



2024 CYBER SECURITY REPORT





YOU
DESERVE
THE BEST
SECURITY

CONTENTS

04	CHAPTER 1 INTRODUCTION TO THE 2024 CYBER SECURITY REPORT BY MAYA HOROWITZ, VP RESEARCH
07	CHAPTER 2 TIME LINE OF NOTABLE 2023 CYBER EVENTS
25	CHAPTER 3 CYBER SECURITY TRENDS <ul style="list-style-type: none">26 Ransomware Zero-days and Mega Attacks30 Expanding Attack Surface: The Emerging Risk of Edge Devices34 State-Affiliated Hacktivism and Wipers Become the New Normal38 Tokens under Attack: The Cloud's Achilles Heel41 PIP Install Malware: Software Repositories Under Attack
46	CHAPTER 4 GLOBAL ANALYSIS
70	CHAPTER 5 HIGH PROFILE GLOBAL VULNERABILITIES
75	CHAPTER 6 CHECK POINT INCIDENT RESPONSE PERSPECTIVE
81	CHAPTER 7 INSIGHTS FOR CISO'S—PREDICTIONS
85	CHAPTER 8 AI: THE CUTTING-EDGE DEFENDER IN TODAY'S CYBERSECURITY BATTLES
93	CHAPTER 9 MALWARE FAMILY DESCRIPTIONS
101	CHAPTER 10 CONCLUSION



INTRODUCTION TO THE 2024 CYBER SECURITY REPORT

MAYA HOROWITZ

VP Research, Check Point



Welcome to the Check Point 2024 Cyber Security Report. In 2023, the world of cyber security witnessed significant changes, with the nature and scale of cyber attacks evolving rapidly. This year, we saw cyber threats stepping out from the shadows of the online world into the spotlight, grabbing the attention of everyone from government agencies to the general public.

The reasons behind these attacks have become as varied as the methods used. Ransomware remained a major threat, with attackers not just after money, but also seeking recognition. Ransomware attacks exploiting zero-day vulnerabilities while using shame sites for publicly revealing who their victims are became more popular, turning ransomware into a sort of competition among cybercriminals. The cost of these attacks went beyond just paying the ransom, with companies like MGM, DP World, and the British Library facing huge expenses to rebuild their systems.

We also saw an increase in hacktivism, where hackers are driven by political or social causes. This type of hacking, once a tool for individual activists, is now being used by governments as a way to attack adversaries indirectly. This was especially noticeable in the wake of events like the Russo-Ukraine war and the Israel-Hamas conflict.

Attackers found new ways to break into systems, with devices like routers and switches becoming easy targets. Big organizations, including Okta and 23AndMe, were hit by attacks that used stolen login details or malicious software.

Artificial Intelligence (AI) played a bigger role in cyber attacks this year. Attackers started using AI tools to make their phishing campaigns more effective. However, the good news is that AI is also being used by cyber defenders to better protect against these threats.

There were some wins against cybercriminals too. Law enforcement agencies, including the FBI, made progress in taking down major threats like the Hive Ransomware network and the Qbot infrastructure. But the comeback of some of these groups reminds us that the fight against cybercrime is ongoing.

This report looks back at the major cyber security events of 2023, offering insights and analysis to help understand and prepare for the challenges ahead. Our goal is to provide valuable information to organizations, policy makers, and cyber security professionals, helping them to build stronger defenses in an increasingly digital world.

We hope you find this report informative and useful in your efforts to keep your digital environments secure.

Maya Horowitz

VP Research at Check Point Software Technologies



TIME LINE OF NOTABLE 2023 CYBER EVENTS

JANUARY

A database containing over 14 million usernames and passwords [was found](#) on a dark web forum, and within this database were more than 100,000 logins for portals belonging to Australian government agencies.

The Vice Society ransomware group has been conducting a series of widespread attacks targeting schools in both the United Kingdom and the United States. In response to these developments, the Federal Bureau of Investigation (FBI) [has issued](#) an official alert regarding the group's activities.



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

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 is [seeing](#) 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.

KillNet, a pro-Russian hacktivists group, [has launched](#) a wide scale operation against the US healthcare sector with multiple DDoS attacks.

JD Sports, UK sportswear retailer, has [announced](#) a data breach that affected approximately 10M clients. The alleged leaked data consists of clients’ online orders placed between November 2018 and October 2020, including full names, emails, phone numbers, billing details, delivery addresses, and more.

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.

The group behind the massive ‘ESXiArgs’ ransomware campaign, which [affected](#) thousands of VMware ESXi hosts, has [updated](#) their malware’s encryption process. The updated version of the malware prevents the potential recovery method that was recommended by researchers, as it now also encrypts the files that could have been used to trigger the recovery process.



Check Point IPS provides protection against this threat (VMWare OpenSLP Heap Buffer Overflow (CVE-2019-5544; CVE-2021-21974))

Social media platform Reddit [suffered](#) a security breach, after an employee fell victim to a phishing attack. According to the company’s statement, while internal documents and source code were stolen, user information and credentials have not been impacted.

One of Israel's leading universities, 'The Israel Institute of Technology' (Technion), has been [targeted](#) by a ransomware attack, forcing it to shut down its network and postpone final exams to the upcoming semester. Suspicions were raised that the attack might be politically or personally motivated, as the perpetrators are a previously unknown group and the ransom note included nonstandard messaging.

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.

Researchers have analyzed multiple campaigns using malicious packages in attempted supply-chain attacks. One Pypi (Python) campaign [created](#) over 450 crypto-related packages that would replace cryptocurrency wallet addresses, while another registered 5 packages that deliver credential-stealing malware. Also observed was an npm (Java) campaign, which delivered a remote-access Trojan.

City of Oakland has [announced](#) a local state of emergency as they are dealing with a ransomware attack that forced the city to take its IT systems offline.

The massive ESXiArgs ransomware campaign continues to expand, and recently [affected](#) over 500 hosts with the majority located in France, Germany, the Netherlands, the U.K., and Ukraine.

As OpenAI introduced a paid ChatGPT tier called ChatGPT Plus, threat actors are now [offering](#) so called free access to the platform, luring users to download malicious apps or visit phishing websites.

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)

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 victims' 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 [discovered](#) security flaws in chess.com that could allow users to manipulate game results. Using the vulnerability, researchers were able to reduce opponent's time and thus to win games.

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

The Italian luxury sports car maker Ferrari [has announced](#) a data breach following an extortion attack on the company's IT systems. The leaked data consists of the company's clients' personal information including full names, addresses, email addresses, and phone numbers.

Check Point Research [has detected](#) malicious packages on PyPI, Python package index, that use phishing techniques to hide its malicious intent. The malicious packages stealthily downloading and executing obfuscated code as part of their installation process, leading to supply chain risks.



Check Point CloudGuard Spectral provides protection against this threat.

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](#))

Researchers have been [tracking](#) the hacktivist group Anonymous Sudan, which had been engaged in launching multiple DDoS attacks on organizations in Europe, Australia, Israel and more, often in response to what is perceived as anti-Muslim activity. The group is currently considered and identified as a sub-group of the Russia affiliated hacktivists group Killnet, and supports its agendas.

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.

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

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)

Check Point Research [revealed](#) new Android malware called FluHorse. The malware mimics legitimate applications, most of which have more than 1,000,000 installations. The malware steals victims' credentials and Two-Factor Authentication (2FA) codes. FluHorse targets different sectors of Eastern Asian markets and is distributed via emails.



Check Point Harmony Mobile provides protection against this threat (FLU_HORSE_STR)

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 data storage giant Western Digital [has confirmed](#) a data breach that exposed the personal information of the company's clients. The leaked data includes names, billing and shipping addresses, email address and phone numbers. The threat actors claimed they are not affiliated with the ALPHV (aka Black Cat) ransomware gang but would use that group's leak site to threaten and extort the company.

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 [has published](#) a report on GuLoader—a prominent shellcode-based downloader that has been used in a large number of attacks to deliver a wide range of the “most wanted” malware. GuLoader’s payload is fully encrypted, what allows threat actors to store payloads using well-known public cloud services, and bypass antivirus protections.

Check Point Threat Emulation provides protection against this threat (Dropper.Win.CloudEyE.*)

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

Progress disclosed a [vulnerability in MOVEit](#) Transfer and MOVEit Cloud (CVE-2023-34362) that could lead to escalated privileges and potential unauthorized access to the environment. Upon discovery, Progress launched an investigation, provided mitigation steps and released a security patch, all within 48 hours. Unfortunately, during that time, cybercriminals associated with Russian-affiliated ransomware group Clop exploited the vulnerability and launched a supply chain attack against MOVEit users. Among them was payroll services provider Zellis, who was the first to disclose a security breach, although many others have been impacted.

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.*)

An Illinois hospital faced [closure](#) as a result of a ransomware attack, making it the first healthcare facility to shut down due to such an incident. The attack on SMP Health in 2021 disrupted the hospital's capability to submit claims to insurers, including Medicare and Medicaid, for several months. This situation led to a severe financial downturn for the hospital.

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 researchers have [discovered](#) a sophisticated malware affecting a European medical institution. The attack is attributed to Camaro Dragon (Mustang Panda), a Chinese state-sponsored APT group. The threat actors employ malicious USB drives as an initial access vector in order to target restricted networks, and their payload includes a module that further infects any additional USB drive that is plugged into an infected host. It is believed that the malware thus propagated beyond the attackers' initial intent, likely inadvertently infecting dozens of organizations worldwide.



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

JULY

Check Point Research [identified](#) a malicious modified version of the popular messaging application Telegram. The malicious application installs Triada Trojan which can sign up the victim for various paid subscriptions, perform in-app purchases and steal login credentials.

500GB of data has [leaked](#) from American television channel Nickelodeon as a result of a suspected breach. The data includes scripts, animation files and full episodes of content, and has been confirmed by the TV channel as legitimate, yet decades old. The said breach occurred during January this year, due to an authentication vulnerability on a feedback portal.

Check Point Research [has released](#) an analysis of Google's generative AI platform Bard, presenting several scenarios where the platform permits to generate malicious content. Threat actors could utilize Bard to generate phishing emails, malware keylogger and a basic ransomware code.

The Microsoft Exchange email account espionage campaign, which has been attributed to Chinese threat actor 'Storm-0558', has reportedly [accessed](#) the email account of United States ambassador to China and compromised hundreds of thousands of individual United States government emails. Researchers [warn](#) that the method used in the campaign could also have targeted user accounts other Microsoft services, such as OneDrive and Azure environments.

The Norwegian government has [reported](#) that a software platform, used by 12 key ministries, suffered a cyberattack. It happened after hackers exploited a zero-day authentication bypass vulnerability in Ivanti's Endpoint Manager Mobile (EPMM).

AUGUST

Prospect Medical Holdings, a major healthcare services provider that operates 16 hospitals and 166 outpatient clinics and centers in the US, [suffered](#) a significant ransomware attack. The attack has disrupted the company's operations in at least three states, and forced hospitals to divert patients to other facilities. No ransomware gang has publicly claimed responsibility for the attack yet.

Check Point researchers [share](#) the latest findings of NPM-based vulnerabilities that were discovered in over 50 popular packages, putting countless projects and organizations at risk.



Check Point CloudGuard CNAPP provides protection against this threat

Discord.io has [confirmed](#) that the company is handling a data breach exposing the information of 760,000 members, which led to the temporarily suspension of services. This comes after a cybercriminal going by the moniker Akihirah has posted the database of Discord in an underground forum.

An ongoing espionage campaign [targeting](#) dozens of organizations in Taiwan has been discovered. Researchers have attributed the activity to a Chinese APT group dubbed Flax Typhoon, which overlaps with Ethereal Panda. The threat group minimizes the use of custom malware, and instead uses legitimate tools found in victims' operating systems to conduct its espionage operations.

Pro-Russian hackers have [disrupted](#) train services in northwest Poland by gaining access to the railway's designated frequencies. The hackers broadcasted the Russian national anthem, as well as a speech of the Russian president Putin during the attack.

SEPTEMBER

The FBI [announced](#) operation ‘Duck Hunt’ dismantling the Qakbot (Qbot) malware operation that is active since at least 2008. Qakbot has been known to infect victims via spam emails with malicious attachments and links, while also serving as a platform for ransomware operators. It has impacted over 700,000 computers worldwide including financial institutions, government contractors and medical device manufacturers. Check Point Research [shared](#) its analysis of the Qakbot malware and its operations over the years.



Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Trojan.Wins.Qbot; Trojan.Win.Qbot; TrojanDownloader.Win.Qbot; Trojan-PSW.Win32.Qakbot; Trojan.WIN32.Qakbot)

Check Point [warns](#) of a recent Email phishing campaign abusing the data visualization tool—Google Looker Studio. Attackers use the tool to send slideshow emails to victims from official Google accounts, instructing them to visit 3rd party websites to collect cryptocurrency. The websites will then prompt the victims to input their credentials and thus to steal them.



Check Point Harmony Email provides protection against this threat.

Check Point researchers have [analyzed](#) the potential impact of the emerging generative AI technology on election influencing operations. Generative AI is capable of constructing individually tailored audio-visual propaganda to target voters on a massive scale, causing a heightened risk to democratic election integrity. To combat the issue, Google will [require](#) disclosure on political advertisements involving AI.

The American resort, casino and hotel chain MGM [has suffered](#) a cyber-attack that resulted in widespread disruption across the company’s hotels and casinos, and has shut down its internal networks as a precaution. The cyber-attack paralyzed the company’s ATMs, slot machines, room digital key cards and electronic payment systems. ALPHV ransomware affiliate, has claimed responsibility for the attack. Check Point Research is [sharing](#) its analysis insights on the activity of the ALPHV group during the last 12 month.

Monti ransomware gang [has claimed](#) responsibility for a cyber-attack on New Zealand's third-largest university, Auckland University of Technology. The threat actors claim to have stolen 60GB of data, giving the victim a deadline of October 9th to pay a ransom.



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

Check Point Research [has discovered](#) new version of the BBTok banking malware, which targets clients of over 40 Mexican and Brazilian banks. The research highlights newly discovered infection chains that use a unique combination of Living off the Land Binaries (LOLBins), which results in low detection rates. The research also reveals some of the threat actor's server-side resources used in the attacks, targeting hundreds of users in Brazil and Mexico.



Check Point Threat Emulation and Harmony Endpoint provide protection against this threat (Banker.Wins.BBTok; Banker.Win.BBTok; Technique.Wins.SuxXll; Trojan.Win.XllAddings)

OCTOBER

Check Point researchers have [detected](#) a phishing campaign exploiting popular file-sharing program Dropbox. The threat actors use legitimate Dropbox pages to send official email messages to the victims, which will then redirect the recipients to credential stealing pages.

Check Point researchers have [discovered](#) multiple critical vulnerabilities affecting the WEB3 social media platform Friend.tech. The set of vulnerabilities can allow attackers to access and modify database values belonging to the company, as well as gain access to paid features.

The American Rock County Public Health Department, which serves more than 160K people across Wisconsin area, [has been](#) a victim of a ransomware attack that forced officials to take some systems offline. Cuba ransomware gang has claimed responsibility for the attack, claiming to have stolen financial documents, tax information and more.

-  **Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Win.Cuba, Ransomware.Wins.Cuba.ta.*)**
-

LockBit ransomware gang [has claimed](#) responsibility for an alleged attack on the multibillion-dollar IT products and services reseller CDW. The gang has demanded \$80M ransom and threatened to release stolen data, said to include employee badges, audits, commission payout data and more. The company has isolated the affected servers, which are claimed to be non-customer-facing.

-  **Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Win.Lockbit; Gen.Win.Crypter.Lockbit; Ransomware.Wins.LockBit.ta; Ransomware_Linux_Lockbit)**
-

The FBI and CISA have [released](#) a joint Cybersecurity Advisory under their #StopRansomware campaign, warning of and diving into AvosLocker ransomware, which operates under a ransomware-as-a-service (RaaS) model. They focus on technical details and the group's TTPs to assist mitigation and defense.

-  **Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Wins.Avoslocker.ta.A, Gen.Win.Crypter.AvosLocker.B, Ransomware.Win.AvosLocker.B, Ransomware_Linux_AvosLocker)**
-

Attackers have [gained access](#) to parts of the network of the cloud identity authentication giant Okta. The hackers managed to gain access to the firm's support unit for at least two weeks and have attempted to use tokens copied from support tickets to access the firm's customers' networks. Reportedly, the firm only became aware of the incident when a customer reported that a support ticket token being abused.

Check Point Research has [analyzed](#) cyber activity related to the first ten days of the Israel-Hamas war. Multiple hacktivist groups, Middle Eastern, Islamic, and Russian-affiliated, have intensified their operations against Israel. Various attack vectors have been observed, including DDoS, defacement, and information leakage from some Israeli websites—most of those with very limited impact.

Stanford University [has been](#) a victim of cyber-attack that affected the systems of its Department of Public Safety (SUDPS). Akira ransomware gang claimed responsibility for the attack, which allegedly resulted in the exposure of 430GB of university's data.



Check Point Harmony End Point and Threat Emulation provides protection against this threat (Ransomware_Linux_Akira; Ransomware_Wins.Akira)

NOVEMBER

Boeing has acknowledged that a cyber-attack had [affected](#) its parts and distribution business, and that the company is working with law enforcement to investigate. Earlier this week, ransomware group LockBit has added Boeing to its victim page and claimed to have stolen large amounts of data.



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

Check Point Research has [revealed](#) an ongoing espionage campaign of Scarred Manticore—threat actor tied to the Iranian Ministry of Intelligence and Security (MOIS). The attacks rely on LIONTAIL, an advanced passive malware framework installed on Windows servers. The current campaign is targeting high-profile organizations in the Middle East, focusing on government, military, and telecommunications sectors.



Check Point IPS, Threat Emulation and Harmony Endpoint provide protection against this threat (Backdoor.WIN32.Liontail.A/B, APT.Wins. Liontail.C/D)

Check Point Research [released](#) a recent review of the evolving cyber events in light of the Israel-Hamas war. The recent weeks revealed that pro-Palestinian hacktivist groups have broadened their scope beyond Israel, mainly targeting countries perceived as Israeli allies. These cyber operations aim to have informational and retaliatory effect, however, have limited reported damage. Notably, the target choice is set by the groups' previously established interests, in addition to evolving geopolitical events.

US unit of China's largest bank, the Industrial and Commercial Bank of China (ICBC), has suffered a ransomware attack that disrupted some of its financial services systems, reportedly affecting liquidity in US Treasuries. LockBit ransomware gang is reportedly behind the attack.



Check Point Threat Emulation and Harmony Endpoint provide protection against this threat (Ransomware.Wins.LockBit.ta*; Ransomware.Win.Lockbit; Gen.Win.Crypter.Lockbit.AI; Ransomware_Linux_Lockbit)

Russia-affiliated military intelligence group SandWorm is reportedly responsible for an attack against 22 critical infrastructure companies in Denmark. The attacks, most severe in Danish history, have compromised industrial control systems and forced companies from the energy sector to work offline.

Check Point Research conducted an experimental deep dive to test ChatGPT's malware analysis capabilities. The findings focus on the guidance the AI system requires in order to expand its capabilities and deliver a verdict.

Nevada-based medical transcription company, Perry Johnson & Associates (PJ&A), has disclosed a data breach that affected more than 9M patients at multiple healthcare providers in the US. The exposed data includes patients' names, addresses, dates of birth, Social Security Numbers, and medical records. The attack is considered as one of the most severe medical data breaches in recent years.

Check Point Research, using Threat Intel Blockchain system, uncovered an ongoing sophisticated Rug Pull scheme that managed to pilfer nearly \$1M. The actor behind this scheme was traced, unveiling the perpetrator lured unsuspecting victims into investing using the crowd's hype around ill-gotten gains.

DECEMBER

Check Point Research [provided](#) highlights about Cyber Av3ngers group activity, which has taken responsibility on defacing workstations at Pennsylvania's Aliquippa municipal water authority. Following the attack, CISA has [published](#) an advisory about this hacktivists group which is affiliated to Iranian Revolutionary Guard Corps (IRGC) and reportedly hit multiple water utility companies in the United States by targeting Unitronics' PLC devices.

The American Greater Richmond Transit Company (GRTC), which provides services for millions of people, [has been](#) a victim of cyber-attack that impacted certain applications and parts of the GRTC network. The Play ransomware gang claimed responsibility for the attack.



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

Check Point Research [exposes](#) a troubling trend in the cryptocurrency landscape. Deceptive actors are manipulating pool liquidity, sending token prices soaring by 22,000%. The manipulation of pool liquidity resulted in a swift and calculated theft of \$80,000 from unsuspecting token holders. This incident sheds light on the evolving strategies scammers employ to exploit decentralized finance platforms.

Ukraine's largest mobile operator, Kyivstar, was [hit](#) by "largest cyber-attack on telecom infrastructure in the world", rendering millions without mobile and internet services for at least 48 hours. Reportedly, the attack also affected air raid sirens, ATMs, and point-of-sale terminals. Russia-affiliated group Solntsepek, who was previously linked to Russian military group Sandworm, claimed responsibility for the attack. Another Russia-aligned group, Killnet, claimed responsibility, however its involvement hasn't been proved. Kyivstar has 24.3 million mobile subscribers and over 1.1 million home internet subscribers.



CYBER SECURITY TRENDS

Ransomware Zero-days and Mega Attacks

Several major ransomware attacks in 2023 exploited zero-day vulnerabilities. Unlike other ransomware trends we covered previously, whether or not other actors adopt this strategy depends solely on economic considerations: Does the yield of a multi-victim ransomware attack justify the going price of a zero-day exploit used to accomplish it? To answer this question, we review these attacks and the ecosystem that makes them possible.

In its current state, the term ransomware doesn't only refer to encrypting data, but is used to characterize cyberattacks where a financially motivated actor has gained significant control over the victim's assets and exerts pressure to extort money.

This criminal ecosystem is made up of ever-changing groups and individuals who engage in a delicate balancing act, simultaneously seeking public attention and "fame" to attract potential affiliates and maintain their reputation while avoiding too much attention from law enforcement. The actors frequently engage in rebranding, which makes attribution challenging.

When we analyze attack trends within the ransomware ecosystem, we frequently examine the new features introduced by Ransomware-as-a-Service (RaaS) providers to enhance their operational capabilities. These can range from evasion techniques like intermediate encryption mechanisms or restarting in safe-mode to enhanced encryption speeds. Other enhancements include extended extortion tactics, such as data theft and the threat of data exposure, as well as the implementation of stolen data indexing, and compatibility with additional operating systems. Another important development we [saw](#) in 2023 was that ransomware versions for Linux became the standard.

Ransomware's impact on business operations has escalated and reached a peak in 2023, as seen by multiple high-profile attacks including ALPHV's breach of [MGM Resorts International](#). This particular attack resulted in extensive data theft and significant disruption to business operations, with MGM estimating damage costs at \$100 million. In addition, the Australian ports operator [DP World](#) experienced a severe ransomware attack that disrupted 40% of the country's container trade for several days. As reported, this attack did not involve encryption, which underscores the evolving nature of these threats.

This past year saw a notable increase in large-scale ransomware cyberattacks affecting multiple victims, with some incidents impacting hundreds or even thousands of organizations. The CL0P RaaS group exploited a zero-day vulnerability in the [GoAnywhere](#) secure file transfer tool, resulting in breaches that affected over 130 organizations. In early June, CL0P exploited a zero-day vulnerability that enabled it to access the [MOVEit](#) file-transfer software, which led to the compromise of more than 2,600 organizations. CL0P conducted a similar attack back in 2021 when it [exploited](#) zero-day vulnerabilities in Accellion's legacy File Transfer Appliance to breach the databases of multiple clients. In all these cases the targets were carefully selected on account of a high volume of customers, data quality, and the ability to spread the attack to additional victims.

Notably, CL0P chose not to encrypt victims' data but threatened to expose or sell it. This extortion strategy can adversely affect even those victims who regularly maintain backups and employ data restoration procedures. It also decreases the chance of detection during the "noisy" encryption phase of an attack and relieves cybercriminals of the burden of managing decryption keys and the associated "customer service" responsibilities related to multiple file decryption.

Zero-day exploits are highly sought after and are traded in a thriving market. The price of zero-day exploits depends on the targeted system and the nature of the vulnerabilities and can range from several thousand dollars to as much as \$2.5 million (on mobile platforms). Prices publicly presented by legitimate platforms like [Zerodium](#) reflect what's going on in parallel criminal underground markets. The sellers' credibility in these markets depends on the reputation established from previous transactions and the deposits used as collateral. In the screenshot below, an underground seller with a substantial history and deposit offers a Windows Local Privilege Escalation (LPE) exploit for sale for \$150K (before negotiations). For comparison, you can buy Windows LPE vulnerabilities on Zerodium for \$80K.

The screenshot shows a forum post with the following details:

- Title:** [Sale] 0day Win Lpe
- Author:** [REDACTED] (Published on October 11, 2023)
- Description:** Selling 0day lpe under the winch, a new vector.
- Technical Details:** Vulnerable wines10-11, servers 19-22 architecture x64.
- Offer Details:** The set includes binar-ehe and source, all in one hand. Price 150k.
- User Profile:**
 - megabyte (User icon: orange circle with a yellow star)
 - Paid registration (5 publications)
 - Registration date: 10/26/20 [REDACTED]
 - Activities: security / security Deposit 0.545668 \$
- Message:** First contact / questions in PM. There are only reviews in the topic. Thank you for your attention.
- Buttons:** + Quote

Figure 1: Zero-day Windows LPE vulnerability offered in an underground forum.

Zero-day vulnerabilities have limited shelf lives. The more they are exploited, the higher the likelihood of detection and subsequent patching. Unlike adding features to malware, investing in a zero-day vulnerability, whether through purchase or development, represents a recurring cost that must repeat for each campaign and thus has to be covered by the income generated from a relatively short-lived attack.

Whether zero-day exploitation becomes a common practice depends on the direct yield of each attack. Some estimate CL0P could earn \$75-100M from the MOVEit attack alone. Estimates of actual ransom payments can be challenging, but it is safe to assume that, at least in some cases, they more than cover the zero-day cost.

After the MOVEit attack, exploitation of zero-day vulnerabilities for ransomware attacks continued. Threat actors associated with CL0P were observed exploiting a zero-day vulnerability within the SysAid IT support software, potentially impacting over 5,000 customers. The company disclosed in an advisory that it became aware of this new vulnerability (CVE-2023-47246) on November 2, but the earliest reports of the exploitation date back to October. Beyond CL0P, Akira and Lockbit, two of the most prolific ransomware actors, have been exploiting a zero-day vulnerability (CVE-2023-20269) in Cisco appliances, enabling attackers to conduct brute force attacks against existing accounts.

Other financially-motivated advanced groups, like [DarkCasino](#), have [exploited](#) the WinRAR vulnerability (CVE-2023-38831) to steal from online traders. The suggested price for a WinRAR RCE exploits by [Zerodium](#) is \$80K. In another incident, the Nokoyawa ransomware was deployed by a financially motivated actor after [exploiting](#) a zero-day in the Windows Common Log File System (CLFS) for privilege elevation.

The likelihood of a growing trend in the use of costly zero-day exploits depends primarily on economic considerations. If threat actors are convinced that the potential returns outweigh the investment, we can expect an increase in these types of attacks. Giving in to extortion attempts provides a short-term solution to an immediate crisis, but in the long-term this only emboldens the attackers. Effectively safeguarding against zero-day attacks presents a complex challenge, which emphasizes the importance of implementing robust measures such as endpoint anti-ransomware solutions, Data Loss Prevention (DLP) mechanisms, and Extended Detection and Response (XDR) products.



SERGEY SHYKEVICH

Threat Intelligence
Group Manager,
Check Point Software
Technologies

In the world of ransomware deployment, the decision to use high-cost zero day exploits is predicated on the potential returns that hackers believe they will get.

We should assure that the returns don't outweigh the investment. To mitigate the growing risk of these types of attacks—implement advanced security tools, including anti-ransomware solutions, DLP and XDR.

Expanding Attack Surface: The Emerging Risk of Edge Devices

Often under-prioritized in security strategies, edge devices have long been exploited by cybercriminals to setup botnets for DDoS attacks and to orchestrate spam campaigns.

In an ongoing trend that has reached its zenith this year, edge devices have become the target of nation-state APTs and financially motivated advanced threat actors, who are using them either as a part of a sophisticated exfiltration infrastructure or as entry points for penetrating broader network systems of carefully selected entities and devices. Initially leveraged by state actors using expensive zero-day exploits and custom-made malware, this strategy has since been adopted by financially motivated sophisticated groups who exploit misconfigurations and known vulnerabilities in unpatched systems for ransomware attacks.

Edge devices like routers, switches, VPN hardware and security appliances are often neglected in security analyses. They are difficult to log and monitor, lack EDR protection and serve as security devices in and of themselves and are thus often overlooked, left with default passwords, inadequately patched, or reach patchless end-of-life status. Vulnerable, these internet-facing devices have been routinely exploited to construct botnets. The Mirai malware and its many spinoffs, for example, infamously infect Linux routers using default passwords, leveraging them for DDoS attacks and spam campaigns. Since these breaches do not necessarily directly affect the networks, they hardly received any attention.

Edge device exploitation has undergone significant changes in recent times, now conducted by nation-state APTs to construct stealthy-communication and exfiltration infrastructure for covert operations. A recent Check Point [research](#) report revealed a Chinese operation targeting TP-Link routers with dedicated firmware malware. The state-sponsored Camaro Dragon APT deployed a custom backdoor called “Horse Shell” to maintain persistence as well as for file transfer and network tunneling, thus anonymizing their communication through a chain of infected nodes. This methodology of using compromised routers as covert networks for C&C obfuscation was previously reported as [RedRelay](#) and [ZuoRAT](#) and continued to thrive in 2023.



Edge devices are not only targeted for use as components of communication infrastructure, but also as initial entry points into networks. In a sophisticated operation [reported](#) by Microsoft in May, the Chinese state-sponsored Volt Typhoon APT group employs a dual strategy. This group exploited SOHO (Small Office/Home Office) edge devices and integrated them into their communication [infrastructure](#) later called the KV-botnet. This botnet was then used to disguise command and control (C&C) communications from other compromised edge devices within critical infrastructure organizations in the United States.

Unlike Camaro Dragon, this case did not involve dedicated firmware malware but rather the KV-botnet comprised of end-of-life Cisco and DrayTec routers as well as NETGEAR firewalls. Fortinet FortiGuard devices in critical U.S. infrastructure were separately breached, serving as gateways for espionage and potential disruption, with hidden communication via the KV-botnet.

Not only end-of-life unpatched known vulnerabilities are used to exploit edge devices. Mandiant researchers [reported](#) extensive zero-day exploitation and employment of customized malware to target edge and network devices by Chinese APTs like UNC3886 and UNC4841. UNC3886 has used dedicated customized malware to target Fortinet security devices and VMware servers, devices without EDR solutions.

UNC4841 conducted a global espionage [campaign](#) by exploiting a zero-day vulnerability in another edge device, the Barracuda Email Security Gateway (ESG). In one of the more aggressive campaigns reported this year, attackers targeted public and private sector entities worldwide with an emphasis on those in the Americas. Almost a third of the affected organizations identified were government agencies. In response to discovery and mitigation efforts, attackers deployed additional malware [designed](#) to maintain persistence on a subset of breached entities. This aggressive persistent campaign has led to the exceptional supplier recommendation to [replace](#) all ESG appliances, as they are deemed unsafe.

Edge devices are not exploited exclusively by Chinese actors. Russia's military intelligence affiliated APTs extensively used this strategy against Ukrainian targets during the ongoing conflict. Since the start of the Russian-Ukrainian war, a barrage of [cyber-attacks](#) significantly damaged Ukraine's energy, media, telecommunications, and financial industries, as well as government agencies. The intensity and volume of these attacks were facilitated by compromising edge devices, enabling Russian threat actors to maintain persistent access to targeted networks and conduct multiple attacks over time. The Russian-linked APT28 group was observed deploying the [JaguarTooth](#) malware, which was specifically designed to exploit vulnerabilities in CISCO IOS routers, which despite being reported back in 2017, have still proven to be effective.

Broadening their cyber-attack landscape beyond Ukraine, in late 2023, the Russian APT Sandworm targeted Denmark's infrastructure and energy sectors. In what signals a significant escalation, the group [executed](#) attacks on 22 Danish entities, leveraging two zero-day vulnerabilities in Zyxel firewalls. This strategic move to compromise critical facilities in Denmark, targeting vulnerable edge devices provided attackers with remote code execution (RCE) capabilities on beached platforms. As a result, several companies were forced to halt normal operations and temporarily resort to 'Island Mode' functioning. This shift underscores Sandworm's extensive capability to exploit vulnerabilities and coordinate attacks on a wide scale.

Financially motivated ransomware groups are also targeting edge devices. [CACTUS](#), [Akira](#), and [LockBit](#) exploit misconfigured or vulnerable Citrix and Fortinet VPN devices in their attacks. Groups such as [FIN8](#), [LockBit](#), and Medusa leveraged critical unpatched vulnerabilities in Citrix NetScaler devices to compromise large companies. These attacks progressed to the deployment of persistent webshells that remain active even after the patching and rebooting. Breaches using edge devices often culminate in ransomware attacks deployed to compromised networks.

Previously targeted primarily by Mirai-like botnets for spam and DDoS attacks, edge devices are now exploited by more sophisticated actors in precise operations. They are used as communication infrastructure for other campaigns, as initial access points or as a means of disrupting their original networks. What started as a sophisticated method, practiced by nation-state actors to gain stealthy access, was later adopted by financially motivated attackers using existing toolkits.

This focused targeting of edge devices has

proven effective for breaching high-profile targets while avoiding detection for extended periods. Without timely patching, sufficient monitoring and detection systems, specifically for edge devices, publicly-facing network devices will remain a massive blind-spot. As the threat landscape evolves, so should our security solutions and monitoring capabilities.



ELI SMADJA

Security Research
Group Manager,
Check Point Software
Technologies

The escalating threat that is edge device exploitation demands a recalibration of security strategies. We must fortify our cyber security infrastructure.

Leverage the recommendations outlined in this section —Securing against sophisticated edge device attacks is critical for businesses in 2024.

State-Affiliated Hacktivism and Wipers Become the New Normal

The nature of hacktivism, which uses cyber-attacks to promote political or social objectives, has significantly evolved in recent years. Initially characterized by grassroots individuals and loosely organized collectives, it has now shifted toward substantial government involvement.

In its current form, a major portion of cyber activities are conducted by state-affiliated hacktivist groups. These entities act as fronts, publicizing the yields of activities conducted by nation-state advanced persistent threat (APT) units. By hiding behind hacktivist group facades, nation-states can foster an illusion of popular support, and distance themselves from the attacks and avoid retaliatory actions.

This new modus operandi is also characterized by the increasing use of wipers designed to maximize operational disruption. Notably, these trends were shaped during the Russian-Ukrainian war and have parallels in the ongoing conflict between Israel and Hamas. However, despite the intensity of these activities and the substantial resources invested, the actual impact they have on the dynamics of warfare is questionable.

Anonymous Sudan, an entity that emerged in early 2023 and is commonly [affiliated](#) with Russia, has been actively targeting Western entities under the guise of supporting Islamic causes. This group has executed numerous Distributed Denial-of-Service (DDoS) attacks on a global scale, impacting critical infrastructure and various other sectors.

The high-profile targets of Anonymous Sudan include the infrastructure and websites of companies such as [Microsoft](#), [Twitter \(X\)](#), [Telegram](#) and [Scandinavian Airlines](#). In the single year of its existence, Anonymous Sudan has been responsible for some of the most successful DDoS attacks ever recorded, including a major [assault](#) on Microsoft's services. The group's operations consist of collaborations with Russian-affiliated attack groups like Killnet, particularly when it comes to cyberactivity related to the Russian-Ukrainian war and anti-Western entities. Unlike other hacktivist collectives, Anonymous Sudan is believed to [utilize](#) rented server infrastructure for its attacks, suggesting it has access to substantial financial resources. These characteristics, coupled with the predominant use of English and Russian and the

minimal use of Arabic (despite it being the official language of Sudan), have led researchers to speculate that there is a definite connection to or support from Russia.

In December 2023 the biggest destructive attack since the beginning of the Russia-Ukrainian war, was [executed](#) against Ukraine's largest mobile network operator—Kyivstar. Previously low-profile hacktivists group Solntsepyok, took responsibility on this attack. Ukraine links this hacktivist activity to Sandworm APT group, which is operated by Russian military intelligence. Reportedly, the attack completely destroyed the core of the telecom's operator.

In recent years, Iran has also significantly developed and [employed](#) its cyber capabilities, while focusing heavily on cyber-enabled influence operations. This trend has escalated within the context of the Israel-Hamas war. Unlike Russian state-affiliated hacktivism, which primarily focuses on distributed denial-of-service (DDoS) attacks, Iranian-associated hacktivist groups have adopted a more aggressive and technologically advanced approach focusing on destructive and hack-and-leak operations.

Historically, Iran has been a strong [supporter](#) of Hamas in terms of financial aid and training, and this has intensified since the beginning of the war, on October 7th 2023. Following a strategy similar to Russia's, Iran has deployed cyber "hacktivist" forces to engage in digital warfare.

The Iranian-affiliated hacktivist KarMa group launched its English-speaking telegram channel on October 8, quickly gaining significant attention with over 10,000 subscribers. KarMa serves as a cyber persona, an online front for the Iranian Ministry of Intelligence and Security (MOIS) which operates the "[Scarred Manticore](#)" APT, the Dev-0842, and several other groups. Through its Telegram channel, KarMa disseminates information obtained from breaches of Israeli entities by Scarred Manticore espionage operations. Some of these breaches were accompanied by wiper attacks, which inflicted damage on the affected companies' infrastructures. The [deployed](#) Linux and Windows dedicated wiper, called "BiBi-Wiper" after Israeli PM Benjamin Netanyahu, was attributed to Dev-0842. This is typical of the increasing prevalence of destructive malware, which has become a new norm in hacktivist operations.

The same mode of operation was previously [used](#) by Iranian-affiliated actors against Albanian government entities in 2022. In a series of attacks, a cyber persona called "Homeland Justice" operated a dedicated Telegram channel and website that was used to leak materials of Albanian Government entities whose systems were breached and suffered wiper attacks. The attacks were executed by MOIS-affiliated actors, including Scarred Manticore and Dev-0842. This pattern of using cyber personas operating dedicated communication channels for leaking breached materials and wiper attacks reflects a consistent strategy employed by these Iranian-affiliated groups. During December 2023, Iranian "Homeland Justice" [resumed](#) to its activity, with another wave of destructive cyber-attacks against key Albanian entities.

Another Iranian MOIS affiliated APT group known as Agrius or DEV-0227, launched a separate attack on the Israeli Ziv hospital in late November of 2023. While Agrius has a [history](#) of deploying wipers that are sometimes disguised as ransomware, [the attack](#) on Ziv reportedly failed to disrupt the hospital's network, although sensitive information was stolen. Similar to how KarMa operates, the stolen data was later [published](#) on the Telegram channel and website of another cyber persona named Malek Team, which also appeared in the early days of the war.

[Cyber Toufan Operations](#), another recently introduced Iranian-affiliated cyber persona, was launched in November 2023 and operates a Telegram channel in Arabic and English. This group disclosed information obtained from various Israeli businesses following a [breach](#) of an Israeli hosting service. Similar to previous incidents, this breach involved data theft followed by destructive malware. Other Iranian-affiliated hacktivist groups that had been dormant but were reactivated during the current conflict include [AlToufan](#) and Moses Staff, attributed to the Islamic Revolutionary Guard Corps (IRGC).

A significant portion of these cyber operations is focused on information and psychological warfare. This is where the main objective is to disclose supposedly successful cyber-attacks, thus emphasizing the targeted victims' vulnerabilities. These threat actors commonly exaggerate the

impact of their destructive operations that actually occurred and also publish news or data from fictitious attacks. Cyber Av3ngers, a group acting as a front for Iranian-affiliated activities, [published](#) details of attacks dating back to 2022, some of which were already reported by other groups. This strategy of blending genuine breach reports with fabricated ones is also employed by several other online groups, including one known as [Soldiers of Solomon](#), which is closely related to the Cyber Av3ngers. Those groups' main focus was on programmable logic controllers (PLCs) and IOT cameras. Both Cyber Av3ngers and Soldier of Solomon were publicly [attributed](#) to the IRGC.

Similar to the Russian cyber-operations during the Ukraine conflict, which [expanded](#) a few months into the war to target additional Western countries in particular NATO member states, Iranian cyber activities also [extended](#) their reach westward. For example, Cyber Av3ngers [targeted](#) Israeli-made digital control panels, breaching several US and [Irish](#) water facilities.

Reflecting on the patterns observed in the [Ukrainian](#) conflict, cyber activities in this recent conflict were not solely the domain of state-affiliated hacktivist groups. In the first weeks of the Israeli-Hamas war, the cyber warfare landscape saw [numerous](#) regional hacktivist groups, predominantly with Islamic affiliations, step up their activities together with the formation of hundreds of new anti-Israeli hacktivist groups.

These groups primarily emerged on Telegram. The operations carried out by these organic hacktivist entities mainly involved minor DDoS attacks and website defacements. The impact of these activities was generally minor, with their effects largely limited to screenshots shared on Telegram channels. However, [significant](#) DDoS attacks were observed in the early stages of the conflict, with Israeli websites facing intense targeting.

In the midst of this, Russian-affiliated hacktivist groups did not maintain neutrality. Notably, Anonymous Sudan claimed responsibility for several [cyber-attacks](#) against Israel. These included a strike on the official Israeli app used for incoming-missile-alerts to the civil population, and an attack that took down the digital [domain](#) of The Jerusalem Post, a leading English-language Israeli newspaper.

Hacktivism has evolved to a point where state-affiliated groups now dominate much of the impactful cyber activity. Despite this heightened involvement from hostile governments, and the increased focus on destructive and disruptive activities, the actual effectiveness of these cyber operations remains debatable. A significant portion of this activity often goes unnoticed in the mainstream media, overshadowed by conventional warfare reports. As a result, these cyber actions often leave only a minimal impression on public opinion. Considering their limited visible impact, there is a question of whether resources allocated to such cyber endeavors are justified. The ongoing assessment of the effectiveness of these state-backed cyber operations will be crucial in determining their future role in modern warfare strategies.



OMER DEMBINSKY

Data Research Group Manager,
Check Point Software
Technologies

In cyber warfare, “knowing thy enemy” is riddled with greater complexity than ever before, as hacktivists commonly represent hidden interests.

Both public and private sector entities are vulnerable to hacktivist attacks, while the frequency and magnitude of the attacks depends mostly on geopolitical events.

Tokens Under Attack: The Cloud's Achilles Heel

In the wake of the COVID-19 pandemic and the subsequent transition to remote work, the distinctions between on-premise and cloud-based assets have narrowed considerably. Users need to access systems remotely, which necessitates robust authentication services for secure login. The popularity of Single Sign-On (SSO) mechanisms for third-party applications has further increased the potential exposure, as a single point of failure allows access to multiple services. To prevent or mitigate credential theft and credential stuffing, corporations have escalated their security protocols, mandating more robust authentication methods such as Multi-Factor Authentication (MFA). However, threat actors have in turn developed strategies to circumvent these enhanced security measures, primarily by exploiting stolen access tokens from already authenticated sessions. These tactics are employed by nation-state actors as well as financially motivated cybercriminals.

Contrary to the previously documented Man-in-the-Middle attacks, which typically utilize frameworks such as Evilginx to intercept communication between the victim and the service provider to compromise user credentials and tokens, the majority of these recent attacks involve recovering tokens directly from third-party or cloud service providers.

Access management and sanitization of sensitive data is challenging, especially when dealing with large amounts of data. This can lead to inadvertent access token exposure, even in professional organizations. In September 2023, an unrestricted Azure SAS token was improperly used by Microsoft to share a bucket of open-source AI training data. This led to the accidental [exposure](#) of 38 terabytes of data that included sensitive information, private keys and passwords.

Usually, attackers have to work harder to breach network systems. In a sophisticated [cyber-attack](#) discovered in July, the Chinese APT group known as Storm-0558 successfully compromised multiple email accounts belonging to at least 25 organizations, including several U.S. Federal agencies. This breach was achieved by exploiting a stolen Microsoft account (MSA) consumer signing key. This key, integral to Microsoft's security infrastructure, is used to digitally sign and authenticate tokens during the login process to consumers' Microsoft accounts. According to Microsoft's findings, the attack most likely began with the compromise of a Microsoft engineer's account, which gave the attackers access to

the engineer's debugging environment. Within this environment, the attackers located an MSA key that was inadvertently left in an unsanitized crash dump. Subsequently, this key was utilized to generate fraudulent authentication tokens for Outlook Web Access and Outlook.com, which enabled unauthorized access to multiple customer accounts. Remarkably, the compromised key dates back to April 2021.

Such attacks are not limited to cloud service providers. Managed service providers, authentication companies, and any entities that may have access tokens and related sensitive information are also targeted. In a notable incident in October 2023, Okta, a prominent part of the identity and authentication supply chain, experienced a significant security breach that [affected](#) its entire customer-support user base. The [breach](#) was initiated through stolen credentials, which enabled unauthorized access to Okta's customer support management system. This access further led to the compromise of customer-uploaded files, including HTTP Archive (HAR) files that contain critical data like cookies and session tokens. If not sanitized prior to upload, these compromised artifacts can be used to log in to or hijack system sessions. Customers later reported attempts to use their stolen artifacts to gain unauthorized access to their systems. Okta had already suffered a serious [breach](#) in 2022.

In some instances, cybercriminals exploit access to cloud-based collaboration services such as Microsoft Teams to leverage social engineering. Microsoft [reported](#) a notable example in August 2023 involving a Russian APT group known as Midnight Blizzard. This group leveraged MS Teams to circumvent Multi-Factor Authentication (MFA) procedures and acquire user tokens. Initially, Midnight Blizzard infiltrated the Microsoft 365 tenants of small businesses, establishing new domains within these tenants under the guise of technical support entities. These domains were then utilized for phishing attempts sent over Microsoft Teams in which the attackers tried to get MFA codes from users in external companies.

The attack methodology involved sending chat requests and messages through Teams, with the attackers impersonating technical support or a security team. They persuaded users to enter a specific code into their Microsoft Authenticator app. This enabled the attackers to access the users' Microsoft 365 accounts and engage in other unauthorized activities.

Cyber-attacks using stolen tokens can be conducted in a top-down approach, as seen in the attacks on Microsoft and Okta, where the compromise of service-providers allowed access to their clients' systems. Alternatively, the process can go bottom-up, starting with the breach of a customer's system. In this scenario, locating tokens and sensitive data allows the attacker to penetrate cloud services and facilitate lateral movement throughout the victim's network.

An example of such an attack was seen at a leading Israeli university. In the [reported](#) disruptive attack, actors linked to the Iranian government infiltrated a top-ranked university, the Technion – Israel Institute of Technology. The attackers gained on-premises access by exploiting unpatched vulnerabilities and eventually gained entry to a privileged account that had access to the Azure AD

agent. They then extracted plaintext credentials for a privileged Azure AD account, which enabled them to wreak havoc on the Azure environment, deleting server farms, virtual machines, storage accounts, and more.

The remote nature of cloud infrastructure management brings unique challenges in identity verification and security. Recent attack trends demonstrate that cloud security is even more vulnerable than previously thought. Advanced threat actors are increasingly bypassing end users and targeting cloud service providers directly. This worrying shift necessitates a concerted response from all involved stakeholders. Incorporating comprehensive data sanitation methods is critical for ensuring robust security in cloud environments, beyond traditional configuration management and Multi-Factor Authentication (MFA).



LOTEM FINKELSTEIN

Director, Threat Intelligence & Research
Check Point Software Technologies

As the cloud services space grows, novel security risks are emerging.

Last year's incidents underscore the challenges and the need for innovative methodologies to mitigate the latest cloud security issues.

There is a pressing need to devise robust approaches that deter threat actors from targeting both end users, as well as service providers.

PIP Install Malware: Software Repositories Under Attack

For decades, software developers have used third-party software packages and libraries to speed up development cycles. With the emergence of open-source package management platforms like PyPi, NPM, NuGet and RubyGems, it has never been easier to access a treasure trove of software packages for any need and purpose. Unfortunately, as with all popular things, threat actors find ways to abuse them for their own gain.

Malicious software packages have always been a security concern, especially in corporate environments. Over the past year, there has been a large increase in the number of malware spread through open-source package platforms, while just in the first quarter of 2023, approximately 6,800 malicious packages were [identified](#). Hundreds of thousands of users downloaded the malicious packages throughout the year. The top five malicious packages campaigns of the year alone led to 300,000 downloads and potential infections.

Python .py files now constitute 7% of the malicious files downloaded from the internet, compared to only 3% in our previous annual report. All of this happens via several common attack vectors like package name typosquatting, package brandjacking, and dependency confusion attacks. All of this emphasizes the importance of code legitimacy verification, especially for code written by unknown software developers.

During the software development process, programmers often use pre-existing packages that contain desirable functionality from code-sharing sources. This widespread practice has several advantages, including reducing the time required to write code and come up with solutions to complex problems. In most cases, pre-existing code performs efficiently and was already tested for bugs and edge cases. As a result, many open-source libraries and packages are available in every programming language.

The use of open-source libraries and packages raises several security concerns that can be exploited by threat actors. Due to the nature of open-source libraries, anyone can contribute and upload their code, making it difficult to track and verify shared code. A prime example is PyPI (Python Package Index), which is the main repository of software packages for the Python programming language. Despite recent [attempts](#) to mitigate these threats, PyPI heavily relies on user reports to ensure package security. Often, by the time they are reported and removed, the malicious packages may already have hundreds of downloads.

Most programmers do not check the integrity of open-source code before they add it to their own. It is challenging to understand the flow of code written by someone else, especially if it contains thousands of lines. In many cases, programmers are not aware of all possible security risks inherent in a piece of code, and even if they review it, they might miss malicious artifacts.

These malicious components can infect target networks, steal and exfiltrate sensitive information such as passwords and credit card information, and download additional malware components.

Creating a malicious open-source package is often straightforward and can have a significant impact. In this type of attack, the threat actor is not only targeting the developer who downloads the malicious package, but also the developer's customers who use their trusted software and thus precipitating a software supply-chain attack.

Over the years, several prominent attack vectors for open-source software package platforms were developed by threat actors and proven feasible by security researchers. The most common one is typosquatting. In this type of attack, the threat actor publishes malicious packages with slightly misspelled names or variations of popular legitimate packages, in the hope that a user will unintentionally download the malicious version. Packages are typically installed using a command such as "package_manager_name install package_name", for example, "npm install async". Therefore, a small mistake in the package name can unknowingly result in the installation of a malicious package.

In June 2023, researchers [uncovered](#) a campaign containing over 160 malicious Python packages that had over 45,000 downloads. The threat actor uploaded Python packages resembling some of the most popular packages. Among them was a malicious package called "reaquests", designed to mimic the Python package "requests" that is widely used for HTTP request operations by millions of users.

Not just Python libraries but all repositories that use open-source code sharing are targeted. The NuGet repository, an open-source package manager and software distribution system for .NET libraries, was used to [launch](#) a significant typosquatting campaign. The fraudulent packages were downloaded over 150,000 times in a single month before they were removed from the NuGet repository. The malicious packages contained a PowerShell script that was executed upon installation and triggered a download of a second-stage payload. The final payload was a custom crypto stealer called “Impala Stealer” which steals user credentials for cryptocurrency exchange platforms.

Cybercriminals don’t just exploit typos to deliver malicious packages. In package brandjacking, the threat actor creates malicious packages with the same names as the legitimate ones in the hopes of fooling users into downloading them.

In a recent attack against Mac computers, threat actors [created](#) a malicious version of the crypto library Cobo Custody Restful to deploy malware. The malicious version had the same name as the legitimate one and was stored in the PyPI registry. The threat actors took advantage of the fact that this package does not have an official distribution through the PyPI registry and is distributed only via GitHub. If the installation destination is not explicitly specified, the pip install manager prioritizes the malicious PyPI version over the legitimate GitHub version.

It’s not only package management platforms that are exploited. Threat actors try to subjugate existing legitimate accounts that host open-source code, such as GitHub, to add malicious code to legitimate packages. This method was demonstrated by researchers who [took over](#) a popular NPM package with more than 3.5 million weekly downloads by acquiring an expired domain name associated with one of the package maintainers. The recovered domain allowed them to reset the GitHub password, making it possible to publish Trojanized versions of the NPM packages.

In contrast with package brandjacking, dependency confusion attacks trick the package manager instead of the user. The threat actor exploits a vulnerability in the way that many package managers download dependencies during a software build process. The attacker publishes a package with the same name as a popular package on a public repository, whereas the original one is located in a private repository. This tricks the software installer script into pulling malicious code files. A research report from April 2023 [states](#) that 49% of all organizations are vulnerable to this attack vector.

Earlier this year, security researchers [discovered](#) that PyTorch, a widely-used machine-learning framework developed by Meta Platforms, had been compromised. The attack was initiated when a threat actor uploaded a malicious package to the

PyPI repository with the same name and a higher version number than the legitimate package, causing dependency confusion. This attack affected thousands of machines and resulted in information theft.

Malicious open-source packages are used by both prolific threat actors and nation-sponsored actors. The following attack was [attributed](#) to the infamous North Korean group Lazarus. In August 2023, the group uploaded several malicious packages to the PyPI repository. They camouflaged one of the packages as a VMware vSphere connector module named “vConnector”. Another package mimicked “prettytable”, a popular Python tool for printing tables in an attractive ASCII format. The legitimate package “prettytable” has more than 9 million monthly downloads, while the malicious version “tablediter” received 736 downloads.

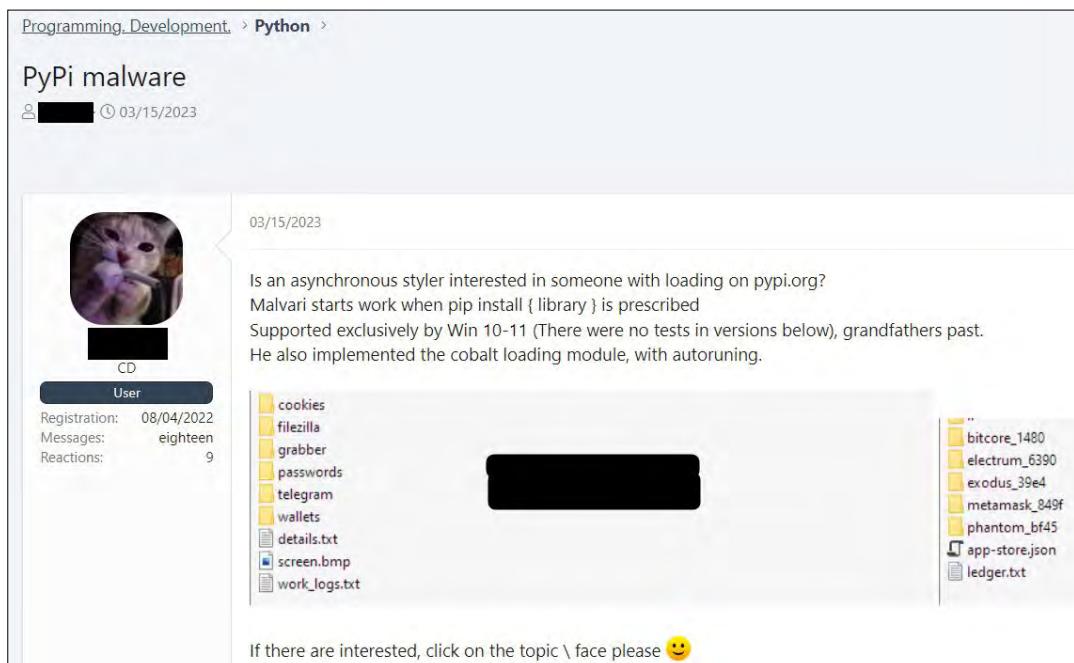


Figure 2: PyPI malware being distributed on an underground forum.

In addition, on Russian-language underground forums, Check Point researchers have observed the distribution of malware tailored for the PyPi registry. This allows attackers to launch malicious attacks easily, without prior warning.

The spread of malicious packages in open-source software repositories is a growing concern that requires heightened attention and proactive measures from both developers and users. While the benefits of open-source

software are undeniable, the rising wave of attacks such as typosquatting, brandjacking, and dependency confusion reveals the limitations of these platforms. The ease of exploiting package management platforms like PyPi, NPM, and NuGet underscores the critical need for enhanced security protocols and thorough code review practices. Developers must prioritize security to protect end-users from the consequences of these malicious infiltrations.



ORI ABRAMOVSKY

Head Of Data Science,
Check Point Software
Technologies

“Software repositories, like PyPi and NPM, face a surge in malicious attacks, with 6,800 identified in Q1 2023 alone.”

Threats include typosquatting, brandjacking, and dependency confusion, emphasizing the need for enhanced security and code review practices to safeguard users.



GLOBAL ANALYSIS

CYBER ATTACK CATEGORIES BY REGION

GLOBAL

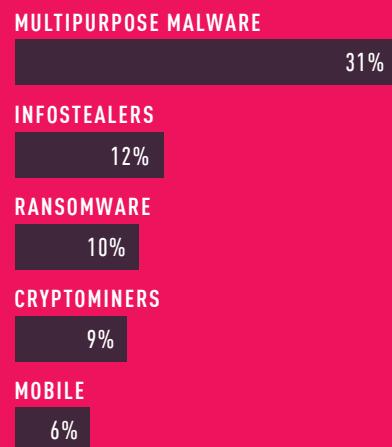


Figure 3: Percentage of organizations affected by malware type globally in 2023.

AMERICAS

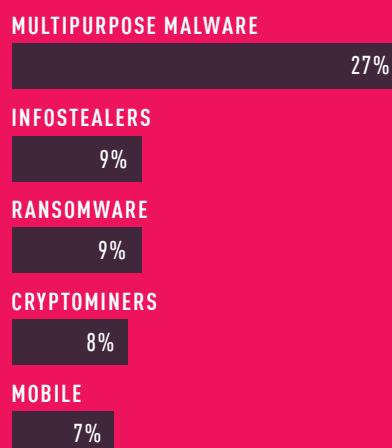


Figure 4: Percentage of organizations affected by malware type in the Americas in 2023.

CYBER ATTACK CATEGORIES BY REGION

EMEA



MULTIPURPOSE MALWARE

32%

INFOSTEALERS

12%

RANSOMWARE

10%

CRYPTOMINERS

8%

MOBILE

5%

Figure 5: Percentage of organizations affected by malware type in EMEA in 2023.

APAC



MULTIPURPOSE MALWARE

35%

INFOSTEALERS

15%

CRYPTOMINERS

13%

RANSOMWARE

11%

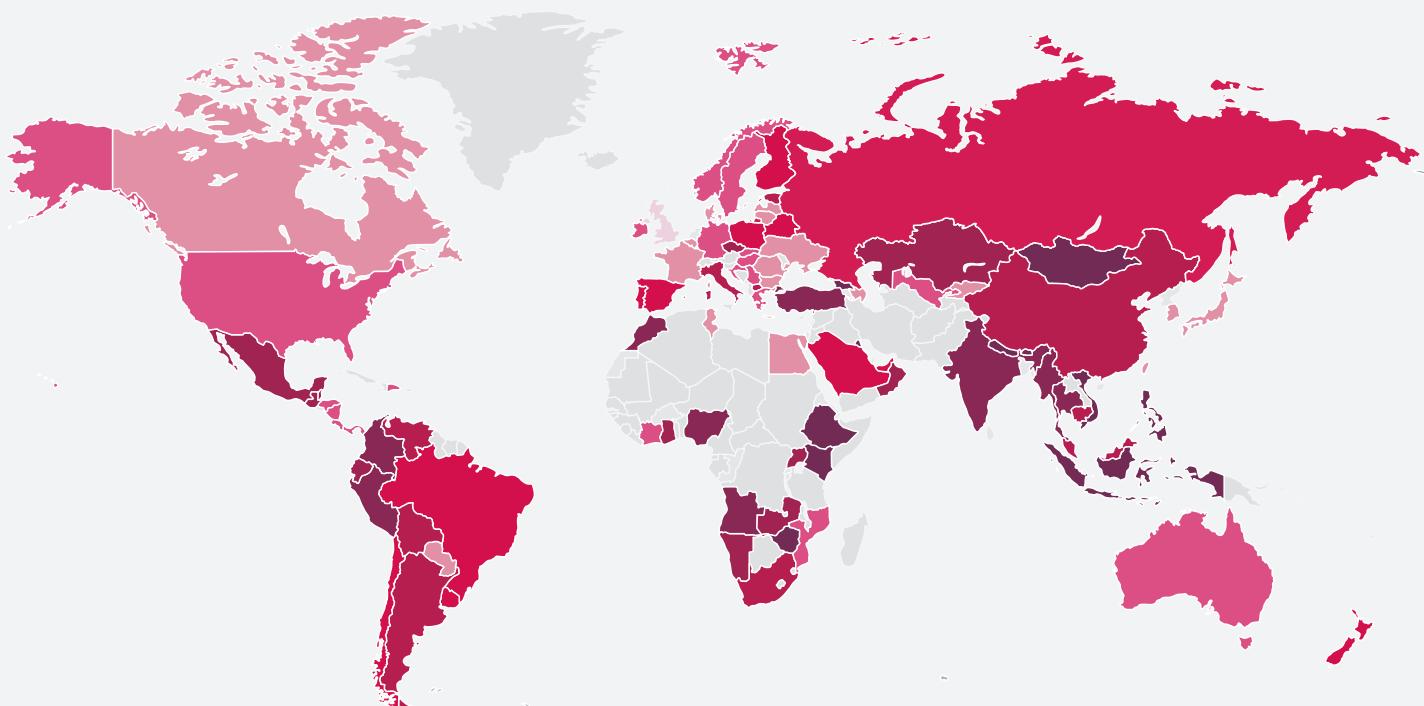
MOBILE

8%

Figure 6: Percentage of organizations affected by malware type in APAC in 2023.

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

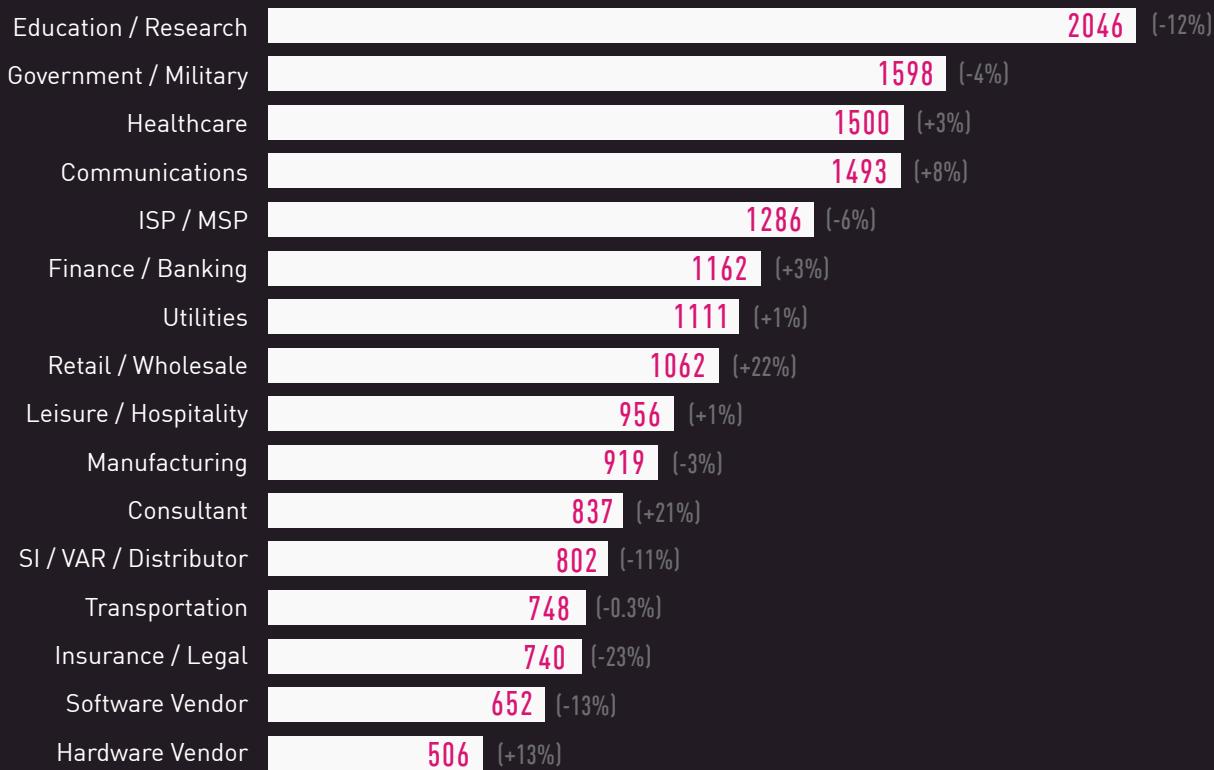


Figure 8: Global Average of weekly attacks per organization by Industry in 2023 [% of change from 2022].

The education, government, and healthcare sectors continue to be prime targets for cyber-attacks. Enhanced awareness and a large number of impactful attacks during the last few years have led to the launch of significant improvements in education sector security protocols, which may have contributed to a small, recent decrease in the number of attacks against this sector. However, the average educational institution is still hit with over 2,000 attack attempts weekly. Some attacks have been part of larger campaigns, such as those involving Johns Hopkins University and the University System of Georgia, which were [compromised](#) by the CL0P ransomware through the MOVEit managed file transfer software.

Schools are particularly vulnerable to cyber-attacks due to the vast amounts of sensitive personal information they have in their systems and lower levels of investment in cybersecurity. The private sector—including retail, wholesale manufacturing, and financial institutions—is more likely to acquiesce to ransom demands than public sector groups, and has seen an increase in targeting over the previous year. Access to these institutions is often traded in underground markets.



Figure 9: Postings in an underground forum selling access to retail companies.

In 2023, the cybersecurity landscape experienced a worrying surge in ransomware attacks across various sectors. Ransomware attacks now account for 10% of all malware types detected by Check Point sensors. This trend is further underscored by CPIRT (Check Point Incident Response Team) data and victim postings on ransomware “shame sites.” According to CPIRT data, nearly half of all the incidents they handled involved ransomware and the reported number of ransomware victims has reached nearly 5,000 victims, a marked increase from the 2,600 reported in 2022.

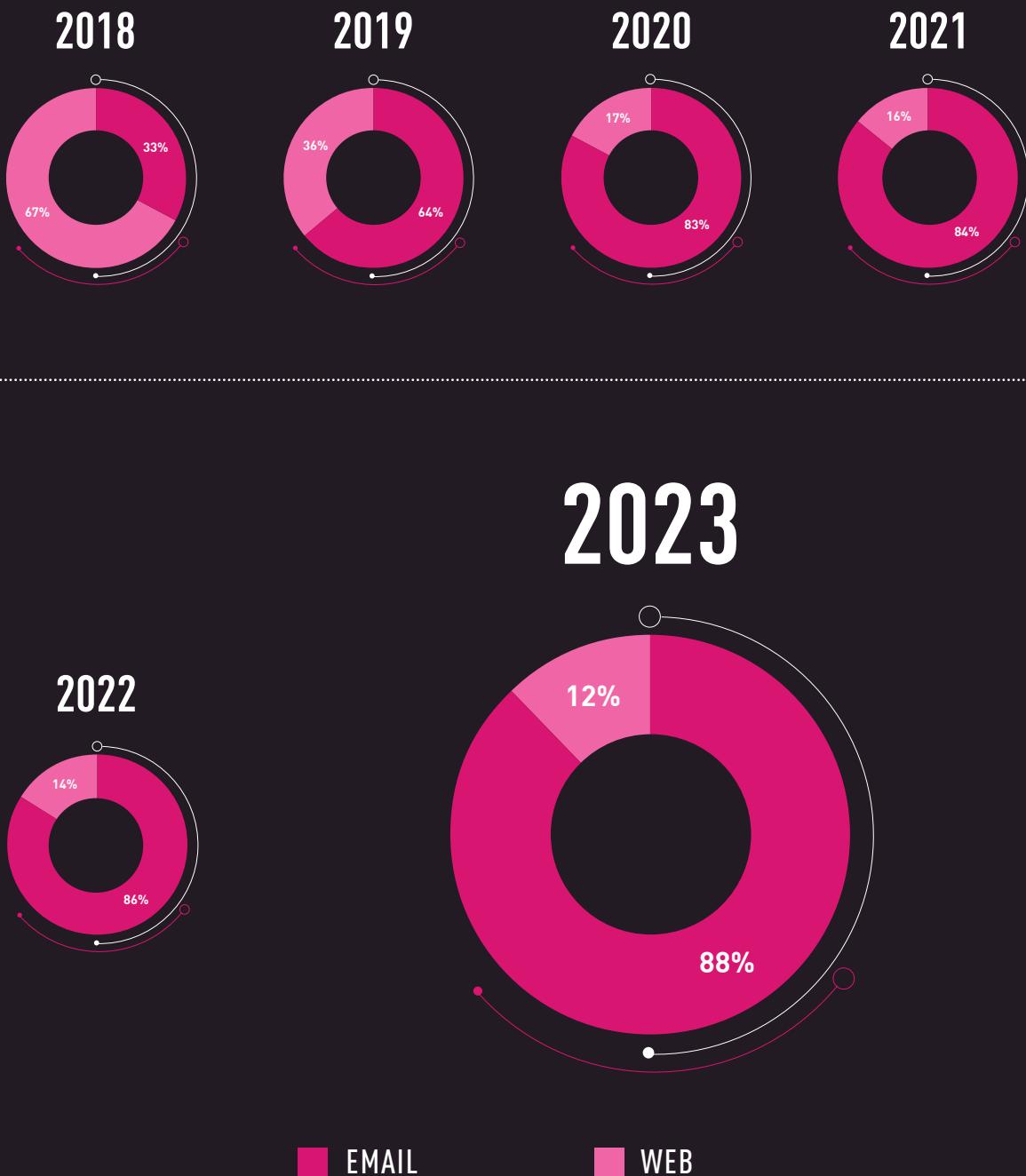


Figure 10: Delivery Protocols—Email vs. Web Attack Vectors in 2018-2023.

TOP MALICIOUS FILE TYPES—WEB VS. EMAIL

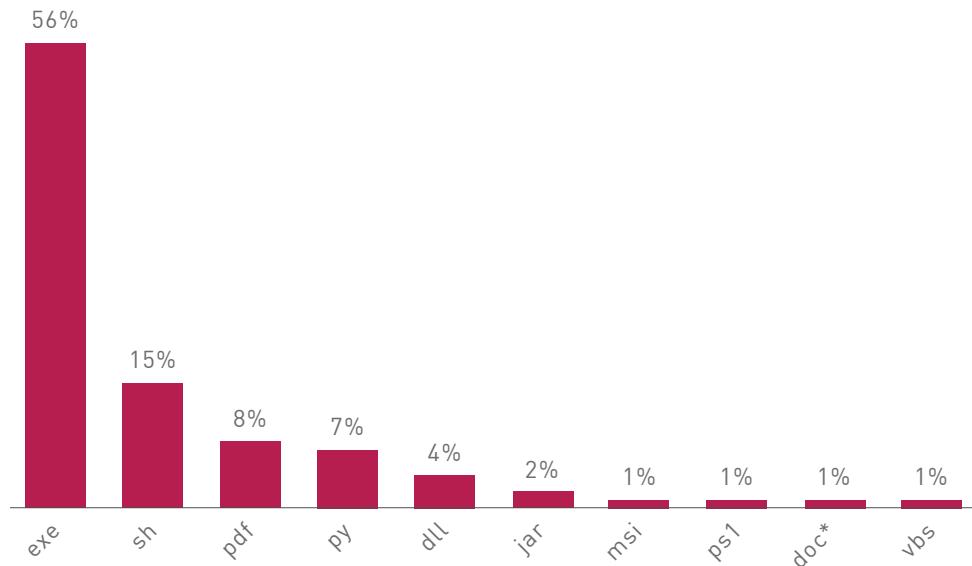


Figure 11: Web—Top malicious file types in 2023.

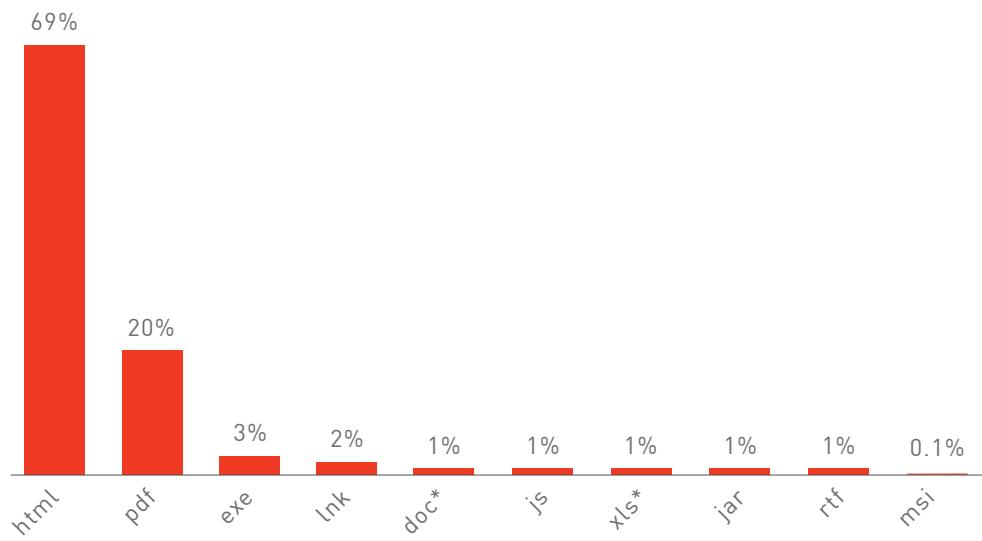


Figure 12: Email—Top malicious file types in 2023.

xls* includes common Office Excel files such as .xls, .xlsx, .xlsm

doc* includes common Office Word files such as .doc, .docx, docm, and .dot

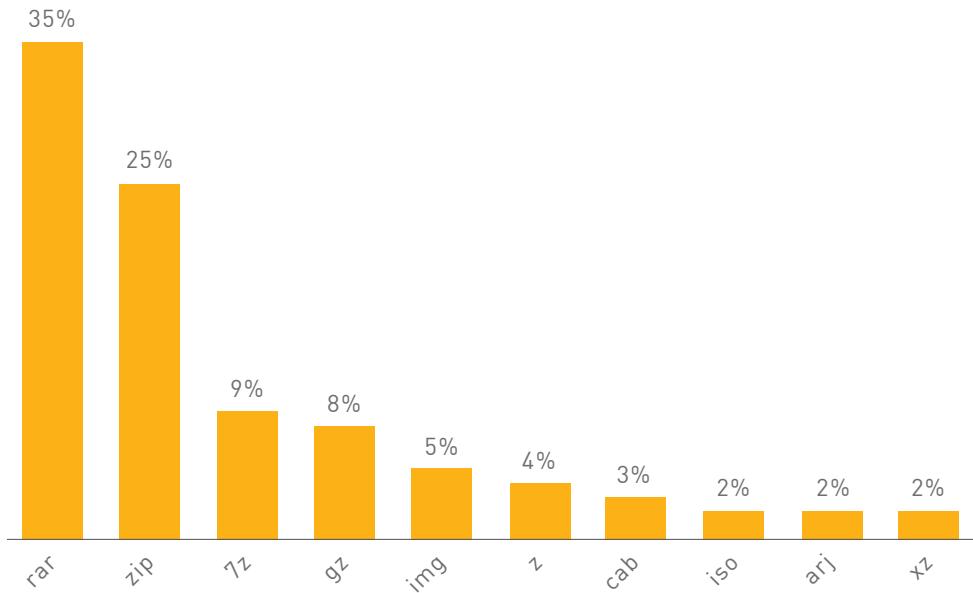


Figure 13: Email-delivered malicious archive file types in 2023.

Email-based attacks continue to be the dominant initial infection vector. Eighty-eight percent of all malicious file deliveries occur through email, with the remainder downloaded directly from the internet. Threat actors have adapted to email protection strategies and are exploring innovative delivery techniques. Following Microsoft's [restrictions](#) on Office VBA macros in files from external sources denoted with the Mark-of-the-Web (MotW), there was a sharp decrease in the prevalence of malicious Office files, from nearly 50% in 2022 to 2% in 2023. Notable alternative attack vectors include HTML files and various archive file types. In particular, the exploitation of HTML files saw a significant uptick. HTML files comprise 69% of all malicious file attachments.

Threat actors use HTML files in several ways. They are used in phishing schemes to imitate legitimate website login pages and steal user credentials. They can include malicious JavaScripts or exploits to unpatched browser and browser-plugins. As demonstrated in recent CP<R> [research](#), these tactics are not limited to low-level criminals but are also utilized by advanced APT actors. Other uses of HTML include [HTML smuggling](#), or auto download for executables and redirections to other malicious URLs. Legitimate use cases of email-delivered HTML are unusual and therefore organizations should consider implementing restrictions.

Utilization of various archive files has also been on the rise. The contents of password-[protected](#) archives are hidden from many security services, thus forming an effective attack vector. Other formats like .img and .iso depend on the software used for their extraction to propagate the MotW functionality, which is used to prevent malicious attempts. While Microsoft has [fixed](#) this feature, other providers like 7-zip have [opt-in policies](#), thus decreasing the effectiveness of the MotW protection mechanism.

The increased detection of malicious .py files, ranking fourth in the list of the most common web-delivered malicious file types, indicates a rising use of malicious code packages. This trend is explored in detail in a separate section. The continued decrease in the use of executables as malicious email attachments, which dropped from 26% in 2022 to just 3% in the past year, can be attributed to restrictive corporate policies, the integration of security mechanisms by popular email service providers, such as Google and Microsoft, and enhanced user awareness.

GLOBAL MALWARE STATISTICS

Data comparisons presented in the following sections are based on data drawn from the [Check Point Threat Cloud](#) between January and December 2023.

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

Top Malware Families

■ GLOBAL

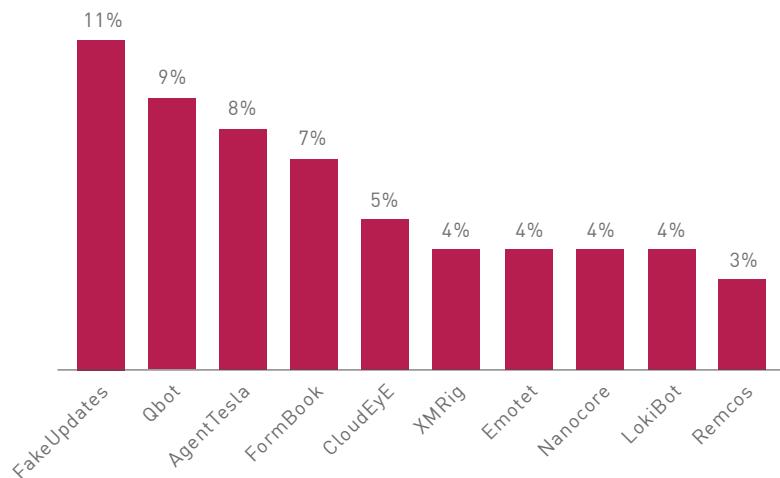


Figure 14: Most prevalent malware globally—2023

■ AMERICAS

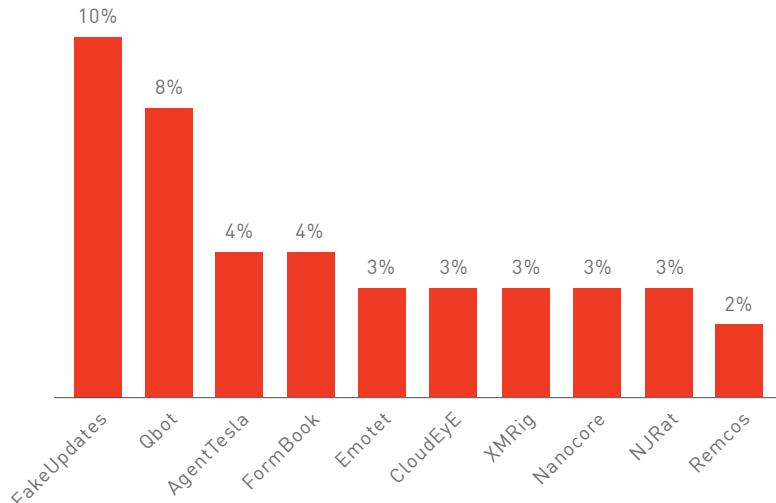


Figure 15: Most prevalent malware in the Americas—2023

■ EUROPE, MIDDLE EAST AND AFRICA (EMEA)

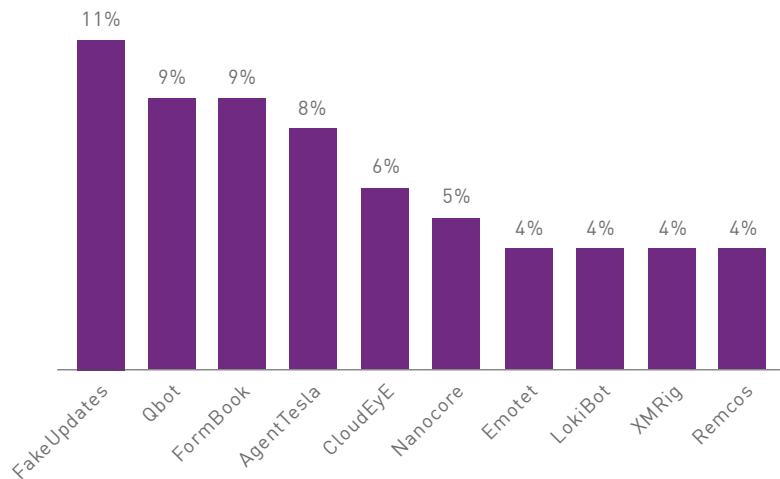


Figure 16: Most prevalent malware in EMEA—2023

■ ASIA PACIFIC (APAC)

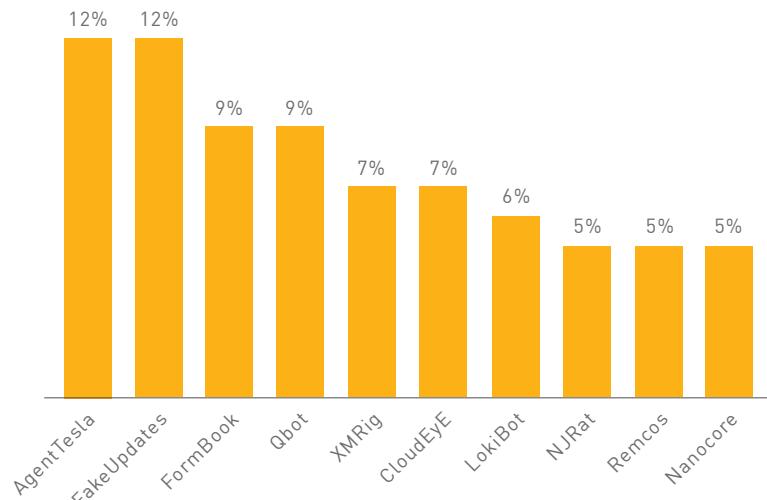


Figure 17: Most prevalent malware in APAC—2023

GLOBAL ANALYSIS OF TOP MALWARE

At the top of Check Point's list for the most prevalent malware globally in 2023 is a scheme called FakeUpdates. Also known as SocGholish, it relies on a network of compromised websites to redirect users to fake software and browser updates. In turn, these fake updates trick users into downloading and executing a JavaScript downloader that acts as the initial access point, [enabling](#) further compromise through other malware such as GootLoader, NetSupport and DoppelPaymer. The network of compromised websites is linked to [TA569](#), a prolific threat actor who serves as an Initial Access Broker (IAB).

TA569 is suspected of selling initial access to malware victims in a pay-per-install (PPI) pricing model to other cybercriminals who can then leverage compromised systems to deploy ransomware. The infection chain begins when a victim visits a compromised website, whether they were lured there by a phishing email or they access it directly. On the website itself, the victim may encounter a fake browser update request, or fake Captcha puzzles, and security software updates, then leading to malware infection.

Qbot, also known as QakBot or PinkslipBot, ranks second on our list. Qbot is a Windows malware that was first discovered in 2008 as a banking Trojan. Through many updates and [evolutions](#), it has become one of the most well-known and longest-prevailing malware droppers out there. In fact, Qbot has caused so much damage in terms of data theft and extortion, that in August 2023 the FBI and the Department of Justice [launched](#) an international campaign to dismantle the botnet, remove it from infected servers and seize over \$8 million in illicit profits. In December, Qbot was [observed](#) in new phishing campaigns.

Emotet has long persisted on Check Point's most prevalent malware list. Despite its diluted operational mode, it affected 4% of corporate networks globally, mostly in the first quarter of the year. Emotet was [taken down](#) in a Europol-led global effort in November 2021, but made a measured comeback in 2022, orchestrated by the cybercrime group Mealybug (AKA TA542) through multiple spam campaigns alternating with prolonged periods of silence.

After Microsoft restricted the exploitation of VBA macros in downloaded documents (the principal method used in Emotet's campaign), Mealybug went on to explore alternative infection methods. In 2023, Mealybug was [observed](#) trying out different techniques, and in March began using VBScript-embedded OneNote files in their campaigns. Upon downloading the file, the victims were lured to click the 'View' button to see the document contents, which would then download the Emotet DLL. This campaign was planned to coincide with tax season deadlines in the United States.

TOP MULTIPURPOSE MALWARE

GLOBAL

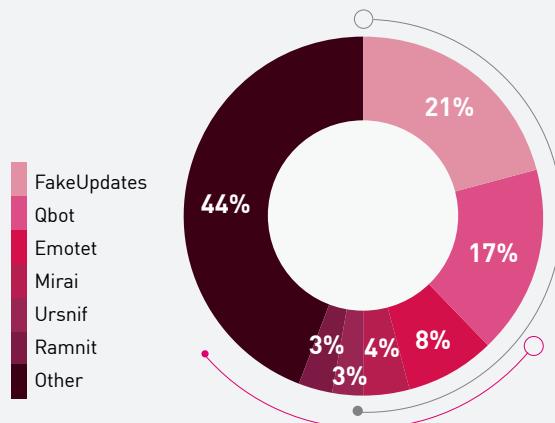


Figure 18: Most prevalent multipurpose malware globally—2023

AMERICAS

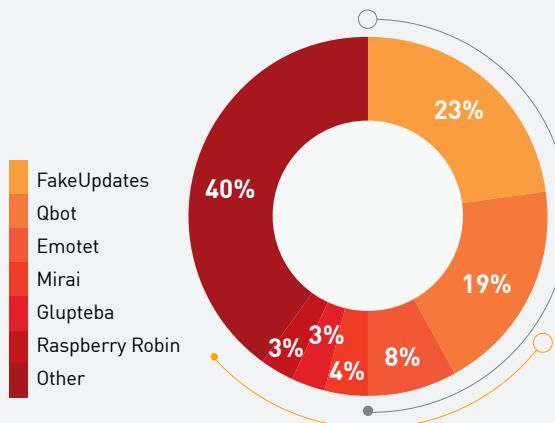


Figure 19: Most prevalent multipurpose malware in the Americas—2023

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

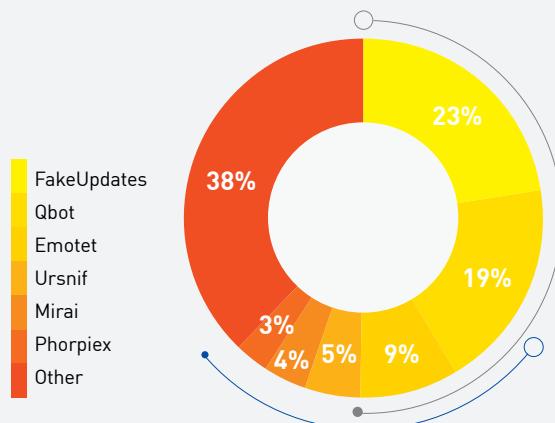


Figure 20: Most prevalent multipurpose malware in EMEA—2023

ASIA PACIFIC (APAC)

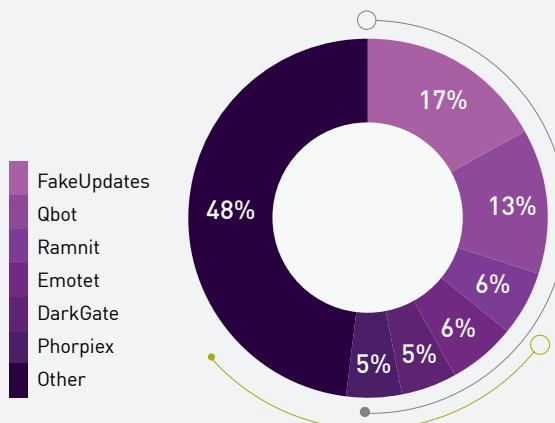


Figure 21: Most prevalent multipurpose malware in APAC—2023

MULTIPURPOSE MALWARE GLOBAL ANALYSIS

As in our previous report, we have merged two malware categories, banking Trojans and botnets and introduced instead a new unified category called 'multipurpose malware'. This change reflects the evolution of many banking Trojans, which have acquired additional functionalities.

In addition to FakeUpdates, Qbot, and Emotet, which were discussed in the [previous section](#), DarkGate, a Windows RAT developed in Delphi, has also risen in popularity and is especially prominent in campaigns targeting entities in the APAC region. In the latter half of 2023, [DarkGate](#) gained significant notoriety for its ability to evade security system detection. In contrast to Emotet and Qbot, which run their own infection campaigns and subsequently sell access and infections, DarkGate employed a more [direct](#) sales strategy in a Malware-as-a-Service (MaaS) model. It was directly advertised on underground forums to a select group of customers, highlighting its new capabilities and limited availability. Conducted by a broad range of actors, campaigns delivering DarkGate utilize numerous techniques, including [phishing](#) and [Teams](#) messages.

CURRENT PRICES

Payments only in crypto (BTC, ETH, MONERO, ETC..)
 1 DAY PACKAGE -> 1000\$ (YOU CAN BUY THIS PACKAGE ONLY 1 TIME WITH EACH ██████████ ACCOUNT)
 MONTHLY - 15,000\$
 1 YEAR UPDATED -> 100,000\$

MAIN FEATURES ->

DOWNLOAD & EXECUTE ANY FILE DIRECTLY TO MEMORY (native,.net x86 and x64 files)
 HVNC
 HANYDESK
 REMOTE DESKTOP
 FILE MANAGER
 REVERSE PROXY
 ADVANCED BROWSERS PASSWORD RECOVERY (SUPPORTING ALL BROWSER AND ALL PROFILES)
 KEYLOGGER WITH ADVANCED PANEL
 PRIVILEGE ESCALATION (NORMAL TO ADMIN / ADMIN TO SYSTEM)
 WINDOWS DEFENDER EXCLUSION (IT WILL ADD C:/ FOLDER TO EXCLUSIONS)
 DISCORD TOKEN STEALER
 ADVANCED COOKIES STEALER + SPECIAL BROWSER EXTENSION THAT I BUILD FOR LOADING COOKIES DIRECTLY INTO A BROWSER PROFILE
 BROWSER HISTORY STEALER
 ADVANCED MANUAL INJECTION PANEL
 CHANGE DOMAINS AT ANY TIME FROM ALL BOTS (Global extension)
 CHANGE MINER DOMAIN AT ANY TIME FROM ALL BOTS (Global extension)
 REALTIME NOTIFICATION WATCHDOG (Global extension)
 ADVANCED CRYPTO MINER SUPPORTING CPU AND MULTIPLE GPU COINS (Global extension)
 ROOTKIT WITHOUT NEED OF ADMINISTRATOR RIGHTS OR .SYS FILES (COMPLETELY HIDE FROM TASKMANAGER)
 INVISIBLE STARTUP, IMPOSSIBLE TO SEE THE STARTUP ENTRY EVEN WITH ADVANCED TOOLS

Figure 22: DarkGate pricing and offering on an underground forum during 2023.

TOP INFOSTEALER MALWARE

■ GLOBAL

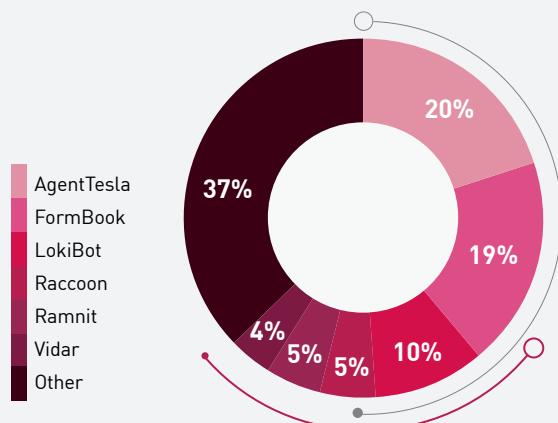


Figure 23: Top infostealer malware globally—2023

■ AMERICAS

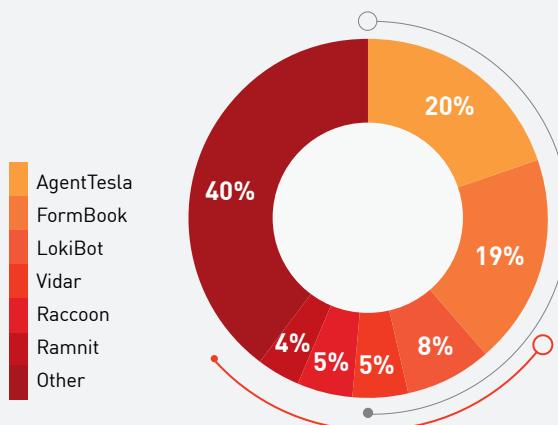


Figure 24: Top infostealer malware in the Americas—2023

■ EUROPE, MIDDLE EAST AND AFRICA (EMEA)

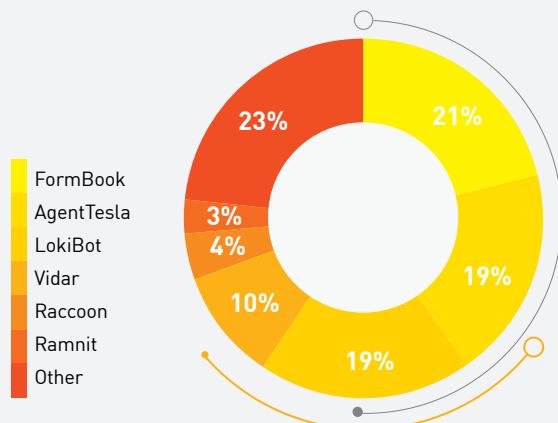


Figure 25: Top infostealer malware in EMEA—2023

■ ASIA PACIFIC (APAC)

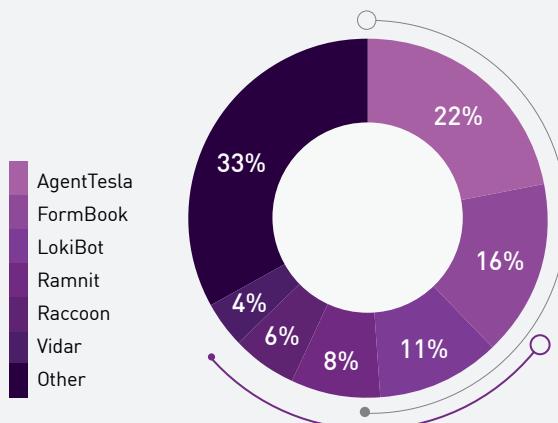


Figure 26: Top infostealer malware in APAC—2023

INFOSTEALER MALWARE GLOBAL ANALYSIS

The infostealer malware market operates mainly in a Malware-as-a-Service (MaaS) model, involving several key players. At the heart of this ecosystem are MaaS providers, who focus on developing and maintaining both the malware and its operational infrastructure. Infostealer operators, who either rent or purchase the malware, deploy them in cyber-attack campaigns against victim platforms. Underground marketplaces are crucial for trading the data harvested from these campaigns.

In the past year, this ecosystem has seen only minimal changes, with malware such as AgentTesla, FormBook, and LokiBot remaining prevalent. The accessibility of these infostealers is evident in their pricing on underground forums, where they are offered for monthly subscriptions ranging from \$60 to \$1,000 USD. This tiered pricing structure accommodates a wide spectrum of threat actors, from novices to seasoned hackers. In addition, there are the Initial Access Brokers, who utilize the purchased data to breach networks, often leading to extensive exploitation by ransomware.

AgentTesla, first identified in 2014, is a MaaS with keylogging capabilities and is one of the infostealers commonly detected by CP<R>. Its [current](#) version has been enhanced to steal credentials from multiple applications, including web browsers, VPN software, FTP services, and email clients. Beyond credential theft, AgentTesla has functionalities for collecting system information, disabling anti-malware processes, and capturing clipboard contents. AgentTesla is adept at extracting credentials from system registries and configuration files, and it transmits this stolen data to its command and control (C&C) server. Notably, this malware is marketed on underground forums through low-cost subscription models, making it accessible to cybercriminals with limited technical expertise.

TOP CRYPTOMINING MALWARE

■ GLOBAL

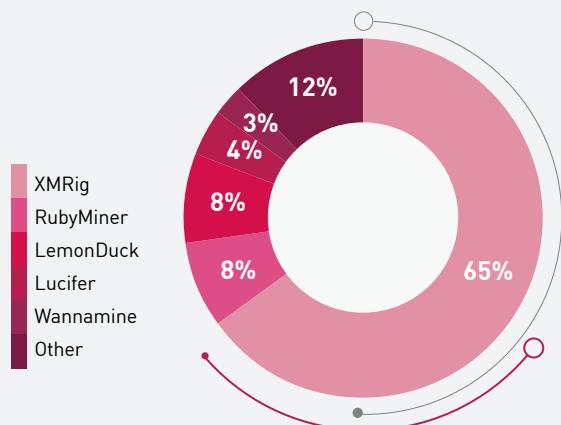


Figure 27: Top cryptomining malware globally—2023

■ AMERICAS

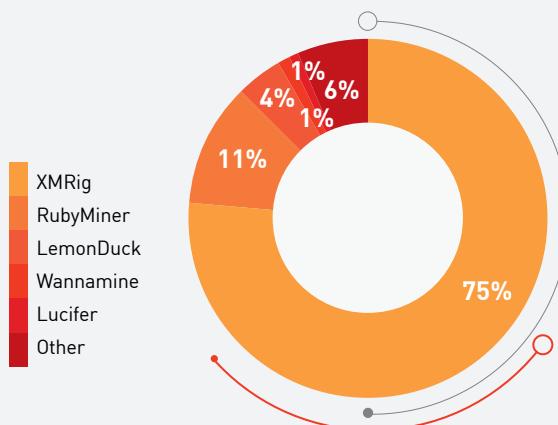


Figure 28: Top cryptomining malware in the Americas—2023

■ EUROPE, MIDDLE EAST AND AFRICA (EMEA)

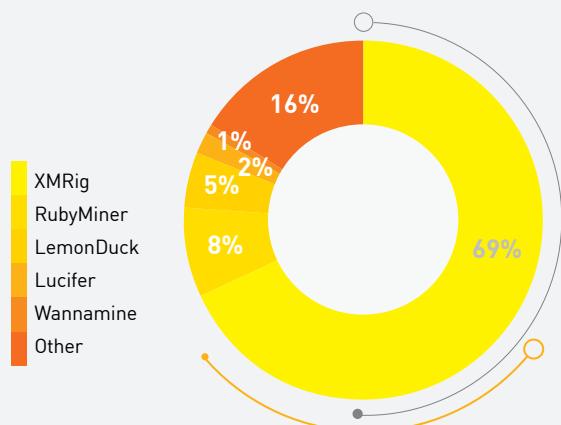


Figure 29: Top cryptomining malware in EMEA—2023

■ ASIA PACIFIC (APAC)

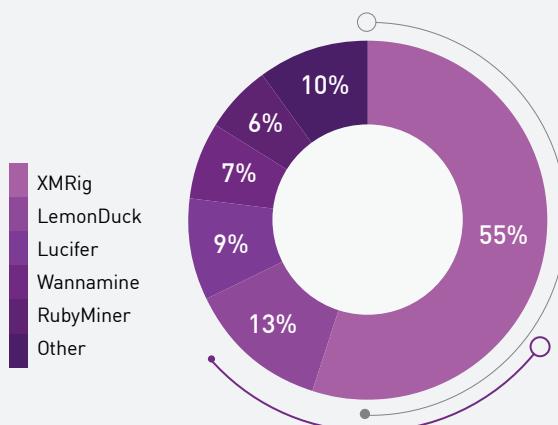


Figure 30: Top cryptomining malware in APAC—2023

CRYPTOMINERS GLOBAL ANALYSIS

Illegal cryptomining saw a decrease in 2023 due to Bitcoin rates not rebounding to their 2021 peak and the continued [increase](#) in mining difficulty. Only 9% of global corporate entities were affected by cryptominers in 2023, compared to 16% in 2022. With the increase in GPU (Graphics Processing Unit) prices, some threat actors are now specifically [targeting](#) graphic designers and engineering platforms for their enhanced GPU capabilities as miners. Monero remains [profitable](#) for mining, and its common open-source mining tool, XMRig, was used in 65% of cryptomining attacks in 2023. Cryptominers are integrating additional malicious functionalities, transforming some of them, like [LemonDuck](#), into multifaceted threats that span beyond their core function of mining cryptocurrency. In some instances, as with the [StripedFly](#) malware, cryptomining activities might just be a cover for more complex espionage operations.

Cloud infrastructure continues to be a target for cryptomining exploitation. In October, researchers [reported](#) a years-long operation that exploited poorly secured IAM keys to access cloud environments for deploying Monero miners. Often, the same access that allows threat actors to install a cryptominer is later used for additional exploitation and breaches. This makes the presence of cryptominers a potential precursor to broader security issues.

TOP MOBILE MALWARE

■ GLOBAL

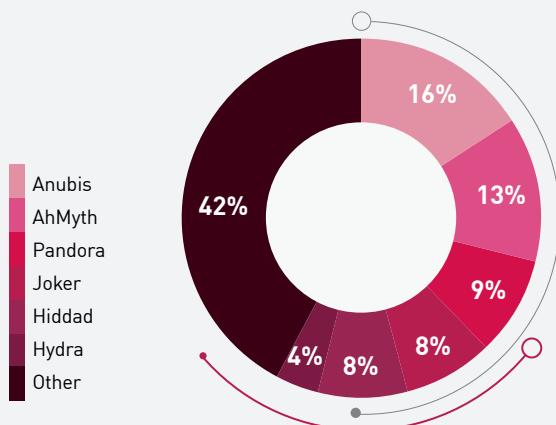


Figure 31: Top mobile malware globally—2023.

■ AMERICAS

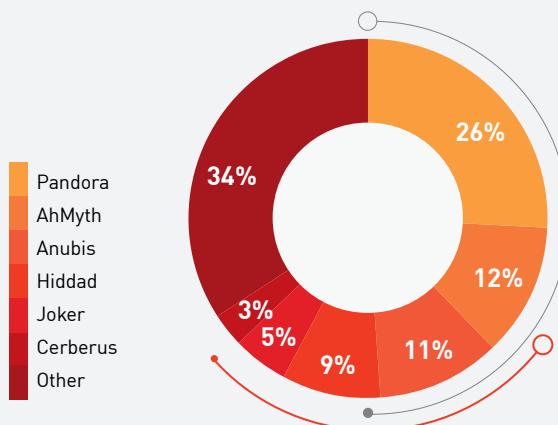


Figure 32: Top mobile malware in the Americas—2023.

■ EUROPE, MIDDLE EAST AND AFRICA (EMEA)

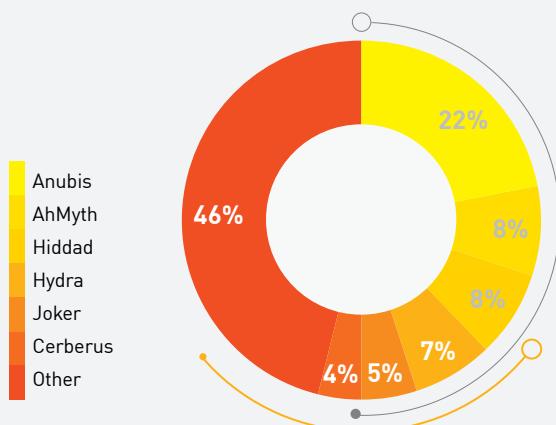


Figure 33: Top mobile malware in the EMEA—2023.

■ ASIA PACIFIC (APAC)

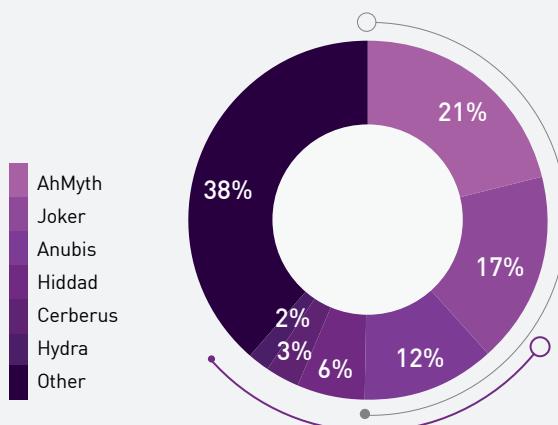


Figure 34: Top mobile malware in the APAC—2023.

MOBILE MALWARE GLOBAL ANALYSIS

Mobile devices are prime targets for cyberattacks, largely due to their central role in our daily lives and the wealth of valuable data that they contain. These devices not only store personal and financial information but may also serve as potent surveillance tools, given their capabilities to track location, record audio, and capture images.

The AhMyth Android Remote Access Trojan (RAT) is an open-source malware freely available on [GitHub](#) that is often used as basis for attack campaigns. Not surprisingly, it occupies a significant position on the Check Point top mobile malware charts. A variant of the malware, AhRat, was [found](#) in a weaponized app called 'iRecorder—Screen Recorder' available in the Google Play Store with over 50,000 downloads.

A “clean” version of the application has been available for Android users since 2021, and the malicious characteristics were only added later. In addition to iRecorder’s self-explanatory screen-grabbing feature, its malicious update includes sound recording and data exfiltration capabilities, including retrieval of saved web pages, images, audio, video, document, and archive formats. The spyware functionalities may suggest a cyber-espionage campaign, which is not uncommon in the mobile malware world. For example, there is the [Kamran](#) Android malware which is specifically designed to target Urdu-speaking victims in Pakistan, or the Chinese-aligned APT operated [BadBazaar](#) Android spyware.

As always, these types of malware are also often exploited for financial gain by cyber criminals. For example, the newly emerged [Chameleon](#) Android banking Trojan targets Australian and European users’ mobile banking and cryptocurrency applications. A similar [campaign](#) was observed in India, where malicious apps impersonating banks and government services were distributed via social media platforms. Ransomware was also given a new spin within the Android ecosystem: [SpyLoan](#) applications were spread through Google Play Store to over 12 million users in Asia, Africa and South America. The malware collected victims’ personal and financial data from their mobile devices, which it used to harass and blackmail them to extort funds.

RANSOMWARE

This section features information derived from almost 200 ransomware "shame sites" operated by double-extortion ransomware groups, 68 of which posted the names and information of victims from 2023. Cybercriminals use these sites to amplify pressure on victims who do not pay the ransom immediately. The data from these shame sites carries its own biases but still provides valuable insights into the ransomware ecosystem, which is currently the number one risk to businesses. The data presented below was collected for the period between January and December 2023.

In 2023, a total of 68 active ransomware groups reported they had breached the systems of and publicly extorted over 5,000 victims. This marks a substantial increase over past years. The ransomware events only intensified as 2023 went on. H2 recorded more than 2,800 victims compared to 2,200 in the first half of the year. Lockbit emerged as the most active during this period, responsible for 21% of the reported incidents with over 1,050 cases. Typically, threat actors grant victims a one-to-two-week grace period to meet the ransom demands. Victims who pay the ransom are not publicly exposed, which suggests that the actual number of victims could be significantly higher.

TOP DOUBLE-EXTORTION RANSOMWARE ACTORS

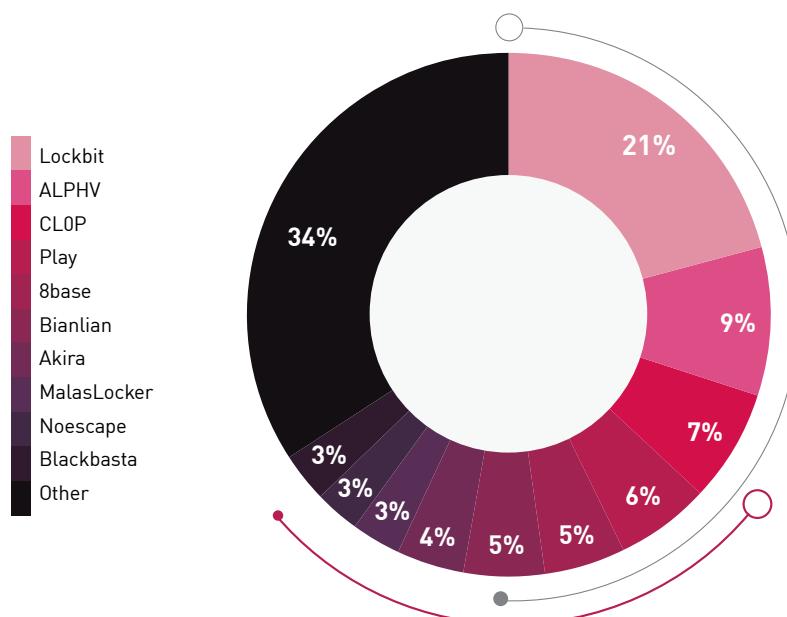


Figure 35: Most active ransomware actors by number of victims, as reported on shame sites in 2023.

ALPHV, also known as BlackCat, targeted over 440 victims in 2023 and was the focus of a law enforcement [operation](#). In December, a US-led operation resulted in the takedown of the group's websites and the release of a decryption tool. [According](#) to CISA, since the beginning of its operations, the group compromised more than 1,000 victims and received ransom payments totaling nearly \$300 million. The group has since resumed its criminal operation and its [presence](#) on the Dark Web.

CL0P's activity is underrepresented in this count. In early June, CL0P exploited a zero-day vulnerability that allowed it to gain access to the [MOVEit](#) file-transfer software, leading to the compromise of over [2,600](#) organizations. Most of the victims' identities were not disclosed on its shame site and therefore not included in the above count. CL0P also utilized alternative methods to further extort its victims. CL0P's use of zero-day exploits this year also included an attack on [GoAnywhere](#), which is detailed in another [section](#) of this report.

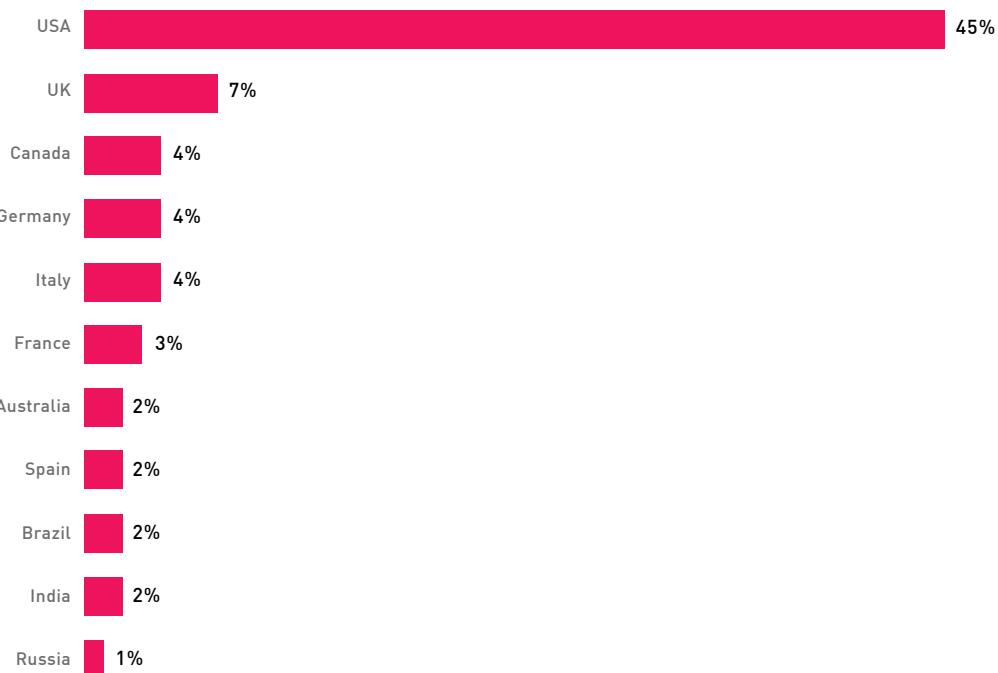


Figure 36: Victims by country, as reported on shame sites—2023.

In terms of geographical distribution, 45% of the affected companies are situated in the United States, followed by the United Kingdom at 7%, and Canada, Germany, and Italy each at 4%. The presence of Russian victims on the chart above in 2023 can be attributed primarily to two actors: [MalasLocker](#) and [Werewolves](#). Cyberattacks on entities from the former Soviet Union remain relatively infrequent. MalasLocker, active in the first part of 2023, adopted an unconventional approach by replacing traditional ransomware demands with requests for charitable donations.

When analyzing the industry sectors affected by ransomware attacks, data from the Check Point Threat Cloud highlights the education, government, and healthcare sectors as the primary targets. However, the ransomware victim

landscape offers a different view. Manufacturing and retail sectors exhibit the highest number of victims, while government and education entities are positioned lower in the target hierarchy. In December 2023 alone, prominent companies like Coca-Cola Singapore (DragonForce), Nissan Motor Australia (Akira), Kraft Heinz (Snatch), Xerox (Inc ransom) were all claimed as victims by double-extortion ransomware groups.

The aforementioned discrepancy likely arises from differences in the willingness of these sectors to comply with ransom demands, with educational and governmental organizations being less inclined to make payments. These sectors are primarily targeted for the exploitation of their data, including personal and technical information, rather than for extortion-based attacks.

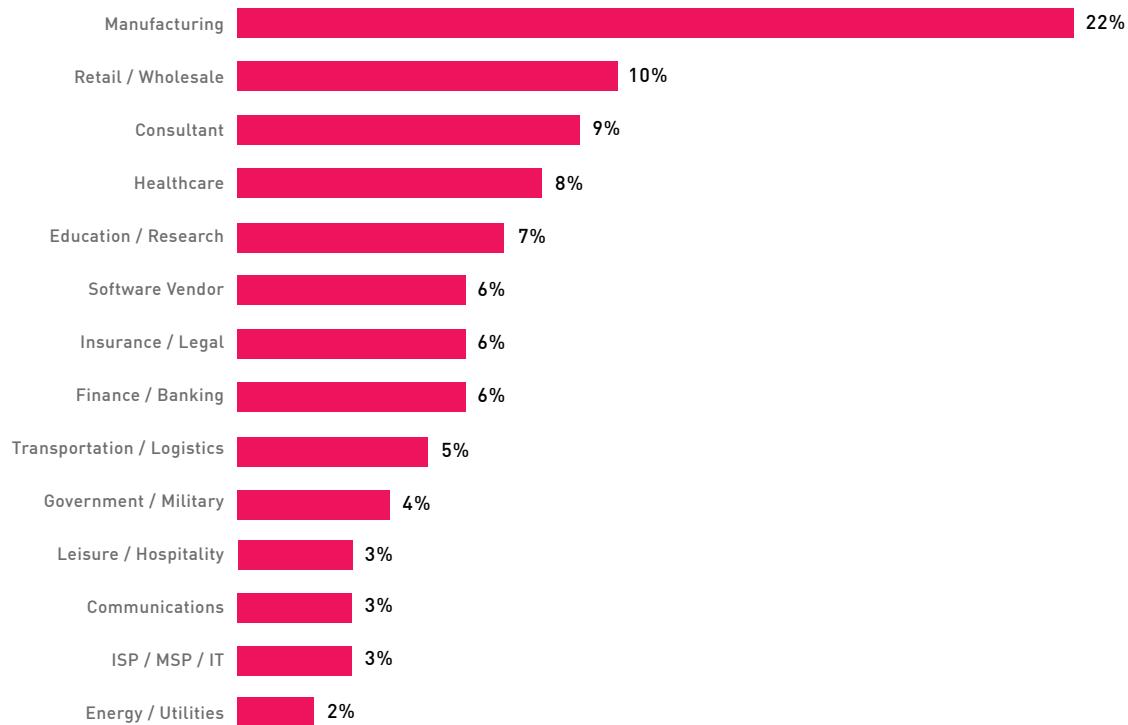


Figure 37: Industry distribution of ransomware victims, as reported on shame sites—2023.



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 2023.

PAPER CUT (CVE-2023-27350)

This is a critical RCE (Remote Code Execution) vulnerability with a CVSS score of 9.8 in PaperCut, a print management software with a user base of more than 100 million users. Disclosed with a patch-released in March of 2023, this flaw can lead to the exposure of sensitive information and breach of entire networks. Following its disclosure, it was quickly [leveraged](#) by various malicious actors, including the delivery of [Lockbit](#) and [CL0P](#) ransomware. It was also exploited by [state-sponsored](#) APT groups. Check Point data shows that 9% of organizations have been impacted by this vulnerability in 2023.

MOVEIT (CVE-2023-34362)

This critical SQL injection vulnerability in MOVEit MFT (Managed File Transfer Software) was exploited in 2023's most prolific ransomware [campaign](#), impacting more than 2,700 organizations globally. The vulnerability was exploited by the CL0P ransomware group prior to its public disclosure and utilized to deploy a web shell named LEMURLOOT, which was then used to steal data from MOVEit Transfer databases. The large number of victims and the amount of data led CL0P to [change](#) its extortion techniques, relying on data extortion instead of encrypting and publishing stolen data on Torrents. Check Point data shows that 7% of organizations have been impacted by this vulnerability in 2023.

GO ANYWHERE (CVE-2023-0669)

This is a critical RCE vulnerability in the GoAnywhere MFT software (Managed File Transfer) disclosed in February 2023. Prior to its disclosure, the flaw was actively [exploited](#) by the CL0P ransomware gang, leading to significant data breaches in more than 130 organizations. This incident highlights the growing trend of ransomware operators using zero-day vulnerabilities to conduct their attacks. Check Point data shows that 2.5% of organizations have been impacted by this vulnerability in 2023.

BARRACUDA (CVE-2023-2868)

This is a critical remote command injection vulnerability identified in the Barracuda Email Security Gateway (ESG) appliance, which is [exploited](#) using malicious file attachments. The vulnerability was actively exploited as early as October 2022 by a Chinese APT actor in an aggressive campaign that impacted organizations on a global scale, with a significant focus on government agencies. Following the release of patches and containment efforts, the attackers adapted their techniques by altering their malware and employing additional persistence mechanisms to maintain access. As a result, both Barracuda and the FBI recommended that customers immediately [replace](#) compromised ESG devices.

MICROSOFT OUTLOOK (CVE-2023-23397)

This is a critical privilege escalation vulnerability in Microsoft Outlook, discovered in March 2023 with a CVSS rating of 9.8. The flaw enables attackers to hijack users' authentication hashes via specially crafted emails. The vulnerability was actively [exploited](#) by groups including the Russian-affiliated APT28.

CITRIXBLEED (CVE-2023-4966)

This critical [vulnerability](#) in Citrix NetScaler platforms allows remote unauthenticated attackers to extract system memory data which includes session tokens. These are then used to hijack legitimate sessions, bypassing password and MFA procedures. Due to its ease of use and the availability of proof-of-concept exploits, CitrixBleed was extensively exploited by several ransomware groups including [LockBit](#), [Medusa](#) and [Akira](#).

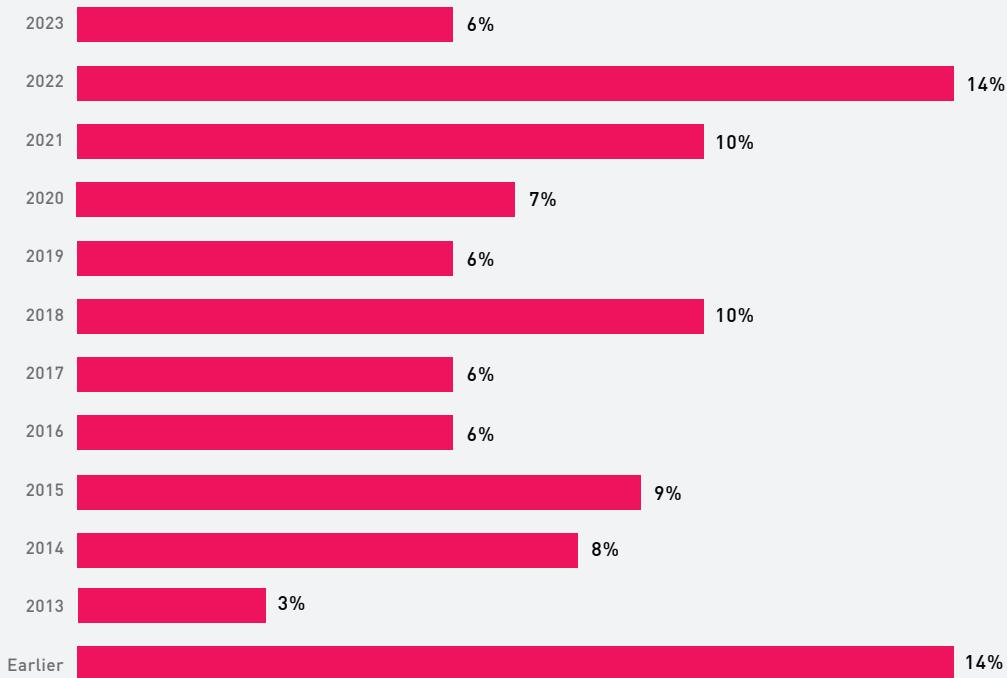


Figure 38: Percentage of attacks leveraging vulnerabilities by Disclosure Year in 2023.

In 2023, there was a noticeable shift in the cyber threat landscape, with newly disclosed vulnerabilities being rapidly exploited by attackers. Data indicates that vulnerabilities reported in 2023 and 2022 were responsible for 6% and 14% of all exploitation attempts, respectively. This demonstrates that recent vulnerabilities are more severe and easy to exploit and are adopted and weaponized by threat actors much faster than others. In comparison, relatively new vulnerabilities, disclosed between 2021 and 2023, accounted for over 30% of exploitation attempts, a marked increase from only 17% observed in 2021 for vulnerabilities disclosed between 2019 and 2021. This trend represents a departure from previous reliance on delayed update practices, by exploiting older, unpatched vulnerabilities, as evidenced by the "long-tail" distribution pattern seen in previous years.

MALICIOUS INFRASTRUCTURE BY TLD (TOP LEVEL DOMAIN)

This section highlights the most frequently used malicious Top-Level Domains (TLDs) as observed through Check Point's ThreatCloud AI in 2023. Domains, whether used to disguise phishing sites or serving as command and control (C&C) centers for major botnets, are critical components in a threat actor's infrastructure. Understanding trends associated with various TLDs equips defenders with another tool for assessing potential risks. Several factors may influence threat actors' preference for a specific TLD, including the targeted organization they aim to impersonate, the availability of the TLD with their preferred domain registrar, or the cost associated with acquiring the TLD.

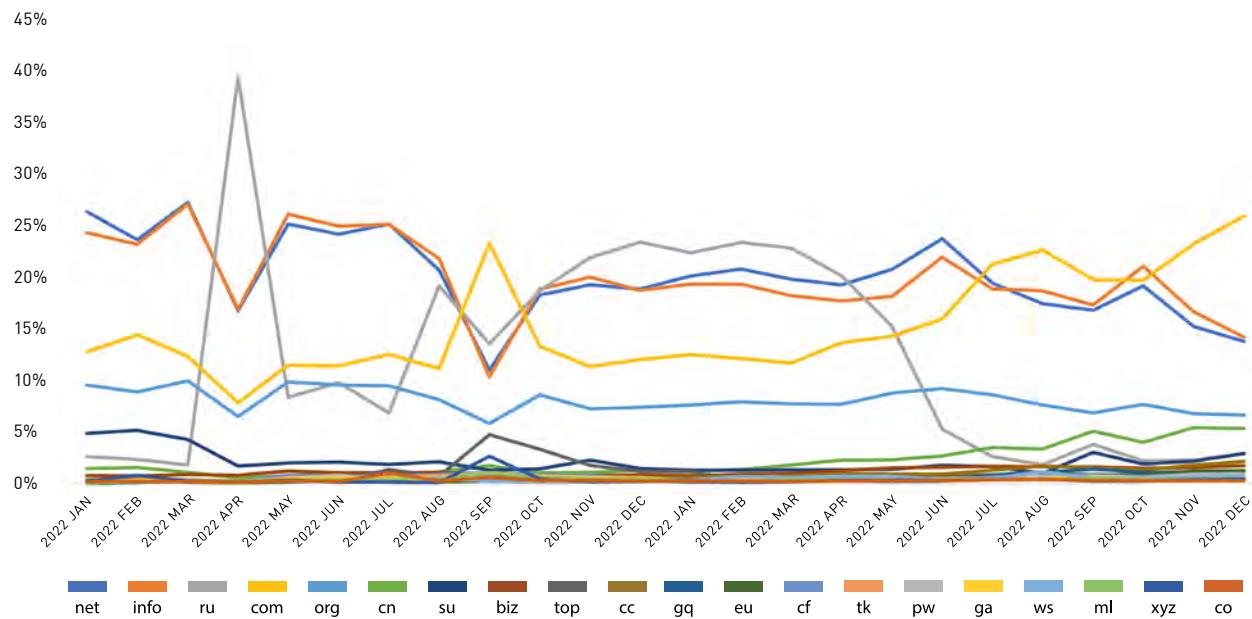


Figure 39: Percentage of new malicious domains by TLD per month 2022-2023.

The noticeable increase in new malicious .RU domains, which began in early 2022 and reached nearly 40% of new malicious domains at the onset of the Russian invasion of Ukraine, has since returned to pre-war levels, now averaging less than three percent of new malicious domains registered monthly. During this intense period, .RU domains consistently ranked third or fourth among all malicious TLDs. The Russian state-aligned Gamaredon APT group is a frequent user of malicious .RU domains, and is known for registering hundreds of domains through the REG.RU registrar in recent years.



CHECK POINT INCIDENT- RESPONSE TEAM (CPIRT) PERSPECTIVE

This section is based on the experience and data from a wide array of CPIRT analyses and mitigation cases, not limited to Check Point product users. CPIRT typically steps in after the clear manifestation of malicious activity, such as files encrypted by ransomware, identified email compromises, or the detection of unauthorized malware files or processes. Analysis of initial threat indicators, or 'triggers', offers a different perspective of the threat landscape.

Our Incident Response Team was contacted following an EDR security alert in a customer's environment. Mimikatz, a notorious credential-stealing tool, was caught in the act and blocked by the EDR system. This unusual activity raised immediate concerns, indicating the presence of an adversary and its attempt to unobtrusively navigate the network. The client, realizing the potential gravity of the situation, reached out to CPIRT for assistance.

UNDERSTANDING INCIDENT TRIGGERS

We define incident triggers as the first indication of a compromise that prompted the client to seek IR services. Ransomware stands out as the predominant factor, accounting for approximately 30% of all Incident-Triggers. Ransomware attacks are often highly visible and severely disruptive, requiring immediate action.

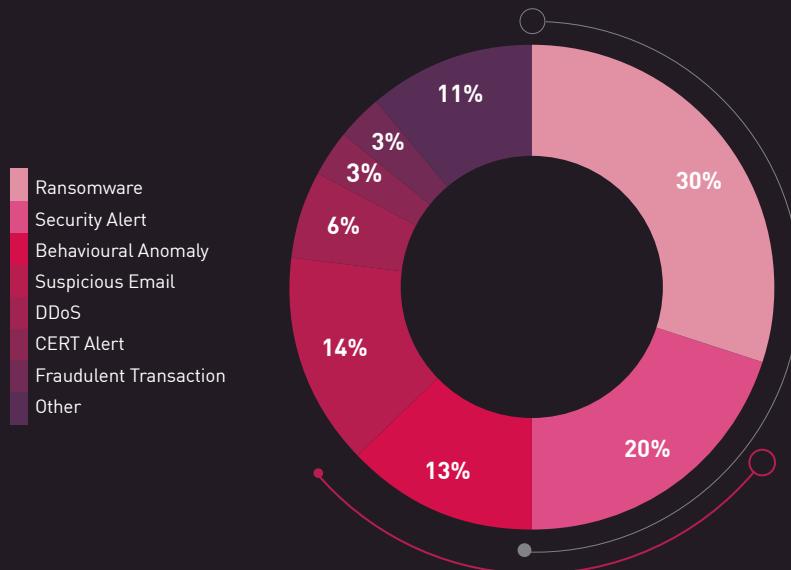


Figure 40: Breakdown of CPIRT cases by Incident trigger in 2023.

Twenty percent of CIPRT cases in 2023 were triggered by an alert from a security product in the customer's environment. These are often alerts of the highest severity, while lower severity alerts do not usually require the same response. Interestingly, behavioral anomalies, which include any unusual activity that the regular user observes and that deviate from established patterns, prompted 13% of incident response (IR) engagements. This high percentage reflects their significance as a red flag for potentially severe security issues. However, it is important to keep in mind that reports of behavioral anomalies are often less reliable and may result in False Positives.

In the graph above, the suspicious email category refers to any suspect inbound or outbound email activity. Suspicious outbound emails are extremely concerning, as they often indicate an email compromise in the organization. If not detected in time, these incidents may lead to an unauthorized money transfer, which is another common IR trigger that comprised 3% of our cases in 2023.

Incident triggers that are less frequent but still critical include CERT alerts, in which the initial indication of compromise is provided by the local CERT, and dark web monitoring, in which the initial alert comes from finding mentions on underground forums of a breach or offers to buy initial access. Despite their lower prevalence, these triggers often indicate sophisticated and severe threats that can have significant ramifications if not addressed promptly.

As we delved deeper into the incident, the plot thickened. We detected signs of data exfiltration, coupled with the discovery of a RAT (Remote Access Tool) and encryption binaries on the Active Directory server. These elements were prepared for a wide-scale deployment across the network—the unmistakable precursors of a ransomware attack, mere minutes from execution.

TOP ATTACK TYPES

"Top Attack" refers to the category of the attack, not the indicator that triggered the investigation. Analysis of the top attack types shows that ransomware is the most prevalent threat type, accounting for 46% of IR cases. Business Email Compromise (BEC), at 19% of the cases, is detected through indicators such as suspicious email activity or fraudulent money transfers.

In 2023, attacks that aimed to steal specific user identities, such as BEC, browser hijacking, and account takeover were even more prevalent, with an increase of over 20% over the previous year. Contributing to this increase was the growing reliance on cloud infrastructure as well as the prominence of access brokers, who sell credentials and access to organizations.

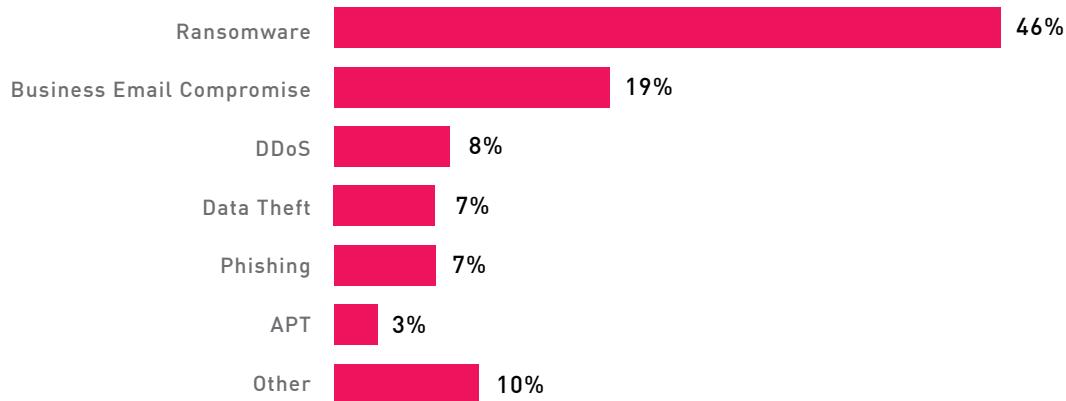


Figure 41: Breakdown of CPIRT cases by Attack Type in 2023.

POPULAR TOOLS USED IN ATTACKS

The CPIRT analysis reveals that tools such as AnyDesk and TeamViewer, which are typically benign remote-desktop applications, are increasingly used by threat actors for Command and Control. In fact, AnyDesk alone was used in 39% of the incidents that we analyzed this year. This tactic underscores a stealth approach by attackers, who are leveraging tools that evade traditional malware detection. These tools, originally intended for legitimate use, are increasingly used by threat actors, which makes it more complicated to distinguish between conventional and malicious activities on networks. In contrast, known malicious tools, such as Mimikatz and CobaltStrike were involved in 26% and 16% of breaches, respectively.

Further investigation into the incident revealed the use of AnyDesk as the remote command tool of choice by the attackers, providing them with persistent access to the compromised systems. Their initial access did not trigger security alerts, allowing the threat actor to hide in plain sight.

RANSOMWARE: THE PRINCIPAL THREAT

Several families emerge as particularly prominent in the 2023 CPIRT ransomware threat landscape. Notably, the 'Royal' ransomware has rapidly evolved to become a potent threat, accounting for a significant number of incidents. In most cases, phishing was used as the initial access vector, often deploying malicious PDFs or employing callback phishing tactics to install remote desktop access. In addition, Royal actors repurposed tools like Cobalt Strike, NSudo, and PsExec for the second stages of the attacks.

ALPHV (BlackCat) ransomware demonstrated its versatility as it was used to attack various systems, including Windows, Linux, and VMware instances. As ALPHV operates as a Ransomware-as-a-Service (RaaS) model, deployed by distinct affiliates, we saw a variety of entry vectors and TTPs used before its deployment, making each incident unique and challenging to predict and defend against.



TIM OTIS

Head of Global Detection
and Response,
Check Point Software
Technologies

“Not all breaches are leveraged immediately. The initial breach often begins when threat actors use mass scanners to exploit newly discovered vulnerabilities in devices across the internet. However, even after patching, webshells and other persistence mechanisms can remain intact. These footholds are often later sold by Initial Access Brokers (IABs) and may resurface months or years later in subsequent attacks.”

These vulnerabilities, particularly ProxyShell and Citrix RCE (CVE-2023-3519), can enable threat actors to install webshells on internet-facing vulnerable devices. The devices targeted in those vulnerabilities, such as Exchange servers and NetScaler Gateways, are often internet-facing, constituting prime targets. Once compromised, these devices continue to function as dormant footholds for the threat actor, even after patching.

While diving deeper into the incident and trying to locate the initial infection vector, we identified CVE-2023-3519, a remote code execution vulnerability in Citrix NetScaler systems as the initial point of compromise. This vulnerability had been exploited to deploy a webshell on the device, which remained undetected even after the system was patched. This oversight allowed the threat actor to maintain network access. Three months post-exploitation, this webshell was activated by another threat actor who intended to deploy ransomware. Fortunately, due to the customer's alertness and CPIRT's prompt response, the ransomware attack was successfully thwarted before it could inflict damage.

This reality creates a false sense of security for administrators who believe patched devices are secure, while actually, a threat actor's foothold might have been established much earlier. In our investigations this year, the longest period noted for a dormant threat was 22 months.

Following the patching of vulnerabilities, security procedures must include security scans to remove possible backdoors, webshells and other persistence mechanisms. Organizations must also continue to monitor for any anomalies that may indicate covert threats within network infrastructure.



INSIGHTS FOR CISO'S— PREDICTIONS

The threat landscape is vast. Cyber security technologies are advancing, but with a limited budget, you're probably strategically mapping out how your organization should allocate resources.

As you consider how to best mature your cyber security infrastructure this year, Check Point's global team of CISOs can offer some insight.



JONATHAN 'JONY'
FISCHBEIN

- Global CISO, EMEA,
Check Point Software
Technologies

Ransomware will continue and become highly evasive

Ransomware attacks will increase. They will also continue to impact organizations of all sizes, extorting millions of dollars from victims. Most notably, the threats will become increasingly evasive.

While enterprises are adopting a lot of security tools, they're often not enough, as oftentimes, they're not interoperable.

Many security professionals erroneously believe that a ransomware attack won't happen to their organization, and so they don't take adequate action. What organizations really need are better prevention and detection tools.

It's very important that organizations take a holistic approach to ransomware and develop a strategy for mitigation. And it's not enough to just have solutions that ward off ransomware.



DERYCK MITCHELSON

- Field CISO EMEA,
- Check Point Software
- Technologies

Organizations will continue to see a surge in cyber attacks and data breaches, resulting in an explosion of class action lawsuits and litigation that could negatively affect CISOs

Litigation is becoming increasingly common. There's no doubt about it. Many major enterprises have experienced breaches and paid out significant sums of money on the back of them.

The issue won't solely affect larger organizations. Smaller organizations will be affected as well and will likely pay out millions in order to satisfy shareholders and individuals who have been breached.

This increase in data breach class actions is really concerning. There's been a two-fold increase in them from 2022 to 2023.

Further, recent survey results show that 62% of CISOs are concerned about their personal liability when it comes to breaches. What's driving this? The first item is the Uber case, where the Uber CISO was found guilty.

**PETE NICOLETTI**

Field CISO, Americas,
Check Point Software
Technologies

*AI-based tools will be used by cyber criminals to steal financial resources*

Something that Check Point Research has just begun to point out is that criminals are using unregistered and unguarded AI tools and engines for nefarious purposes. Those tools aren't subject to laws and regulations.

Cyber security professionals are liable to see what could be termed 'ghost guns' or 'unserialized weapons' used in the AI fight. Check Point's ThreatCloud and other power-packed products help mitigate this issue, but in the future, more will need to be done to address it.



AI: THE CUTTING-EDGE DEFENDER IN TODAY'S CYBERSECURITY BATTLES

In the ever-evolving landscape of cybersecurity, artificial intelligence (AI) has emerged as a game-changer, revolutionizing the way we prevent, protect against and respond to cyber threats. AI's transformative impact in this domain is profound, offering unprecedented advantages in identifying, analyzing, and neutralizing cyber risks. By leveraging complex algorithms and machine learning, AI systems can swiftly detect patterns indicative of malicious activities, often identifying threats far more rapidly than traditional methods. This capability is particularly crucial in an era where cyberattacks are becoming increasingly sophisticated and frequent. AI's ability to adapt and learn from new threats means it continuously improves its defense strategies, making it an indispensable ally in the ongoing battle against cybercrime. The integration of AI in cybersecurity not only enhances the efficiency and effectiveness of security measures but also significantly reduces the time and resources required to combat these digital dangers, thereby safeguarding our digital world with greater precision and intelligence.

Infinity AI Copilot Transforming Cyber security with Intelligent GenAI Automation and Support—More security. Less time and effort.

Leveraging the convergence of AI and cloud technologies, Infinity AI Copilot addresses the growing global shortage of cyber security practitioners by boosting the efficiency and effectiveness of security teams.

Reduce up to 90% of the time needed to perform common administrative tasks with a Generative AI security solution that harnesses automation and collaborative intelligence.

Unlike other AI models that work in a silo, Infinity AI Copilot delivers broad platform support for a variety of use cases—helping manage security across the entire Infinity Platform.

Infinity AI Copilot knows the customer's policies, access rules, objects, logs, as well as all product documentation—allowing it to provide contextualized and complete answers.

Key Capabilities:

-  **Accelerate security administration:** Infinity AI Copilot saves up to 90% of the time needed for administrative work for security tasks including event analysis, implementation, and troubleshooting. Security professionals can dedicate more time to strategic innovation, thanks to the time saved.
-  **Manage and deploy security policies:** manage, modify and automatically deploy access rules and security controls, specific to each customer's policy.
-  **Improve incident mitigation and response:** leverage AI in threat hunting, analysis and resolution.
-  **Oversee all solutions and environment:** AI Copilot oversee all products across the entire Check Point Infinity Platform—from network to cloud to workspace—making it a true comprehensive assistant.
-  **Made simple natural language processing:** Interacting with Infinity AI Copilot GenAI is as natural as a conversation with a human. It understands and responds via chat in any language, making it easier for users to communicate and execute tasks. This natural language capability fosters seamless interaction and effective task execution.

[ThreatCloud AI](#) is Check Point's Big Data Intelligence engine. It uses 50+ AI and Machine Learning technologies that identify and block emerging threats that were never seen before. Out of the 50 AI-based engines 11 uses Deep Learning technology and 38 Classic Machine Learning technology.

During 2023 we've added 12 new engines:

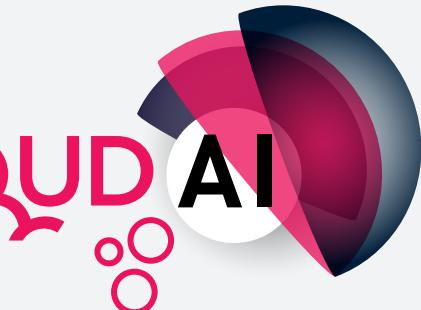


ThreatCloud AI aggregates and analyzes big data telemetry and millions of Indicators of compromise (IoCs) every day. Its threat intelligence database is fed from 150,000 connected networks and millions of endpoint devices, as well as Check Point Research and dozens of external feeds. ThreatCloud AI updates newly revealed threats and protections in real-time across Check Point's entire security stack.

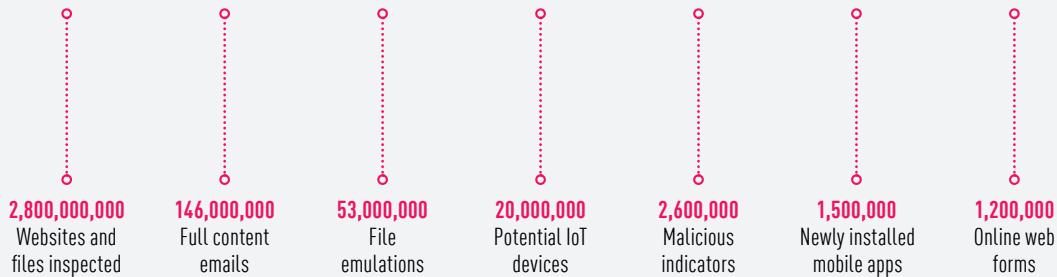
COLLABORATIVE SECURITY—THREATCLOUD AI

AI is All About Your Data

THREATCLOUD AI



**COUNTED
DAILY!**



BIG DATA THREAT INTELLIGENCE

Here are some of the ways ThreatCloud AI prevents emerging cyber threats:

ThreatCloud Graph: A Multi-Dimensional Perspective on Cyber Security

This innovative feature is moving beyond the traditional analysis of standalone entities, such as URLs, IPs, and domain names. ThreatCloud Graph delves into the interconnected web of relationships between these entities, unveiling a multi-dimensional perspective on cyber threats.

ThreatCloud Graph's innovative approach in analyzing the interconnected web of relationships in the cyber threat landscape provides a powerful tool for proactive threat prevention, insightful attack detection, and robust defense against zero-day threats.

Main Benefits:

1

Holistic Threat Prevention

ThreatCloud Graph offers a comprehensive view of cyber threats by analyzing the relationships between various entities, such as URLs, IPs, and domain names. This approach goes beyond examining standalone threats, providing a multi-dimensional perspective that focuses on proactive prevention.

This holistic perspective allows for a deeper understanding of how threats are interconnected and how they operate within larger networks and campaigns.

2

Graph Patterns and Attack Insight

By identifying unique patterns of relations between different cyber entities, ThreatCloud Graph provides valuable insights into malicious activities. This feature is particularly useful in detecting and understanding complex attacks like DNS poisoning. The ability to recognize these patterns and links between common entities facilitates the early detection and prevention of sophisticated cyber threats, enhancing overall security.

3

Preventing Zero-Day Emerging Threats

Leveraging the knowledge of ThreatCloud AI, ThreatCloud Graph is adept at preventing emerging threats, including zero-day attacks. It establishes the reputation of URLs, domains, and IP addresses based on their relations to previously known malicious artifacts. This preemptive approach, which does not rely solely on detected malicious content, allows for the early identification and blocking of potential threats, ensuring robust protection against the most advanced and emerging attacks.

AI-powered Brand Spoofing Prevention

Expanding our zero-phishing offering, we've introduced our innovative AI-powered engine to prevent local and global brand impersonation employed in phishing attacks, collaboratory protecting across networks, emails, mobile devices, and endpoints, with 40% higher catch rate than traditional technologies.

The newly developed engine blocks links and browsing associated with local and global brands that have been impersonated and exploited as bait to deceive victims in phishing attacks, spanning multiple languages and countries.

AI-Powered Brand Spoofing Prevention



Protect your organization against
brand impersonation phishing
attacks



Real time blocking of access
to links that impersonate
international or local brands



40% higher catch rate than
traditional technologies

Preemptive, real-time prevention



Utilizing innovative AI technologies, new domains are auto inspected upon registration to identify potential brand spoofing attempts and are blocked before they can even be used in an attack

Collaborative protection with ThreatCloud AI



Immediately apply zero brand spoofing protection across any attack vector including email, files, SMS and more, across your Network, Endpoint, Mobile and SaaS.

Deep PDF—AI powered engine which provides accurate and precise identification of malicious PDF's without relying on static signatures

Deep PDF', an innovative AI model, and an integrated part of [ThreatCloud AI](#), takes a giant leap forward in identifying and blocking Malicious PDFs used in global scale phishing campaigns. These attacks can be activated via a variety of vectors, including email, web downloads, HTML smuggling, SMS messages and more. Check Point Quantum and Harmony products protect these vectors, so our customers remain protected.

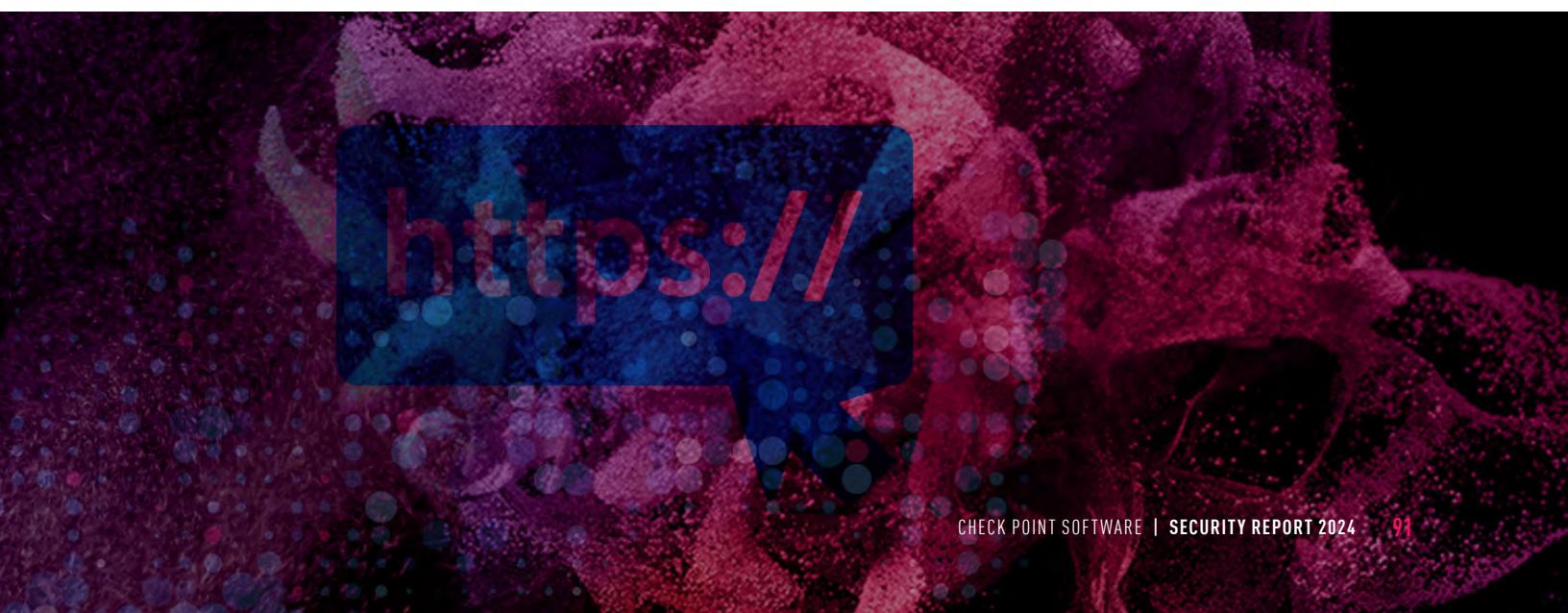
Deep PDF'- How it work?

'Deep PDF' engine examines the PDF structure, embedded images, URLs and Raw content, looking for phishing layout. The power of this model is not just in the sheer volume of files it can detect, but also in its precision, making it an asset in the constant battle against [phishing campaigns](#) and spam.

Researchers in Check Point found that PDF files have similar structure. 'Deep PDF' search, among other things, for:

- Malicious links.
- URL placement on the document.
- Image placement on the page.

We encode these abstract characteristics and much more to features and trained 'Deep PDF' to distinguish between benign and malicious PDF files.



LinkGuard: a New Machine Learning Engine Designed to Detect Malicious LNK Files

- LinkGuard is an Machine Learning engine designed to detect malicious LNK files, now Integrated into ThreatCloud AI
- LNK files are often seen as harmless shortcuts, but are frequently used by cybercriminals to deliver malware and enable social engineering attacks.
- The new engine excels at identifying obfuscation techniques, leveraging linguistic analysis to achieve an impressive 90%+ detection rate

LinkGuard is designed to tackle one of the Internet's sneakiest threats: malicious LNK files. These deceptive files, often camouflaged as harmless shortcuts, can wreak havoc on your system.

LinkGuard's mission is clear: to detect these malicious LNK files by identifying malicious code execution and analyzing command-line arguments.

The Essence of LinkGuard

LinkGuard is another AI-powered engine, designed to go deep into the world of LNK files, dissecting them to their core. Its ingenious approach involves examining the very essence of these files to determine if they harbor any signs of foul play. By scrutinizing the command-line arguments hidden within LNK files, LinkGuard can pinpoint any traces of malicious intent. It's like having a digital detective that tirelessly hunts for threats, allowing you to fortify your system with confidence.

How LinkGuard Works

LinkGuard uses three fundamental principles:

- 1 **Unmasking Obfuscation:** LinkGuard excels at exposing the obfuscation techniques employed to hide malicious code within LNK files, ensuring that even the most cunning attempts at evasion are thwarted.
- 2 **Linguistic Analysis:** Leveraging, LinkGuard deciphers malicious themes embedded within LNK files using natural language processing (NLP) . It identifies subtle linguistic patterns indicative of malicious intent.
- 3 **Recognizing Familiar Tactics:** LinkGuard effectively identifies similarities to well-known malicious code execution, promptly recognizing tactics employed by cyber adversaries.

By combining these three powerful capabilities, LinkGuard forms a invaluable shield against LNK-based cyber threats. It not only fortifies your cybersecurity defenses but also contributes to a safer digital environment.



MALWARE FAMILY DESCRIPTIONS

AgentTesla

AgentTesla is an advanced RAT functioning as a keylogger and information stealer that is capable of monitoring and collecting the victim's keyboard input, taking screenshots, and exfiltrating credentials to a variety of software installed on a victim's machine (including Google Chrome, Mozilla Firefox and the Microsoft Outlook email client).

Akira

Akira Ransomware, first reported in the beginning of 2023, targets both Windows and Linux systems. It uses symmetric encryption with CryptGenRandom() and Chacha 2008 for file encryption and is similar to the leaked Conti v2 ransomware. Akira is distributed through various means, including infected email attachments and exploits in VPN endpoints. Upon infection, it encrypts data and appends a ".akira" extension to file names, then presents a ransom note demanding payment for decryption.

ALPHV

BlackCat (aka ALPHV) operates in a ransomware-as-a-service (RaaS) business model. BlackCat ransomware is highly customizable and allows for attacks on a wide range of corporate environments. It targets both Linux and Windows systems, and is coded in Rust.

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.

BiBi Wiper

BiBi Wiper is a data-wiping malware targeting both Windows and Linux systems. Initially identified in attacks against Israeli targets, it's known for its destructive capabilities, and is designed to overwrite data in targeted directories with junk data and append a ".BiBi" extension to filenames.

CACTUS

CACTUS Ransomware is a destructive malware that encrypts files on a victim's computer and adds a unique ".CTS1" extension to each encrypted file. The ransomware is known for exploiting vulnerabilities in network systems, particularly VPN appliances, to gain access and spread within targeted networks. It employs OpenSSL for encryption using AES and RSA.

CLOP

CLOP is a ransomware that was first discovered in early 2019 and mostly targets large firms and corporations. CLOP is operated by a Russian-language cybercriminal gang and employs a "steal, encrypt, and leak" strategy. It gained recent notoriety for exploiting vulnerabilities in public-facing infrastructure like Accellion FTA and MOVEit Transfer, enabling it to exfiltrate and encrypt sensitive data from victim organizations. CLOP has been involved in significant "big game hunter" ransomware attacks, targeting a variety of industries without specific regional focus and avoiding organizations within the Commonwealth of Independent States (CIS).

CloudEye

CloudEye is a downloader that targets the Windows platform and is used to download and install malicious programs on victims' computers.

DarkGate

DarkGate, active since December 2017, is a sophisticated Malware-as-a-Service (MaaS) known for its wide-ranging capabilities, including credential theft, keylogging, screen capturing, and remote access. DarkGate emerged as a prominent threat within cybercriminal circles (mainly underground forums). The malware has adapted to circumvent security defenses and is used in diverse attack strategies, including phishing emails and exploiting communication platforms like Microsoft Teams.

DoppelPaymer

DoppelPaymer, first noticed in 2019, is a sophisticated ransomware strain, evolving from the earlier BitPaymer. It targets a wide range of sectors, with no specific industry preference, and uses the Dridex Trojan for initial infiltration through spear-phishing emails. DoppelPaymer is known for its double extortion tactic and was involved in several notable attacks on major organizations worldwide.

Emotet

Emotet is an advanced and modular multipurpose malware. Emotet was once employed as a banking Trojan, and now is used as a distributor 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.

FakeUpdates

Fakeupdates (AKA SocGholish) is a downloader written in JavaScript. It writes the payloads to disk prior to launching them. Fakeupdates led to further system compromise via many additional malware, including GootLoader, Dridex, NetSupport, DoppelPaymer, and AZORult.

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 that 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.

GootLoader

GootLoader is a stealthy malware, primarily used as a first-stage downloader attacking Windows-based systems. Initially serving as a downloader for the GootKit banking Trojan, it has evolved into a multi-payload malware platform capable of delivering sophisticated second-stage payloads like Cobalt Strike beacon and REvil ransomware. GootLoader uses SEO poisoning to redirect victims to compromised websites for drive-by download campaigns, impacting various industries across multiple countries. It employs advanced techniques like reflective loading and PowerShell commands for persistence and evasion.

Horse Shell

Horse Shell is a custom malware utilized by the Chinese state-sponsored hacking group "Camaro Dragon" for targeting European foreign affairs organizations. Discovered in January 2023, this malware infects residential TP-Link routers, enabling attackers to gain complete control over these devices. Horse Shell operates as a backdoor, executing shell commands, transferring files, and using the router as a SOCKS proxy for communications.

Impala Stealer

Impala Stealer is a crypto-stealing malware targeting .NET developers through malicious NuGet packages. It operates by installing a persistent backdoor to access and steal cryptocurrency account details, utilizing typosquatting to disguise itself as legitimate software packages

JaguarTooth

JaguarTooth is a Cisco IOS malware that targets and modifies routers' authentication mechanisms to allow unauthenticated backdoor access. It collects and exfiltrates device and network information, including firmware versions and network configurations, via the Trivial File Transfer Protocol (TFTP). JaguarTooth was deployed through the exploitation of a known Simple Network Management Protocol (SNMP) vulnerability, CVE-2017-6742.

KV-botnet

The KV-Botnet, linked to the China-linked threat actor Volt Typhoon, is a sophisticated botnet that primarily targets small office/home office (SOHO) router devices. Active since at least February 2022, it consists of two complementary activity clusters named KV and JDY.

LemonDuck

LemonDuck is a cryptocurrency-mining botnet which targets victims' computer resources to mine the Monero virtual currency. It employs various methods to spread across the network, such as sending infected RTF files using email, psexec, WMI, and SMB exploits, including the infamous Eternal Blue and SMBGhost threats that affect Windows 10 machines.

LEMURLOOT

LEMURLOOT is a web shell malware associated with the CL0P ransomware group, designed to exploit a critical SQL injection vulnerability (CVE-2023-34362) in the MOVEit Transfer managed file transfer (MFT) application. LEMURLOOT is written in C# and requires a hard-coded password for authentication. This malware was instrumental in significant data theft and extortion attempts by the CL0P group.

LockBit

LockBit is a ransomware, operating on 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 the Commonwealth of Independent States.

LokiBot

LokiBot is a commodity info stealer for Windows. It harvests credentials from a variety of applications, web browsers, email clients, IT administration tools such as PuTTY, and more. LokiBot was sold on hacking forums and its source code is believed to have leaked, thus allowing for a range of variants to appear. It was first identified in February 2016.

Lucifer

Lucifer is a hybrid malware known for its capabilities in both cryptojacking and launching Distributed Denial-of-Service (DDoS) attacks. Leveraging multiple high and critical severity exploits, Lucifer originally targeted the Windows system. However, it recently evolved into a multi-platform and multi-architecture malware targeting Linux, and IoT devices, and has separate ARM and MIPS versions.

Medusa

Medusa ransomware, active since June 2021, is a Ransomware-as-a-Service (RaaS) model employing a double-extortion tactic (encrypts and exfiltrates data, threatening to leak or sell it if the ransom isn't paid.)

Mirai

Mirai is an infamous Internet-of-Things (IoT) malware that tracks vulnerable IoT devices, such as web cameras, modems and routers, and turns them into bots. The botnet is used by its operators to conduct massive Distributed Denial of Service (DDoS) attacks. The Mirai botnet first surfaced in September 2016 and quickly made headlines due to some large-scale attacks including a massive DDoS attack used to knock the entire country of Liberia offline, and a DDoS attack against the Internet infrastructure firm Dyn, which provides a significant portion of the United States internet's infrastructure.

Nanocore

NanoCore is a Remote Access Trojan (RAT) 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, cryptocurrency mining, remote control of the desktop and webcam session theft.

NetSupport

NetSupport malware, identified as a Remote Access Trojan (RAT), targets sectors like education, government, and business services. Originally a legitimate remote administration tool, NetSupport was repurposed by threat actors for malicious activities such as monitoring behavior, file transfer, and infiltrating networks.

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.

Nokoyawa

Nokoyawa is a Windows-based ransomware family first identified in February 2022 and is known for double extortion attacks. This ransomware, initially written in C and later rewritten in Rust, demonstrates coding similarities with the Nemy and Karma ransomware families. The ransomware is known to exploit vulnerabilities like CVE-2023-28252 in attacks.

Phorpiex

Phorpiex is a botnet (a.k.a Trik) that has been active since 2010 and at its peak controlled more than a million infected hosts. It is known for distributing other malware families via spam campaigns as well as fueling large-scale spam and sextortion campaigns.

Qbot

Qbot AKA Qakbot is a banking Trojan that first appeared in 2008. It was designed to steal a user's banking credentials and keystrokes. Often distributed via spam email, Qbot employs several anti-VM, anti-debugging, and anti-sandbox techniques to hinder analysis and evade detection.

Raccoon

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

Ramnit

Ramnit is a modular banking Trojan first discovered in 2010. Ramnit steals web session information, giving its operators the ability to steal victim credentials for all services, including bank accounts and corporate and social network 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.

RedRelay

RedRelay is a shared proxy network utilized by various threat actors including the Chinese cyber espionage actor Red Vulture. RedRelay employs features like multi-hop proxying and encrypted communication, making analysis and attribution challenging. The network is constructed from a combination of threat actor-operated virtual private servers (VPS) and compromised devices.

Remcos

Remcos is a RAT that first appeared in the wild in 2016. Remcos distributes itself through malicious Microsoft Office documents that are attached to SPAM emails and is designed to bypass Microsoft Windows UAC security and execute malware with high-level privileges.

RubyMiner

RubyMiner was first seen in the wild in January 2018 and targets both Windows and Linux servers. RubyMiner seeks out vulnerable web servers (such as PHP, Microsoft IIS, and Ruby on Rails) and uses them for cryptomining activity using the open source Monero miner XMRig.

StripedFly

StripedFly, originally misclassified as a cryptocurrency miner, is a complex and versatile wormable malware framework. Its impact is worldwide, infecting more than a million victims since at least 2017.

Ursnif

Ursnif is a variant of the Gozi banking Trojan for Windows, whose source code was leaked online. It has Man-in-the-Browser capabilities to steal banking information and credentials for popular online services. In addition, it can steal information from local email clients, browsers and cryptocurrency wallets. Finally, it can download and execute additional files on the infected system.

WannaMine

WannaMine is a sophisticated Monero crypto-mining worm that spreads the EternalBlue exploit. WannaMine leverages Windows Management Instrumentation (WMI) permanent event subscriptions to spread and maintain persistence.

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.

ZuoRAT

ZuoRAT is a Remote Access Trojan (RAT) with a focus on small office/home office (SOHO) routers. Derived from the Mirai botnet, it has been operating since at least 2020. ZuoRAT employs extensive network reconnaissance, data collection, and the hijacking of network communications.



CONCLUSION

As we transition into the new year, last year's patterns and lessons should become the foundation upon which we build new and resilient strategies.

Proactive identification of emerging trends, recognition of vulnerabilities, and an understanding of threat actor methodologies are critical to developing effective and sustainable cyber security programs.

The Security Report is designed to empower cyber security leaders with the knowledge and foresight required to remain a step ahead of cyber adversaries.

From the rise of ransomware zero-days to the emerging risks posed by hacktivism, organizations urgently need to adapt and adopt new security measures.

In an era where technology evolves at a breakneck pace, the insights shared here serve as a roadmap for navigating cyber security landscape in 2024 and beyond.

CONTACT US

WORLDWIDE HEADQUARTERS

5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel
Tel: 972-3-753-4599
Email: info@checkpoint.com

U.S. HEADQUARTERS

959 Skyway Road, Suite 300, San Carlos, CA 94070
Tel: 800-429-4391

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

