Acronis

Report
H1 2024

Acronis Cyberthreats Report, H1 2024:

Email attacks surge 293%, new ransomware groups emerge

Acronis Threat Research Unit

Table of contents

Authors:

Alexander Ivanyuk
Senior Director, Technology

Candid Wuest
VP of Product Management

Irina Artioli
Cyber Protection Evangelist

Introduction and summary

The biannual Acronis Cyberthreats Report covers the global threat landscape, as encountered by Acronis sensors and analysts in the first half of 2024. General malware data presented in the report is gathered from January – May of 2024 and reflects threats targeting endpoints we observed in this time frame.

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

Key findings:

- The most targeted countries for malware attacks in Q1 2024 were Bahrain, Egypt and South Korea.
- Nearly 28 million URLs were blocked at the endpoint by Acronis in Q1 2024, a 3% increase over Q4 2023.
- 27.6 % of all received emails were spam — 1.5% contained malware or phishing links.
- Each malware sample lives an average of 2.3 days in the wild before it disappears — 82% of samples were only seen once.
- There were 1,048 publicly reported ransomware cases in Q1 2024, a 23% increase over Q1 2023.
- Three highly active groups were the primary contributors to ransomware attacks, collectively responsible for about 35% of the attacks.
- LockBit accounted for 20% of ransomware attacks, followed by BlackBasta and Play with 7.1% and 7.0% respectively.

Top cybersecurity trends in the first half of 2024:

- Ransomware continues to be a major threat to small and medium-sized businesses, including government, health care and other critical organizations. Recently, ransomware makers have abused vulnerable drivers to get a foothold in systems and disable security tools.
- More IT companies are being compromised, threatening the overall cybersecurity industry.
- AI is a commonly used tool in cyberattacks, but it has not assumed the full cyberattack kill chain.
- In the first quarter of 2024, Powershell T1059.001 was the most frequently detected MITRE technique.
- The number of email attacks detected in H1 2024 surged by 293% compared to the first half of 2023.

What you will find in this report:

- The top security / threat trends Acronis observed in H1 2024.
- The dangers of AI development.
- An overview of the role of vulnerabilities in data breaches.
- General malware statistics, with a deep-dive analysis of the most dangerous threats.
- Ransomware statistics and key families analyzed.
- The top vulnerabilities that contributed to the success of attacks.
- Acronis security recommendations.

1 Key cyberthreats and trends in H1 2024

1. Ransomware gangs continue to wreak havoc

Looking back at H1 2024, the following ransomware gangs were the most active in terms of total numbers of victims:

LockBit (413) **Play (135)** **8Base (115)** **BlackBasta (113)** **Hunters International (100)**

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

In February 2024, a significant milestone was achieved in the battle against cybercrime: The infamous LockBit ransomware gang was taken down (at least partially). This criminal organization had been a thorn in the side of businesses and governments worldwide, perpetrating some of the most disruptive and costly cyberattacks in recent history.

Operation Cronos, led by the U.K.'s National Crime Agency (NCA) with support from Europol, Eurojust and global law enforcement agencies, disrupted LockBit ransomware gang operations. The task force seized control of 34 servers that comprised LockBit's primary infrastructure, as well as 14,000 accounts used for hosting tools and storing stolen data. Additionally, authorities confiscated 200 cryptocurrency wallets and 1,000 decryption keys, which were instrumental in developing a publicly available decryptor tool.

The months-long operation resulted in the compromise of LockBit's primary platform and critical infrastructure, leading to the takedown of 34 servers in multiple countries, including the Netherlands, Germany, Finland, France, Switzerland, Australia, the United States and the United Kingdom. But just weeks later, LockBit became active again, despite the arrests of several LockBit members.

Another big player, the BlackCat ransomware group, also known as ALPHV, vanished in March after what appears to have been an exit scam following a substantial $22 million payout. The initial signs of the exit scam emerged when BlackCat's darknet website displayed a banner claiming it had been seized by law enforcement. This was quickly debunked by cybersecurity experts who noted inconsistencies in the source code of the seizure notice, indicating it was a fraudulent claim designed to mislead affiliates and victims. The NCA confirmed they had no involvement in any operation against BlackCat at the time.

BlackCat's operators claimed on social media that they were "screwed over" by the authorities and hinted at selling their ransomware source code for $5 million. This move is typical of an exit scam in which cybercriminals attempt to cash out before completely disappearing. As we have seen before, BlackCat likely wanted to get off the radar after receiving a large ransomware payout and then reappear under another name.

U.S. / IT sector / INC Ransom

Attackers compromised the U.S. division of Xerox Business Solutions (XBS), potentially exposing a limited amount of personal information, according to a statement from the parent company Xerox Corporation, which reported a revenue of $7.06 billion in 2023. XBS specializes in document technology and services, offering products such as printers, copiers, digital printing systems and related consultation and supply services.

The INC Ransom ransomware gang claimed responsibility for the attack, adding Xerox Corporation to its extortion portal, asserting the theft of sensitive data and confidential documents. Although the attack allegedly had no impact on Xerox or XBS operations, a preliminary investigation suggests some personal information was exposed. Data samples on the INC Ransom data leak site include email communications, payment details, invoices, filled-out request forms and purchase orders.

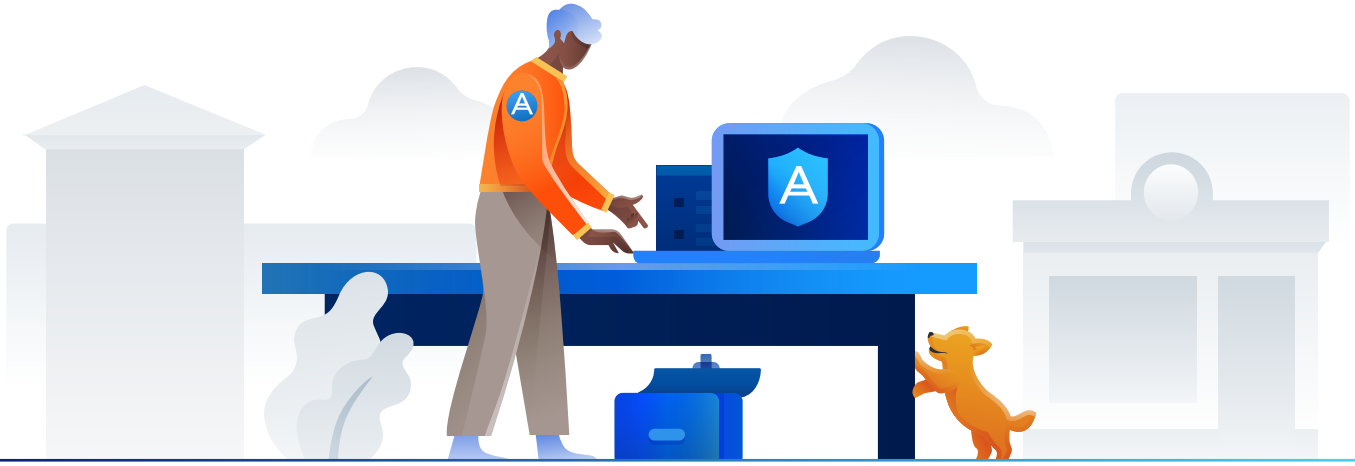
U.S. / Transportation / Medusa

The Kansas City Area Transportation Authority (KCATA) fell victim to a ransomware attack that affected its public transit operations in metropolitan Kansas City. KCATA is responsible for the Metro Area Express (MAX) bus rapid transit service and 78 local bus routes across seven counties. The company promptly disclosed the attack, initiating an investigation and notifying relevant authorities, while external experts were engaged to restore impacted systems.

Despite the ransomware incident, KCATA said that its services, including fixed-route buses and paratransit services, remain unaffected, except for the temporary disruption of calls to regional RideKC call centers. The Medusa ransomware gang has claimed responsibility for the attack, and threatened to release stolen data unless a $2 million ransom was paid, with an option to extend the deadline for $100,000 per day.

U.K. / Utilities / BlackBasta

The BlackBasta ransomware group announced it attacked Southern Water, a major U.K. water utility, and threatened to release 750 gigabytes of stolen data, including personal and corporate documents. Southern Water employs over 6,000 people, with an annual turnover exceeding €1.2 billion and delivers water and wastewater services for East Kent, parts of Sussex, Hampshire and the Isle of Wight.



Germany / Automotive / BlackBasta

Car maker Hyundai Motor Europe, a Germany-based division of Hyundai Motor Company, was hit by a BlackBasta ransomware attack, with attackers claiming to have obtained 3 TB of corporate data. Initially, the Hyundai Motor Group attributed the issues to routine IT problems. Upon further investigation and disclosure of additional information regarding the data theft, Hyundai confirmed the cyberattack. The company acknowledged unauthorized access to a portion of its network, with collaboration from external cybersecurity experts and legal authorities.

France / Energy / Cactus

Schneider Electric, a major player in energy management and automation, fell victim to a Cactus ransomware attack that resulted in the theft of corporate data. Schneider Electric employs over 150,000 people worldwide. The attack targeted the Sustainability Business division, causing disruptions to Schneider Electric's Resource Advisor cloud platform.

Reports suggest terabytes of corporate data were pilfered during the attack, with Cactus demanding payment to refrain from leaking the stolen data. The Sustainability Business division advises enterprise clients on renewable energy solutions and aids them in navigating climate regulatory frameworks globally. Notable clients potentially affected by the breach include Allegiant Travel Company, Clorox, DHL, DuPont, Hilton, Lexmark, PepsiCo and Walmart.

Italy, Belgium / Manufacturing / 8Base

The 8Base ransomware group hit several companies in Belgium and Italy in H1 2024. Victims included Sprimoglass, with an annual revenue of $86.2 million, and Federchimica (Italian Federation of the chemical industry), which encompasses 1,450 companies with approximately 94,000 employees. According to 8Base, the stolen data included invoices, receipts, accounting documents, personal data, certificates, employment contracts, confidentiality agreements, personal files and more.

Despite the lack of details on the breach methods, it's evident that 8Base strategically targets smaller enterprises to evade law enforcement's attention. Consequently, victims often face the dilemma of whether to pay the ransom to resume operations swiftly or confront significant financial consequences.

U.S. / Health care / BlackCat

The UnitedHealth Group CEO confirmed the payment of a $22 million ransom to attackers who breached its subsidiary, Change Healthcare, which provides payment and revenue management solutions and which merged with UnitedHealth's Optum unit in 2022.

The breach caused significant disruptions across the health care sector and left many doctors temporarily unable to fill prescriptions or receive payments for their services. BlackCat ransomware group claimed responsibility for the attack, which succeeded due to a server lacking multifactor authentication.

U.S. / Government / LockBit

The LockBit ransomware group claimed responsibility for disrupting the City of Wichita's IT systems, including online bill payment, prompting authorities to shut down affected services. Wichita, Kansas is home to nearly 400,000 people and is a key economic center. The city was added to the LockBit ransomware group's extortion portal, with the group threatening to publish stolen files if the ransom wasn't paid. Reportedly, city investigations are still ongoing to determine if data was stolen, but LockBit's usual tactics include stealing data prior to file encryption.

France / Health care/ LockBit

Hôpital de Cannes - Simone Veil (CHC-SV) in France faced severe operational disruption in April 2024 due to a cyberattack, prompting the hospital to halt nonemergency procedures and appointments and take all computers offline. Subsequently, the hospital received a ransom demand from the LockBit 3.0 ransomware gang. The hospital refused to pay the ransom and instead forwarded the demand to law enforcement. LockBit threatened to leak stolen files on the dark web, but the hospital asserted that they would not yield to the ransom demand and promised to notify affected individuals if data leakage occurred. In May 2024, the hospital confirmed that leaked data published on LockBit's website indeed belonged to Simone Veil.

Situated along the French Riviera, the 869-bed hospital caters to approximately 150,000 outpatients, accommodates 50,000 emergency room visits, conducts 9,000 surgeries, and oversees 1,500 births annually, with a workforce of over 2,000 doctors and staff members.

Australia / Real estate / BlackSuit

Australian property valuation specialist Herron Todd White reportedly lost over 300 gigabytes of data to the BlackSuit ransomware gang. As a result, major banks in Australia suspended all new work with Herron Todd White. The prolific BlackSuit gang claimed responsibility for the attack, posting details of the data exfiltrated to its darknet leak site. While BlackSuit did not disclose specific ransom demands or deadlines, they indicated possession of substantial data, including paperwork and customer databases. The attack has prompted concern among employees and ex-employees of the company. Herron Todd White has an extensive presence across Australia, claiming its network covers 95% of the population. After reporting the attack, the company assured clients it was resolving the issue, but declined further comment on the incident.

Netherlands / High tech / Dark Angels

Dutch chipmaker Nexperia confirmed a network breach in March 2024 after a ransomware gang leaked samples of allegedly stolen data. Nexperia,

a subsidiary of Chinese company Wingtech Technology, operates semiconductor fabrication plants in Germany and the U.K., producing various electronic components. The company stated that it promptly shut down affected IT systems, launched investigations with third-party experts, and reported the incident to authorities.

Dunghill Leak, linked to the Dark Angels ransomware gang, claimed responsibility for the attack, threatening to leak 1 TB of confidential data if a ransom wasn't paid, including design, engineering, commercial and client data. The Dunghill Leak site is known for pressuring attacked organizations into paying ransoms by threatening to publish stolen data, similar to previous incidents involving the Dark Angels group.

Japan / Manufacturing / Hunters International

In April, the Hunters International ransomware operation hit Hoya Corporation and demanded a $10 million ransom to decrypt files and refrain from releasing stolen data. Hoya, a Japanese company with a revenue of $5.609 billion in 2023, specializes in optical instruments, medical equipment, and electronic components, and operates globally with 160 offices and subsidiaries in over 30 countries and 43 laboratories.

The attack disrupted production and order processing across several business divisions, leading to IT outages. The ransomware group demanded a ransom to prevent the release of an alleged 1.7 million stolen files totaling 2 TB. Despite no files surfacing on the Hunters International site and no public claim of responsibility, evidence suggests ransom negotiations, with a strict "No Negotiation / No Discount Policy" was imposed by the attackers.

Italy / Fashion / Hunters International

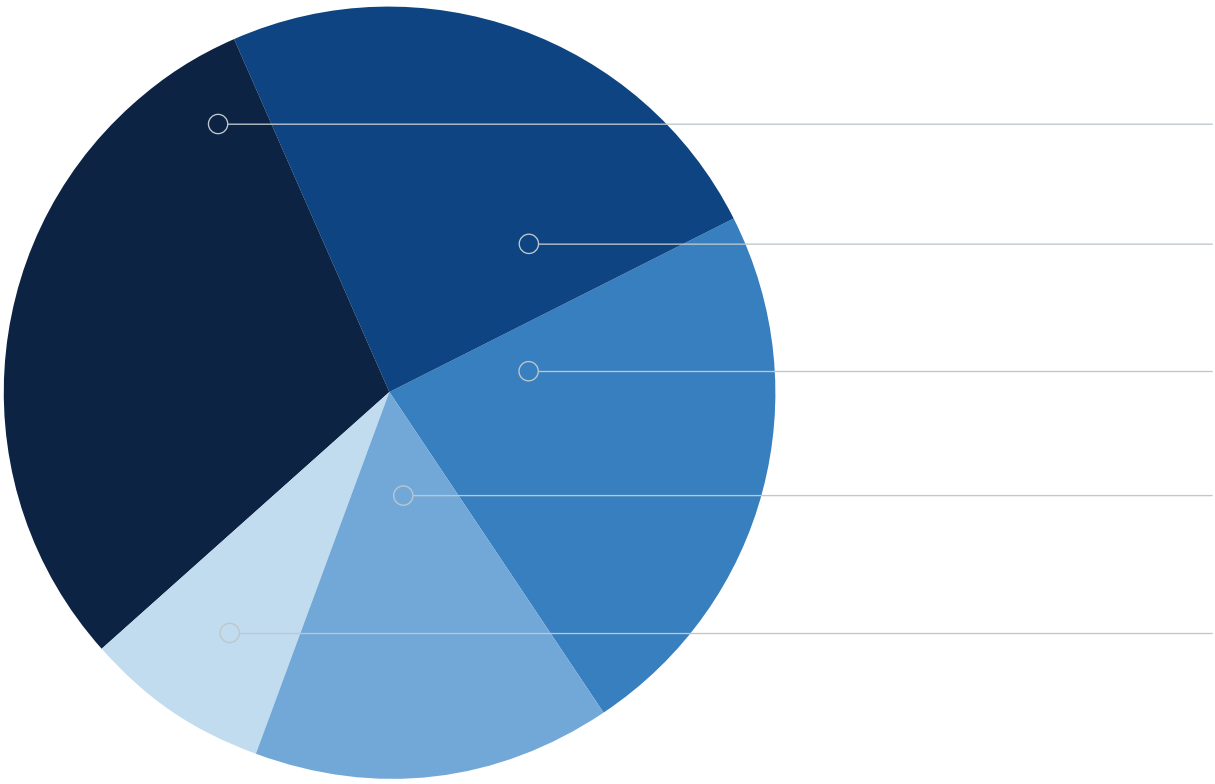
Also in April, Hunters International ransomware group added Benetton Group to its data leak site. A renowned global fashion company headquartered in Italy, Benetton Group had annual revenue of over €1 billion in 2023. Hunters International threatened to disclose 33.8 MB of clients' data if ransom demands were not met within a specified time frame.

There were hundreds of other ransomware cases in H1 2024, which continue to demonstrate a few key security issues:

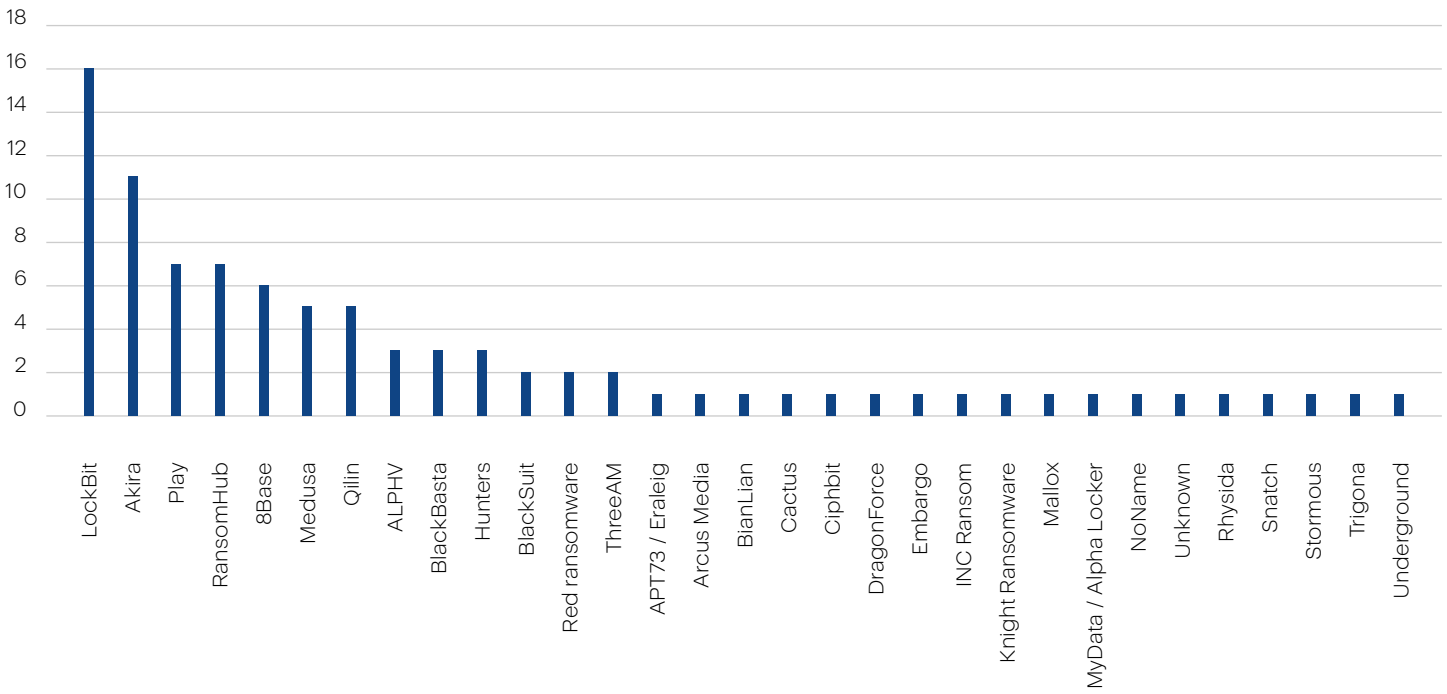
- There is often a lack of strong security solutions in place that are able to detect the exploitation of zero-day vulnerabilities. With behavior-based detection and exploit prevention technology — which are a part of the Acronis Cyber Protect security stack — it's possible to prevent most of these attacks.
- Delayed patching remains an issue. Organizations are failing to update vulnerable software in a timely manner after a fix becomes available.
- Attackers often manage to gain domain administrative rights and then uninstall security tools.
- Proper data backup following the 3-2-1 backup rule is a must for all organizations. Immutable backup space can often be the last line of defense.

MSPs under attack

Attack vector	Number of attacks
Phishing	27
RDP	22
Unpatched vulnerabilities	21
Abuse of valid accounts / credentials	13
Trusted relationship	7



Ransomware groups



Attacks on MSPs now occur on regular basis. Here are three notable cases from H1 2024:

1. Tietoevry ransomware attack

In January 2024, Finnish IT and cloud services provider Tietoevry suffered a ransomware attack targeting one of its data centers in Sweden, disrupting Swedish government agencies, universities and businesses. The Akira ransomware group was identified as the culprit, notably affecting Primula, a payroll and HR company used by many Swedish universities and government authorities. The company employs approximately 24,000 people worldwide and had a 2023 revenue of $3.1 billion. Tietoevry reported the incident to the police and acknowledged the severity of the attack, which was part of a broader pattern of Akira's activities in Finland since June 2023.

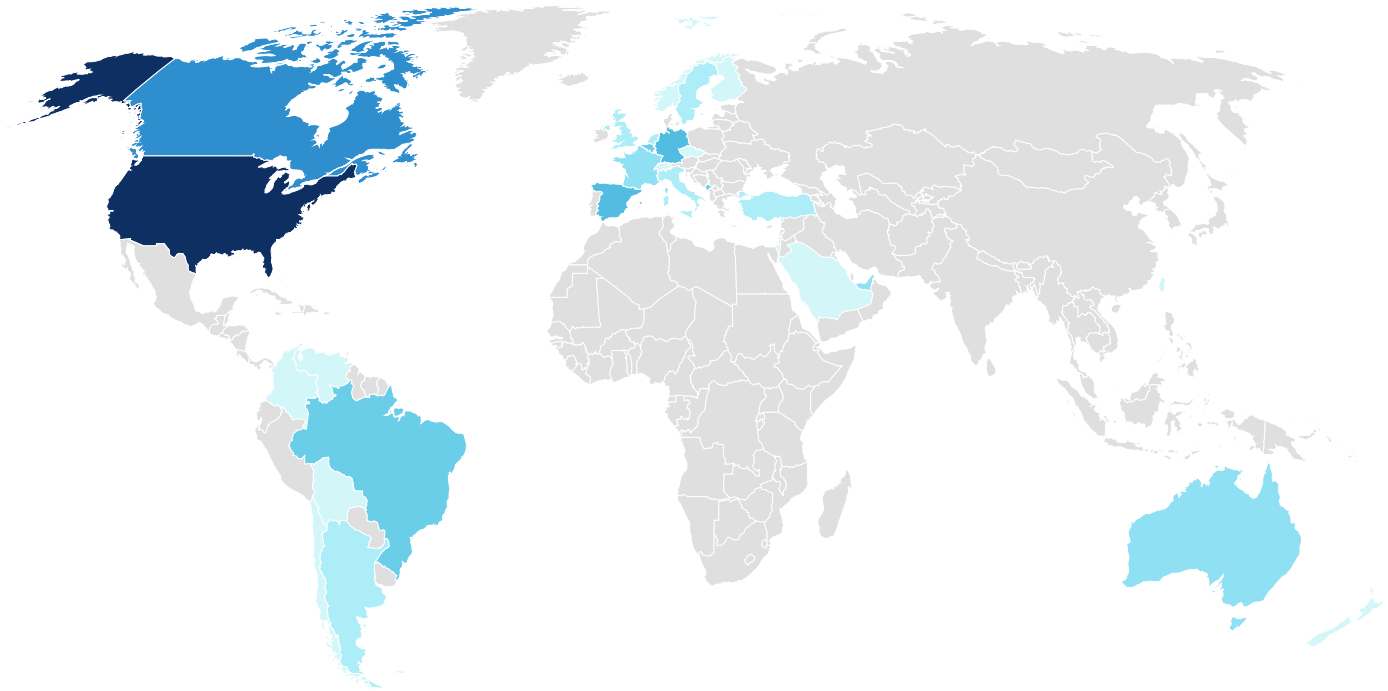
2. Seven Seas Technologies

In April 2024, UAE-based Seven Seas Technologies reportedly fell victim to a ransomware attack by Rhysida, which demanded 6 BTC (approximately $400,000). The ransomware group posted the IT services provider on its leak site, along with screenshots of passports, maintenance contracts, and other confidential information, including PII documents, and has already published a sample of the exfiltrated data. Seven Seas Technologies has not confirmed Rhysida's claims, and further details about the attack are limited.

3. Scanda

In May, Scanda, a Mexican IT consulting and security solutions provider with 25 years of experience, was hit by LockBit. The company, which generates $23.6 million in annual revenue, had 387 GB of data exfiltrated, including personal identification information, corporate documents, legal information, financial data, payroll, employee personal data, correspondence, customer information, contracts and database backups.

Most targeted countries for attacks on MSPs



How MSPs are attacked

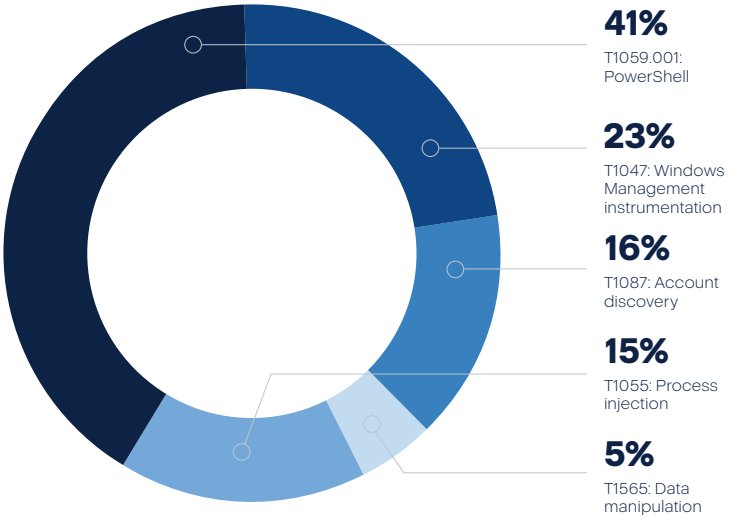
To breach MSP defenses, threat actors employ the tactics and techniques we see in most successful cyberattacks:

- **Phishing and social engineering**: These deceptive tactics trick MSP employees into divulging sensitive information or executing malicious actions, facilitating unauthorized access and data breaches.
- **Vulnerability exploits**: Cybercriminals exploit weaknesses in software, operating systems and network infrastructure to gain initial access to MSP networks, often leveraging known vulnerabilities with publicly available exploit code.
- **Credential compromise**: Attackers steal MSP credentials through various means, including phishing, credential stuffing, vulnerability exploits in remote access solutions, etc.
- **Supply chain attacks**: Threat actors infiltrate trusted software updates with malware, bypassing traditional security measures and gaining widespread access to client networks.

Most used MITRE techniques

The MITRE ATT&CK Framework categorizes adversary behavior into tactics and techniques. This helps malware analysts efficiently identify, assess and respond to threats. The collected information is based on Acronis telemetry from Acronis Cyber Protect Cloud Advanced Security + XDR from January 1 to March 31, 2024.

Top 5 most frequently seen MITRE ATT&CK techniques, Q1 2024



Recommended defense strategies for MSPs

To mitigate cyberthreats effectively, MSPs must adopt a comprehensive security strategy:

- **Security awareness training:** Educate MSP employees about cybersecurity best practices, including how to recognize and report phishing attempts, social engineering tactics and other suspicious activities.
- **Incident response planning:** Develop and regularly test an incident response plan to ensure MSPs can effectively detect, contain, mitigate and recover from security incidents to minimize disruption and damage.
- **Multifactor authentication (MFA):** Enforce MFA for all privileged accounts and critical systems to add an additional layer of security to prevent unauthorized access.
- **Network segmentation:** Segment MSP networks to contain and isolate potential security incidents to limit the lateral movement of attackers and reduce the impact of breaches.
- **Endpoint security with EDR / XDR:** Deploy advanced endpoint protection solutions with capabilities such as AI and behavioral analysis, threat intelligence integration and automated remediation to detect and mitigate malware infections.
- **Data encryption and data loss prevention:** Encrypt sensitive data both in transit and at rest, and deploy DLP solutions to monitor and prevent unauthorized data exfiltration to safeguard critical information from compromise.
- **Continuous monitoring and threat intelligence:** Utilize SIEM solutions to continuously monitor MSP networks for signs of compromise and integrate threat intelligence feeds to stay abreast of emerging threats and evolving attack techniques.
- **Patch management**: Implement robust patch management processes to promptly apply security updates and patches across all systems and software to reduce the risk of exploitation by known vulnerabilities.

Conclusion

In a landscape fraught with cyberthreats, MSPs must remain vigilant and proactive in defending against malicious actors seeking to compromise their systems and their clients' data. By adopting a multilayered security approach, fostering a culture of cybersecurity awareness and staying abreast of emerging threats and best practices, MSPs can strengthen their defenses and protect the digital assets entrusted to their care. Through collaboration, innovation and a steadfast commitment to cybersecurity, MSPs can continue to serve as trusted partners in safeguarding organizations against the ever-evolving threat landscape.

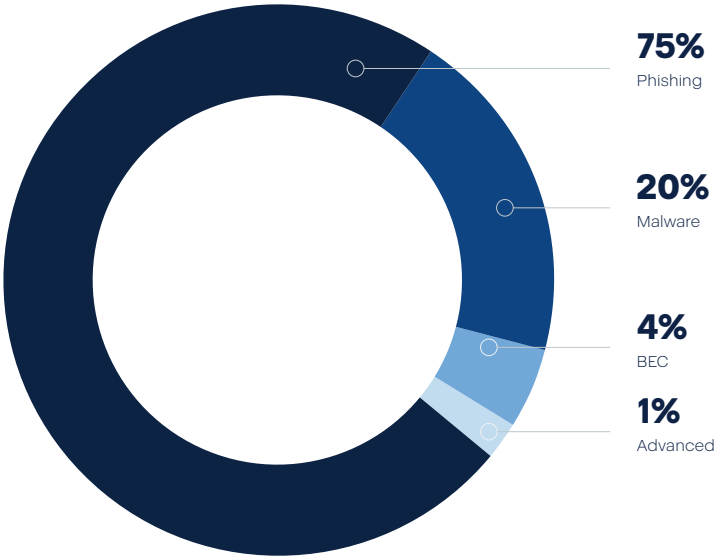
Phishing and malicious emails remain the main vector of infection

The following email and phishing statistics were aggregated from Acronis Cyber Protect Cloud with Advanced Email Security, which is powered by Perception Point. The data was gathered in the first half of 2024 and is combined with Acronis telemetry data for malware and URL blocks on the endpoints. Later in this report, you'll find a dedicated section highlighting a collection of malicious websites that have been blocked.

In the first half of 2024, organizations experienced a significant surge in email communications, with the number of emails per organization increasing by 25%. This rise in email volume has been paralleled by a concerning 47% increase in email attacks targeting these organizations. Alarmingly, 40% of users faced at least one attack.

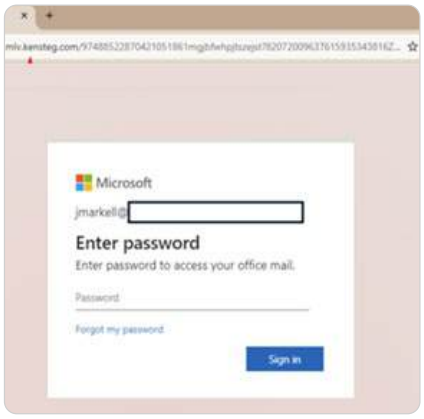
Among the attacks, 26% of users encountered phishing attempts through malicious URLs, demonstrating cybercriminals' continued reliance on what is still the #1 attack type. Additionally, 13% of users received malware via email, highlighting the diverse methods attackers employ to compromise systems and steal sensitive information. Finally, social engineering increased 5% since H1 2023, while malware attacks decreased from 11% in H1 2023 to 4% in H1 2024.

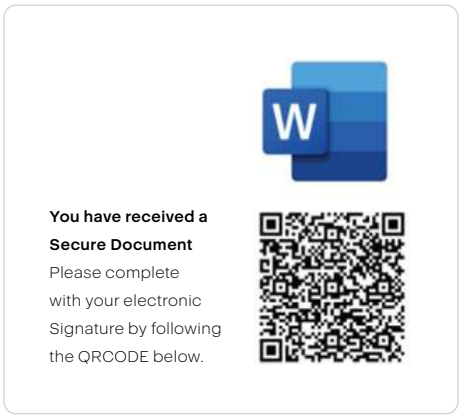
Currently, one in three emails is unsolicited. The spam rate has dropped to 27.6%, an improvement from 30.3% in the first half of 2023. Despite this reduction, the proportion of emails with malicious content has increased slightly to 1.5%, up from 1.3% in the same period last year. This underscores the persistent issue of email threats, even as spam control has improved.

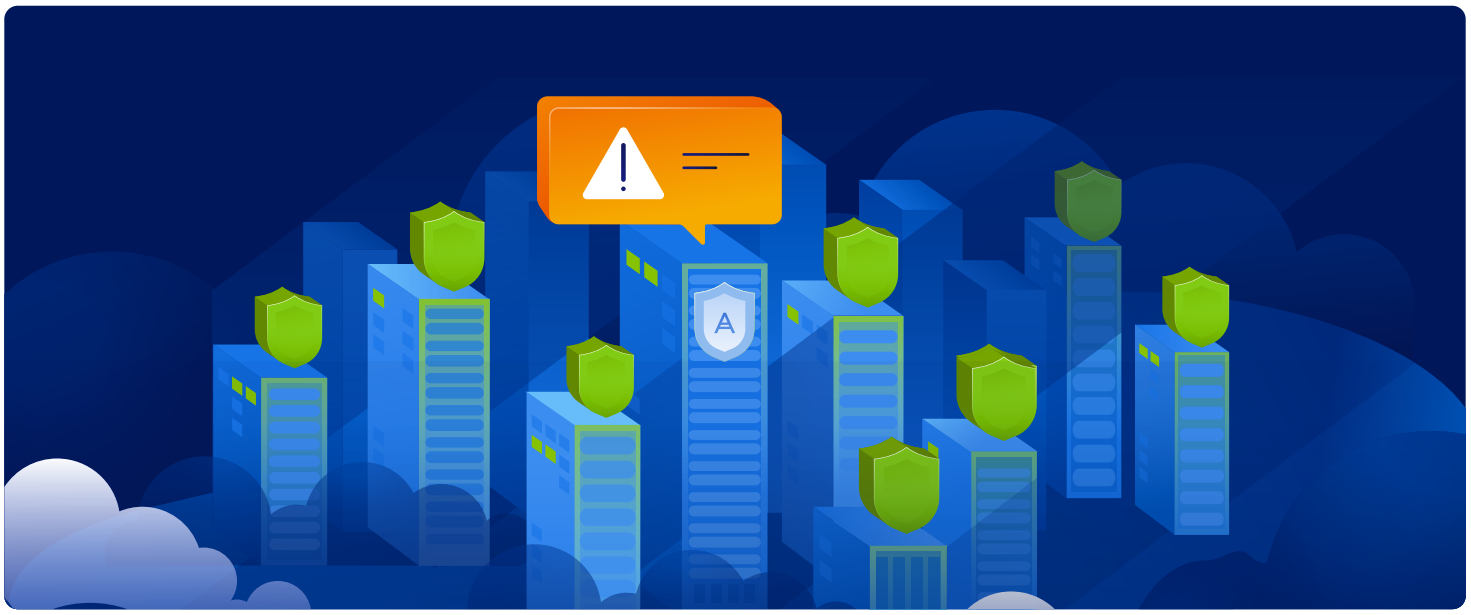


Phishing trends

An emerging cybersecurity trend is “login impersonation.” In this scheme, an attacker sends an email to a user with a file attached. The attacker’s display name is set to “Shared File Access,” making the email appear to be a fax-to-email communication. The attached PDF contains a QR code that the user is instructed to scan to access the document. However, scanning the QR code directs the user to a fake Microsoft login page designed to steal their credentials.

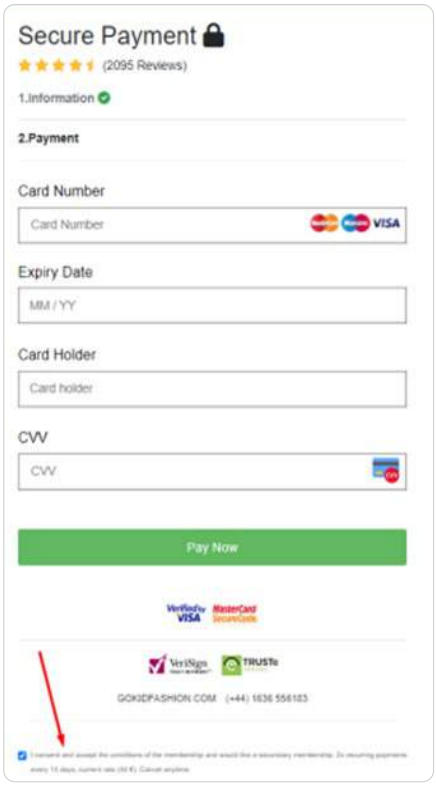




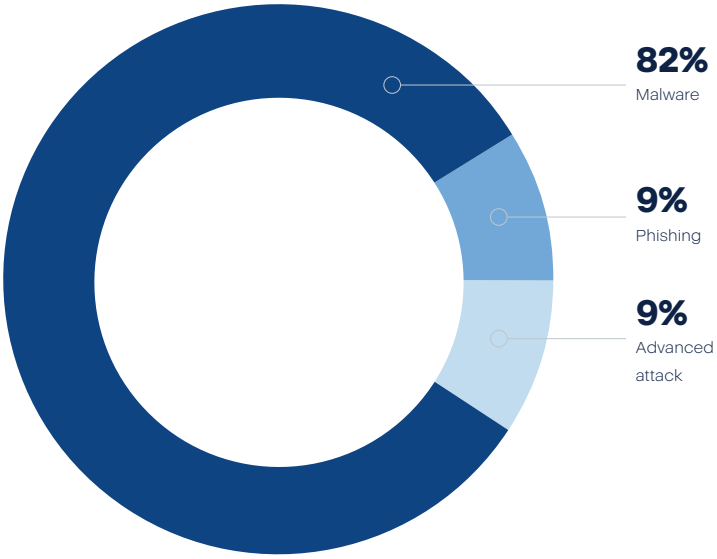


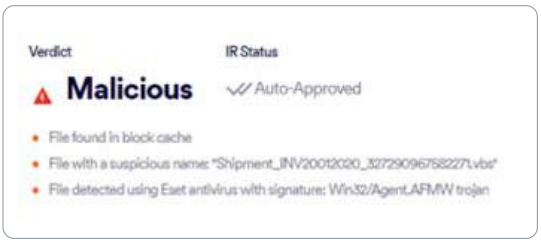
Soccer scam

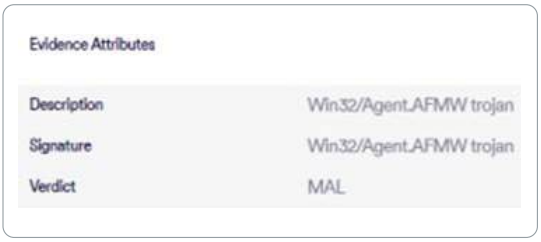
A new scam has emerged in which individuals receive an email allegedly from UEFA EURO claiming the user has been randomly selected as a soccer fan to win a UEFA EURO 2024 getaway. The email includes a list of winners, with the recipient's name cleverly added as the last winner on the list. The email urges the recipient to click a "Next" button to confirm their response. Clicking the button redirects the user to a landing page with trivia questions about EURO 2024, which, regardless of the user's answers, leads to a congratulatory message stating they can purchase a MacBook Pro for only €2.00. The user is then taken to a form requesting personal information, followed by a fraudulent payment page asking for credit card details. Submitting this information sends it directly to the attackers. Additionally, a preselected checkbox at the bottom of the page consents to terms that could result in contractual complications and significant financial losses.



Another growing trend is attacks within collaboration tools, where phishing and advanced attacks comprise nearly 20% of the attacks and 82% comprise malware-based attacks.







In the below described SharePoint attack, a .zip archive file was uploaded to SharePoint, which contained another .zip file inside. This layered compression suggests an attempt to obscure the file's contents and facilitate the transfer of potentially harmful files undetected. The second .zip file includes a .vbs file, which in turn contains a VBS script designed to execute a malicious payload within Windows or Internet Explorer. This payload deploys a trojan malware variant capable of various tasks, such as downloading, installing or running additional malware on the targeted device and functioning as a keylogger to collect sensitive data. The trojan is engineered to perform a range of malicious activities, including data theft and unauthorized installation and execution of further malware.

Vulnerabilities continue to be the key to data breaches

In the intricate dance between cybersecurity defenders and malicious actors, vulnerabilities serve as the linchpin. They are the chinks in the armor, the weaknesses waiting to be exploited. In the realm of data security, vulnerabilities play a pivotal role, often being the gateway through which data loss and ransomware attacks occur. Understanding their significance and the mechanisms by which they are exploited is paramount in fortifying our digital defenses.

One of the primary pathways through which vulnerabilities lead to data loss is via unauthorized access. When a vulnerability exists within a system or application, it creates an opportunity for attackers to bypass security measures and gain entry into networks or databases. Once inside, they can exfiltrate sensitive information,

ranging from PII to intellectual property, financial records and trade secrets. This data can then be used for various malicious purposes, including ransom extortion, identity theft, financial fraud or espionage.

During the first half of 2024, we saw on average 400 disclosed data breaches per month, so it is safe to say we are dealing with thousands of cases of data loss per year, ranging from large cases involving the data of billions of people to smaller cases, affecting medium-sized or small businesses.

Notable vulnerabilities registered in H1 2024 include:

- **CVE-2024-3094 (XZ):** A backdoor discovered in the XZ data compression utility package allowed attackers to insert malicious code into the source code, enabling them to send commands to infected servers.
- **CVE-2024-20656:** A Visual Studio vulnerability enabled attackers to elevate their privileges in the system by executing a DACL reset attack on Windows.
- **CVE-2024-1708:** A ScreenConnect vulnerability allowed attackers to gain administrator privileges in ScreenConnect's web application to exploit the server for malicious purposes.
- **CVE-2024-21412:** A Windows Defender vulnerability enabled attackers to bypass the SmartScreen Filter by tricking the system into believing that a file was already in the system at the time of launch.

- **CVE-2024-29059:** A Google Chrome browser vulnerability allowed attackers to execute arbitrary code on affected systems.

The above vulnerabilities correlate with what Acronis identified as the three most common entry points in H1 2024:

1. Vulnerable remote access services like Ivanti or ScreenConnect.

2. Vulnerable access control features like Windows SmartScreen.

3. Vulnerable office applications, particularly exploits for the Microsoft Office suite, which were surpassed by a WinRAR vulnerability in 2023.

Tech companies are being increasingly compromised

Among all the victims we observed in H1, IT and especially security vendors were highly targeted, along with MSPs.

Dropbox

In May 2024, Dropbox disclosed a security incident in which hackers gained unauthorized access to customer data and authentication secrets through its eSignature service, HelloSign. The breach occurred due to a third-party service vulnerability that allowed attackers to exploit an API flaw and access customer information. Although Dropbox did not specify the number of affected users, it confirmed that the breach impacted a subset of HelloSign users who had created accounts before December 14, 2023.

The compromised data included customer names, email addresses and documents uploaded to HelloSign. Additionally, authentication tokens and secrets used to access HelloSign accounts were also exposed. Dropbox took immediate action to address the issue, including revoking compromised tokens and enhancing security measures to prevent similar incidents in the future.

Dell

Also in May, Dell issued a warning about a potential data breach affecting approximately 49 million customers. The breach reportedly involved unauthorized access to Dell's network, potentially compromising sensitive customer information. While Dell has not provided specific details about the nature or extent of the breach, the company is taking proactive steps to investigate the incident and implement necessary security measures.

GitLab

In May, the Cybersecurity and Infrastructure Security Agency (CISA) issued a warning regarding an actively exploited vulnerability in GitLab, a popular source code management platform. The vulnerability, identified as CVE-2024-3277, allows attackers to take over user accounts and gain unauthorized access to sensitive information stored on the platform. Exploitation of this bug has been observed in real-world attacks, highlighting the severity of the issue and the urgent need for remediation.

The vulnerability stems from a flaw in GitLab's user authentication mechanism, which could be exploited by attackers to bypass authentication controls and hijack user accounts. Once compromised, attackers can potentially access and manipulate source code repositories, project files and other confidential data stored on the platform. CISA advises organizations using GitLab to prioritize the installation of security updates provided by the vendor to mitigate the risk of exploitation.

GitLab has acknowledged the vulnerability and released security updates to address the issue. However, organizations must ensure prompt installation of these updates to protect their systems and data from exploitation.

A big hit to privacy

Research by Citizen Lab uncovered security vulnerabilities in popular Pinyin keyboard apps. Chinese language keyboards face a unique challenge due to the vast number of characters in the language. To overcome this challenge, Input Method Editor (IME) software is utilized. One widely used IME scheme is Pinyin, which enables Mandarin pronunciation using the Latin alphabet. However, this convenience comes with security risks as some Pinyin apps upload keystrokes to the cloud for processing.

Baidu's Pinyin app, for example, employs weak encryption, making users' keystrokes vulnerable to interception. Similarly, apps from Samsung, Xiaomi, OPPO, Honor and iFLYTEK use compromised encryption methods, posing risks to user privacy. While some companies addressed the identified issues, some, like Baidu, Vivo and Xiaomi, failed to fully rectify the vulnerabilities despite efforts from Citizen Lab.

The severity of these security breaches cannot be underestimated, given the widespread use of Pinyin keyboard apps in China. With over 95% market share and approximately 780 million users, Pinyin poses a significant risk of smartphone surveillance. This billion-user keystroke leak is compounded by the challenge some users face in updating their apps, exacerbating the persistence of these vulnerabilities.

Additionally, we saw a concerning development involving an online service called Spy.pet scraping over 10,000 servers throughout Discord. The collected data, which included messages from 600 million users across 14,000 servers, was being sold for as little as $5 via cryptocurrency. While Spy.pet does not scrape direct messages, it exposes messages posted in servers, raising significant privacy concerns.

Although Spy.pet's activities are alarming, users should be aware that messages posted on servers are not necessarily private. Anyone who joins a server can view all posted messages, potentially leading to unauthorized data scraping. One significant issue is that if this huge amount of data is properly correlated with the help of AI, a threat actor can establish a victim's digital persona, including habits, personality, interests, etc. All these personal details makes spear phishing as well as impersonation much easier.

Generative AI — ChatGPT and other AI tools in cybercrime

The explosion of generative AI in 2023 made AI not only a mainstream topic on everyone's minds, but also an accessible tool for the masses. Both attackers and defenders began exploring AI's potential to aid their efforts. With new models like GPT-4o emerging, the interest in AI for cybersecurity shows no signs of fading.

As detailed in our previous report, some attackers have already started using generative AI and large language models (LLMs) in their attacks, though these methods have not yet dominated the cyberthreat landscape. Most attackers continue to find success with semi-manual attacks and automation tools.

We can differentiate between two main types of AI threats:

- **AI-generated threats:** These are malware and other threats that are created using AI techniques, but do not incorporate AI in their operations. AI is merely a tool for their creation.
- **AI-enabled malware:** This type of malware integrates AI within its functionality. It may contain a complete AI model, such as an LLM, but more commonly, it communicates with a backend AI model for logic. Such threats can adapt to their surroundings and modify their behavior.

AI-enabled threats, also known as AI-powered malware, are still very rare and primarily exist as proof-of-concept examples. The current limitations of these threats outweigh the benefits for attackers, who continue to succeed using unpatched vulnerabilities, stolen passwords and automated scripts for their cyberattacks. The main use of generative AI models by attackers is to create and update automation scripts, thereby scaling their attacks and increasing their efficiency.

The most common AI-generated attacks we currently encounter include:

Malicious emails: Text can be written in multiple languages and tailored to personal situations by extracting information from social media. Feedback loops can be incorporated to adapt the messaging based on previous success rates.

Deepfake business email compromise (BEC): BEC scams are popular not only via email but also via voice or video calls. Convincing deepfake video calls of executives can persuade employees to transfer money or send gift cards.

Deepfake extortion: Use of deepfake images has elevated extortion scams like sextortion. Victims are now

threatened with pornographic images featuring their faces, which will be released to their friends if ransom demands are not met.

KYC bypass: The improved quality of deepfakes allows attackers to create fake identification cards to bypass KYC processes of cryptocurrency brokers or pass biometric voice authentication of online banking systems.

Script generation: Automation scripts and tools that help in the end-to-end process of cyberattacks can significantly reduce the time it takes to launch and scale an attack.

Malware generation: AI can be used to generate simple malware, such as information stealers, or to modify the source code of existing malware, making it harder to detect with signatures.

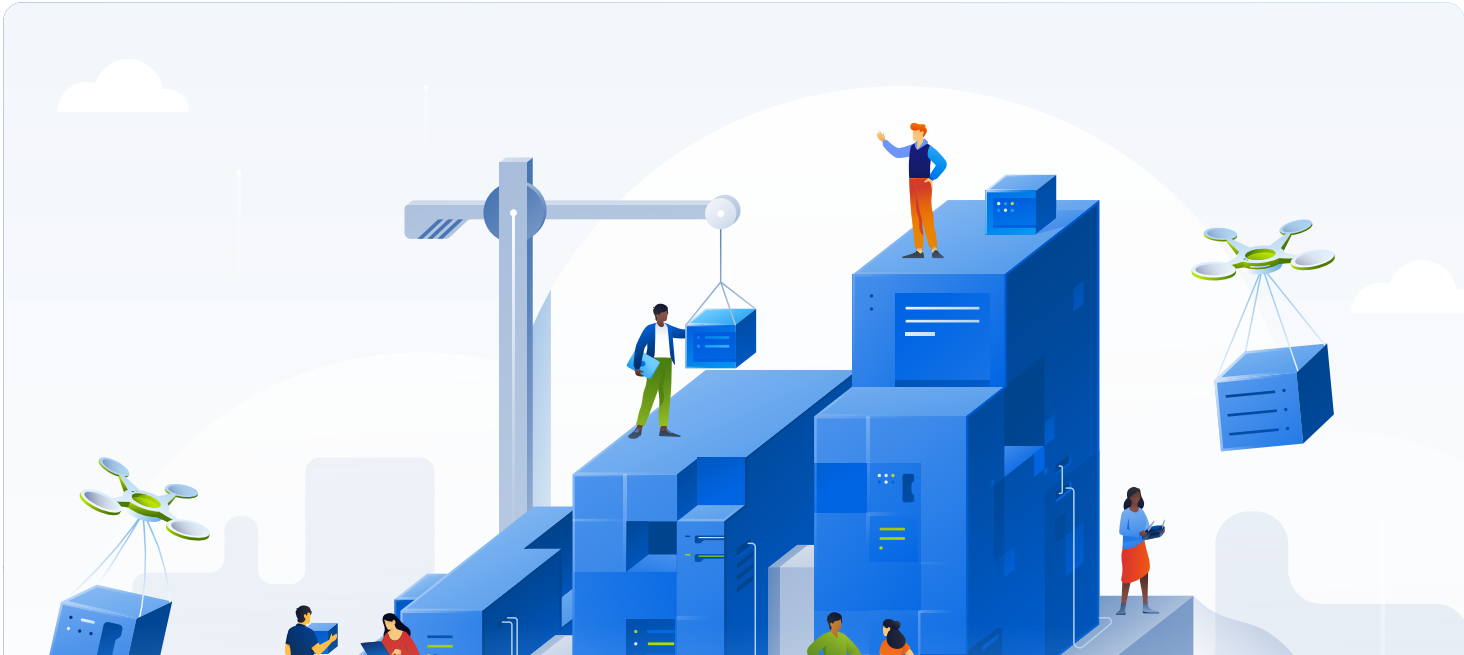
In November 2023, four individuals were arrested in China for using ChatGPT, which is prohibited in the country. The group had employed generative AI to create ransomware and deepfake content for extortion. This incident not only exemplifies how cybercriminals are attempting to use generative AI for cyberattacks, but also highlights the difficulty of completely restricting access to LLMs. Specific models like WormGPT and FraudGPT, which lack common filtering restrictions, are already available.

This demonstrates that AI is primarily used by cybercriminals for specific areas during their attacks — especially those involving social engineering and automation. While AI theoretically can assist attackers at every stage of the cyberattack kill chain, we have not yet seen this extensively utilized. Here are some examples of how AI could be used in the cyberattack kill chain:

- **Reconnaissance:** Analyze large data sets from scans and social media to identify patterns, automate target profiling and make selections.
- **Weaponization:** Generate malicious payloads.
- **Delivery:** Generate personalized phishing emails or deepfake lures and create automation scripts for payload delivery.
- **Exploitation:** Conduct automated network scans and exploit vulnerabilities.
- **Installation:** Generate scripts and malware for lateral movements within a network.
- **Command and control:** Create obfuscated communication channels adapted to the environment.
- **Actions on objectives:** Automate profitable data and credential harvesting, as well as efficiently analyze exfiltrated data for follow-up attacks.

We have also noticed an increase in attacks against AI. These are fairly basic attacks, such as stealing access credentials and reselling them on underground forums. Another attack method involves overwhelming LLMs with requests. This DoS attack not only degrades service quality for users, but also consumes response tokens, driving up the cost for the service owner who pays for the responses.

If you use generative AI in your organization, you should follow best practices to protect against data leaks, privacy issues, false code responses, underlying biases and model data poisoning. Many jurisdictions are currently preparing or releasing new laws and compliance guidelines arround the use of AI.



The importance of AI in cyberdefense

The importance of real-time AI analysis is evident as we move towards an AI vs. AI cyber battle, where human reaction times are insufficient. We need AI to detect and stop attacks 24/7 and collaborate with experts to take appropriate responses to ensure business continuity. Generative AI functionalities, such as those available in Acronis Cyber Protect Cloud, can help administrators automate routine tasks to reduce human error and free up time for more critical tasks.

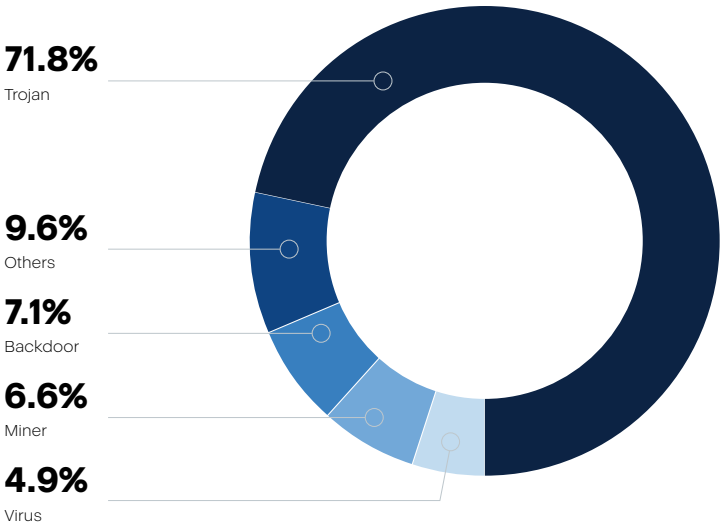
Using sophisticated AI models to detect and predict cyberattacks, such as transformer models to analyze malware behavior sequences, can help identify sophisticated attacks. To date, neither AI-generated nor AI-enabled threats were able to bypass modern detection capabilities completely — very often the behavior they exhibit is still detectable with current cyber protection solutions if applied correctly. Generative AI can also help prioritize attacks, explain their impact to analysts, act as an "expert-in-the-box" advising on best practices for next steps, and mitigate the cybersecurity skills gap that many organizations face.

2 General malware threats

In January, about 17.9% of Acronis customers had at least one malware attack successfully blocked on their endpoints. The percentage peaked at 28% in April. These still high percentages suggest that, despite security awareness training and patching, about two out of every 10 threats makes it to the endpoint. Furthermore, because these statistics are based on endpoint detections, any proxy or email protection applied earlier in the chain did not prevent these threats.

Another prevalent trend in the first half of 2024 is malvertising, which continues to deceive users into downloading fake software by leveraging Google Ads and SEO poisoning.

Month	Percentage of clients with blocked malware
January	17.9%
February	20.8%
March	26%
April	28%
May	23.8%



AV-TEST

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

The most common malware type is Trojan horses, making up more than half of blocked threats. Below are the most commonly seen malware families for H1 2024, once again revealing a clear focus on bots and information stealers:

- RedLine Stealer
- Agent Tesla
- FormBook
- njRAT
- Remcos
- Raccoon Stealer
- Emotet
- NanoCore
- AsyncRat
- IcedID

Acronis has identified a 5% increase in the number of new malware samples appearing in the wild since Q4 2023. Independent malware testing lab AV-TEST recorded 328,960 new malware samples per day in Q1 2024, compared to 312,874 in Q4 2023. This proportion matches the number of new samples seen by Acronis Cyber Protection Operation Centers.

The average lifetime of a malware sample in June 2024 was a mere 2.3 days, after which it disappeared and was never seen again by Acronis. In May 2024, this figure was down to 2.1 days. Malware is shorter lived than ever, as attackers use automation to create new and personalized malware at blazing speeds in an effort to bypass traditional signature-based detection. Of all the samples observed, 82% were seen only once across our customer base.

The country with the most clients experiencing malware detections in May 2024 was the United States (19.2%), followed by Brazil (10.7%) and Italy (6.9%).

Monthly percentage of global detections by country

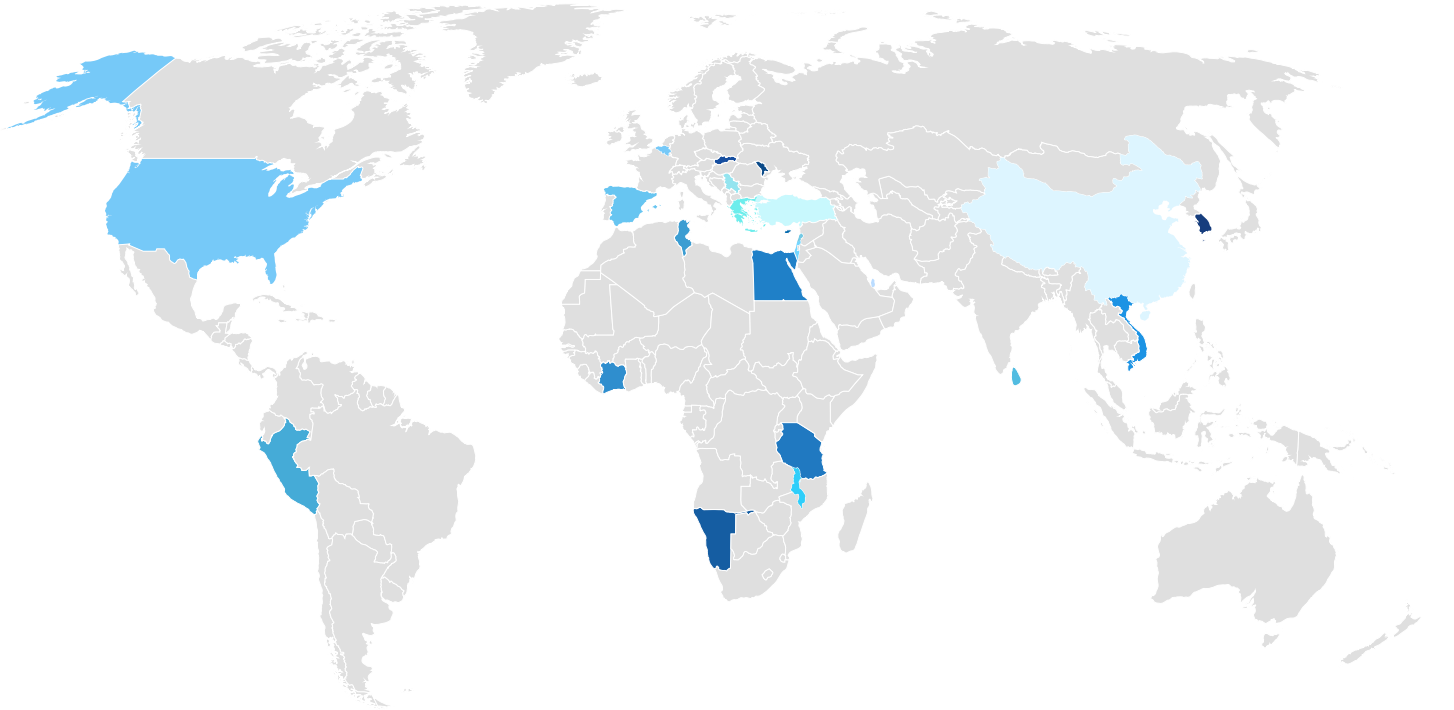
Country	January 2024	February 2024	March 2024	April 2024	May 2024
Australia	1.9%	2.1%	1.6%	1.7%	1.7%
Brazil	10.5%	12.5%	10.6%	10.1%	10.7%
Canada	4.8%	5.5%	3.9%	4.2%	3.9%
France	3.6%	5.5%	4.1%	4.2%	3.9%
Germany	8.6%	9.9%	6.9%	6.5%	6.4%
Italy	5.6%	2.6%	6.3%	6.4%	6.9%
Japan	2.4%	7.5%	2%	2%	2%
Netherlands	1.2%	1.4%	1.1%	1.1%	1%
Singapore	5.5%	4.2%	2.8%	3.7%	3%
South Africa	1.2%	5%	1.6%	1.7%	1.7%
Spain	2.9%	4.1%	3.2%	3.2%	3.5%
Switzerland	3.6%	1.1%	3.5%	3%	2.9%
United Arab Emirates	0.8%	1.9%	0.9%	0.8%	1%
United Kingdom	4.3%	6.1%	4.7%	4.5%	4.6%
United States	16.3%	28.2%	21.4%	21%	19.2%

If we normalize the number of detections per active client per country, we get a slightly different distribution. The following table shows the normalized percentage of clients per country with at least 25 malware detections per country in April 2024.

Rank	Country	Percentage of clients with malware detections in April 2024 (normalized)
1	Bahrain	63.2%
2	South Korea	49.4%
3	Republic of Moldova	48.5%
4	Slovakia	47.3%
5	Namibia	47.3%
6	Cyprus	43%
7	Tanzania	42.6%
8	Egypt	42.6%
9	Singapore	41.7%
10	Vietnam	40.5%

Rank	Country	Percentage of clients with malware detections in April 2024 (normalized)
11	Ivory Coast	40.3%
12	Tunisia	39.4%
13	Peru	39.3%
14	Sri Lanka	38.7%
15	Malawi	38.3%
16	Spain	37.5%
17	Israel	37.3%
18	Lebanon	36.7%
19	Belgium	33.8%
20	United States	33.7%
21	Qatar	33.7%
22	Greece	33.3%
23	Serbia	32.9%
24	Turkey	32.3%
25	China	31.8%

Top 25 countries: Normalized detection rates, April 2024



Percentage

31.8% 63.2%

Normalized malware detections by focus countries

Country	January 2024	February 2024	March 2024	April 2024	May 2024
Australia	17.1%	16.4%	20.4%	23.4%	20.1%
Brazil	22.6%	23.3%	31.1%	31.7%	28%
Canada	8.2%	9.2%	11.2%	14.4%	12.1%
France	14.4%	19.4%	24.0%	26.7%	20.4%
Germany	20.2%	21.7%	25.6%	27.5%	23.7%
Italy	18.2%	13.2%	27.9%	30.1%	26.8%
Japan	14%	20.9%	15.7%	16.7%	14.1%
Netherlands	18.4%	20.4%	25.9%	26.1%	21.9%
Singapore	43.9%	38.0%	29.6%	41.7%	29%
South Africa	14.2%	33%	25.9%	27.9%	23%
Spain	32.2%	16.6%	40.5%	37.5%	31.2%
Switzerland	17.3%	22.5%	24.0%	24.8%	20.4%
United Arab Emirates	17.6%	18.8%	29.1%	29.3%	29.3%
United Kingdom	13.8%	17.5%	20%	19.5%	16.5%
United States	16%	24.9%	30.9%	33.7%	26.8%

Ransomware threats

Falling victim to ransomware is among the greatest concerns for organizations globally. And it's no wonder, as the number and frequency of ransomware attacks remain high.

While law enforcement has made several arrests and increased the pressure on ransomware groups, some attacks are being thwarted earlier in the process — such as at the email lure or malicious URL stage — resulting in the final ransomware not being downloaded. As a result, these attacks are not included in current statistics.

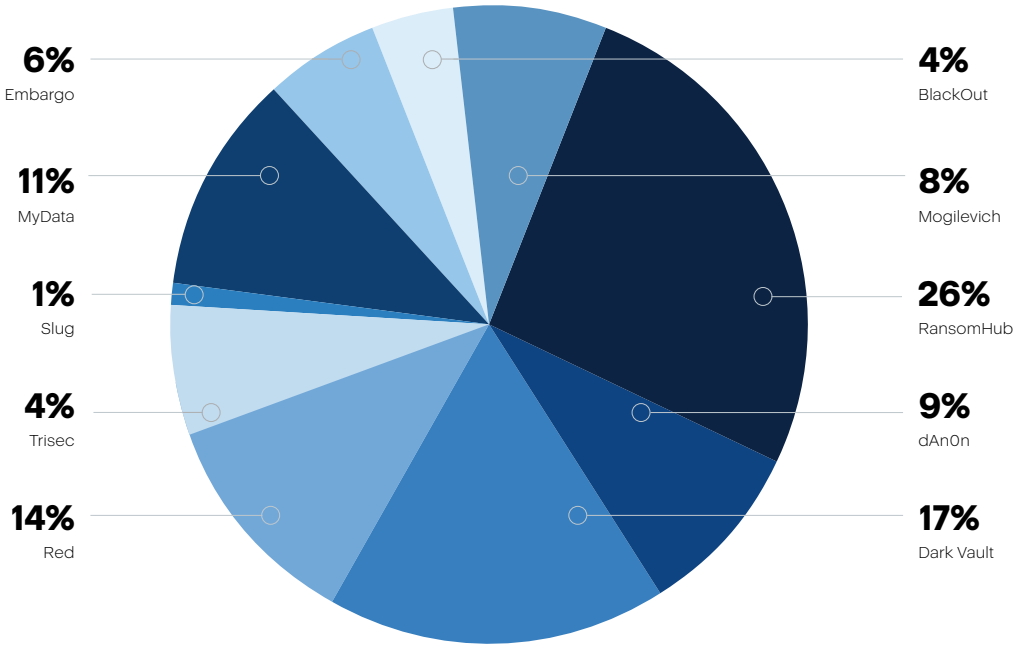
Despite these developments, the availability of LLMs like ChatGPT has enabled cybercriminals to increase the number of attacks further through automation and repetition. This has led to a growing number of players in the ransomware market.

In this section, we review data spanning from January to April 2024 that was intercepted and safeguarded by our threat-agnostic Acronis Active Protection. We also analyze data that has been made public on the underground leak sites of ransomware operators.

In Q1 2024 we saw the appearance of 10 new groups, which together claimed 84 cyberattacks globally.

New ransomware groups, Q1

- Mogilevich (7)
- RansomHub (22)
- dAn0n (8)
- DarkVault (14)
- Red (12)
- Trisec (3)
- Slug (1)
- MyData (9)
- Embargo (5)
- BlackOut (3)

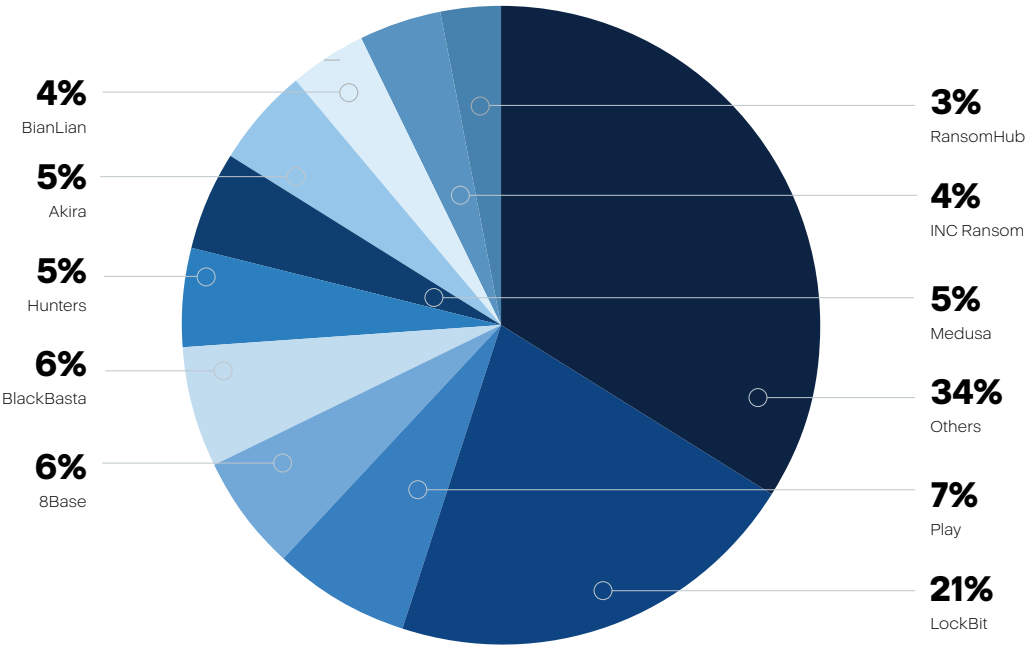


Among the top 10 most active ransomware families we observed and tracked in Q1 2024, three highly active groups stand out as the primary contributors, collectively responsible for about 35% of the attacks. Among these groups, LockBit takes the lead, accounting for 20% of attacks, followed by BlackBasta and Play with 7.1% and 7% respectively.

Q1 2024 produced 1,048 publicly mentioned ransomware cases, a 23% increase over Q1 2023. The below graph shows the number of ransomware cases from January to May 2024.

Ransomware group activity, Q1 2024

- LockBit
- Play
- 8Base
- BlackBasta
- Hunters International
- Medusa
- Akira
- BianLian
- INC Ransom
- RansomHub

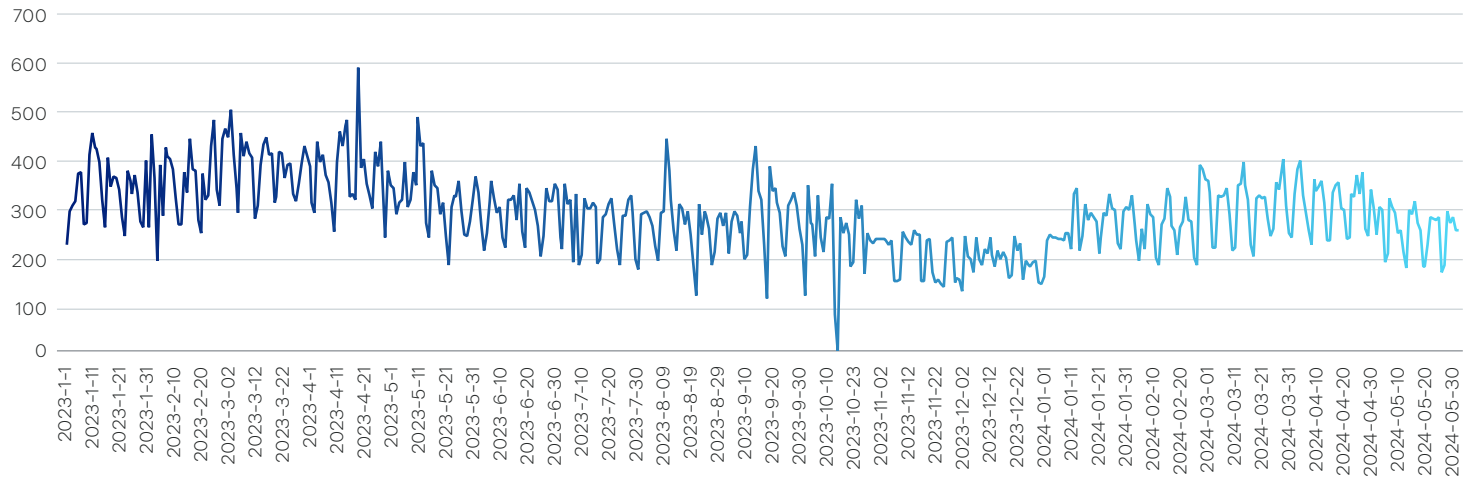


It should be noted that the mentioned statistics represent only a portion of the overall picture, as certain victims choose to negotiate with, and ultimately pay their attackers to avoid public exposure. Unfortunately, paying a ransom does not provide any guarantee that the stolen data will be deleted on the attacker's end. Historical cases have revealed that victims who complied with ransom demands were later targeted for additional extortion, witnessed their data being sold to other malicious actors or had their data leaked online.

Daily ransomware detections

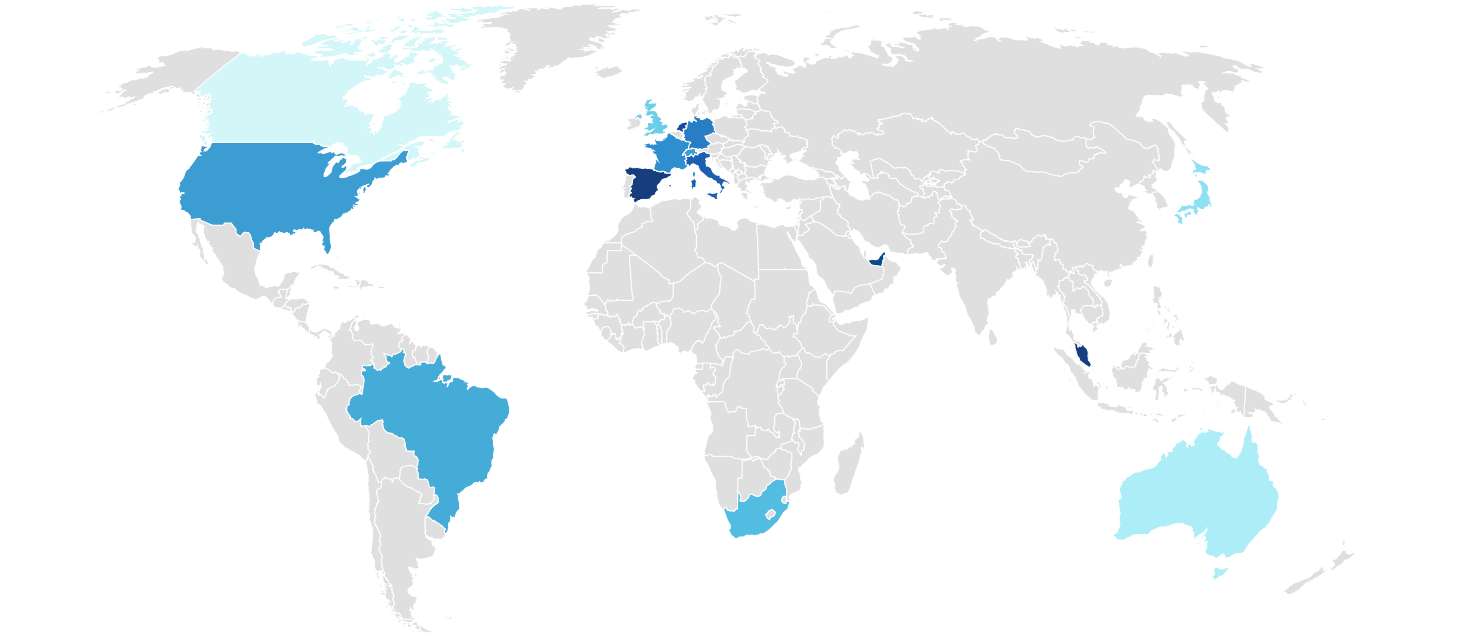
The number of ransomware detections increased 32% from Q4 2023 to Q1 2024, though the number of monthly ransomware detections has stayed relatively flat for 2024.

Daily ransomware detections globally



Ransomware detections in 2024 peaked on March 28, while May 25 saw the least ransomware activity.

Ransomware detections, April 2024



We've normalized the number of ransomware detections, considering only machines with more than 25 detections and countries where we have more than 150 installations.

Normalized ransomware detections by focus countries

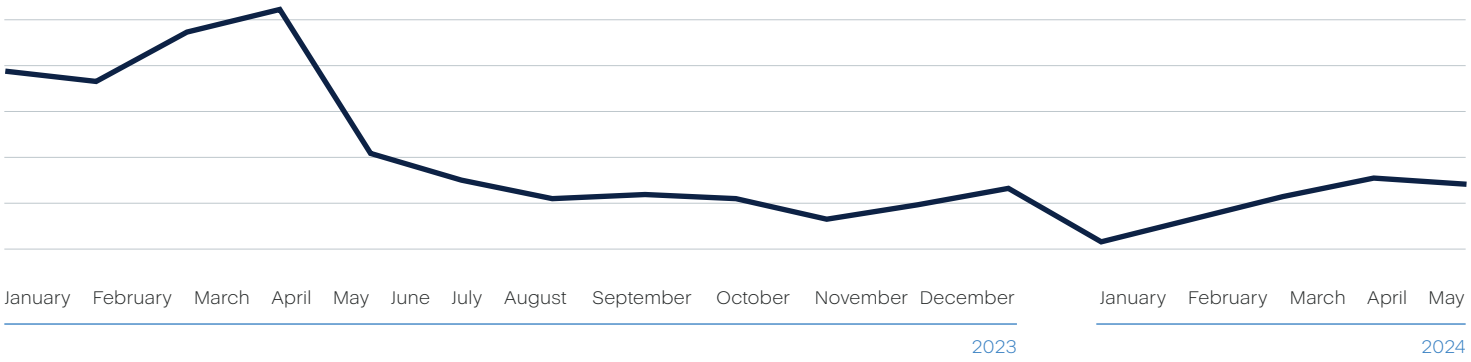
Country	Ransomware detections in Q1 2024	Ransomware detections in April 2024	Ransomware detections in May 2024
Australia	2.6%	1.1%	0.7%
Canada	5.5%	2%	1.7%
France	4.1%	1.6%	1.3%
Germany	13.4%	5.4%	4.5%
Italy	1.9%	0.8%	0.5%
Japan	16.5%	5.6%	4.5%
Netherlands	4.3%	1.8%	1.5%
Spain	4.5%	1.1%	0.9%
United Kingdom	2.5%	0.9%	0.6%
United States	5.4%	1.7%	1.7%

Telemetry data in focus countries

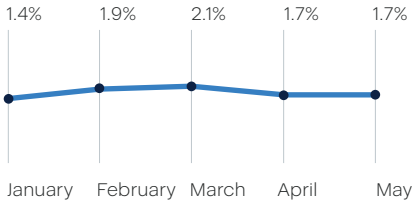
Cybercriminals don't discriminate — they target businesses of all sizes and industries. Their interest is simply sensitive data, which they can sell to earn money and keep the cycle going.

U.S.

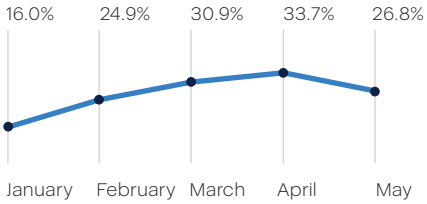
U.S. ransomware detections



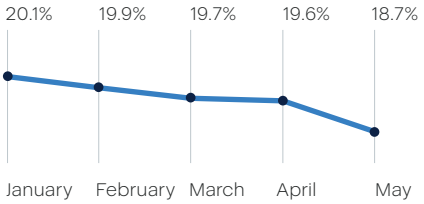
Ransomware detections



Malware detections

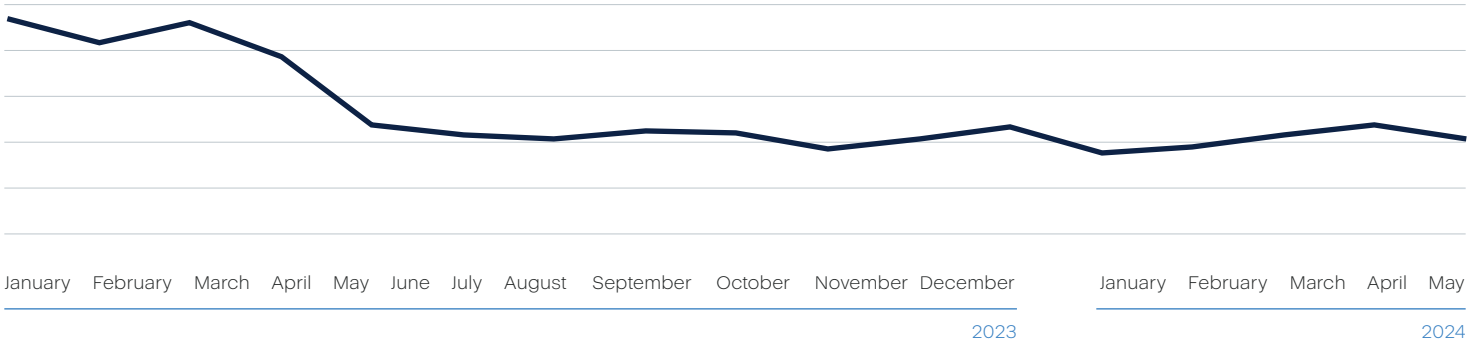


URL detections

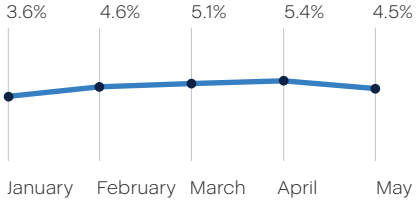


Germany

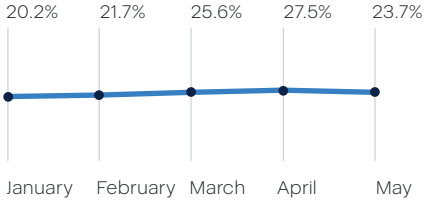
Germany ransomware detections



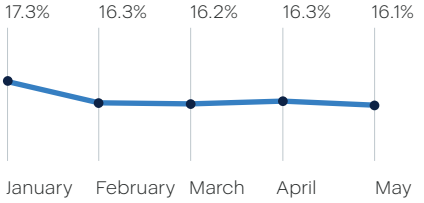
Ransomware detections



Malware detections

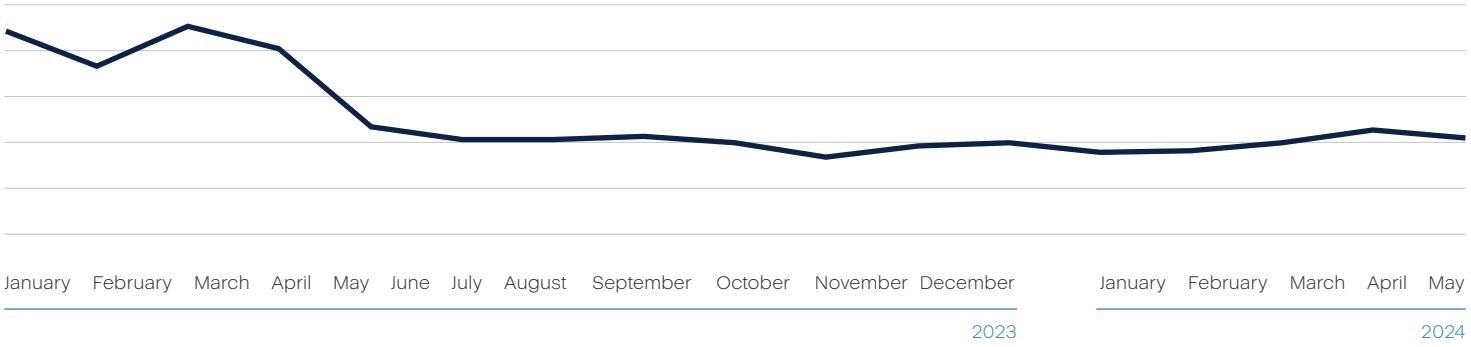


Url detections

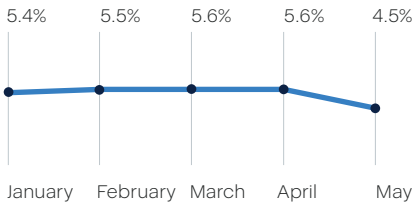


Japan

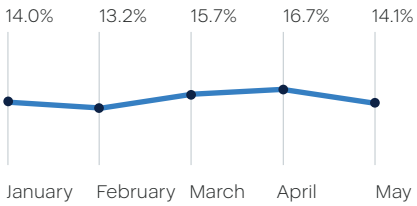
Japan ransomware detections



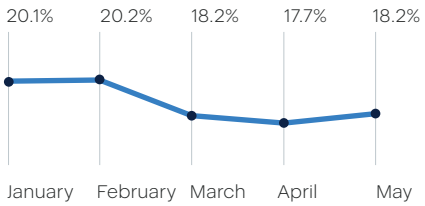
Ransomware detections



Malware detections

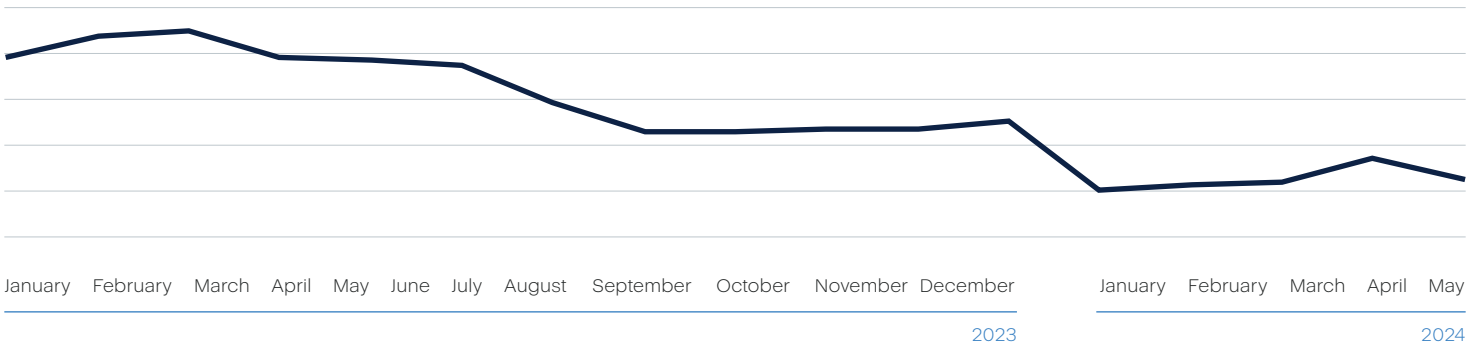


URL detections

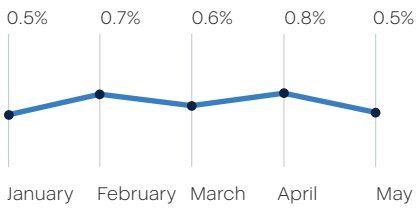


Italy

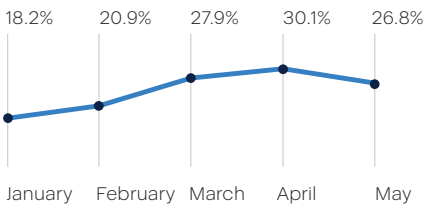
Italy ransomware detections



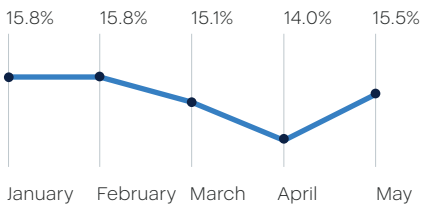
Ransomware detections



Malware detections

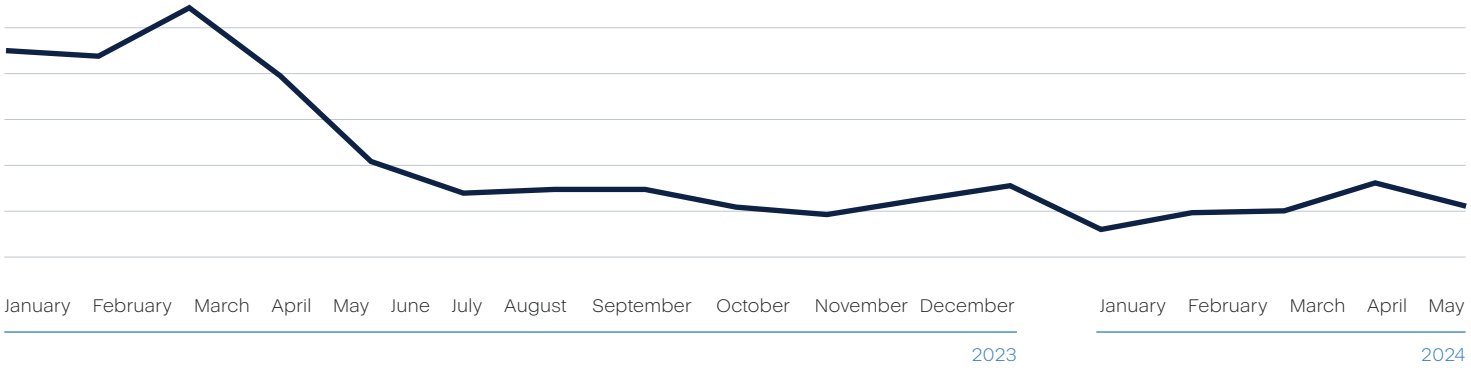


Url detections

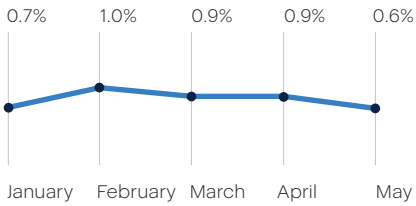


U.K.

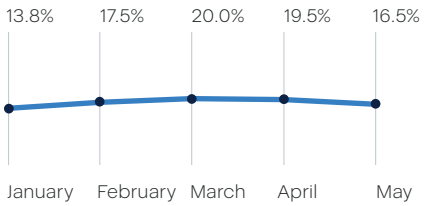
U.K. ransomware detections



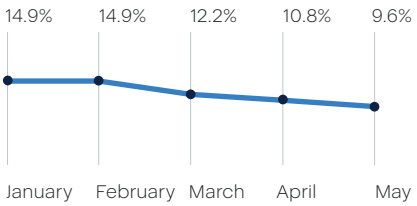
Ransomware detections



Malware detections

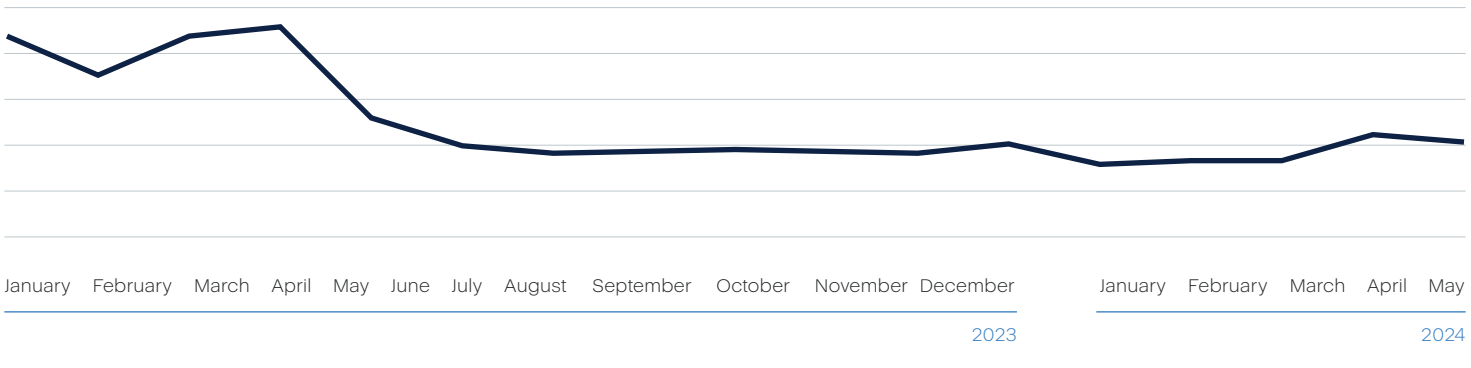


URL detections

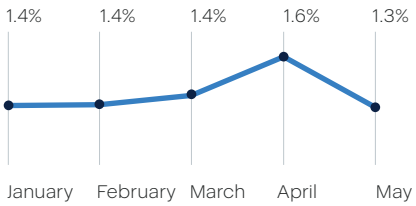


France

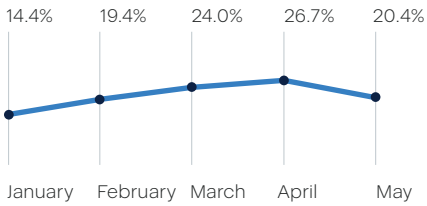
France ransomware detections



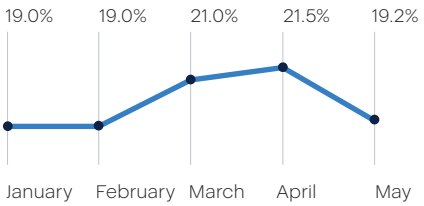
Ransomware detections



Malware detections

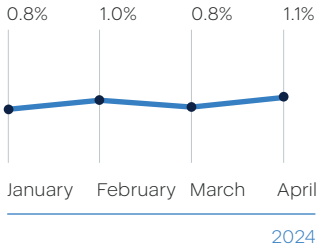


Url detections

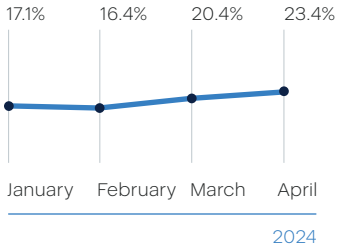


Australia

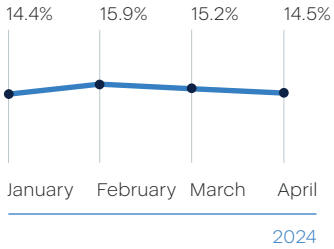
Ransomware detections



Malware detections



URL detections

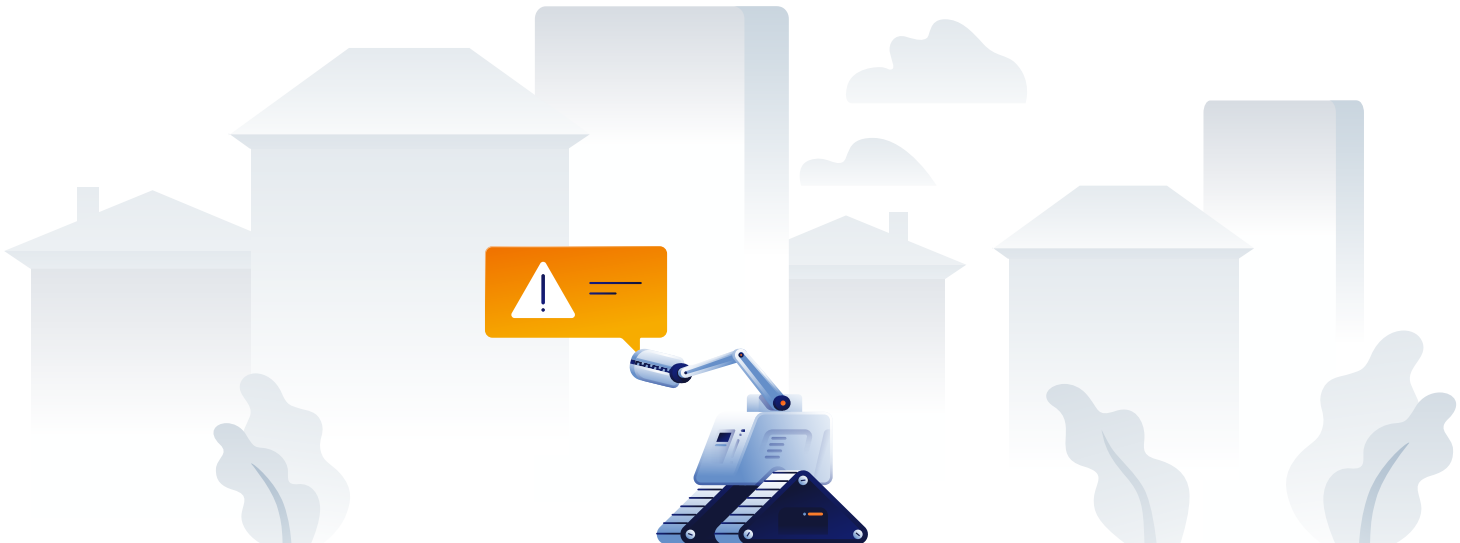


Malicious websites

Acronis Cyber Protection Operation Centers blocked 27,994,848 phishing and malicious URLs in H1 2024. This constitutes a 3% spike over Q4 2023 (27,292,197).

Malicious URLs continue to be a common tool for cybercriminals to deliver their payloads and compromise systems. Despite advances in email filtration and security software, many malicious URLs still manage to slip through basic security defenses and reach users' endpoints. These URLs are often embedded in the emails, which are designed to look legitimate and lure users into opening them. Recent statistics show that over 30% of phishing emails are still being opened. Once clicked, the URL may redirect the user to a fake login page or to download a malware-laden file.

Month	Blocked URLs
January	10,258,621
February	8,432,586
March	9,303,641
April	11,526,276
May	13,406,456



An average of 17.5% of endpoints tried to access malicious URLs in Q1 2024, up slightly from 15.7 % in Q4 2023.

Month	Percentage of users that clicked on malicious URLs
January	17.3%
February	17.7%
March	17.5%
April	17.5%
May	17.1%

The country with the largest percentage of blocked malicious URLs at the endpoint in April 2024 was India with 28.7%, followed by Colombia with 27.3% and South Korea with 24.1%.

Similar to the malware detection statistics, we normalized the numbers depending on the number of active machines in each country with at least 10 blocked URLs.

Top 15 countries: Blocked URLs, normalized

Rank	Country	Percentage of blocked URLs in April 2024
1	India	28.7%
2	Colombia	27.3%
3	South Korea	24.1%
4	Brazil	21.8%
5	France	21.5%
6	Mexico	20.9%
7	United States	19.6%
8	Japan	17.7%
9	Netherlands	16.7%
10	Singapore	16.3%
11	Germany	16.3%
12	Australia	14.5%
13	Italy	14%
14	United Kingdom	10.8%
15	Canada	6%

3

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

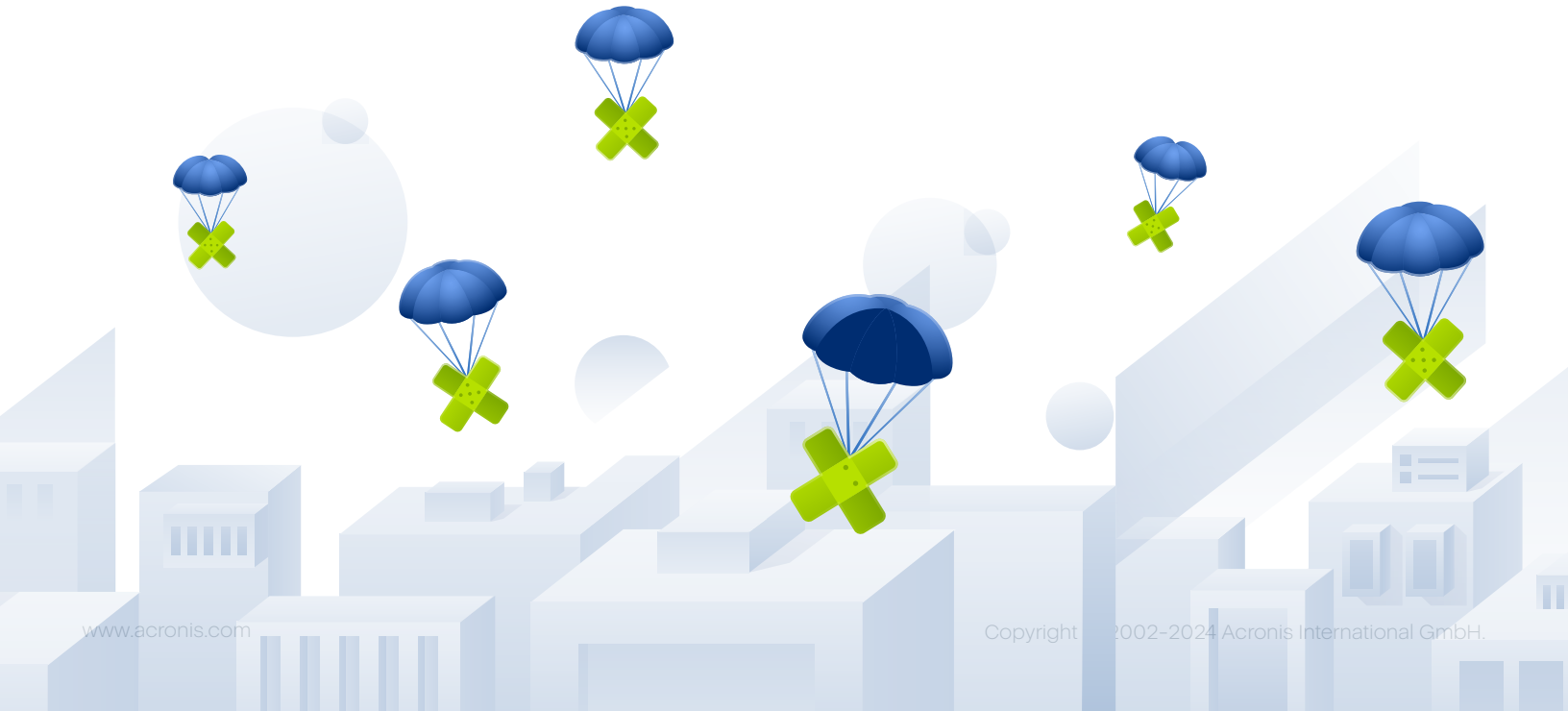
The increase in cyberattacks, data leaks and ransomware outbreaks reveals that the current approach to cybersecurity is failing. This failure is the result of weak technologies, heightened complexity and human mistakes caused by clever social engineering tactics.

Backup is essential for when cybersecurity solutions fail, but backup solutions can be compromised or disabled, and often perform slowly, causing businesses to lose a lot of money to downtime. Even if backup solutions are working well and remain uncompromised in an attack, it usually takes hours or days to restore systems and data to an operational state.

Patch your OS and apps

Many attacks succeed due to unpatched vulnerabilities. With a solution like Acronis Cyber Protect, you're covered with embedded vulnerability assessment and patch management functionalities. We track all discovered vulnerabilities and the fixes that have been released to address them, and allow admins or technicians to easily patch all endpoints with a flexible configuration and detailed reporting. Acronis Cyber Protect 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. Be sure to patch high-severity vulnerabilities first and follow the success report to check that patches were applied properly.

If you don't use Acronis Cyber Protect or another solution with patch management functionality, staying on top of this is much harder. At the very least, you need to ensure that Windows gets all necessary updates and that they're installed promptly — users tend to ignore system messages, especially when Windows asks for a restart. This is a big mistake. Be sure that auto-updates are enabled for popular software vendors like Adobe and that apps like PDF Reader are also updated promptly.



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

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

Because emails can contain malicious attachments, you should always double check where they originated and whether you were expecting them. Before you open any attachment, it should be scanned by your anti-malware solution.

Ensure your cybersecurity solution is properly configured

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

But an anti-malware solution is not enough — it must be configured properly:

- A full scan should be performed at least once per day.
- Updates should occur hourly or daily, depending on how often they are available.
- It should be connected to its cloud detection mechanisms. With Acronis Cyber Protect, this is enabled by default, but you need to ensure that internet access remains available and isn't accidentally blocked for 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 be sure that the license is legitimate if you're using a paid version from a security vendor.

Keep passwords and working spaces private or switch to passwordless authentication

Ensure that your passwords (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 passwords, 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 multifactor authentication.

Even when working from home, don't forget to lock your laptop or desktop and limit access to it. There are many cases when people simply could steal sensitive information from an unlocked PC.

Finally, passwordless authentication reduces the risk of password-related breaches, which are common due to weak, reused or stolen passwords. By leveraging biometric data, such as fingerprints or facial recognition, hardware tokens, or email / phone verification, passwordless authentication provides a higher level of security. Attackers cannot easily replicate these factors, thus minimizing the risk of unauthorized access.

Have proper cybersecurity protection at place

Nonintegrated solutions allow multiple security gaps that can be leveraged by security threats. To address these gaps, businesses should move to an integrated solution combining cybersecurity, EDR / XDR, backup and disaster recovery. Eliminating a patchwork of siloed tools helps you maintain optimal performance, eliminate compatibility issues and ensure rapid recovery. For example, if a threat is missed or detected while your data is being altered, data will be restored from a backup immediately.

With an integrated solution, everything runs through a single agent — it knows when data is lost and needs to be restored. This isn't possible when you use separate anti-malware and backup products, each with its own agent. An individual anti-malware solution may stop the threat, but 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 is a highly reliable and efficient cybersecurity solution that is natively integrated with data protection and endpoint management and is built specifically for the operational needs of MSPs. With integrated cybersecurity, data and endpoint protection, Acronis Cyber Protect Cloud provides reliable and efficient cybersecurity for MSPs that reduces both downtime and the time and cost required to prevent and remediate security incidents.

Acronis is a global cyber protection company that provides natively integrated cybersecurity, data protection, and endpoint management for managed service providers (MSPs), small and medium businesses (SMBs), and enterprise IT departments. Acronis solutions are highly efficient and designed to identify, prevent, detect, respond, remediate, and recover from modern cyberthreats with minimal downtime, ensuring data integrity and business continuity. Acronis offers the most comprehensive security solution on the market for MSPs with its unique ability to meet the needs of diverse and distributed IT environments.

A Swiss company founded in Singapore in 2003, Acronis has 45 locations across the globe. Acronis Cyber Protect is available in 26 languages in 150 countries and is used by over 20,000 service providers to protect over 750,000 businesses. Learn more at www.acronis.com

Acronis

Learn more at
acronis.com