Acronis

Report
H2 2024

Acronis Cyberthreats Report, H2 2024: The rise of AI-driven threats

Acronis Threat Research Unit

Table of contents

Introduction and summary 4

Part 1. Key cyberthreats and trends for the second half of 2024 6

1. 2024 Ransomware reality: A 5% increase and APT-linked ransomware groups eyeing MSPs 7
- How attackers exploit RMMs
- Recommended defense strategies for MSPs
- Prevention
- Detection
- Response

2. Phishing and malicious emails remain the main vectors of infection 21
- Notable cases and phishing trends

3. Data breaches: A growing crisis for businesses 23
- Key data breaches: July to December 2024
- Industries most impacted
- Second half vs. first half of 2024
- Emerging trends and lessons learned
- Conclusion

4. AI-generated cyberthreats: Challenges needed to be addressed 26

The rise of AI-generated cyberthreats 26
- 1. Exploitation of AI by cybercriminals
- 2. Generative AI and malware creation
- 3. North Korea's use of AI for cyber operations
- 4. AI-driven software supply chain attacks
- 5. FBI warning on AI-powered fraud schemes

5. The dual nature of AI: Innovation vs. misuse 27

6. Four recommendations for mitigating AI-driven threats 27

7. Conclusion 27

Part 2. General malware threats 28

Ransomware threats 31
- Daily ransomware detections
- Focus countries: Normalized ransomware detections by quarter

Ransomware activity in focus countries 33
- U.S.
- Germany
- Japan
- U.K.
- France

Malicious websites 36

Part 3. Vulnerabilities discovered in products of key software vendors 38

Top vulnerabilities of 2024 exploited in the wild
Microsoft, Adobe and others: Regular patchwork
Recommendations
Conclusion

Part 4. Predictions for 2025 45

Ransomware will continue to dominate
Key investment areas in cybersecurity
Cloud security infrastructure and IoT
AI's role in cyberattacks and defenses
Nation-state-sponsored attacks in geopolitical conflicts
Challenges faced by MSPs
Emerging trends in cybersecurity

Part 5. Acronis recommendations to stay safe in the current and future threat environment 49

Keep passwords and working spaces private
Patch your OS and apps
Prepare for phishing attempts, and don't click suspicious links
Ensure your cybersecurity solution is properly configured

Authors:

Alexander Ivanyuk
Senior Director, Technology

Irina Artioli
Cyber Protection Evangelist, Acronis Threat Research Unit

Robert Neumann
Head of Acronis Threat Research Unit

Introduction and summary

The biannual Acronis Cyberthreats Report covers the global threat landscape as encountered by the Acronis Threat Research Unit (TRU) and Acronis sensors in the second half of 2024. General malware data presented in the report is gathered from July – December of 2024 and reflects threats targeting endpoints we observed in this timeframe.

Based on over 1,000,000 unique endpoints distributed around the world, the report includes statistics focused on threats targeting Windows operating systems, as they are much more prevalent than those targeting macOS and Linux.

Key findings:

- The United Arab Emirates, Singapore and Italy were the most targeted focus countries for malware attacks in December 2024.
- Over 48 million URLs were blocked at the endpoint by Acronis in Q4 2024, a 7% increase compared to Q3 2024.
- 31.4% of all received emails were spam in H2 2024, and 1.4% contained malware or phishing links.
- The United Arab Emirates had the largest percentage of blocked malicious URLs at the endpoint in December 2024 (16.2%), followed by Brazil with 13.2% and Singapore with 12%.
- 1,712 ransomware cases were publicly mentioned in Q4 2024. RansomHub, Akira, Play and KillSec were among the top contributors, with 580 victims in total. The Cl0p ransomware group was highly active in December, with 68 victims.

Top cybersecurity trends from July — December 2024:

- In 2024, ransomware increasingly targeted critical industries, including transportation, health care and manufacturing, with attackers using personalized tactics and AI-driven strategies to exploit vulnerabilities and demand higher ransoms. This trend reflects a shift towards more sophisticated, large-scale attacks aimed at maximizing disruption and financial gain, highlighting the critical role MSPs play in protecting organizations with advanced security measures and incident response strategies.
- Data breaches continue to dominate and wreak havoc among businesses worldwide.
- ChatGPT and similar generative AI systems are being increasingly used to launch cyberattacks, create malicious content and automate attacks.
- The number of email-based attacks detected in second half of 2024 increased 197% compared to the second half of 2023, while the number of attacks per organization within the same time frame increased by 21%.

What you will find in this report:

- The top cybersecurity / threat trends Acronis observed in the second half of 2024.
- Why MSPs and MSSPs are under constant threat, and how they should prepare.
- The dangers of AI development.
- An overview of recent data breaches.
- General malware statistics and a deep-dive analysis of the most dangerous threats.
- Ransomware statistics and key families analyzed.
- Vulnerabilities that contribute to successful attacks.
- Cybersecurity recommendations for the coming months.

1

Key cyberthreats and trends for the second half of 2024

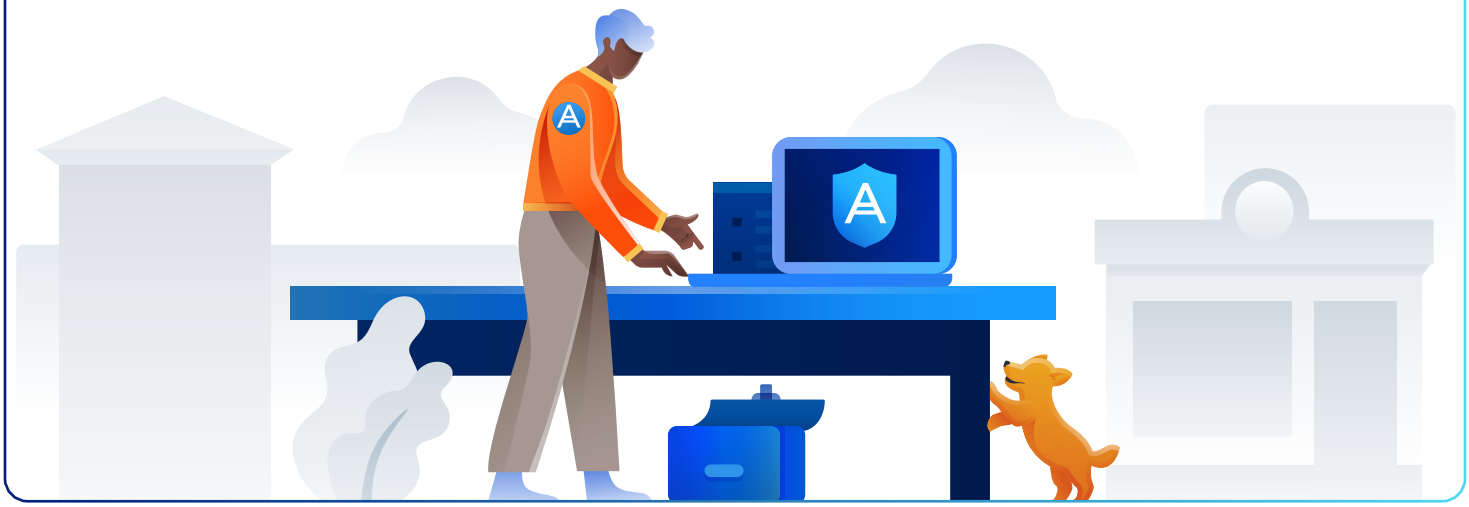
1. 2024 ransomware reality: A 5% increase and APT-linked ransomware groups eyeing MSPs

Let's take a look into the activities of these top gangs, as well as some other notable ransomware incidents from July – December 2024.

U.S. / financial sector / RansomHub / LockBit

Patelco Credit Union, a California-based credit union with over $9 billion in assets and more than 400,000 members through 37 branches, experienced a RansomHub ransomware attack in May 2024. Personal customer data stolen in late June 2024 was published on the gang's extortion portal in August 2024. The attack began with unauthorized access in late May and forced a two-week shutdown of Patelco Credit Union's banking systems in June, affecting 726,000 customers, according to Maine's Attorney General's Office. Patelco confirmed in mid-August that stolen data included names, Social Security numbers, driver's license numbers, dates of birth and email addresses.

In a separate case, Evolve Bank & Trust notified 7.6 million Americans of a data breach from a LockBit ransomware attack. In June, LockBit threatened to publish 33TB of data, claiming they breached the U.S. Federal Reserve — the data leaked was actually from Evolve. An investigation revealed that an Evolve employee clicked on a malicious link, allowing the attacker to access and download Evolve's database. Although customer funds remained safe, several fintech customers, including Affirm, Wise and Bilt, were affected.



U.S. / technology sector / Play

Microchip Technology Incorporated, an American chipmaker with revenue of $8.439 billion in 2023, disclosed that a cyberattack disrupted its operations across multiple manufacturing facilities. The incident forced the company to shut down and isolate affected systems, impacting its ability to meet customer orders across various sectors, including automotive, aerospace and defense. The chipmaker has around 123,000 customers from multiple industry sectors. The Play ransomware group claimed to have breached Microchip's internal systems, and partially leaked the allegedly stolen data, including personal information and financial records. Microchip disclosed in November 2024 that the incident cost the company $21.4 million.

U.S. / manufacturing sector / RansomHub

Halliburton, a leading oil services company with revenue of $23.02 billion in 2023, confirmed a cyberattack that led to the shutdown of some of its systems. The company became aware of unauthorized access and activated its cybersecurity response plan, launching an investigation with external advisors. The exact nature of the cyberattack remains undisclosed, but is rumored to be linked to the RansomHub ransomware group. In November 2024, Haliburton revealed that the attack resulted in $35 million in charges related to lost or delayed revenue.

Canada / transport sector / Rhysida

The Port of Seattle fell victim to a ransomware attack by the Rhysida gang on August 24, affecting both the port and Seattle-Tacoma International Airport. The attackers demanded 100 bitcoins ($5.8 million) and threatened to publish 3TB of stolen data, including sensitive personal information. The Port refused to pay the ransom, leading to disruptions in airport services like check-in kiosks and Wi-Fi. Rhysida posted some data online, including personal documents and employee information. Despite the attack, most systems were restored within a week, with ongoing efforts to fully recover.

India / technology / financial / RansomEXX

A ransomware attack targeting C-Edge Technologies, a joint venture of SBI and TCS, disrupted banking services for nearly 300 small banks across India, leaving millions of customers unable to access payment systems like ATMs and Unified Payments Interface (UPI). The attack, attributed to the RansomEXX group, encrypted systems at C-Edge and its collaborator, Brontoo Technology Solutions, forcing the National Payments Corporation of India (NPCI) to isolate the affected banks from retail payment systems. This disruption primarily impacts cooperative and regional banks serving rural and semi-urban areas, though these banks account for only 0.5% of the country's payment volume.

U.K. / public services / BianLian

BianLian ransomware attackers emailed Sable International customers to pressure the U.K.-based immigration services provider into paying a ransom after a cyberattack disrupted its servers, website and other portals. Investigations confirmed that client data from various countries had been stolen. Sable International contacted affected customers and advised them not to engage with the attackers.

France / sports / entertainment / Brain Cipher

The Grand Palais Réunion des musées nationaux (Rmn) in France experienced a ransomware attack on August 3, 2024. The institution manages several major museums and cultural sites, including those hosting Olympic events like fencing and Taekwondo. Despite the cyberattack, Olympic events proceeded without disruption, and the museums under Grand Palais Rmn's management continued normal operations. However, the attack targeted the central computer system and caused temporary shutdowns of bookstores and boutiques, which were later restored to autonomous operations.

Forty small museums were also impacted. Four weeks after the attack, Brain Cipher claimed responsibility and demanded payment of an undisclosed ransom within 48 hours.

Switzerland / MSP / Helldown

Hug Witschi AG, a Swiss IT company, reported that a cyberattack affected its internal servers and resulted in data loss. The company, with help from internal staff and external experts, worked to restore system access while investigating the exposed data. The Helldown ransomware group claimed responsibility for the attack, reportedly stealing 67GB of data.

South Korea / automotive / energy sector / Hunters International

Hanon Systems, a global leader in automotive thermal energy management, was hit by a ransomware attack for the third time in recent years — this time by the Hunters International group. Hunters disclosed 2.3TB of stolen data on the dark web, including resumes, contact details, employee ID photos and 1,632,481 files containing confidential information about the company's global equity structure. Hanon Systems promptly reported the attack to the Korea Internet & Security Agency and notified affected employees the next day.

Spain / retail / Medusa

Tendam, the Spanish fashion giant behind brands like Cortefiel and Pedro del Hierro, experienced a ransomware attack, with attackers demanding $800,000 to prevent the leak or sale of 724GB of stolen data. The attack, attributed to the Medusa group, raised concerns at a crucial moment for the company, as it celebrated the 50th anniversary of Pedro del Hierro and prepared

for a potential IPO. Despite the cyberattack, Tendam stated that its store operations remained unaffected, though the company is still assessing the extent of the data breach.

Philippines / HR services / Medusa

In September, the Medusa ransomware group attacked AZPIRED, a major global outsourcing provider based in the Philippines, exfiltrating 205.7GB of sensitive data, including company records, HR files, financial documents and client information. The attackers demanded $100,000, threatening to either leak or delete the stolen data if not paid. Screenshots of employee photos and internal documents have already been shared as proof of the breach, exposing the company to significant reputational damage, identity theft risks and legal consequences.

Israel / law / BianLian

Also in September, Pearl Cohen, a leading Israeli law firm specializing in intellectual property, fell victim to a cyberattack by the BianLian group, which stole 1.2TB of data, including client and employee information. Despite the breach, the firm refused to pay the ransom demand, and its operations were unaffected as the attack was limited to a single system, with no disruption to core systems like email or document management. Pearl Cohen emphasized that the stolen information was neither encrypted nor locked, and the incident did not impact the firm's ongoing operations.

Philippines / real estate / Sarcoma

In October, Sarcoma ransomware attacked Suntrust Properties, a major real estate developer in the Philippines. Attackers stole 1TB of data, including sensitive personal and corporate information such as employee and clients' government-issued IDs, signed legal documents and SQL databases with corporate real estate information. The ransomware group has publicly released samples of the compromised data, heightening concerns. While Suntrust Properties has been notified of the breach, there has been no official statement from the company, and the incident was initially unverified until Sarcoma ransomware claimed responsibility in early October 2024.

France / digital automation and energy management / GREP / Hellcat

Schneider Electric confirmed a breach of its developer platform after a hacker, known as "Grep," stole 40GB of data from Schneider's JIRA server. The hacker claimed to have accessed 400,000 rows of user data, including 75,000 unique email addresses and full names of employees and customers, using exposed credentials. Grep, now part of the newly rebranded Hellcat ransomware group, demanded $125,000 in "baguettes" to prevent the data from being leaked. Schneider Electric mobilized its incident response team, and no impact on its products or services was reported. However, in December, Hellcat released 40GB of files stolen from Schneider, suggesting that the company refused to pay the ransom.

Brazil / retail / Medusa

In November, Lojas Marisa confirmed that a ransomware attack temporarily disrupted its website and physical store operations. The company reported that it was a victim of the Medusa ransomware group, which gained access by exploiting unpatched vulnerabilities and hijacking legitimate accounts. Marisa took immediate action by isolating and suspending

part of its systems to protect data, and operations have since resumed. Medusa ransomware group set a ransom of $300,000 to prevent the leak of an undisclosed amount of data.

U.K. / MSP / SafePay

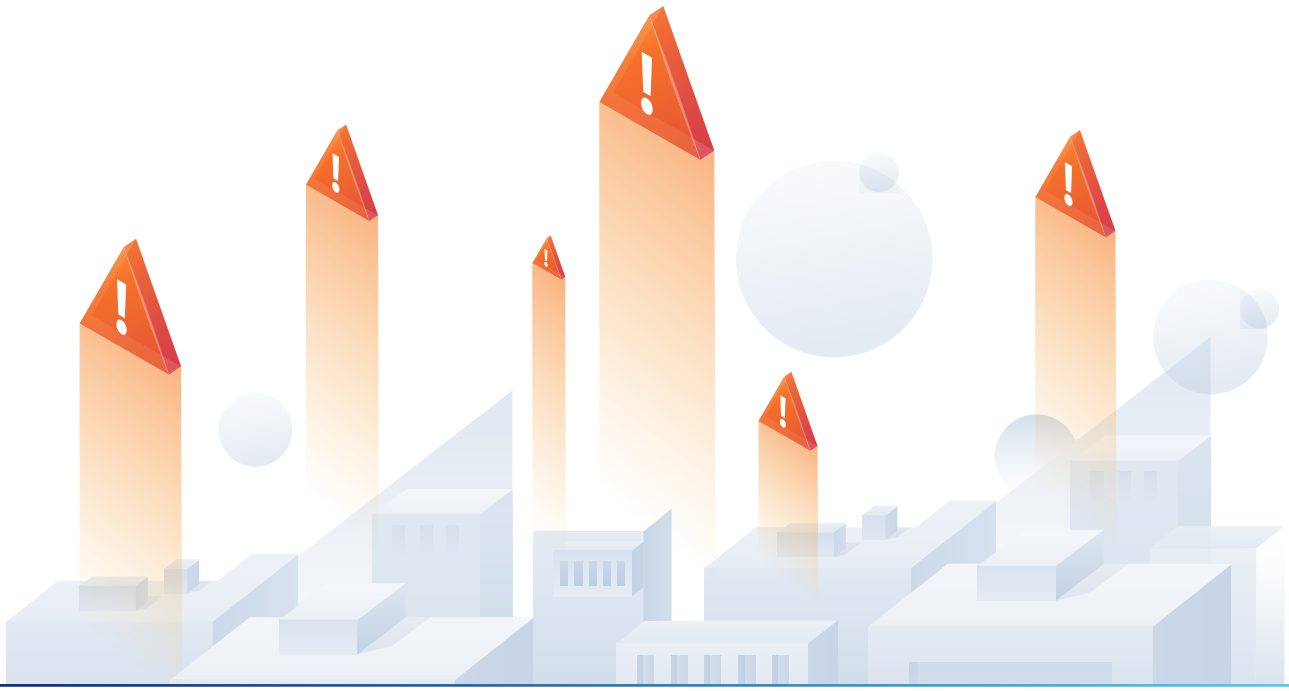
The SafePay ransomware gang claimed responsibility for an October cyberattack on U.K. telematics firm Microlise, which provides tracking services for major clients like DHL and Serco. SafePay alleges to have stolen 1.2TB of data, including information affecting Microlise's operations, such as tracking systems for prisoner transport vans. While Microlise confirmed data theft and disruptions, it did not explicitly confirm ransomware involvement, but reports of service interruptions pointed to it. SafePay, a newly emerged group, demanded a ransom with a 24-hour deadline, threatening to leak the stolen data if their demands were not met.

U.S. / health care / Embargo

In November, Memorial Hospital and Manor in Bainbridge, Georgia, was hit by a ransomware attack that disrupted the access to its electronic health record system. The hospital, which serves Decatur County and surrounding areas, reported the issue, saying that although the attack did not affect patient care, the hospital had to switch to pen-and-paper processes. IT specialists began system recovery after antivirus software flagged the threat. The hospital warned of potential longer wait times but did not disclose whether any data breach occurred. The Embargo ransomware gang, active since April 2024 and responsible for other U.S. health care attacks, took responsibility for the Memorial Hospital attack and claimed theft of 1.15TB of data.

U.S. / software / Termite

A November ransomware attack on Blue Yonder, a major supply chain technology provider with revenue of $1.28 billion, disrupted services for several of its 3,000 global clients, including major retailers and food manufacturers. The incident caused delays in delivery, inventory management and payroll processes for companies like Starbucks, Morrisons and Sainsbury's. Starbucks reported manual workarounds to ensure



employees were paid, while Morrisons and other U.K. grocery chains resorted to backup systems to manage fresh food supplies. Blue Yonder, owned by Panasonic, stated that its public cloud environment was unaffected, and several clients, including DHL and Tesco, confirmed they experienced no significant impacts.

Italy / education / RansomHub

In September, RansomHub claimed to have stolen 18GB of data from a minisite of the Department of Mathematics at the University of Genoa. The attackers gave the university 13 days to pay an undisclosed ransom. It remains unclear what kind of information was compromised in the breach.

Mexico / government / RansomHub

The RansomHub gang claimed to have breached the Mexican government's federal website, gob.mx, in November. The group alleged it exfiltrated 313GB of data, including contracts, financials and confidential files, and threatened to release the stolen information unless an undisclosed ransom was paid within ten days. RansomHub posted over 50 sample files, which included personal information about federal employees and signed government documents.

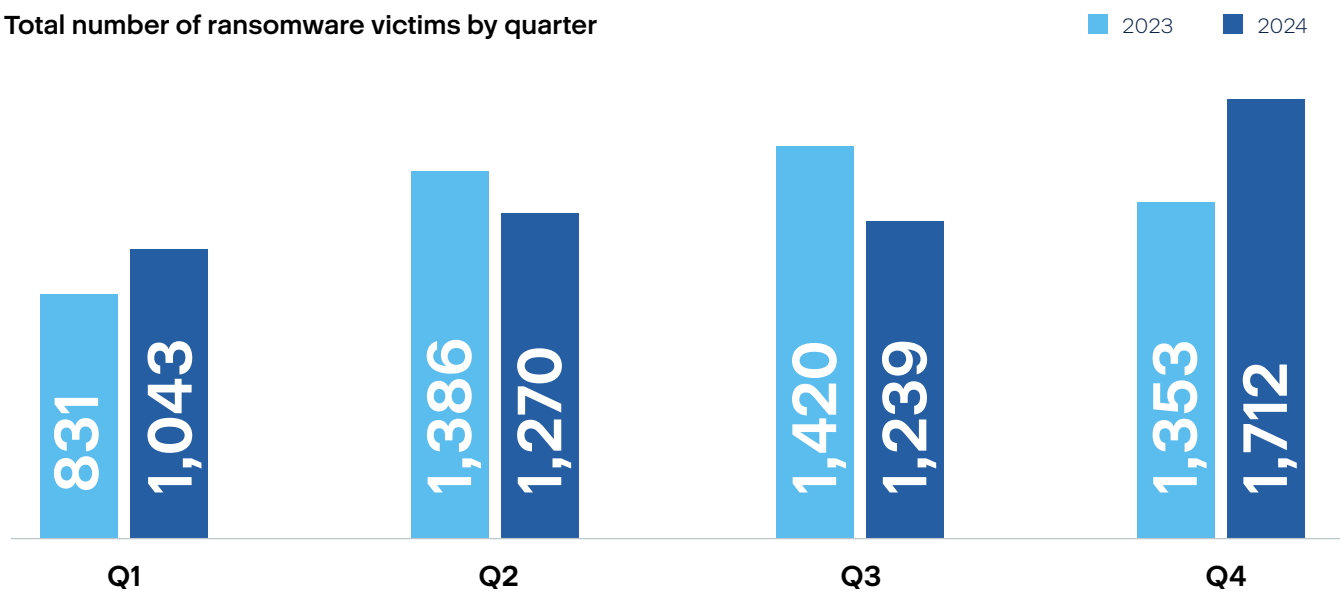
Kuwait / health care / Unknown

Kuwait's Health Ministry experienced a cyberattack that disrupted systems at several hospitals, as well as the Sahel health care app. While some systems, including those at the Kuwait Cancer Control Center and in offices that manage the national health insurance system, were restored using backups, the Ministry of Health remained offline when the attack was reported in September. Officials stated that critical databases were not breached, but certain systems were shut down to implement security updates. No ransomware gang has claimed responsibility, though Kuwait has faced similar attacks in the past by Rhysida and Vice Society.

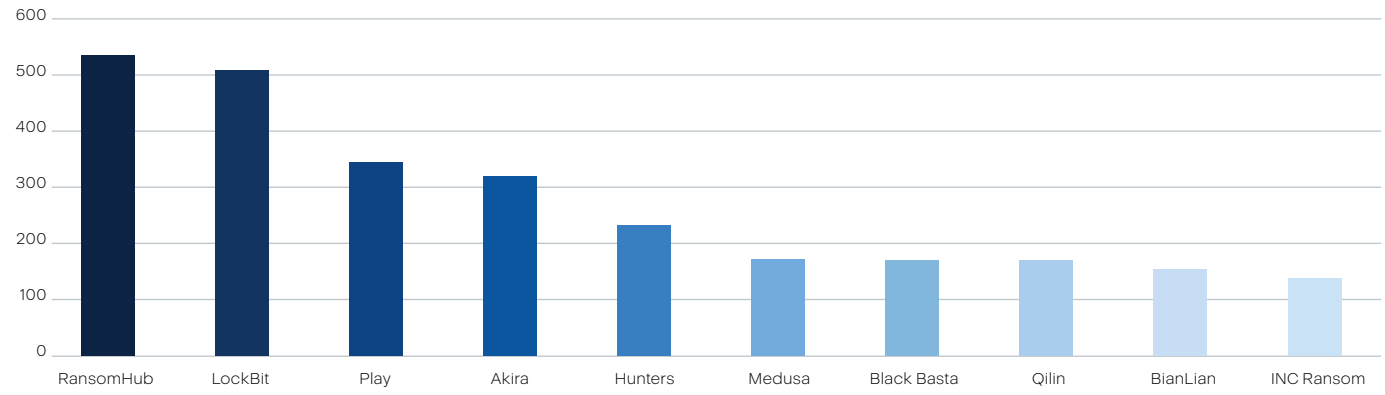
Multicountry / Multiindustry / Cl0p / Termite

In December, the Cl0p ransomware group threatened to release data stolen from more than 60 organizations via vulnerabilities in Cleo's file transfer tools. These flaws, CVE-2024-50623 and CVE-2024-55956, allowed attackers to steal data without authentication. In late December, Cl0p released a partial list of victims. Termite, a newer ransomware group, is also suspected of exploiting Cleo vulnerabilities. The attacks highlight ongoing risks from third-party software vulnerabilities, showing that supply chain threats remain a critical concern.

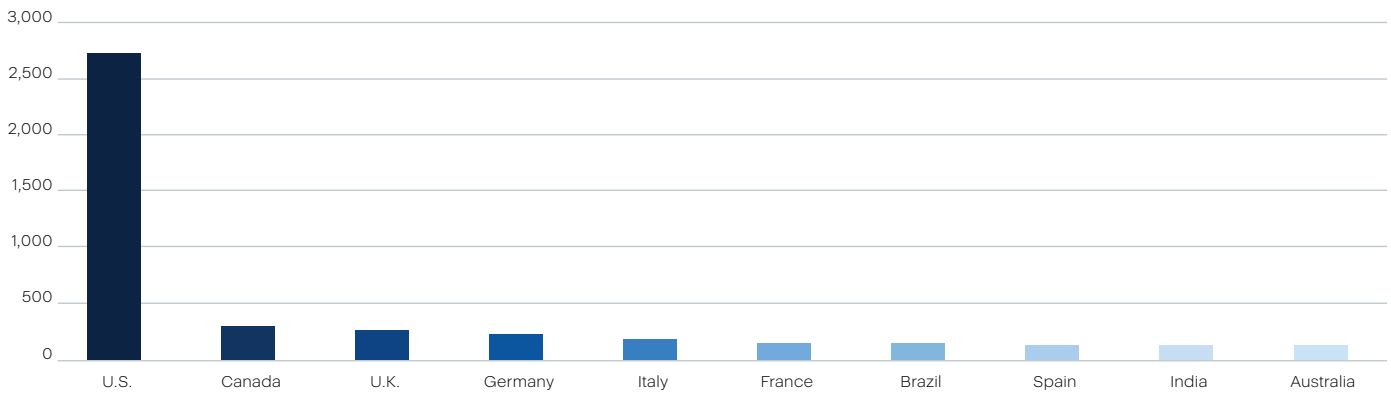
Total number of ransomware victims by quarter



Top ransomware groups



Top 10 countres

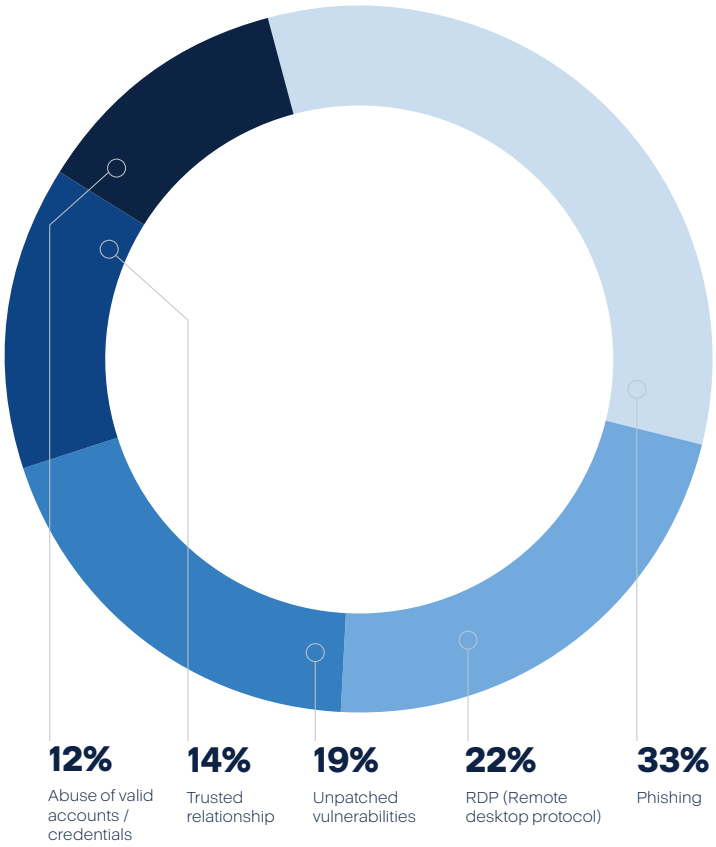


MSPs under attack

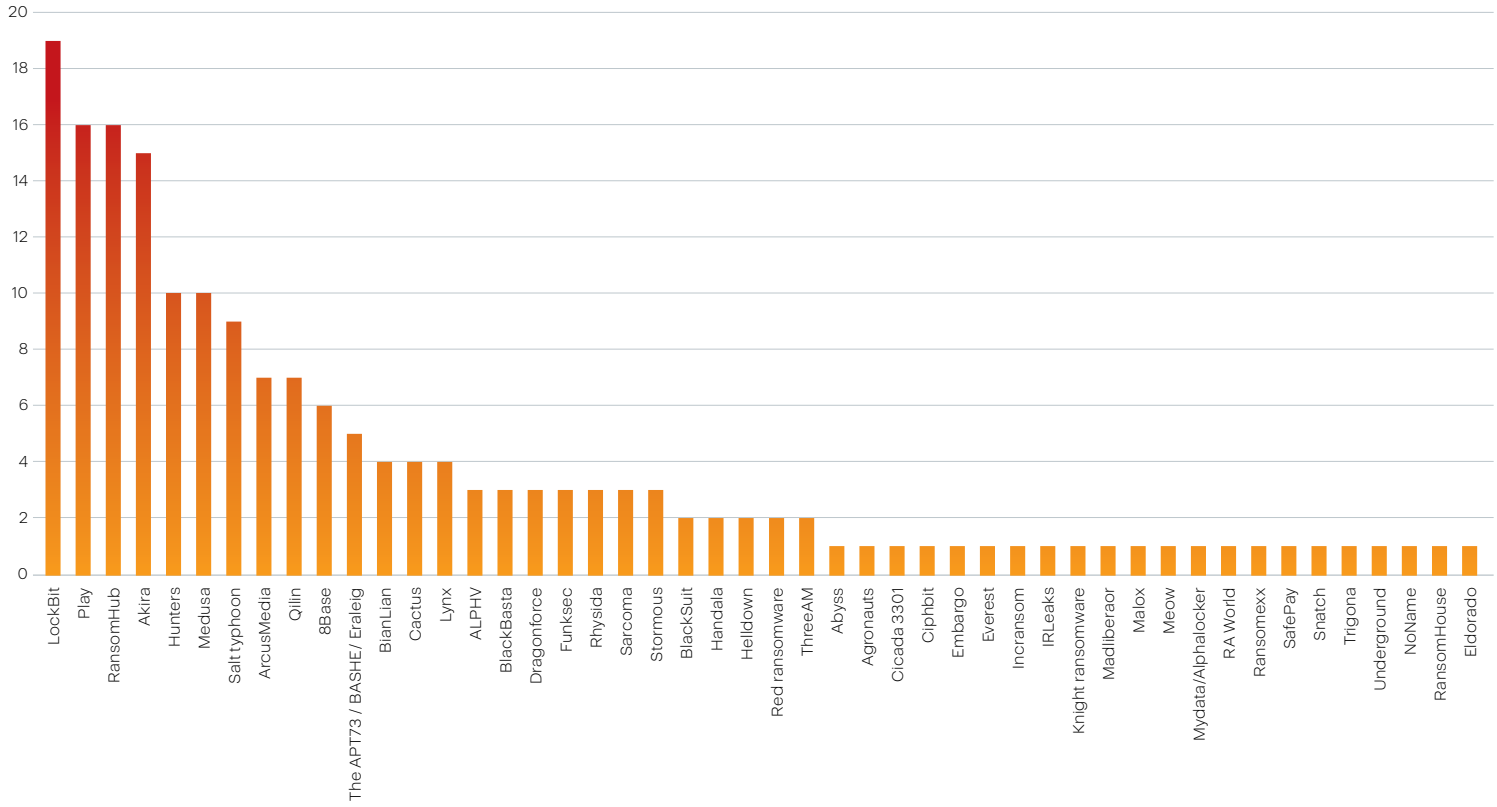
We have continued to monitor attacks on managed service providers (MSPs) and have extended the data from January to December 2024. Our analysis revealed 185 claimed incidents in which attackers predominantly used email phishing campaigns, followed by compromised remote access tools, with weak RDP passwords being a key entry point. The credential weaknesses also affect VPNs and firewalls, allowing attackers to bypass authentication controls and infiltrate critical systems.

MSPs are increasingly becoming prime targets for attackers, and they face the same types of initial attack vectors as other victims. Our extended analysis of MSP attacks throughout 2024 revealed that phishing remains the dominant method, with 62 incidents recorded, followed by abuse of RDP, exploitation of unpatched vulnerabilities and trusted relationship attacks. Credential compromise and supply chain infiltration also remain significant entry points. These vectors, while not new, continue to be alarmingly effective against MSPs, highlighting gaps in basic security practices.

Initial attack vectors



Ransomware groups targeting MSPs



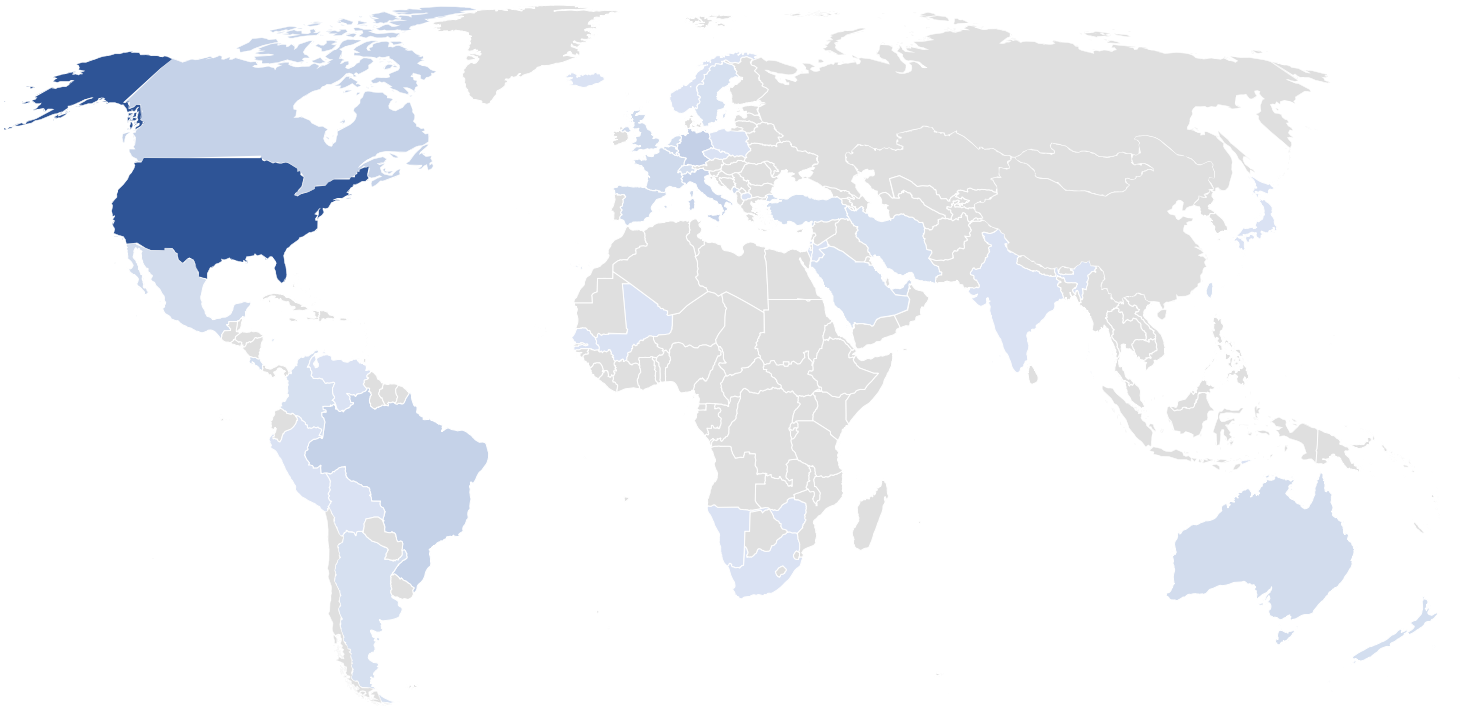
Attacks on MSPs now occur on a regular basis. TRU's H1 Cyberthreats Report explored cases from January 2024 to May 2024. Below are three cases from H2 of 2024:

1 The Meow ransomware gang allegedly attacked Banx Systems, a New Zealand VoIP and IT support company with revenue of $5.4 million. The group posted details of the attack on their darknet site in August, announcing a data pack containing over 15GB of confidential information. The post claimed that the stolen data included client information, financial documents and other confidential records. The Meow gang is selling the data for either $35,000 to a single buyer or $12,000 to multiple buyers. This is the first attack by Meow in the Australia and New Zealand region, though they claimed 128 victims in 2024.

2 In June, IT services firm Insula refused to pay a ransom after the BianLian ransomware gang claimed to have stolen 400GB of data, including project files, client information and company source codes. Insula confirmed the breach affected its corporate network, but stated the threats were promptly contained and the ransom demand ignored. The compromised data reportedly included staff and customer names, contact details and addresses. Affected individuals were notified following the incident. Insula reported the breach to the Australian Cyber Security Centre, the Office of the Australian Information Commissioner, and Victoria Police's cybercrime unit.

3 In October, Polish IT services provider Atende confirmed a ransomware attack that led to the theft of 1.2TB of sensitive data, including contracts, employee personal data and login credentials. The company refused to pay the ransom, declaring its commitment to standing against cybercriminals and thanking its customers for their support. The attack, claimed by Hunters International, involved a single file server and did not compromise Atende's other systems or services. Following the breach, the company reported the incident to authorities, including the District Prosecutor's Office and CERT Polska, and cautioned customers about potential phishing and spoofing attempts.

Most targeted countries for attacks on MSPs



Percentage

1% 62%

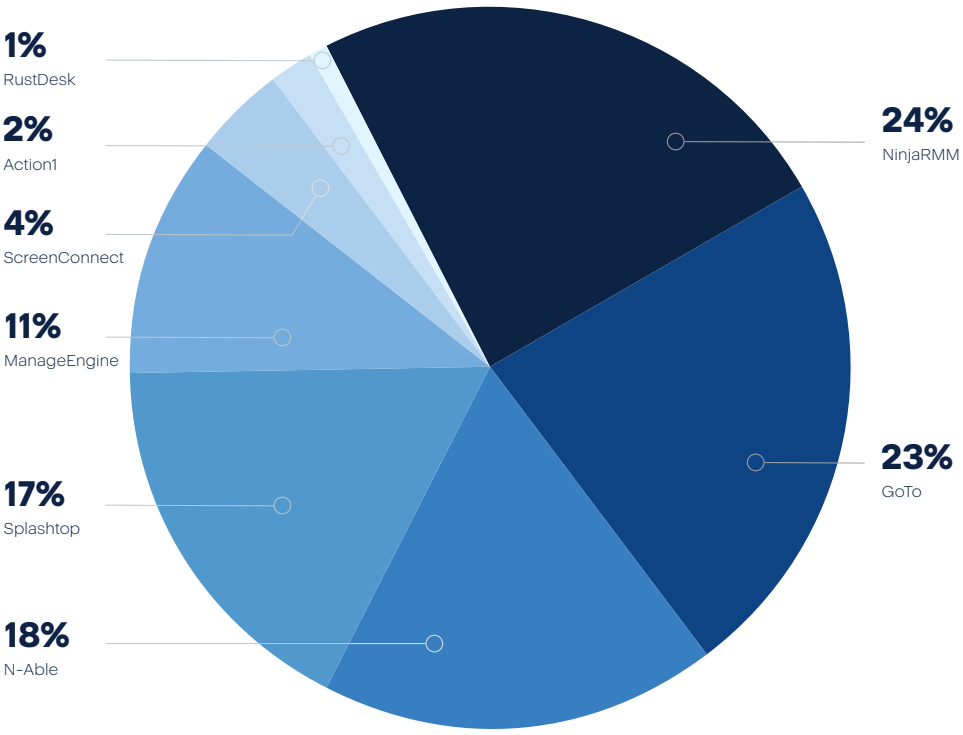
However, the emerging and more concerning trend is the targeting of MSPs by advanced persistent threat (APT)-linked ransomware groups. These sophisticated actors employ similar tactics, like exploiting unpatched network devices and employing "living-off-the-land" (LotL) techniques to maintain long-term access to critical systems, and the purpose motivation of the attacks has expanded to espionage. The most vivid examples of these include the past year's attacks of Salt Typhoon targeting U.S. commercial telecommunications infrastructure. This shift underscores the evolution of the threat landscape, where MSPs are no longer just opportunistic targets but strategic points of entry for high-stakes cyberattacks. It is imperative for MSPs to strengthen defenses with advanced threat detection, continuous patch management and rigorous monitoring of access credentials to mitigate these evolving risks. The involvement of APT-linked groups signals the need for an immediate and more robust approach to securing MSP infrastructures.

How attackers exploit RMMs

Rising risk of remote management

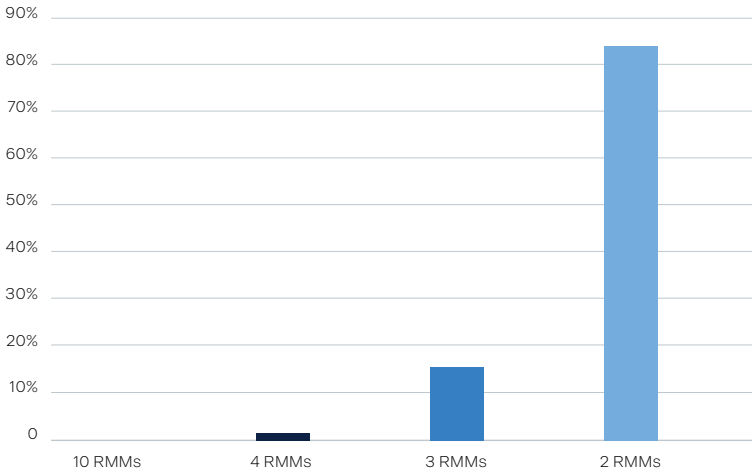
In our modern digital life — especially in the world of MSPs — having the ability to remotely manage servers and workstations has become mandatory. Long gone are the days of on-site management. It had its fair share of prime time in previous decades; however, the more that technology-enabled companies were able to access their systems without the need to physically access them, the less strict they became about their remote access policies. Recent changes to the way people carry out their work in the post COVID-19 era — including fully remote or hybrid — sped up the process even more. Today's remote monitoring and management (RMM) landscape consists of dozens of different solutions, including top players such as Ninja, GoTo or N-Able — everyone can find one suited for their specific needs.

Most frequently used RMMs, H2 2024



Having the extra comfort and convenience that RMM tools can provide does not come without a downside — any remote management solution will open the attack surface significantly and can easily become an additional risk that needs to be mitigated. In past years, we have seen waves of attacks gathering initial access by either exploiting vulnerabilities in such applications, using leaked credentials, hacking their way in with brute force or deploying yet another popular RMM software on top of existing ones to achieve persistence. Our telemetry shows that it is not uncommon to have multiple software packages deployed and used within the same organization with no clear benefits. Such circumstances make it even easier for attackers to deploy their own without being noticed.

Number of tenants



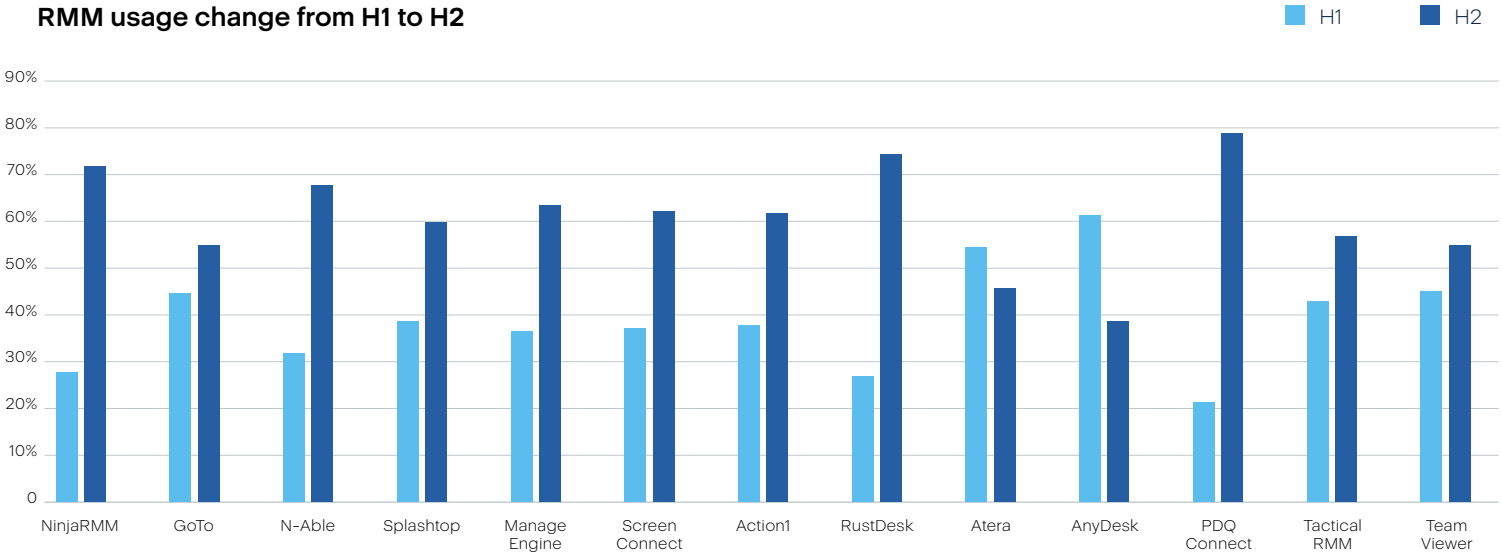
As the adoption of RMM solutions significantly increases and the solutions become more complex, organizations must understand the risks involved and take additional steps to ensure their network remains locked down from unauthorized access. Failing here could easily result in a successful ransomware attack with all of its consequences, as RMM tools remain favorites of threat actors behind such campaigns.

We strongly recommend that companies review their existing policies, ensure that only necessary RMM applications are installed and update those applications frequently. Finally, appropriate access control must be in place and access should be granted only to necessary people.

RMM tools

Action1
DWAgent
LogMeIn
Parsec
RemotePC
SorillUs
TightVNC
AnyDesk
eHorus
ManageEngineRMM
PDQ Deploy
RemoteUtilities
Splashtop
TrendMicro Basecamp
Atera
FixMeIt
MeshAgent
PowerAdmin
RPort
SuperOps
Twingate
ASG Remote Desktop
Fleetdeck
MobaXterm
Pulseway
RSAT
Supremo
ZeroTier
BeAnywhere
GoToAssist
N-Able
Radmin
RustDesk
Syncro
ZohoAssist
Chrome Remote Desktop
ITarian
NetSupport
Remote Desktop Plus (RDP+)
ScreenConnect
TacticalRMM
Domotz
Level.io
NinjaOne
Remote Manipulator System (RMS)
SimpleHelp
TeamViewer

RMM usage change from H1 to H2



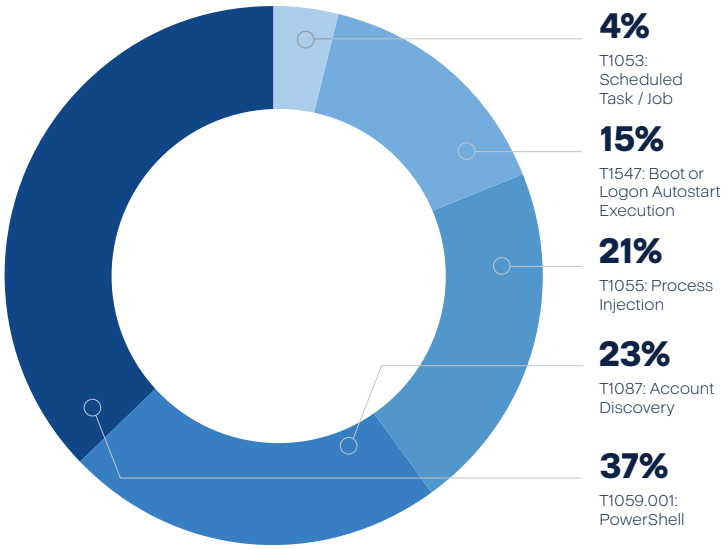
Most used MITRE techniques

Protecting networks in a rapidly evolving threat landscape requires focused prioritization on the techniques adversaries use most frequently. Drawing from the MITRE ATT&CK® framework, which categorizes adversarial behavior into tactics, techniques and procedures, we analyzed five critical techniques that have proven both impactful and challenging to detect. Understanding and mitigating these techniques is vital for MSPs to fortify their defenses.

The collected information is based on Acronis telemetry from Acronis XDR from April 1 to December 31, 2024.

No.	Technique ID	Technique name
1	T1059.001	PowerShell
2	T1087	Account Discovery
3	T1055	Process Injection
4	T1547	Boot or Logon Autostart Execution
5	T1053	Scheduled Task / Job

Top 5 most frequently seen MITRE ATT&CK techniques, Q2-Q4 2024



1. PowerShell (T1059.001)

Summary: Threat actors often exploit PowerShell, a powerful scripting tool, to execute malicious scripts, download payloads or obfuscate commands, blending seamlessly into legitimate system activities.

Detection: Monitor PowerShell logs for suspicious command-line arguments, unusual base64-encoded payloads, or unexpected network connections initiated by scripts. EDR solutions can also flag anomalous behavior.

Mitigation: Enforce strict execution policies (e.g., allow only signed scripts), disable PowerShell for users who do not need it and utilize logging and script block logging for enhanced visibility.

2. Account Discovery (T1087)

Summary: Attackers query user or account information to understand the target environment and identify privileged accounts for lateral movement. This can involve commands like net user or LDAP queries in Active Directory environments.

Detection: Monitor logs for excessive or unusual account enumeration activities. Focus on systems running unexpected administrative commands or querying domain controllers.

Mitigation: Limit the visibility of account information through least privilege principles, disable unnecessary accounts and use tools like honeypot accounts to detect enumeration attempts.

3. Process Injection (T1055)

Summary: This technique enables attackers to inject malicious code into legitimate processes, evading detection and gaining stealthy execution. Examples include DLL injection and APC (Asynchronous Procedure Call) injection.

Detection: Look for anomalous API calls (e.g., CreateRemoteThread) and monitor processes for unexpected memory modifications or behavior. EDR solutions can provide real-time detection of injection attempts.

Mitigation: Implement EDR with behavior-based detection, enable memory integrity features and enforce strict application control policies to reduce exploitation opportunities.

4. Boot or Logon AutoStart Execution (T1547)

Summary: Adversaries achieve persistence by adding malicious entries to Registry Run keys, startup folders or scheduled tasks, ensuring execution during system boot or user logon.

Detection: Continuously monitor modifications to the Registry Run keys, startup folder and scheduled tasks. Use behavioral analysis to detect unexpected programs initiating at startup.

Mitigation: Employ application whitelisting, restrict permissions for modifying autostart locations, and use Group Policy Objects (GPOs) to enforce restrictions on startup settings.

5. Scheduled Task / Job (T1053)

Summary: Scheduled Task / Job is a commonly exploited technique in which attackers abuse task scheduling functionalities, such as Windows Task Scheduler, to execute malicious code persistently or at specific intervals. These tasks often blend into legitimate system activities, aiding attackers in evading detection.

Detection: Monitor the creation and modification of scheduled tasks, paying close attention to tasks with unusual names, execution times or command-line arguments, as well as the use of task scheduling tools like schtasks.exe for unusual or suspicious activity. Analyze system logs for tasks triggered by unexpected accounts or outside normal operating hours.

Mitigation: Restrict permissions for creating or editing scheduled tasks to authorized users. Regularly audit task schedules to identify and remove unauthorized or suspicious entries. Implement EDR tools to detect and block malicious task behavior and enforce policies to prevent unauthorized script execution.

Threat actors are increasingly leveraging stealth tactics, often employing techniques like Process Injection or PowerShell obfuscation, to bypass traditional defenses. To counter these evolving threats, MSPs must adopt a layered security model. This includes:

Prevention: Enforce strict policy controls, implement network segmentation and leverage application whitelisting.

Detection: Use advanced tools like EDR and SIEM (security information and event management) for real-time monitoring and behavioral analysis.

Response: Partner with a managed SOC to ensure 24/7 monitoring and rapid incident response.

Recommended defense strategies for MSPs

By combining proactive measures with advanced detection capabilities, MSPs can better anticipate adversarial tactics and create a security ecosystem that makes lateral movement and persistence significantly harder for attackers to achieve.

Prevention

- **Security awareness training:** Train MSP employees to recognize phishing attempts, social engineering tactics and other suspicious activities to ensure they follow cybersecurity best practices.
- **Multifactor authentication (MFA):** Enforce MFA for all privileged accounts and critical systems to add an extra layer of defense against unauthorized access.
- **Network segmentation:** Divide MSP networks into isolated segments to limit lateral movement and reduce the potential impact of breaches.
- **Patch management:** Establish a robust patch management program to quickly apply updates and security patches, and minimize exposure to known vulnerabilities.
- **Data encryption and loss prevention:** Encrypt sensitive data in transit and at rest and deploy data loss prevention (DLP) solutions to prevent unauthorized data exfiltration.

Detection

- **Continuous monitoring and threat intelligence:** Implement solutions for real-time network monitoring, integrating threat intelligence to identify emerging threats and stay ahead of evolving attack methods.
- **Endpoint security with EDR / XDR:** Use advanced endpoint detection and response (EDR) solutions equipped with AI and behavioral analytics to detect and flag malware, lateral movement and other malicious activities.

Response

- **Incident response planning:** Develop and routinely test an incident response plan to ensure MSPs can swiftly detect, contain and recover from security incidents while minimizing operational disruption.
- **Automated remediation:** Leverage EDR / XDR tools with built-in remediation features to neutralize threats quickly.
- **Post-incident analysis:** Conduct thorough reviews of incidents to identify root causes, update defenses and prevent similar breaches in the future.

This layered approach ensures MSPs proactively prevent cyberthreats, detect suspicious activities in real time and respond efficiently to minimize damage and downtime.

2. Phishing and malicious emails remain the main vectors of infection

The below email and phishing statistics are collected from Advanced Email Security for Acronis Cyber Protect Cloud, which is powered by Perception Point. Acronis and Perception Point work together to protect organizations to ensure they remain safe from email-borne threats. The data was gathered for the second half of 2024 (July to November) and combined with Acronis telemetry data for malware and URL blocks on the endpoints.

The number of email-based attacks detected in the second half of 2024 increased 197% compared to the second half of 2023, while the number of attacks per organization within the same time frame increased by 21%. Almost 50% of users were attacked at least once, 29% of users experienced at least one phishing attack via URL, and 14% of users experienced at least one malware detection.

Total users attacked

47%

Monthly average

Phishing URLs

29%

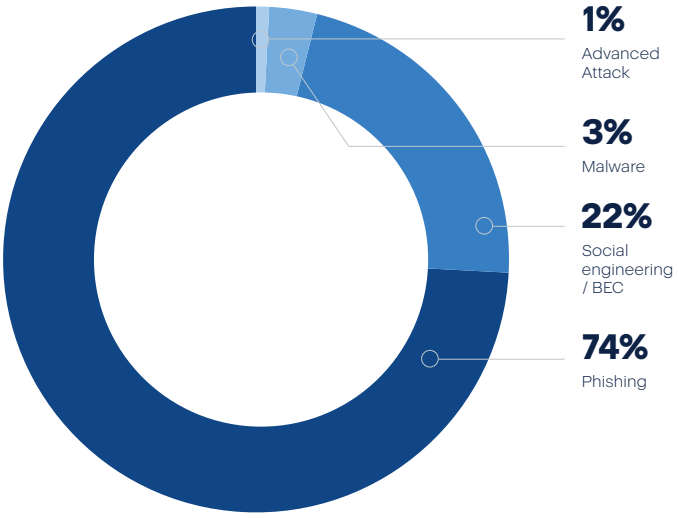
Monthly average

Files containing malware

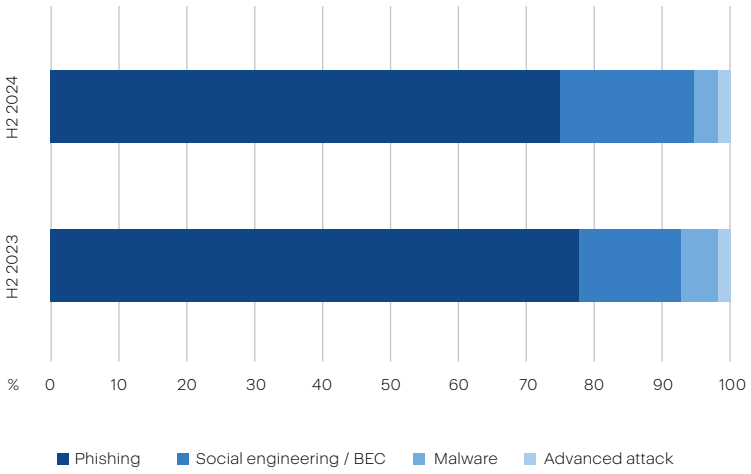
14%

Monthly average

Phishing is still the number one threat



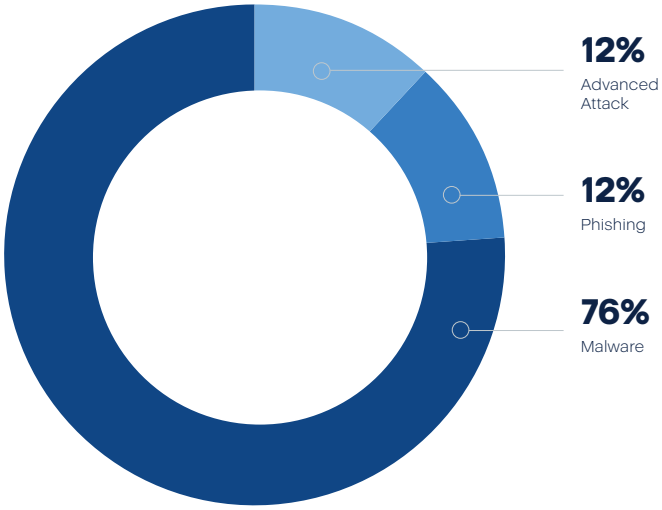
Social engineering attempts have increased 7% compared to one year ago



As expected, in the second half of 2024, we observed a 12% increase in the number of files and URLs per scanned email, compared to H2 2023. This means that organizations now need to be even more vigilant, as the average number has risen to approximately three files and URLs per scanned email. Advanced Email Security for Acronis Cyber Protect Cloud is often deployed as a second layer of email filtering on top of the basic filtering present in most email services.

Collaboration apps were heavily attacked as well, with phishing and ATPs accounting for almost 25% of total threats. The majority, unsurprisingly, were launched with malware infection attempts.

Attacks on collaboration apps



Overall, the increase in the number of attacks and growing percentage of sophisticated email-borne attacks in Q4 2024 mirrored those during Q3 2023. This once again emphasizes the crucial importance of multilayered protection in business environments.

Notable cases and phishing trends

Cybercriminals conducted large-scale YouTube-oriented campaigns by impersonating popular brands to approach content creators with fake promotion and partnership offers. These emails often included a link to an agreement, which led to the deployment of Lumma Stealer, with email addresses extracted from YouTube channels using a parser.

Another tactic involved quishing (QR code phishing) campaigns, in which phishing emails contain a PDF attachment with a QR code that redirects users to fake Microsoft 365 login pages for credential harvesting. Attackers also exploited trusted platforms like Cloudflare Pages and Cloudflare Workers© to create fake Microsoft 365 login pages and CAPTCHA checks that misled users into sharing credentials.

Phishing attacks increasingly use HTML email attachments disguised as invoices or HR policies, embedding JavaScript code that redirects users to phishing sites or executes malicious actions under false pretenses. Trusted platforms such as Docusign, Adobe InDesign and Google AMP are also leveraged to trick users into clicking on links that harvest credentials. In one example, fraudulent emails claiming to be from Okta's support team aimed to deceive users into revealing login credentials, potentially compromising organizational systems.

WhatsApp, another popular attack vector, was used to send phishing messages targeting Indian users. The emails urged victims to install malicious banking or utility apps for Android which were capable of stealing financial information. These campaigns exploit trusted brands and familiar platforms to lower suspicion and increase the likelihood of success. They highlight the growing sophistication of phishing attacks and the creative use of technology to exploit human trust. Organizations and individuals must remain vigilant and adopt multilayered defenses against such tactics. From credential harvesting to malware deployment, these campaigns underscore the importance of comprehensive cybersecurity measures.

In conclusion, as cyberthreats continue to evolve, maintaining robust email / messaging / collaboration app security is imperative for protecting organizational assets and ensuring operational resilience. By adopting comprehensive security strategies and fostering a culture of awareness, organizations can effectively mitigate the risks associated with email-based attacks.

3. Data breaches: A growing crisis for businesses

The latter half of 2024 marked a significant escalation in data breaches worldwide, targeting a wide spectrum of industries. From financial services to health care and retail, cybercriminals left a trail of compromised data and heightened anxiety about cybersecurity resilience. Let's look into the industries most affected, and compare these incidents to those from the first half of the year and earlier trends.

Key data breaches: July to December 2024

1. SRP Federal Credit Union breach (December 2024)

In December 2024, SRP Federal Credit Union suffered a cyberattack that affected over 240,000 individuals. Hackers accessed sensitive personal data, including Social Security numbers, driver's license numbers, financial information and dates of birth, over a two-month period. The ransomware group Nitrogen claimed responsibility, allegedly stealing 650GB of data.

2. Comcast customer data breach (October 2024)

A breach at Financial Business and Consumer Solutions (FBCS), a debt collection agency, exposed personal data of over 237,700 Comcast customers, including Social Security numbers and birthdates. The incident, linked to a ransomware attack earlier in the year, highlighted risks from third-party service providers.

3. National Public Data breach (August 2024)

National Public Data, which specializes in background checks, faced a massive breach compromising 2.9 billion rows of data. The stolen information included names, Social Security numbers and addresses, exposing millions of individuals. The breach stemmed from a third-party hack that began in late 2023 and persisted into mid 2024.

4. Bloom Hearing Specialists (October 2024)

Australian audiology company Bloom Hearing Specialists experienced a ransomware attack that compromised data for tens of thousands of patients. Stolen information included health records, financial details and government identification numbers, underscoring the vulnerability of health care systems.

5. Hot Topic retail breach (October 2024)

Retailer Hot Topic saw 350 million customer records exposed after the hacking group Dark X infiltrated its systems. This breach emphasized the retail industry's susceptibility to attacks leveraging malware like infostealers.

6. Disney ransomware incident (July 2024)

The entertainment giant Disney experienced a huge breach that exposed over 1.1TB of sensitive data, including 44 million messages, 18,800 spreadsheets and internal project details. The incident underscores the entertainment sector's growing exposure to cyberthreats.

7. Virgin Media breach (July 2024)

Virgin Media reported a breach affecting 900,000 customers due to an unsecured database, exposing personal information like names, addresses and contact details.

8. Prudential Finance cyberattack (February – July 2024)

Prudential Finance reported unauthorized access to customer data in a cyberattack, prompting upgrades to its security measures in February. Only in July did they reveal that over 2.5 million people had their personal information compromised in a February data breach.

9. Evolve Bank breach (July 2024)

Evolve Bank & Trust suffered a breach affecting 7.6 million individuals, exposing sensitive identification details.

10. Fortinet customer data breach (September 2024)

Fortinet confirmed that data from a "small number" of its over 775,000 customers had been compromised. The hacker reportedly accessed information from an Azure SharePoint site and allegedly released it after Fortinet declined to meet ransom demands.

Industries most impacted

1. Financial services

Financial institutions remain prime targets, with breaches like those at SRP Federal Credit Union and Evolve Bank exposing millions of customers' sensitive data. The cost of breaches in this sector is among the highest, with incidents averaging $6 million in damages.

2. Health care

Health care faced sustained attacks, as seen with Bloom Hearing Specialists. The average cost of a health care breach rose to almost $10 million in 2024, marking it as the most expensive industry for data loss for the 13th consecutive year.

3. Retail

Retailers like Hot Topic saw significant breaches, driven by attackers leveraging malware to infiltrate customer data systems.

4. Utilities and energy

The surge in attacks on U.S. utilities highlighted the sector's growing vulnerabilities. As power grids become more digital, outdated software and poor segmentation increase exposure.

5. Technology

Firms like Comcast and Virgin Media demonstrated the ongoing risk in the tech sector, particularly through third-party service providers.

Second half vs. first half of 2024

In the first half of 2024, data breaches affected over one billion individuals, representing a fivefold increase compared to the same period in 2023. The second half of the year, while slightly less devastating in terms of total victims, featured several high-profile incidents involving sensitive personal and financial data.

Globally, over 422 million records were exposed in Q3 2024 alone, reflecting a continued threat level comparable to previous years' peaks. However, ransomware attacks saw a noticeable increase in sophistication, often combining social engineering with technical exploits to infiltrate organizations.

When compared to breaches from 2023, a clear shift in attack vectors is evident, with ransomware groups increasingly targeting third-party service providers and cloud-based systems.

Emerging trends and lessons learned

- Incidents like those at Comcast and National Public Data show the growing reliance on third-party vendors, which often serve as weak links in cybersecurity defenses.
- Groups like Nitrogen have refined their ransomware tactics, targeting not only primary organizations but also their supply chains.
- Cloud systems are increasingly under attack, with human error cited as a primary cause of breaches. Companies must double down on training and automation to secure their cloud environments.
- Each industry faces unique challenges, from outdated infrastructure in utilities to extensive compliance requirements in health care. Tailored solutions are essential to address these sector-specific vulnerabilities.

Conclusion

The data breaches of 2024 highlight an evolving and relentless threat landscape. As attackers grow bolder and more innovative, organizations must stay one step ahead by investing in advanced threat detection, building resilient systems and fostering a culture of cybersecurity awareness.

The lessons from 2024 should serve as a wake-up call for governments, businesses and individuals alike. In 2025, a renewed focus on proactive defenses and cross-industry collaboration will be critical to mitigating the risks posed by cybercriminals.

Here are five key recommendations to prevent data breaches, even if you already have cybersecurity in place:

1. Implement MFA: Even with strong cybersecurity defenses, relying solely on passwords can leave systems vulnerable. MFA adds an extra layer of security by requiring a second form of verification, such as a code sent to a mobile device, reducing the chances of unauthorized access.

2. Conduct regular security audits and penetration testing: Cyberthreats are constantly evolving, so it's crucial to regularly test your security systems for vulnerabilities. Conduct security audits and penetration tests to identify weaknesses before attackers can exploit them.

3. Implement least privilege access control: Limit access to sensitive data to only those employees who absolutely need it for their roles. By applying the principle of least privilege, you can minimize the potential damage caused by compromised accounts or insider threats.

4. Encrypt sensitive data: Encryption ensures that even if data is intercepted or stolen, it remains unreadable without a decryption key. Encrypt sensitive data both at rest and in transit to minimize the impact of any breach.

5. Train employees on security best practices: Human error is often the weakest link in security. Regularly train employees on recognizing phishing attempts, creating strong passwords and following company policies on data protection to reduce the risk of breaches caused by negligence or lack of awareness.

4. AI-generated cyberthreats: Challenges needed to be addressed

AI-assisted cyberthreats have surged as one of the most pressing concerns in 2025. As AI continues to revolutionize various industries, it has also empowered cybercriminals to launch increasingly sophisticated attacks. From malware development to social engineering, AI is both a tool for innovation and a weapon in the hands of malicious actors.

The rise of AI-generated cyberthreats

AI-powered tools like OpenAI's ChatGPT, WormGPT and other generative models have become central to cybercriminals' arsenals. These tools allow attackers to create malicious scripts, spear-phishing emails and even ransomware with minimal technical expertise. As these AI-driven threats increase in scale and sophistication, the need for advanced cybersecurity solutions becomes more critical.

Here's a closer look at the key AI-related threats that emerged in 2024:

1. Exploitation of AI by cybercriminals

OpenAI has confirmed that threat actors are using ChatGPT and other generative AI tools to develop malware, spread misinformation and launch spear-phishing campaigns. In a series of recent cases, cybercriminal groups have leveraged AI to enhance their attacks:

- TA547, also known as Scully Spider, used an AI-generated PowerShell loader to deploy the Rhadamanthys infostealer.
- The Chinese group SweetSpecter targeted OpenAI employees with phishing emails containing malicious attachments, further demonstrating how cybercriminals are harnessing AI to craft more effective attacks.

Moreover, groups like Iran's CyberAv3ngers and North Korea's state-sponsored hackers have used AI tools like ChatGPT to enhance their attacks on critical infrastructure and steal sensitive data. These developments reflect the growing capabilities of low-skilled attackers who can now carry out sophisticated operations with the help of generative AI.

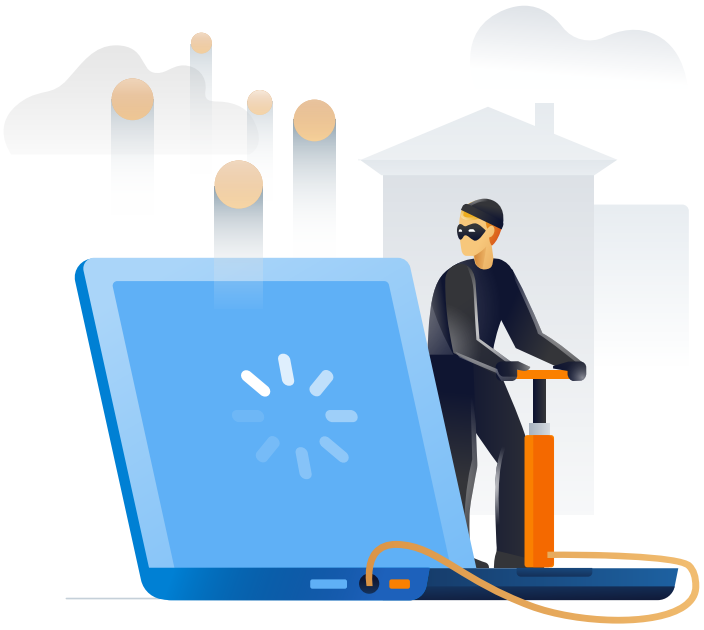
2. Generative AI and malware creation

Generative AI tools, including unregulated models such as WormGPT, FraudGPT and DarkBERT, are empowering cybercriminals to create custom malware and hacking scripts with ease. A striking example comes from a 25-year-old in Japan who used ChatGPT to write ransomware in just six hours.

Such AI models allow cybercriminals to bypass traditional defenses by generating novel attack vectors that evade detection. This trend necessitates a robust, multilayered defense strategy.

3. North Korea's use of AI for cyber operations

North Korea's cyber operations have become increasingly sophisticated with the integration of AI. By leveraging AI to create fake LinkedIn profiles and deepfake videos, North Korean hackers have successfully infiltrated global companies. These deceptive, AI-generated personas have led to significant breaches, including the theft of cryptocurrency and sensitive defense data.



4. AI-driven software supply chain attacks

The widespread adoption of AI-powered tools has made the software supply chain a prime target for cybercriminals. In one recent incident, attackers uploaded malicious packages to the Python Package Index (PyPI) repository, impersonating popular AI models like ChatGPT and Claude. These packages, which garnered thousands of downloads, contained a Java-based infostealer called JarkaStealer. Upon installation, the malware stole sensitive data, including web browser information and session tokens.

5. FBI warning on AI-powered fraud schemes

The FBI has raised alarms about the use of AI to enhance the scale and sophistication of fraud schemes. From romance scams to fake investment promotions, AI-generated content is making it easier for cybercriminals to deceive victims. By creating realistic text, images and even deepfake videos, attackers can craft more convincing and widespread fraud campaigns.

5. The dual nature of AI: Innovation vs. misuse

The rise of AI in cybercrime illustrates the dual nature of this technology. On one hand, AI offers immense potential for innovation, with applications in fields like health care, finance and logistics. On the other hand, its misuse is enabling cybercriminals to create more sophisticated, scalable and automated attacks. This highlights the urgent need for comprehensive cybersecurity strategies that can keep pace with rapidly evolving threats.

In response to the rise of AI-driven cyberthreats, Acronis continues to enhance its cybersecurity offerings, ensuring that businesses and individuals are equipped to defend against the next generation of cyberattacks. Acronis Advanced Security + XDR provides proactive monitoring, AI-powered threat detection and real-time response capabilities, enabling organizations to neutralize emerging threats before they cause significant harm.

6. 4 recommendations for mitigating AI-driven threats

1. Implement multilayered security: Leverage a combination of behavioral analysis, heuristic detection and AI-driven monitoring to detect and block AI-generated threats.

2. Stay updated on AI vulnerabilities: Regularly update software and security protocols to protect against AI-driven vulnerabilities and exploit attempts.

3. Educate employees and partners: Awareness is key. Provide regular training on recognizing AI-powered phishing attempts, deepfakes and other social engineering tactics.

4. Utilize AI for defense: Just as cybercriminals use AI to enhance their attacks, cybersecurity vendors should also use AI to detect and neutralize threats faster and more effectively.

7. Conclusion

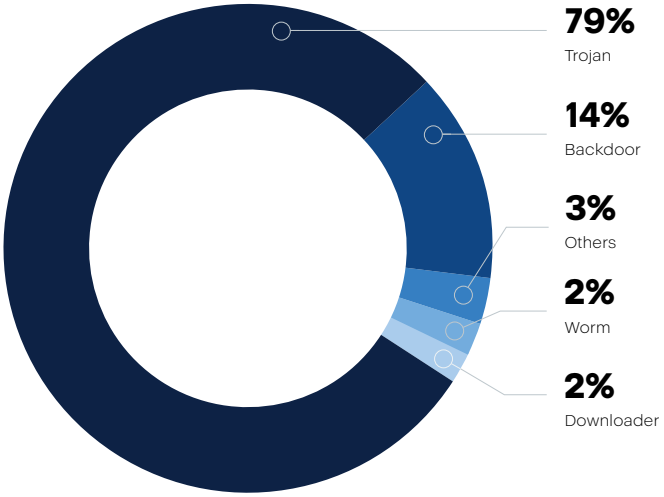
The rise of AI-assisted cyberthreats represents a significant shift in the cybersecurity landscape. As AI continues to empower both attackers and defenders, it is crucial for organizations to adopt robust, AI-driven security measures to stay one step ahead. Acronis' advanced security solutions are designed to address these challenges, providing comprehensive protection against the growing threat of AI-powered cybercrime. By combining proactive monitoring, behavioral analysis and AI-powered defense mechanisms, businesses can defend against the evolving landscape of AI-driven threats.

2

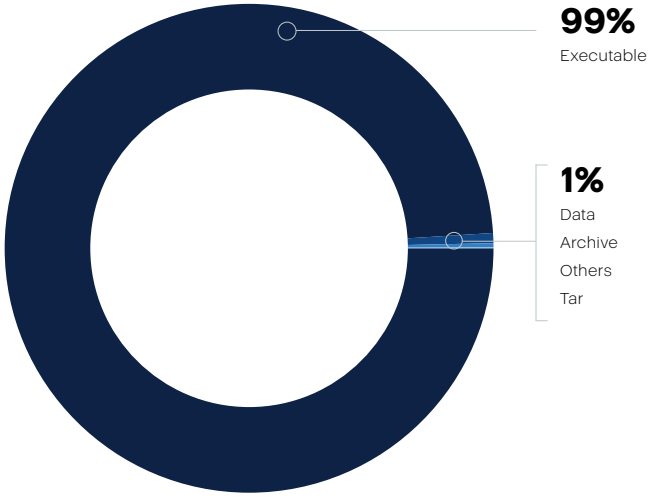
General malware threats

In January, about 17.9% of Acronis customers had at least one malware attack successfully blocked on their endpoints. In September, malware attacks peaked at 26.6% and dropped slightly to 22.8% by December, which was closer to the 23.1% average for the year.

These figures underscore the critical importance of detection efforts within a robust, multilayered security strategy. Even with awareness training and proactive patching, approximately two out of every ten threats still evade initial defenses and reach the endpoint. This highlights a gap in earlier layers of protection, such as proxy filters and email security systems, emphasizing the need for advanced EDR capabilities to catch what slips through the gaps.



Malware types detected in the first two weeks of December 2024 (source: av-test.org)

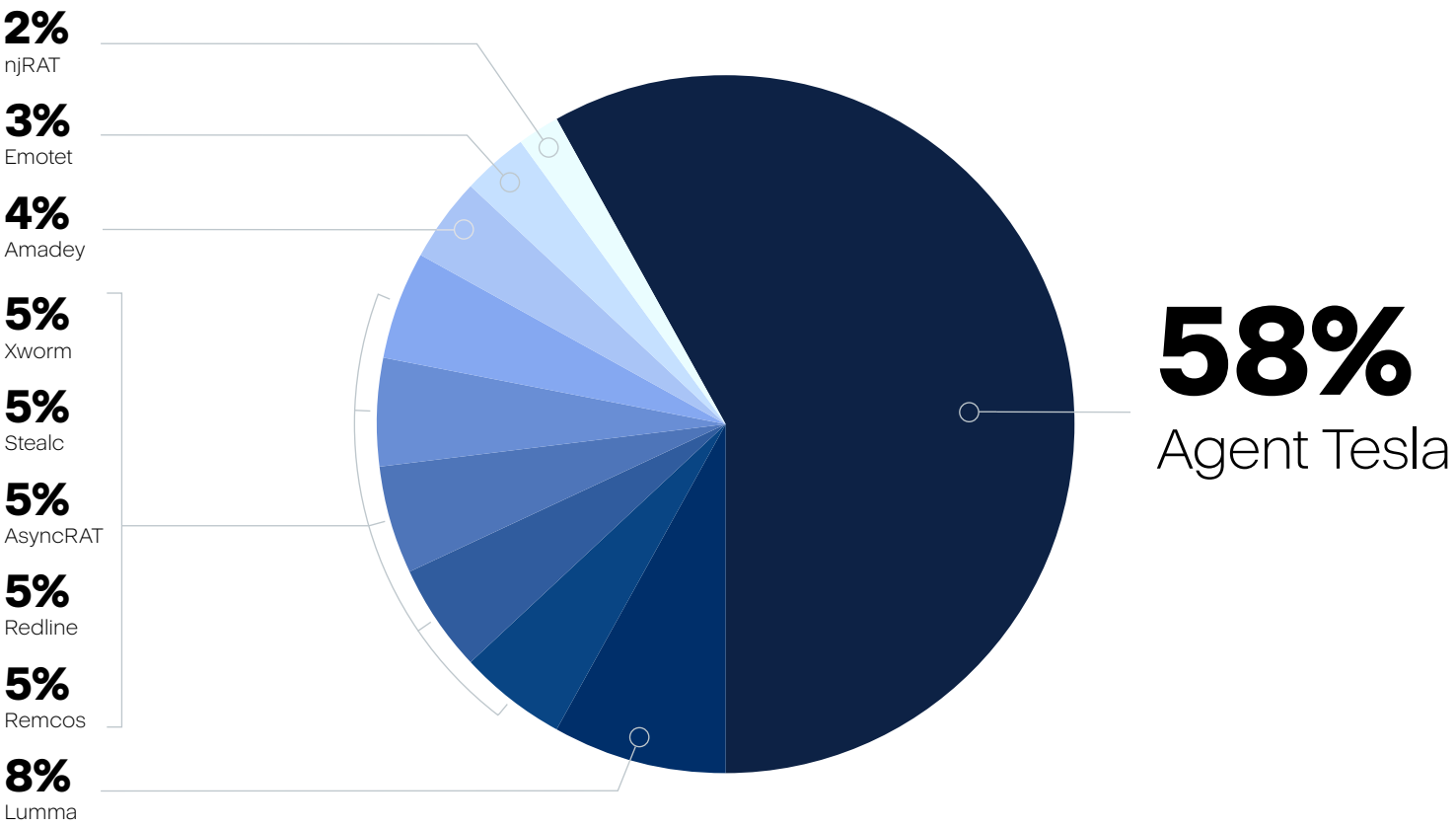


Windows file types detected in the first two weeks of December 2024 (source: av-test.org)

Month in 2024	Percentage of clients with blocked malware
January	17.9%
February	20.8%
March	26%
April	28%
May	23.8%
June	22.7%
July	22.8%
August	21.1%
September	26.6%
October	21.3%
November	23.4%
December	22.8%

The most common malware type are Trojan horses, making up 75% of the blocked threats. Below is a list of the 10 most commonly seen malware families for H2 2024, with a clear focus on information stealers and remote access trojans:

- Lumma
- Agent Tesla
- AsyncRAT
- Remcos
- Stealc
- Redline
- Xworm
- Amadey
- Emotet
- njRAT



Since Q4 2022, we have seen more than a 50% increase in the number of new malware samples appearing in the wild. Independent malware testing lab AV-TEST recorded 289,530 new malware samples per day in Q4 2024 and 219,741 per day in Q1 2024, compared to 162,430 in Q4 2023.

This proportion matches the number of new samples seen by Acronis TRU. This increase could be the result of some spikes along the year, as well as more targeted distribution methods of malware — for example, through malware droppers and distribution chains.

In a recent article, Acronis TRU analyzed a case in which threat actors employed a complex chain starting with a phishing email containing a RAR archive, which held a malicious Visual Basic Script (VBS) file titled "Citación por embargo de cuenta" (translated as "Summons for account garnishment"). The VBS file's purpose was to lure Spanish-speaking recipients into immediate execution, triggering a multilayered infection chain that used various script languages. This chain ultimately aimed to deploy well-known malware families such as DCRat, the Rhadamanthys infostealer and Remcos.

While the campaign's sophistication highlights how attackers obscure payloads to evade detection, it also introduces points of failure that security solutions can exploit to disrupt the attack. Analysis revealed similar campaigns with the same infection chain but different final payloads, showcasing the versatility and adaptability of these tactics.

Notably, DCRat ranked 11th among the top malware families used in this campaign, falling just outside the top 10 dominated by threats like Remcos which landed at fourth place. The continued use of both dated and advanced malware via layered delivery emphasizes the importance of robust security solutions capable of detecting malicious activity at any stage of the chain.

While the main threat families in downloaders, infostealers and ransomware have advanced in functionality, there has been little evidence of entirely new techniques emerging.

In December 2024, customers in the United Arab Emirates, Singapore and Italy experienced the most malware detections among customers in all focus countries.

We normalized the number of detections per active client in each country. The table below presents the normalized percentage of clients per focus country that recorded at least 25 malware detections in December 2024.

Normalized malware detection rates in focus countries

Country	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEPT	OCT	NOV	DEC
Australia	17.1%	16.4%	20.4%	23.4%	20.1%	18%	20.1%	17.4%	21.5%	17.7%	19.4%	25.8%
Brazil	22.6%	23.3%	31.1%	31.7%	28%	28.4%	28%	24.9%	37.2%	27.4%	27.2%	29%
Canada	8.2%	9.2%	11.2%	14.4%	12.1%	12.%	12.1%	12.6%	15.1%	11.6%	14.6%	15.2%
France	14.4%	19.4%	24%	26.7%	20.4%	20.1%	20.4%	19.4%	25.9%	20.5%	24.7%	28.4%
Germany	20.2%	21.7%	25.6%	27.5%	23.7%	22.5%	23.7%	22.9%	24.4%	20.2%	25.3%	26.7%
Italy	18.2%	13.2%	27.9%	30.1%	26.8%	25.1%	26.8%	22%	29.7%	21.8%	24.9%	30.6%
Japan	14%	20.9%	15.7%	16.7%	14.1%	13.1%	14.1%	12.6%	14.8%	12%	15.2%	24.3%
Netherlands	18.4%	20.4%	25.9%	26.1%	21.9%	20.2%	21.9%	20.3%	23.4%	18.5%	21.6%	25.9%
Singapore	43.9%	38%	29.6%	41.7%	29%	28.7%	29%	25.7%	28.7%	28.5%	24.2%	31.6%
South Africa	14.2%	33%	25.9%	27.9%	23%	21.4%	23%	18.9%	24.9%	19.6%	20.2%	27.9%
Spain	32.2%	16.6%	40.5%	37.5%	31.2%	29.8%	31.2%	27.1%	33.3%	25.9%	29%	30.3%
Switzerland	17.3%	22.5%	24%	24.8%	20.4%	19.5%	20.4%	18.5%	19.7%	14.9%	19.8%	26%
United Arab Emirates	17.6%	18.8%	29.1%	29.3%	29.3%	28.5%	29.3%	26.7%	36.6%	29.7%	29.7%	32.8%
United Kingdom	13.8%	17.5%	20%	19.5%	16.5%	14.7%	16.5%	14.5%	16.1%	13.4%	14.3%	21.2%
United States	16%	24.9%	30.9%	33.7%	26.8%	24.1%	26.8%	23.1%	25.4%	21.3%	21.9%	25.9%

Ransomware threats

The rise of AI tools has dramatically lowered the barriers to creating ransomware, enabling even low-skilled individuals to execute advanced attacks. Cybercriminals have exploited Large Language Models (LLMs) like ChatGPT to automate and scale ransomware operations, as seen in cases where a Japanese attacker crafted ransomware in hours and Chinese criminals used VPNs to access ChatGPT for extortion schemes.

Unregulated AI tools like WormGPT and FraudGPT further empower low-skilled actors to develop phishing and hacking tools, expanding the pool of attackers. With a surge in data breaches providing sensitive information for exploitation, ransomware attacks have become more frequent and severe. This growing complexity demands AI-driven solutions and a multilayered cybersecurity approach, as traditional defenses are no longer sufficient. Organizations must adopt advanced threat detection, automated responses and comprehensive security strategies to navigate the evolving ransomware landscape effectively.

Still, ransomware remains a top concern for individuals and organizations worldwide due to its persistent frequency and impact. From July to December 2024, our Acronis Active Protection blocked numerous ransomware attacks globally. We also analyzed data published on underground leak sites by ransomware operators.

Daily ransomware detections

The number of ransomware detections stayed relatively flat for 2024, increasing only 8% in Q4 2024 compared to Q4 2023. Overall, from 2023 to 2024, the number of detections decreased by 15%.

The daily number of ransomware detections also appears to be relatively stable, with no significant spikes recently and only a slight upward trend overall. This reinforces the importance of maintaining high resilience, as well as the frequent testing and adoption of an incident response plan.

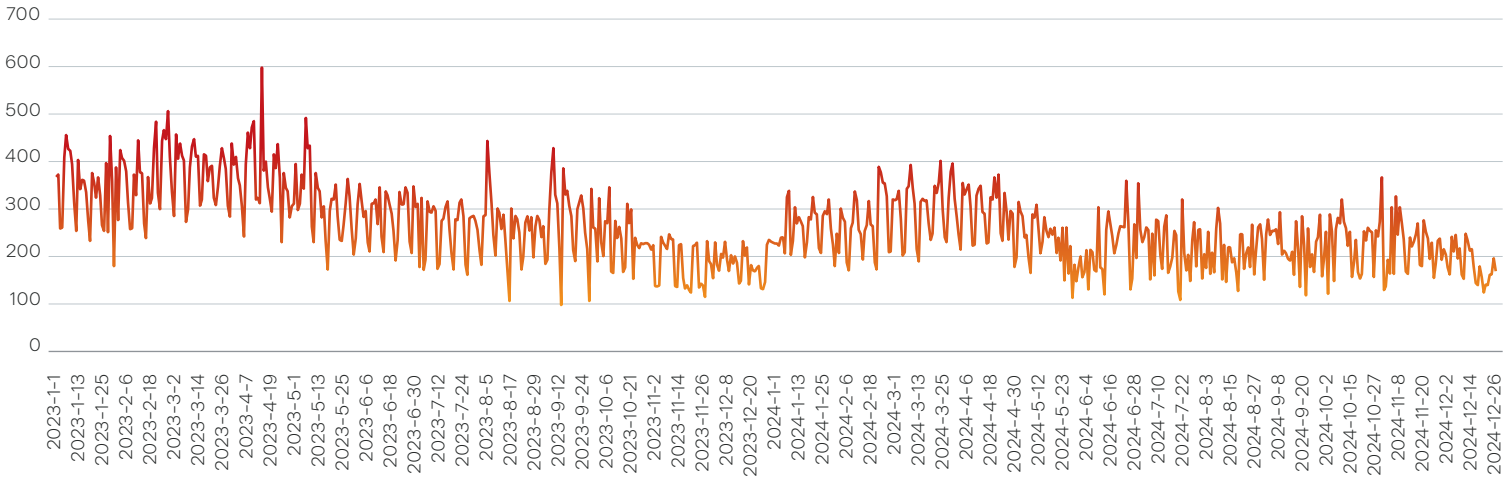
Such procedures are crucial for ensuring that companies are well-prepared to defend against and respond to ransomware attacks.

Daily ransomware detections globally

Ransomware detections peaked on March 28, 2024, while July 25 saw the lowest number of detections in 2024.

In the below chart, we have normalized the number of ransomware detections, considering only machines with more than 25 detections and countries where we have more than 150 installations.

Daily ransomware detections 2023–2024



Normalized ransomware detections in focus countries

Country	Q1 2024	Q2 2024	Q3 2024	Q4 2024
Australia	2.6%	2.6%	1.9%	1.3%
Canada	5.5%	5.1%	4.5%	3.9%
France	4.1%	4%	2.7%	2.5%
Germany	13.4%	13.8%	10.4%	10.9%
Italy	1.9%	2%	1.1%	1.3%
Japan	16.5%	13.7%	12.7%	10.3%
Netherlands	4.3%	4.5%	3.4%	2.8%
Spain	4.5%	2.8%	1.9%	1.5%
United Kingdom	2.5%	2%	1.5%	1.3%
United States	5.4%	4.8%	4%	3.5%

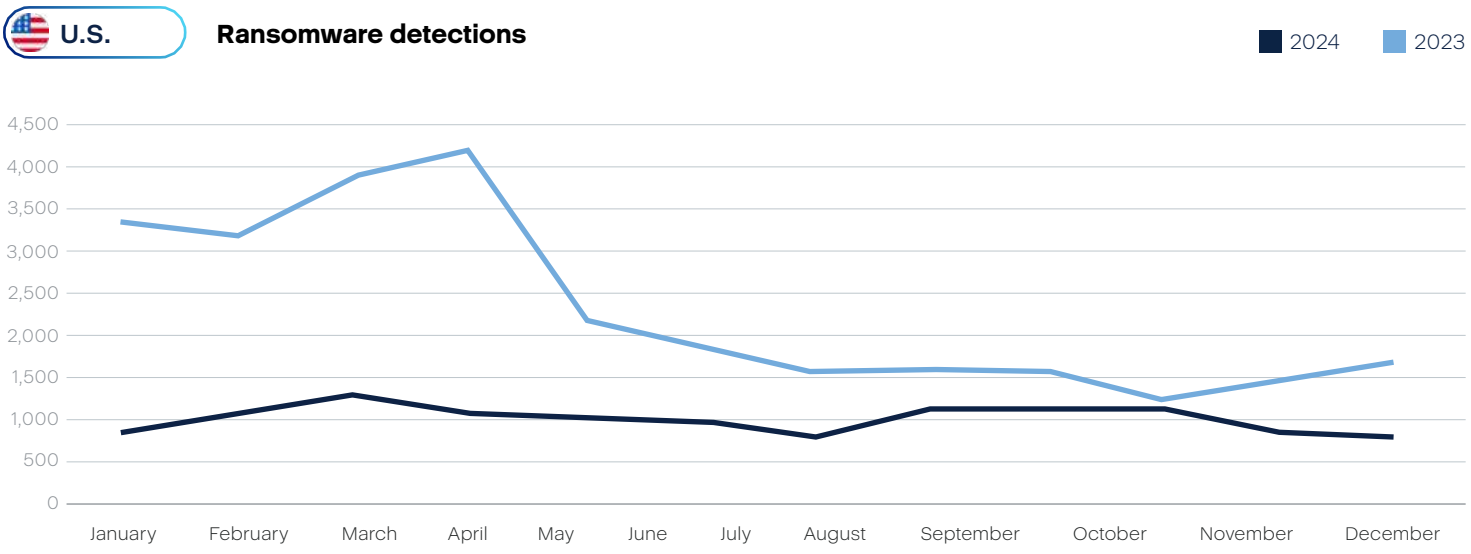
Ransomware activity in focus countries

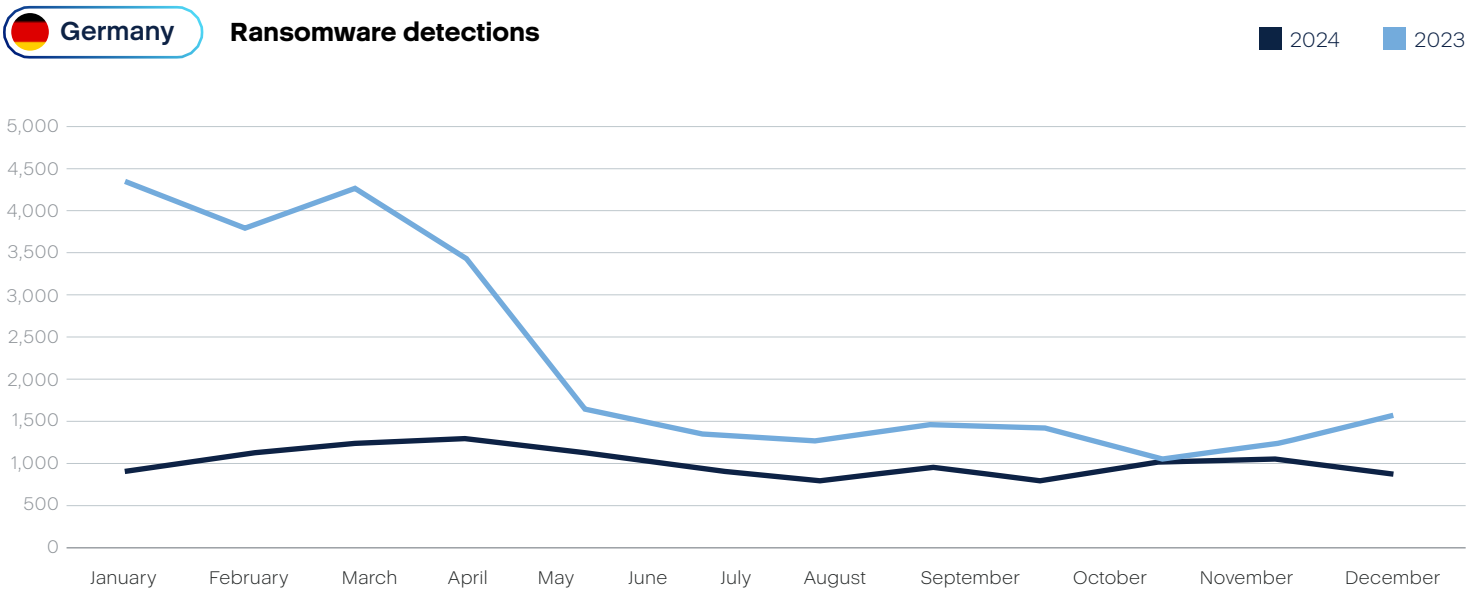
Ransomware remains a persistent threat, affecting organizations across industries and regions. Certain cybercriminal groups tend to focus on specific targets, shaping attack patterns over time.

The following graphs highlight monthly ransomware detections at the endpoint, revealing a common trend of a nearly flat trajectory in 2024. Key observations include:

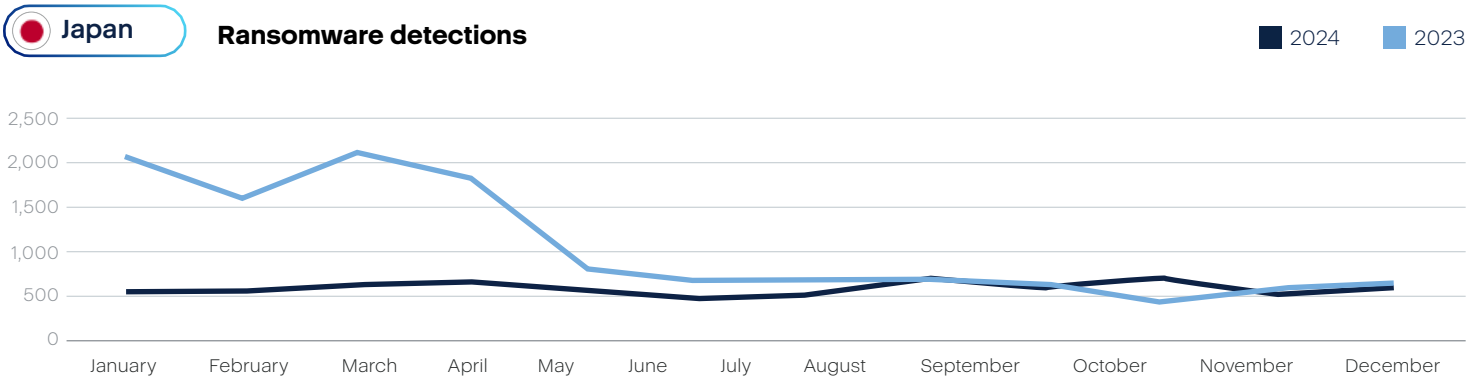
- A significant drop of over 100% in ransomware detections in most months when comparing H1 2023 to H1 2024.
- A continuation of the downward trend seen at the end of 2023, with 2024 showing consistently low activity across all selected countries.

This shift underscores the growing caution among organizations, many of which are implementing comprehensive, defense-in-depth strategies. These approaches combine endpoint protection, regular updates and advanced threat detection capabilities, fostering a more resilient posture against ransomware threats.

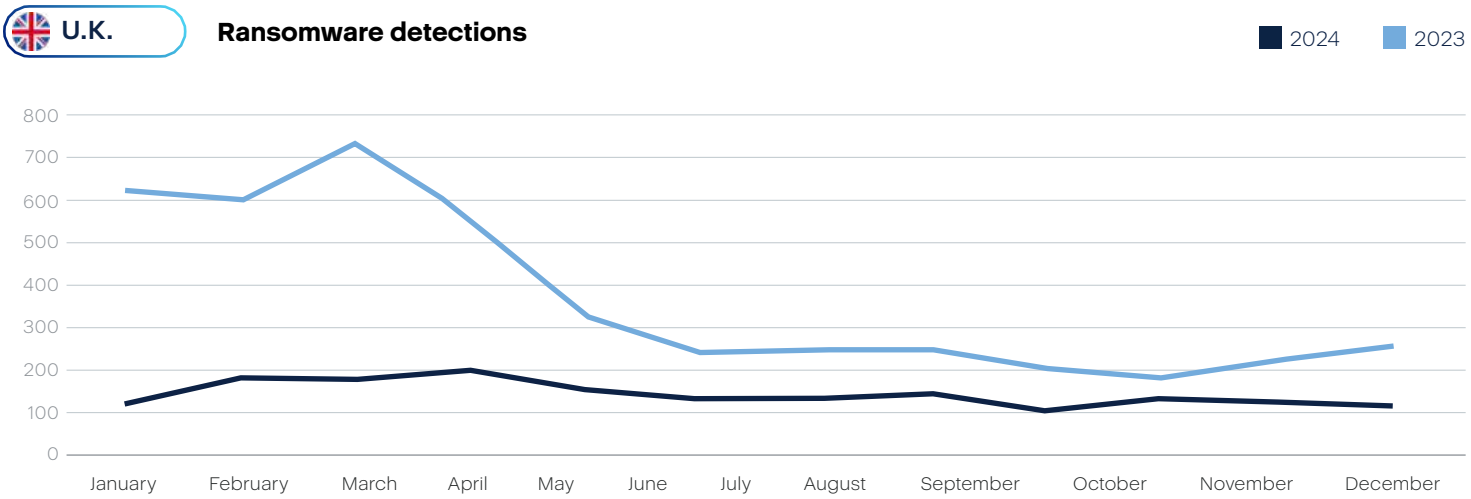




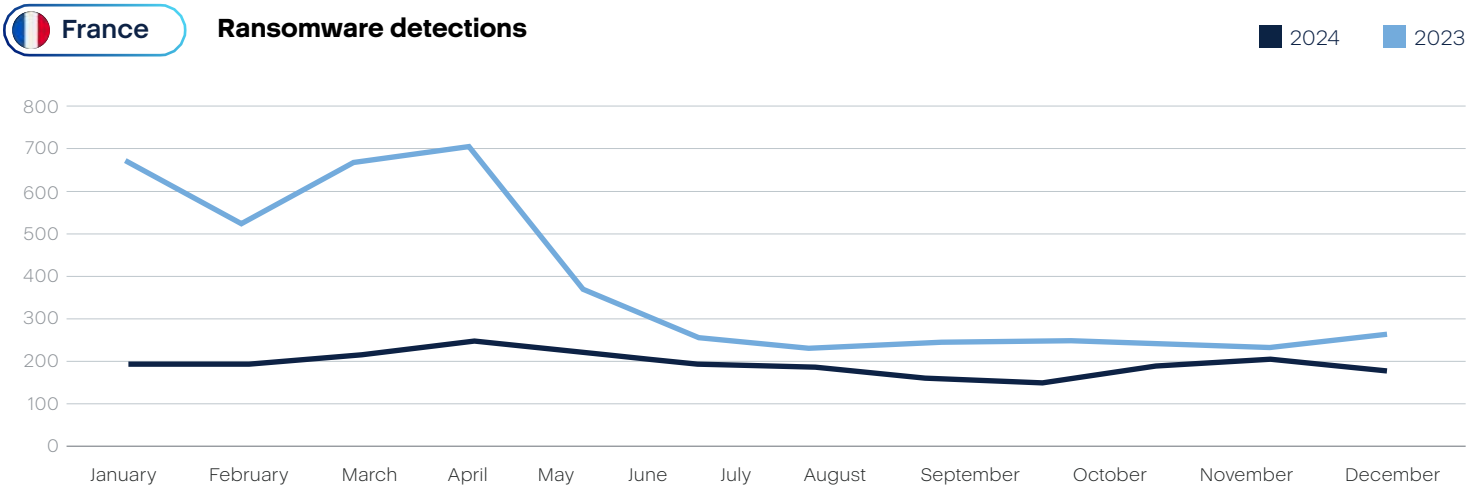
Japan **Ransomware detections**



U.K. **Ransomware detections**



France **Ransomware detections**



Middle East and Africa region

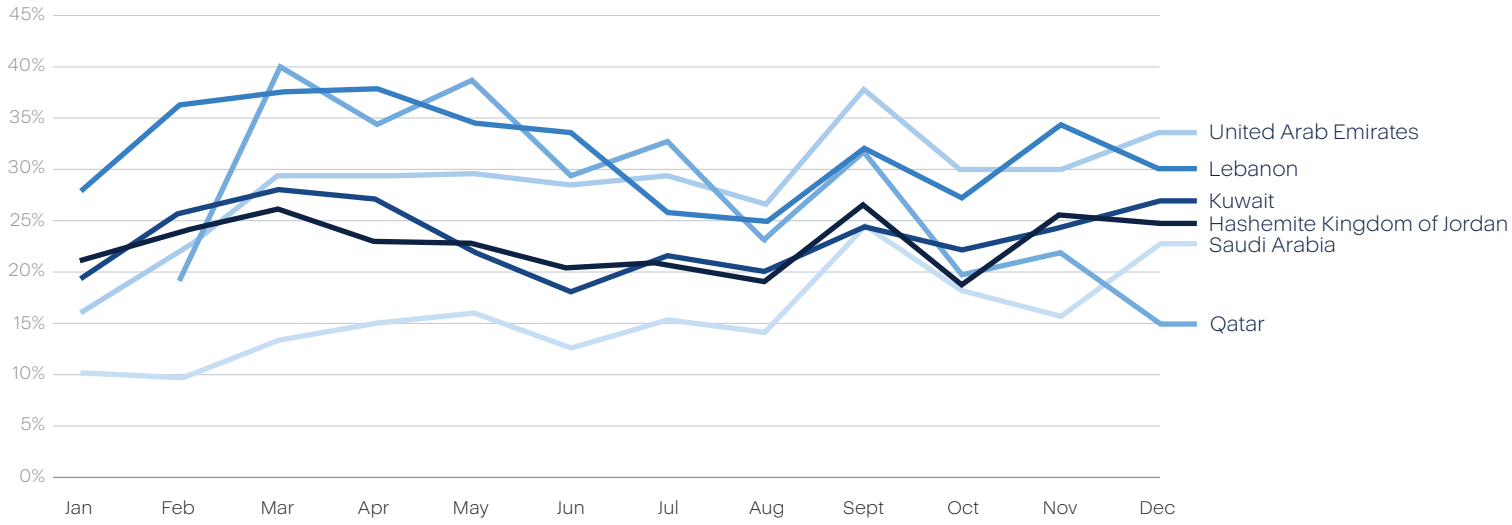
The telemetry data on malware detections across Middle Eastern countries reveals significant trends and variations throughout the year. Lebanon consistently experienced the highest detection rates, with peaks surpassing 35% in February, March and April — likely due to targeted campaigns exploiting regional vulnerabilities or increased phishing and ransomware activity. Similarly, Qatar saw sharp spikes in February and April, reaching over 35%, which may indicate seasonal campaigns or increased exposure during major events requiring online services.

Moreover, those types of campaigns exploit outdated infrastructure, geopolitical tensions and sectors undergoing rapid digital transformation, such as health care, energy and financial services. The United Arab Emirates (UAE) showed a significant malware detection increase in September, possibly driven by a rise in BEC attacks or APTs targeting its thriving financial and technology sectors.

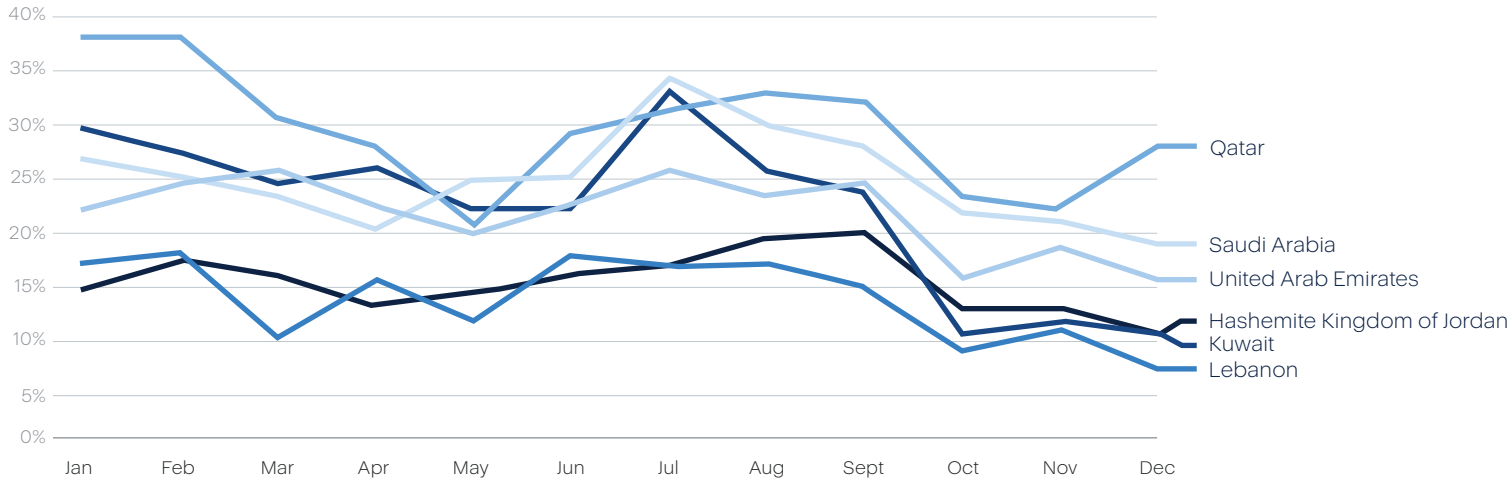
In contrast, Saudi Arabia exhibited a relatively stable detection trend with minor fluctuations, maintaining malware levels below 20% for most of the year, suggesting stronger baseline defenses or fewer high-profile incidents. Kuwait experienced a drop midyear but surged again in November, reflecting a likely wave of email-based attacks or a resurgence of malware targeting governmental or industrial systems. The Hashemite Kingdom of Jordan maintained lower detection rates throughout the year, with only a slight rise in September and November, which may suggest fewer cyber incidents or underreporting.

Overall, the trends underscore how cybercriminals in 2024 are leveraging increasingly complex delivery chains, AI-powered tools and phishing campaigns to breach organizations in the Middle East. The high frequency of ransomware incidents — combined with malicious campaigns targeting critical infrastructure — demands a proactive and integrated strategy across the region. Stronger investments in endpoint security, AI-driven threat detection and regional collaboration are critical to mitigate evolving cyberthreats.

Malware detections



URL detections



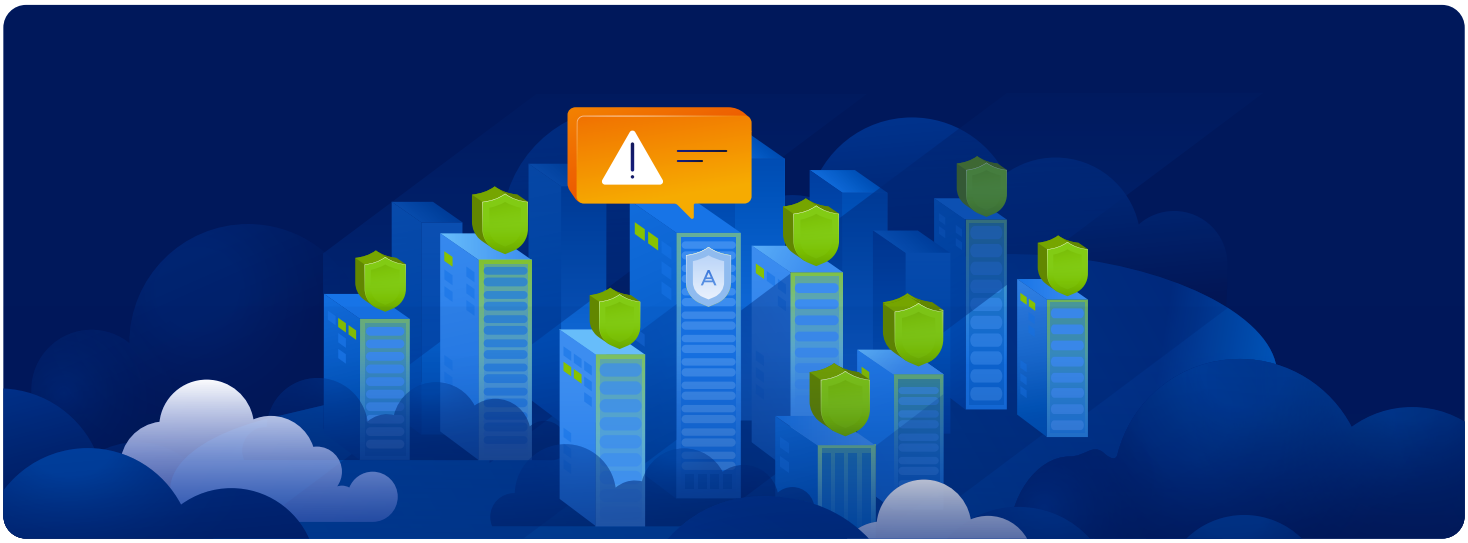
Malicious websites

Acronis blocked 48,274,660 phishing and malicious URLs in Q4 2024. This increase in detections — a 7% jump from Q3 (44,983,415) — can be explained by heightened online activity during the holiday shopping season, particularly on days like Black Friday and Cyber Monday. Campaigns like the infamous "Phish n' Ships," which has infected over 1,000 legitimate online stores, exploit this period by redirecting users to fraudulent sites that steal payment and personal data.

Cybercriminals also employ advanced tactics, such as SEO manipulation, fake delivery notifications and spoofed shopping sites to deceive users with seemingly legitimate offers and alerts.

These tactics underscore the necessity of a comprehensive security approach that integrates AI-powered detection, MFA and behavioral analysis to outpace these evolving threats. Businesses and consumers alike must stay vigilant, combining proactive monitoring with incident response plans to mitigate risks during this high-stakes season.

Month	Blocked URLs	Total for the quarter
January	10,258,621	
February	8,432,586	27,994,848
March	9,303,641	
April	11,526,276	
May	13,406,456	37,243,111
June	12,310,379	
July	10,894,190	
August	15,294,700	44,983,415
September	18,794,525	
October	18,392,962	
November	12,584,732	48,274,660
December	17,296,966	



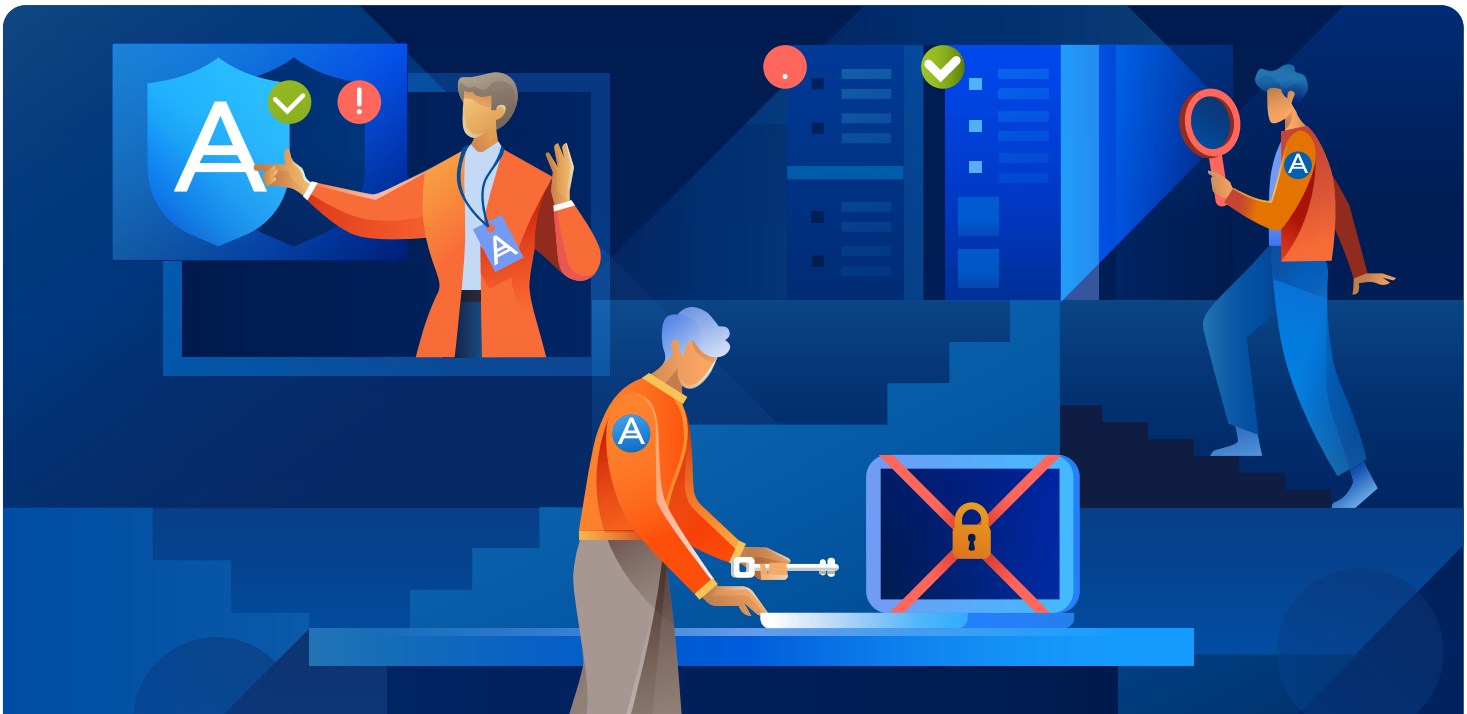
An average of 19.2% of endpoints tried to access malicious URLs in Q3 2024, up from 16.2% in Q4 2023. In September, attempts to access malicious URLs spiked at 19.2% but then dropped to 11.5% in December.

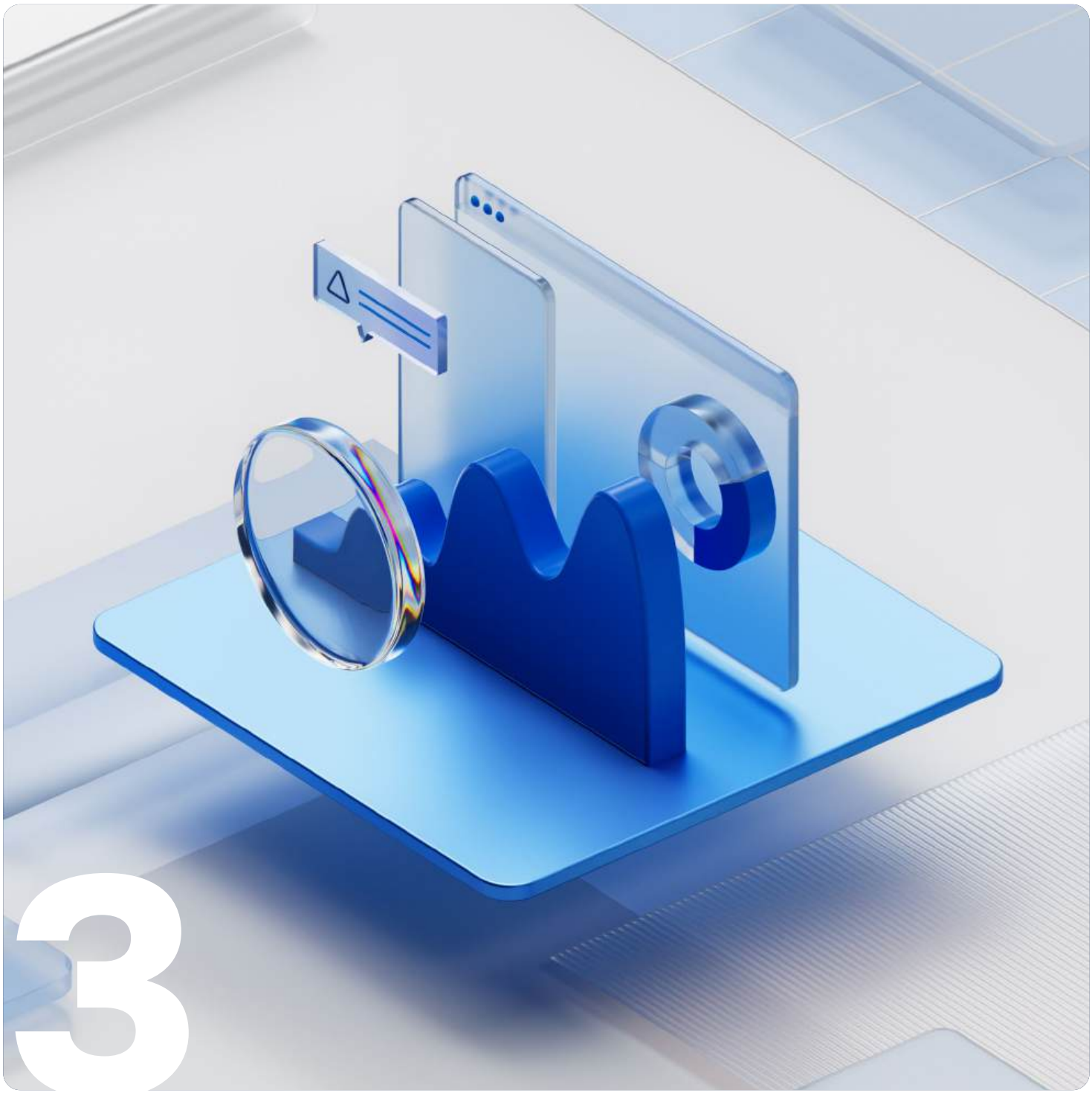
Month	Percentage of users that clicked on malicious URLs
January	17.3%
February	17.7%
March	17.5%
April	17.5%
May	17.1%
June	17.6%
July	19.3%
August	19.1%
September	19.2%
October	12.9%
November	14.9%
December	11.5%

Among all focus countries, the United Arab Emirates had the largest percentage of blocked malicious URLs at the endpoint in December 2024 (16.2%), followed by Brazil with 13.2% and Singapore with 12%.

Rank	Country	Percentage of blocked URLs in December 2024
1	United Arab Emirates	16.2%
2	Brazil	13.2%
3	Singapore	12%
4	Germany	11.9%
5	United States	11.3%
6	South Africa	11.1%
7	France	9.9%
8	Netherlands	9.9%
9	Australia	9.8%
10	Canada	9.3%
11	Spain	8.6%
12	Italy	7.5%
13	Japan	7.4%
14	United Kingdom	7.2%
15	Switzerland	6.6%

Similar to the malware detection statistics, we normalized the numbers based on the number of active machines in each country with at least 25 blocked URLs.





3

Vulnerabilities discovered in products of key software vendors

In the second half of 2024, the cybersecurity landscape was marked by a significant increase in software vulnerabilities. As of November 2024, the Common Vulnerabilities and Exposures (CVE) database cataloged over 240,000 vulnerabilities. For instance, in September 2024 alone, nearly 2,800 vulnerabilities were disclosed. Notably, cross-site scripting (CWE-79) continues to be the most dangerous software weakness, ascending to the top of the Common Weakness Enumeration (CWE) list.

Additionally, the automotive industry faced scrutiny as vulnerabilities in web portals of major car manufacturers, including Kia, were discovered. These flaws allowed unauthorized control over vehicle features, emphasizing the need for improved web security in connected vehicles. The period also saw a rise in zero-day exploitations, with attackers increasingly targeting unpatched vulnerabilities to compromise enterprise systems.

In response to a significant CrowdStrike incident in July 2024, Microsoft announced the Windows Resiliency Initiative. This initiative aims to enhance Windows security and recovery capabilities, including features like Quick Machine Recovery and improved controls over applications and drivers. These measures are designed to prevent future vulnerabilities and improve system resilience.

Cybersecurity vendors were attacked and exploited as well, including U.K. cybersecurity firm Sophos, which engaged in a complex battle with Chinese hackers intent on exploiting Sophos' firewall products. The hackers, traced to Chengdu, China, are linked to groups like APT41 and APT31 and have targeted numerous high-profile entities, including military facilities and government agencies.

Top vulnerabilities of 2024 exploited in the wild

Here are 10 notable vulnerabilities discovered and exploited by cybercriminals in the second half of 2024:

1. CVE-2024-20767: An improper access control vulnerability in Adobe ColdFusion allowed attackers to execute arbitrary code on affected systems. This flaw was actively exploited in the wild.

2. CVE-2024-35250: A vulnerability in the Microsoft Windows Kernel-Mode Driver permitted attackers to perform untrusted pointer dereference, leading to potential system compromise. This issue was also actively exploited.

3. CVE-2024-2193: The GhostRace vulnerability, a variant of the Spectre-V1 attack, affected major CPU architectures, including Intel, AMD and ARM. It allowed attackers to exploit speculative race conditions, potentially leading to unauthorized data access.

4. CVE-2024-2201: A vulnerability in certain Intel CPU families, known as InSpectre Gadget, could be exploited entirely in user space without root access, bypassing existing mitigations and leading to potential data leaks.

5. CVE-2024-28746: The Register File Data Sampling (RFDS) vulnerability in Intel Atom processors allowed attackers to sample register file data, potentially leading to sensitive information disclosure.

6. CVE-2024-43451: A critical remote code execution vulnerability in Windows Scripting Languages was exploited by attackers to execute arbitrary code by convincing users to visit malicious websites.

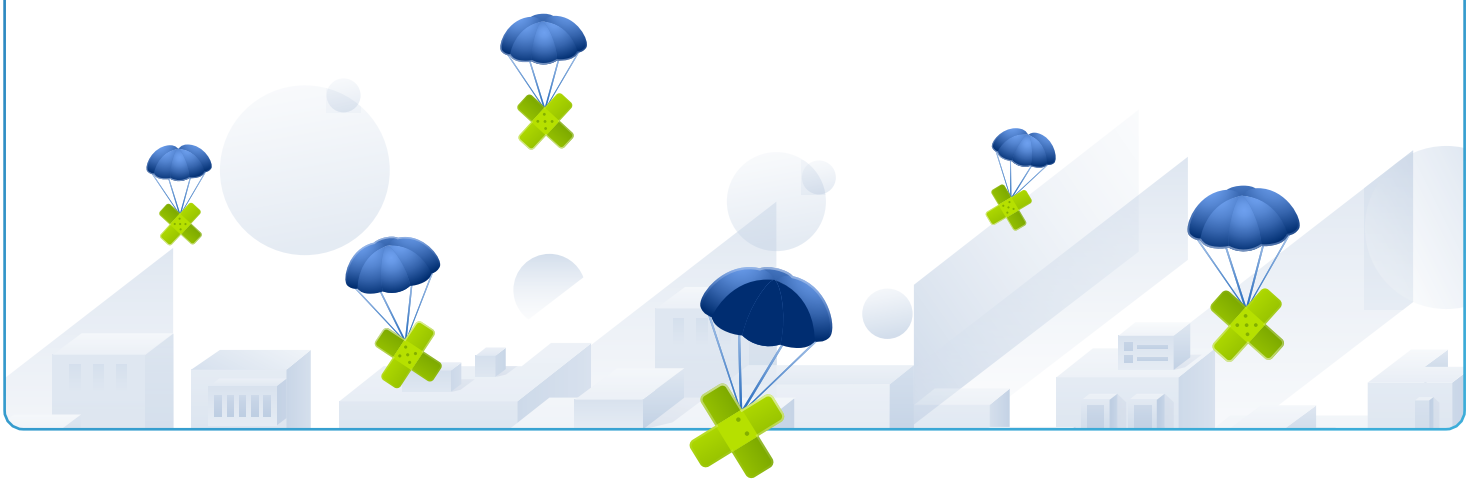
7. CVE-2024-49039: A critical remote code execution vulnerability in Microsoft Exchange Server allowed attackers to execute arbitrary code by sending specially crafted emails, leading to potential system compromise.

8. CVE-2024-43498: A critical remote code execution vulnerability in Windows Graphics Component permitted attackers to execute arbitrary code by persuading users to open specially crafted files.

9. CVE-2024-43639: A critical remote code execution vulnerability in Windows Media Foundation allowed attackers to execute arbitrary code by convincing users to open malicious media files.

10. CVE-2024-34102: A critical vulnerability in Adobe Commerce and Magento Open Source could lead to arbitrary code execution, posing significant risks to e-commerce platforms.

These vulnerabilities highlight the ongoing challenges in cybersecurity, emphasizing the need for timely updates and robust security measures to protect systems against exploitation.



Microsoft, Adobe and others: Regular patchwork

Throughout the period from July to December 2024, Microsoft addressed a total of more than 600 vulnerabilities, with almost 30 classified as critical RCE flaws.

July 2024 142 vulnerabilities, including five critical remote code execution (RCE) flaws and four zero-day vulnerabilities.

August 2024 120 vulnerabilities, including three critical RCE flaws and two zero-day vulnerabilities.

September 2024 87 vulnerabilities, including four critical RCE flaws and three zero-day vulnerabilities.

October 2024 98 vulnerabilities, including six critical RCE flaws and two zero-day vulnerabilities.

November 2024 87 vulnerabilities, including four critical RCE flaws and four zero-day vulnerabilities.

December 2024 73 vulnerabilities, including 16 critical and 54 important severity vulnerabilities. December updates also included a fix for a zero-day vulnerability known to be exploited in the wild.

Between July and December 2024, Adobe addressed a total of 247 vulnerabilities across 16 products. The vulnerabilities varied in severity, with several classified as critical, posing significant risks to users.

July 2024 Adobe released security updates addressing a total of 30 vulnerabilities across multiple products. Notably, vulnerabilities in Adobe Acrobat and Adobe Reader were among the most critical. The patched issues included flaws that allowed for arbitrary code execution, which could have been exploited remotely, potentially compromising users' systems. Adobe also addressed vulnerabilities in Adobe Flash Player and Adobe Photoshop, which, if left unpatched, could have enabled attackers to escalate privileges and gain unauthorized access to sensitive system data.

August 2024 Adobe addressed 72 vulnerabilities across its products. Key updates focused on Adobe Acrobat and Adobe Experience Manager, with several vulnerabilities in these tools involving issues such as cross-site scripting (XSS) and privilege escalation. These vulnerabilities could allow attackers to bypass security restrictions and execute malicious code, posing a significant threat to both individual users and organizations.

September 2024 Adobe released a particularly large batch of security updates, with a total of 35 vulnerabilities addressed. A significant portion of these patches related to Adobe Acrobat and Adobe Reader, in which 23 vulnerabilities were fixed, including several that allowed arbitrary code execution. These vulnerabilities were considered critical due to their potential to compromise user systems, highlighting the need for constant monitoring and rapid response to vulnerabilities in widely used software products. Adobe also patched seven vulnerabilities in Adobe Photoshop, primarily related to privilege escalation, which could have allowed attackers to gain elevated system privileges and access sensitive information.

October 2024 Adobe addressed 21 vulnerabilities across its products. The vulnerabilities were spread across Adobe Acrobat, Adobe Flash Player and Adobe Experience Manager. Several issues allowed attackers to exploit vulnerabilities remotely, while others targeted privilege escalation and potential information leaks. These patches were vital in maintaining the integrity and security of the Adobe ecosystem — especially for enterprise users who rely on Adobe products for critical workflows.

November 2024 Adobe continued its pattern of addressing security flaws with a focus on Adobe Acrobat and Adobe Reader, patching 18 vulnerabilities. These vulnerabilities were mostly related to arbitrary code execution, and several were classified as critical due to the ease with which attackers could exploit them. Additionally, patches were released for other Adobe products, such as Adobe Photoshop, in which privilege escalation vulnerabilities were addressed. These patches ensured that Adobe's widely used software remained protected against the increasing sophistication of cyberthreats.

December 2024 December was a particularly active month for Adobe, with the company addressing over 160 vulnerabilities. These updates spanned a range of Adobe products, including Adobe Acrobat, Adobe Reader, Adobe Photoshop and Adobe Flash Player. Many of the issues addressed involved arbitrary code execution, privilege escalation and information disclosure vulnerabilities, which were critical in nature. Adobe's timely response to these vulnerabilities was essential in protecting users from potentially catastrophic attacks.

The increasing frequency and severity of vulnerabilities in widely used products emphasize the growing cybersecurity challenges businesses and individuals face. With cyberthreats becoming more sophisticated, organizations must adopt robust security practices, including regular patching and security awareness training, to mitigate the risks posed by vulnerabilities in software products.

Overall, Adobe's vulnerability patching efforts reflect the challenges of securing widely used software products, and the company's proactive approach serves as an example for other software vendors to follow in maintaining a secure digital environment for users.

chrome

Over the second half of 2024, Google Chrome addressed a considerable amount of critical vulnerabilities, many of which had the potential for significant exploitation. The vulnerabilities spanned a variety of components, including the browser's renderer, JavaScript engine and other internal processes, exposing users to potential remote code execution (RCE), data leakage and privilege escalation attacks.

July 2024

A new Chrome version was released addressing July's V8 JavaScript vulnerability, and Google urged all Chrome users to update immediately. Additionally, on August 19, 2024, Microsoft reported a zero-day flaw in Chrome's V8 JavaScript and WebAssembly engine, tracked as CVE-2024-7971. This vulnerability was a type confusion flaw, allowing for remote code execution and already being exploited in the wild. Google published an advisory two days later, and the vulnerability was added to the U.S. Cybersecurity and Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities catalog five days after the vendor publication.

August 2024

Google released Chrome 127 to the stable channel, addressing 24 vulnerabilities, 16 of which were reported by external researchers. Among the vulnerabilities patched, memory safety bugs were predominant, accounting for half of the externally reported issues, including four high-severity ones. The update resolved five high-severity vulnerabilities, including three use-after-free flaws in Downloads, Loader and Dawn, an out-of-bounds memory access in ANGLE, and an inappropriate implementation in Canvas.

A critical zero-day vulnerability — CVE-2024-7965 — was discovered in Google Chrome's V8 JavaScript engine on July 30, 2024. Google responded swiftly, releasing an emergency patch after confirming active exploitation in the wild.

September 2024

Multiple vulnerabilities were discovered in Google Chrome, the most severe of which could allow arbitrary code execution. Exploitation of these vulnerabilities could allow an attacker to install programs, view or change data or create new accounts with full user rights. CVE-2024-7971, primarily impacting Google Chrome versions prior to 128.0.6613.84, was followed by CVE-2024-7965, another critical flaw in Chrome's V8 JavaScript engine. Both vulnerabilities were actively exploited, prompting urgent patches. Both were also added to the CISA's Known Exploited Vulnerabilities catalog, with patches strongly urged for deployment by mid-September 2024. CVE-2024-7971 was rated as a high-severity flaw with a Common Vulnerability Scoring System (CVSS) score of 8.8.

October 2024

Google released Chrome 130, addressing two vulnerabilities. CVE-2024-10487, a critical out-of-bounds write issue in Dawn, the WebGPU standard, was reported by Apple's Security Engineering and Architecture team just a week before the release. Although the potential exploitation of this issue has not been disclosed, out-of-bounds write vulnerabilities generally lead to arbitrary code execution. The second patched vulnerability was CVE-2024-10488, a high-severity use-after-free issue in WebRTC.

November 2024

Google confirmed the discovery of 12 security issues affecting all users of the Chrome web browser, including vulnerabilities that could lead to remote code execution and security feature bypass.

December 2024

Google confirmed the discovery of four high-severity vulnerabilities in the Chrome browser, which were patched in an update. The vulnerabilities, for which the researchers received $75,000 in hacker bounties, included:

- **CVE-2024-12692:** A type confusion vulnerability in the V8 JavaScript rendering engine.
- **CVE-2024-12693:** An out-of-bounds memory access in the V8 JavaScript rendering engine.
- **CVE-2024-12694:** A use-after-free vulnerability in the Chrome browser compositing function.
- **CVE-2024-12695:** An out-of-bounds write vulnerability in the V8 JavaScript rendering engine.

These vulnerabilities further emphasize the need for proactive patching and the importance of maintaining up-to-date software in the face of growing cyberthreats. The constant discovery and patching of zero-day flaws and critical vulnerabilities indicate that Chrome, like many other widely used software platforms, is a prime target for cybercriminals and nation-state actors alike.

Recommendations

Given the severity of these vulnerabilities, it is imperative for users and administrators to:

- **Apply security updates promptly:** Regularly check for and install security updates from Microsoft, Adobe and Google to protect against known vulnerabilities.
- **Monitor bulletins:** Stay informed by subscribing to security bulletins from these vendors to receive timely information on new vulnerabilities and patches.
- **Implement robust security practices:** Employ comprehensive security measures, including firewalls, intrusion detection systems and regular security assessments, to mitigate potential threats.

Conclusion

The consistent discovery and remediation of these vulnerabilities highlight the importance of regular system updates and the need for organizations to maintain robust patch management practices to mitigate potential security risks.

The presence of zero-day vulnerabilities, particularly those exploited in the wild, underscores the necessity for organizations to adopt a proactive security posture, including the implementation of advanced threat detection and response strategies.

4

Predictions for 2025

Ransomware will continue to dominate

Ransomware is projected to grow in both volume and sophistication, with cybercriminals increasingly using AI to automate and scale their attacks. By 2025, new ransomware variants might not only encrypt data, but also target cloud backups, making recovery nearly impossible without strong defenses in place. The 2021 Colonial Pipeline attack, which led to widespread fuel shortages, exemplifies the growing impact of such cyberattacks on critical infrastructure. As businesses continue migrating operations to the cloud, these environments will become prime targets for ransomware.

Double extortion, in which attackers demand a ransom to both decrypt files and prevent the release of sensitive data, will also gain traction. Organizations will need to invest in tools like EDR for continuous monitoring and fast incident response, along with cyber resilience strategies to ensure swift recovery after an attack.

Key investment areas in cybersecurity

In 2025, organizations will prioritize investments in XDR and EDR to protect against more advanced cyberthreats. XDR will help consolidate threat detection across endpoints, networks and servers, providing a unified view of security events. These tools will be essential for detecting emerging threats like AI-driven spear-fishing and automated ransomware attacks.

The rapid adoption of cloud platforms like AWS and Microsoft Azure will also push businesses to focus on cloud security. Misconfigurations in cloud services, such as in the 2019 Capital One breach, will continue to pose significant risks. And cloud-native security solutions will become essential for monitoring and safeguarding workloads.

Zero trust architecture (ZTA) will be increasingly implemented to prevent unauthorized access, and adopting Identity and Access Management (IAM) systems

will be crucial to ensuring that no user or device is trusted by default — even within the network.

Cloud security infrastructure and IoT

A major vulnerability in 2025 will be cloud infrastructure security. Misconfigurations or weak password practices can expose sensitive data, as demonstrated by various breaches in which databases were accidentally left open to the public. To mitigate these risks, businesses will need to adopt automated configuration management and encryption-by-default policies.

Another critical security gap will be internet of things (IoT) security. The exponential growth of IoT devices, ranging from smart home gadgets to medical equipment, will introduce numerous new attack surfaces. Organizations will need to secure IoT devices through regular firmware updates, proper segmentation and strong access controls.

Insider threats will remain a significant risk. Both malicious and accidental breaches from employees or contractors can lead to data leaks. Businesses will need to implement role-based access controls (RBAC) and use anomaly detection tools to detect and respond to suspicious behavior.

AI's role in cyberattacks and defenses

AI will have a profound impact on both cyberattacks and defenses by 2025. On the offensive side, cybercriminals will leverage AI to automate brute-force attacks, phishing schemes and vulnerability scanning. AI will also make it easier for attackers to create realistic deepfakes — AI-generated videos or voices that impersonate trusted individuals, such as CEOs, to trick victims into transferring funds.

The rise of LLMs like GPT will increase the risk of adversarial attacks, in which attackers manipulate the model's output for malicious purposes. Attackers might also exploit vulnerabilities in LLMs' training data, leading to backdoor attacks that can skew results for biased or harmful outcomes.

Additionally, embedding extraction attacks could target AI systems to recover sensitive information, such as credit card details or intellectual property, stored within the embeddings used by LLMs. Protecting this data will be vital, especially in industries with sensitive or regulated information like health care, finance and legal services.

On the defensive side, AI will enhance threat detection by analyzing vast amounts of data to identify attack patterns in real time. Machine learning algorithms will help predict and respond to evolving threats, adapting to new tactics and malware variants. Automated incident response — in which AI systems autonomously block or isolate compromised systems — will become a standard defense mechanism.

Nation-state-sponsored attacks in geopolitical conflicts

With rising global tensions, nation-state-sponsored cyberattacks are expected to increase in 2025. Conflicts in regions like Eastern Europe, the Middle East and the Indo-Pacific will see cyber tools used to disrupt economic and political stability. Smaller targets, particularly MSPs, will become prime vectors for attacks aimed at broader geopolitical objectives.

MSPs, which serve small and medium-sized businesses (SMBs), are especially vulnerable due to their critical role in supporting sectors like health care, finance and energy. Cyberattacks on MSPs could provide attackers with access to multiple clients at once, amplifying the scope of

the attack. In 2025, MSPs could be used as launch points for broader intrusions into national infrastructure.

State-sponsored attackers will increasingly focus on asymmetric warfare tactics, including disinformation, espionage and sabotage. Cyberattacks on critical infrastructure, like energy grids or water treatment facilities, could destabilize regions without resorting to military intervention.

Challenges faced by MSPs

In 2025, MSPs will face significant challenges in securing complex IT environments. With businesses adopting hybrid cloud models and integrating IoT devices, MSPs will need to manage security across diverse infrastructures. Protecting clients from supply chain attacks, in which attackers infiltrate networks through compromised third-party vendors, will remain a top concern. The SolarWinds breach in 2020 highlighted the devastating consequences of these attacks.

Compliance with data protection regulations like GDPR (General Data Protect Regulation), HIPAA (Healthcare Insurance Portability and Accountability Act), and CCPA (California Consumer Privacy Act) will also be a growing concern for MSPs, as stricter privacy laws emerge globally. MSPs will be under increasing pressure to ensure their clients' data is handled securely and in compliance with these laws.

The cybersecurity talent shortage will also continue to be a challenge, with many MSPs struggling to hire skilled professionals. By 2025, MSPs will increasingly rely on AI-driven tools to automate routine security tasks, allowing staff to focus on more complex incident response. Ongoing security training will be essential to bridge this talent gap.

Emerging trends in cybersecurity

As quantum computing continues to develop, businesses will face a new challenge in safeguarding data from attacks that could break current encryption methods. Quantum computers can perform calculations exponentially faster than classical computers, threatening the security of widely used algorithms like RSA. By 2025, businesses will need to explore quantum-resistant cryptography to protect sensitive information.

Another key trend is the rise of AI-powered malware. Just as AI helps defenders detect attacks, cybercriminals will develop AI-driven malware that can evade detection and adapt to changing defenses. These polymorphic threats can alter their code dynamically, making them harder to identify with traditional antivirus software.

With ARM architecture gaining popularity in consumer devices and servers, the emergence of ARM-specific malware is a growing concern. As ARM-based devices, like those from Apple and Microsoft, become more common, attackers may target vulnerabilities unique to ARM processors, especially within the Windows on ARM ecosystem. Additionally, cross-platform malware could spread across ARM and x86 architectures, broadening the attack surface.

In conclusion, businesses in 2025 must prepare for more sophisticated threats fueled by ransomware, AI and quantum computing. Investing in advanced cybersecurity solutions like EDR, XDR and cloud security will be crucial. MSPs will play a pivotal role in securing diverse IT environments, but will face challenges related to supply chain security, talent shortages and regulatory compliance.

5

Acronis recommendations to stay safe in the current and future threat environment

Modern cyberattacks, data leaks and ransomware outbreaks all reveal the same thing: The current approach to cybersecurity is failing, and failure is the result of weak technologies, heightened complexity and human mistakes caused by clever social engineering tactics.

Backup is essential when cybersecurity solutions fail. At the same time, if backup solutions are compromised or disabled, or if they perform slowly, a business could experience significant financial losses due to downtime. Even if backup solutions are working well and remain uncompromised in an attack, it could take hours or days to restore systems and data to an operational state.

To solve these problems, we recommend an integrated cyber protection solution that combines XDR, EDR, anti-malware, DLP, email security, vulnerability assessments, patch management, RMM and backup capabilities in a single agent. This integration lets you maintain optimal performance, eliminate compatibility issues and ensure rapid recovery; this way, if a threat is missed or detected while your data is being altered, the data will be restored from a backup immediately. And because everything runs through a single agent, the solution knows when data is lost and needs to be restored.

This functionality isn't possible when you use separate anti-malware and backup products, each with its own agent. Your anti-malware solution may stop the threat, but some data may already be lost. The backup agent won't know about this automatically and data will be restored slowly — if at all.

Acronis Cyber Protect Cloud makes data recovery unnecessary by detecting and eliminating threats before they can damage your environment. This is achieved with our enhanced, multilayered cybersecurity functionality.

Acronis XDR brings the visibility needed to understand attacks, while simplifying the context for administrators and enabling efficient remediation of any threats. No matter what cybersecurity solutions you have in place, always follow basic security rules and critical procedures.

Keep passwords and working spaces private

Ensure that your (and your employees') passwords are strong and private. Never share passwords with anyone, and use long, unique passwords for every service.

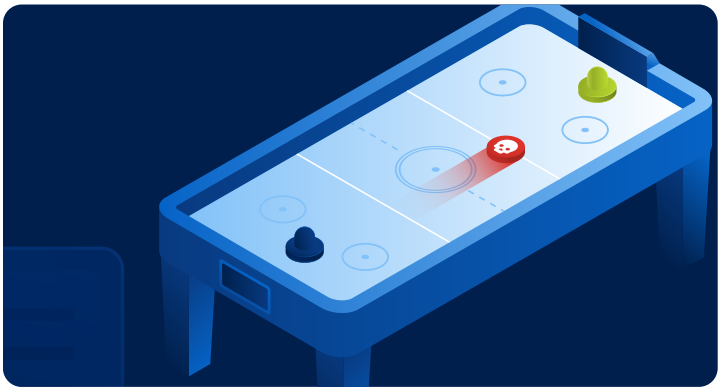
To help you remember them, use password manager software. Alternately, the easiest way to construct strong passwords is to create a set of long phrases that you can remember. Eight-character passwords are easily brute forced. Where possible, use MFA.

Even when working from home, you should lock your laptop or desktop and limit access to it. There are many cases when people could steal sensitive information from an unlocked PC.

Patch your OS and apps

Many attacks succeed due to unpatched vulnerabilities, but staying up to date with the latest vulnerabiltiies and patching them in a timely manner is challenging. Ensure that Windows receives all necessary updates and that updates are installed promptly — users tend to ignore system messages, especially when an operating system encourages a restart. In addition, ensure that auto-updates are enabled for popular software vendors like Adobe and that apps like PDF Reader are also updated promptly.

Acronis Cyber Protect Cloud features embedded vulnerability assessment and patch management functionalities. Acronis tracks all discovered vulnerabilities and the fixes that have been released to address them, allowing admins or technicians to easily patch all endpoints with flexible configuration and detailed reporting. Acronis Cyber Protect Cloud supports not only all embedded Windows apps, but also 300 popular third-



party apps, including telecommunications tools like Zoom and Slack, and popular VPN clients used in remote work. Patch high-severity vulnerabilities first and follow the success report to check that patches were applied properly.

Prepare for phishing attempts, and don't click suspicious links

New phishing messages and malicious websites appear in large numbers every day. They are often filtered out at the browser level, but cyber protection solutions like Acronis Cyber Protect Cloud offer additional dedicated URL filtering functionality. Remember that malicious links can come from anywhere: instant messenger apps, email, forum posts, etc. Don't click links you don't need to click or that you didn't expect to receive.

Ensure your cybersecurity solution is properly configured

Acronis Cyber Protect Cloud uses many well-balanced and tuned security technologies, including several detection engines. We recommend using it instead of an embedded Windows solution.

But just having anti-malware defenses in place is not enough; they must be configured properly:

- A full scan should be performed daily at minimum.
- A product should get updates daily or hourly, depending on how often updates are available.
- A product should be connected to its cloud detection mechanisms. With Acronis Cyber Protect Cloud, this is enabled by default, but you need to ensure that internet access remains available and isn't accidentally blocked by anti-malware software.
- On-demand and on-access (real-time) scans should be enabled and react on every new software installed or executed.

Additionally, don't ignore messages coming from your anti-malware solution — read them carefully, and ensure that the license is legitimate if you're using a paid version from a security vendor.

Control the risks related to AI usage

To ensure safe and responsible use of these technologies, businesses must implement clear policies governing AI usage. Establishing guidelines on how AI tools should be used and restricting the upload of sensitive or proprietary data to external AI platforms, are critical first steps. Alongside these policies, organizations must adopt AI-specific security measures, such as monitoring tools to detect unauthorized access and using endpoint security solutions to prevent the misuse of generative AI tools.

Data privacy compliance is another crucial aspect. Businesses must adhere to regulations like GDPR, CCPA or India's Digital Personal Data Protection (DPDP) Act (2023) by employing encryption and access controls to safeguard sensitive data when interacting with AI systems. Cybersecurity teams should also be educated about AI vulnerabilities, including adversarial attacks that target machine learning systems.

Monitoring and analyzing AI activity is crucial for maintaining security. Organizations should continuously track their AI systems for unusual behavior, such as unauthorized outputs or data exfiltration. Logging and auditing interactions with AI tools can help identify potential misuse.

As AI becomes increasingly integrated into business operations, it offers transformative benefits but also introduces new risks. Generative AI, while powerful, can be exploited for malicious purposes, such as generating phishing emails and deepfakes or exploiting vulnerabilities in systems. By implementing robust policies, enhancing security measures and fostering employee awareness, businesses can mitigate risks while leveraging AI's potential responsibly. Proactive systems monitoring and adherence to regulatory standards will ensure AI enhances rather than compromises

Acronis

Acronis Threat Research Unit

Learn more at
acronis.com