cp<r>
CHECK POINT RESEARCH

13th Annual Edition

THE STATE OF CYBER SECURITY 2025

Top threats, emerging trends, and CISO recommendations

CHECK POINT™

TABLE OF CONTENTS

01

INTRODUCTION

THE STATE OF CYBER SECURITY 2025

INTRODUCTION

I'm happy to introduce the 13th annual edition of Check Point's State of Cyber Security. 2024's advancements like AI and cloud infrastructure improved our daily lives but also benefited cyber criminals. This report highlights the real-world impact of these changes, offering 2025 insights and recommendations from and for CISOs.

With over a decade of analysis, Check Point Research insights come from unparalleled data sources that no other company combines. We gather attack telemetry from networks, cloud, email, endpoints, and mobile devices across enterprise and SMB customers. By incorporating incident response, dark web, and open-source findings, we achieve visibility in over 170 countries to reveal global and regional trends.

The 2025 State of Cyber Security report highlights key threats, including:

- The AI tactics that swayed a third of global elections through disinformation.
- A 58% surge in infostealer attacks, focusing on corporate access.
- Ransomware attacks shift from encryption to data exfiltration extortion, with Healthcare now the second most targeted.
- Hybrid networks enabling lateral movement between on-premise and cloud.
- Hardware and Software supply chains saw the highest attack surge attacks

I want to emphasize Check Point's commitment to customer security. In 2024, edge devices were exploited to access enterprise networks through leaked credentials and vulnerabilities. One of the many disclosed zero-day vulnerabilities was in a Check Point product: the VPN Information Disclosure vulnerability (CVE-2024-24919). We promptly disclosed it, released a patch within a day, and proactively supported the few potentially affected customers with incident response and mitigation. Our dedication to protecting customers is in our DNA.

While Check Point aims to protect our customers with our research, we hope this report serves the needs of the broader industry as well, as we combine forces and share knowledge. On behalf of the Check Point family, I hope this report is useful to both security practitioners as well as C-level executives.

Enjoy the read!

Maya Horowitz, VP Research

MAYA HOROWITZ

VP Research

2024 CYBER SECURITY EVENTS

THE STATE OF CYBER SECURITY 2025

THE CYBER SECURITY EVENTS THAT DEFINED 2024

Q1

JAN

After disclosing two zero-day vulnerabilities, Ivanti's Connect Secure VPNs faced mass exploitation. Thousands of VPN devices were compromised, impacting victims like the U.S. Cyber security and Infrastructure Security Agency (CISA).

Check Point Research uncovered an NFT scam targeting holders of over 100 popular projects. Scammers send seemingly legitimate airdrops that link to fraudulent websites. Victims are tricked into connecting their wallets, granting attackers access to their funds.

Microsoft reported an attack by the Russian group Midnight Blizzard (Nobelium), which used a password spray attack to compromise corporate email accounts, including those of senior leadership, cyber security, and legal staff.

> **Check Point Harmony Endpoint and Threat Emulation protect against this threat (APT.Win.APT29; APT.Wins.Nobelium)**

HealthEC LLC experienced a data breach that affected 4.5 million individuals, compromising names, addresses, DOBs, SSNs, medical and billing information, and health insurance data.

FEB

Exploiting a Fortinet vulnerability, Chinese state-backed hackers targeted an unclassified military research network in a cyber espionage operation against the Dutch Defense Ministry, marking the Netherlands' first public attribution of a cyber attack to China.

A high-severity vulnerability in Google Chrome's V8 JavaScript engine, CVE-2024-0517, was identified. The flaw could allow a remote attacker to exploit heap corruption via a crafted HTML page. Google has since patched the vulnerability.

> **Check Point Harmony IPS protects against this threat (Google Chrome Out of Bounds Write (CVE-2024-0517))**

Check Point Research discovered a critical Remote Code Execution (RCE) vulnerability in Microsoft Outlook, dubbed #MonikerLink (CVE-2024-21413). #MonikerLink allows remote attackers to deploy a link that bypasses the Protected View Protocol, potentially leading to credentials leakage and RCE capabilities. Microsoft has since patched the vulnerability.

> **Check Point IPS blade protects against this threat (Microsoft Outlook Malicious Moniker Link Remote Code Execution (CVE-2024-21413)**

The US Department of Justice disrupted the KB botnet, used by the China-affiliated APT Volt Typhoon to mask its identity while targeting critical infrastructure in the US. The group exploited vulnerable, end-of-life Cisco and NetGear SOHO devices for initial access. In response, CISA and the FBI released guidance for vendors on securing SOHO routers.

> **Check Point Threat Emulation protects against this threat (APT.Wins.VoltTyphoon; InfoStealer.Wins.VoltTyphoon)**

MAR

The ALPHV ransomware gang attacked UnitedHealth Group's subsidiary, stealing six terabytes of data. U.S. military clinics and hospitals worldwide were disrupted, necessitating manual prescription processes.

> **Check Point Harmony Endpoint and Threat Emulation protect against this threat (Ransomware.Wins.BlackCat.ta.*; Ransomware.Win.BlackCat)**

Cutout.Pro, an AI-powered photo and video editing service, experienced a data breach that exposed the personal data of 20 million users, including email addresses, hashed passwords, and IP addresses.

Chinese APT group Earth, Krahang, targeted 70 government entities worldwide in a cyber espionage campaign, active since early 2022, utilizing vulnerabilities in internet-facing servers and spear-phishing tactics.

Check Point Research tracked the financially motivated threat actor Magnet Goblin, who exploited one-day vulnerabilities in servers like Ivanti Connect Secure VPN, Magento, and Qlik Sense. The actor deployed a new Linux version of NerbianRAT and WARPWIRE JavaScript credential stealer while proving quick adoption of exploits.

> **Check Point IPS and Harmony Endpoint protect against this threat (RAT_Linux_Nerbian_*)**

THE CYBER SECURITY EVENTS THAT DEFINED 2024

Q2

APR

Check Point researchers detected a typosquatting campaign comprised of over 500 malicious packages deployed on PyPI (Python Package Index), posing risks of PII theft malware installation.

Check Point CloudGuard Code Security protects against this threat.

Russian-speaking hacktivist group RGB-TEAM breached the website of Russia's prosecutor general and leaked 100,000 criminal records from 1993 to 2022 on Telegram. Data included details on crimes such as theft and drug trafficking.

An AT&T data breach exposed the personal information of approximately 51M former and current clients, potentially including full names, home addresses, email addresses, phone numbers, social security numbers, AT&T account numbers, and AT&T passcodes.

Check Point Research reports a wave of scam attacks in which attackers use various methods, including malicious QR codes and phishing emails, to gain US taxpayers' credentials to steal IRS refunds.

The US and UK announced a criminal indictment and sanctions against APT31, a group of Chinese hackers, for their role in alleged attacks against US and UK governmental officials. Check Point Research explored the group's use of zero-day vulnerabilities.

MAY

Check Point Research uncovered a cyber espionage campaign targeting African and Caribbean governmental organizations. Attributed to Chinese threat actor Sharp Dragon, the campaign adopts Cobalt Strike Beacon as the payload, enabling backdoor functionalities like C2 communication and command execution while minimizing the exposure of their custom tools. This approach suggests a deeper understanding of their targets.

The Czech Republic, Germany, and NATO revealed an espionage campaign targeting Czech institutions through a Microsoft Outlook vulnerability attributed to the Russian state-affiliated group, APT28, which has been conducting a long-term espionage effort across Europe.

A Dell data breach affected 49 million customers after their database was listed on a hacking forum. The exposed data includes full names, home addresses, and order details.

A data breach exposed 500 GB of biometric data from India, affecting police, military personnel, and public workers during elections. The leak involved unsecured databases from ThoughtGreen Technologies and Timing Technologies, including fingerprints and facial scans. The information could be leveraged to manipulate biometric systems in Indian elections.

JUNE

Data from Ticketmaster and Santander Bank has been put up for sale on a cyber crime forum by ShinyHunters, a notorious cyber gang. The breach potentially exposes the personal information of millions of customers. Reports indicate that the threat actor gained access to Ticketmaster and Santander by using the stolen credentials of one employee from Snowflake, a large cloud storage company.

Japanese crypto exchange DMM Bitcoin confirmed a data breach that resulted in losing $308 million in BTC, one of the largest crypto heists.

China-linked Water Sigbin 8220 Gang exploited vulnerabilities in Oracle WebLogic (CVE-2017-3506 and CVE-2023-21839) to deploy cryptocurrency mining malware using PowerShell scripts with hexadecimal URL encoding and fileless execution techniques.

Check Point IPS protects against this threat (Oracle WebLogic WLS Security Component Remote Code Execution (CVE-2017-10271), Oracle WebLogic Server Improper Access Control (CVE-2023-21839))

Check Point Research analyzed Rafel RAT, an open-source remote administration tool for espionage and ransomware attacks on Android devices. The malware targeted high-profile organizations, especially in the military sector, with victims mainly from the U.S., China, and Indonesia. It enables data exfiltration, surveillance, and complete device control, resulting in severe privacy and security breaches.

Check Point's Harmony Mobile protects against this threat.

THE CYBER SECURITY EVENTS THAT DEFINED 2024

Q3

JULY

Check Point Research identified the Stargazers Ghost Network, consisting of 3,000 GitHub repositories that distribute malware and malicious links through phishing schemes using a Distribution as a Service (DaaS) model. The network has shared various types of malware, such as Atlantida Stealer and RedLine, and has generated significant profits.

> **Check Point Harmony Endpoint and Threat Emulation protect against this threat (InfoStealer.Win.Atlantida.*, Trojan.WIN32.AtlantidaStealer*, InfoStealer.Wins.Lumma.ta*, InfoStealer.Win.Lumma*, Injector.Win.RunPE.C, Loader.Wins.GoBitLoader.A, Trojan.Wins.Imphash.taim.LV, InfoStealer.Wins.Redline.ta.BY)**

RockYou2024, a leak of nearly 10 billion plaintext passwords from multiple data breaches, poses significant risks for credential stuffing and brute-force attacks that could affect various online accounts and services.

45M records from Rite Aid were stolen in a ransomware attack, allegedly including clients' identifying information and Rite Aid rewards numbers. RansomHub ransomware group claimed responsibility and threatened to leak the stolen data.

> **Check Point Threat Emulation and Harmony Endpoint protect against this threat (Ransomware.Win.RansomHub; Ransomware.Wins.RansomHub.ta.*)**

Location safety app Life360 and project management tool Trello suffered data breaches due to API vulnerabilities. Personal information of Life360's 442,519 customers was exposed, while 21.1GB of Trello's data was leaked. Threat actor 'emo' claimed responsibility and shared the stolen data on the dark web.

AUG

Check Point Research found that over 20K Ubiquiti cameras and routers are vulnerable (CVE-2017-0938) to amplification attacks and privacy risks due to exposed UDP ports 10001 and 7004. These ports permit unauthorized access to device information, which could be exploited for technical and social engineering attacks.

Check Point Research noted a rise in Server-Side Template Injection (SSTI) vulnerabilities that allow attackers to execute commands and access sensitive data. Notable cases involve Atlassian Confluence and CrushFTP. These vulnerabilities pose significant risks, such as data theft and reputation damage, reflected in a rise in critical CVEs

> **Check Point IPS protects against this threat (Python Server-Side Template Injection, Java Server-Side Template Injection, PHP Server-Side Template Injection, Ruby Server-Side Template Injection, Node.js Server-Side Template Injection, Expression Language Server-Side Template Injection)**

Following the July Venezuelan presidential elections, Check Point Research revealed that hacktivist groups Anonymous Venezuela and Cyber Hunters launched DDoS attacks and hacking attempts against the government, driven by allegations of election fraud linked to Nicolás Maduro's administration.

> **Harmony Endpoint and Threat Emulation protect against this threat (InfoStealer.Wins.PhemedroneStealer.*)**

SEPT

93GB of sensitive data was stolen from Planned Parenthood's Montanna branch by the ransomware group RansomHub, primarily affecting the organization's administrative IT systems.

> **Check Point Threat Emulation and Harmony Endpoint protect against this threat (Ransomware.Win.RansomHub; Ransomware.Wins.RansomHub.ta.*)**

Check Point Research identified an Iranian cyber campaign targeting Iraqi governmental networks using malware Veaty and Spearal. Techniques include a passive IIS backdoor, DNS tunneling, and C2 communication via compromised emails, indicative of ties to the APT34 group. The campaign likely utilizes social engineering for initial infection and has a sophisticated C2 infrastructure.

> **Check Point Threat Emulation and Harmony Endpoint protect against this threat (APT.Wins.Oilrig.ta.B/C/D/E, APT.Win.OilRig.F, APT.Win.OilRig.WA.G, APT.Win.OilRig.H)**

The FBI, CISA, and NSA report that Russian GRU Unit 29155 has targeted Ukraine with website defacements, data theft, and WhisperGate malware, disrupting aid efforts. They also targeted sectors globally, including government, finance, transportation, energy, and healthcare.

> **Check Point Threat Emulation and Harmony Endpoint protect against this threat (Trojan.Win.WhisperGate; Trojan.Wins.WhisperGate.ta.*; Trojan.Wins.WhisperGate)**

A vulnerability in the ChatGPT macOS app allowed attackers to implant persistent spyware, SpAIware, into the app's memory through indirect prompt injection, enabling continuous data exfiltration of user inputs and future chat sessions. OpenAI has since resolved the issue.

THE CYBER SECURITY EVENTS THAT DEFINED 2024

Q4

OCT

Check Point Research analyzed 'Operation MiddleFloor,' a disinformation campaign targeting Moldova's government and education sectors before the October 2024 elections. The Russian-aligned group Lying Pigeon uses spoofed emails to spread false information about EU membership while collecting data for potential malware attacks.

A new phishing-as-a-service platform called Mamba 2FA targets adversary-in-the-middle phishing attacks. It mimics Microsoft 365 login pages and bypasses multi-factor authentication, stealing credentials and cookies sent to attackers via a Telegram bot.

The FBI and CISA investigate breaches by the Chinese government-affiliated group Salt Typhoon at U.S. telecommunications companies, including AT&T, Verizon, and Lumen Technologies. The attacks targeted wiretapping systems and devices of President-elect Trump, former Vice President Harris, and other notable politicians.

NOV

The FBI, the US Department of Treasury, and the Israeli National Cyber security Directorate (INCD) released a joint Cyber security Advisory attributing a large-scale phishing campaign impersonating the INCD and targeting Israeli organizations to the Iranian cyber group Emennet Pasargad. Check Point Research analyzed the malware, tracking its evolution and learning.

> **Check Point Threat Emulation and Harmony Endpoint protect against this threat (Behavioral.Win.FakeChrome.B and Trojan.Wins.FakeUpdater.A)**

Check Point Research monitored a large-scale phishing campaign dubbed CopyRh(ight)adamantys, which uses the latest version of the Rhadamanthys stealer (0.7). This campaign targets regions like the U.S., Europe, East Asia, and South America, using a copyright theme and impersonating various companies, tailoring each email from different Gmail accounts.

> **Check Point Threat Emulation and Harmony Endpoint protect against this threat (InfoStealer.Wins. Rhadamanthys.ta.V, InfoStealer.Wins.Rhadamanthys.*, and InfoStealer.Wins.Rhadamanthys.*)**

Check Point Research tracked the WIRTE threat actor, linked to Hamas-affiliated Gaza Cybergang, conducting espionage against entities in the Palestinian Authority, Jordan, Iraq, Egypt, and Saudi Arabia, and has expanded to disruptive attacks connected to SameCoin malware targeting Israeli entities in 2024.

> **Check Point Threat Emulation and Harmony Endpoint protect against this threat (APT.Wins.Wirte.ta.A/B/C/D/E/F, ransom.win.honey, and infoastealer.win.blackguard.d)**

DEC

Check Point Research uncovered a novel exploit of Godot Engine—a gaming development platform—to execute malicious GDScript code. The technique enables attackers to deliver malware across platforms like Windows, macOS, Linux, Android, and iOS, while evading detection by most antivirus solutions. Malicious loader, "GodLoader", used this technique and already infected over 17,000 machines.

> **Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Technique.win. GDscript.*, Dropper.Win.Godot.*)**

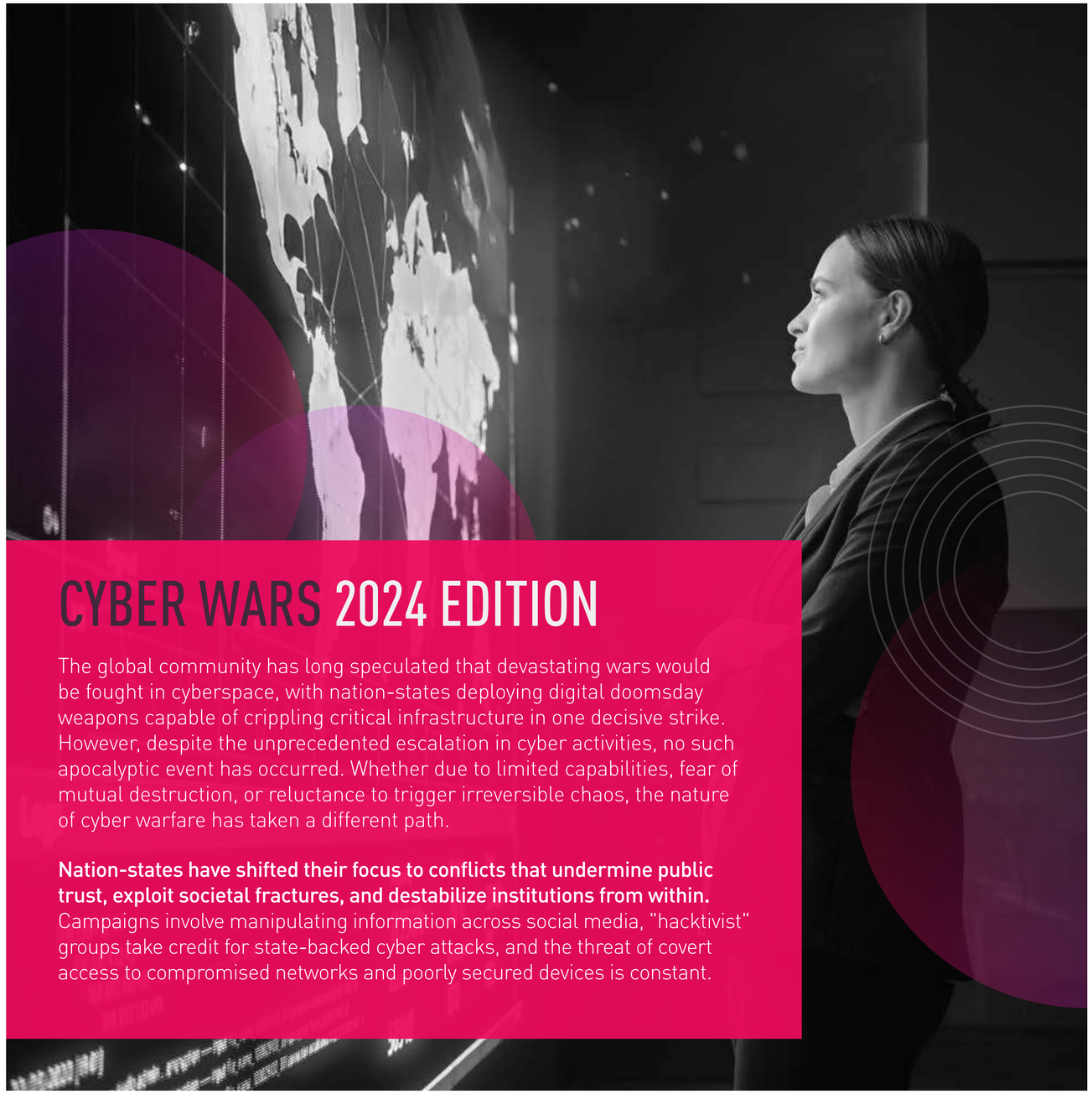
Check Point Research analyzed Akira ransomware's latest variant, written in Rust, that primarily targeted ESXi bare metal hypervisor servers in early 2024. The report showed how Rust idioms, boilerplate code, and compiler strategies were used to create complex assembly.

> **Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware_Linux_ Akira_C/D, Ransomware.Wins.Akira.G/H)**

Ukrainian intelligence agency HUR confirmed a DDoS against Russia's Gazprombank, one of Russia's largest banks, which aimed to disrupt financial operations related to Russia's war efforts in Ukraine.

CYBER SECURITY TRENDS

THE STATE OF CYBER SECURITY 2025



CYBER WARS 2024 EDITION

The global community has long speculated that devastating wars would be fought in cyberspace, with nation-states deploying digital doomsday weapons capable of crippling critical infrastructure in one decisive strike. However, despite the unprecedented escalation in cyber activities, no such apocalyptic event has occurred. Whether due to limited capabilities, fear of mutual destruction, or reluctance to trigger irreversible chaos, the nature of cyber warfare has taken a different path.

Nation-states have shifted their focus to conflicts that undermine public trust, exploit societal fractures, and destabilize institutions from within. Campaigns involve manipulating information across social media, "hacktivist" groups take credit for state-backed cyber attacks, and the threat of covert access to compromised networks and poorly secured devices is constant.

DISINFORMATION AND INFLUENCE OPERATIONS

In 2024, disinformation campaigns reached new levels of complexity, driven by the integration of AI and large language models (LLMs). These operations focused on global events, with nation-states like China, Russia, and Iran accused of using advanced tactics to manipulate public opinion, undermine trust, and interfere with elections to destabilize democratic processes.

Based on Check Point Research's findings, **AI was utilized in at least one third of the elections that took place** worldwide between September 2023 and February 2024, either by candidates themselves or potentially by foreign actors. Recent instances demonstrate this development, such as the Russian-linked APT group CopyCop targeting the June 2024 USA primary elections with fabricated news segments featuring deepfake portrayals of political figures. Distributed through X (formerly known as Twitter) and Facebook, this content exploited platform algorithms to target specific voter demographics. AI-generated bots further disseminated divisive narratives, posing as genuine opinion pieces to polarize the electorate.

Iranian campaigns, often linked to the Islamic Revolutionary Guard Corps (IRGC), also targeted the US presidential elections by attacking prominent political figures in "hack-and-leak" operations. Journalists, activists, and lobbyists were also targeted through social engineering, impersonations, phishing, and credential-harvesting malware. These operations demonstrated Iran's ability to blend disinformation with cyber infiltration to sway public perception.

Meanwhile, Chinese-aligned actors used AI-generated deepfake videos portraying false endorsements and misleading public service announcements. These videos, widely circulated on platforms like X and TikTok, aimed to discredit candidates and deepen partisan divides. Additionally, viral posts embedded with skewed polling questions seemingly portrayed support for certain candidates or fabricated evidence of fraud, undermining trust in the electoral process.

Beyond the high-profile presidential elections in the US, Taiwan's and Romania's presidential elections and Moldova's EU referendum became prime targets for cyber-enabled disinformation warfare. Chinese-attributed campaigns used AI-generated articles and social media posts to mimic legitimate news sources, discredit candidates, and sway

public opinion. Deepfake videos portraying candidates making controversial statements circulated widely, while misleading polling questions suggested declining support for specific candidates. In Romania, Russian interference leveraged fake social media accounts and manipulated content to promote far-right candidate Călin Georgescu. After Georgescu unexpectedly won the first round, declassified intelligence revealed the extent of foreign interference, prompting an unprecedented annulment of the election results and scheduling a new vote. In Moldova, a campaign called "Operation MiddleFloor", attributed to a Russian-aligned group, targeted government and education sectors using spoofed emails and documents to spread anti-EU narratives and undermine trust in pro-European leadership.

The Paris Olympics became another key focus for disinformation. Russian-linked Storm-1679 spread false narratives about corruption, biased officiating, and threats of violence. Automated accounts and bots amplified these claims to discredit the event and disrupt Western unity. More aggressively, the Iranian group Emennet Pasargad exploited vulnerabilities in the Olympics' display system provider to disrupt broadcasts and spread anti-Israel propaganda and sent threats to Israeli athletes from a fake persona imitating the French group GUD.

These attacks on democracies and Western political alliances such as NATO have become increasingly effective and dangerous as democratic countries face ever-growing challenges**. Online cultural wars, social media-fueled populism, and politicized media platforms using advanced algorithms to tailor favorable content created fertile ground for foreign actors to undermine public trust**. The dissemination of content that aligns with or supports propaganda from specific states has already taken root, deepening societal divides.

Democracies have responded by tightening regulations and recognizing disinformation as a threat to critical infrastructure. The U.S. Department of Homeland Security highlighted election meddling as a threat, while Canada expanded the CSIS Act for better intelligence sharing. The European Union imposed strict rules on platforms like Meta to curb Russian disinformation. OpenAI and Microsoft are disturbing accounts associated with groups from China, Iran, Russia, and North Korea.

DESTRUCTIVE AND DISRUPTIVE MALWARE

Nation-states increasingly relied on destructive malware as an important weapon in cyber warfare. These "loud" operations, characterized by wiper malware and other disruptive tools, targeted critical infrastructure, disrupting essential services and spreading chaos.

Amidst the heightened tensions in the Middle East, Iran and other regional threat groups demonstrated the destructive potential of wiper malware. Void Manticore, an Iranian group linked to the Ministry of Intelligence and Security (MOIS), deployed the No-Justice Wiper under the guise of hacktivist personas like Karma and Homeland Justice. These campaigns targeted critical Israeli infrastructure and private organizations, erasing data and disrupting services.

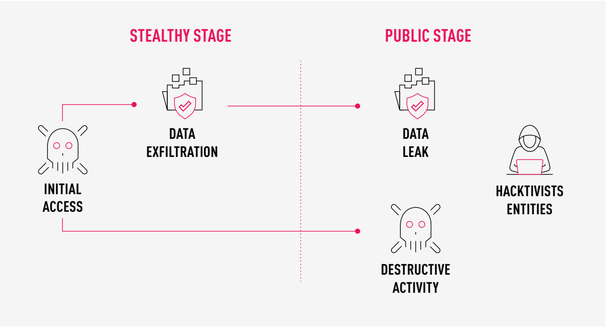


Figure 1 – Iran's typical warfare campaign tactics.

Similarly, the Hamas-linked group WIRTE showcased its evolving cyber capabilities by using the SameCoin wiper variant to target hospitals and municipalities in Israel, exacerbating the psychological and logistical toll of the ongoing conflict.

In Eastern Europe, Russian-linked groups continued to weaponize destructive malware as part of its broader hybrid warfare strategy in Ukraine. The notorious Russian-affiliated APT44 (also known as Sandworm) introduced AcidPour, an advanced wiper variant of the AcidRain malware. AcidPour was deployed to disrupt Ukrainian critical infrastructure, telecom networks, and internet service providers. This malware was designed not only to destroy systems but also to embed itself deeper into environments, exfiltrating sensitive military plans and severing vital communication channels. These operations underscored Russia's intent to leverage cyber tools as a vital support mechanism in its geopolitical conflicts.

DISRUPTION PREPARATION – POSSIBLE "RED BUTTONS"

While some nations embraced these high-impact, one-time attacks, others, like China, took a quieter approach. They penetrated deep within critical systems, laying the groundwork for potential large-scale disruption in the future. Chinese-affiliated actors now focus on infiltrating critical infrastructure and maintaining a persistent, undetected presence. Exploiting vulnerabilities in edge devices such as routers, VPN appliances, and IoT systems, groups like APT41 and Bronze Butler gained unauthorized access to less secure network components, allowing them to collect intelligence and establish a potential

"red button" capability—access that could be used for future large-scale disruptions. This strategic positioning, particularly evident in US targets, enables Chinese actors to silently prepare for potential conflicts while avoiding the immediate visibility and retaliation that come with destructive operations.

Chinese APT group Volt Typhoon exemplified this approach by intensifying its focus on exploiting firewalls and routers in US critical infrastructure. Using living-off-the-land (LOTL) techniques, Volt Typhoon relied on legitimate administrative tools within compromised environments to evade detection. This allowed the group to bypass conventional cyber security measures and maintain a covert presence, positioning itself for future actions.

Adding another layer to this covert strategy, Salt Typhoon targeted major internet service providers (ISPs), including AT&T and Verizon, exploiting vulnerabilities to intercept and manipulate network traffic. Additionally, Chinese-linked actors used Operational Relay Boxes (ORBs), which are networks of compromised VPS and IoT devices, to maintain persistence, relay commands, and gather intelligence. Often managed by contractors within China, ORBs enabled these attackers to remain embedded in compromised systems, discreetly relaying commands and gathering intelligence.

"HACKTIVIST" GROUPS

Last year, the blurred boundaries of state-backed cyber warfare became increasingly evident as nation-states relied on a sprawling network of online personas to serve their geopolitical agendas. Many of these figures, presenting themselves as ideologically motivated independent hacktivists, were fronts for state-sponsored APT groups. **By amplifying divisive narratives and targeting public trust, the hacktivist groups became critical components of more extensive influence operations, allowing their sponsors to obscure their direct involvement while leveraging patriotic rhetoric to amplify their impact.** Amid a backdrop of declining public interest and increasing fatigue, a notable trend emerged in 2024: the formation of alliances, where disparate groups united under shared banners to create a stronger, more cohesive front.

On the individual front, Iranian-backed hacktivist groups also intensified their activities, primarily focusing on Israeli and Albanian targets. Groups such as Malek Team and Handala Hack conducted defacement campaigns, hack and leak operations, and disruptions and claimed responsibility for breaching Israeli networks and exfiltrating terabytes of sensitive data. Karma, associated with Iran's Ministry of Intelligence and Security (MOIS), deployed destructive tools like the BiBi and No Justice wipers against Israeli organizations. The Cyber Avengers, linked to the Islamic Revolutionary Guard Corps (IRGC), targeted critical infrastructure, including power grids and water systems in Israel, the US, and Ireland. The Iranian group Homeland Justice also attacked Albanian governmental institutions in retaliation for hosting the opposition group Mujahedin-e-Khalq (MEK). These activities highlight Iran's adept use of proxy groups to merge hacktivism with state-directed cyber warfare, advancing its geopolitical interests while maintaining plausible deniability.

Similarly, Russian actors also exemplified this tactic, with groups like KillNet, NoName057(16), and the Cyber Army of Russia targeting critical infrastructure in countries aligned against Russia. These groups carried out mostly Distributed Denial of Service (DDoS) attacks and other manipulations, disrupting government and private sector operations in Ukraine and pro-Ukrainian countries.

Beyond their individual efforts, Russian-aligned hacktivists expanded their influence by forming alliances with foreign actors. A notable example is the High Society hacktivist collective, which incorporates over 20 Russian-affiliated cyber gangs, including Russian-linked groups like People's Cyber Army, NoName057(16) and UserSec. High Society joined the 7 October Union, a pro-Palestinian hacktivist collective of over 40 groups, many of which are linked to Iran. This alliance, named Holy League, targeted NATO, Europe, Ukraine, and Israel, with notable campaigns like the coordinated DDoS and propaganda efforts targeting NATO's 75th Anniversary Summit in Washington. The campaign sought to undermine public support for NATO's backing of Ukraine, blending cyberattacks with psychological manipulation to influence public opinion.

Figure 2 – telegram post about the creation of the "Holy League".

In 2024, hacktivist activity underscored the evolving dynamics of alliances and influence in cyberspace, reflecting geopolitical tensions between the East and West. Groups such as the Holy League symbolized shared strategic goals among Russian and Iranian-affiliated actors. These alliances often mirrored real-world political developments: for example, after South Korea sent observers to Ukraine during North Korea's involvement with Russian forces, Russian-linked groups NoName057(16) and Z Pentest launched retaliatory DDoS attacks and industrial hacks on South Korean entities. By emphasizing their united fronts through recurring declarations of collaboration, these groups sought to sustain attention, bolster their psychological impact, and amplify global influence in the increasingly complex landscape of modern cyber conflict.

NORTH KOREA'S CYBER DRIVEN FINANCIAL WARFARE

Where other nations deploy hacktivists to disrupt and destabilize, North Korea's cyber efforts transcend the pretense of activism. Instead, Pyongyang engineered a vast and interconnected apparatus of cyber operations that meld financial crime with espionage to help sustain its embattled regime under the weight of international sanctions.

North Korea's "financial warfare" is a delicate balancing act: ransomware and cryptocurrency theft fund the regime's nuclear ambitions, missile programs, and other weapons development, while espionage campaigns gather intelligence to enhance military and technological capabilities.

Lazarus Group, the prime example of North Korea's cyber criminal machine, spearheaded operations in 2024 with characteristic sophistication. One operation disguised as a tank-themed cryptocurrency game exploited a zero-day vulnerability in Google Chrome to deploy the Manuscrypt backdoor. The goal wasn't just to steal cryptocurrency but also to add an element of espionage. A stolen wallet today might fund a stolen military blueprint tomorrow.

Subgroups like BlueNoroff further refined this approach. Their "Hidden Risk" campaign lured cryptocurrency traders with convincing phishing emails and fake news websites designed to manipulate transactions and siphon funds into the regime's coffers. It also demonstrated how disinformation deployment strategies can be leveraged into cyber crime.

Andariel, another of the regime's APTs, blurred the line between financial theft and destruction. It targeted US healthcare organizations encrypting critical systems to extort cryptocurrency payment using cyber crime-oriented Play ransomware. These operations weren't just about immediate financial gain but also served as a testing ground for tactics that could disrupt vital sectors in a geopolitical crisis.

Even the employment landscape became a battlefield. In 2024, Western companies unwittingly welcomed North Korean operatives posing as remote IT freelancers. By infiltrating corporate environments under false identities, these operatives achieved a dual purpose: generating hard currency for the regime and gaining potential access to sensitive organizational networks.

FROM PREDICTED CATASTROPHIC STRIKES TO CONTINUOUS BATTLES

In a broader view of this year, cyber warfare has fragmented into smaller, continuous battles across multiple domains instead of catastrophic strikes aimed at crippling nations at a single blow. These conflicts rarely have clear winners or losers but mostly succeed in eroding trust, weakening institutions, and blurring the boundaries between state and civilian spheres.

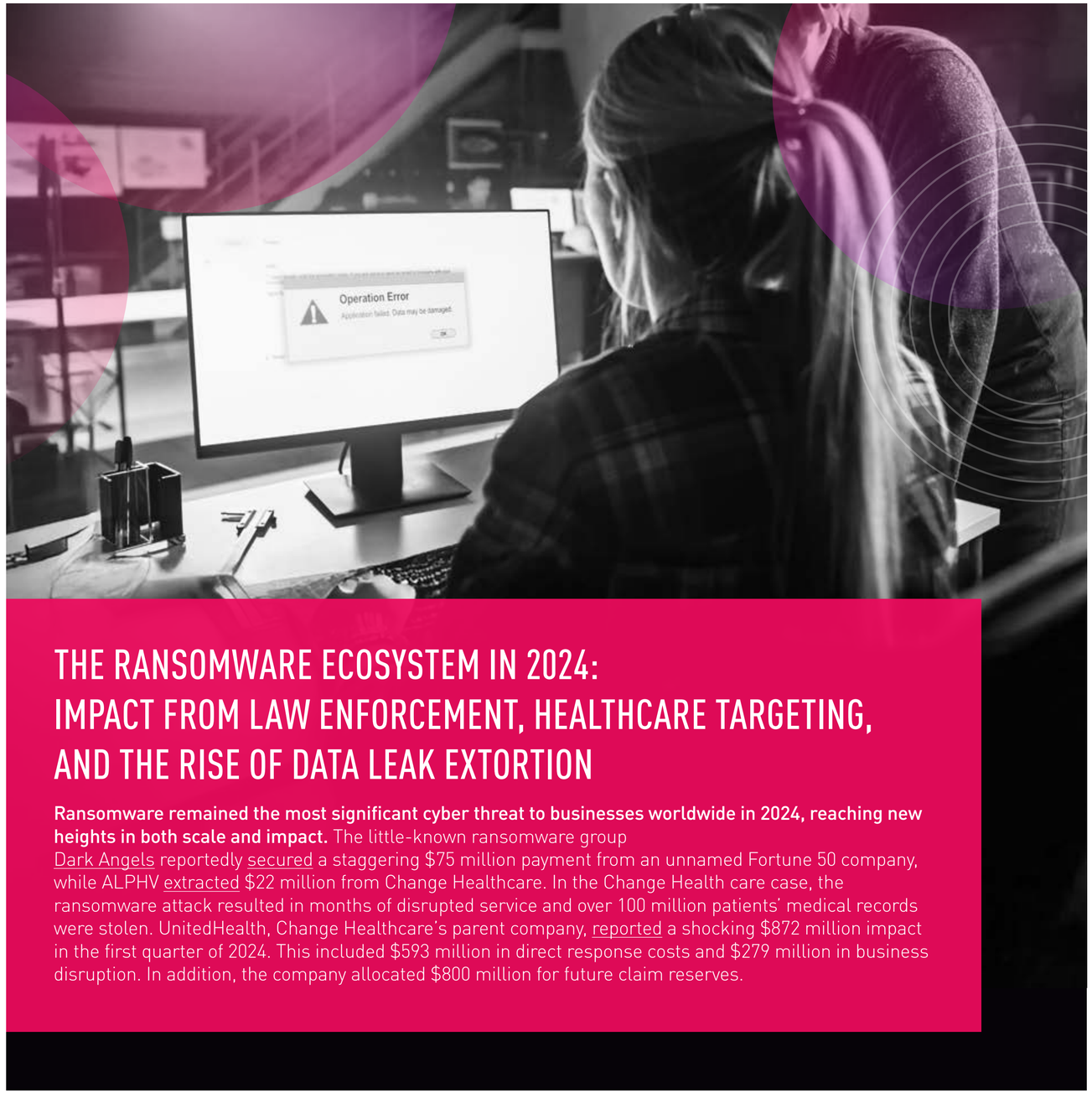
Influence operations emerged as a key front, with AI-powered disinformation campaigns targeting elections, societal cohesion, and geopolitical stability. Simultaneously, destructive malware, hacktivist fronts, and financial cyber crime served as tools for coercion, destabilization, and self-sustenance in the case of heavily sanctioned regimes like North Korea.

While democracies attempt to adapt by tightening regulations and investing in cyber defenses, the battleground has already shifted beneath their feet. Cyber warfare is no longer confined to digital infrastructure but has permeated the social fabric. Battles over information and perception threaten to outlast the physical systems they were once expected to target.

> "Today's cyber warfare has evolved from immediate destruction to encompassing campaigns that lay the foundations for eroding systems—whether social or physical. Now, nation-states wield cyber 'weapons' like AI-generated deepfakes and social media manipulation that weaken democratic processes over time while their covert operations secure access to critical infrastructure, setting the stage for future attacks."

ELI SMADJA

Security Research Group Manager



THE RANSOMWARE ECOSYSTEM IN 2024: IMPACT FROM LAW ENFORCEMENT, HEALTHCARE TARGETING, AND THE RISE OF DATA LEAK EXTORTION

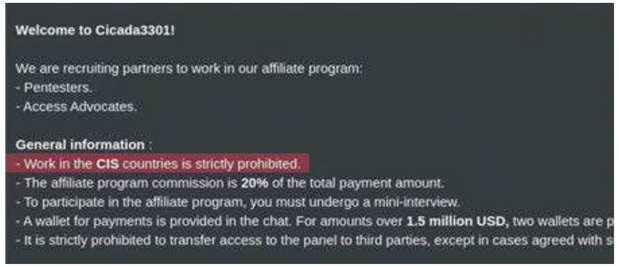
Ransomware remained the most significant cyber threat to businesses worldwide in 2024, reaching new heights in both scale and impact. The little-known ransomware group Dark Angels reportedly secured a staggering $75 million payment from an unnamed Fortune 50 company, while ALPHV extracted $22 million from Change Healthcare. In the Change Health care case, the ransomware attack resulted in months of disrupted service and over 100 million patients' medical records were stolen. UnitedHealth, Change Healthcare's parent company, reported a shocking $872 million impact in the first quarter of 2024. This included $593 million in direct response costs and $279 million in business disruption. In addition, the company allocated $800 million for future claim reserves.

Despite this increase, the median ransom payment in 2024 remained at approximately $200,000, with most attacks unfolding quietly with little public attention.

Aside from high-profile cases, the threat landscape fundamentally changed this year. Sustained law enforcement pressure and inter-criminal disputes brought about the downfall of LockBit, a dominant player in the ransomware landscape for many years, and its main rival, ALPHV. Their exits paved the way for the new threat group RansomHub to rise. Furthermore, the healthcare sector which was once thought to be less targeted due to its role, became a prime focus for cybercriminals. Finally, threat actors increasingly shift from traditional encryption-based tactics to pure data extortion, signaling a more streamlined and dangerous approach.

LAW ENFORCEMENT OPERATIONS AND THEIR EFFECT ON THE RANSOMWARE ECOSYSTEM

While cyber security measures offer protection, they are insufficient to counter what has become businesses' foremost cyber threat —ransomware. Efforts to combat attacks are hindered by a lack of international cooperation, as Russia, North Korea, and Iran either tolerate or actively support such activities.


Welcome to Cicada3301!

We are recruiting partners to work in our affiliate program:
- Pentesters.
- Access Advocates.

General information :
- Work in the **CIS** countries is strictly prohibited.
- The affiliate program commission is **20%** of the total payment amount.
- To participate in the affiliate program, you must undergo a mini-interview.
- A wallet for payments is provided in the chat. For amounts over **1.5 million USD,** two wallets are p
- It is strictly prohibited to transfer access to the panel to third parties, except in cases agreed with s

Figure 3 - Dark-web post, specifying recruitment conditions to the Cicada3301! group prohibiting activity against Russian affiliated entities (Commonwealth of Independent States -CIS).

Addressing this threat requires sustained and coordinated international law enforcement efforts such as sharing intelligence, coordinating legal frameworks, and jointly pursuing perpetrators

and taking down their infrastructure. Encouragingly, 2024 saw several effective examples of such operations.

In previous years, takedown operations successfully targeted major ransomware groups such as Hive, Ragnar, and others. In February 2024, Operation Cronos, a coordinated international law operation led by the UK's National Crime Agency (NCA) and the FBI, struck a significant blow to LockBit, the dominant group in the Ransomware-as-a-Service (RaaS) ecosystem. The operation seized LockBit's data leak sites (DLS) and dismantled critical infrastructure, significantly disrupting their operations. Authorities took control of 34 servers across multiple countries, including the Netherlands, Germany, and the United States. The campaign continued through October and arrested key players in Poland and Ukraine while French and US judicial authorities issued indictments. Law enforcement agencies obtained and released LockBit's decryption keys and internal data, exposing the group's operations and affiliate networks to further scrutiny.

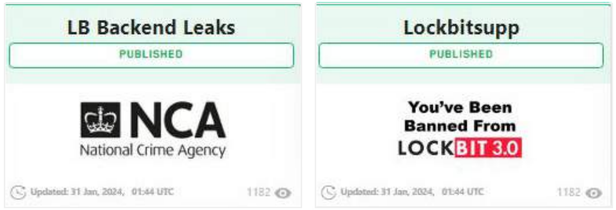


Figure 4 - Screenshots from the LockBit shame-site undermining its reputation (source: NCA).

The operation aimed not only to dismantle LockBit's technical infrastructure but also to tarnish its image in cybercriminal circles. LockBit's reputation was crucial to its operations, as evidenced by its active engagement in criminal forums and media interviews. The group's leader, known as LockBitSupp, frequently interacted on these platforms, promoting their ransomware services and maintaining a public persona. This visibility was integral to recruiting affiliates and assuring victims of their "professionalism" in handling ransom payments and data.

Following Operation Cronos, LockBit's activity significantly declined. Once their internal communications and affiliate identities were exposed, their trust was lost. LockBit attempted to project a "business as usual" image by publishing fake lists of recycled, or victims of other attackers, a phenomenon that has increased with the shift to data-based extortion. Despite LockBit's attempts to re-establish operations, ongoing law enforcement pressure and the loss of credibility within the cybercriminal community hinder their resurgence. However, in the last week of 2024, the group announced a new version, LockBit 4.0. Only time will tell if this marks a resurgence for the criminal organization.

ALPHV was another major RaaS actor to exit the scene. At the end of 2023, they suffered from a law enforcement operation but briefly recovered and aggressively resumed operations against healthcare entities.

In February 2024, an ALPHV affiliate attacked Change Healthcare. The group withheld all $22 million from the affiliate, denying the affiliate's share. The group then faked a seizure notice on their DLS and announced their retirement.

While the removal of these two dominant groups impacted the ransomware landscape in the short and long term, it did little to curb the ecosystem's volume of attacks. In fact, the number of published victims rose steadily. This resilience highlights the nature of RaaS operations: independent affiliates remain largely unaffected by the downfall of a single brand or operator and simply migrate to other platforms. Free of prior allegiances, these affiliates find alternative RaaS groups that offer the necessary infrastructure, leak sites, and support services, ensuring that their pipeline of ransomware attacks remains intact.

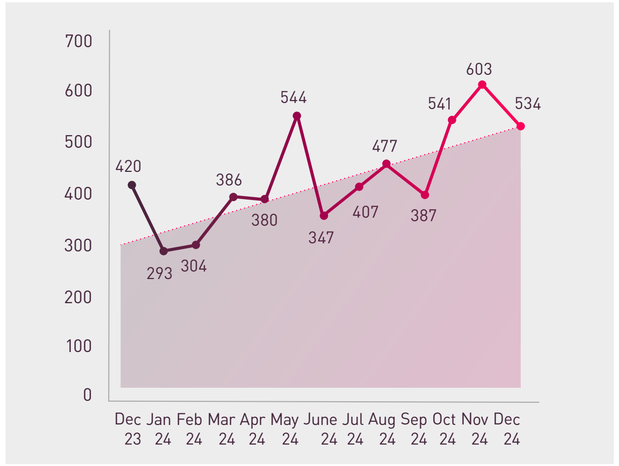
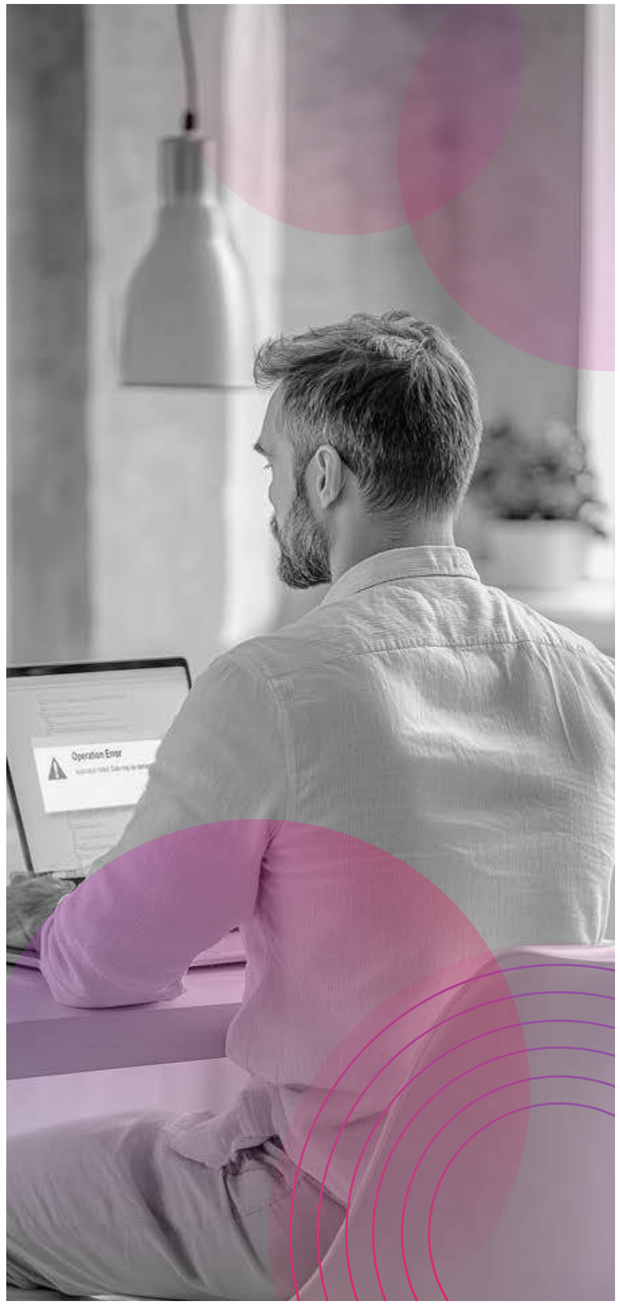


Figure 5 - Total number of victims reported on ransomware data leak sites.



In the immediate aftermath, no single entity could replicate the market dominance previously held by LockBit and ALPHV. While RansomHub seemed poised to assume a leading role, its position was far from guaranteed. Instead, the landscape entered a period of competitive fragmentation, with mid-sized actors, like Akira, Play, Medusa, Dan0n, Hunters, and Bianlian, scrambling to recruit affiliates and build momentum

The fallout from ALPHV's withholding an affiliate's ransom share, combined with LockBit's damaged reputation and the availability of leaked ransomware code, fueled the rise of more autonomous operators. An increasing number of smaller, independent groups emerged, unwilling to rely on established RaaS frameworks or share profits with centralized operators. By leveraging leaked code, these actors customized their own ransomware strains and infrastructures, reducing dependence on major RaaS providers and fostering a more decentralized and competitive ecosystem.

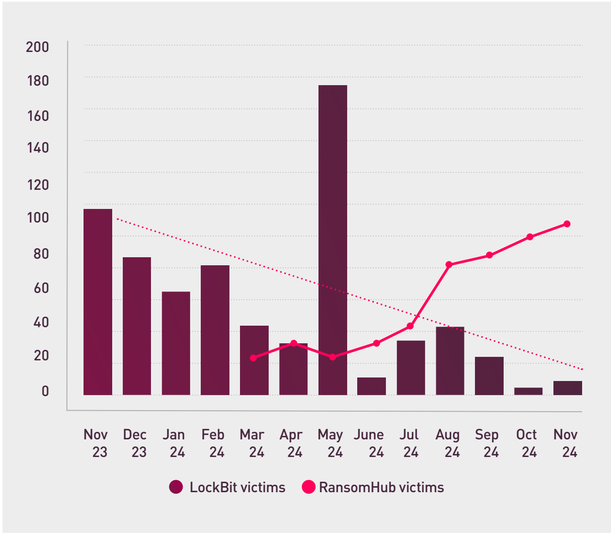


Figure 6 - Data leak sites reported victims of LockBit vs. RansomHub. in 2024

As 2024 closed, RansomHub emerged as the new dominant player, accounting for 16% of reported victims in November. Over 40 other double-extortion ransomware groups remained active during the same period, each maintaining their own data leak sites and targeting new victims.

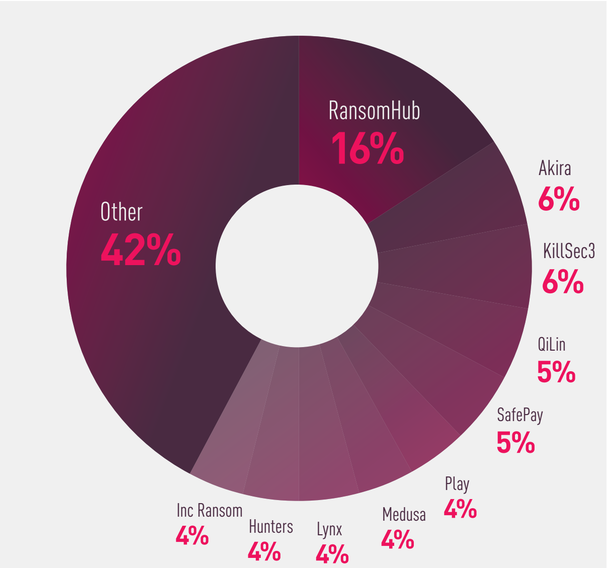


Figure 7 - Data leak sites victims by actor, November 2024.

HEALTHCARE UNDER FIRE

The migration of ransomware groups to targeting healthcare organizations underscores the gradual decline of previously established "ethical" guidelines. In the early months of the COVID-19 pandemic, many RaaS operators publicly declared hospitals and medical providers off-limits. However, over time, these restrictions weakened. Some RaaS administrators adopted a more nuanced approach. While they discouraged outright service disruption, such as encrypting critical systems, they permitted the theft of sensitive medical data. Affiliates could then extort victims by threatening to leak patient information and pressure healthcare entities to pay without directly endangering patients.

This approach deteriorated further after the law enforcement operation against ALPHV. The group openly encouraged affiliates to specifically target hospitals. By February 2024, the healthcare and medical sectors became the most targeted sectors for ALPHV, making up approximately 30% of their reported victims.

Figure 8 - ALPHV permitting affiliates to "block hospitals, nuclear power plants, anything, anywhere." (source).

The critical nature of healthcare operations means that prolonged system downtime is unacceptable due to the risk it poses to patients. As demonstrated by the Change Healthcare attack, this significantly increases the likelihood of ransom payments.

Healthcare and medical organizations now account for 10% of all publicly reported ransomware victims, making healthcare the second most targeted sector in 2024, trailing only the manufacturing industry.

While the high-profile Change Healthcare attack captured global attention, many other significant incidents highlight this troubling trend. In February 2024, a Phobos ransomware attack targeted Romania's healthcare system, directly impacting 25 hospitals and causing operation disruptions at over 100 additional facilities due to its effect on the Hipocrate Information System (HIS). As a result of being disconnected from the internet, hospitals experienced slower medical services, delayed patient care, and significantly reduced operational capacity.

In June, Synnovis, a crucial pathology services provider for major London hospitals, was hit by the Qilin (Agenda) ransomware group. The attack involved a $50 million ransom demand and the leak of approximately 400GB of sensitive data. The breach led to the cancellation of over 6,000 medical appointments and procedures. The disruption also caused a shortage of blood donations in the UK's National Health Service (NHS).

Many healthcare victims are now targeted by ransomware attacks: 19% for Bianlian, 23% for INC Ransomware, and 10% for RansomHub, despite its policy of avoiding non-profit organizations and hospitals (see the image below). This underscores the increasing focus on threat actors in this sector.

Notably, over 65% of healthcare-related victims are based in the US, disproportionately high compared to their share in the broader ransomware ecosystem. The importance of healthcare operations and their limited capacity to withstand extended disruptions make them particularly attractive targets. All indications suggest that this troubling trend will persist into 2025.

Figure 9 - RansomHub official policy from their DLS.

THE SHIFT TO EXTORTION OF DATA EXFILTRATION (DXF)

The encryption phase of a ransomware attack presents significant challenges for attackers. It is inherently "noisy" which increases the risk of detection and interception. Managing multiple victims adds to the complexity as it requires distributing unique decryption keys and providing "customer support" for data recovery. Both tasks are resource-intensive and operationally demanding. Ransomware groups rely heavily on their reputation for reliably restoring encrypted data to maintain victim trust and secure payments. If decryption fails, it undermines this trust and reduces the likelihood of future ransom payouts. Additionally, dependence on encryption increases the affiliates' reliance on RaaS platforms. This reliance can reduce their profits while increasing their exposure to law enforcement agencies.

Victims' willingness to pay ransoms for encryption-based attacks has steadily decreased due to repeated instances where payments failed to lead to data recovery, along with organizations becoming more proficient at maintaining up-to-date backups. Data from Coveware, a US-based ransomware response firm, highlights the trend: **the percentage of encryption-based cases resolved through ransom payments declined from 75% in 2019 to 32% by Q3 2024. In contrast, data exfiltration only extortion maintained a steady payment resolution rate of about 35%.** This shift, combined with increased operation costs of managing decryption efforts, has led many ransomware actors to abandon encryption in favor of DXF-only operations.

10%
OF RANSOMWARE VICTIMS ARE HEALTHCARE

65%
OF HEALTHCARE-RELATED VICTIMS ARE BASED IN THE US

Early adopters of the data exfiltration only trend, such as Karakurt and Lapsus$, paved the way for others to follow. By 2024, established groups like BianLian, a Russian-speaking ransomware group, fully transitioned to DXF-only extortion and abandoned encryption altogether. Similarly, Meow, an older ransomware group previously engaged in double extortion, re-emerged this year, focusing solely on data sales, offering stolen data at different price points, and allowing victims to "buy back" their information to prevent public exposure.

New actors have also emerged exclusively as "data-selling platforms." For example, Bashe (also known as Eraleign), which first appeared in April 2024, operates purely as a data exfiltration only based extortion platform. It offers a dedicated data leak site (DLS) and a negotiation platform without providing encryption services or additional tools.

Figure 10 - Bashe Operation Policy, from their data leak sites.

This approach also created opportunities for false victim claims. Without the visible disruption caused by encryption, threat actors can more easily recycle previously leaked data and falsely claim credit for new attacks. This tactic complicates tracking ransomware campaigns and identifying genuine perpetrators as multiple groups claim responsibility for the same victim.

The rise of data exfiltration-only extortion marks a critical shift in cyber security priorities. Organizations must now focus on strengthening Data Leak Prevention (DLP) strategies by leveraging advanced monitoring and detection systems to identify and mitigate potential breaches earlier. As the financial and operational incentives for data exfiltration-only attacks continue to grow, this trend will likely persist this year as more ransomware groups adopt these tactics to streamline operations and evade detection.

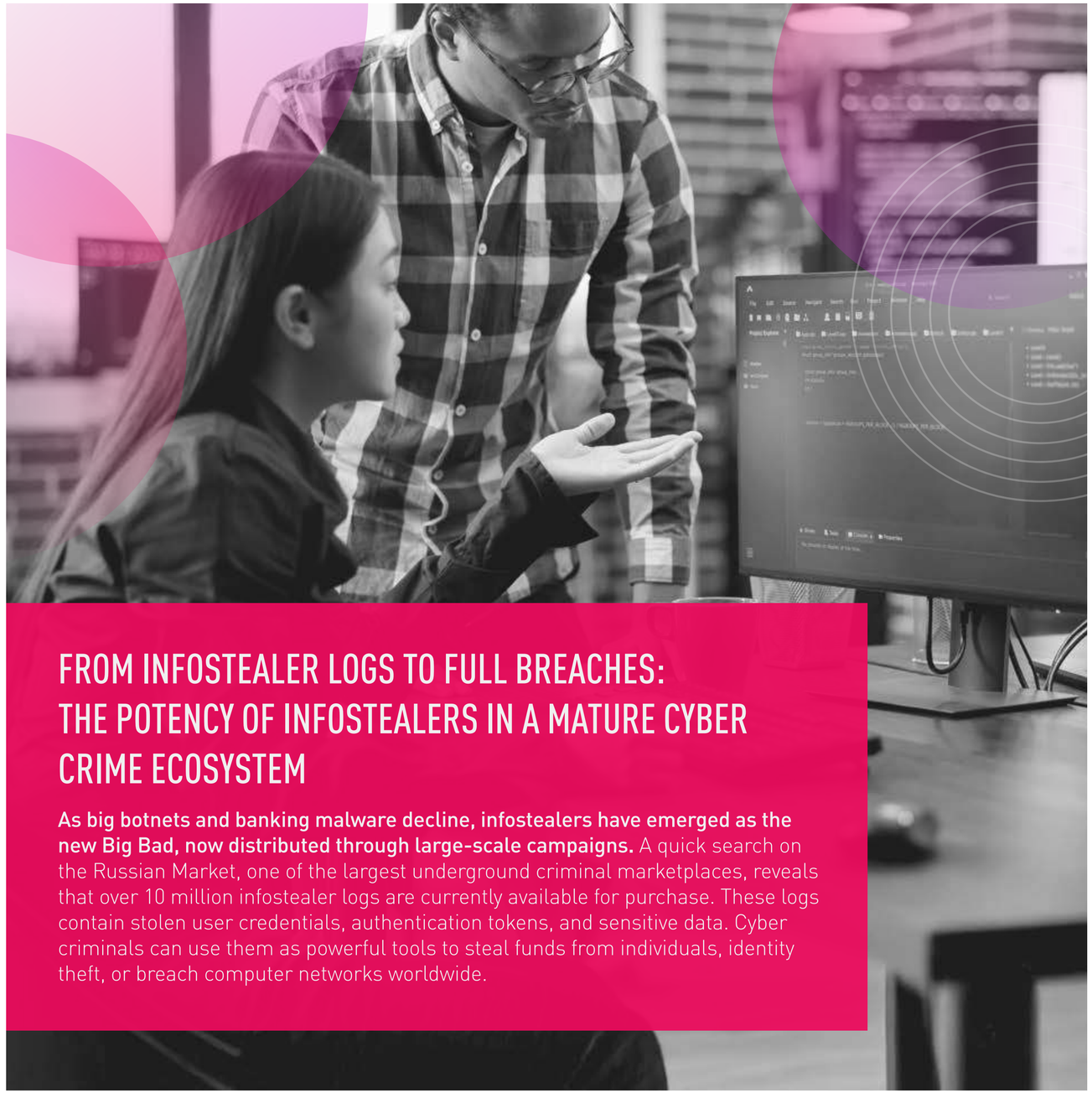
NAVIGATING RANSOMWARE'S EVOLVING LANDSCAPE

The ransomware landscape in 2024 reflects a dynamic and increasingly complex threat environment. Law enforcement successes against major groups have opened the door for new actors, with RansomHub emerging as the most prominent. At the same time, the erosion of ethical boundaries concerning attacks on healthcare organizations highlights a growing ruthlessness among threat actors. Additionally, the strategic shift from encryption-based extortion to DXF introduces new challenges, requiring organizations to adapt their defensive strategies to focus on data protection, monitoring, and rapid threat detection.

"Each year, the ransomware environment becomes progressively complicated. While law enforcement successfully dismantled larger Ransomware as a Service (RaaS) groups, new groups emerged this year. Additionally, the shift from encryption-based extortion to data extortion brings new challenges. However, one thing remains consistent: the need to adapt and enhance data protection, monitoring, and rapid threat detection."

OMER DEMBINSKY

Data Research
Group Manager



FROM INFOSTEALER LOGS TO FULL BREACHES: THE POTENCY OF INFOSTEALERS IN A MATURE CYBER CRIME ECOSYSTEM

As big botnets and banking malware decline, infostealers have emerged as the new Big Bad, now distributed through large-scale campaigns. A quick search on the Russian Market, one of the largest underground criminal marketplaces, reveals that over 10 million infostealer logs are currently available for purchase. These logs contain stolen user credentials, authentication tokens, and sensitive data. Cyber criminals can use them as powerful tools to steal funds from individuals, identity theft, or breach computer networks worldwide.

As we examine the cyber landscape in 2024, infostealers are in the spotlight. This is not only due to the evolution of their methods and tactics but also because the broader criminal ecosystem has matured and specialized, making these threats more effective. Infostealers have gained significant power due to their ability to efficiently manage, quickly process, and sell large quantities of logs. They serve as the first step toward full-scale corporate network breaches. A crucial aspect of infostealer distribution is that it mostly relies on a "spray-and-pray" approach rather than directly targeting corporate networks. Despite this strategy, one of its main goals is to extract credentials for accessing corporate resources on BYOD (Bring Your Own Device). Cyberint, a Check Point company, reports that over 70% of devices infected by infostealers are personal rather than corporate or managed.

DEFINING INFOSTEALERS

Infostealers, often called "stealers", are malware engineered to covertly extract sensitive data from compromised systems, primarily targeting browser data. They can also exfiltrate files from the infected machines and take screenshots. Stealers are spread through phishing emails or malicious downloads. Once they infiltrate a computer, they can harvest a wide range of valuable information that can be used for further cyber crime or fraudulent activities. This includes usernames and passwords, financial details, system configurations, browser cookies, and cryptocurrency wallets. Infostealers are marketed on the Dark Web as Malware-as-a-Service (MaaS), where buyers receive customer support, regular updates, and detailed documentation, lowering the barrier to entry for would-be cyber criminals.

Figure 11 - A darkweb forum thread promoting the sale of a Lumma infostealer.

THE INFOSTEALER MARKET

The infostealer market is robust and highly competitive, with pricing that reflects the product's sophistication and the level of support the developers offer. For example, RedLine Stealer is available for approximately $150 per month, StealC costs around $200, and Lumma's price tag is about $250. Threat actors who operate these malware services, often referred to as "affiliates," purchase licenses and use the stealers in individual infection campaigns within the MaaS model. The data, or "logs," collected by the affiliates, consist of batches of information stolen from individual computers. The logs are then sold or traded on platforms like Telegram or underground criminal marketplaces like the Russian Market, typically for about $10 each. The stolen information fuels illicit activities, including financial fraud, identity theft, and further cyberattacks, thereby perpetuating a broader cyber crime ecosystem.

Figure 12 - Lumma Stealer logs stolen from a French computer for sale on the Russian Market.

Session tokens and cookies are among the most desirable types of data harvested by infostealers. These artifacts are particularly valuable because they provide immediate access to user accounts without needing login credentials. Acquiring "fresh" or recently stolen logs is critical, as active session cookies are time -sensitive. If harvested and sold promptly, they can hijack ongoing sessions and bypass Multi-Factor Authentication (MFA) mechanisms that many security systems rely on. Many cyber criminals often analyze data obtained from infostealers to uncover credentials for corporate accounts. These credentials can provide an initial foothold within a corporate network or grant access to critical resources. Targets often include credentials and tokens for VPN accounts, Microsoft 365 accounts, corporate messaging systems, and more.

To address this significant security risk, Google introduced App-Bound encryption in July. However, by September, several infostealers had already adopted techniques to bypass this protection and decrypt the sensitive stolen data.

The need for rapid exploitation highlights another key area where infostealer vendors compete: the efficient presentation and classification of stolen data. Advanced operator panels and download mechanisms are developed to provide affiliates with quick and clear access to the logs. Some systems offer automatic streaming of logs to Telegram channels, enabling near real-time exploitation of live session tokens. Effective user interfaces not only facilitate rapid access but also automatically parse and highlight high-value credentials, enhancing the efficiency and appeal of the malware to affiliates.

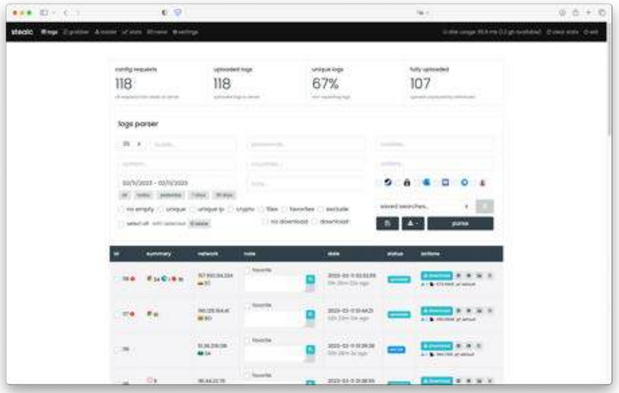


Figure 13 - StealC panel view.

The infrastructure supporting these malicious activities is often comprehensive and maintained by the MaaS vendors themselves. This infrastructure can include a mechanism for panel authentication, command-and-control (C2) servers that deliver additional plugins and updates, and secure locations for storing and downloading stolen data. Dependency on extensive infrastructure can sometimes prove to be the malware's Achilles' heel, as law enforcement agencies can target and seize these resources to disrupt MaaS operations.

THE DISTRIBUTION OF INFOSTEALERS

Infostealer campaigns are driven by affiliates who purchase licenses from developers and independently operate infection campaigns. **To spread the malware, they use creative methods, including phishing emails, malvertising, distributing fake or**

cracked software, deceptive advertisements, and counterfeit websites mimicking legitimate platforms like cryptocurrency services, AI tools, and groupware applications. Affiliates may also exploit platforms like GitHub to host malicious repositories, as seen in campaigns using fraudulent accounts to disseminate popular infostealers. Other tactics involve phishing templates that target users seeking cracked software, fake CAPTCHA pages designed to trick users into downloading malware, and malicious Google ads that redirect to counterfeit download sites. Unlike developers, who focus on creating and updating the malware, the affiliates entirely determine the distribution, resulting in a wide range of innovative infection campaigns.

MONETIZATION AND THE CYBER CRIMINAL ECOSYSTEM

To understand the full impact of infostealers, we must examine their role within the broader cyber criminal ecosystem. Many infostealer operators depend on clients and effective distribution channels to monetize the data they steal. Underground markets and Telegram channels provide immediate platforms where sellers can offer their stolen data, and buyers can efficiently search for specific logs that suit their objectives.

Initial Access Brokers (IABs) leverage this information to gain initial footholds in corporate networks. Access obtained through stolen credentials is highly valuable and can be further monetized. In many cases, IABs resell access to carefully selected targets on other forums, attracting ransomware affiliates keen to exploit these opportunities. These affiliates then deploy ransomware, often acquired from Ransomware-as-a-Service (RaaS) providers, to execute their attacks.

Figure 14 - Ad offering access to corporate networks.

The funds generated from successful ransomware attacks fuel this entire ecosystem. The stolen personal data offers other lucrative avenues for cyber criminals. Personally Identifiable Information (PII), financial details, and credit card numbers can be used for identity theft, fraud, and unauthorized transactions resulting in Business Email Compromise (BEC). All these activities rely on a mature and functioning criminal infrastructure that facilitates the exchange, sale, and exploitation of stolen data.

90% OF BREACHED COMPANIES PREVIOUSLY HAD CORPORATE CREDENTIALS LEAKED IN A STEALER LOG

Credentials and session cookies stolen from employee home computers can be used to breach corporate networks. One study revealed that 90% of breached companies had corporate credentials leaked in a stealer log before the breach. This statistic underscores the critical role that infostealers play in enabling more significant cyber attacks and emphasizes the importance of addressing this threat within the broader context of cyber security.

Earlier this year, the Snowflake mega data breach exposed sensitive information from over 165 organizations, including Advance Auto Parts, Ticketmaster, and Santander Bank,

affecting millions of customers. The breach most likely started with credentials extracted by infostealers and sold online.

ANALYSIS OF INFOSTEALERS IN THE WILD

An analysis of logs offered for sale on platforms like the Russian Market reveals which infostealers are most prolific in terms of harvested data. Lumma Stealer, first reported in 2022, is currently the most prominent infostealer, with the highest number of logs available for sale. RisePro, Vidar,

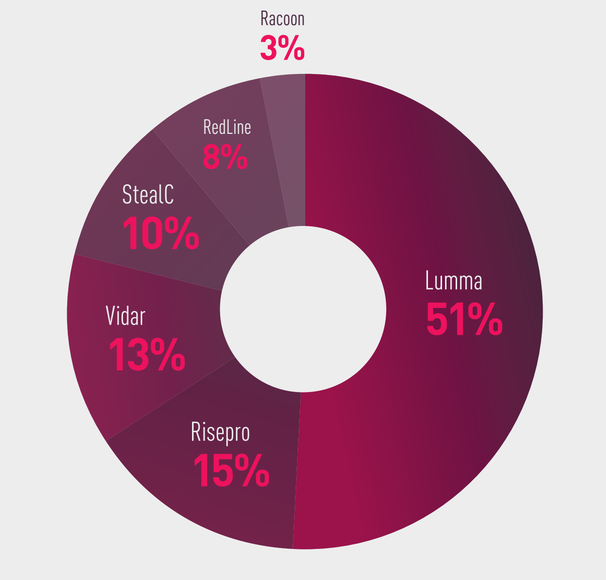


Figure 15 - Logs on Russian Market by infostealer family (November 2024).

and StealC follow it. This data suggests that these malware families have been particularly effective in recent campaigns or have extensive distribution channels.

Insights from the analysis of Check Point gateway data reveal a different perspective on infostealer activity. In these datasets, AgentTesla emerges as the most active infostealer, closely followed by FormBook (detailed statistics are provided in the next chapter). The differences between these data sources can be attributed to the types of victims analyzed. Check Point data primarily focuses on corporate entities, whereas Russian Market data encompasses a broader spectrum of victims, most of whom are personal device users.

Further data analysis from Cyberint, a Check Point company, highlights the top URL credentials stolen from infected machines. While many of these URLs belong to major internet services and social media platforms, as expected, other frequently visited sites include Roblox, Discord, Twitch,

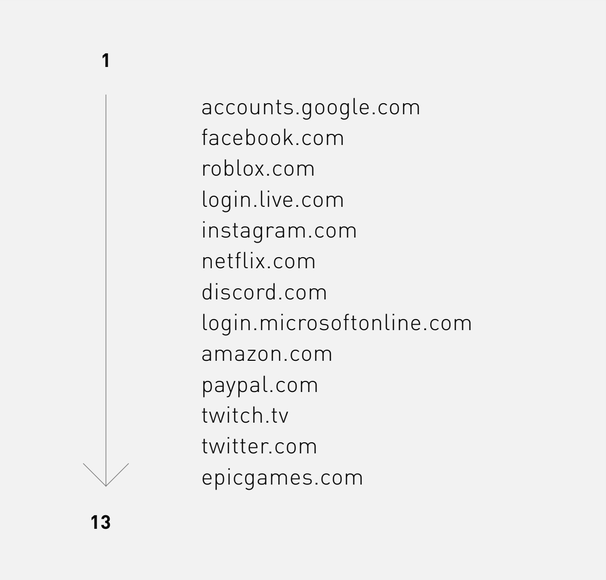


Figure 16 - Top URLs that appear in infostealer data, according to data from Cyberint, a Check Point company.

and EpicGames. This suggests that "gamers" may be more susceptible to infostealer infections, likely due to less stringent internet hygiene practices in these communities.

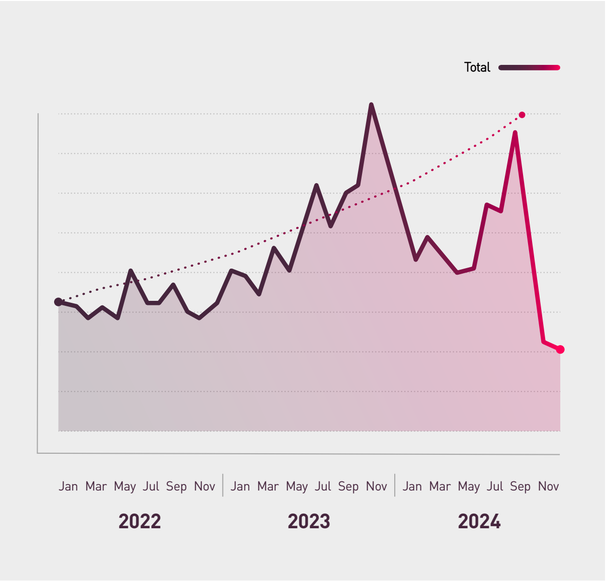


Figure 17 - RedLine logs found on tracked Telegram channels 2022-2024 (Cyberint, a Check Point Company).

Another significant observation is the growth trajectory of specific malware families. For example, the prevalence of the RedLine Stealer has more than quadrupled over the past three years.

The increase in infostealers can be attributed to the decrease in the popularity of botnets. In May, a coalition operation called "Endgame" targeted the infrastructures of botnets used to distribute malware, focusing on groups such as IcedID, Smokeloader, Pikabot, Bumblebee, SystemBC, and Trickbot. As a result of Endgame, over 100 servers were dismantled, and more than 2,000 domains used by these cyber criminals were seized. These botnets previously played a central role in malware distribution, and their disruption has dramatically impacted the ecosystem, indirectly contributing to the rise of infostealers.

Infostealers' popularity has not gone unnoticed by international law enforcement coalitions. Two closely related infostealer families, RedLine and Meta, were the focus of a major law enforcement operation known as "Magnus." In October, this operation resulted in the seizure of multiple servers and domains associated with these malware strains.

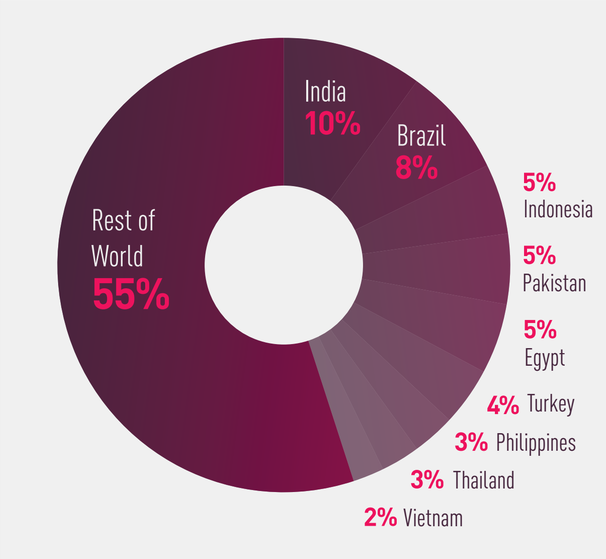


Figure 18 - Logs on the Russian Market, by country of origin.

Geographical analysis of the logs offered for sale also yields important insights. A substantial portion of the logs in the Russian Market originates from India and Brazil.

Although Infostealer technology hasn't drastically evolved over the past year, the environment in which the malware operates has transformed dramatically. Infostealers now hold a prominent position in the cyber offensive landscape. The maturation of the market for infostealer products and the logs they generate enables IABs to efficiently search for and exploit valuable credentials, ultimately enabling them to breach corporate networks.

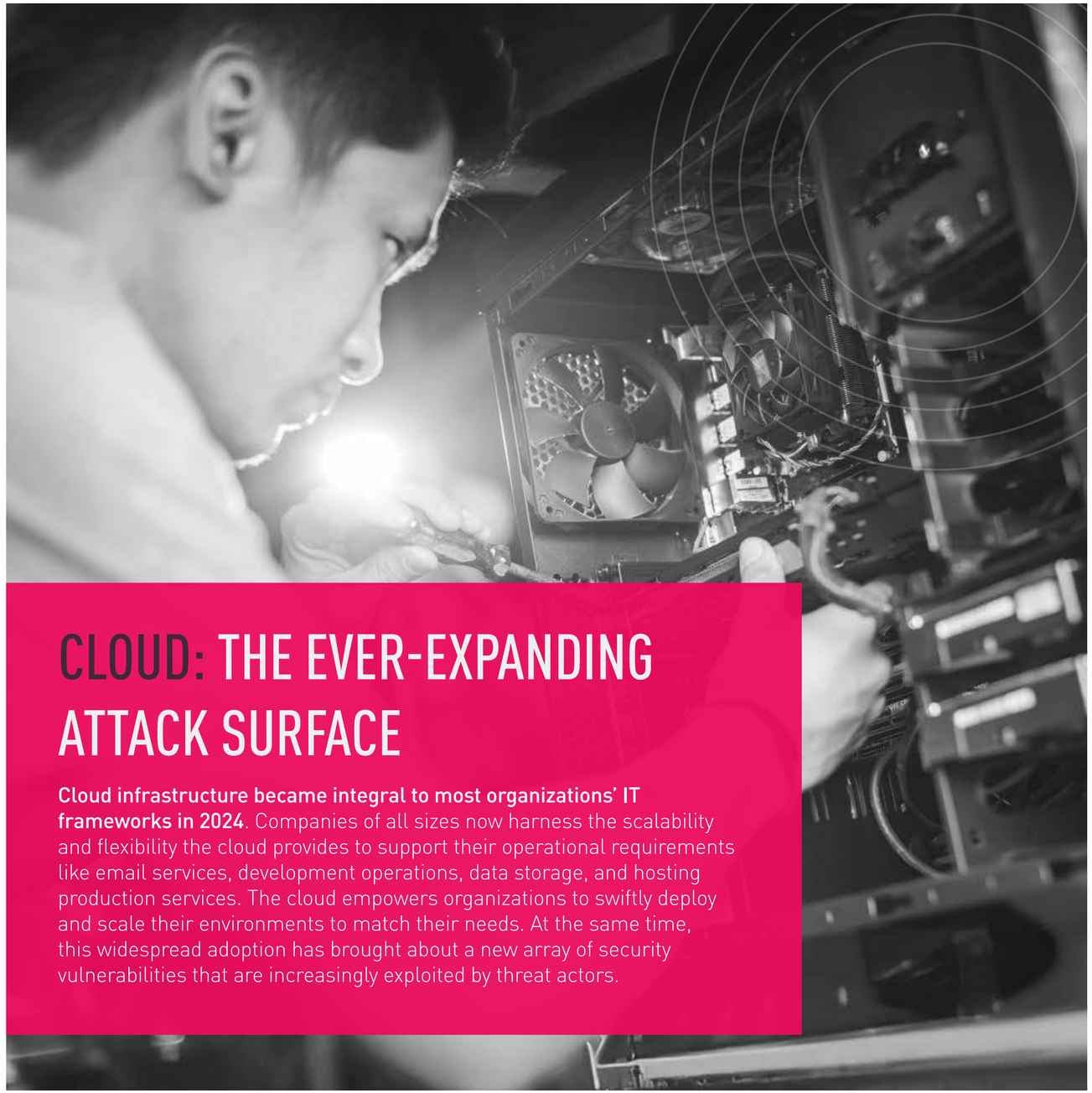
COMBATING INFOSTEALERS: STRENGTHENING CORPORATE SECURITY IN THE AGE OF REMOTE WORK

The potential corporate attack surface has expanded with the widespread adoption of remote work and BYOD policies as employees access corporate assets from personal devices, extending business networks to individual home environments. Logs' rapid delivery and searchability allow IABs to quickly identify potential entry points to corporate networks, often bypassing MFA mechanisms with stolen valid session cookies found on personal devices.

To combat these evolving threats, businesses must extend their security measures to cover the expanded surface area, including employee access points. Organizations should actively search for indications of company-related artifacts being sold on criminal markets to preempt potential breaches. By broadening protective strategies and staying vigilant, companies can strengthen their defenses against the sophisticated and interconnected threats posed by modern infostealers.

> Following the decline of the big botnets, infostealers have become a significant and wide-scale threat. They offer cyber criminals efficient ways to steal credentials and session tokens, contributing to financial fraud and identity theft and acting as an entry point to corporate networks. As companies increasingly adopt remote work and bring-your-own-device (BYOD) policies, it is essential that they implement protective strategies.

SERGEY SHYKEVICH
Threat Intelligence
Group Manager



CLOUD: THE EVER-EXPANDING ATTACK SURFACE

Cloud infrastructure became integral to most organizations' IT frameworks in 2024. Companies of all sizes now harness the scalability and flexibility the cloud provides to support their operational requirements like email services, development operations, data storage, and hosting production services. The cloud empowers organizations to swiftly deploy and scale their environments to match their needs. At the same time, this widespread adoption has brought about a new array of security vulnerabilities that are increasingly exploited by threat actors.

CLOUD ADMINISTRATION'S COMPLEXITY

The complexity of administering cloud infrastructure adds a significant layer of vulnerability that cannot be resolved with a simple patch. **The rapidly evolving ecosystem and the multitude of cloud providers, each offering dozens of services, terminologies, and security mechanisms, create complexity that is hard to navigate.** As a result, administrators are often overwhelmed by the amount of settings and configurations required to secure their environments effectively. This leads to the exposure of resources online or penetrable environments that allow easy privilege escalation paths.

An example of such administrative complexity can be seen with Non-Human Identities (Service Accounts, API Keys, Built-in Users, etc.), which proved hard to secure. In January 2024, Microsoft failed to secure its own Azure environment when an advanced nation-state threat group, Midnight Blizzard, breached Microsoft's production environment via misconfigured OAuth Application and Service Principles. This allowed attackers to pivot from testing to production environments and access internal systems, source code, and Microsoft executives' emails.

Known misconfigurations and poor security practices continue to play a significant role in driving large-scale data breaches. For example, in India, 500GB of personal information and biometric data of millions of individuals, including law enforcement and military personnel, were exposed on a misconfigured S3 bucket. Microsoft's S3 bucket alternative, Azure Blob Storage containers, is also susceptible to misconfigurations. A Fujitsu employee publicly exposed vast amounts of sensitive data, including private client information, emails, AWS keys, and plaintext passwords. BMW likewise suffered from an exposed storage container, leaking secret keys for accessing private buckets and credentials for other cloud services.

In the realm of poor API security practices, the developers of the Rabbit R1—an AI-driven personal assistant device—were notified after hard-coded API keys for third-party services were found in their codebase. These keys were overly permissive, essentially granting the ability to read all chat responses from every customer, potentially revealing sensitive information.

The absence of robust authentication and access controls in some organizations—particularly the lack of Multi-Factor Authentication (MFA) for cloud services—contributed to a significant data loss incident this year. Attackers targeted Snowflake, a cloud data warehousing platform, using usernames and passwords obtained through various infostealers. This allowed them to access the Snowflake accounts of at least 165 companies, exfiltrate sensitive data, and issue extortion demands.

THE HAZARDS OF HYBRID ENVIRONMENTS

Integrating on-premises resources with cloud services through Identity and Access Management (IAM) providers, such as Microsoft Entra ID, has become standard practice. These configurations aim to streamline IAM and enable Single Sign-On (SSO) authentication. **However, these integrations have also become prime targets for cyber attacks given their ability to facilitate bidirectional lateral movement.** While organizations benefit from distributing their data and resources across cloud and on-premises systems, attackers exploit the same pathways to deploy destructive attacks, exfiltrate sensitive data, or establish backdoors within organizations.

Companies using cloud-based email services like Microsoft 365 have discovered that compromised on-premises networks can also expose their cloud assets. When attackers gain control of an on-premises environment, they can pivot to cloud environments through several pathways like Azure AD Connect servers (via Microsoft Entra Connect Sync user) or hybrid user accounts. For example, in 2024, the financially motivated threat actor Storm-0501 launched multi-stage attacks that compromised hybrid cloud environments, performed lateral movement from on-premises to the cloud, and deployed backdoor accounts before ultimately launching ransomware across the network. The same tactic was used in 2023, when an Iranian-based threat group, Mango Sandstorm (aka Mercury) and Storm-1084, targeted Israeli organizations. The attackers leveraged the pivot to cloud environments to dump email conversations, send emails, and deploy destructive attacks on cloud assets.

In another case, a financially motivated threat actor named UNC3944 (aka Scattered Spider) exploited highly privileged Okta SSO accounts to extend their intrusion from on-premises infrastructure to multiple cloud and SaaS applications, including vCenter, CyberArk, SalesForce, Azure, CrowdStrike, AWS, and GCP. The attacker could then perform reconnaissance inspections of the Okta web portal to identify available applications, perform role assignments to these applications, and thus move laterally through multiple cloud providers and victims' assets.

SSO ACCOUNTS UNDER ATTACK

Securing SSO accounts has become an increasingly concerning and daunting task. **Threat actors, especially advanced threat groups, are conducting large-scale credential stuffing and "low and slow" brute-force attacks on SSO providers and cloud services**. In April 2024, Okta researchers observed a significant credential stuffing operation against its service, where attackers employed residential proxy services and other anonymizers to avoid detection. Similarly, Microsoft researchers reported an advanced Chinese-speaking group that leveraged thousands of compromised SOHO devices to execute low-volume password spray attacks on accounts behind Microsoft's SSO, attempting only one or two passwords per day per user account.

As corporations depend on external SSO providers to protect against brute-force attacks and other malicious techniques, they also trust the providers' logs and global visibility to detect suspicious activity. This dependency raises concerns about reliance on third-party security practices, manifested in Microsoft's September report that some customers received only partial log collection due to a systems issue.

THE POPULARITY OF AI

AI also impacts the cloud, as generative AI (GenAI) solutions are offered as a service by all major cloud service providers (CSPs). **Companies choose large language model (LLM) solutions from CSPs instead of using GenAI services like ChatGPT directly via an API for various reasons.** For one, they can build, train, and deploy custom models tailored to their specific business needs or use Retrieval-Augmented Generation (RAG) to integrate their proprietary knowledge bases and datasets. Another reason is data privacy and protection; by leveraging CSP-based solutions, companies have greater control over their data, ensuring that chat content is not used to train public models.

Naturally, threat actors will find ways to exploit these new technologies for their own financial benefit. Until recently, actors mainly focused on hijacking cloud resources to perform crypto jacking (crypto mining) on a single vulnerable server or a Kubernetes cluster. This year, attackers found a new opportunity called LLMjacking. After a cloud account is compromised, attackers take control of existing hosted LLM models or attempt to deploy new ones. In one instance, attackers used an LLM proxy to resell access to these LLMs to third parties. In another case, attackers combined LLM jailbreaks—a technique to remove limitations on banned chat topics—to sell uncensored role-playing chatbot characters that were NSFW.

As state-affiliated threat groups from Russia, China, and Iran were "caught" by Microsoft and OpenAI abusing ChatGPT to research advanced topics, create tools, and find vulnerabilities, some threat actors may pivot to private LLM instances for improved operational security.

SECURITY CHALLENGES IN CLOUD INFRASTRUCTURE

This year's incidents underscore the critical security challenges emerging from the widespread adoption of cloud infrastructure. Complex administration, misconfigurations, and vulnerabilities in hybrid environments have led to significant breaches. As cloud technologies continue to evolve, so will the tactics of those seeking to exploit them. Proactive measures will be critical to protecting ever-complex cloud environments.

"As cloud offerings continue to grow, so does the cloud attack surface. Recent incidents highlight the need for continuous posture management and proactive threat prevention across hybrid and multi-cloud environments to detect and block sophisticated attacks"

MICHAEL ABRAMZON

Threat Intelligence
and Research Architect

THE EVOLVING THREAT OF EDGE DEVICES AND ORBS

Over the past year, both cyber criminals and state-sponsored actors have significantly increased their exploitation of edge devices as an initial access vector. Edge devices, like routers, firewalls, and VPN appliances, are particularly appealing given their lack of dedicated security solutions. They are often exploited to set up anonymization infrastructure commonly referred to as Operational Relay Boxes (ORBs). ORBs represent a type of network infrastructure that cyber threat actors use to anonymize and relay communications across various devices, many of which are compromised, creating covert channels that evade detection.

Traditionally, edge devices have been a primary interest for state-sponsored actors, especially those associated with Chinese threat groups. **However, cyber crime groups have increasingly targeted these assets, adopting similar tactics to achieve financial gains.**

In 2024, the number of disclosed zero-day vulnerabilities affecting edge devices significantly increased, with over a dozen specifically targeting various vendors' devices. These vulnerabilities received a CVSS risk score of eight or higher, underscoring their critical severity and potential impact.

A notable development is the rise of complex botnets used as ORBs. One of the most sophisticated is the Raptor Train botnet, orchestrated by the Chinese APT group Flax Typhoon, which assembled over 200,000 compromised devices, including small office/home office (SOHO) routers, NAS systems, and IP cameras. Organized into multi-tiered layers, the botnet's structure supports a command-and-control (C2) system through the "Sparrow" platform, enabling remote operations, DDoS attacks, and espionage. The attackers leverage both zero-day and known vulnerabilities, creating a scalable, persistent attack infrastructure with global reach. Through these devices, Flax Typhoon maintains operational control, posing significant risks for both public and private sector entities.

Flax Typhoon is not the only Chinese-aligned actor operating through ORBs. Another state sponsored actor linked to China is Volt Typhoon, known for targeting critical US infrastructure. This group has operated through a different network to hide its activities. The KV-botnet is a sophisticated network of compromised SOHO routers and firewall devices that primarily target end-of-life (EoL) equipment from manufacturers like Cisco and NetGear. This network is used by several Chinese actors, complicating attribution efforts.

In addition to state-affiliated actors, **financially motivated attackers also use proxy services powered by compromised IoT and EoL devices**. The Faceless proxy network, built upon a legacy botnet called TheMoon, comprises over 40,000 compromised devices. Cyber criminals use these older routers as anonymizing nodes to obscure malicious activity like data exfiltration and credential stuffing. The reliance on EoL devices underscores a major risk: thousands of unsupported devices remain vulnerable to compromise, providing attackers with a resilient infrastructure that circumvents conventional defenses.

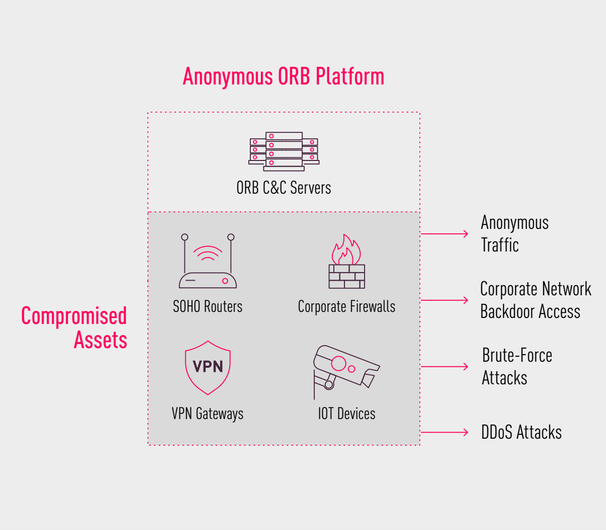


Figure 19 – ORB infrastructure overview.

This year, **corporate edge devices increasingly faced zero-day exploitation as attackers continued repurposing them for broader network penetration.** In early 2024, high-severity vulnerabilities were discovered in Ivanti Connect Secure and Palo Alto Networks' PAN-OS GlobalProtect, allowing for remote code execution and multifactor bypass. Both nation-state actors and ransomware groups exploited these devices as entry points for accessing and compromising sensitive environments. Such zero-day exploits in edge devices have significant consequences as these devices are not easily patched, given their critical role in the main network flow. Patching edge devices can shut down network services for some time, which can lead to considerable operational consequences.

Some actors have turned to exploiting edge devices as a methodology. Magnet Goblin, a financially motivated actor that first emerged in 2024, focuses on rapidly exploiting newly disclosed vulnerabilities in widely used edge devices. Their campaigns have targeted Ivanti Connect Secure VPNs and popular software like Magento and Qlik Sense to deploy custom malware. Magnet Goblin's toolkit includes NerbianRAT, a cross-platform remote access Trojan (RAT), and MiniNerbian, a Linux backdoor. The actor's emphasis on swiftly exploiting edge device vulnerabilities highlights a broader trend in financially motivated attacks against these critical components, using tools like WARPWIRE, a credential-stealing JavaScript to access sensitive data in real time.

Check Point's SSLVPN appliance was also targeted through the path traversal vulnerability identified as CVE-2024-24919. This exploit allowed attackers to access and read files on SSLVPN devices, including sensitive password hashes and configuration files. When these devices are configured with weaker authentication methods, like username-and-password access, they are prone to unauthorized data reads. This attack demonstrates the evolving focus on edge devices by different threat actors, who can rapidly exploit any emerging vulnerabilities.

While cyber criminals have improved their exploitation of edge devices, state-sponsored actors continue demonstrating their technological superiority. They use zero-day exploits

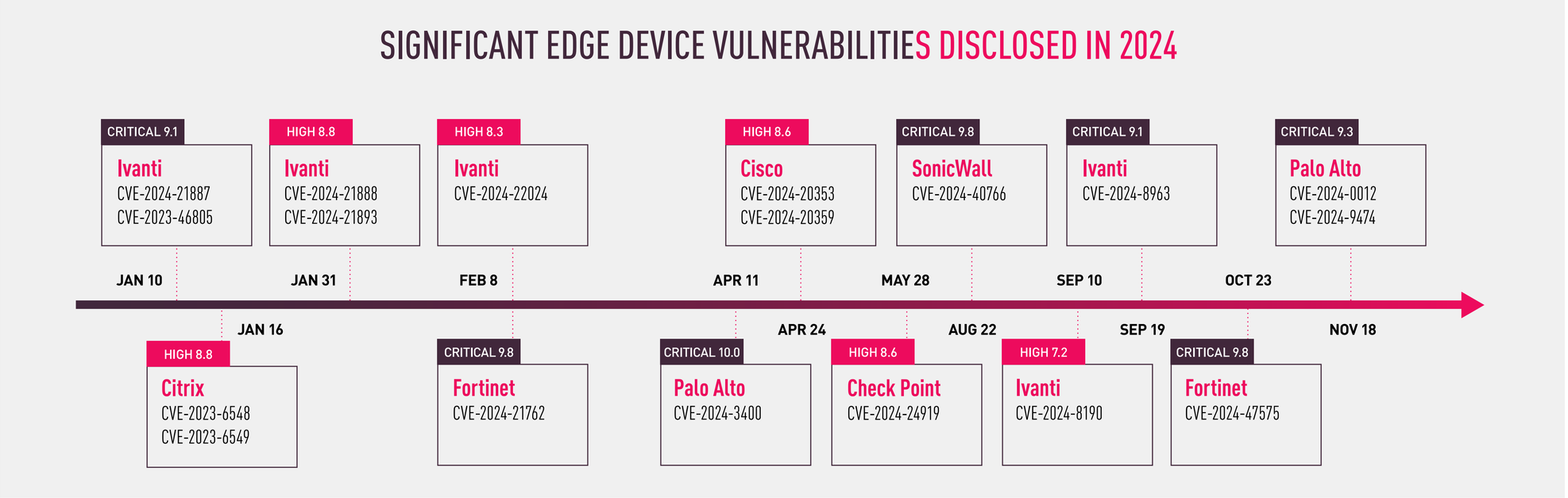


Figure 20 – Timeline of disclosed edge device vulnerabilities in 2024.

to deploy custom implants tailor made for specific devices. Cisco's Adaptive Security Appliances (ASA) were targeted in a sophisticated campaign known as ArcaneDoor. Exploiting weaknesses in ASA, this operation enabled nation-state actors to infiltrate government and industrial networks, obtain sensitive information, and set up long-term espionage capabilities. Throughout the campaign, the threat actors leveraged a unique implant, custom-made for the affected devices, indicating significant research and development efforts.

Many custom implants for various security products were discovered. One such effort, codenamed Pacific Rim, suggests Chinese actors have been targeting perimeter devices, such as Sophos firewalls and VPN gateways, for several years. Pacific Rim used various tactics to exploit vulnerabilities in internet-facing services, including CVE-2020-12271 and CVE-2022-1040, and enabled access to critical network points. Once compromised, these devices become part of an ORB network that supports covert command and control (C2) channels that evade detection. The attackers used advanced techniques in their operation, such as rootkit implants and obfuscated hotfixes, to maintain persistence and conceal their presence on compromised devices. This allowed the operation to pivot from edge devices to internal network assets, focusing on high-value targets across the Indo-Pacific region. Pacific Rim's sustained and strategic approach emphasizes the vulnerabilities in edge devices, particularly in sectors where comprehensive monitoring and timely patching are difficult to achieve.

While those sophisticated backdoors have become more common over time, it's important to note that many "classic" threats from unsecured edge devices are still present in the cyber ecosystem. In September 2024, CloudFlare began defending against a months-long DDoS campaign that was disclosed as the largest attack volume ever reported by any organization. These high packet rate attacks appear to originate from multiple types of compromised devices, including MikroTik devices, DVRs, and web servers. The high bitrate originated from a large number of compromised ASUS home routers, which were probably exploited using a critical vulnerability. Currently, this large-scale attack has not been attributed to any state-sponsored actor or cyber crime group.

In 2024, large-scale botnets built from vulnerable and unmonitored edge devices have become an indispensable part of advanced threat actors' arsenals, whether used for anonymization, network exploitation, persistence, or record-breaking DDoS attacks.

ORBs and botnets like Raptor Train and Faceless use decentralized C2 infrastructures that can dynamically switch between compromised devices. This allows attackers to rotate nodes and effectively evade detection. Some malware variants, like TheMoon, employ advanced evasion strategies, including in-memory-only execution and frequent IP switching, which further complicates mitigation efforts. Together with the ongoing cycling of infected devices, these tactics present significant challenges for defenders.

Originally a tactic used by nation-state actors for covert infiltration, **the strategy of targeting edge devices has now been co-opted by financially motivated attackers leveraging off-the-shelf toolkits**. This approach has enabled breaches of high-value targets while remaining undetected for extended periods. The persistent targeting of edge devices highlights a critical security gap. Publicly exposed network devices will remain at considerable risk without prompt patching, comprehensive monitoring, and robust detection systems.

> "With thousands of unsupported devices at risk of attack, threat actors have access to infrastructure that bypasses traditional security measures. Timely patches, thorough monitoring, and strong detection systems will be crucial"

LOTEM FINKELSTEIN

Director, Threat Intelligence and Research

04

GLOBAL ANALYSIS

THE STATE OF CYBER SECURITY 2025

CYBER ATTACK CATEGORIES BY REGION

GLOBAL

39%	19%	6%	2%
Multipurpose Malware	Infostealer	Mobile	Crypto Miners

AMERICAS

32%	15%	4%	1%
Multipurpose Malware	Infostealer	Mobile	Crypto Miners

EMEA

42%	20%	6%	2%
Multipurpose Malware	Infostealer	Mobile	Crypto Miners

APAC

42%	28%	8%	5%
Multipurpose Malware	Infostealer	Mobile	Crypto Miners

Figure 1 - Percentage of organizations affected by malware type in 2024.

Figure 1 shows attacks according to malware type. These numbers exclude general scans and only deal with direct attacks, which enabled us to classify the type of malware and its intention.

In 2024, there was a notable increase in attempted attacks by both Infostealers and Multipurpose malware. Multipurpose malware (RATs, botnets, and bankers) is frequently used in the initial stages of an attack to drop additional tools and expand the attackers' control over the breached system. It's therefore unsurprising that this is the most common malware type, with 39% of organizations affected in 2024. This figure marks a significant 25% increase compared to 2023 when only 31% of organizations faced similar attempts.

58% INCREASE OF INFOSTEALER INFECTION ATTEMPTS IN 2024

Infostealer infection attempts also increased significantly, from 12% to 19% of organizations affected in 2024, a 58% increase. The rise in infostealer attacks, typically distributed in mass campaigns rather than targeting specific victims, reflects a maturing ecosystem and an increasing demand for stolen infostealer logs containing credentials, session cookies, and other personal information. Infostealers are used for multiple malicious activities, ranging from direct fraud via stolen financial credentials to leveraging stolen session cookies for breaching corporate networks. Additional details on recent developments in the infostealer ecosystem are provided in the Trends chapter, and a dedicated data section will be provided later in this chapter.

Crypto miner attacks, installed without the system owners' knowledge, dropped significantly, from 9% to just 2% of organizations affected. Most crypto miners we have seen target the Monero cryptocurrency, whose mining difficulty (computational effort required to mine Monero) nearly doubled this year, rising from an average of 260G in January to nearly 450G in December. This critically decreases their profitability. Further details about crypto miners are presented in a dedicated section.

GLOBAL THREAT INDEX MAP

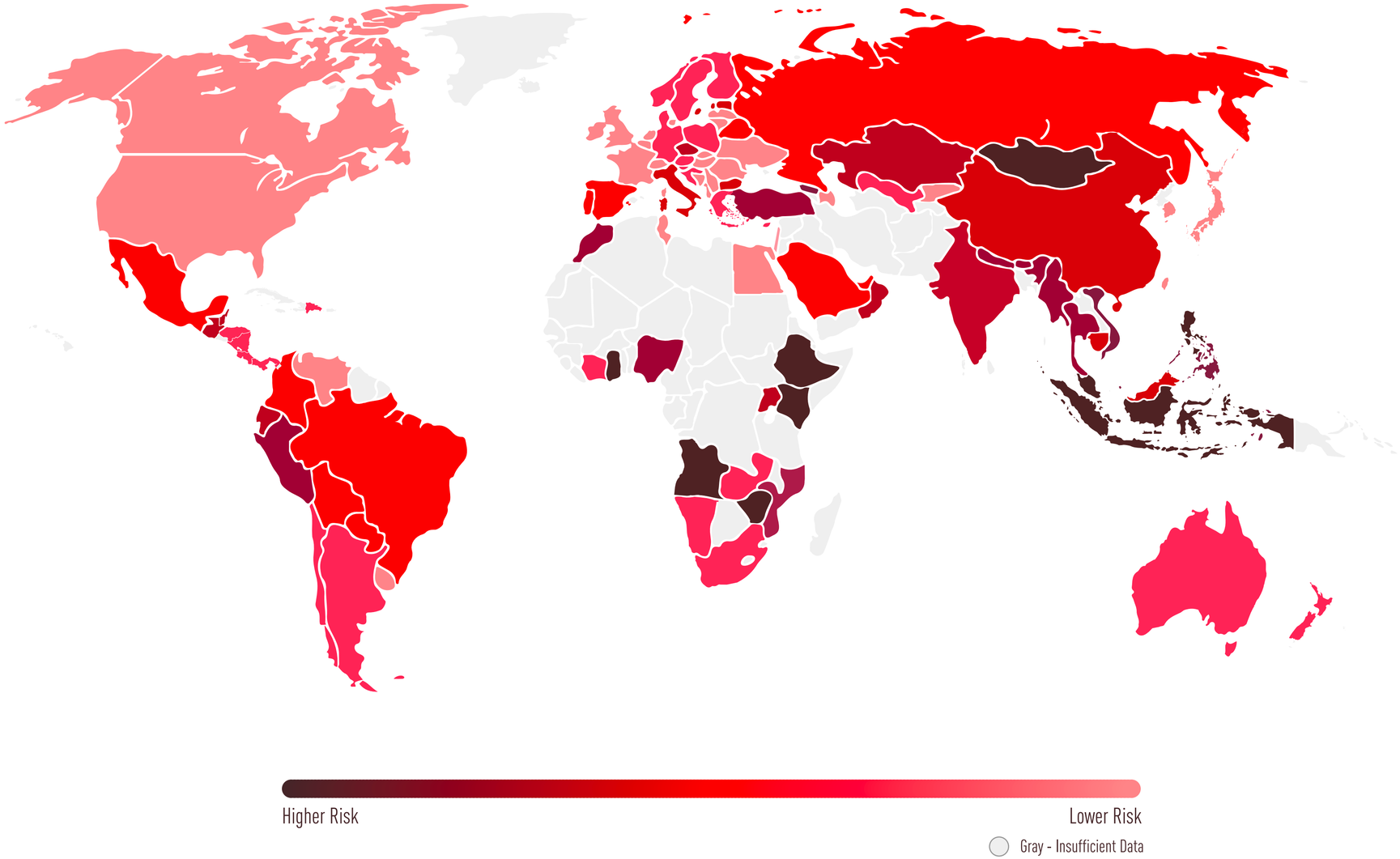


Figure 2 - The map displays the cyber threat risk index globally, demonstrating the main risk areas around the world.

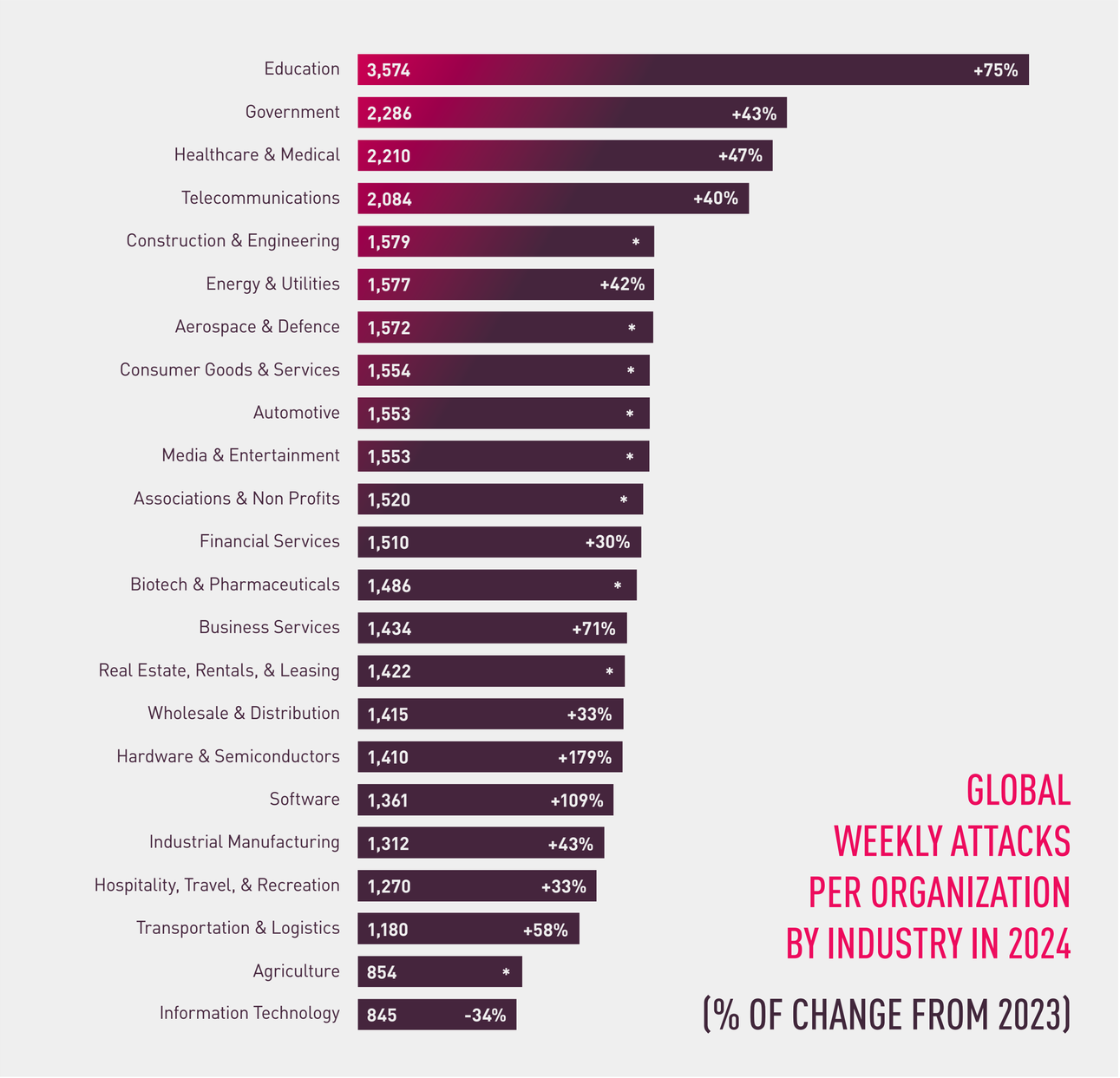


Figure 3 - Global average of weekly attacks per organization by industry in 2024 [% of change from 2023].
[*] Newly introduced sectors which were not part of the previous report.

ATTACKS PER ORGANIZATION

The overall global attacks against organizations significantly increased in the past year, with the average number of weekly attacks per organization reaching 1,673. This is 44% higher than in 2023. Figure 3 illustrates the average number of weekly attacks per organization by industry. In 2024, there was a significant increase in the number of attacks per week across most sectors. The education sector experiences the highest volume, with a 75% year-over-year (YoY) increase, surpassing an average of 3,574 weekly attacks. Education institutions were specifically targeted for personal information collection. This persistent rise in attack rates impacts universities, schools, and educational departments and services.

The healthcare sector also witnessed a 47% increase in average weekly attacks. Cyber criminals are increasingly abandoning their previous self-imposed prohibitions against targeting healthcare services. The health sector is particularly vulnerable to prolonged service disruptions (as noted in the earlier Ransomware section) and the highly sensitive nature of patient data they hold.

The technological supply chain sector, including software, hardware, and semiconductor companies, also experienced a significant surge in cyberattacks. Notably, the hardware and semiconductor industries saw the sharpest rise, with a staggering 179% increase in average weekly attacks, with the total number now exceeding 1,400. This spike can be attributed to the growing global demand for hardware and the heightened focus on AI technologies. As critical components of modern infrastructure and innovation, these industries have become prime targets for cyber criminals seeking to exploit supply chain vulnerabilities for financial gain, espionage, or disruption.

THE OVERALL GLOBAL ATTACKS AGAINST ORGANIZATIONS SIGNIFICANTLY INCREASED IN THE PAST YEAR, WITH THE AVERAGE NUMBER OF WEEKLY ATTACKS PER ORGANIZATION REACHING 1,673. THIS IS 44% HIGHER THAN IN 2023

ATTACK VECTORS

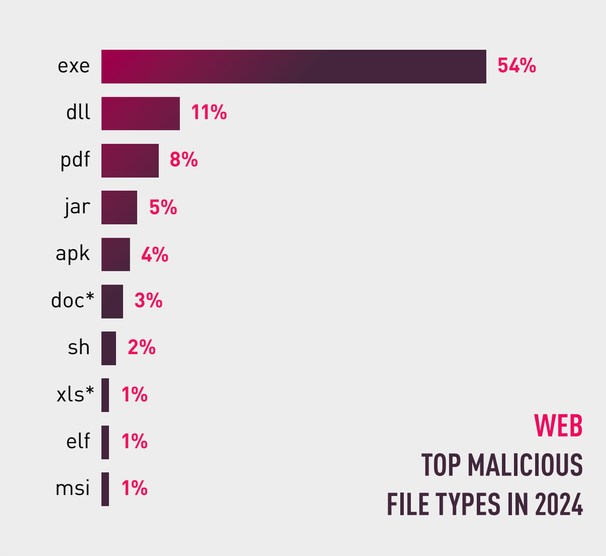


Figure 4 - Web – Top malicious file types in 2024.
xls includes common Office Excel files such as .xls, .xlsx, .xlsm, and more*
doc includes common Office Word files such as .doc, .docx, docm, and .dot*

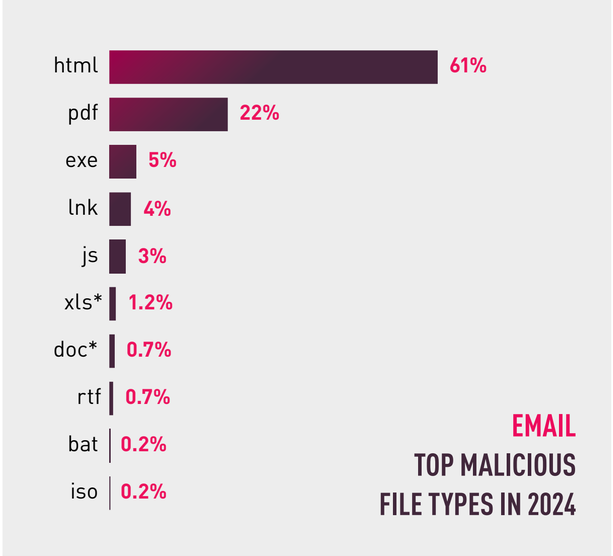


Figure 5 - Email – Top malicious file types in 2024.
xls includes common Office Excel files such as .xls, .xlsx, .xlsm, and more*
doc includes common Office Word files such as .doc, .docx, docm, and .dot*

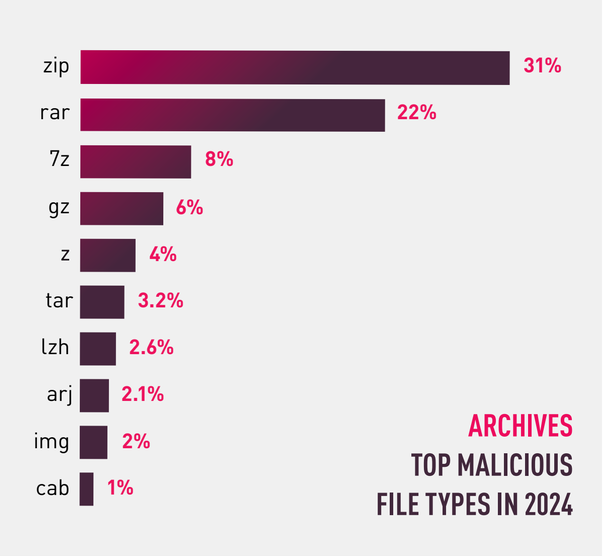


Figure 6- Top malicious archive file types in Email and Web in 2024.

	2021	2022	2023	2024
EMAIL	84%	86%	89%	68%
WEB	16%	14%	11%	32%

Figure 7 - Delivery protocols—Email vs. Web attack vectors in 2021-2024.

68% OF ATTACKS ORIGINATE FROM EMAIL

61% OF EMAIL-DELIVERED MALICIOUS FILES INCLUDE HTML ATTACHMENTS

Email-based attacks remain the dominant initial attack vector, with **68% of attacks originating from email.** This persists despite a significant rise in web-delivered attacks (32%), which is primarily attributed to the dominance of infected-website-based malware distribution frameworks such as *FakeUpdates*.

The decline of malicious macro attacks within Office documents has led to a shift in tactics: most malicious emails now contain HTML files or PDF documents. Malicious uses of HTML files include phishing and credential theft, often achieved by replicating legitimate login pages. Additional use cases include more advanced techniques like HTML smuggling, redirection to malicious websites, browser exploits, and other methods. Notably, **61% of email-delivered malicious files include HTML attachments**.

Malicious PDF files is another prevalent attack vector that is found in 22% of malicious emails. These typically involve embedding JavaScript code or embedded links within the document, which can either trigger malware downloads or redirect victims to malicious websites. In some cases, PDFs exploit vulnerabilities in outdated PDF reader software to execute code on the victim's machine.

Malicious archive files have also become a common attack vector in cyber campaigns, leveraging formats like ZIP, RAR, 7z, and more. Among these, ZIP files are the most common, and account for 31% of malicious archives, followed by RAR files at 22% and

7z files at 8%. Archive files are particularly effective for evading detection, as they compress malicious payloads and obfuscate their content, making it harder for security solutions to analyze them.

A notable challenge for security mechanisms arises when attackers use password-protected archives. These archives cannot be scanned for malicious content without the password, which is often included in the body of the email or shared separately. By encrypting the archive's content, threat actors attempt to bypass automated defenses. Once extracted, these archives can deliver malware directly to the victim's system. Attackers often use multi-stage delivery, where the initial archive file contains seemingly harmless documents or scripts that, when executed, download the actual malicious payload from a remote server. The increased use of archive files highlights the evolving tactics of cyber criminals to exploit weaknesses in email security and leverage user trust to execute attacks successfully.

Malicious DLL files (Dynamic Link Libraries), often delivered within compressed archives, are commonly used in DLL side-loading or DLL hijacking techniques. In these cases, attackers exploit vulnerable legitimate applications by placing a malicious DLL file in the same directory as a trusted executable. When the application runs, it loads the malicious DLL instead of the intended one, allowing the attacker to execute arbitrary code. This technique is particularly effective for evading detection, as the legitimate application acts as a trusted carrier for the malicious payload and DLLs.

Web-delivered attacks often rely on drive-by downloads, compromised websites, or deceptive ads to deliver these files, highlighting the importance of web filtering, updated security software, and user awareness to mitigate such threats. Web-delivered malicious files are on the rise, leveraging file formats like EXE, DLL, and PDF to distribute malware. Among these, EXE files are the most prevalent, accounting for 54% of web-delivered malicious files. These executable files are often disguised as legitimate software or updates, tricking users into downloading and running them. DLL files comprise 11% of these attacks, while PDF files represent 8%.

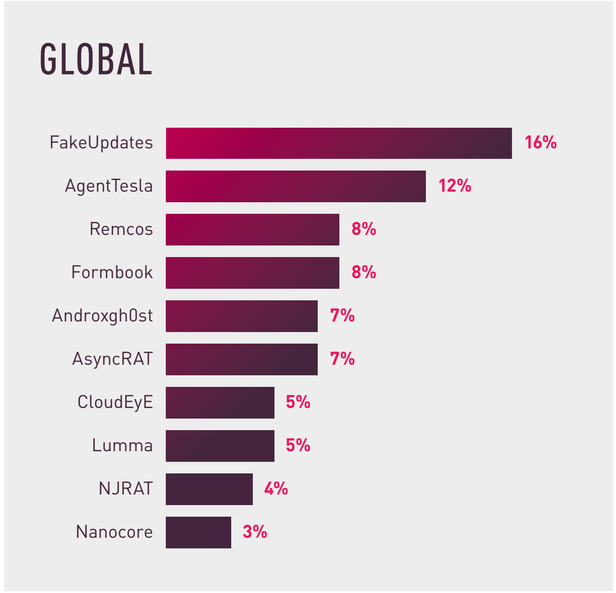


Figure 8 - Most prevalent malware globally – 2024.

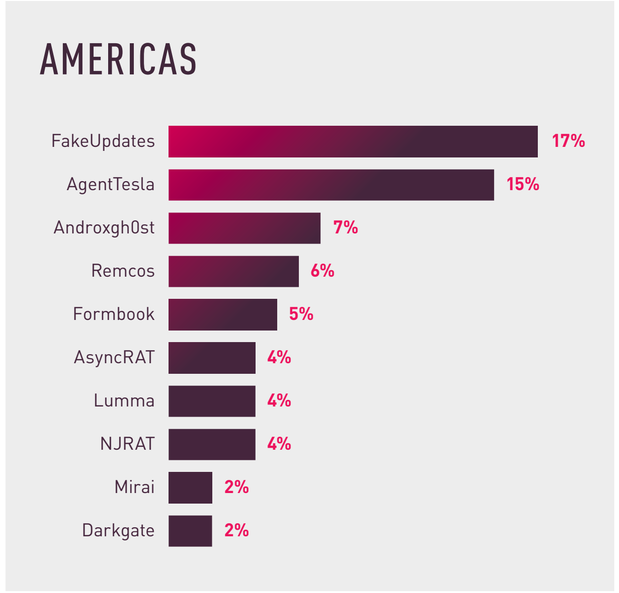


Figure 9 - Most prevalent malware in the Americas – 2024.

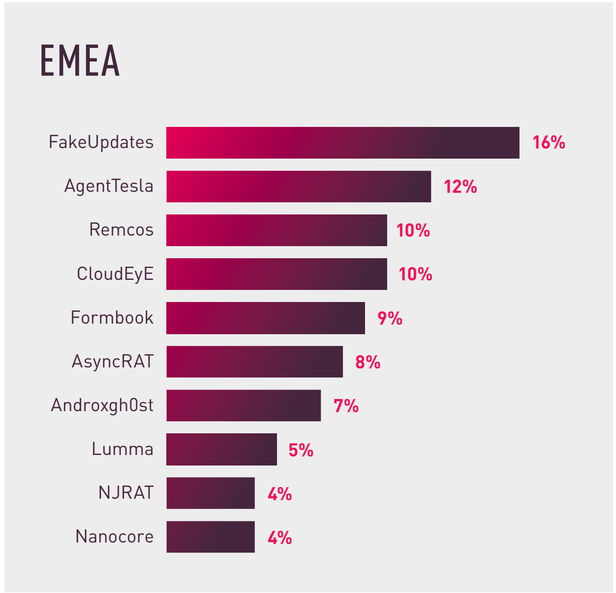


Figure 10 – Most prevalent malware in EMEA – 2024.

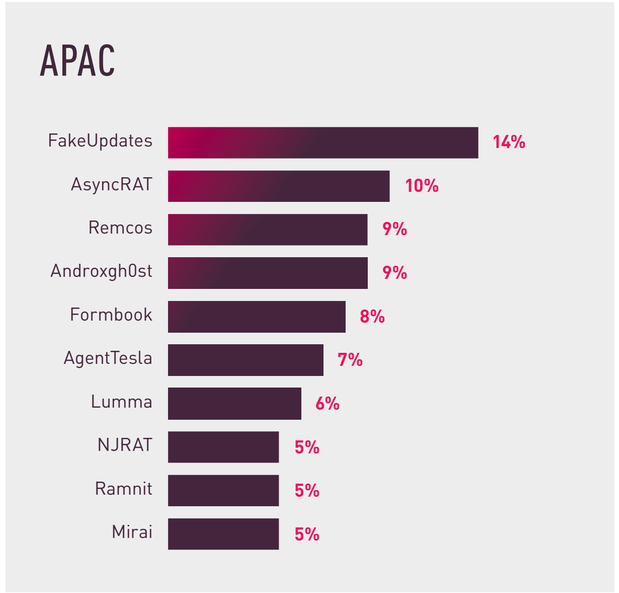


Figure 11 - Most prevalent malware in APAC – 2024.

GLOBAL MALWARE STATISTICS

Data comparisons presented in the following sections are based on data drawn from the Check Point ThreatCloud Cyber Threat Map between January and December 2024.

For each region below, we present the most prevalent malware in 2024, and the percentage of corporate networks impacted by each malware family.

GLOBAL ANALYSIS OF TOP MALWARE

Our analysis highlights the most frequently detected malware families identified by Check Point's network protections. It is important to note that these families are not necessarily the most sophisticated or dangerous but are the most widely distributed.

FakeUpdates (SocGholish) continues to lead Check Point's most prevalent malware rankings for 2024. This malware operation relies on a network of compromised websites to distribute malware disguised as fake browser or software update prompts. The deceptive prompts trick users into downloading and executing a JScript-based downloader which in turn downloads additional malware. The network of compromised websites is attributed to TA569, a prominent Initial Access Broker (IAB) believed to operate on a pay-per-install (PPI) model. TA569 provides system access to other cyber criminals, who often deploy ransomware or other malicious payloads.

Qbot, one of the oldest and most versatile malware families, experienced a dramatic decline over the past year. Previously at second place in our rankings, Qbot's activity was significantly disrupted in late 2023 following a multinational operation led by the FBI which targeted and dismantled its infrastructure. Since then, many threat actors who previously distributed Qbot shifted to other malware strains, including DarkGate.

AgentTesla, a regular presence in our most prevalent malware list since 2020, specializes in stealing sensitive information from infected systems. Check Point Research continues to monitor this infostealer that is frequently deployed in global campaigns. AgentTesla can extract a wide range of data from compromised machines, including keystrokes, login credentials from web browsers, and credentials from email clients.

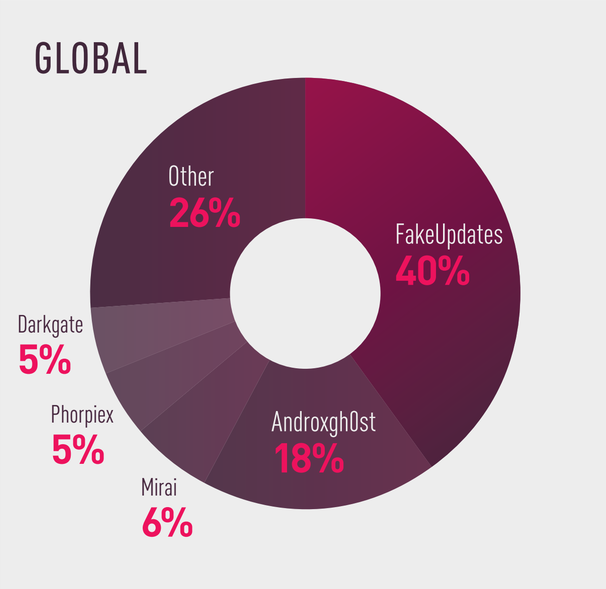


Figure 12 - Most prevalent multipurpose malware globally – 2024.

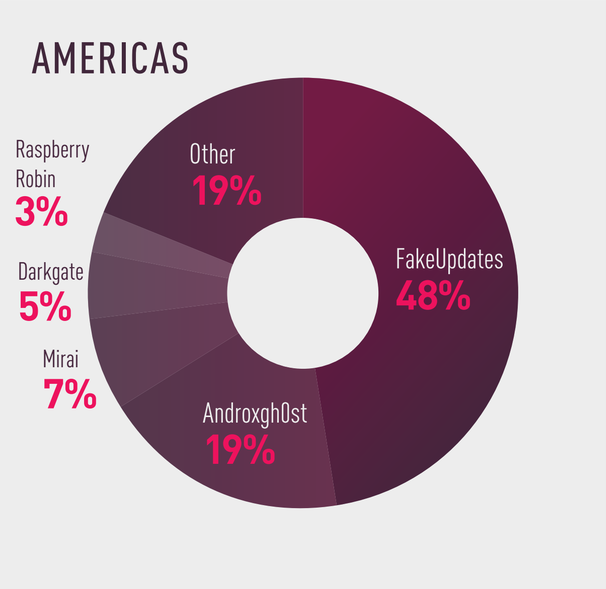


Figure 13 - Most prevalent multipurpose malware in the Americas – 2024.

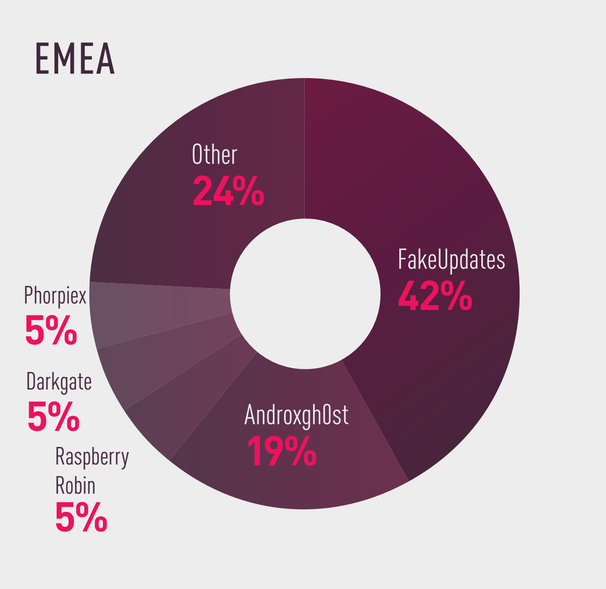


Figure 14 - Most prevalent multipurpose malware in EMEA – 2024.

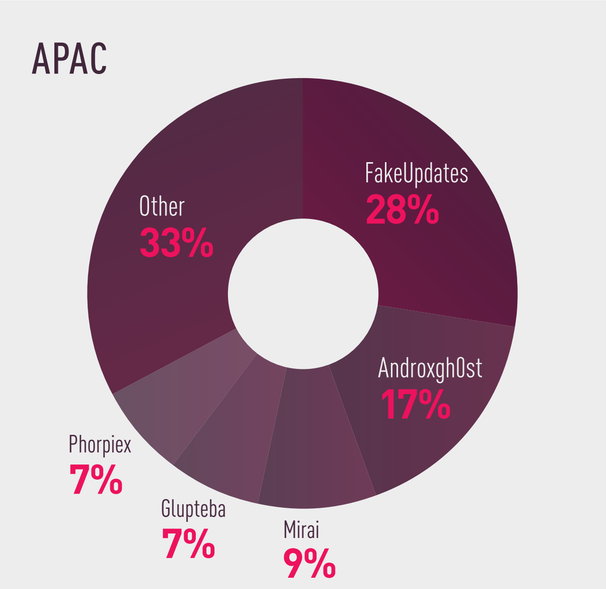


Figure 15 - Most prevalent multipurpose malware in APAC – 2024.

MULTIPURPOSE MALWARE GLOBAL ANALYSIS

Multipurpose malware includes Remote Access Trojans (RATs), botnets, and banking trojans —categories that are continually updated as malware capabilities evolve. Malware classifications are dynamic and upgrades permitting additional functionalities may require reclassification to a new category. Check Point continuously monitors these developments, updating malware classifications and occasionally redefining entire categories to better reflect the evolving threat landscape.

DarkGate serves as a prime example of multifaceted malware. Beyond its core RAT, downloader and information-stealing functionality, DarkGate incorporates crypto mining capabilities, making it difficult to fit neatly into traditional malware categories. However, such complexities are not anomalies. These categories remain critical for understanding the main intent behind specific attacks and identifying overarching trends within the cyber criminals ecosystem.

Intensive law enforcement activity throughout the year has significantly reshaped the cyber threat landscape. In May 2024, a multinational coalition executed Operation Endgame, targeting botnet infrastructure responsible for distributing malware. This operation disrupted malware distribution networks linked to groups such as IcedID, Smokeloader, Pikabot, Bumblebee, SystemBC, and Trickbot. The operation dismantled over 100 servers, seized more than 2,000 domains, and led to the arrest of four individuals—one in Armenia and three in Ukraine—while also freezing illegal assets.

Botnets historically played a central role in malware distribution. Their dismantling has triggered significant changes, including a noticeable shift toward infostealers, which are often more decentralized and widely used among individual cyber criminals. This decentralization makes infostealer activity harder to target through centralized enforcement operations.

As a result of these disruptions, the multipurpose malware market has shifted considerably compared to last year. Qbot and Emotet, which previously dominated the space, have been replaced by FakeUpdates (40%), Androxgh0st (18%), Phorpiex (5%), Darkgate (5%) and Raspberry Robin malware families.

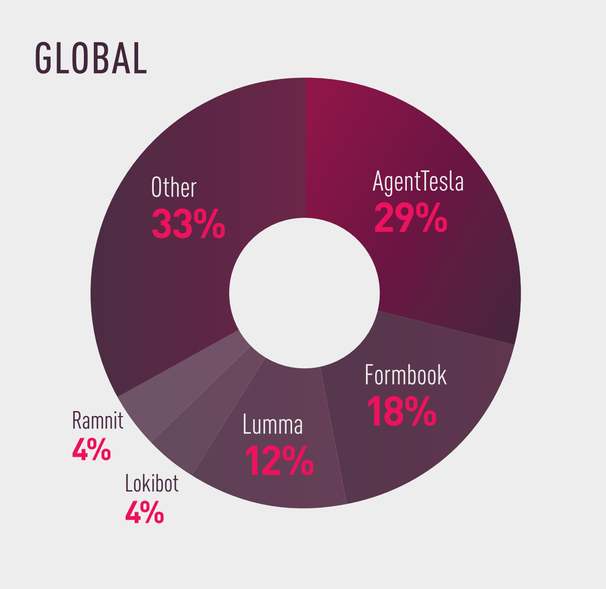


Figure 16 - Top infostealer malware globally – 2024.

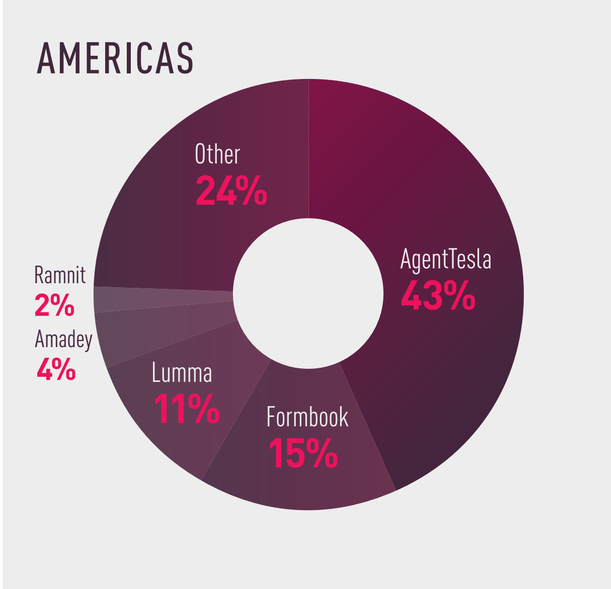


Figure 17 - Top infostealer malware in the Americas – 2024.

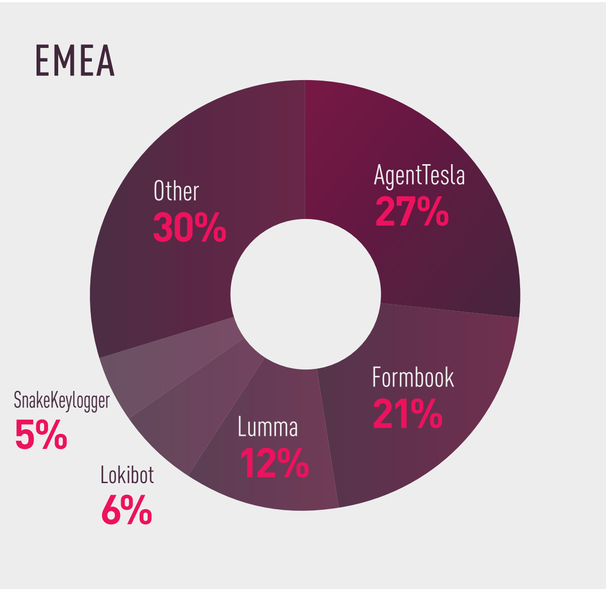


Figure 18 - Top infostealer malware in EMEA – 2024.

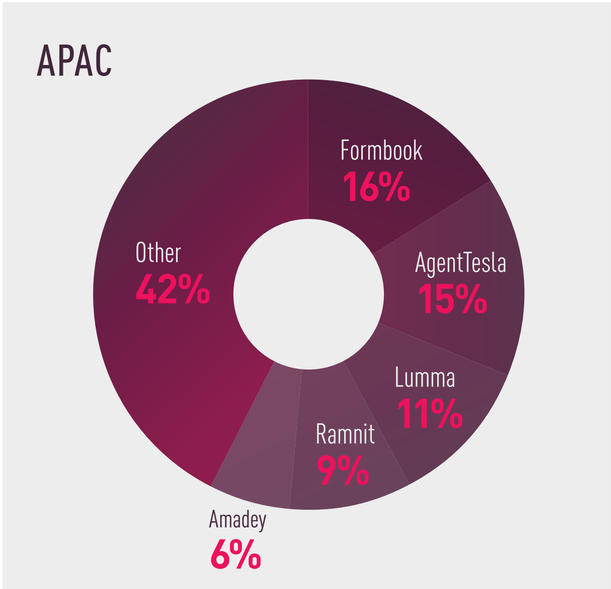


Figure 19 - Top infostealer malware in APAC – 2024.

INFOSTEALER MALWARE GLOBAL ANALYSIS

In 2024, the infostealer malware landscape continued to be dominated by previously known, established threats such as AgentTesla which accounted for 29% of all detections, Formbook for 18%, and Lumma for 12% of the detections. Despite the absence of significant new entrants, there was still a 58% increase in infostealer infection attempts compared to the previous year, and there is a combination of several possible reasons that can explain it.

Traditional malware distribution channels were disrupted by law enforcement operations, such as Operation Endgame in May 2024 which targeted major botnets like IcedID, Smokeloader, and Trickbot, dismantling over 100 servers and seizing more than 2,000 domains. Cyber criminals may be turning to infostealers as an alternative. In addition, the maturation of the cyber criminals ecosystem increased demand for data harvested by infostealers, commonly referred to as "logs." These logs, containing sensitive information such as credentials and personal data, are sold on underground marketplaces to other cyber criminals seeking to exploit this information.

As a result, infostealers are playing an increasingly pivotal role in the evolving threat landscape. A comprehensive analysis of these trends is provided in the subsequent chapters.

The Styx Stealer, investigated by Check Point Research, is one new infostealer that appeared this year. Styx is derived from the Phemedrone Stealer and is designed to exfiltrate sensitive information such as saved passwords, cookies, autofill data from various browsers, cryptocurrency wallet details, and session data from messaging platforms like Telegram and Discord. It also gathers system information, including hardware specifics and external IP addresses, and can capture screenshots to assess the environment prior to executing its payload. Notably, Styx Stealer incorporates features like auto-start, clipboard monitoring, crypto-clipping, enhanced sandbox evasion, and anti-analysis techniques. Unlike its predecessor, which was available for free, Styx Stealer is sold through a subscription model, with prices ranging from $75 for a monthly license to $350 for a lifetime subscription.

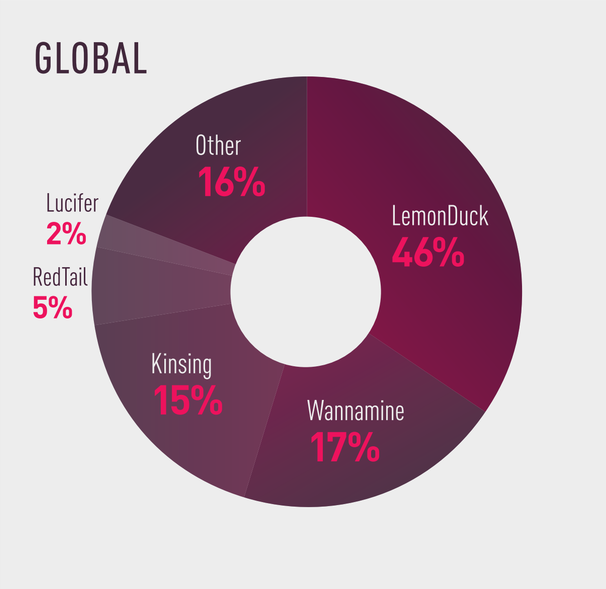


Figure 20 - Top crypto mining malware globally – 2024.

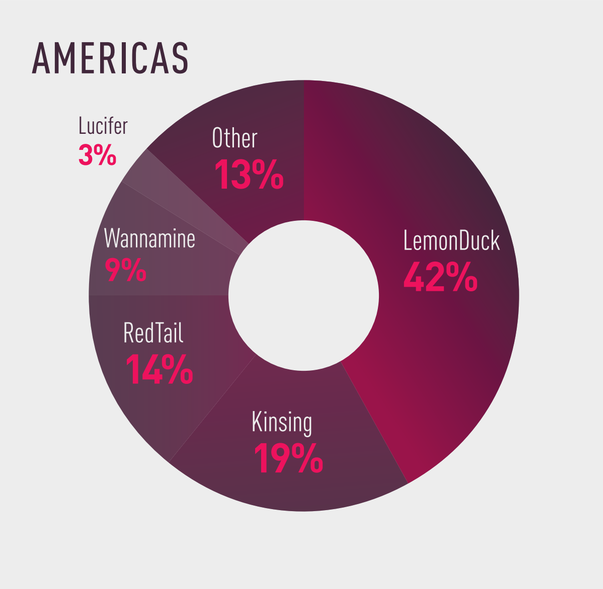


Figure 21 - Top crypto mining malware in the Americas – 2024.

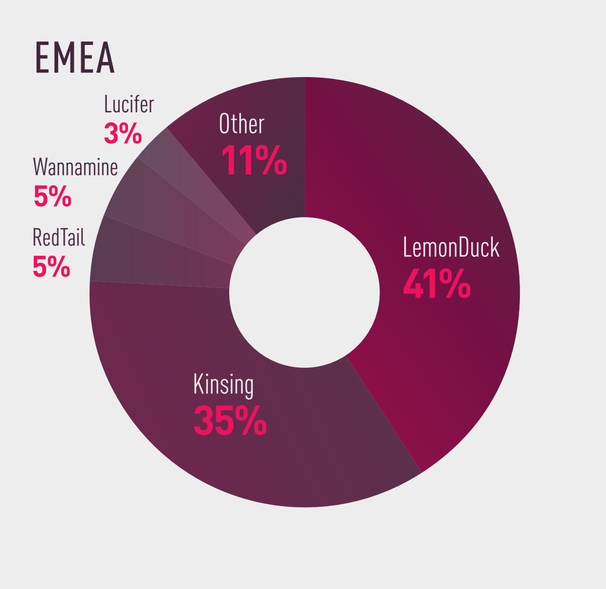


Figure 22 - Top crypto mining malware in EMEA – 2024.

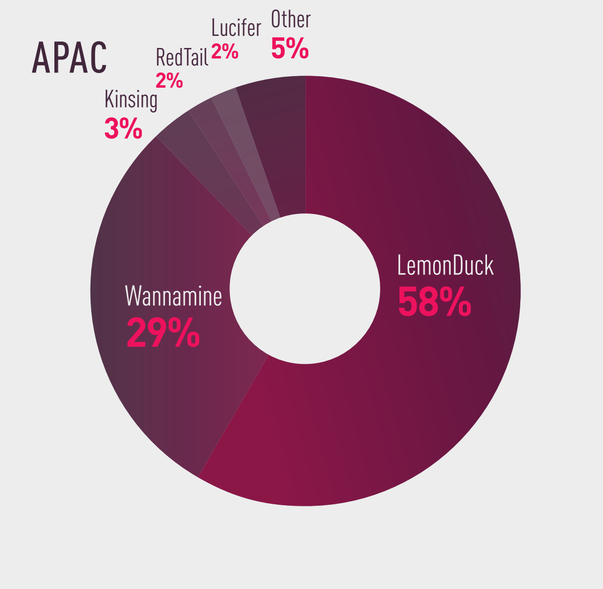


Figure 23 - Top crypto mining malware in APAC – 2024.

CRYPTO MINERS GLOBAL ANALYSIS

In 2024, the cryptocurrency sector underwent significant regulatory and market developments, resulting in an upswing. Bitcoin surpassed the $100,000 mark in December and reached an all-time high of $103,649. However, **the number of crypto mining attacks declined, from impacting 9% of corporations in 2023 to just 2%.**

Illegal crypto miners focus on Monero (XMR) due to its robust privacy features, which render transactions virtually untraceable, as well as its CPU-friendly mining and lower computational requirements. However, Monero's value remained relatively stagnant throughout the year, while its mining difficulty (computational effort required to mine Monero) nearly doubled from an average of 260G in January to almost 450G in December. The sharp increase in difficulty drastically reduced mining profitability and many illegal crypto mining operations scaled back, leading to a decline in crypto mining attacks.

In 2024, **LemonDuck** remained one of the most prevalent crypto mining malware strains and was deployed in 46% of all attempted crypto mining attacks. Initially discovered in 2018, LemonDuck evolved from a simple crypto miner into a highly sophisticated, modular, and cross-platform malware with capabilities that now include credential theft, self-propagation, and fileless, in-memory mining operations. These added features make it versatile and difficult to detect. Recent activity shows that LemonDuck operators are actively exploiting Server Message Block (SMB) vulnerabilities, specifically the EternalBlue exploit, to infiltrate Windows systems. LemonDuck campaigns use a variety of attack vectors, including phishing emails with malicious attachments, brute-force attacks targeting RDP and SSH, weaponized USB drives containing .LNK files, and other infiltration techniques.

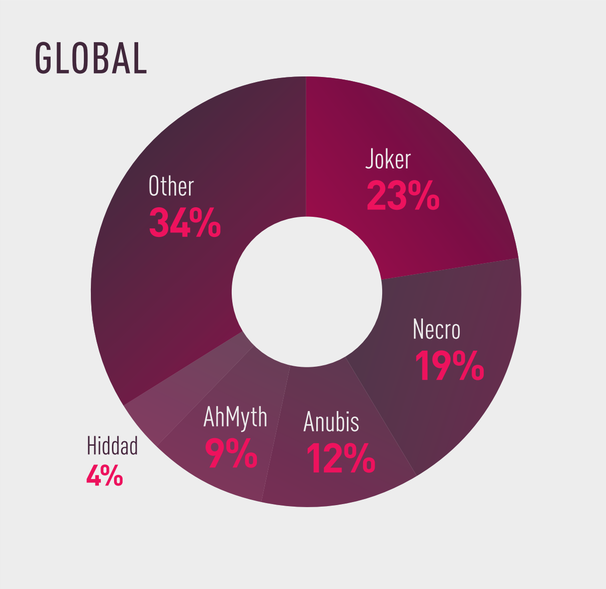


Figure 24 - Top mobile malware globally – 2024.

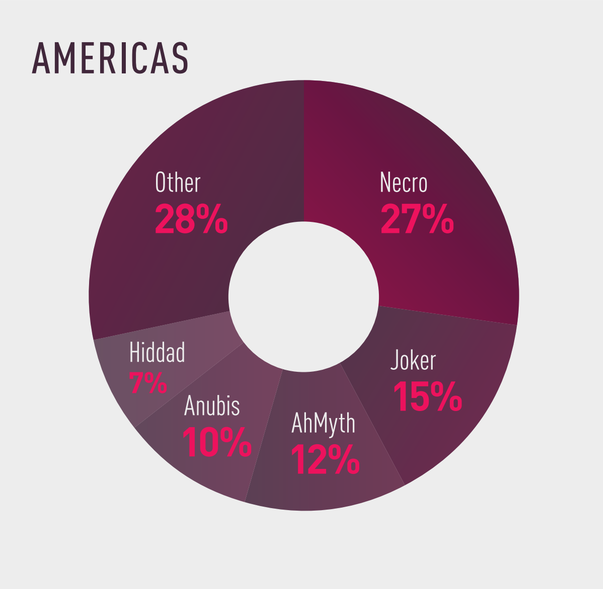


Figure 25 - Top mobile malware in the Americas – 2024.

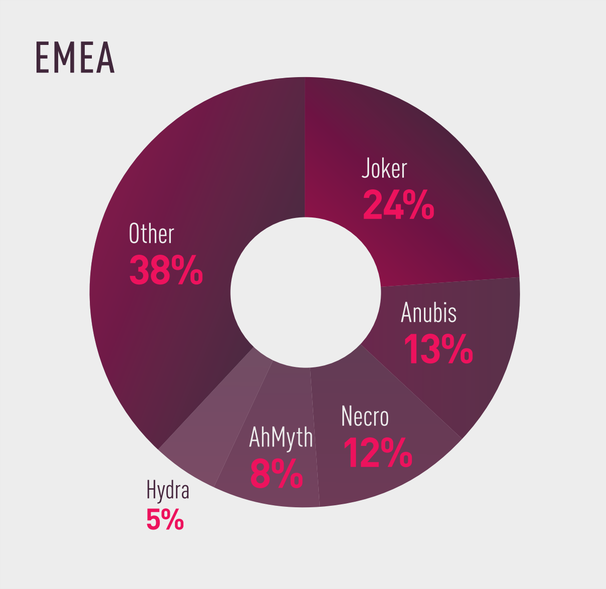


Figure 26 - Top mobile malware in EMEA – 2024.

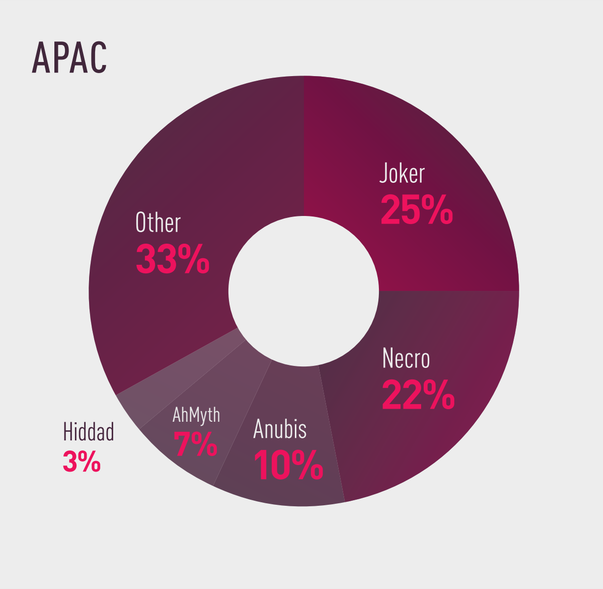


Figure 27 - Top mobile malware in APAC – 2024.

MOBILE MALWARE GLOBAL ANALYSIS

In 2024, more than 60% of global internet traffic originated from mobile devices. The sensitive data stored on these devices is highly sought after, not only by cyber criminals seeking financial gain but also by state-sponsored actors engaged in espionage and intelligence gathering.

Rafel RAT, an open-source Android Remote Access Trojan, is widely used for espionage purposes, as revealed by this Check Point Research report. Our investigation found that it was deployed in approximately 120 distinct malicious campaigns, many of which targeted high-profile organizations, including entities within the military sector. Rafel RAT enables threat actors to exfiltrate sensitive data, contact lists, and Two-Factor Authentication (2FA) messages, gain access to accounts, and bypass multi-factor authentication mechanisms. Notably, the espionage group APT-C-35, also known as the DoNot Team, was observed leveraging Rafel RAT in their operations, which highlights the malware's adaptability and effectiveness across a diverse range of threat actor profiles and objectives.

The most prevalent mobile malware in 2024 (23%) was **Joker**, a notorious malware targeting Android devices since 2017. Joker's primary objective is to covertly subscribe users to premium services by simulating user clicks and intercepting SMS messages and notifications. A notable case involved a Joker variant embedded in the app Beauty Camera in the Google Play Store, which garnered over 100,000 downloads. While the app appeared legitimate, it secretly downloaded additional resources from remote command and control (C2) servers, enabling further malicious activities.

The rise of **Necro** (19%) in the top three mobile malware across all regions is unsurprising. First identified in 2019, Necro is a dropper malware designed to download and execute additional payloads. Recently, Necro was distributed through two malicious applications in the Google Play Store with a combined 11 million downloads. Beyond Google Play, Necro was also identified in unofficial repositories, embedded into popular apps and games like WhatsApp, Minecraft, Stumble Guys, and others.

Two other prominent mobile threats, **Anubis and AhMyth**, are still widely used due to their publicly available source code. Anubis, originally developed as a banking Trojan, evolved to include Remote Access Trojan (RAT) functionality, keylogging, audio recording, and even ransomware-like features. Its versatility makes it a preferred tool for threat actors targeting financial institutions. AhMyth, initially created as an educational project and made public on GitHub, has been integrated into malicious campaigns.

RANSOMWARE

This section presents data and insights drawn from over 140 ransomware Data Leak Sites (DLS) operated by more than 90 double-extortion ransomware groups. The details of more 5,200 companies have been published on data leak sites by cyber criminals who use these platforms to increase pressure on organizations that refuse to comply with ransom demands. Corporations that pay the ransom generally do not appear on the DLS and are therefore excluded from this dataset, introducing an inherent bias. However, the information shared on these criminal DLS offers valuable perspectives on the ransomware landscape. The data analyzed here covers the period from January to December 2024.

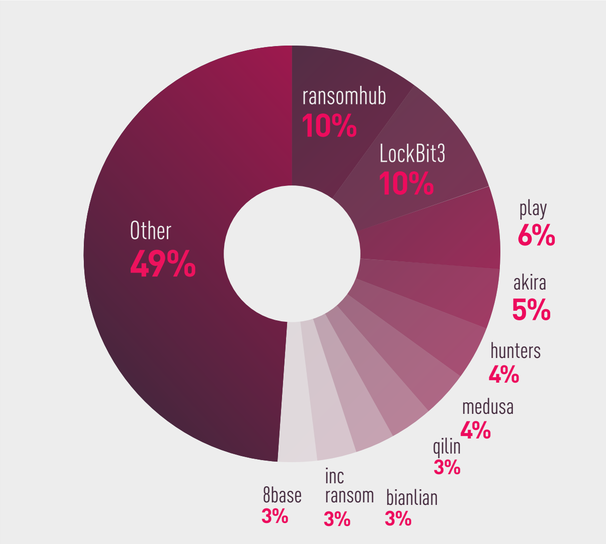


*Figure 28 - Ransomware double-extortion groups, by percentage of total published victims in 2024.**

Two of the most dominant ransomware actors in 2023 have become inactive during 2024. LockBit, which accounted for 21% of victims in 2023, and ALPHV, responsible for 9%, either ceased or significantly reduced their victim postings. LockBit's decline is attributed to the Cronos law enforcement operation, while ALPHV's inactivity results from a combination of law enforcement actions and internal disputes with affiliates. Although LockBit still appears to be the second most prolific ransomware actor in 2024, the majority of its victim postings took place in the first half of the year. By the final months of 2024, LockBit reported less than five victims per month. However, in the last week of 2024, the group announced a new version, LockBit 4.0. Only time will tell if this marks a resurgence for the criminal organization. (More details are available in chapter - 03)

The decline of these two major criminal groups reshaped the ransomware landscape. There is greater fragmentation within the ecosystem, as numerous smaller groups now account for a larger share of the total annual victims. While the top 10 most active groups were responsible for over 66% of all posted victims in 2023, their combined share dropped to just 51% in 2024. RansomHub's rise as the leading double-extortion group can be attributed to their successfully attracting many former LockBit and ALPHV affiliates who lack the capability or choose not to operate independently.

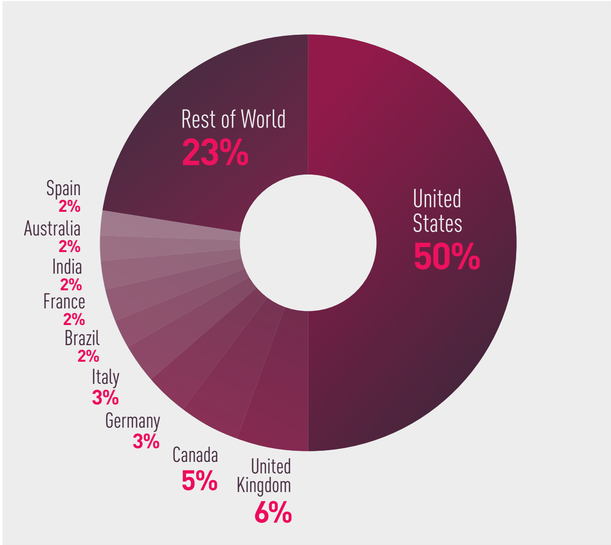


Figure 29 - Victims by country, as reported on data leak sites – 2024.

In terms of geographical distribution, 50% of the companies affected this year are in the United States, followed by the United Kingdom at 6%, Canada at 5%, and Germany and Italy at 3% each.

However, when adjusted for population size, the picture changes. While the U.S. remains statistically the most targeted country, the differences between the countries become less pronounced. Many industrialized nations counted between 2 and 6 corporate victims per 1 million inhabitants, highlighting a broader, global exposure to ransomware attacks.

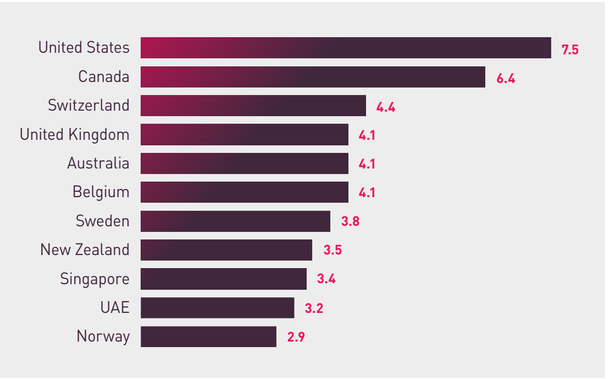


Figure 30 - Ransomware corporate victims per 1M capita, per country.

In the RaaS (Ransomware as a Service) model, affiliates select their victims independently, leading to a geographical distribution of victims that reflects broader ecosystem trends rather than the RaaS operator preferences. Operators can impose restrictions, such as prohibiting attacks on former Soviet republics or non-profit organizations or those involved in healthcare. However, some groups demonstrate a more distinct geographical focus. For instance, the ransomware group known as "RA Group" disproportionately targets Germany, where over 20% of its published victims are located, while KillSec focuses heavily on India, with 30% of its victims located there.

An analysis of the global average of weekly attacks per organization by industry (Figure 3) shows that the education, government, and healthcare sectors are the most frequently targeted. However, looking specifically on ransomware extortion, according to DLS data, manufacturing emerges as

** Data from the DLS covers the period of January 1, 2024 to December 23, 2024.*

the most impacted sector, while government and education rank lower in the victim hierarchy. This discrepancy likely reflects sector-specific differences in their willingness to comply with ransom demands, as government and educational organizations are generally less inclined to pay, making them less attractive targets for ransomware actors.

In 2024, ransomware actors increasingly targeted healthcare and medical service providers, making this sector the second most targeted industry.

Further details on this year's ransomware developments can be found in a dedicated section.

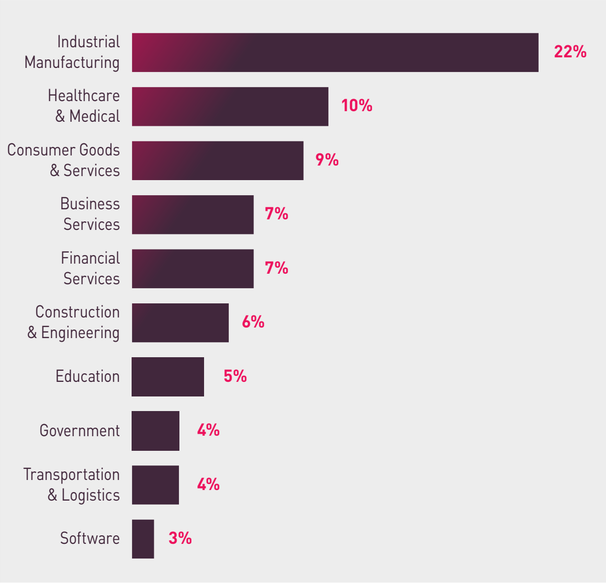


Figure 31 - Industry distribution of ransomware victims, as reported on shame sites – 2024.

HIGH PROFILE GLOBAL VULNERABILITIES

THE STATE OF CYBER SECURITY 2025

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 prominent and interesting attack techniques and exploits observed by Check Point Research (CP<R>) in 2024.

PHP CGI ARGUMENT INJECTION (CVE-2024-4577)

CVE-2024-4577 is a critical command injection vulnerability in PHP that specifically affects Windows systems running Apache with PHP-CGI, and was exploited within a day of its release. Notably, the vulnerability mainly affects Windows installations using Chinese and Japanese language locales, although other installations are also targeted. Disclosed as part of a patch released in June 2024, the issue arises from Windows' "Best-Fit" behavior during character encoding conversions, which can cause the PHP CGI module to misinterpret certain characters as PHP options. This enables unauthenticated users to inject arguments into the PHP binary, leading to remote code execution or the exposure of sensitive data.

Following its disclosure, the vulnerability was quickly leveraged by multiple malicious actors, including for ransomware deployment, and **we observed it impacting more than 25% of corporation networks.** The vulnerability was also used to deploy malware such as the Msupedge backdoor, Gh0st RAT, RedTail crypto miners, and XMRig.

IVANTI COMMAND INJECTION (CVE-2024-21887)

In early 2024, a critical command injection vulnerability, CVE-2024-21887, was discovered in Ivanti's Connect Secure and Policy Secure gateways. This flaw allows attackers to use administrative privileges to execute arbitrary commands on a compromised system. When combined with CVE-2023-46805, an authentication bypass vulnerability, attackers can achieve remote code execution without authentication. These vulnerabilities were actively exploited by Chinese state-sponsored hackers to implant web shells, steal sensitive data, and establish persistence on compromised devices.

VMWARE ESXI AUTHENTICATION BYPASS (CVE-2024-37085)

In June 2024, a critical authentication bypass vulnerability was disclosed in Broadcom VMware's ESXi hypervisor. This flaw affects the integration of ESXi with Active Directory (AD) for user management. Specifically, when an ESXi host is joined to an AD domain, it automatically grants full administrative privileges to members of a domain group named "ESX Admins." Notably, this group does not exist by default in AD, and ESXi does not verify its existence upon domain integration. Therefore, any domain user with permissions to create groups can establish and assign users to an "ESX Admins" group, thereby obtaining full administrative access to the ESXi host. This vulnerability was actively exploited by multiple ransomware operators, including Storm-0506, Storm-1175, Octo Tempest, and Manatee Tempest. In some instances, the observed post-compromise technique resulted in Akira and Black Basta ransomware deployments.

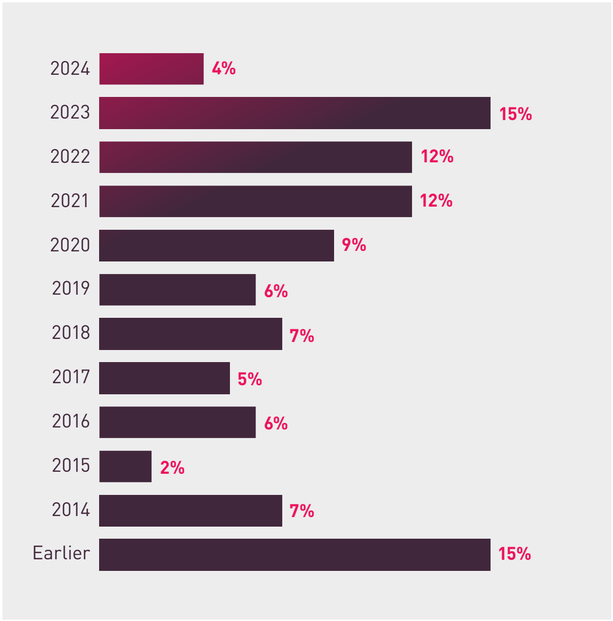
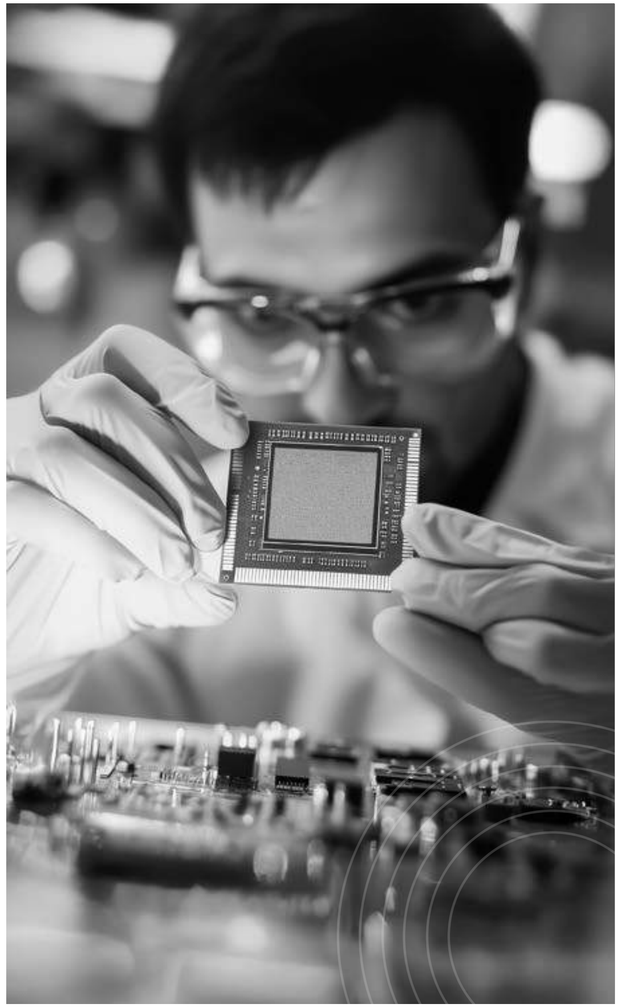


Figure 1 - Percentage of attacks leveraging vulnerabilities by disclosure year in 2024.

An analysis of attack data reveals that vulnerabilities disclosed in 2024 and 2023 accounted for 4% and 15%, respectively, of all exploitation attempts. Recent vulnerabilities are increasingly severe, easier to exploit, and adopted by threat actors more rapidly than in the past. However, threat actors continue to target older vulnerabilities, with over 57% of exploitation attempts focusing on CVEs published in 2020 or earlier. This underscores a persistent issue where systems remain unpatched for years, even after patches are available.



INCIDENT RESPONSE PERSPECTIVE

THE STATE OF CYBER SECURITY 2025

This section is based on the experience and data collected from a wide range of Check Point Incident Response Team (CPIRT) incident investigation and mitigation cases. Unlike the other sections, the data presented here is from case studies of actual events that triggered incident reports, not limited to Check Point product users. Most attacks compromised their targets and provide us with a different perspective into the threat landscape and the practical challenges faced by organizations during active breaches.

INCIDENT TRIGGERS

Clients contact Check Point's Incident Response team due to one or more triggers originating from various sources such as automated security alerts, user reports, service disruptions, or intelligence gathered from third parties, vendors, or government agencies. Collecting and analyzing these triggers helps us understand how threats are discovered, which threat indications are more likely to prompt immediate action, and how speed and efficacy of incident responses can be enhanced.

The primary goal of security teams is to respond as soon as possible before an attack reaches the impact stage involving service disruption or data theft. **2024 marks the first time security alerts become the leading trigger for incidents, surpassing service disruptions as the primary indicator for initiating incident response.**

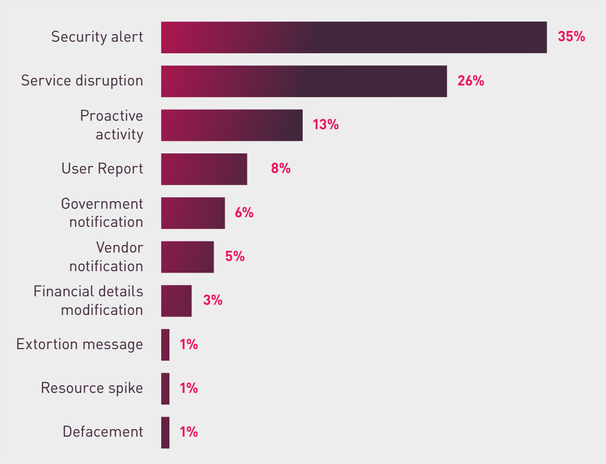


Figure 1 - Most Common Triggers for contacting Incident Response.

Of the cases where CPIRT was contacted this year 35% were triggered by an alert from a security product, compared to just 20% of our cases from the previous year. This shift indicates a significant rise in the expertise of security teams and advancements in detection and prevention technologies. Organizations are progressively adept at recognizing alerts from security systems and identify breaches before they escalate to service disruptions.

For example, CPIRT witnessed multiple attempted ransomware attacks that were detected after a mass installation of remote access tools such as Any Desk and Screen Connect, but before the encryption stage began. CPIRT have seen multiple cases this year where security teams responded quickly to the installation alerts and were able to mitigate the attack before the ransomware encryptor was deployed.

Another noticeable increase is in the number of alerts originating from teams' proactive investigations and Cyber Emergency Response Team (CERT) or government notifications. This reflects growing awareness of communication anomalies and active investigations into intelligence and Dark Web sources and indicates enhanced and increasingly mature cyber security measures across the industry.

By focusing on early detection through security alerts and proactive measures, organizations can respond more effectively to threats and reduce the impact of cyber incidents.

SECURITY ALERTS

Organizations can increasingly identify threats before they escalate into the final attack stages. Analyzing the different types of alerts that prompt security teams to initiate their incident response processes provides valuable insights into how teams should be trained and operate in these situations.

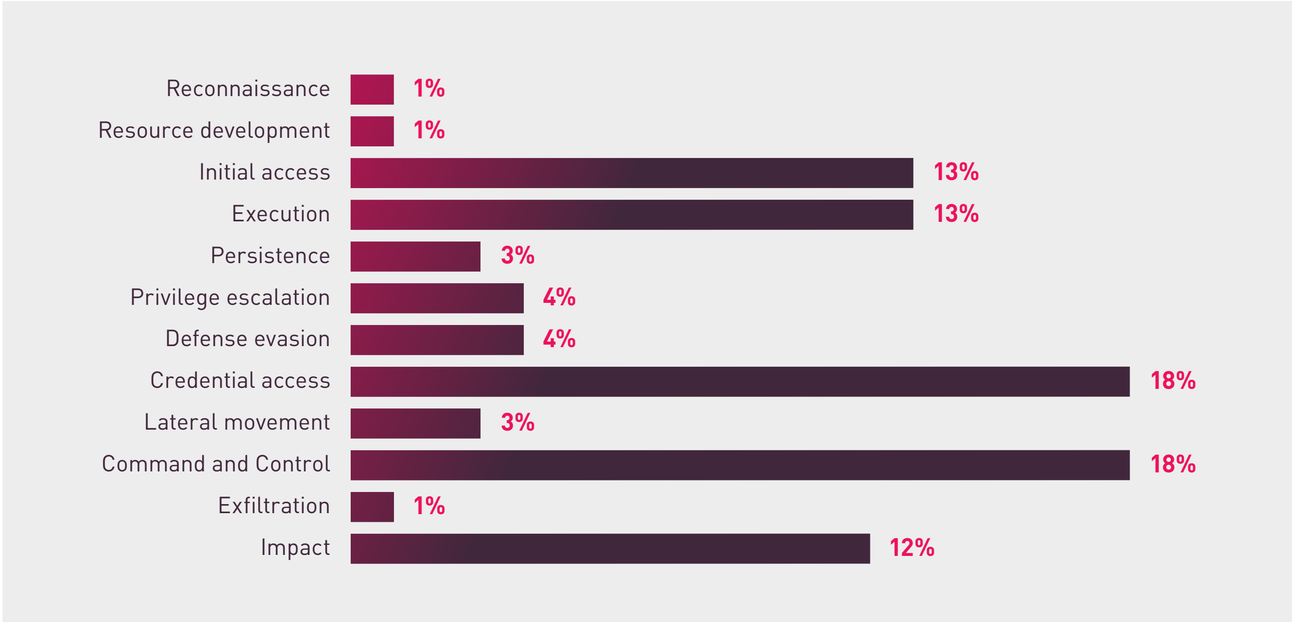


Figure 2 – Attack tactics in security alerts that trigger incident responses, ordered by MITRE ATT&CK Matrix.

A breakdown of the security alerts triggered by MITRE ATT&CK tactics reveals that Command and Control (C2) communication is the most common trigger to incident response. Malicious activity related to C2 communication can often be detected by relatively simple means, such as indicators of compromise (IoCs), suspicious network signatures, or unusual outbound traffic patterns. In addition, security solutions that detect these activities, such as Intrusion Prevention Systems (IPS) and Anti-Bot/Anti-Virus (AB/AV) modules, are widely implemented across industries. These tools enhance visibility into C2 actions and contribute to the high detection rate at this stage.

The next highest tactic alert that prompts IRT involvement is Credential Access. While this tactic may not generate the highest volume of alerts from security products, in many of the CPIRT cases analyzed, **Credential Access is often the tactic that leads security teams to escalate an alert into a full incident response.** Credential Access attempts include the use of tools such as Mimikatz to dump the Lssas.exe process and exfiltrate the NTDS.dit file from a DC. These alerts are rarely overlooked or justified as legitimate user behavior. For this reason, they usually trigger immediate and decisive action by security teams.

SERVICE DISRUPTIONS

As in previous years, service disruptions remain a prominent trigger for incident response. Service disruptions include attacks such as ransomware, where the service disruption is caused by encryption and renders critical resources inaccessible; blocking traffic, which prevents legitimate communications; and DDoS attacks that overwhelm the system capacity, making legitimate services unavailable.

CASE STUDY:
RAPID RESPONSE TO A RANSOMWARE THREAT

Earlier this year, the Check Point Managed Detection and Response (MDR) team alerted a customer in North America about a potential ransomware threat. Within minutes, the team detected the installation of AnyDesk on multiple devices across the organization. The analysts quickly identified this as a security incident and escalated the issue to the incident response team to initiate mitigation and investigation protocols.

Rapidly installing remote-control tools across multiple devices is a known tactic, technique, and procedure (TTP) of ransomware operators. As such, detecting this activity immediately triggered a swift reaction from the experienced analysts.

In this case, it was discovered that the remote-control tools were distributed via Group Policy Object (GPO). Upon examining domain controller (DC), an encryptor binary was found in a public folder, ready to be deployed to all devices within the domain.

Thanks to the analysts' quick response, the threat was mitigated before the encryptor could be distributed, thus preventing a potentially severe ransomware attack.

ALERTS FROM GOVERNMENT AGENCIES AND SECURITY VENDORS

In 2024, incident triggers stemming from alerts issued by government agencies and security vendors increased.

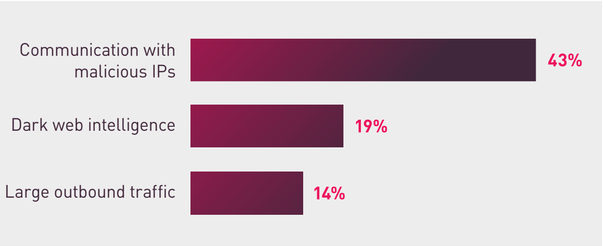


Figure 3 - Top 3 causes for government and security vendors alerts.

Many of these alerts are based on network traffic linked to malicious IP addresses, often identified as indicators of compromise (IoCs) associated with specific threat actors. Similar traffic monitoring can also lead to alerts about unusually large outbound data transfers to suspicious destinations, typically indicating threat actors' exfiltration activities.

Monitoring of the Dark Web by government agencies and security vendors is another critical source of information leading to potential security alerts. This includes information about leaked credentials or sensitive company data shared on Dark Web forums and markets.

Such third-party alerts serve as crucial early warnings, allowing organizations to respond proactively to credible external intelligence before the threats escalate. Since these alerts come from trusted entities and usually undergo professional analysis before issuance, they are highly reliable. This prompts organizations to act swiftly and initiate incident investigations. **Organizations should not rely exclusively on external entities and should regularly conduct proactive monitoring of the Dark Web to facilitate early breach detection.**

CHECK POINT RESEARCH

CASE STUDY: RESPONDING TO A GOVERNMENT CERT ALERT ON DATA EXFILTRATION

In October 2024, a CPIRT case was triggered by a European government CERT alert, indicating that an IP address of the organization was transmitting large amounts of data to an IP associated with command-and-control (C2) activities. The provided IP address was the organization's external NAT IP, prompting the SOC team and CPIRT to investigate firewall and DNS logs to identify the specific device on the network responsible for the data transmission.

The investigation revealed that the domain controller (DC), which was also used as a file server, was the source of the data transmission. On the server, CPIRT discovered archiving tools and a recent installation of **FileZilla.**

CPIRT assisted the customer in determining what data might have been exfiltrated and conducted a thorough investigation to identify any additional footholds the threat actor might have established within the organization.

USER REPORTS

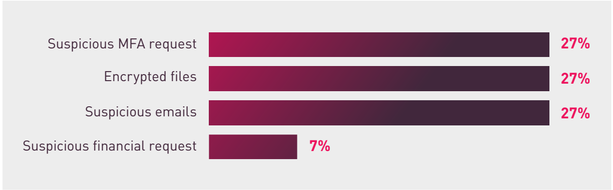


Figure 4 - Top causes for users to report incidents.

User reports provide an additional source for threat detection by identifying malicious activities that are not easily detected by other security mechanisms. As users become more security-conscious it provides an additional layer to the organization's defense strategy. In 2024, most user reports were of overt malicious activities, such as file encryption resulting from ransomware attacks. However, users increasingly reported suspicious multi-factor authentication (MFA) attempts that they did not initiate. Reports of suspicious emails and phishing attempts also frequently led to the detection of malicious activities.

PROACTIVE THREAT HUNTING

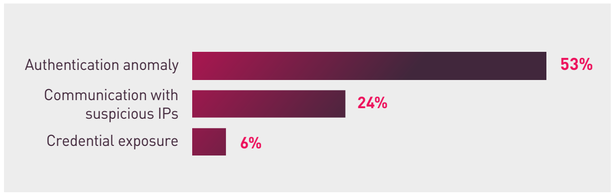


Figure 5 - Findings in proactive activities that trigger incidents.

The past year saw a rise in incidents triggered by proactive activities and threat-hunting led by security teams, as opposed to responses to system alerts. These incidents often originate from examining system logs, user behavior, and network traffic uncharacteristic of the environment. Security teams that are experts in their own network topology can more easily identify suspicious activities than external security products.

Key areas to focus on proactively include abnormal behavior by 'admin users' and suspicious traffic patterns that do not align with regular operational flow, like traffic to and from countries with which the organization does not do business.

By proactively searching for hidden indicators of compromise, organizations can detect and mitigate threats that evade automated detection tools, reinforcing a layered security approach.

ATTACK TYPES

In 2024, ransomware continues to dominate the cyber security threat landscape. The most prevalent ransomware family in incident response cases this year is **LockBit**, followed by **Akira** and **Black Basta**.

Other notable threat types are Business Email Compromise (BEC) and DDOS attacks. Twenty-five percent of the CPIRT case attacks were identified and prevented in early stages, making it difficult to determine the type of attack.

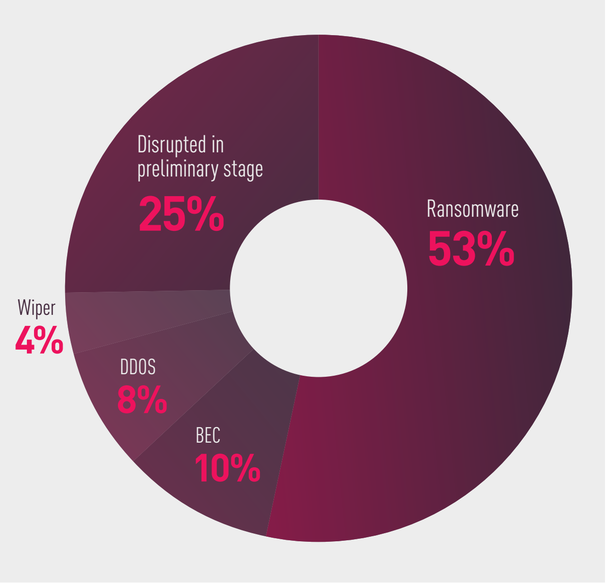


Figure 6 - Main attack categories in CPIRT 2024 cases.

ESXI RANSOMWARE

In 2024, 11% of the ransomware attacks investigated specifically targeted VMware ESXi servers, which are virtualized environments central to many enterprise infrastructures. By focusing on ESXi servers, attackers can render multiple critical servers inaccessible by compromising a single device. This strategy allows them to cause substantial disruption without infecting the entire network or server base with encryption malware. Ransomware groups targeting VMware ESXi servers include the Akira ransomware group which has been exploiting two remote code execution (RCE) vulnerabilities in ESXi: CVE-2023-20867 and CVE-2024-37085.

11%

OF THE RANSOMWARE ATTACKS INVESTIGATED SPECIFICALLY TARGETED VMWARE ESXI SERVERS, WHICH ARE VIRTUALIZED ENVIRONMENTS CENTRAL TO MANY ENTERPRISE INFRASTRUCTURES.

CONCLUSION

The CPIRT 2024 findings show encouraging progress in early threat detection and proactive security measures among organizations. Security alerts have overtaken service disruptions as the primary trigger for incident response, and there is greater engagement in proactive threat hunting and user awareness. These insights emphasize the need for continued vigilance, refinement of detection capabilities, and collaboration with external intelligence sources to strengthen cyber security resilience.

> In 2024, the experiences and data collected by Check Point's Incident Response Team demonstrate that organizations that prioritize security alerts and harness insights from the data are better equipped to thwart threats before they escalate, ultimately safeguarding their critical assets.

TIM OTIS

Head of Incident Response
& Managed Detection and Response

2025 INDUSTRY PREDICTIONS: THE FUTURE OF CYBER SECURITY

THE STATE OF CYBER SECURITY 2025

Cloud Platforms Become the Backbone of Cyber Security

Cloud-based platforms are increasingly serving as the foundation for cyber security, with AI-driven integration proving more effective than standalone tools. By bringing together various security operations, these platforms reduce complexity, allowing organizations to tackle threats and vulnerabilities in the cloud with greater efficiency and effectiveness. Solutions like CNAPP, ASPM, and DSPM merge to create all-encompassing security posture management (SPM) suites.

As new tools such as Application and Data SPM emerge, they will likely be integrated into a broader Cloud Native Application Protection Platform (CNAPP), potentially leading to the development of what could be called Extended Security Posture Management (XSPM). Integrating Attack Surface Management within this new category illustrates how these platforms can offer more value than a simple collection of point solutions, fundamentally changing how organizations address vulnerabilities.

Rising Risks of AI Misuse and Data Breaches

As AI technologies integrate into personal and workplace environments, concerns about their misuse are growing. This year, the potential for data breaches caused by employees inadvertently sharing sensitive information with AI platforms like ChatGPT or Google's Gemini is a significant risk. Employees might input confidential information, such as financials, to generate reports or analyses, often without realizing that unauthorized individuals could store and access this data. Establishing stricter controls on AI tools within an organization's systems will be crucial for striking a balance between enhancing productivity while ensuring data privacy protections.

AI Powered Financial Crime

2024 began with headlines reporting on sporadic but successful instances of Generative AI powered financial crime. Cyber criminals recognized the potential of GenAI and started investing in its integration into various technological tools, particularly for Business Email Compromise (BEC) and Know Your Customer (KYC) bypass methods. These threats will become more prevalent this year, as cyber criminals are actively working to implement GenAI in these malicious services.

Rising Supply-Chain Attacks on Open-Source Projects

As open-source projects gain popularity, they increasingly become attractive targets for malicious actors aiming to covertly exploit vulnerabilities in widely used software. Following the sophisticated multi-year operation that insert a backdoor into Linux XZ Utils, we can expect new similar attack attempts and the discovery of previously implanted backdoors. This escalating threat highlights the urgent need for enhanced security measures and icnreased vigilance within the open-source community.

Decentralization of Cyber Crime Ecosystems

Recent successes by law enforcement in combating major ransomware operations and botnets have prompted malicious actors to transition towards smaller, more decentralized networks, methodologies, and operations. Large ransomware projects have restructured into smaller groups, while infostealer-driven ecosystems have emerged as the primary means of facilitating initial access. This decentralization necessitates that defenders adapt their strategies, highlighting the importance of enhanced collaboration and intelligence sharing.

Increased Regulatory Demands and Stricter Cyber Insurance Standards

Organizations will face increasing pressure due to new cyber security regulations, including the EU IoT Regulations, SEC Cyber security Disclosure Rules, the Digital Operational Resilience Act (DORA), and the NIS2 Directive. Compliance with these frameworks will demand a significant investment of time and resources for initiatives such as policy development and new security technologies.

While these regulations aim to improve security measures, they also create additional operational complexities. This requires businesses to devote more attention and effort to meet these standards. Moreover, cyber insurance policies are anticipated to become more stringent, with insurers enforcing stricter controls and compliance requirements as prerequisites for coverage. This will further intensify the regulatory challenges organizations must navigate.

The Growing Cyber Security Talent Gap

The global shortage of cyber security professionals poses a significant challenge for organizations trying to defend against the rising complexity and volume of cyber threats. While organizations invest in versatile security products, the need for more skilled experts to effectively manage and integrate these tools results in a fragmented and inefficient security approach. Dependence on numerous vendors and insufficient in-house knowledge expose organizations to attacks as their security measures become increasingly difficult to manage and less effective. Companies will have to streamline security operations and prioritize the upskilling of staff to maintain resilience.

CISO RECOMMENDATIONS

THE STATE OF CYBER SECURITY 2025

1. Adopt a multi layered approach within your security stack

Organizations should implement a multi-layered security strategy that includes regular data backups, employee training on phishing awareness, and robust email filtering to mitigate ransomware and information stealers. Utilizing endpoint detection and response (EDR) tools can help identify and isolate threats early. Also, maintaining strict access controls and employing least privilege principles can limit potential breach damage. Regularly updating software and systems to patch vulnerabilities and conducting regular security assessments and incident response drills are essential to ensure preparedness against attacks.

2. Prioritize advanced cloud security solutions

Organizations should prioritize API security, identity management, and a zero-trust architecture to address cloud vulnerabilities. Strong API gateways and regular security assessments can mitigate data exchange risks. Implementing least-privilege access and multi-factor authentication is essential for securing resources. A zero-trust model enhances security by verifying users and devices before access. Cloud security posture management (CSPM) tools identify and fix misconfigurations, while cloud workload protection platforms (CWPP) secure workloads. These strategies collectively help manage cloud infrastructure risks effectively.

3. Leverage AI for Prevention and Detection

Harness the power of advanced artificial intelligence technologies to enhance prevention and detection strategies. By developing robust, AI-driven systems, organizations can effectively identify and mitigate potential threats before they escalate. This proactive approach involves implementing automated solutions that leverage AI capabilities to provide timely and accurate detection of issues in real time. Such systems improve overall security and streamline response efforts, enabling teams to act swiftly and efficiently against emerging challenges.

4. Gain 360 visibility across your attack surface

Criminals exploit vulnerabilities from bring-your-own-device practices and cloud-native applications, increasing the risk of breaches due to issues like hard-coded credentials and weak authentication. They often use legitimate credentials and tools, blurring the line between regular user activity and malicious actions. Organizations must understand the link between identity, cloud, endpoint, and data protection to identify these threats across multiple systems. With the average enterprise using over 45 security tools, data silos can lead to visibility gaps. A unified security platform with AI capabilities enhances visibility and control, improving breach detection and prevention while saving time and money.

5. Develop a customer-trust program to ensure compliance

Organizations must establish a customer trust program to ensure compliance in today's rapidly changing regulatory environment. Implementing automation for compliance can streamline adherence to stringent regulations and reduce human error during audits and reporting. Prioritizing data sovereignty allows businesses to maintain control over sensitive information. By incorporating privacy by design, companies can proactively protect customer data, enhance security, and stay ahead of digital threats. This approach fosters a strong compliance framework that ultimately builds customer trust.

6. Implement Vulnerability and Risk Management Program

The rapid emergence of new vulnerabilities, particularly zero-day attacks, poses a significant challenge for vulnerability management. Edge devices, which are often publicly accessible, are especially at risk. To effectively manage these risks, assessing their threat levels and prioritizing them accordingly is essential, allowing for prompt patching. External-facing assets and critical systems should be the primary focus.

Furthermore, using threat intelligence alongside external attack surface management provides valuable visibility into

> As we reflect on the incidents of 2024, it's essential to focus on the key elements that led to attackers' success and the strategic mitigations defenders can employ to thwart such threats. This introduction summarizes vital insights gained and provides actionable recommendations for cyber security professionals. These guidelines serve as a practical framework to enhance defenses and prevent severe incidents outlined in this report by addressing common systemic issues and mistakes that have historically contributed to cyber attacks.

JONATHAN FISCHBEIN

Check Point Software Global CISO
EMEA & LATAM

how adversaries perceive your security measures. With this insight, you can implement immediate prevention strategies.

7. Choose a security manufacturer that you trust

When choosing a security manufacturer that embodies digital trust, look for a company with a proven track record of effective security practices and low vulnerability rates. Prioritize vendors that ensure prompt patch releases, allowing users to address potential threats swiftly. Additionally, evaluate their incident response strategies and history of handling breaches.

8. Optimize security operations

Given the shortage of skilled cyber security personnel, AI is essential to improving efficiency so teams can better manage and prioritize threats management. AI tools can automate repetitive tasks, minimizing time spent on tasks like event analysis and troubleshooting with automation. Security professionals can focus on strategic innovation and proactive measures with streamlined processes.

9. Focus on Resilience and Incident Response

Organizations must prioritize operational resilience as they face growing threats from ransomware and geopolitical cyber warfare. To strengthen your IT strategy, ensure that your operations are effectively segregated. This approach will enhance your incident response in the event of an attack. Additionally, regularly assess and update your disaster recovery plans to minimize disruptions caused by cyberattacks or IT outages.

User education is crucial in preventing malware infections. Employees should be aware of the sources of files and emails and whether they can trust senders. The most common ransomware infection methods are still phishing emails and malicious web downloads. Increased user awareness often prevents attacks. Educate your users and encourage them to report anything unusual or suspicious to security teams immediately.

ABOUT CHECK POINT SOFTWARE TECHNOLOGIES LTD.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading AI-powered, cloud-delivered cyber security platform provider protecting over 100,000 organizations worldwide. Check Point leverages the power of AI everywhere to enhance cyber security efficiency and accuracy through its Infinity Platform, with industry-leading catch rates enabling proactive threat anticipation and smarter, faster response times. The comprehensive platform includes cloud-delivered technologies consisting of Check Point Harmony to secure the workspace, Check Point CloudGuard to secure the cloud, Check Point Quantum to secure the network, and Check Point Infinity Core Services for collaborative security operations and services.

CONTACT US

WORLDWIDE HEADQUARTERS

5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel

Tel: 972-3-753-4599

Email: info@checkpoint.com

U.S. HEADQUARTERS

100 Oracle Parkway, Suite 800, Redwood City, CA 94065

Tel: 800-429-4391

UNDER ATTACK?

Contact our Incident Response Team:

emergency-response@checkpoint.com

CHECK POINT RESEARCH

To get our latest research and other exclusive content,

Visit us at www.research.checkpoint.com

www.checkpoint.com