for stronger protections for organizations.

This report analyzes the threat landscape in the first six months of 2023, using examples of these real-world events, attack statistics and more, to help you understand the major threats of today and how to stop them from causing disruption and damage within your organization. We hope it helps raise awareness of those threats, and in turn helps to stop your organization becoming the next victim.

Maya Horowitz

VP Research at Check Point Software Technologies



02

TIMELINE OF NOTABLE CYBER EVENTS—H1 2023

JANUARY

Researchers have discovered a previously unknown Linux malware that exploits 30 vulnerabilities in multiple outdated WordPress plugins and themes to inject malicious JavaScripts into websites based on a WordPress CMS (Content Management System). The malware targets both 32-bit and 64-bit Linux systems, giving its operator remote command capabilities.

Check Point Harmony Endpoint provides protection against this threat (Backdoor_Linux_WordPressExploit_B)

Check Point Research reports that threat actors in hacking forums have started making use of AI tools like ChatGPT, in order to create malware and attack tools such as info-stealers and encryptors.

Britain's international mail service, Royal Mail, has had its operations disrupted by a cyberattack. The service has instructed its users not to post mail, as it is unable to dispatch packages to their destinations. The LockBit ransomware gang has been confirmed as the perpetrator of the attack, and is threatening to leak stolen data if its ransom demand is not met.

Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Win.Lockbit)

Check Point Research reported attempts by Russian cybercriminals to bypass OpenAI's restrictions, to use ChatGPT for malicious purposes. In underground hacking forums, hackers are discussing how to circumvent IP addresses, payment cards and phone numbers controls—all of which are needed to gain access to ChatGPT from Russia.

FEBRUARY

Check Point Research has flagged the Dingo crypto Token, with a market cap of $10,941,525 as a scam. The threat actors behind the token added a backdoor function in its smart contract, to manipulate the fee. Specifically, they used the "setTaxFeePercent" function within the token's smart contract code to manipulate the buying and selling fees to an alarming 99%. The function has already been used 47 times, and investors of Dingo Token can potentially risk losing all their funds.

Arnold Clark, one of Europe's largest car retailer, has been a victim of a Play ransomware attack. The threat actors claim to have 467GB of data including names, contact details, dates of birth, vehicle information, passports or driver's licenses, national insurance numbers, and bank account details.

Check Point Threat Emulation provides protection against this threat (Ransomware.Wins.PLAY.A)

.....

Check Point Research exposed two malicious code packages, Python-drgn and Bloxflip, distributed by threat actors, leveraging package repositories as a reliable and scalable malware distribution channel.

.....

Check Point's researchers found that threat actors are working their way around ChatGPT's restrictions to create malicious content and to improve the code of a basic Infostealer malware from 2019.

.....

Check Point Research identified a campaign against entities in Armenia, using a new version of OxtaRAT—an AutoIt-based backdoor for remote access and desktop surveillance. The threat actors have been targeting human rights organizations, dissidents, and independent media in Azerbaijan for several years, amid rising tensions between Azerbaijan and Armenia over the Lachin corridor.

Check Point Threat Emulation and Anti-Bot provides protection against this threat (Trojan.Win.OxtaRAT.A; Trojan.WIN32.OxtaRAT)

.....

Community Health Systems, one of the leading healthcare providers in the US, has confirmed that it was affected by the recent attacks targeting a zero-day vulnerability in Fortra's GoAnywhere MFT file transfer platform, revealing that the breach exposed personal information of almost 1 million patients.

Check Point IPS provides protection against this threat (GoAnywhere MFT Insecure Deserialization)

.....

Microsoft has released security updates to a total of 77 flaws in the latest Patch Tuesday. Nine vulnerabilities have been classified as 'Critical' as they allow remote code execution on vulnerable devices, and three are actively exploited in attacks (CVE-2023-21823, CVE-2023-21715 and CVE-2023-23376).

Check Point IPS provides protection against these threats (Microsoft Windows Graphics Component Elevation of Privilege (CVE-2023-21823); Microsoft Office Security Feature Bypass (CVE-2023-21715); Microsoft Windows Common Log File System Driver Elevation of Privilege (CVE-2023-23376) etc.)

.....

One year into the Russia-Ukraine war, Check Point Research marks September 2022 as a turning point, as weekly cyber-attacks against Ukraine decreased by 44%, while cyber-attacks against some NATO countries increased by nearly 57%. Further analysis of this year lists wipers and hacktivism as key trends.

MARCH

Pierce Transit, a public transit operator that serves over 18K people daily in Washington State, has been a victim of a ransomware attack conducted by LockBit gang. The ransomware group claimed it stole correspondence, non-disclosure agreements, customer data, contracts and more.

Check Point Threat Emulation and Harmony Endpoint provide protection against this threat (Ransomware.Win.Lockbit)

Israel's National Cyber Directorate has asserted that Iranian APT group MuddyWater, known to be affiliated with Iran's Ministry of Intelligence and Security, is behind the cyberattack on the Technion, one of Israel's leading universities. The attack was masked as a regular ransomware attack and had significantly disrupted the university's activities.

Check Point Harmony Endpoint and Threat Emulation provide protection against this threat.

Check Point researchers have *uncovered* a cyber-espionage campaign by Chinese APT group SharpPanda. The campaign has targeted government entities in South-East Asia, and has utilized the Soul framework to establish access to vicitms' network and exfiltrate information.

Check Point Threat Emulation and Anti-bot provide protection against this threat (Trojan.WIN32.SharpPanda)

Check Point Research has revealed the FakeCalls Android Trojan, which can mimic over 20 financial apps and engage in voice phishing by simulating conversations with bank employees. This malware, designed for the South Korean market also extracts private data from victims' devices.

Check Point Harmony Mobile and Threat Emulation provide protection against this threat.

Check Point Research has analyzed ChatGPT4 and identified five scenarios that allow threat actors to by bypass the restrictions and to utilize ChatGPT4 to create phishing emails and malware.

New victims of Clop ransomware gang that leveraged for the attack purpose a zero-day security flaw (CVE-2023-0669) in the Fortra GoAnywhere Managed File Transfer system were disclosed. Among those are the American luxury brand retailer Saks Fifth Avenue, and City of Toronto.

Check Point IPS, Threat Emulation and Harmony Endpoint provide protection against this threat (GoAnywhere MFT Insecure Deserialization (CVE-2023-0669); Ransomware.Win.Clop; Ransomware_Linux_Clop_A; Ransomware_Linux_Clop_B)

Researchers have uncovered a new variant of the FakeGPT Chrome extension, dubbed "ChatGPT-For-Google", based on an open-source project affecting thousands victims daily. The variant steals Facebook session cookies and compromises accounts under a cover of a ChatGPT integration for Browser, using malicious sponsored Google search results.

APRIL

Both Windows and macOS versions of 3CXDesktopApp, a VoIP application of 3CX Communications Company, were compromised and used to distribute Trojanized versions in a large-scale supply chain attack. In this widespread campaign, dubbed SmoothOperator, threat actors have misused 3CX's application with a malicious file that is loaded using 3CXDesktopApp and beacons to the attacker's infrastructure. More than 600,000 companies worldwide which use 3CX may be affected by this attack. The attack is linked to the North Korean Lazarus group, and is tracked as CVE-2023-29059.

Check Point Threat Emulation and Harmony Endpoint provide protection against this threat (Trojan-Downloader.Win.SmoothOperator; Trojan.Wins.SmoothOperator)

Australia's largest gambling and entertainment firm, Crown Resorts, has disclosed that it is being extorted by CL0P ransomware group. This extortion attempt is also a result of CL0P's group exploitation of Fortra GoAnywhere vulnerability.

Check Point Threat Emulation and Harmony Endpoint provide protection against this threat (Ransomware.Wins.Clop; Ransomware.Win.Clop; Ransomware_Linux_Clop)

Check Point Research has released an extensive publication and analysis of the Rhadamanthys infostealer that was launched on the dark web in September 2022. CPR showcases a step-by-step disassembly breakdown of how the malware compiles its own database of stolen Google Chrome information in order to send back to the C2 server.

Check Point Threat Emulation provides protection against this threat (InfoStealer.Wins.Rhadamanthys)

.....

Various Muslim-affiliated hacktivist groups have launched "OpIsrael", targeting Israeli websites with DDoS. Among the targets hit by Anonymous Sudan, were Israeli government subdomains, as well as websites of universities, hospitals, media journals, airports and several Israeli companies.

.....

Check Point Research has discovered a new strain of ransomware dubbed Rorschach, which was deployed via DLL sideloading of a legitimate, signed security product. This ransomware is highly customizable with technically unique features previously unseen in ransomware, and is one of the fastest ransomware observed, by the speed of encryption.

Check Point Harmony Endpoint provides protection against this threat.

.....

Check Point Research has discovered three vulnerabilities (CVE-2023-28302, CVE-2023-21769 and CVE-2023-21554) in the "Microsoft Message Queuing" service, commonly known as MSMQ. The most severe of these, dubbed QueueJumper by CPR (CVE-2023-21554), is a critical vulnerability that could allow unauthenticated attackers to remotely execute arbitrary code in the context of the Windows service process mqsvc.exe.

Check Point IPS provides protection against this threat (Microsoft Message Queuing Remote Code Execution (CVE-2023-21554))

.....

Check Point Research flags a sharp increase in cyberattacks targeting IoT Devices, with 41% increase in the average number of weekly attacks per organization during the first two months of 2023, compared to 2022. On average, every week, 54% of organizations suffer from attempted cyber-attacks targeting IoT devices, mostly in Europe followed by APAC and Latin America.

Check Point Quantum IoT Protect provides protection against this threat

.....

Check Point Research warns about an increase in discussions and in trade of stolen ChatGPT accounts, with a focus on Premium accounts. Cyber criminals leak credentials to ChatGPT accounts, trade premium ChatGPT account and use Bruteforcing tools for ChatGPT, which allow cyber criminals to get around OpenAI's geofencing restrictions and get access to the previous queries of existing ChatGPT accounts.

.....

Capita, a professional outsourcing company based in London, has provided an update on a recent cyber incident they experienced, acknowledging that data was exfiltrated from their systems one week prior to the outage. The company revealed that approximately 4% of its server infrastructure was accessed by hackers who stole files. The BlackBasta ransomware group, known to operate from Russian-speaking regions, has been identified as the perpetrator of the attack.

Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Win.BlackBasta)

The Check Point research team has uncovered new techniques used by the Raspberry Robin malware. These methods include several anti-evasion techniques, obfuscation, and anti-VM measures. The malware also exploits two vulnerabilities in Win32k (CVE-2020-1054 and CVE-2021-1732) in order to elevate its privileges.

Check Point Threat Emulation and IPS provide protection against this threat (Trojan.Wins.RaspberryRobin; Microsoft Win32k Elevation of Privilege (CVE-2021-1732), Microsoft Win32k Elevation of Privilege (CVE-2020-1054))

MAY

Microsoft warns of a recent wave in exploitation of CVE-2023-27350, a critical-severity remote code execution vulnerability in PaperCut Application servers. According to reports, the vulnerability is being utilized by threat actors to deliver the ClOP and LockBit ransomware variants. PaperCut has released a patch addressing the vulnerability.

Check Point Harmony Endpoint and Threat Emulation provide protection against these threats (Ransomware.Wins.Clop; Ransomware.Win.Clop; Ransomware_Linux_Clop, Ransomware.Win.LockBit; Ransomware.Wins.Lockbit)

Check Point Research reveals new findings related to Educated Manticore, an activity cluster with strong overlap with Phosphorus, an Iranian-aligned threat actor operating in the Middle East and North America. Educated Manticore adopted recent trends and started using ISO images and possibly other archive files to initiate infection chains

Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (APT.Wins.APT35.ta)

After launching a devastating attack on the city of Oakland on April, the Play ransomware gang has taken responsibility for another attacks in the United States on Massachusetts city of Lowell. The gang claims to have stolen an undisclosed amount of data that includes passports, government IDs, financial documents and more.

Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Win.Play)

.....

Check Point Research has noticed a surge in cyberattacks leveraging websites associated with the ChatGPT brand. These attacks involve the distribution of malware and phishing attempts through websites that appear to be related to ChatGPT, to lure users into downloading malicious files or disclose sensitive information.

.....

The Swedish-Swiss multinational automation company ABB has been a victim of a ransomware attack conducted by the Russian Black Basta ransomware group. The threat actors have attacked the company's Windows Active Directory, affecting hundreds of devices. To prevent the spread of ransomware to its customers, ABB terminated VPN connections with other networks.

Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Win.BlackBasta; Ransomware.Wins.Blackbasta)

.....

Check Point Research had discovered a custom firmware implant tailored for TP-Link routers that has been linked to a Chinese state-sponsored APT group tracked as Camaro Dragon, which shares similarities with Mustang Panda. The implant was used in targeted attacks aimed at European foreign affairs entities, and it features several malicious components. This includes a custom backdoor named "Horse Shell", which enables the attackers to maintain persistent access, build anonymous infrastructure and enable lateral movement into compromised networks.

Check Point Quantum IoT Protect and Threat Emulation provide protection against this threat (APT.Wins.HorseShell)

.....

The FBI, CISA, and ACSC warn that the BianLian ransomware group has shifted its tactics to extortion-only attacks. Instead of encrypting files and demanding a ransom, the group now focuses on stealing sensitive data and threatening to release it unless a payment is made.

Check Point Threat Emulation provides protection against this threat (Ransomware.Win.GenRansom.glsf.A)

.....

Check Point Research elaborates on the latest Chinese state sponsored attacks and their use of network devices. This follows a joint Cybersecurity Advisory that United States and international cybersecurity authorities issued on Chinese state-sponsored cyber actor, also known as Volt Typhoon. This actor have compromised "critical" cyber infrastructure in a variety of industries, including governmental and communications organizations.

JUNE

One of the United States' largest dental insurers, MCNA, has notified regulators that information of 8.9 million of the company's customers has been leaked as a result of a ransomware attack. Notorious ransomware gang LockBit has claimed the attack, and has allegedly posted the data in its shame blog.

Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Win.LockBit; Ransomware.Wins.Lockbit)

A zero-day SQL injection vulnerability (CVE-2023-34362) affecting MOVEit Transfer, a managed file transfer platform, has been widely exploited in the wild for weeks. The vulnerability could lead to information disclosure, and experts worry that a large number of organizations have had their data stolen. Experts are concerned about a potential large-scale extortion campaign, similar to the Fortra GoAnywhere zero-day campaign by ClOP ransomware group earlier this year.

Check Point IPS blade provides protection against this threat (MOVEit Transfer SQL Injection (CVE-2023-34362))

Check Point Research has published an analysis of a backdoor tool used by the Chinese APT group Camaro Dragon. The backdoor tool, dubbed TinyNote, is written in Go and includes a feature bypassing Indonesian antivirus software SmadAV, which is popular in Southeast Asian countries. The APT group's victims likely include embassies in Southeast Asian countries

Check Point Threat Emulation provides protection against this threat (APT.Wins.MustangPanda.ta.)*

The Estonia-based cryptocurrency wallet service Atomic Wallet has confirmed a cyber-attack that compromised customers' wallets, resulting in the loss of more than 35M dollars. Researchers suggest with high confidence that the North Korean state-backed Lazarus Group is responsible for the attack.

Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (APT.Win.Lazarus; APT.Wins.Lazarus)

.....

Check Point Research has identified an ongoing operation against targets in North Africa involving a previously undisclosed multi-stage backdoor called Stealth Soldier. The backdoor primarily operates surveillance functions such as file exfiltration, screen and microphone recording, keystroke logging and stealing browser information.

Check Point Threat Emulation provides protection against this threat (Trojan.Wins.StealthSoldier)

.....

The Louisiana Office of Motor Vehicles (OMV) and the Oregon DMV Services have released statements warning US citizens of a data breach exposing millions of driver's licenses. This comes after the Clop ransomware gang had hacked the agencies' MOVEit Transfer security file transfer systems and stole the stored data.

Check Point IPS blade, Harmony Endpoint and Threat Emulation provide protection against this threat ([Progress MOVEit Transfer Multiple Vulnerabilities); Webshell.Win.Moveit, Ransomware.Win.Clop, Ransomware_Linux_Clop; Exploit.Wins.MOVEit)

.....

Check Point provides details about the MOVEit vulnerability, its exploitation and the attack, as well as the major impact it had on variety of organizations across the world.

.....

Two of the largest airlines in the world, American Airlines and Southwest Airlines, have stated they are handling data breaches due to an incident involving a hack of Pilot Credentials, a third-party vendor. The breach, which occurred at the end of April, has included the illicit obtainment of documents related to almost 9,000 applicants in the pilot and cadet hiring process to both airlines. Despite that, there has not been an impact on the airlines' own networks or systems.

.....

Hawaii's largest university, the University of Hawai'i, has disclosed that one of its campuses had suffered a ransomware attack. The impact of the attack had not been made public by the university, but ransomware gang NoEscape, which has assumed responsibility for the attack, claimed to have exfiltrated 65 GB of sensitive data from the university's network.

Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Win.NoEscape)

.....

03

THE FIRST HALF OF 2023 AT A GLANCE

CHAPTER 3

The first half of 2023 saw significant developments in ransomware, methods of infection, hacktivism, mobile threats, and the use of AI by threat actors. This overview explores these evolving security challenges and sheds light on how they might influence the future cybersecurity landscape. In particular, we will focus on the rise of mega ransomware attacks, and the growing role of AI in enabling and accelerating cyberattacks and malicious activities. As is always the case with cybersecurity, these threats are constantly changing, which in turn demands a proactive approach to defense.

RANSOMWARE

Ransomware currently poses the most significant threat to businesses, in terms of the sophistication of attacks and the damage that they cause. The damages comprise of both direct ransom payments, and indirect business costs such as recovery and remediation expenses, impact on stock market performance, as well as legal implications and brand damage.

Ransomware is constantly evolving and becoming more sophisticated with added functionality that makes attacks more targeted and successful. This is predominantly driven by escalating competition among Ransomware-as-a-Service (RaaS) groups, all seeking to recruit more partners and maximize their 'sales'. In many cases these groups are criminal mirror-images of conventional businesses, with research and development teams, quality assurance departments, specialist negotiators, even HR staff. They may have dozens or even hundreds of employees, with revenues in the hundreds of millions of dollars. The rivalry between groups (after all, there is no honor amongst thieves) has led to quicker encryption of victims' data, innovative evasion techniques, and lower commission rates for partners. For example, leading entities like LockBit, Alphv, BlackBasta, and AvosLocker all incorporated an evasion technique that utilizes the restart-in-safe-mode function in an attempt to neutralize security services and make it more difficult to recover infected computers. Another noteworthy development is the surge in ransomware variants for different operating systems; the most dominant being for Linux and offered by RaaS groups including LockBit, Royal, CL0P, BianLian, and ViceSociety.

Ransomware groups have also begun to execute mega-scale attacks, exploiting vulnerabilities in widely-used corporate software to simultaneously infect multiple victims.

Both the CL0P and LockBit ransomware groups also achieved widespread infections in the first half of the year, either through supply-chain attacks and extortion or by exploiting zero-day vulnerabilities.

LockBit claimed to breach 60 companies by exploiting vulnerabilities in their cloud service provider, Cloud51. At the beginning of the year, CL0P took responsibility for attacks exploiting a zero-day vulnerability in the GoAnywhere MFT secure file transfer tool, resulting in breaches of more than 130 organizations. In early June, CL0P also announced that they had exploited a vulnerability in the MOVEit file-transfer program, leading to hundreds of new victims, mostly major corporations and governmental organizations.

One of these is Zellis, an HR services provider that suffered a subsequent supply-chain attack affecting its clientele. Among those impacted were the government of Nova Scotia, British Airways, the Boots drugstore chain, and the BBC news organization.

All the abovementioned are combined with a continued shift from data encryption to data theft, and pressure that is applied not only on the target, but also on its partners and customers to secure ransom payment. This attack method is also known as triple extortion, which we witnessed during a campaign carried out against the University of Manchester in June 2023. Clearly, ransomware continues to be big business for criminals, and they are constantly probing for new vulnerabilities and new ways to use them for extortion.

We found evidence of thousands of ransomware victims in the first half of 2023, totaling over 2,000 victims, with ransomware attacks by over 40 ransomware groups. We expect to see the same, if not more in the second half of 2023.

LOTEM FINKELSTEEN

Director of Threat Intelligence & Research, Check Point Software Technologies

> **Mega-scale ransomware attacks have continued this year, impacting large numbers of organizations as attackers exploit new software vulnerabilities. We have also seen how ransomware-as-a-Service groups (RaaS) are competing to attract affiliates and maximize their revenues by offering faster encryption and new evasion techniques. Some are skipping the encryption phase entirely and relying on threats of data exposure to extort money, or even destroying data completely. It is assumed that this new ransomware business model is being utilised to cut out the overhead costs of trying to build stronger ransomware. Organizations need to ensure their defences are updated to protect themselves against these increasingly complex, damaging threats.**

USB DRIVES

In the same way that vinyl LPs and even music cassettes have become popular again, older attack methodologies sometimes re-emerge, exemplified by the recent resurgence of USB-based cyberattacks conducted by both cybercriminals and nation-state actors. One of the oldest known attack vectors, the humble USB drive, is currently a significant conduit for contemporary malicious cyber operations. The attackers again see the USB drives as the best way to infect air gapped, segmented or just highly protected networks. In 2022, the FBI issued a warning about a campaign aimed at US defense firms with the attackers mailing USB drives loaded with malicious payloads.

The Raspberry Robin worm stands out among such attacks. It is recognized as one of the top common malware variants on our multipurpose malware list and is distributed via infected USB drives through the exploitation of "autorun.inf" files or clickable LNK files. This worm has been linked to the FIN11 threat actor, with successful infections serving as a launchpad for subsequent attacks.

Nation state threat actors are currently leveraging USB-borne infections, even those caused by legacy malware like ANDROMEDA (which dates back to 2013) to hijack their infrastructure. Regardless of whether Turla or Tomiris is the culprit, USB infections remain a potent method for gaining initial access to systems.

The China-related espionage threat actor Camaro Dragon reportedly utilized USB drives as a vector to infect organizations all over the world. USB drives were recently also used by Shuckworm, believed to be part of the Russian cyber espionage group Gamaredon, in a cyber espionage campaign targeting the Ukrainian military and associated individuals.

ELI SMADJA

Security Research Group Manager, Check Point Software Technologies

"Getting access to well protected organizations is not always easy. Awareness of phishing and improvement in cyber security solutions make it difficult to spread widely, which is why we are seeing USB drives once again being used as a vector for malware to infiltrate organizations worldwide. By staying informed and vigilant, and adopting proactive endpoint security measures, businesses can effectively defend against USB-based attacks and safeguard their valuable assets from cyber threats.

HACKTIVISM

State-affiliated hacktivism, first seen in 2022, was another dominant threat in the first half of 2023. Hacktivist groups select their targets based on nationalistic and political motivations. The infamous Russian-affiliated Killnet group started the year off by attacking Western healthcare organizations and later announced their intention to shift to acting as a "private military hacking company."

Another hacktivist group, "Anonymous Sudan", first appeared in January 2023 and has been particularly active, operating under the veil of counter-offensive cyberattacks to allegedly retaliate for anti-Muslim activities. While promoting a pro-Islamic narrative, this group has collaborated with the Pro-Russian Killnet, sparking speculation about a potential Russian affiliation. The group targets Western organizations, with Scandinavian Airlines a notable victim of a disruptive DDoS attack. The group also tried to implement an extortion strategy, most likely as part of its information operations, insisting on payment to halt their attacks. Their targets expanded to include US organizations, particularly in the healthcare sector. Recently Microsoft was victimized, resulting in substantial disruption of key Microsoft Outlook services, including email and calendar availability, as well as some disruption to the availability of the Microsoft Azure Portal.

All this shows us that state-affiliated hacktivism, even though its focus is primarily on denial-of-service campaigns, can cause real disruption. The groups are using much larger and powerful botnets, and from a magnitude perspective, we also see an escalation in the scale of DDoS attacks, with the highest recorded at more than 71M requests per second, which indicates an intensifying trajectory of hacktivist operations.

SERGEY SHYKEVICH

Threat Intelligence Group Manager, Check Point Software Technologies

"Hacktivism targeting both private and government organizations became even much more significant threat in 2023. Hacktivist groups aim high and can take down even the biggest national or international websites using powerful DDoS capabilities. Current hacktivists are no longer distributed individuals, but more state affiliated groups that serve political narratives. However, the impact of those disruptive DDoS attacks can be minimized if organizations put in place the correct mitigation processes.

MOBILE THREATS

Check Point Research has been monitoring various mobile cyberattack campaigns since the start of the year. For example, the FluHorse malware, designed to target East Asian victims, effectively camouflages itself as popular Android applications and aims to extract Two-Factor Authentication (2FA) codes along with other sensitive user data. In another campaign disclosed in March, attackers circulated malware known as FakeCalls, which is designed to simulate over twenty distinctive financial applications and generate fraudulent voice calls.

In the areas of sophisticated espionage operations, researchers reported a campaign called Triangulation that utilizes zero-click exploitation to take control of iOS devices, continuing a trend of large-scale exploitation of previously unknown vulnerabilities in Apple products.

ALEXANDER CHAILYTKO

Cyber Security, Research & Innovation Manager, Check Point Software Technologies

> **Mobile devices are still a tempting target for hackers, whether for stealing data or for covert surveillance by remote control. Attackers target popular, widely used apps which users would consider safe, or exploit new vulnerabilities in Android and iOS to spread malware of all types. It's an important reminder that the majority of mobile devices are still under-protected, despite the amount of sensitive personal and corporate data they hold.**

ARTIFICIAL INTELLIGENCE

A review of 2023 would be incomplete without acknowledging the significant advancements made in Artificial Intelligence. ChatGPT has brought a groundbreaking revolution in AI accessibility. The implications of AI's capabilities have led to bold predictions ranging from significant transformations of the job market to potential existential threats to humanity. In the cyber arena, this paradigm shift has already been felt in significant ways. Last year, Check Point researchers demonstrated that criminals can harness AI to create sophisticated social engineering content. They can also craft ever more deceptive phishing emails, develop malicious VBA macros for Office documents, produce code for reverse shell operations, and more.

Shortly afterward, a Check Point Research publication showed examples in the wild of cybercriminals already using ChatGPT to produce infostealers and encryption tools. OpenAI employed various mechanisms to restrict malicious use of ChatGPT, but threat actors were quick to invent new ways to bypass those restrictions, effectively launching a massive cyber arms race. Russian threat actors have explored ways to bypass OpenAI's geo-fencing restrictions.

Another paper showed how defense mechanisms integrated into the latest version, ChatGPT4, could be bypassed and cybercriminals are actively seeking new ways to use ChatGPT and its widespread awareness for malicious purposes. Legislators' efforts to prevent the use of AI for social engineering are at a preliminary stage and a solution is yet to be found.

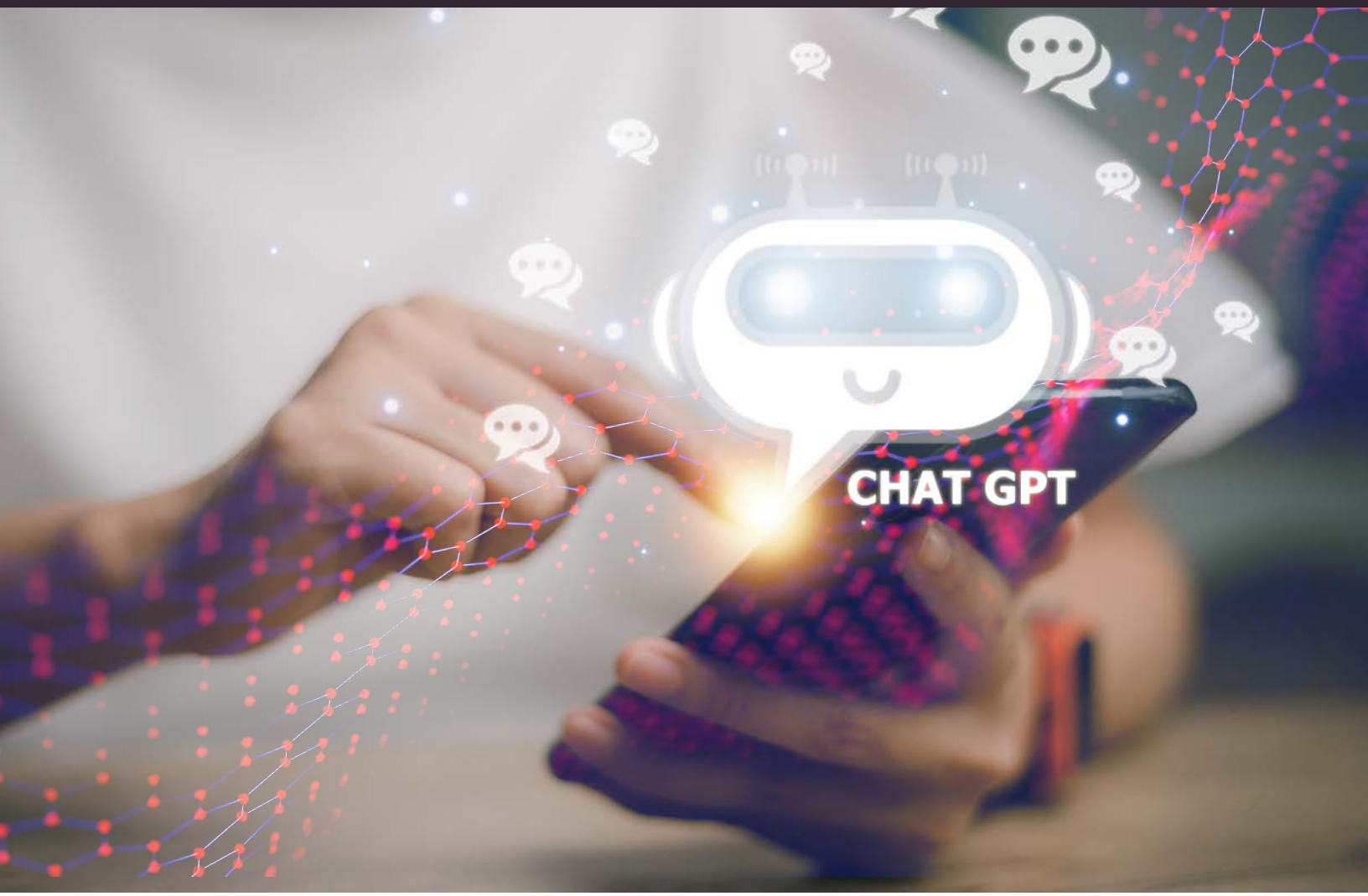
The launch of ChatGPT in late 2022 was a catalyst for other generative AI tools such as Google Bard, which became publicly available in March 2023. In the same way that we were able to bypass restrictions in other generative AI platforms, we were able to use Bard AI to generate phishing emails, malware keylogger to monitor keystrokes and basic ransomware code.

Since its publication in November 2022, ChatGPT has succeeded in a wide range of activities including passing MBA exams at Wharton, passing the US medical licensing exam, and has exhibited its wider production capabilities across numerous other areas. Given its potential for both good and evil, there are calls for enhanced regulation to stop misuse and the spread of misinformation. Some countries, including Italy, have opted to ban the use of generative AI altogether, while others such as the European Union are drafting a first-of-its-kind AI Act to control or restrict AI systems.

ODED VANUNU

Head of Products Vulnerabilities Research, Check Point Software Technologies

> This year, we've seen how AI tools such as ChatGPT can be used by bad actors, even those without technical knowledge, to create new malware and accelerate other malicious activities such as social engineering and fake content. But those same tools can also be used to craft code that is useful to society, for example in helping combat cybercrime. AI is an immensely powerful technology, and we are working to ensure that it's used as a force for good with our own ThreatCloudAI engine, using big data threat intelligence to stop even the most advanced attacks.

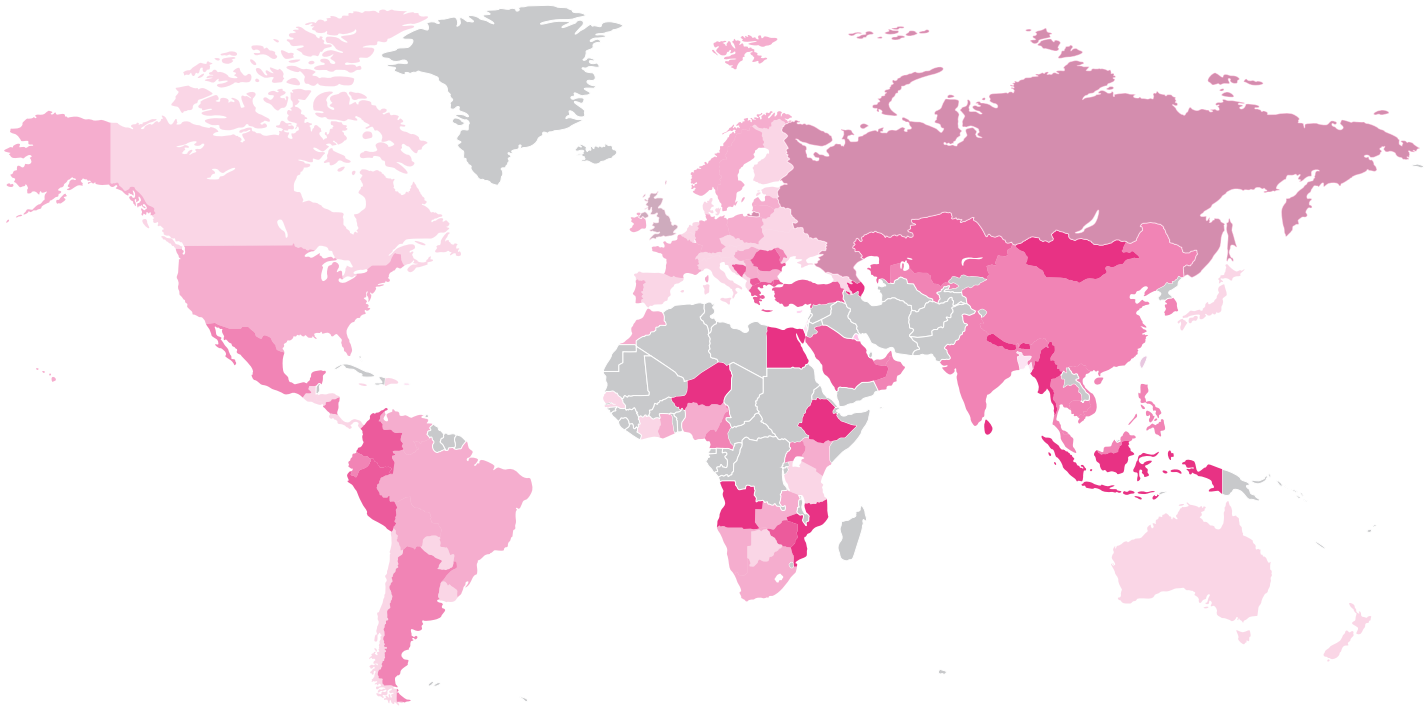


CHAPTER 4

04 GLOBAL ANALYSIS

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 1. Global Threat Index Map

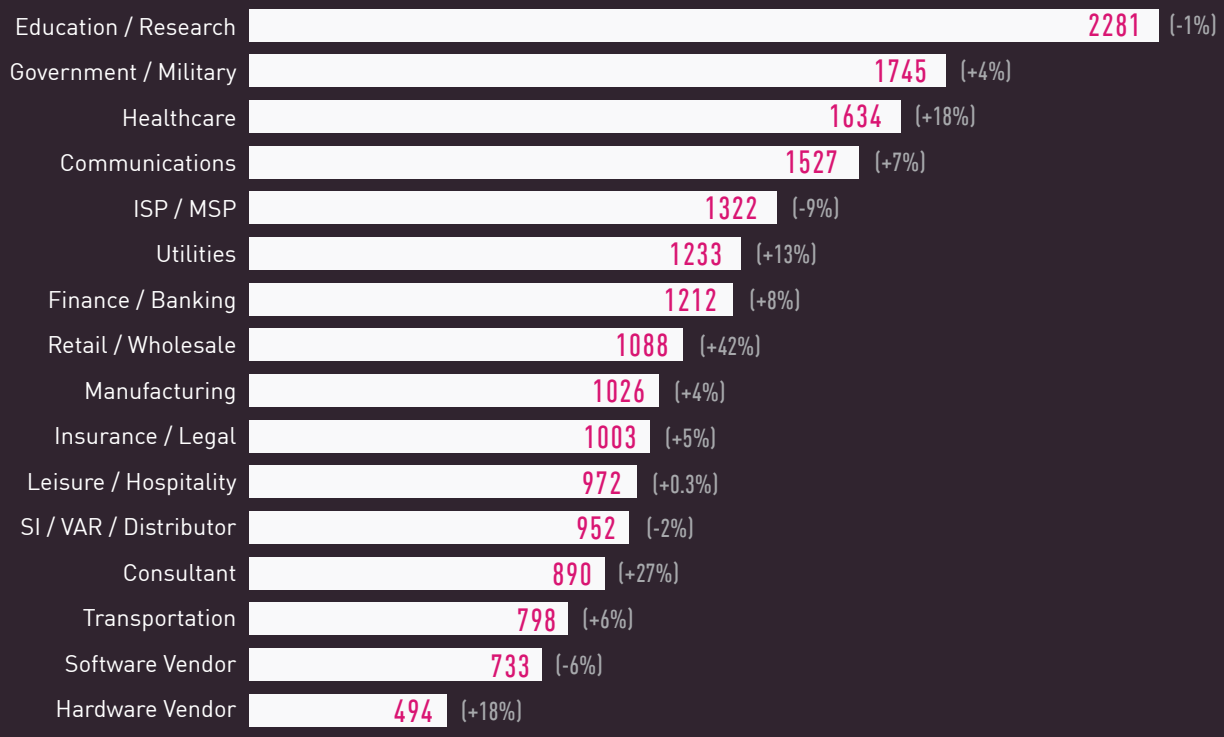


Figure 2. Global Average of weekly attacks per organization by Industry in H1 2023 [change in percentage from H1 2022].

Education, government and healthcare remain the sectors that most frequently experience cyberattacks. This has been confirmed from different sources and across multiple geographical regions, but comparing the data from ransomware attacks reveals that the manufacturing and retail sectors are the most attacked and extorted sectors by ransomware groups. One explanation for this discrepancy could be that manufacturing and retail are private sectors with the ability to pay the ransom. Attacks on the education and government sectors are aimed at stealing personally identifiable information (PII) and restricted data, both commercial and private. The underground market for "fullz", a person's full-information package, is fed by a seemingly never-ending series of breaches of educational and healthcare institutions. The healthcare sector is ranked high on both indexes.

The highest increase of the attacks is against the retail sector, which correlates with the retail sector being one of the top extorted sectors by ransomware, as well as the modus operandi of stealing payment card data that this sector processes and stores.

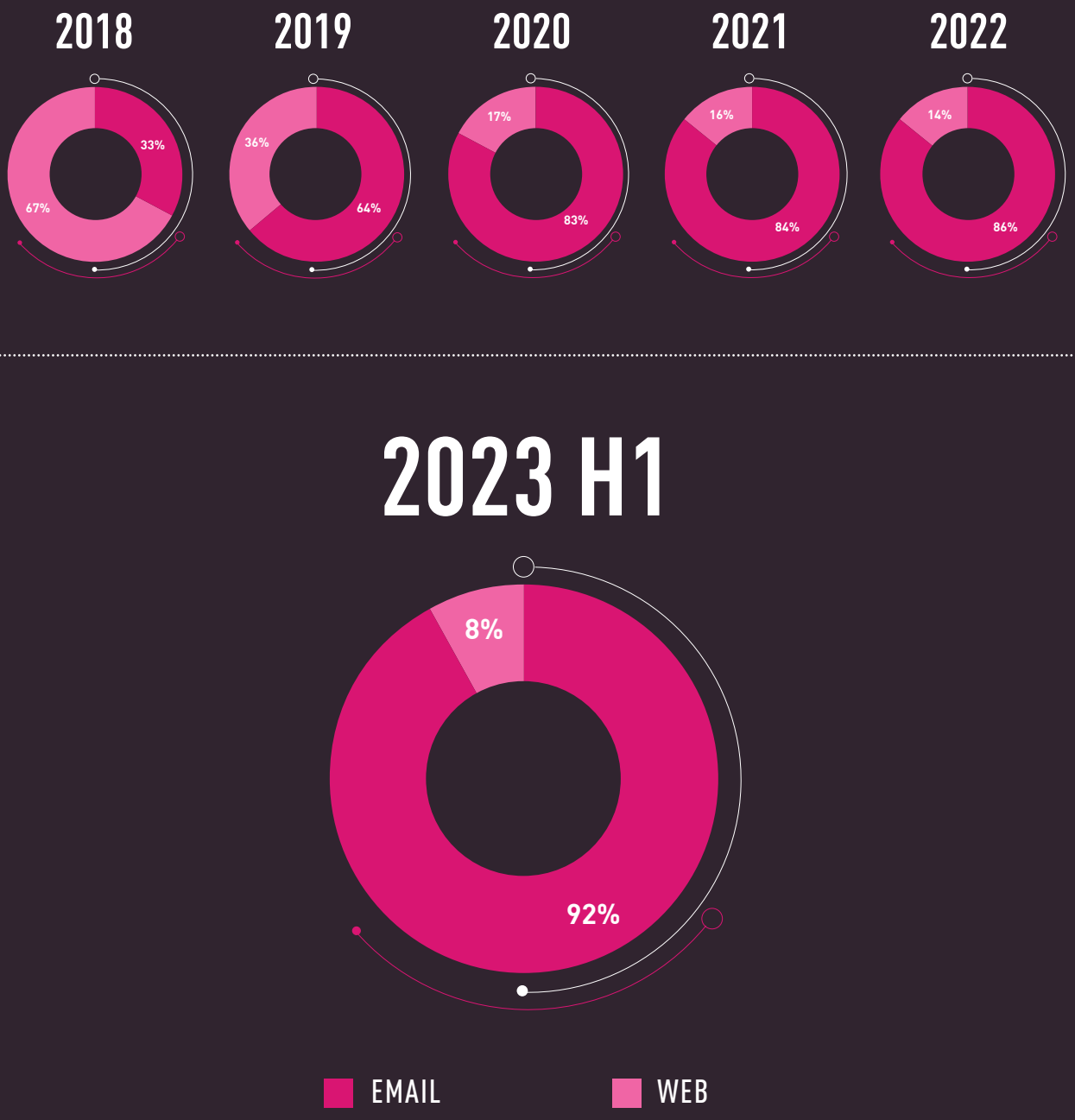


Figure 3. Delivery Protocols—Email vs. Web Attack Vectors in 2018-2023.

TOP MALICIOUS FILE TYPES—WEB VS. EMAIL

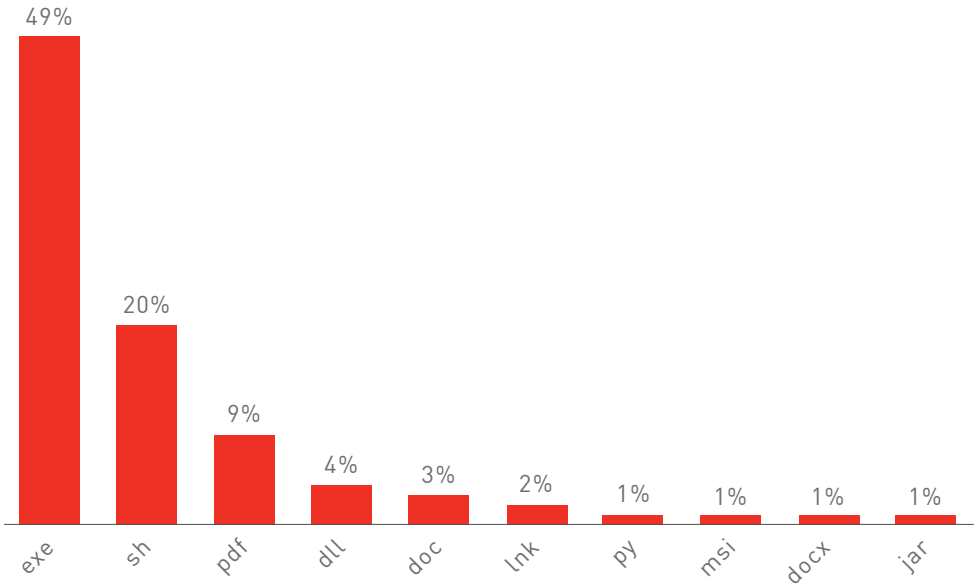


Figure 4. Web delivered malicious files by type in H1 2023.

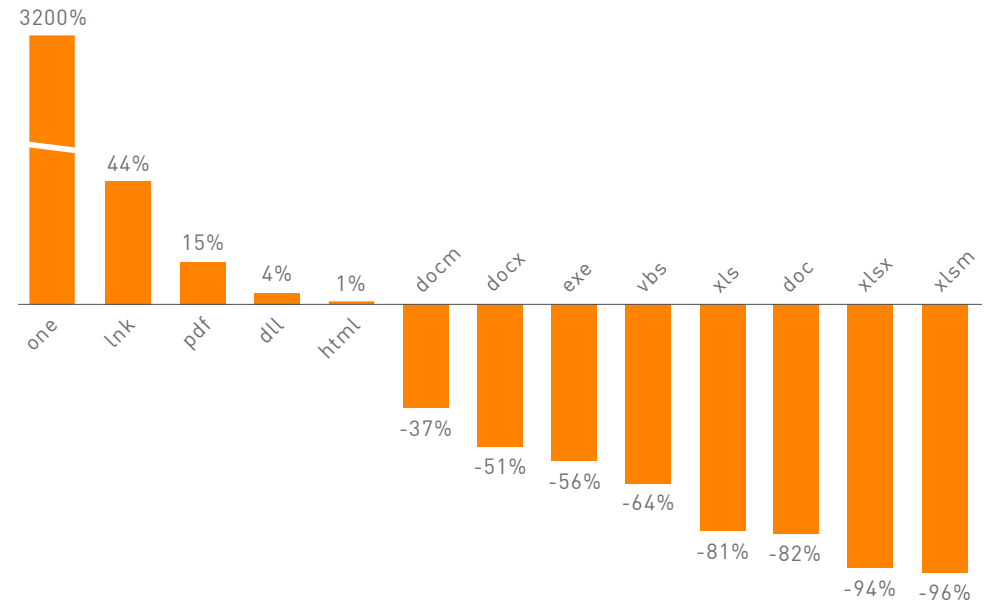


Figure 5. Email delivered malicious files, change in prevalence in H1 2023 compared to 2022.

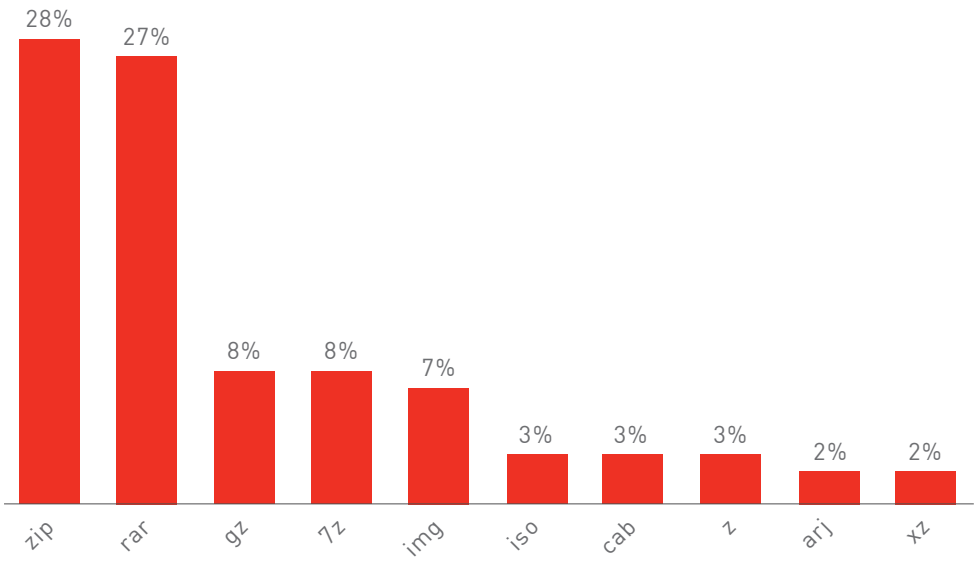


Figure 6. Email delivered malicious archive file types in H1 2023.

Email remains the primary vehicle for launching attacks, delivering 92% of all malicious payloads. There was a dramatic drop in the use of malicious Office files since Microsoft essentially started eliminating in-document macros, a rich source of potential exploitation, in 2022. Our data reflects an 81-96% reduction in the prevalence of malicious Excel files and a substantial decrease in other Office formats. This shift is largely attributable to major malicious spam (malspam) entities like Qbot and Emotet, in the past responsible for high-volume campaigns, which have resorted to alternative infection chains.

Instead, there has been a diversification of the infection chains and a marked increase in the use of ZIP, RAR, ISO images, and other archive formats, as well as HTML and LNK files. These have proven attractive to threat actors with a broad range of abilities. We also increasingly see threat actors utilizing DLL files as the final step in email-initiated infection chains and reducing the use of EXE files.

Notably, OneNote files (.one)—a component of the Microsoft Office suite which was seldom used previously—are widely exploited for cyberattacks. Despite the requirement of user interaction (double-clicking) to execute embedded files and attachments within OneNote, there has been a significant increase in attacks leveraging this technique since the start of the year. This strategy has enabled the distribution of malware such as Qbot, AsyncRAT, Redline, AgentTesla, and IcedID.

Exploitation of PDF files is not a new trend, but its frequency is increasing and is projected to continue. For example, Qbot was used to launch an extensive campaign in April this year in which it deployed malicious PDF files in multiple languages.

GLOBAL MALWARE STATISTICS

The following sections of this report present data comparisons that are based on data drawn from the Check Point ThreatCloud Cyber Threat Map between January and June 2023.

For each of the regions below, we present the percentage of corporate networks impacted by each malware family, for the most prevalent malware in H1 2023.

TOP MALWARE FAMILIES

GLOBAL

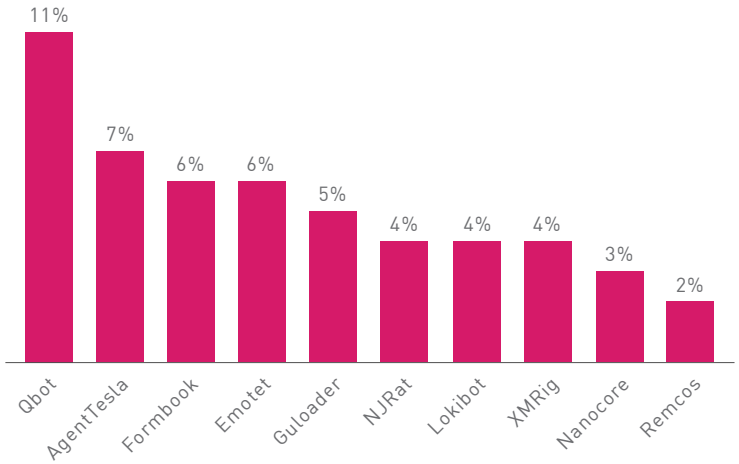


Figure 7. Most prevalent malware globally—H1 2023

AMERICAS

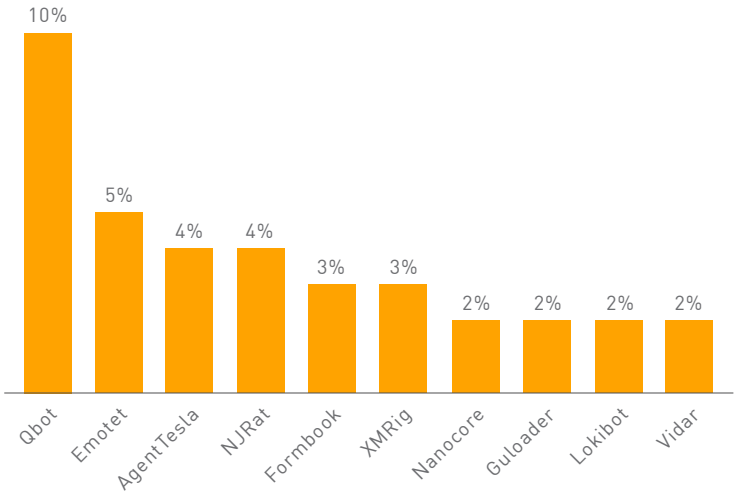


Figure 8. Most prevalent malware in the Americas—H1 2023

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

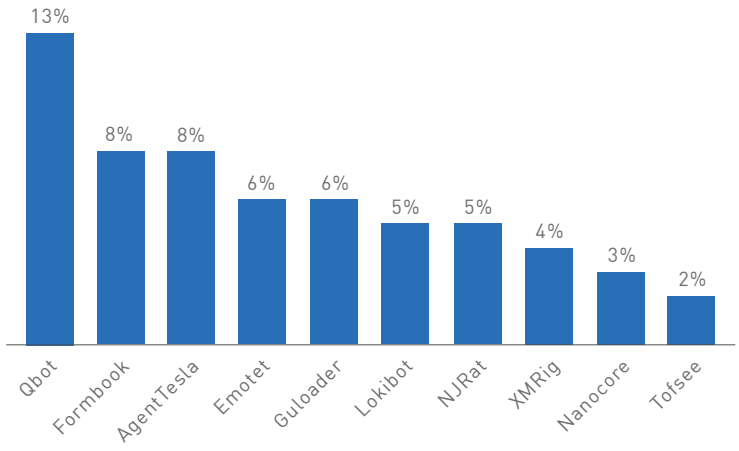


Figure 9. Most prevalent malware in EMEA—H1 2023

ASIA PACIFIC (APAC)

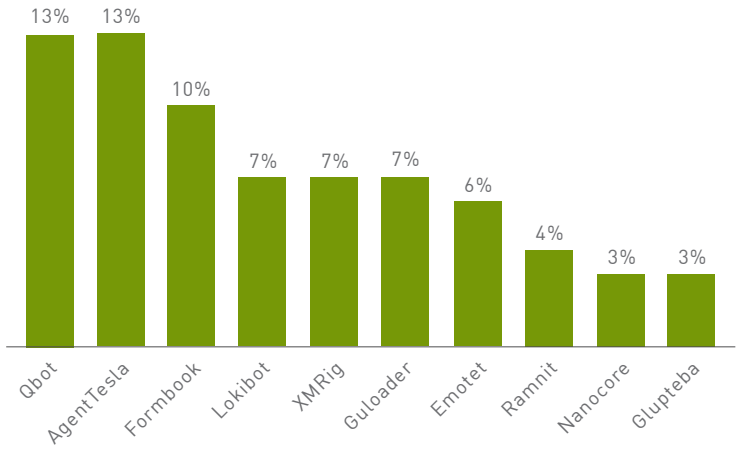


Figure 10. Most prevalent malware in APAC—H1 2023

GLOBAL ANALYSIS OF TOP MALWARE

The leading malware families fall into two primary categories. The first includes multipurpose malware such as Qbot, Emotet, and Glupteba. These are ongoing, large-scale botnet operations used for various purposes including data theft and providing system access and infectious code to other malicious actors. The second category consists of infostealers like AgentTesla, Formbook, and Lokibot. These types of malware are traded on underground forums and used by threat actors to steal diverse types of data ranging from login credentials to financial and corporate accounts, and up to credit card details.

With the evolution of the illicit market for access-brokers—those selling access to already infected victims—there has been a proportional increase in the number of infostealers. These infostealer infections typically represent the initial stage in this market, often managed by less technically proficient actors who later sell the pilfered data to more advanced actors to be used in more sophisticated attacks.

Qbot, a multipurpose malware known for its widespread phishing campaigns, was the most commonly detected malware in the first half of 2023. It is frequently utilized to deliver other malware families, including potential ransomware. Since January, Qbot orchestrated multiple malspam campaigns, compromising victims' systems through various methods. These include, but are not limited to, the use of OneNote files, PDF files, HTML smuggling, ZIP files, and more. Emotet is utilizing alternative file types, including the use of malicious OneNote files in a broad campaign in March.

The Guloader downloader released a new version in May which features fully encrypted payloads and advanced anti-analysis techniques. NjRat started the year with a comprehensive campaign infecting targets in the Middle East and North Africa.

XMrig remains the most prevalent crypto-miner which is used to generate revenue on infected platforms, often an early warning sign of a more serious infection.

MALICIOUS INFRASTRUCTURE BY TLD (TOP LEVEL DOMAIN)

In this report, we unveil a new statistical metric highlighting the most frequently utilized malicious Top-Level Domains (TLDs), as observed through Check Point's ThreatCloud AI since January 2022.

Domains, whether disguised as phishing sites or serving as the command and control (C&C) center of a prominent botnet, are frequently pivotal components of a threat actor's infrastructure. By understanding the various trends associated with TLDs, defenders can acquire another tool to evaluate the potential risk posed by certain TLDs to their organization.

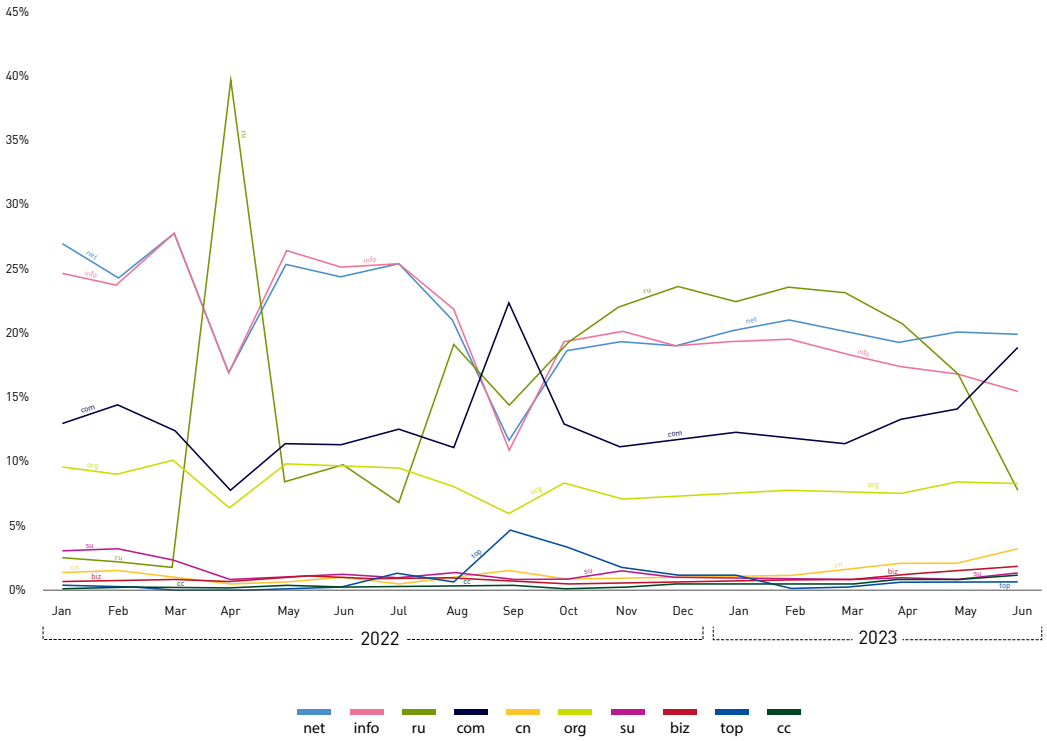


Figure 11. Percentage of new malicious domains by TLD per month.

Although TLDs are often thought of as something more stable in the threat landscape and as of something you do not need to keep tabs on, the recent introduction of Google's new .ZIP gTLD seemed to shatter this narrative. Google's announcement of the new .ZIP and .MOV gTLDs, which are identical to known file types, was greeted with dissatisfaction and scrutiny by the security community, as it showed new and unexpected behavior in existing applications, as well as presented even more ways to fool users and cause them to fall victim to phishing attacks.

Numerous factors may influence a threat actor's choice of one TLD over another. These include the specific organization they aim to impersonate, the availability of a particular TLD with their preferred domain registrar, or even the cost associated with the TLD.

Although less prevalent domains such as .xyz or .tk are often deemed more likely to be malicious, larger TLDs like .com and .net continue to be the more common choice for conducting malicious activities.

Presenting these statistics for the first time, we also include a historical review of 2022. In a somewhat surprising finding, we noticed a significant shift in the distribution of malicious TLDs starting from April 2022, a little more than a month after the onset of the Russian invasion of Ukraine on February 24. The proportion of malicious .RU domains in the group of all malicious TLDs surged dramatically from 2% to nearly 40%. Since then, .RU domains have consistently held the 3rd or 4th spot among all malicious TLDs. The Russian state-aligned Gamaredon APT is a regular "customer" of malicious .RU domains and is known for registering hundreds of domains through the REG.RU registrar over the past few years.

RANSOMWARE

This section does not use Check Point direct sensor data, but features information derived from more than 120 ransomware "shame-sites." Cybercriminals use these sites to amplify pressure on victims who do not pay the ransom immediately. Although this data comes from a dubious source and carries its own biases, it still provides valuable insights into the ransomware ecosystem, which currently poses the most significant risk to businesses. This data was collected in the period between January and June 2023.

TOP DOUBLE-EXTORTION RANSOMWARE ACTORS

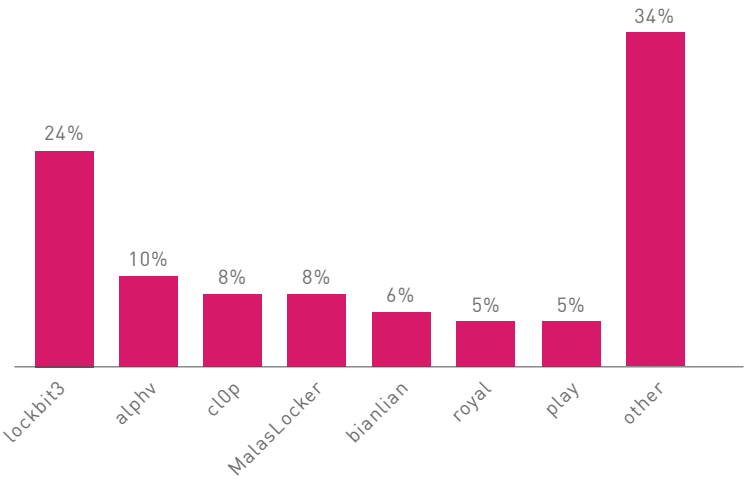


Figure 12. Most active actors by number of victims, as reported on shame sites—H1 2023.

In the first half (H1) of 2023, a total of 48 ransomware groups reported breaching and publicly extorting more than 2,200 victims. Among the active groups, Lockbit3 was the most prolific during this period, accounting for 24% of all reported victims with more than 500 cases. This represents a 20% increase in the number of reported Lockbit3 victims compared to H1 2022.

Veteran groups such as Lockbit, Alphv, and Cl0p have been joined by newer groups like Royal, Play, BianLian, and BlackBasta. The emergence of these new groups is partly attributed to the termination of the Hive and Conti Ransomware-as-a-Service (RaaS) groups. Rebranding is a common strategy employed within the ransomware ecosystem to impede law enforcement investigations. It is likely that the individuals behind these new operations are experienced actors who previously operated under different aliases and groups.

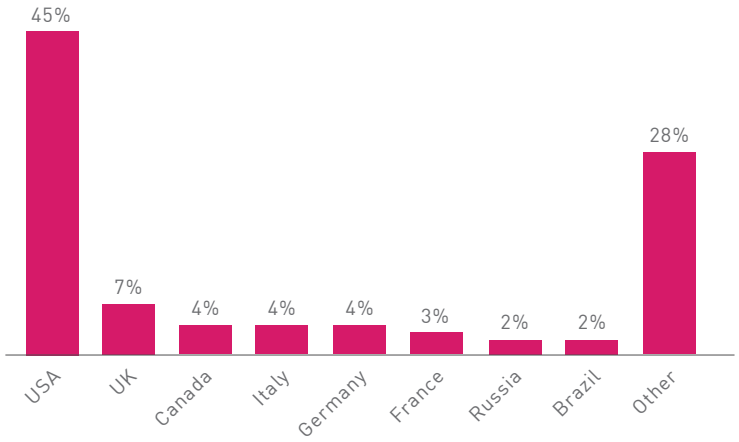


Figure 13. Victims by country, as reported on shame sites—H1 2023.

In terms of geographical distribution, 45% of affected companies are located in the United States, followed by the United Kingdom (7%) and Canada (4%). This distribution pattern aligns with previous years and underscores the focus of American authorities on combating ransomware. This commitment was demonstrated by a US-led operation against the Hive ransomware group in January 2023, when the FBI successfully infiltrated Hive's computer networks, obtained decryption keys, and thereby prevented potential ransom payments of $130 million, all of which ultimately resulted in the group's takedown. The unexpected presence of Russian entities among the victims is attributed to the emergence of a novel actor known as "MalasLocker." Appearing in April 2023, MalasLocker has adopted an unconventional approach by substituting traditional ransomware demands with charitable donations. Notably, MalasLocker has targeted over 170 victims, with approximately 30% of them being Russian entities. This selection of victims within the ransomware ecosystem is highly atypical, as attacks on former Soviet Union targets are usually avoided.

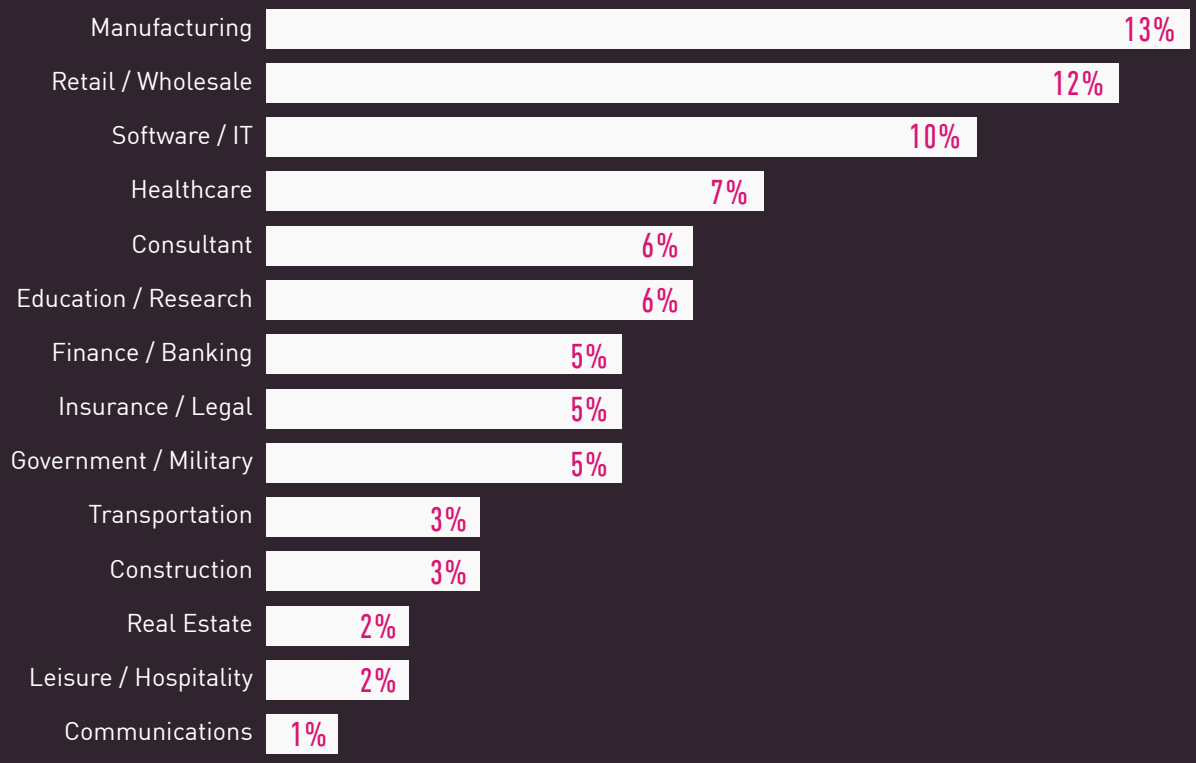


Figure 14. Industry distribution of ransomware victims, as reported on shame sites—H1 2023.

Considering the industry sectors impacted by ransomware attacks, while data drawn from the Check Point ThreatCloud Cyber Threat Map places the education, government, and healthcare sectors as primary targets, the ransomware victim landscape presents a different perspective. Manufacturing and retail produce the most victims, with government and education entities ranking lower in the target hierarchy. This divergence likely stems from the varying capacities and inclinations of these sectors to comply with ransom demands, with educational and governmental organizations being less inclined to make payments and fall victim to attacks primarily aimed at exploiting personal and technical data.

05

HIGH PROFILE GLOBAL VULNERABILITIES

The following information regarding top vulnerabilities is based on data collected by the Check Point Intrusion Prevention System (IPS) sensor net in 2023.

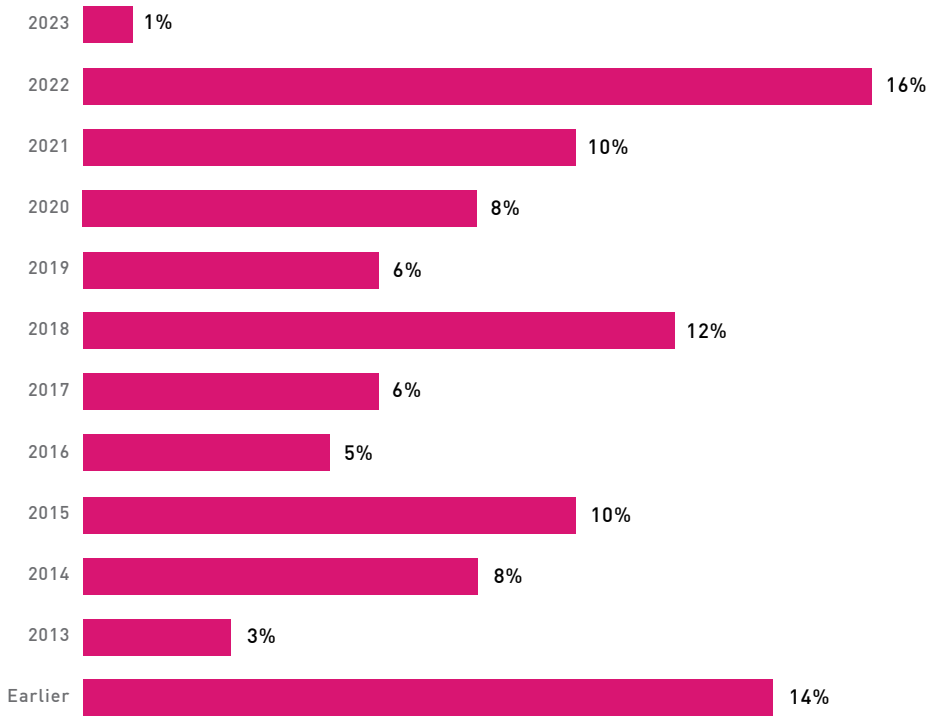


Figure 15. Percentage of attacks leveraging vulnerabilities by disclosure year in H1 2023.

Newly identified vulnerabilities reported in 2023 were almost immediately utilized and implemented by threat actors. Attacks involving CVEs reported in 2022 account for 17% of all detected assaults, suggesting that threat actors are expediting the integration of new vulnerabilities into frequently employed attacks. To put this into perspective, 28% of attacks in the first half of 2023 leveraged new vulnerabilities (starting from 2021), compared to 20% in the first half of 2022 and 17% in the first half of 2021.

06

HOW DEFENDERS ARE LEVERAGING AI TO PREVENT THE NEXT ATTACK

In the rapidly evolving landscape of cybersecurity, artificial intelligence (AI) has emerged as a powerful tool for defending against sophisticated and ever evolving cyberattacks. It has had a profound effect on both the efficacy of ransomware and other attacks methods, and the ability to defend against these advanced campaigns.

One of the key areas where AI is making a significant impact is in threat detection and analysis. AI-powered cybersecurity systems excel at identifying anomalies and detecting previously unseen attack patterns, thereby mitigating potential risks before they escalate.

For example, Check Point's ThreatCloud AI powers all of our solutions using AI technologies with big data threat intelligence to prevent the most advanced attacks while reducing false positives. It aggregates and analyzes big data telemetry and millions of Indicators of Compromise (IoCs) every day. Consider this scenario. A new malicious link is detected and blocked in a zero-day attack in the US. The threat data is immediately shared across all attack vectors with protections for this attack updated in real time. This same zero-day malicious link can then be blocked less than two seconds later in a similar attack in Australia –preventing the attack from causing disruption and damage.

POWERING PREVENTATIVE MEASURES WITH ZERO PHISHING IN CHECK POINT TITAN

Using legitimate brands in phishing attacks has proven to be extremely effective for attackers as it is highly convincing and often successfully tricks even the highest-level executives and security professionals.

In response to this, and to enhance online safety and security, Check Point has introduced an **industry first, inline security technology called 'Zero Phishing' in its Titan release, T81.20**, leveraging patented technology based on dedicated AI engines. The newly developed engine blocks links and websites associated with both local and global brands that have been impersonated and exploited as bait to deceive victims in phishing attacks, spanning multiple languages and countries.

The engine safeguarded more than 6,000 organizations across 140 countries in the first 30 days by effectively preventing potential attacks. This was achieved through the utilization of our advanced Quantum, Harmony, and CloudGuard products.

Check Point has also developed over sixty threat prevention engines that leverage its ThreatCloud AI threat intelligence for zero-day prevention. Our patented inline 'Zero Phishing' technology has prevented dozens of zero-day phishing campaigns. In fact, when tested, 'Zero Phishing' was able to detect x4 more zero-day phishing pages than traditional anti-phishing solutions, and 40% more detections compared to AI-based security vendors. The key advantage of the inline 'Zero Phishing' AI technology is that it doesn't require any installation on an endpoint or mobile devices.

PRACTICAL ADVICE: PREVENTING RANSOMWARE AND OTHER ATTACKS

Against a backdrop of advanced cybersecurity tools, organizations need to exercise good security hygiene across on-premise, cloud and hybrid networks all the way up to the board level. There are several actions that leaders can take to minimize exposure to and the potential impacts of an attack.

Here are a few simple tips to keep you safe:

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.

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 gain access to the employee's computer and begin the process of installing and executing the ransomware on it. 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 on the classic signs and language that are used in phishing emails.

3. Up-to-Date Patches

Keeping computers up-to-date and applying **security patches**, especially those labelled 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

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

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, including scanning and monitoring of emails, and scanning and monitoring file activity for suspicious files.

AI has become an indispensable ally in the fight against cyberthreats. By augmenting human expertise and strengthening defense measures, AI-driven cybersecurity solutions provide a robust shield against a vast array of attacks. As cybercriminals continually refine their tactics, the symbiotic relationship between AI and cybersecurity will undoubtedly be crucial in safeguarding our digital future.

07 MALWARE FAMILY DESCRIPTIONS

AgentTesla

AgentTesla is an advanced RAT which functions as a keylogger and password stealer and has been active since 2014. AgentTesla can monitor and collect the victim's keyboard input and system clipboard, and can record screenshots and exfiltrate credentials for a variety of software installed on a victim's machine (including Google Chrome, Mozilla Firefox and Microsoft Outlook email client). AgentTesla is sold on various online markets and hacking forums.

Andromeda

Andromeda is a modular bot for malicious activity, and was first spotted in 2011. It is used mainly as a backdoor to deliver additional malware on infected hosts, but can be modified to create different types of botnets. Andromeda utilizes various anti-sandboxing and anti-AV capabilities, such as injecting its code into legitimate processes, and is not visible in the task manager.

AsyncRAT

Asyncrat is a Trojan that targets the Windows platform. This malware sends out system information about the targeted system to a remote server. It receives commands from the server to download and execute plugins, kill processes, uninstall/update itself, and capture screenshots of the infected system.

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.

ClOp

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

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.

FakeCalls

FakeCalls is an Android Trojan that can masquerade as one of more than 20 financial applications and imitate phone conversations with bank or financial service employees. This type of attack is called voice phishing.

FluHorse

FluHorse is a malware that features several malicious Android applications that mimic legitimate applications, most of which have more than 1,000,000 installs. These malicious apps steal the victims' credentials and Two-Factor Authentication (2FA) codes.

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.

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.

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, and does not target individuals in Russia or other Commonwealth of Independent States.

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.

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.

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.

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.

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.

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.

08 CONCLUSION

As the conflict in Ukraine continues to drive state-sponsored attacks and hacktivist activity, ransomware is still the leading security threat to public organizations and enterprises globally and shows no signs of slowing down. Why is this? The answer is simple: the technique continues to work, and the malicious actors behind the attacks keep getting paid. And with ransomware-as-a-service groups vying with each other to win new affiliates and grow their revenues, these threat actors are not just getting bigger, they are getting more successful too.

At the same time, we've seen the re-emergence of old hacking tricks in the form of USB-borne malware infections, new easy-to-use AI tools for cyber activities becoming available with the emergence of ChatGPT, and new vulnerabilities being exploited on mobile devices. The only way that organizations can defend themselves against this onslaught of threats is to take an integrated, prevention-first approach to protecting their whole IT estate, from cloud to endpoint. Cyberattacks can, and will, happen. But with the right security technologies in place, the majority of attacks, even the most advanced ones, can be prevented without causing disruption or damage.

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™