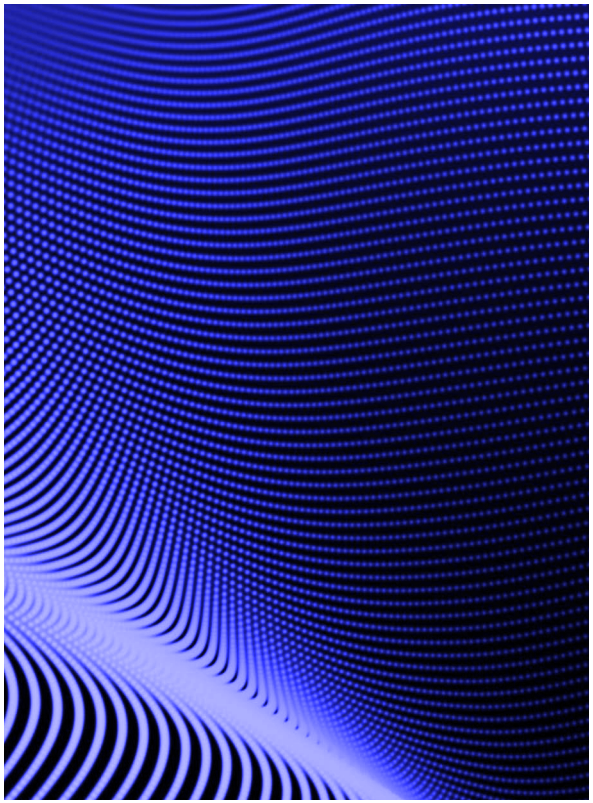
Smarttech
YOUR 24/7 SECURITY PARTNER

Global Cybersecurity Perspectives 2025

Table Of Contents



Foreword

In a world where technology continues to redefine industries and societies, we are witnessing a profound fusion of AI and cybersecurity with data at its very core. This intersection is not just altering how we innovate and protect but also challenging the way we think about opportunity and risk. AI is an active participant in our economic and societal ecosystems, fundamentally altering the ways we process, protect, and exploit data. The ability to harness the potential of AI while protecting critical assets is shaping the digital landscape of today and tomorrow.

In 2024, we saw how geopolitical tensions spilled over into the digital world, blurring the lines between reality and deception. Deepfakes became weapons in the hands of malicious actors looking to manipulate public opinion, undermine institutions, and create chaos. Meanwhile, the democratization of sophisticated attack capabilities has continued to blur the line between highly skilled adversaries and opportunistic threat actors, amplifying the challenges faced by organizations worldwide. From the frontlines of our SOCs, we've seen firsthand how sophisticated and clever attacks are evolving. Many threats out there are blending traditional tools with new tactics, pushing organizations to rethink their defenses.

Supply chain attacks, symbolic of our interconnected times, escalated in scale and complexity throughout the year. We witnessed these attacks grow in scale and sophistication, targeting software providers, vendors, and partners who sit quietly in the background but hold the keys to the kingdom. The fallout wasn't just about stolen data; it was about widespread operational chaos. Trusting your supply chain without verifying its resilience is no longer an option.

Amid these growing challenges, the risks associated with Generative AI came sharply into focus, with many organizations pausing to reconsider its adoption over fears of data exploitation, and for good reason. Without strong data classification and access controls in place, these tools can leave businesses vulnerable to data leaks and regulatory penalties. These changes are enabling organizations to adopt and prioritize data-centric security controls, acknowledging that true resilience begins with safeguarding the very core of their operations.

Looking ahead to 2025, organizations will shift from reactive defense models to proactive strategies that no longer focus on isolated solutions, evolving into a holistic strategy that prioritizes adaptability and foresight. Organizations are focusing on their ability to pivot in real time, building layers of protection that are as dynamic as the risks they counter. With the right mix of innovation, resilience, and collaboration, we can not only counter the threats that lie ahead but also seize the opportunities to build a secure and thriving digital future.

Raluca Saceanu

CEO, Smarttech247

2024 YEAR IN REVIEW

The cybersecurity landscape in 2024 saw a rise in sophisticated attacks and prolonged recovery times, underscoring the persistent challenges organizations face.

Social engineering remained the most prominent attack method, exploiting human vulnerabilities, while malware, denial-of-service attacks, and unpatched systems continued to pose significant risks. Critical industries such as IT, education, and government were prime targets, reflecting their reliance on sensitive data and essential operations.

The financial impact of cyber incidents reached new highs, with data breaches proving costlier than ever, while recovery from these attacks often took months, highlighting gaps in incident response preparedness. To address these challenges, organizations focused on strengthening their defenses, with significant investments in cloud and data security. Emerging technologies like generative AI and advanced threat detection also gained traction, offering promising solutions to combat increasingly complex cyber threats. This evolving landscape emphasizes the critical need for proactive measures and innovative strategies to build resilience against future attacks.

$4.88 Million

Average cost of a data breach

Most Targeted Sectors

Education IT Government

90% of Ransomware Incidents

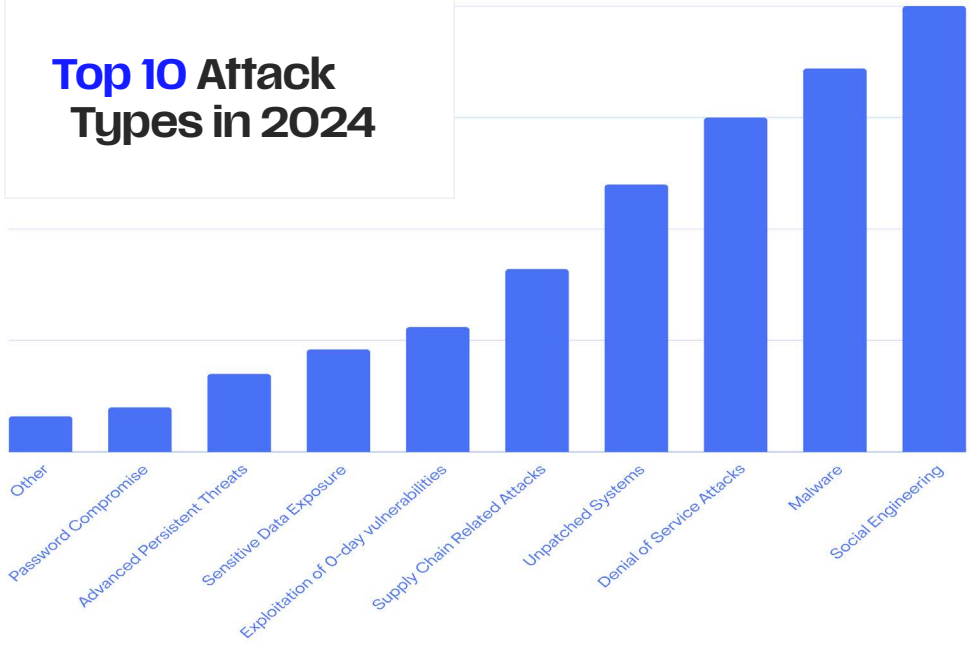
Involved exploiting **unmanaged devices**

40% of CISOs

Identified **data security as a key concern** when implementing AI technologies

Over 35% of breached organizations took longer than 150 days to recover

Top 10 Attack Types in 2024



AI

The adoption of AI saw significant advancements in 2024, fundamentally reshaping both attack methods and defense strategies. AI emerged as both a force multiplier for cybercriminals and a critical line of defense for organizations, driving an escalating arms race in the digital landscape. At the same time, AI enabled organizations to accelerate innovation, enhancing productivity, automating complex processes, and advancing threat detection capabilities.

This year marked a turning point as sophisticated AI systems became widely available, empowering adversaries to automate attacks, exploit vulnerabilities, and manipulate public perception on an unprecedented scale, while simultaneously equipping organizations with tools to innovate, adapt, and defend against these evolving threats.

AI-Driven Attacks: Efficiency and Scale in Criminal Operations

In 2024, AI emerged as a powerful enabler for cybercriminals, allowing them to optimize and industrialize cyberattacks. Criminal groups increasingly leveraged AI to infiltrate systems, evade detection, and automate malicious operations. The dark web became a hub for AI-driven tools, where attackers exchanged malware-laden code, exploited large language models (LLMs) to generate malicious scripts, and injected malware into legitimate software.

These advancements lowered the barrier to entry, enabling attackers with limited expertise to create sophisticated malware, automate phishing campaigns, and breach organizations with greater efficiency. AI-assisted tools further streamlined the development of malicious campaigns, allowing threat actors to refine malware, share vulnerabilities, and exchange critical information at unprecedented speeds. Generative AI models and AI-powered chatbots facilitated the automation of these processes, while advanced tools helped criminals bypass verification systems and encrypt communications to evade detection by cybersecurity professionals. In short, AI transformed cybercrime, empowering malicious actors to operate with greater precision, speed, and scale.

Ransomware operators began using AI to optimize their attack cycles, from identifying vulnerabilities to automating encryption processes. AI-powered ransomware tools scanned networks for weak points, delivered payloads with precision, and generated ransom notes tailored to specific organizations. Groups like LockBit and Akira were observed leveraging AI-enhanced techniques to evade detection and maximize the impact of their campaigns.

AI also enhanced social engineering tactics, such as phishing and credential theft. Threat actors launched highly targeted campaigns using AI to scrape personal data and craft convincing messages. AI-enabled spear phishing attacks combined malware with social engineering, targeting high-value individuals in organizations. Criminals used AI tools to verify information—such as credentials or device details—before launching attacks, increasing their success rate.

Perhaps the most concerning form of using AI for social engineering is in deepfakes, which reached alarming sophistication in 2024. In a prominent incident in Hong Kong, a finance employee at a multinational firm was deceived into transferring $25 million to fraudsters using AI-generated deepfake technology. The attackers orchestrated a video conference where the employee believed he was speaking with the company's Chief Financial Officer and other familiar colleagues. However, each participant in the call was a convincingly realistic deepfake recreation. This case highlights the dangerous evolution of AI-driven social engineering in 2024 which will increase in 2024. By using publicly available images, videos, and recordings, attackers can now clone identities to exploit human trust. Deepfake technology enables criminals to impersonate executives, colleagues, or even family members, creating opportunities for fraud, data breaches, and reputational damage.

AI-Enabled Human Targeting: Precision and Automation

AI-enabled targeting became a critical concern in 2024, particularly for high-value individuals in organizations. Cybercriminals leveraged AI to collect personal and professional information about executives, financial officers, and key personnel. Advanced AI tools scanned social media, internal communications, and publicly available data to create comprehensive profiles of their targets. Once a target was identified, AI tools automated the development of tailored attacks. For example:

- Deepfake audio and video calls were used to impersonate executives during financial fraud attempts.
- AI-generated spear phishing emails mimicked writing styles and organizational language, making them highly convincing.
- Tools like résumé swarming exploited recruitment systems by automating thousands of fake applications, targeting HR personnel to breach organizations' internal systems.

These attacks demonstrated the increasing sophistication of AI as a tool for cybercriminals. Threat actors no longer required human resources to conduct reconnaissance or launch attacks; AI automated these processes with unprecedented precision.

AI Used In Disinformation Campaigns

Nation-state actors and criminal groups have been increasingly using AI-generated content to manipulate public opinion and deceive individuals. China-affiliated threat actors, for example, orchestrated sophisticated influence campaigns during elections worldwide. AI tools were used to generate fake images, videos, and news articles that spread disinformation and undermined trust in institutions.

Similarly, threat actors associated with Russia used deepfake audio and video to impersonate public figures, manipulate narratives, and exploit geopolitical tensions. These AI-enhanced influence operations amplified existing societal divisions and posed significant challenges for governments trying to combat misinformation.

The Risks of Generative AI Tools Inside Organizations

While AI provided organizations with advanced capabilities for security and innovation, the adoption of Generative AI tools introduced significant internal risks. Platforms like Microsoft CoPilot, ChatGPT, and other AI-driven tools were widely adopted to enhance productivity, automate workflows, and analyze data. However, organizations often implemented these tools without proper data classification processes or robust access controls, inadvertently exposing sensitive information. Employees, in their use of AI tools, sometimes input confidential data—such as financial records, trade secrets, or proprietary code—into public AI models, leading to irreversible risks of data leaks.

Beyond generative AI, many organizations lack visibility into how other AI technologies are being utilized across their environments. This creates a critical blind spot, as data processed or stored through AI tools could fall outside secure organizational boundaries, increasing the risk of unauthorized access or loss. Such lapses in oversight not only compromise sensitive information but also place organizations at risk of regulatory fines for failing to meet data protection and compliance standards. This will be a key risk in 2025, forcing organizations to rethink their digital innovation strategies in order to safely adopt AI technologies.

Furthermore, in 2024 we saw cybercriminals exploiting this evolving landscape, leveraging AI tools on the dark web to inject malware into AI-enhanced programs, exchange stolen data, and identify weaknesses in AI-driven systems. These tools allowed threat actors to automate and scale their operations, making the theft of sensitive information faster and more precise.

The convergence of internal AI use with inadequate governance frameworks amplified these risks. Without clear policies to regulate data flow, access permissions, and the integration of generative AI tools, organizations faced a growing challenge in safeguarding their assets. The need for visibility, control, and governance over AI adoption became critical to preventing both accidental data exposure and compliance breaches in an increasingly AI-driven business environment.

Geopolitical Influences In Cybersecurity

The cyber domain has featured in the geopolitical plans for nations states to some degree over the last 20 years. While the espionage, disruptive, destructive and ransomware operations continued during 2024, the overall trend has seen an increase in the “frequency, sophistication and intensity” in the use of cyberspace by threat actors linked to states. Smarttech247 observed the significant impact of geopolitical developments on cybersecurity throughout the past year.

Elections drove targeted cyber campaigns focused on disinformation and disruption, while conflicts in regions such as the Middle East and Ukraine escalated the frequency and sophistication of cyberattacks on critical infrastructure. Furthermore, North Korea strategically utilized IT professionals to support state-sponsored cyber operations, demonstrating the growing complexity of global cyber threats. These developments underscored the deep connection between geopolitics and cybersecurity in shaping the threat landscape.

Elections

2024 saw several high-profile events like the Paris Olympics that were obvious targets for geopolitical motivated attacks, however the sheer number of elections held globally meant that it was an unusual year. 82 countries went to the polls, and technological, as well as societal changes, mean that there are three potential ways that cyber domain operations can impact elections:

- Mis and disinformation operations
- Targeting of election reporting systems
- Hack and leak operations

Since the US election of 2016, states have taken progressive steps to harden both their election reporting systems, and the digital literacy of their populations. Overall, with some notable exceptions, elections were not as impacted as may have been feared at the start of the year. The influence of AI appeared to follow the patterns observed during the EU Parliament elections – while there was some use of unlabeled used of AI by parties, it wasn't a "game changer." Two elections during 2024, at either side of the Atlantic, show how states have attempted to mitigate electoral risks:

Ireland

Ireland's unusual electoral system, based on Proportional Representation – Single Transferable Vote on paper ballots only, mean that the risk of interference in reporting systems is assessed as low. Coimisiún na Meán, the newly formed media regulator, issued advisories to both election candidates and traditional broadcasters in the run up to the election, in what was a coordinated attempt to pre-emptively reduce the influence of online disinformation. Less positively, the National Counter Disinformation Strategy was not published prior to the election, despite the working group being set up in February 2023.

US

The efforts of U.S. agencies, particularly the Cybersecurity and Infrastructure Security Agency (CISA), played a crucial role in strengthening electoral reporting systems, ensuring they operated as expected—just as they did during the 2020 elections. However, federal officials noted the presence of disinformation campaigns, highlighting ongoing attempts to undermine public trust in the electoral process.

One disinformation campaign, linked to Russia, falsely alleged that officials in key swing states were planning to commit electoral fraud. Another featured a video that appeared to show an individual in Pennsylvania, a critical swing state, destroying a ballot paper. Some of the disinformation videos included the logos of law enforcement organizations like the FBI, other were branded with news agencies like the BBC. In September, three Iranians were charged in connection to a "hack and leak" attempt that targeted the Trump campaign. In December authorities reported an attempt by a Chinese linked threat actor to access the information of US politicians through eight separate telecommunications

Middle East Conflict

As the conflict in the Middle East continues to grow, states continue to use the cyber domain to advance their geopolitical aims. The conflict in Gaza remained the Iranian focus with espionage, disruptive and destructive attacks and information operations being reported.

Perhaps the most significant attack was the March compromise of an IT network connected to an Israeli nuclear power station. Parts of the Iranian economy also continued to be targeted by cyber-attacks.

Considering some of the targeted kinetic attacks on members of Hezbollah, Hamas, and the Islamic Revolutionary Guard Corps, it is assessed as likely that IT networks of state and non-state actors in the Middle East remain a significant target for Israel.

Conflict in Ukraine

Both offensive and defensive operations connected to the conflict in Ukraine continued to develop in 2024. It is assessed as likely that Ukraine carried out regular disruptive and destructive attacks in Russia, focusing on critical national infrastructure, its economy including its banking sector, and administration. 2024 saw an increase in the targeting of Ukraine's defense sector compared to 2023.

Hacktivists also continued to target Western countries, particularly in Nordic Countries in DDoS attacks that impacted the availability of services. Of particular note was the September attack on Nordea, the Finnish Headquartered bank, which disrupted online services for a time. It is assessed as likely that at least some of the ongoing cyber events in Sweden and Finland are related to their decision to join NATO.

North Korean IT Workers

2024 saw the development of a new type of insider threat – North Koreans impersonating workers from different countries for remote IT positions. Most organizations have policies in place to counter an insider threat, but the advent of remote work, AI voice clones, and the foreign policy decision of North Korea to fund parts of its State via cybercrime, means that this new aspect must be considered.

The selection of IT workers is intentional, unlike other categories of workers, jobs can largely be carried out remotely, and with privileged account access, they can either enable cyber-attacks by manipulating defenses, or directly exfiltrate the data themselves.

In 2024, geopolitical tensions significantly shaped the cybersecurity landscape in the United Kingdom as well, as the nation faced escalating threats from both state-sponsored and non-state actors. The strained relations between the UK and Russia following allegations of election interference and cyberespionage led to a surge in sophisticated attacks targeting critical infrastructure, including the financial sector and energy grids.

Britain's cyber security chief warned of a rise in hostile activity in the country's cyberspace, with the number of incidents handled by officials rising by 16% in 2024 compared to 2023. Furthermore, the UK NCSC identified ransomware attacks as the most immediate and disruptive threat to the nation's critical infrastructure, including sectors such as energy, water, transportation, health, and telecommunications. This stark warning underscored the escalating risks posed by increasingly sophisticated cybercriminal groups, some of which are linked to geopolitical adversaries, targeting essential services with potentially catastrophic consequences for public safety and economic stability.

Regulators

Regulators appeared to focus their efforts in three main areas during 2024 - providing cyber threat intelligence on geopolitical influenced cyber operations, enhanced law enforcement cooperation, and the introduction of significant legislation.

Organizations like CISA worked with others routinely released alerts regarding threats to Critical National Infrastructure.
Some examples include:

- February 2024 – Alert for risk to Critical National Infrastructure connected to Volt Typhoon, Threat Actor believed to be sponsored by the Peoples Republic of China
- July 2024 – Alert for espionage activities linked to Plutonium, Threat Actor linked to North Korea's Reconnaissance General Bureau
- August 2024 – Alert for Iranian State linked Fox Kitten Threat Actor targeting US, Israeli, and UAE organizations with ransomware
- September 2024 – Alert for risk to Critical National Infrastructure linked to Unit 26165, who are linked to the Russian General Staff Main Intelligence Directorate (GRU)
- December 2024 – Alert on Chinese affiliated threat actor compromising the networks of global telecommunications providers.

While law enforcement cooperation has improved over the years, 2024 saw a significant increase in operations. These are important for two reasons - the disruption of the existing networks, and the deterrence effect that hopefully these operations will have. Cybercrime remains a difficult area to enforce laws, particularly if borders are crossed, so it is important that these efforts are publicized. Significant operations included:

- June 2024 - Operation Morpheus – targeted unlicensed Cobalt Strike servers
- September 2024 – Operation Kraken - joint operation to target the Ghost communication platform
- March to October 2024 – Operation Cronos – three phases of the operation targeting LockBit
- December 2024 – Operation Destabilise – disruption of the Smart and TRG com

Within the European Union, 2024 saw the focus on three significant pieces of legislation that will regulate different aspects of the cyber domain:

- The AI Act was introduced in June, with obligations phased in over three years. Organizations must balance the operational imperative of utilizing GenAI to drive business efficiency, against the requirements of protecting their data and networks. The phased introduction of the AI Act will hopefully ensure that the deployment of AI within organizations is competed in a planned and structured way. However, there is an ongoing debate to whether the EU's approach will further impact the development of its tech sector and overall economic growth, as others take a less cautious approach.
- The October deadline for the incorporation of the NIS 2 Directive was missed by many EU countries, but it is expected that it will be placed in National legislation in 2025. NIS2 increases the scope of sectors that are obligated to structure their approach to cyber security, and also expands on some of those obligations. A key question for the success, or otherwise, of the directive will be the enforcement ability of the various competent authorities.

The Digital Operational Resilience Act will come into force in January 2025, and 2024 saw financial organizations complete their preparations. The DORA reporting requirements are challenging, particularly an initial report within four hours, and organizations will have to continue to focus on this in 2025 to ensure their processes are robust.

Work on upcoming legislation, particularly the Cyber Resilience Act which is expected to be introduced in 2027 continued. Significantly, discussions between the EU-US on a Joint Cyber Safe Products Action Plan took place. This builds on the EU Cyber Resilience Act framework and the proposed US cybersecurity labelling programme Cyber Trust Mark Act.

Improved Tactics & Techniques That Shaped 2024

EDR Whitelisting Vulnerability: Detection Bypassing

One of the most alarming cybersecurity trends in 2024 revolves around the exploitation of endpoint detection and response solutions by leveraging default whitelisting rules. While EDR systems are designed to identify and mitigate threats, many of these tools have introduced dangerous oversights that adversaries have exploited with surprising ease.

A particularly prominent attack vector emerged where threat actors discovered that renaming malicious executables like mimikatz.exe to trusted file names such as explorer.exe or chrome.exe could bypass EDR protections entirely. This is due to default exclusions in the software that prevent certain processes, based on their names, from being thoroughly scanned or monitored.

In one example, a researcher identified specific EDR software (e.g., TrendMicro) where renaming binaries like explorer.exe successfully avoided DLL injections and userland hook monitoring—effectively evading the detection mechanisms. Another researcher made significant progress reverse engineering an EDR solution, using tools like IDA to expose exclusion rules that circumvented entire detection chains. By merely renaming a file, malicious actors were able to render EDR protections useless.

Ivanti Connect Secure: Authentication Bypass & Remote Code Execution

2024 started with a significant cybersecurity incident targeting Ivanti's Connect Secure VPN solution, a widely used enterprise-grade product. Threat actors successfully exploited two high-severity vulnerabilities in tandem:

1. CVE-2024-21887: A critical command injection vulnerability in the web components of Ivanti Connect Secure and Policy Secure (versions 9.x and 22.x). This flaw allows an authenticated administrator to send specially crafted requests to execute arbitrary commands.
2. CVE-2023-46805: An authentication bypass vulnerability that allows attackers to gain unauthorized access to the system.

While CVE-2024-21887 requires administrative privileges (CVSS score: 9.1), combining it with CVE-2023-46805 (CVSS score: 8.9) enables unauthenticated attackers to achieve remote code execution (RCE) with the highest possible privileges. This effectively escalates the risk to a critical 10/10 level. Exploitation of these vulnerabilities began in December 2023 but escalated through early 2024. Threat actors deployed web shells, enabling persistent access to compromised devices, and used the foothold for further lateral movement across networks. The attack severely impacted enterprises relying on Ivanti Connect Secure as a key part of their remote work infrastructure.

Archive.org Data Breach

In October 2024, the Internet Archive, renowned for its Wayback Machine service, suffered a significant breach compromising the personal data of approximately 31 million users. Exposed information included:

- Email addresses
- Usernames
- Bcrypt-hashed passwords

While the use of bcrypt for password hashing demonstrated a positive security practice, the breach still raised concerns about user privacy and long-term data security. On October 20, 2024, Archive.org suffered a second breach, this time involving its Zendesk email support platform. Threat actors reportedly gained access through exposed GitLab authentication tokens, which had previously been flagged but were not remediated in time. The attackers leveraged this access to compromise support emails, further exposing sensitive communications and escalating the overall risk.

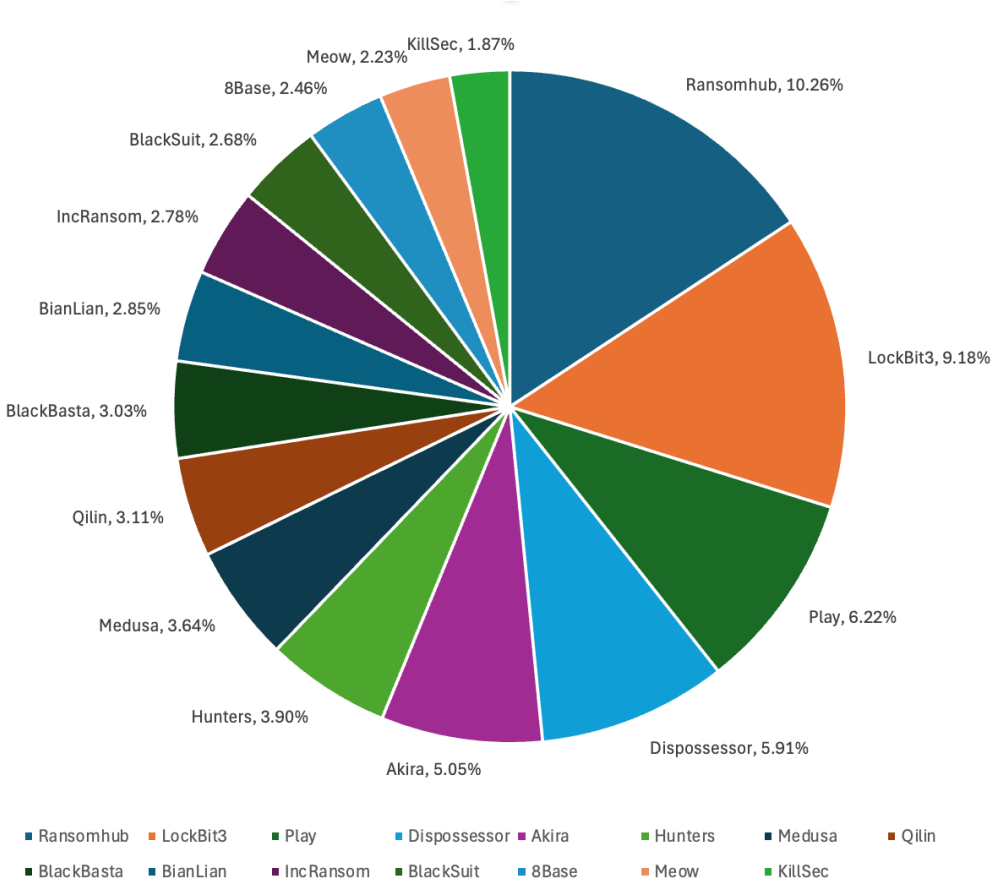
NOTABLE SECURITY INCIDENTS 2024

Incident	Ivanti VPN Exploitation	Change Healthcare Ransomware	Microsoft Executive Breach	Snowflake Data Theft	AT&T Breach	American Water	CDK Global Blue Yonder	Blue Yonder	Synnovis	National Public Data Breach
Size/Impact	Mass exploitation of critical zero-day vulnerabilities contained in Ivanti products.	100 million people affected	Government emails exposed	165 organizations affected	7.6 million current and 65.4 million former customers	Operational disruptions	10,000 U.S. car dealerships affected	Ransomware Attack; Large scale impact on customers including Starbucks, Morrisons etc.	Ransomware attack on a critical supplier of pathology services to UK NHS hospitals	3 billion records exposed affecting 270 million individuals
Adversary	China-linked group UNC5221	Blackcat Alphv	China-linked espionage group	UNC5537	Breach originated from Snowflake attack	Nation-state actors	BlackSuit	Termite Ransomware	Qilin	USDoD
Key Factors	Hackers actively used these flaws to carry out espionage and other types of attacks.	Critical healthcare targeted; $22M ransom paid.	Espionage motives	Major supply chain attack affecting Santander, Ticketmaster etc.	AT&T suffered two breaches in 2024	Critical infrastructure attacks	$25M ransom paid	680GB of data stolen	400GB of data stolen	Filed for bankruptcy

Most Active Ransomware Groups & Strains 2024

In 2024, the ransomware landscape was dominated by several groups and strains that targeted a wide range of industries globally. Below is an overview of some of the most active ransomware entities:

- **RansomHub:** Emerging in 2024, this group quickly established itself as a major player, targeting critical infrastructure and industries worldwide.
- **LockBit 3.0:** The latest iteration of the infamous LockBit ransomware family, LockBit 3.0 continued to target businesses across various sectors, including a significant attack on a major retail chain.
- **Play:** Focused on government and healthcare, Play ransomware remained active, causing widespread disruption in targeted regions.
- **Dispossessor:** A newer strain that targeted mid-sized businesses globally, often evading detection with advanced obfuscation techniques.
- **Akira:** This group maintained its focus on small to medium-sized enterprises, with notable breaches in the education and automotive industries.
- **Hunters:** Known for their precision attacks, Hunters targeted financial services and tech firms, stealing and encrypting sensitive data.
- **Medusa:** Frequently targeting education and healthcare, Medusa caused operational disruptions and exposed sensitive personal data.
- **Qilin:** This ransomware-as-a-service group focused heavily on North American healthcare institutions, demanding significant ransoms.
- **BlackBasta:** Active across multiple sectors, including manufacturing and IT, BlackBasta utilized double-extortion tactics to pressure victims.
- **BianLian:** A rising ransomware group that focused on the technology sector, often employing stealthy infiltration techniques.



- **IncRansom:** A fast-evolving ransomware strain targeting diverse industries, focusing on encryption speed to increase pressure on victims.
- **BlackSuit:** A stealthy ransomware strain, BlackSuit targeted high-value organizations and avoided publicity to evade detection.
- **8Base:** Believed to be a continuation of older ransomware families, 8Base targeted mid-sized enterprises with frequent data breaches.
- **Meow**: This disruptive strain used unconventional encryption techniques to target businesses across different sectors.
- **KillSec:** A newer group that focused on critical infrastructure, executing attacks with high precision and significant impact.

Ransomhub

592 Victims in 2024

The victims span various sectors, including water and wastewater, information technology, government services and facilities, healthcare and public health, emergency services, food and agriculture, financial services, commercial facilities, critical manufacturing, transportation, and communications critical infrastructure.

The group emerged in mid-February 2024 and has already listed several organizations as alleged victims of their attacks, resulting from extortion through encryption and data leaks. The announcement of the sale of the new Ransomware-as-a-Service (RaaS) by RansomHub was published on one of the Russian-origin forums used by cybercrime to advertise malicious services, known as RAMP4U (or RAMP). A user with the nickname and persona of 'koley' announced the affiliate program on February 2, 2024.

In the new RaaS announcement, it was mentioned that the money laundering operation of the paid ransoms is the responsibility of the affiliate. This means that all communication and sending of the decryptor to the victim are done through chat. The split of this RaaS would be 90% of the value for the affiliate and 10% for the developer, who in this case would be the persona of Koley.

The payload would support network propagation and encryption of data both in secure and local mode. According to Koley, the ransomware is designed to operate on platforms such as Windows, Linux, and ESXi, as well as other architectures such as ARM and MIPS.

Lockbit

534 Victims in 2024

LockBit, also recognized as LockBit Black or Lockbit 3.0, is one of the largest Ransomware Groups in the world and has orchestrated extensive cyberattacks across various industries, impacting thousands of organizations globally with its relentless and adaptive strategies. In February 2024, LockBit suffered a critical blow after an international effort to dismantle its operations.

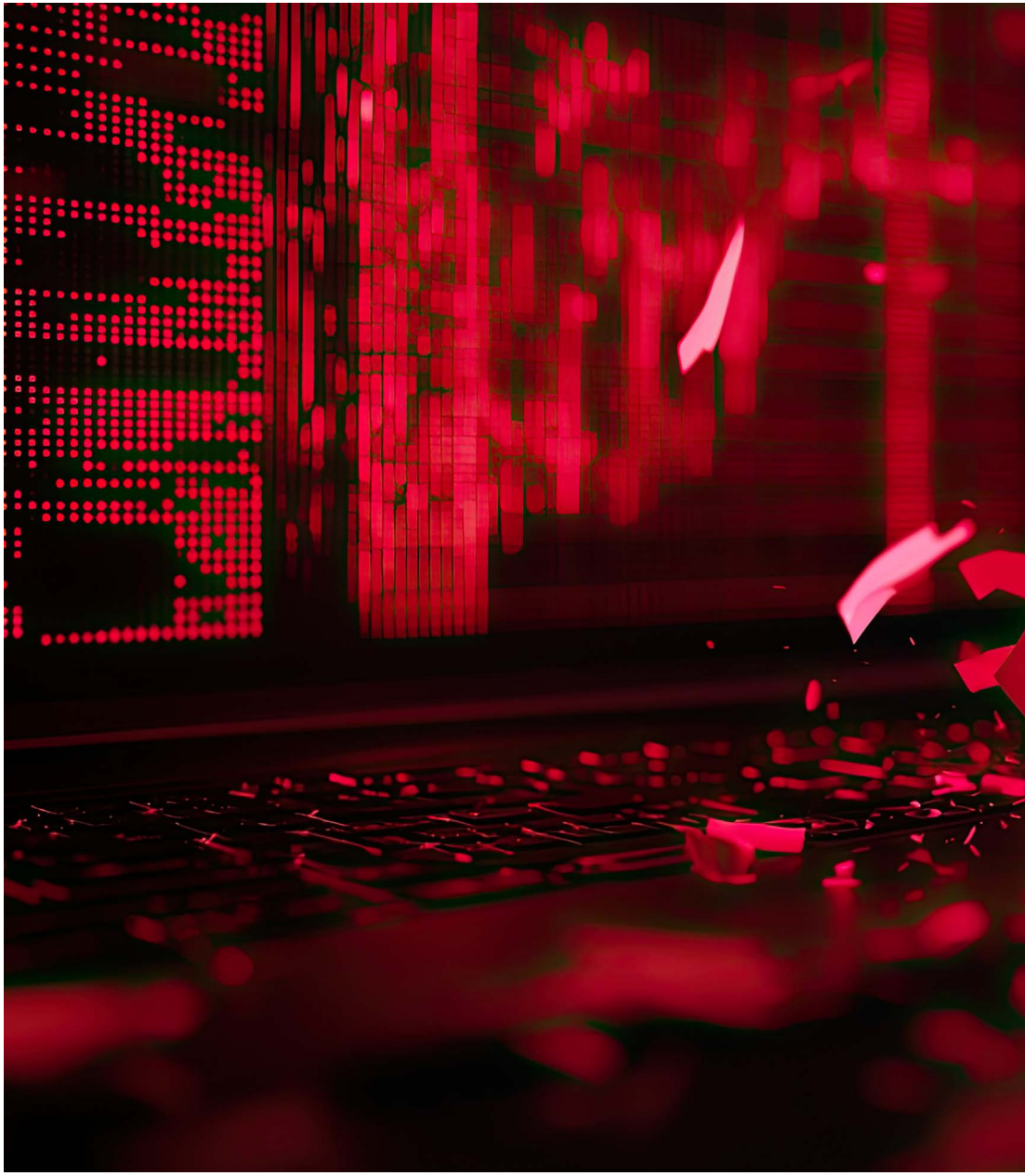
In a mission known as 'Operation Cronos', 10 core countries, including the UK and the US, plus 4 participating countries, including Ukraine, collaborated to seize LockBit's primary servers. In the aftermath of the takedown, LockBit made a new announcement in May 2024. It claimed that it had increased its attack volume, becoming the most active ransomware gang globally.

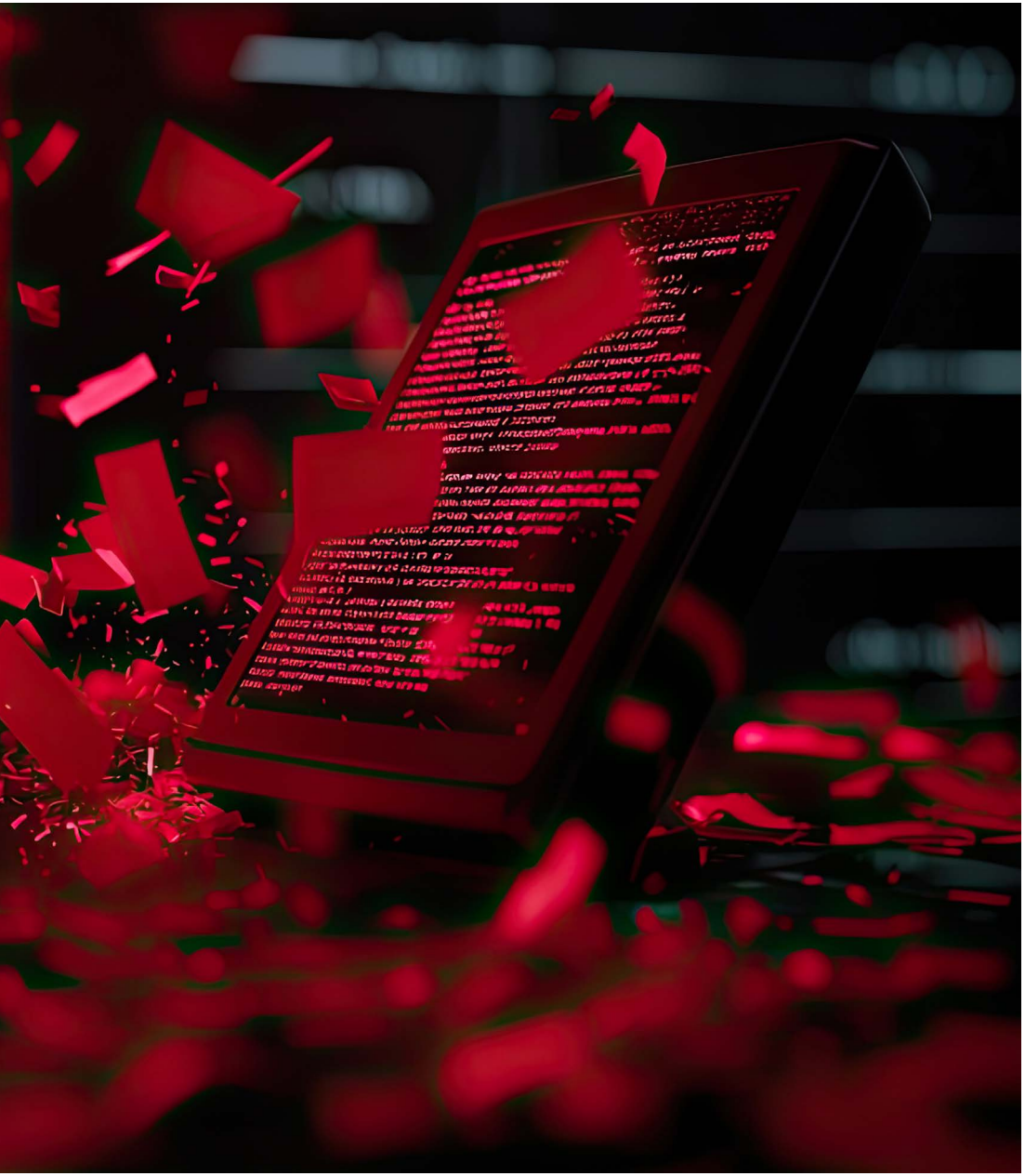
Play

359 Victims in 2024

Initially observed in June 2022, the Play ransomware (a.k.a PlayCrypt) operates through double extortion, targeting numerous organizations in Latin America. Its Initial. Access method is quite similar to other ransomwares, involving attacks such as Phishing, Exposed Services to the Internet, and Valid Account compromises.

On April 19, 2023, the security company Symantec published two new tools developed by the Play group. These tools allow the malicious actor to enumerate and exfiltrate data from the internal network. The post mentions the following: 'Play threat actors use the .NET infostealer to enumerate software and services via WMI, WinRM, Remote Registry, and Remote Service. The malware checks for the existence of security and backup software, as well as remote administration tools and other programs, saving the information in .CSV files that are compressed into a .ZIP file for later manual exfiltration by threat actors.'





Akira

291 Victims in 2024

The Akira ransomware group is said to have emerged in March 2023, and there's much speculation about its ties to the former CONTI ransomware group. It's worth noting that with the end of CONTI's operation, several affiliates migrated to independent campaigns such as Royal, BlackBasta, and others.

According to some reports, Akira affiliates also work with other ransomware operations, such as Snatch and BlackByte, as an open directory of tools used by an Akira operator was identified, which also had connections to the Snatch ransomware. The first version of the Akira ransomware was written in C++ and appended files with the '.akira' extension, creating a ransom note named 'akira_readme.txt,' partially based on the Conti V2 source code. However, on June 29, 2023, a decryptor for this version was reportedly released by Avast. Subsequently, a version was released that fixed the decryption flaw on July 2, 2023. Since then, the new version is said to be written in Rust, this time called 'megazord.exe,' and it changes the extension to '.powerranges' for encrypted files.

Most of Akira's initial access vectors use brute-force attempts on Cisco VPN devices (which use single-factor authentication only). Additionally, exploitation of CVEs: CVE-2019-6693 and CVE-2022-40684 for initial access has been identified.

Updated MITRE ATT&CK Tactics, Techniques and Procedures

The MITRE ATT&CK Framework is a globally recognized knowledge base that documents adversary tactics, techniques, and procedures (TTPs) observed in real-world cyberattacks. It helps security teams better understand attacker behaviors, identify gaps in their defenses, and develop proactive strategies for detection, mitigation, and response. By continuously updating the framework with new TTPs and detection analytics, MITRE ATT&CK empowers organizations to strengthen their security posture and stay ahead of evolving threats.

In 2024, MITRE ATT&CK introduced significant updates to its framework, enhancing the representation of adversary tactics, techniques, and procedures (TTPs).

April 2024 (v15) Updates:

New Techniques in Enterprise

- Abuse Elevation Control Mechanism: TCC Manipulation (v1.0)
- Command and Scripting Interpreter: AutoHotKey & AutoIT (v1.0)
- Compromise Infrastructure: Network Devices (v1.0)
- Create or Modify System Process: Container Service (v1.0)
- Hide Artifacts: File/Path Exclusions (v1.0)
- Hide Infrastructure (v1.0)
- Hijack Execution Flow: AppDomainManager (v1.0)
- Modify Authentication Process: Conditional Access Policies (v1.0)
- Obfuscated Files or Information: Encrypted/Encoded File (v1.0)
- Obtain Capabilities: Artificial Intelligence (v1.0)
- System Binary Proxy Execution: Electron Applications (v1.0)
- System Script Proxy Execution: SyncAppvPublishingServer (v1.0)

New Techniques in ICS

- Encrypted Channel: SSL Pinning (v1.0)
- Exploitation for Initial Access (v1.0)
- Hide Artifacts: Conceal Multimedia Files (v1.0)
- System Network Configuration Discovery: Internet Connection Discovery (v1.0)
- System Network Configuration Discovery: Wi-Fi Discovery (v1.0)

New Techniques in Mobile

- Encrypted Channel: SSL Pinning (v1.0)
- Exploitation for Initial Access (v1.0)
- Hide Artifacts: Conceal Multimedia Files (v1.0)
- System Network Configuration Discovery: Internet Connection Discovery (v1.0)
- System Network Configuration Discovery: Wi-Fi Discovery (v1.0)

October 2024 (v16) Updates:

New Techniques in Enterprise

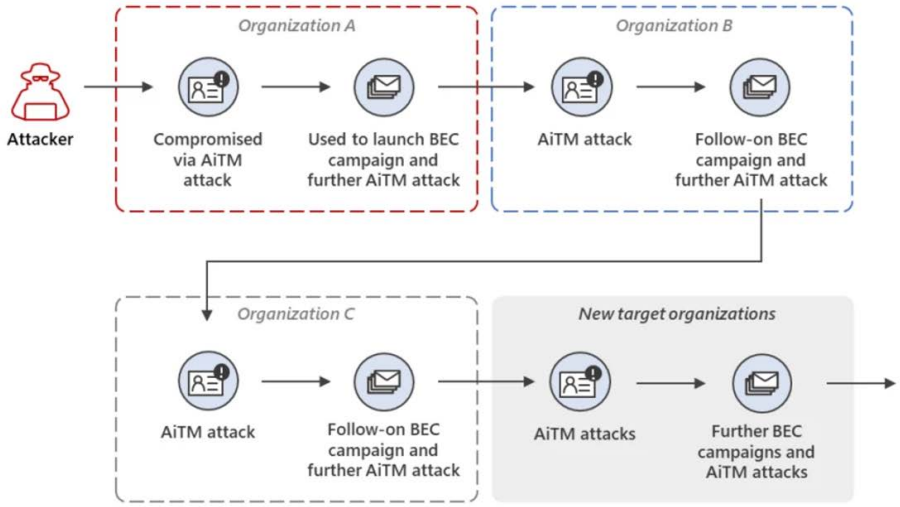
- Account Manipulation: Additional Local or Domain Groups (v1.0)
- Adversary-in-the-Middle: Evil Twin (v1.0)
- Application Layer Protocol: Publish/Subscribe Protocols (v1.0)
- Command and Scripting Interpreter: Lua (v1.0)
- Data Destruction: Lifecycle-Triggered Deletion (v1.0)
- Data from Information Repositories: Customer Relationship Management Software (v1.0)
- Data from Information Repositories: Messaging Applications (v1.0)
- Event Triggered Execution: Udev Rules (v1.0)
- Execution Guardrails: Mutual Exclusion (v1.0)
- Indicator Removal: Relocate Malware (v1.0)
- Masquerading: Masquerade Account Name (v1.0)
- Modify Cloud Resource Hierarchy (v1.0)
- Obfuscated Files or Information: Polymorphic Code (v1.0)
- Resource Hijacking: Bandwidth Hijacking (v1.0)
- Resource Hijacking: Cloud Service Hijacking (v1.0)
- Resource Hijacking: Compute Hijacking (v1.0)
- Resource Hijacking: SMS Pumping (v1.0)
- Steal or Forge Kerberos Tickets: Ccache Files (v1.0)
- Trusted Developer Utilities Proxy Execution: ClickOnce (v1.0)

These updates reflect MITRE ATT&CK's commitment to evolving with the cybersecurity landscape, providing organizations with a comprehensive and up-to-date framework for understanding and mitigating adversary behaviors.

A Growing Focus on Phishing

Phishing attacks in 2024 have grown in sophistication, leveraging legitimate infrastructure and advanced techniques to target organizations across industries. For example, the Smarttech247 security researchers have noted that attackers are increasingly exploiting trusted platforms such as SharePoint to deploy malicious payloads.

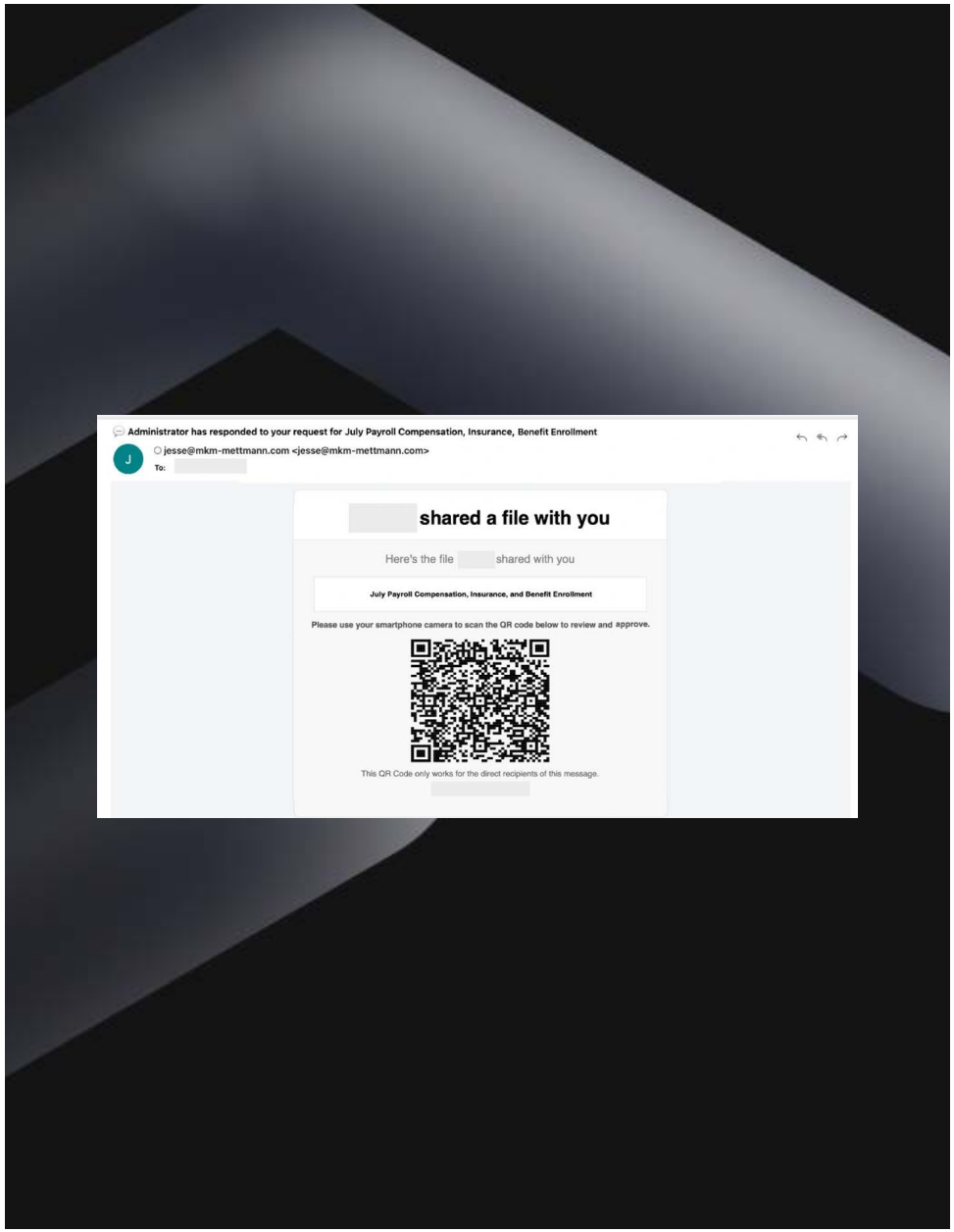
By compromising legitimate accounts, they exploit Microsoft's native notification system, which permits external participants to receive notifications. This method allows malicious emails to bypass standard security filters and appear entirely legitimate. For instance, in May 2024, organizations recorded a surge in attacks using SharePoint notifications, where attackers tricked recipients into downloading malicious files disguised as business documents. The convincing nature of these notifications resulted in significant breaches, as employees were more likely to trust familiar platforms. Another troubling trend involves multi-stage phishing campaigns, which simulate ongoing conversations to gain user trust. Attackers often pose as IT support or HR representatives and send follow-up emails to previously initiated phishing attempts, making the communication appear legitimate. These campaigns frequently incorporate adversary-in-the-middle (AiTM) techniques, where attackers intercept login credentials and multi-factor authentication tokens using reverse proxy servers. In one incident, employees received emails urging them to resolve a technical issue with their accounts.



When users followed the link and entered their credentials, the phishing infrastructure intercepted both their usernames and MFA codes in real time. This allowed attackers to bypass MFA protections entirely and gain unauthorized access to sensitive systems without the users' awareness.

Attackers have also turned to QR code-based phishing to evade detection. Traditional URL-scanning tools are often bypassed when malicious links are embedded in QR codes instead of direct URLs.

The attack typically works by persuading the victim to scan a QR code—sometimes under the pretense of an urgent payment update, account verification, or IT notice. These campaigns are often coupled with AiTM techniques to intercept session cookies or MFA tokens.



Phishing Landscape Evolution: 2022 vs. 2023-2024

Over the past two years, phishing attacks have evolved from generic campaigns to highly targeted and multi-faceted operations. In 2022, attacks typically relied on poorly written emails containing obvious grammatical errors and malicious attachments. By contrast, 2023 and 2024 have seen a shift to sophisticated delivery methods, including the use of QR codes, PDFs, and trusted platforms such as SharePoint. Language and quality have improved dramatically, with attackers leveraging AI to craft well-written, professional-looking emails at scale. Detection techniques have also needed to evolve, moving beyond basic URL scanning to incorporate behavior-based and AI-driven analysis. Organizations that once relied on employee training and static filters now require comprehensive defense-in-depth strategies to address the growing complexity of phishing threats.

Organizations are adapting to these evolving threats through a combination of proactive measures and advanced technologies. Enhanced employee awareness and continuous training programs are helping staff recognize the more subtle forms of phishing, such as QR-based or AI-generated campaigns. While multi-factor authentication remains a cornerstone of organizational security, attackers' ability to bypass it using AiTM techniques has necessitated advancements in MFA technology. Proactive threat-hunting practices, such as identifying suspicious patterns in login activity or email behavior, are becoming essential to preempt phishing campaigns before they succeed. Organizations are also adopting zero-trust architectures, ensuring that every user and device is verified continuously. Additionally, integrating real-time threat intelligence allows organizations to track phishing trends, identify emerging tactics, and respond swiftly to potential breaches.

The sophistication and frequency of phishing attacks observed in 2024 underscore the need for organizations to remain vigilant. As threat actors continue to exploit legitimate services, leverage advanced techniques like AiTM, and incorporate AI tools, the line between legitimate communication and malicious campaigns is becoming increasingly blurred. Safeguarding sensitive information and critical infrastructure requires a collaborative approach, combining advanced detection systems, proactive defenses, and user awareness to counteract these evolving cyber threats effectively.

The Perfect Imposter: How AI-Powered BEC Schemes Hit Hard in 2024

Business Email Compromise remained a critical and growing cybersecurity threat in 2024, posing significant financial and operational risks to organizations. Unlike generic phishing campaigns, BEC attacks are highly targeted, relying on social engineering and impersonation to manipulate trusted relationships within an organization. Attackers carefully craft emails to impersonate executives, suppliers, or other trusted entities, exploiting the urgency and authority conveyed in these messages to trick employees into authorizing fraudulent payments or sharing sensitive information.

In 2024, a major incident underscored the evolving danger of BEC. A Connecticut-based firm fell victim to a carefully orchestrated attack where cybercriminals impersonated a senior finance executive. Using publicly available data and AI tools, attackers crafted convincing emails tailored to the company's ongoing merger process, requesting urgent fund transfers for "legal fees" associated with the deal. The attackers exploited the pressure and confidentiality surrounding the transaction, resulting in a fraudulent transfer of $3.5 million before the breach was detected.

This incident highlights how BEC campaigns are becoming more sophisticated, leveraging AI tools to personalize messages, remove grammatical inconsistencies, and mimic authentic communication patterns. These advancements have made BEC harder to detect, increasing both its volume and success rate in 2024. The financial and reputational impacts of such attacks continue to make BEC one of the most critical threats organizations face today.

Phishing Landscape Evolution: 2022 vs. 2023-2024

Key Focus Area	2022: Traditional Threats	2023-2024: Modern Challenges
Attack Complexity	• Focused on generic, mass phishing campaigns.	• Shift to sophisticated, multi-stage attacks targeting specific organizations and individuals.
Delivery Techniques	• Heavy reliance on direct malicious links and email attachments.	• Use of Adversary-in-the-Middle (AiTM) techniques for credential interception. • Use of trusted services like SharePoint and DocuSign to deliver malicious content. • Integration of QR codes to bypass URL scanning and traditional filters.
Language and Credibility	• Poorly written emails with obvious grammar and spelling errors.	• Highly polished, AI-enhanced emails that mimic legitimate communication with personalized content.

Shifts in Vulnerability Management

The vulnerability management landscape in 2024 has undergone a significant evolution, driven by the increasing sophistication of attack techniques and the shift from volume-based patching to exposure-based strategies.

As attackers adopt timing-based attacks, backdoor exploits, and cache manipulation methods to compromise mature systems, organizations must align their defenses with real-world threats to prioritize actionable vulnerabilities and reduce exposure effectively.

Traditionally, organizations relied on periodic scanning to identify vulnerabilities across operating systems, software, and infrastructure. Success was measured by the sheer number of patches applied, with little emphasis on exploitability or real-world risk. This led to resource inefficiencies, where low-risk vulnerabilities were prioritized while critical, actively exploitable gaps remained unaddressed.

The limitations of this model became clear as attackers shifted tactics, focusing on advanced techniques such as:

- Timing Attacks: Exploiting minute delays or system race conditions to manipulate secure processes.
- Supply Chain Backdoors: As seen in the XZ Utils backdoor, attackers infiltrate widely trusted tools over years to introduce malicious code.
- Cache Poisoning: Leveraging discrepancies across HTTP servers and CDNs to store malicious payloads.

These vulnerabilities underscore the need for a contextual risk-based approach to remediation, rather than relying solely on patching metrics.

1. Rise of Timing-Based Attacks: A New Era of Sophistication

The overall maturity of modern platforms and systems has made traditional attacks less effective. In response, attackers have adopted time-based techniques like race conditions to exploit minute delays and system behaviors. These attacks require a deeper understanding of system processes and are far more complex to execute but can cause devastating consequences.

Windows Downdate: Downgrade Attacks Using Windows Updates

Discovered in August 2024, Windows Downdate exploits a flaw that allows attackers with administrative access to downgrade fully patched Windows systems to earlier, vulnerable versions. This reintroduces previously fixed security issues while the system falsely reports itself as fully updated, making detection exceptionally challenging.

The insidious nature of this attack highlights how time-based vulnerabilities can bypass traditional monitoring systems, potentially exposing organizations to legacy exploits and creating significant operational risks.

2. regreSSHion: A Critical OpenSSH Remote Code Execution Vulnerability

A standout vulnerability in 2024, regreSSHion (CVE-2024-3094) impacts OpenSSH server instances in their default configuration, enabling unauthenticated remote code execution (RCE) with root privileges on glibc-based Linux systems. The scale of exposure is staggering:

- 14 million potentially vulnerable OpenSSH servers were identified on the Internet using tools like Censys and Shodan.

While current exploitation remains constrained to specific distributions (e.g., i386 Ubuntu), this vulnerability demonstrates the severe risks posed by widespread, unpatched systems. The combination of remote exploitability and privileged access underscores the critical need for timely vulnerability management and patching processes.

3. XZ Utils Backdoor: A Cautionary Tale of Supply Chain Risks

One of the most alarming developments in 2024 was the discovery of a malicious backdoor in the Linux xz utility. Introduced by a threat actor using the pseudonym Jia Tan, this backdoor highlights the evolving risks of supply chain attacks. The attacker spent over three years building trust and introducing subtle modifications to the codebase, culminating in a backdoor that allowed attackers to:

- Bypass SSH authentication
- Gain unauthorized remote access to affected systems

Although the backdoor (CVE-2024-3094) had not yet reached widespread production environments, it was detected in development versions of major Linux distributions. This discovery—credited to software developer Andres Freund—emphasizes the importance of rigorous code reviews and supply chain security.

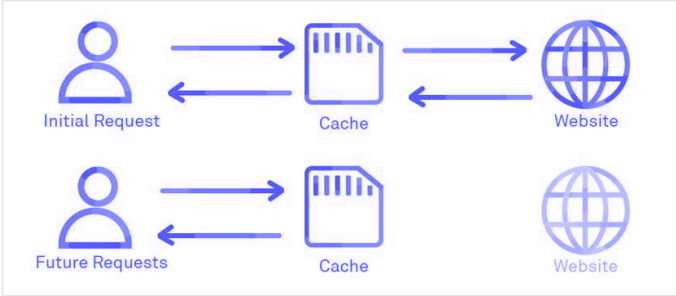


Image Source: AppCheck

4. Cache Attacks: Exploiting Modern Web Infrastructure

Web caching systems, designed to enhance performance and minimize latency, have become a new focus for attackers. In 2024, researchers demonstrated how inconsistencies across HTTP servers and Content Delivery Networks (CDNs) could be exploited for:

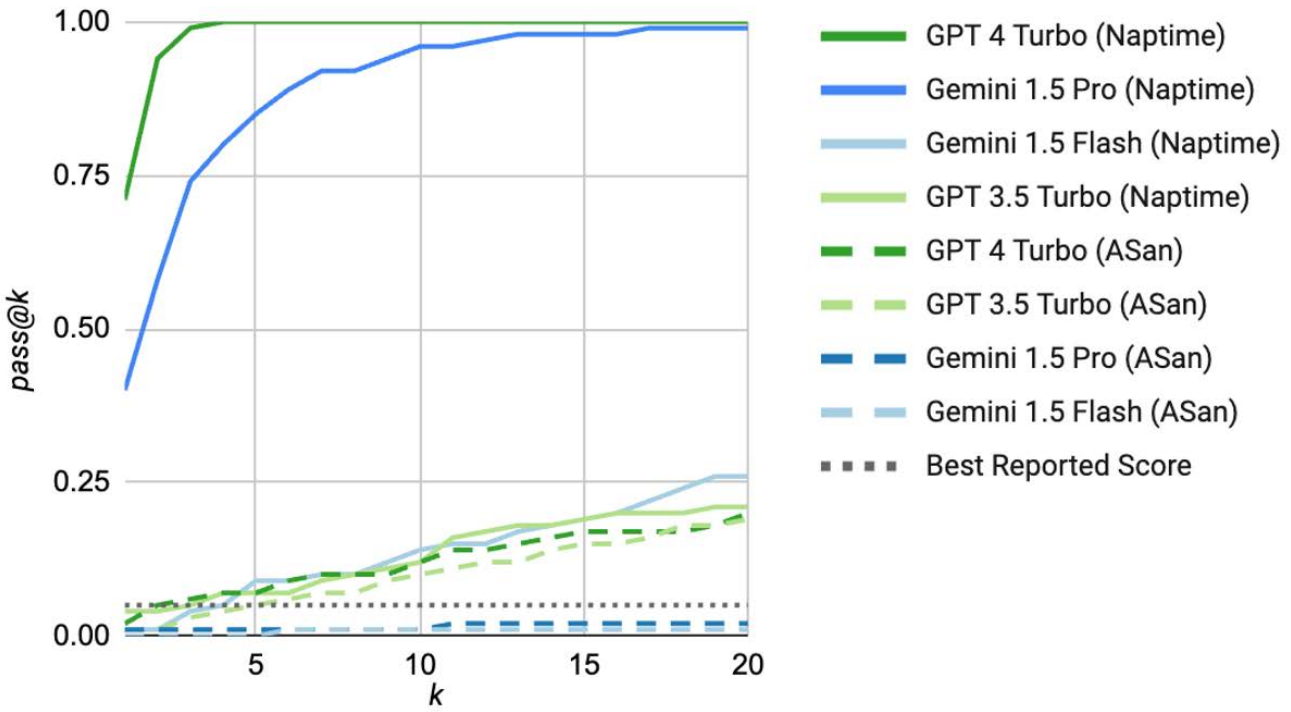
- Web cache poisoning
- Cache deception
- Data hijacking

Attackers manipulated URL discrepancies and normalization processes to trick caches into storing malicious or unauthorized content. This technique allows malicious payloads to propagate across cached responses, affecting large numbers of users and systems.

AI's Impact on Vulnerability Research: Project Naptime

Instead of being merely a vector for exploitation, AI demonstrated its proactive value by assisting researchers in identifying, analyzing, and even patching software flaws. Project Naptime highlighted how LLMs, when provided with the right tools and guidance, could move beyond theoretical benchmarks and deliver tangible results. Researchers moved from skepticism, where AI systems were believed to have minimal impact on cyber exploitation, to a point of measurable success. The benchmark progression was striking: from "LLMs not likely to disrupt cyber exploitation" to "LLMs performing basic vulnerability research with near 100% success."

This paradigm shift underscored AI's role as a force multiplier for security researchers, automating repetitive tasks, reducing manual effort, and enabling faster discovery of flaws across complex systems. By amplifying efficiency, tools like Project Naptime are bridging the gap between human expertise and machine-driven analysis, setting a precedent for the integration of AI in proactive security research. As organizations increasingly adopt AI-driven approaches, this transformation highlights a new era where AI not only protects systems but also fortifies software development lifecycles by preemptively addressing vulnerabilities.



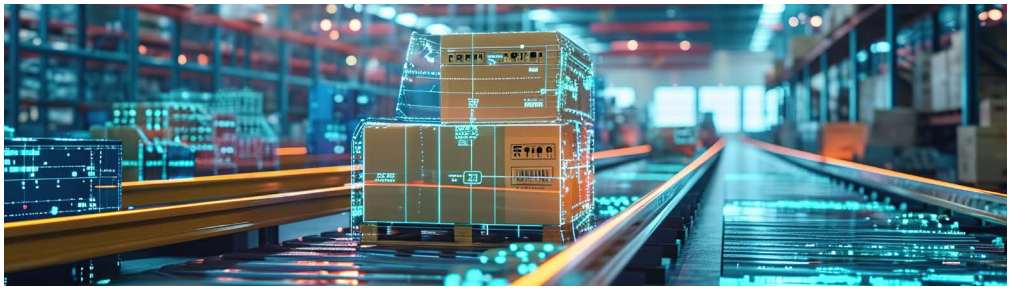
In the buffer overflow tests, the LLM is required to "exploit" a buffer overflow vulnerability to make the program output a score which cannot be achieved in "normal" execution. Reference: Project Naptime, Evaluating Offensive Security Capabilities of Large Language Models.

Supply Chain Vulnerabilities: The Weakest Link in 2024

No organization operates in isolation, and as the adage goes, “a chain is only as strong as its weakest link.” In 2024, supply chain vulnerabilities remained one of the most significant cybersecurity challenges, with multiple incidents demonstrating the cascading impact that disruptions can have across industries. These incidents exposed not just the weaknesses of third-party dependencies but also the need for organizations to rethink how they monitor, evaluate, and secure their broader ecosystems.

The CDK Global Ransomware Attack in June 2024 mentioned earlier in the report was a stark reminder of the consequences of relying on third-party software providers. The BlackSuit ransomware group exploited an unpatched vulnerability within CDK Global's systems, leading to widespread disruption for thousands of car dealerships across the United States. With critical systems for managing inventory, processing sales, and facilitating repairs rendered inoperable, the attack effectively halted operations for days, leading to millions in financial losses and reputational damage. This incident highlighted not only the need for proactive patch management by suppliers but also for organizations to enforce stronger third-party risk assessments to identify and mitigate dependencies on vulnerable systems. For automotive businesses, the breach was a turning point, forcing a reconsideration of reliance on centralized service providers and the need for redundant systems to mitigate operational downtime.

In another significant event, Snowflake's supply chain breach demonstrated the risks of third-party cloud service dependencies. Although the initial breach targeted Snowflake's infrastructure, the ripple effect impacted dozens of its clients, including financial institutions and healthcare organizations, whose sensitive data was exposed or accessed by unauthorized actors. This breach emphasized the vulnerabilities inherent in shared cloud environments and the importance of validating the security protocols of cloud service providers. Organizations relying on cloud infrastructure must now integrate continuous supply chain monitoring tools to detect abnormal activity and ensure their suppliers adhere to rigorous security standards. The breach also reinforced the necessity of data encryption, both at rest and in transit, to minimize damage even in the event of a third-party compromise.



However, it is not always malicious actors that trigger disruption. The CrowdStrike release update incident provided a unique perspective on supply chain challenges in 2024. A flawed software update released by the cybersecurity company unintentionally caused system crashes across critical infrastructure providers, financial institutions, and retail businesses. Major enterprises faced temporary operational paralysis, highlighting that software reliability is just as critical as defense against cyberattacks. This incident served as a wake-up call for organizations to implement stronger change management processes, test updates rigorously before deployment, and maintain contingency plans to minimize the impact of unforeseen disruptions caused by trusted vendors.

Beyond these high-profile cases, smaller-scale supply chain attacks proliferated in 2024, with attackers exploiting overlooked vulnerabilities in smaller third-party vendors to infiltrate larger organizations. In one instance, a manufacturing firm experienced a ransomware attack after an attacker compromised an HVAC provider's software, which was integrated into the manufacturer's operational systems. Such incidents highlight that even seemingly benign third-party relationships can become entry points for cyberattacks. Businesses increasingly recognize the importance of implementing zero-trust principles, requiring suppliers to adhere to least-privilege access policies and undergo routine security audits.

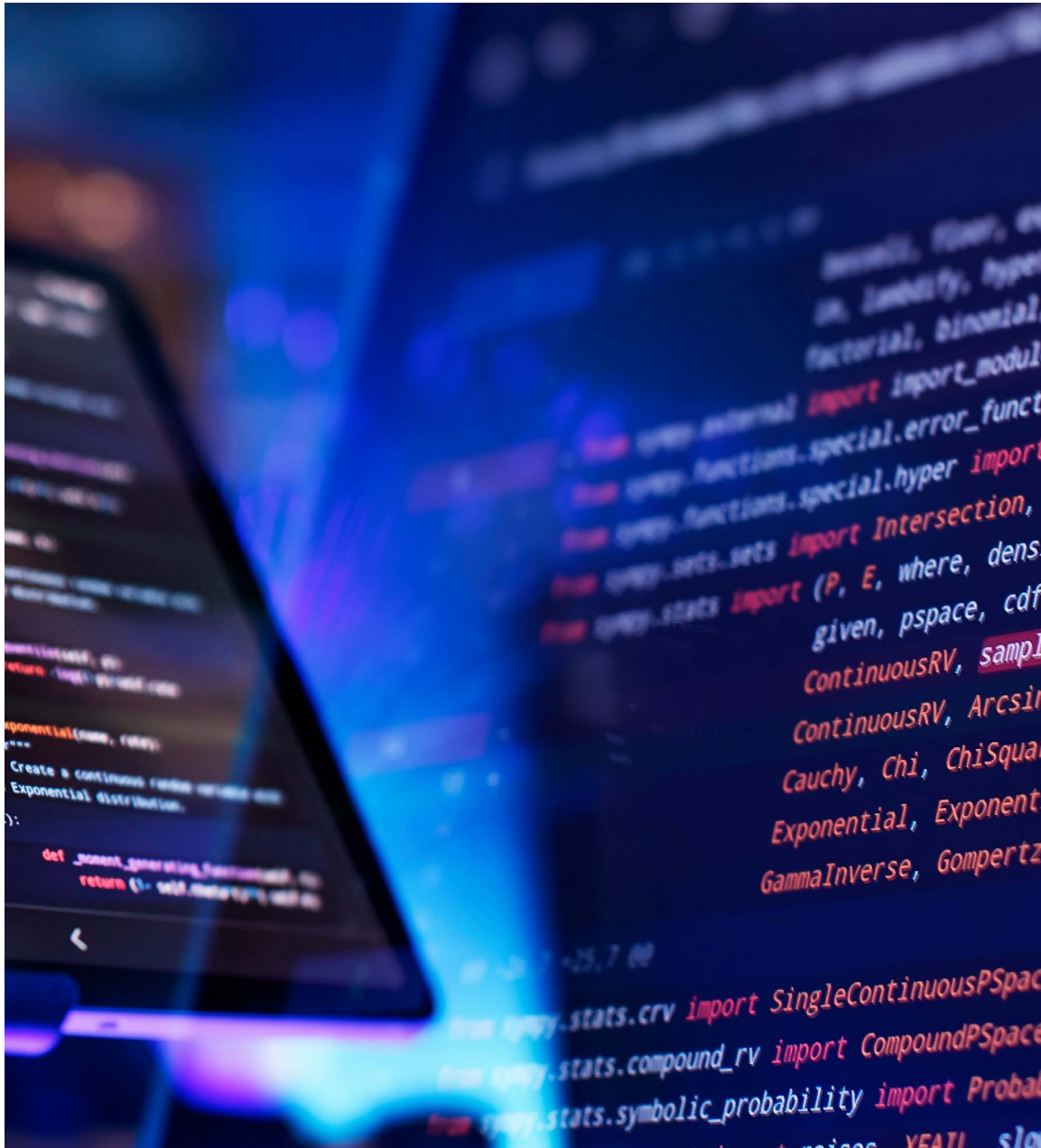
Increased Targeting of Open-Source Software Dependencies in 2024

In 2024, open-source software dependencies emerged as a critical vector for supply chain attacks. Open-source components are foundational to modern software development, with organizations integrating these libraries and frameworks into their applications to accelerate development and reduce costs. However, this reliance also creates significant risks, as vulnerabilities or malicious alterations in widely used dependencies can have widespread and cascading impacts.

Attackers increasingly targeted open-source ecosystems by exploiting vulnerabilities or injecting malicious code into popular repositories. These tactics allowed them to compromise a single component and reach thousands—or even millions—of downstream users.

One notable example from 2024 involved the compromise of a widely used npm package (a JavaScript library). In this incident, attackers compromised the lottie-player npm package by gaining unauthorized access to a developer's account through a phishing attack. They then injected malicious code into the package, which targeted cryptocurrency wallets by exfiltrating sensitive information from applications that integrated the compromised library. Another major incident occurred within the Python Package Index (PyPI) ecosystem, where attackers uploaded packages with names nearly identical to legitimate libraries—a tactic known as typosquatting.

These malicious packages were designed to steal credentials or install backdoors in affected systems. Organizations that unknowingly incorporated these malicious packages into their software pipelines faced significant risks, including compromised customer data and unauthorized access to internal networks.



Operational Technology Attacks: A Growing Threat in 2024

The year 2024 saw a significant surge in cyberattacks targeting Operational Technology environments, with critical infrastructure, industrial processes, and IoT devices increasingly in the crosshairs of cybercriminals and state-sponsored actors.

According to the SANS 2024 ICS/OT Cybersecurity Report, 24% of OT compromises originated from internet-accessible devices, while 20% stemmed from vulnerabilities in employee workstations or removable media. Alarmingly, although ransomware only accounted for 12% of reported incidents, its impact on OT systems was described as potentially catastrophic. Hybrid IT-OT attacks also grew more prevalent, with attackers leveraging IT networks as a pathway to infiltrate OT systems.

These statistics underscore the urgency for organizations to strengthen OT defenses as the threat landscape evolves. Real-world incidents from 2024 illustrate how attackers exploited vulnerabilities in both legacy systems and emerging technologies to disrupt critical services, jeopardize public safety, and impose significant economic costs.

Pro-Russia Hacktivist Campaigns Against Water and Wastewater Systems

Pro-Russia hacktivists, emboldened by geopolitical tensions, targeted North American and European water and wastewater systems (WWS) throughout 2024. In April, several U.S.-based WWS operators reported unauthorized access to their systems via outdated Virtual Network Computing (VNC) protocols. Exploiting weak or default passwords, attackers manipulated Human Machine Interfaces (HMIs) to push pump and blower equipment beyond safe operating parameters. In some cases, this caused tank overflows and alarm silencing, leaving operators temporarily locked out.

While the disruptions were contained by reverting to manual controls, these incidents demonstrated how even unsophisticated threat actors can exploit basic security lapses to disrupt OT operations.

American Water: A Wake-Up Call for Critical Infrastructure

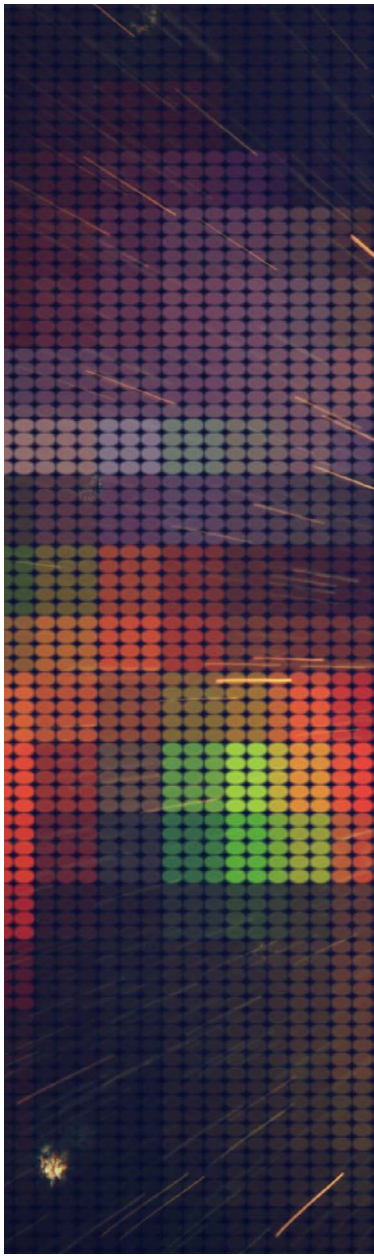
In October 2024, American Water, the largest water utility in the United States, experienced a cybersecurity incident that forced the company to take critical systems offline. While no disruption to water or wastewater services was reported, the company's customer portal and internal systems faced downtime. The incident highlighted the risks associated with interconnected IT and OT networks, where breaches in one system can cascade into others.

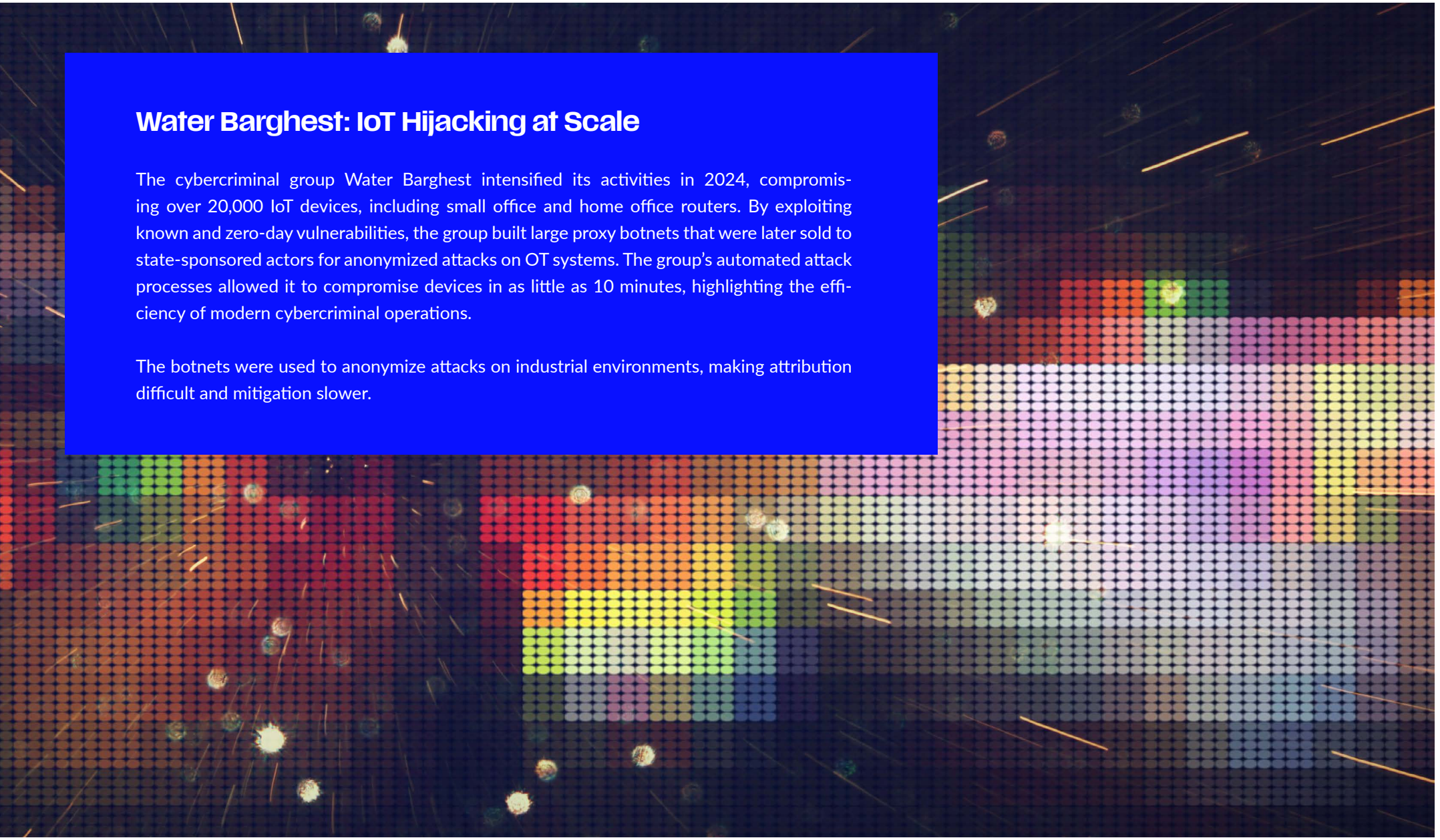
American Water's swift response, which included reverting to manual processes and conducting system integrity checks, mitigated further damage.

Iranian APTs Expand Their Reach

Iranian threat group Emennet Pasargad (Cotton Sandstorm) expanded its operations in 2024, targeting new IT-connected OT assets such as IP cameras. Operating under the guise of legitimate IT companies like ASA, the group leveraged compromised devices to gain access to ICS environments in France and Sweden. These campaigns demonstrated how state-sponsored actors use innovative tactics, such as cover companies, to obfuscate their activities and enhance their operational reach.

Their activities involved harvesting data from IP cameras and attempting to disrupt events like the 2024 Paris Olympics by compromising a French commercial dynamic display provider to disseminate anti-Israel messages.





Water Barghest: IoT Hijacking at Scale

The cybercriminal group Water Barghest intensified its activities in 2024, compromising over 20,000 IoT devices, including small office and home office routers. By exploiting known and zero-day vulnerabilities, the group built large proxy botnets that were later sold to state-sponsored actors for anonymized attacks on OT systems. The group's automated attack processes allowed it to compromise devices in as little as 10 minutes, highlighting the efficiency of modern cybercriminal operations.

The botnets were used to anonymize attacks on industrial environments, making attribution difficult and mitigation slower.

Perspectives for 2025

As cybersecurity risks evolve and organizations adapt to a complex threat landscape, 2025 is set to be a pivotal year. The convergence of emerging technologies, regulatory pressures, and sophisticated threat actors will drive significant shifts in how organizations approach security. Here are key perspectives that will shape the cybersecurity landscape.

1. Insider Threats Amplified by AI

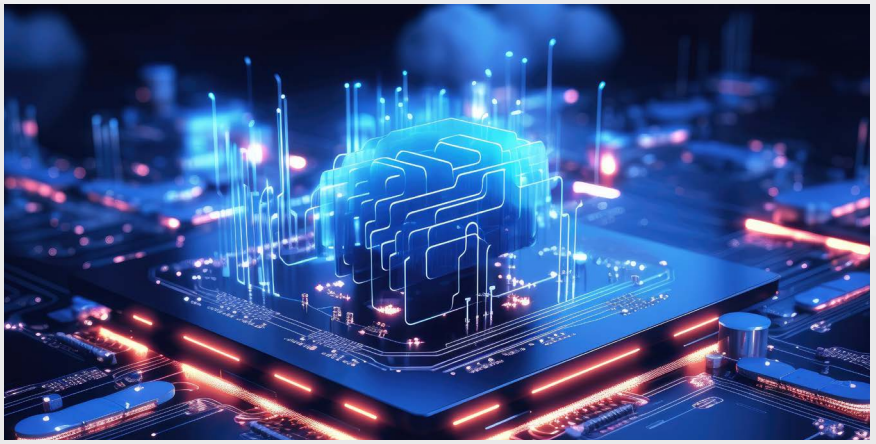
AI's increasing presence in the workplace is redefining the nature of insider threats. Generative AI tools, such as those used for content creation, code development, or report generation, bring productivity gains but also new risks. Employees, either intentionally or inadvertently, may misuse these tools to access or expose sensitive information.
The improper adoption of these tools—particularly without clear data classification, access controls, and AI system oversight will leave organizations vulnerable to significant risks, including data leaks, regulatory fines, and escalated security threats.

Data Leakage and Uncontrolled AI Systems

Many organizations are integrating AI tools like GenAI models (e.g., ChatGPT or CoPilot) without adequately classifying their data or controlling how these tools interact with sensitive information. Employees, often unintentionally, input proprietary information such as trade secrets, financial data, or customer records into AI systems that are hosted externally. Once fed into third-party AI platforms, this data cannot be retrieved or controlled, leading to irreversible leaks and exposure.
Additionally, businesses adopting broader AI technology stacks, including off-the-shelf AI solutions for automation and analytics, may fail to assess how these systems store or process their data. Without strict controls, these tools can introduce shadow AI—unvetted and unmanaged AI deployments that bypass traditional security measures, exposing critical assets to potential breaches.

Regulatory bodies are responding to the rapid proliferation of AI tools with strict frameworks to ensure transparency, accountability, and security. The EU AI Act for example, mandates that organizations using AI systems adhere to compliance requirements, such as risk assessments, system monitoring, and data governance policies. Organizations failing to control their AI systems, particularly those processing sensitive or high-risk data, risk substantial fines and legal consequences under such frameworks.

In response to these challenges, the adoption of Data Detection and Response solutions is becoming a priority. DDR focuses on identifying where sensitive data resides across an organization's repositories, including AI tools, and ensuring that it is classified, monitored, and protected. As organizations continue to integrate AI into workflows, DDR tools can detect unauthorized data usage or exfiltration within AI platforms, monitor AI systems for data leaks, misuse, or misconfigurations – and enforce access controls and prevent sensitive data from being processed by unvetted AI tools.



To mitigate the risks associated with AI technologies, organizations must take proactive steps:

1. Implement an AI Usage Policy: Establish clear policies governing the use of AI tools across the organization. This includes guidelines for data input, tool approval processes, and employee training to prevent accidental data exposure.

2. Enforce Data Classification and Access Controls: Ensure sensitive data is properly classified and protected. Use access controls to restrict what data can be processed by AI systems and who can interact with these tools.

3. Adopt Data Detection & Response Solutions: Integrate DDR solutions to monitor and secure data across AI environments, ensuring real-time detection of leaks or misuse.

4. Conduct AI Risk Assessments: Regularly assess AI systems for vulnerabilities, compliance gaps, and data security risks. Align AI deployments with regulatory requirements like the EU AI Act to avoid penalties.

5. Integrate AI Governance Frameworks: Develop governance frameworks that oversee the lifecycle of AI systems—from procurement and deployment to monitoring and decommissioning—to ensure accountability and security.

> **By 2025, the interplay between human trust and AI misuse will demand robust access controls, data classification, and employee training to mitigate risks.**

2. AI-Powered Cyber-crime-as-a-Service

AI is not just enhancing security defenses but also empowering cybercriminals. The dark web has become a marketplace for Cybercrime-as-a-Service, where unsophisticated attackers can purchase pre-built AI tools for malware generation, phishing automation, and vulnerability exploitation. This democratization of cyber capabilities has lowered the entry barriers for threat actors, enabling even small groups to launch large-scale attacks.

In 2025, AI will streamline the development of malicious campaigns, automate reconnaissance, and enhance payload delivery. Criminals will use AI-powered chat-bots and tools to generate convincing phishing emails, refine malware, and manipulate victims. This surge in cybercrime sophistication will force organizations to invest in AI-driven threat detection systems capable of analyzing behaviors and identifying anomalies in real time.

AI-Enhanced Phishing Campaigns: Cybercriminals leverage AI-powered chatbots and large language models (LLMs) to craft highly personalized and convincing phishing emails that bypass traditional filters. These campaigns dynamically adapt to targets, using real-time data to mimic trusted communications.

Malware Automation: AI is being used to automate malware development, enabling attackers to inject malicious code into legit-imate software at scale. AI models optimize payload delivery and evasion techniques to bypass endpoint protection systems.

Reconnaissance Automation: AI streamlines reconnaissance by scanning vast datasets for vulnerabilities, misconfigurations, and exposed credentials. Attackers use this data to craft target-ed campaigns and prioritize high-value assets.

AI-Assisted Fraud and Deepfakes: Cybercriminals leverage AI tools to generate deepfake videos, impersonating executives to facilitate large-scale financial fraud or ransomware schemes.

Key Recommendations for Organizations

1. Deploy real-time threat monitoring capable of analyzing user behavior and identifying anomalies in real time.

2. Defense-in-Depth Security Measures: Implement multi-layered security strategies that combine endpoint protection, network segmentation, and cloud-based threat analysis.

3. Employee Training and Awareness: Regularly train employees to identify AI-enhanced threats like sophisticated phishing emails and deepfake attacks. Simulate campaigns to test and improve employee resilience against evolving social engineering tactics.

4. Dark Web Monitoring and Threat Intelligence: Integrate dark web threat intelligence solutions to identify emerging AI-driven tools and pre-emptively block malicious activities. Use real-time monitoring to detect leaked credentials, vulnerabilities, or exploits being sold on underground markets.

5. Strict Governance of AI Systems: Develop governance policies for internal AI use, ensuring ethical and secure deployment. Monitor third-party AI tools for vulnerabilities or misuse that could be exploited by attackers.

3. The Advancement of Quantum Computing

The rapid advancement of quantum computing is unfolding faster than anticipated, posing a critical threat to traditional cryptographic systems. Quantum computers, once mature, will have the capacity to rapidly factorize prime numbers, breaking the complex mathematical foundation that underpins these encryption methods. Experts warn that "Q-Day"—the point when quantum computers can render current encryption obsolete—could arrive within just a few years. Researchers highlight that technologically advanced nation-states are already preparing for this eventuality. Governments and adversaries are believed to be actively harvesting encrypted data today, anticipating its future decryption once quantum capabilities mature. This presents an existential threat to data security, particularly for long-term sensitive information such as military plans, intellectual property, personal records, and financial data.

Industries where confidentiality is critical—such as finance, healthcare, and government—face the most significant risks. Sensitive data intercepted now could be decrypted years later, leaving organizations exposed to espionage, intellectual property theft, and severe reputational damage. Agencies around the world are preparing guidelines for organizations to prepare for the threat posed by quantum computing. For example, Singapore's Cyber Security Agency (CSA) will start issuing guidelines in 2025 and they are prioritizing essential service providers, including those in healthcare, telecommunications, finance, and public utilities, as well as select government agencies.

Key Recommendations for Organizations

1. **Conduct a Quantum-Safe Risk Assessment and Inventory:** Organizations should immediately begin assessing their data assets and cryptographic infrastructure to identify vulnerabilities to quantum computing. Prioritize high-value and long-lifespan data, such as healthcare records, trade secrets, and financial information, for early migration to quantum-safe cryptographic standards. This includes creating a detailed inventory of all cryptographic algorithms in use across systems to understand the scope of required upgrades.

2. **Adopt a Phased Transition Plan for Post-Quantum Cryptography:** The transition to post-quantum cryptography (PQC) is a lengthy process that could take over a decade. Organizations must adopt a phased approach that aligns with guidelines and global standards, such as those from NIST.

3. **Monitor Quantum Security Developments and Regulatory Guidance:** Stay informed on emerging quantum security standards and advancements endorsed by regulators. Establish a cross-functional team to track industry progress, evaluate commercial quantum-safe tools, and ensure compliance with evolving regulatory requirements. Early adopters of quantum-safe measures will gain a strategic advantage in securing their systems against future quantum threats.

4. Unified, Integrated Approach For A More Secure 2025

At Smarttech247, we predict that 2025 will bring a more unified and strategic approach to cybersecurity as organizations face increasingly sophisticated threats. Zero Trust principles, powered by AI-driven monitoring, will become central to defense strategies, while cloud and API security tools will play a critical role in securing hybrid infrastructures. Automation will streamline incident response and threat management, helping businesses overcome complexity and resource shortages. Secure enterprise browsers will emerge as a key defense against rising browser-based attacks, and the consolidation of cybersecurity tools will simplify operations and improve efficiency.

We also foresee a shift in the strategic consumption of Threat Intelligence, enabling organizations to proactively prioritize risks and enhance decision-making. Foundational security practices like passwordless authentication (Passkeys and WebAuthn), deception-based tools (honeytokens), and dynamic conditional access will further strengthen organizational resilience. By combining advanced technologies with intelligent threat insights, we believe organizations can build future-ready defenses to successfully navigate an evolving and complex threat landscape. We explain these concepts below and offer recommendations for each item.

The Comeback of Zero Trust Security

Zero Trust Architecture will serve as the cornerstone of organizational cybersecurity strategies. With the principle of “never trust, always verify,” Zero Trust will move beyond identity and access management to encompass real-time monitoring of user behavior and device security. AI-powered systems will play a pivotal role in enabling dynamic verification, identifying and mitigating abnormal activity, such as unauthorized access or lateral movement across networks. Complementary investments in network segmentation, endpoint protection, and multi-factor authentication will further reduce the attack surface, making it harder for attackers to gain persistent access.

This renewed focus on Zero Trust aligns with the growing need to secure cloud environments and APIs as organizations accelerate their digital transformation.

Cloud and API Security Take Center Stage

The rapid adoption of cloud environments and the proliferation of APIs will amplify the importance of cloud-native security tools. Misconfigurations and exposed APIs will remain significant risks, particularly in hybrid cloud ecosystems where data flows across diverse environments. Cyber attackers increasingly target cloud infrastructure due to its critical role in organizational operations. In response, investments in Cloud Security Posture Management (CSPM) and API Threat Management tools will become essential. These tools will offer real-time visibility, automated risk assessments, and remediation capabilities to protect sensitive data and maintain regulatory compliance.

Seamlessly integrating cloud security solutions with broader security frameworks will become a priority, as businesses aim for a unified defense strategy in an era of remote and hybrid work models.

Automation to Address Cybersecurity Complexity

The scale and complexity of modern cyber threats will demand a shift toward automation. Automated workflows for threat detection, incident response, and remediation will enable organizations to respond to attacks in real time, minimizing human intervention and reducing errors. For instance, automated playbooks will allow security teams to manage large volumes of alerts without being overwhelmed, optimizing resource allocation.

Furthermore, automation will help address the global shortage of cybersecurity professionals by enhancing operational efficiency. Organizations will invest in platforms that integrate threat intelligence with automated decision-making, enabling prioritization of actionable risks and streamlined security operations. Automation will serve as the bridge between Zero Trust strategies, cloud security, and emerging tools, ensuring cohesive and efficient cybersecurity defenses.

Secure Enterprise Browsers Gain Traction

With browser-based attacks on the rise, secure enterprise browsers will emerge as a critical line of defense for organizations. These browsers will feature built-in protections against phishing, credential theft, and data exfiltration, ensuring that sensitive corporate data remains secure even when accessed from unmanaged or personal devices. As hybrid and remote work environments become the norm, secure browsers will integrate seamlessly into broader security frameworks, providing an end-to-end security layer.

By offering secure gateways to corporate systems without compromising user experience, enterprise browsers will reinforce Zero Trust principles and contribute to the overall resilience of organizational cybersecurity strategies.

Consolidation of Cybersecurity Tools

In response to the complexity of managing fragmented security solutions, the cybersecurity market will experience significant consolidation in 2025. Organizations will prioritize unified platforms that combine multiple capabilities, such as endpoint protection, vulnerability management, and compliance monitoring. These consolidated solutions will reduce operational costs, simplify management, and improve interoperability across security functions. Vendors offering scalable, multi-functional platforms will dominate the market, catering to organizations striving for efficiency while maintaining robust defenses. This consolidation trend aligns with broader business objectives, as companies seek to streamline their cybersecurity stacks and integrate automation, cloud security, and Zero Trust frameworks into a cohesive strategy

Focusing on the Fundamentals: Passkeys, WebAuthn, and Conditional Access

As organizations adopt advanced cybersecurity strategies, it is equally important to strengthen foundational defenses. Passkeys and WebAuthn, built on the FIDO2 standard, represent the future of passwordless authentication. By replacing traditional passwords with cryptographic key pairs, passkeys ensure that authentication is secure, eliminating risks associated with phishing, credential stuffing, and database breaches. WebAuthn enhances multi-factor authentication (MFA) by binding authentication to secure devices, such as hardware security tokens or biometrics (e.g., fingerprint and facial recognition). These technologies simplify the user experience while protecting against man-in-the-middle attacks and phishing attempts.

Additionally, honeytokens and honeypots are gaining recognition as powerful tools for threat detection. Honeytokens act as decoy assets—fake credentials, files, or API keys—that trigger alerts when accessed by attackers. Honeypots mimic real systems to lure adversaries, enabling organizations to analyze attacker tactics while diverting threats from actual systems. Combined with intrusion detection systems, these deception-based tools provide early warning signals and valuable threat intelligence.

Conditional access further reinforces foundational defenses by dynamically assessing user login contexts. Factors such as device health, location, and user identity are evaluated in real time to enforce access policies. Suspicious activity, such as logins from unfamiliar devices or regions, can trigger additional verification steps or block access entirely. Platforms like Microsoft Azure AD, Okta, and Google Workspace are leading the adoption of conditional access as part of modern Zero Trust frameworks.

By focusing on these fundamentals—passwordless authentication, deception-based defense tools, and conditional access—organizations can build a robust security foundation that complements advanced strategies and protects against evolving cyber threats.

Threat Intelligence as a Strategic Priority

Threat intelligence will continue to evolve as a strategic asset for organizations, enabling them to align cybersecurity efforts with emerging risks. By leveraging real-time threat insights, organizations can prioritize vulnerabilities, allocate resources effectively, and strengthen their defenses against targeted attacks. Tools that integrate threat intelligence with exposure management frameworks will help organizations shift from reactive to proactive security strategies. For instance, businesses will use intelligence to identify and address vulnerabilities actively exploited by ransomware groups or nation-state actors.

5. Data at the Heart of Security: The Changing Role of Data in Cybersecurity Strategies

In 2025, data will take center stage as the driving force behind cybersecurity strategies, transforming how organizations approach their budgets, operations, and overall security posture. As businesses face an increasingly data-driven threat landscape, the lines between data security and cybersecurity will blur, creating a new level of interdependence that fundamentally reshapes priorities.

Organizations are now dealing with exponential data growth across hybrid and multi-cloud environments, making it harder to accurately identify, manage, and protect their most critical assets. Many businesses lack full visibility into their data, where it resides, who has access to it, and how it is being used, which creates security gaps and compliance risks. In response, organizations will look to address these challenges by adopting a more data-centric cybersecurity strategy.

This approach ensures that data visibility, classification, and protection are at the forefront of threat detection and response initiatives. Cybersecurity budgets, traditionally focused on securing networks, endpoints, and applications, will increasingly shift to prioritizing solutions that integrate data security and threat response. Businesses will invest in tools and services that offer both proactive data monitoring and real-time incident detection. In this evolving landscape, the ability to secure sensitive data will not only mitigate risks but also play a pivotal role in maintaining compliance and building stakeholder trust.

The Role of MDR in Data-Centric Cybersecurity

Managed Detection and Response services will evolve to meet the challenges of this data-driven security landscape. Organizations are expected to increasingly outsource their MDR needs as cyber threats grow in complexity and the volume of data becomes harder to manage. MDR vendors that can integrate data detection with incident response will become essential partners for businesses striving to manage their data effectively while staying secure.

By consolidating data security and threat detection capabilities, MDR providers will offer solutions that close visibility gaps and reduce inefficiencies caused by fragmented tools. For example, advanced MDR platforms will incorporate automated data classification, anomaly detection, and behavior analytics, enabling businesses to identify threats faster while protecting their most critical assets. This integrated approach will empower organizations to address high-risk incidents efficiently, ensure 24/7 monitoring, and maintain compliance, making MDR a cornerstone of streamlined cybersecurity strategies in 2025.

Driving a Deeper Connection Between GRC and Cybersecurity

The increased focus on data will also drive a deeper connection between Governance, Risk, and Compliance (GRC) frameworks and cybersecurity practices. Organizations must navigate growing regulatory pressures while addressing data privacy requirements and security risks. As a result, GRC will no longer operate in isolation but instead become an integral part of cybersecurity strategies.

The interconnected relationship between data governance and threat management will reshape compliance initiatives. For example, businesses will need to ensure that sensitive data is not only protected against breaches but also used and stored in compliance with regulations such as GDPR, CCPA, and other emerging global standards. This will require organizations to adopt platforms that integrate GRC processes with data-centric threat monitoring, creating unified workflows that streamline compliance reporting, incident response, and risk management.

As a result, cybersecurity teams will collaborate more closely with compliance officers, aligning data security measures with broader governance and risk strategies. This alignment will improve visibility, reduce operational silos, and ensure that both security and compliance priorities are met without overburdening internal resources.

A New Budget Landscape: From Silos to Integration

The emphasis on data security as part of a broader cybersecurity strategy will also reshape how organizations allocate their budgets. Instead of spending on siloed tools for threat detection, data protection, and compliance, businesses will look for integrated solutions that combine these capabilities. Platforms offering unified data protection, threat intelligence, and incident response will drive greater efficiency and return on investment.

CISOs and security leaders will prioritize investments in services and tools that provide deep visibility into data environments, support real-time threat detection, and ensure regulatory compliance. This strategic approach to spending reflects a shift toward long-term resilience, where cybersecurity and data security are inseparable.

It will be an interesting year, as data will no longer be treated as a standalone challenge, it will be a central element of every cybersecurity strategy. The evolving threat landscape demands a data-centric approach to security, driving deeper integration between MDR services, GRC frameworks, and cyber defenses.

Key Recommendations for Organizations

1. Prioritize Integrated MDR Solutions. Invest in Managed Detection and Response services that combine data detection, threat intelligence, and incident response. This integration ensures businesses can identify, monitor, and respond to threats effectively while maintaining full visibility and control over their critical data assets.

2. Adopt a Data-Centric Security Strategy. Shift cybersecurity priorities to focus on data visibility, classification, and protection. Implement solutions that provide automated data discovery and monitoring to eliminate blind spots, protect sensitive data, and reduce compliance risks across hybrid and multi-cloud environments.

3. Align GRC with Cybersecurity Operations. Strengthen the connection between Governance, Risk, and Compliance and cybersecurity by adopting unified tools that integrate compliance tracking with threat monitoring. This alignment will ensure organizations meet regulatory requirements while proactively managing data risks.

4. Invest in Threat Intelligence for Strategic Decision-Making. Leverage threat intelligence platforms that offer actionable insights into data-driven threats. Focus on consuming threat intelligence strategically to prioritize high-risk threats, anticipate attack trends, and make data-informed decisions to strengthen defenses.

5. Restructure Security Budgets Toward Unified Solutions. Move away from siloed investments and allocate budgets toward integrated platforms that combine data security, threat response, and compliance management. This approach enhances efficiency, reduces costs, and ensures that cybersecurity strategies address both data protection and threat resilience.

This Cybersecurity Perspectives Report has been crafted under the careful guidance of our team, including the leadership of our CEO, Raluca Saceanu. Their collective expertise and strategic insights have played a pivotal role in shaping the content of this report, ensuring its relevance and reliability. The commitment of our leadership team to advancing cybersecurity knowledge underscores the importance of the information presented herein.

We express our gratitude for their valuable contributions.

This report features contributions from:

Alexandru Sandu
Alin Curcan
Alexandru Nicolau
Andrei Constantinescu
Ben Hellis
Ciaran Coulstock
Edward Skraba
Gavan Egan
Giovanni Idda
Ken Sheehan
Mihai Tarba
Miruna Coman
Robert Kehoe
Ronan Murphy

Smarttech
YOUR 24/7 SECURITY PARTNER

Smarttech247 is a multi-award-winning expert Managed Detection & Response (MDR) company and a market leader in Security Operations. Trusted by world's largest global organizations, our expert MDR and AI-enabled unified VisionX MDR platform provides continuous monitoring, advanced threat detection, investigation & response capabilities, 24/7. With a proven 319% ROI, Smarttech247 MDR is trusted by global organizations and we are proud to be a Gartner® recognized vendor in their 2024 Market Guide for Managed Detection & Response.

What we do

At Smarttech247, we help you protect against constant cyber threats and significantly reduce your Security Operations (SecOps) complexities. Our 24/7 expert led managed detection and response (MDR) is geared towards enhancing your cyber resilience and significantly improving your security efficiency.

- 24/7 Managed Detection & Response
- Data & Information Security
- Governance, Risk & Compliance
- Security Validation

VISION X

Respond to threats faster than ever!

Led by human expertise and powered by the VisionX platform, Smarttech247 provides a 24/7 unbeatable Managed Detection and Response (MDR) capability giving you transparent and consolidated security solutions.

- Extended Visibility across entire attack surface
- Seamless & Powerful SIEM & SOAR Integration
- Risk Scoring & Advanced Threat Intelligence

REQUEST A DEMO TODAY!

Tech Excellence Awards – Managed Security Service Provider of the Year
ISO 9001:2015 Company
ISO 27001:2013 Company
IBM Managed Security Service Provider of the Year
Deloitte. 50 Technology Fast 50 2023 IRELAND
Chambers Ireland Cybersecurity Company of the Year 2023
CYBER ESSENTIALS
it@cork LEADERS AWARDS WINNER

Smarttech
YOUR 24/7 SECURITY PARTNER

Contact us today // info@smarttech247.com // www.smarttech247.com