Acronis

Report
H2 2023

# Acronis Cyberthreats Report, H2 2023:

Alarming rise in cyberattacks, SMBs and MSPs in the crosshairs

# Table of contents




**Authors:**

**Alexander Ivanyuk**
Senior Director, Technology

**Candid Wuest**
VP of Product Management

**Irina Artioli**
Cyber Protection Evangelist

# Introduction and summary

Acronis was the first company to implement complete integrated cyber protection to protect all data, applications and systems. Cyber protection requires researching and monitoring threats, as well as abiding by the five vectors of SAPAS: safety, accessibility, privacy, authenticity and security. As part of this strategy, Acronis established four Cyber Protection Operation Centers (CPOCs) around the world to monitor and research cyberthreats 24/7.

The data presented in this report is collected from our flagship products: Acronis Cyber Protect 15, an on-premises solution, and Acronis Cyber Protect Cloud, both of which were launched in 2020. Prior to those releases, Acronis had been a leader in the data protection market with its innovative Acronis Active Protection anti-ransomware technology, which evolved over time to demonstrate Acronis' unique expertise in stopping threats aimed at data. However, it's important to note that the artificial intelligence (AI)- and behavior-based detection technologies that Acronis developed in 2016 have been expanded to address all forms of malware and other potential threats. All of that helped Acronis to become a leader in MSP-related cybersecurity since 2020.

This report explores the threat landscape as encountered by our sensors and analysts in the second half of 2023. General malware data presented in the report was gathered from July – December 2023, and reflects threats targeting endpoints that we observed during these months.

The report represents a global outlook and is based on over 1,000,000 unique endpoints distributed around the world, focusing on 15 countries. Most of the statistics discussed focus on threats for Windows operating systems, as these are much more prevalent than those targeting macOS and Linux.

## Key findings:

- Singapore, Spain and Brazil were the most targeted focus countries for malware attacks in Q4 2023.
- Nearly 28 million URLs were blocked at the endpoint by Acronis in Q4 2023, a 36% decrease compared to Q4 2022.
- 33.4% of all received emails were spam, and 1.5% contained malware or phishing links.
- Each malware sample lives an average of 2.1 days in the wild before it disappears.
- 1,353 ransomware cases were publicly mentioned in Q4 2023. LockBit, Play and ALPHV were among the top contributors. Additionally, the ransomware group Cyber Toufan was highly active in December, with 91 victims.

# Top cybersecurity trends from July – December 2023:

- Ransomware continues to be a major threat to large and medium-sized businesses, including government, health care and other critical organizations. Recently, ransomware attackers have abused vulnerable drivers to get a foothold into systems and disable security tools.
- Data stealers are the second most prevalent threat, causing a majority of data breaches along with traditional usage of stolen credentials.
- ChatGPT and similar generative AI systems are already being used to launch cyberattacks, create malicious content and automate attacks.
- The number of email attacks detected in 2023 has surged by 222% compared with the second half of 2022.

## What you will find in this report:

- The top security / threat trends Acronis observed in the second half of 2023.
- 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 with 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

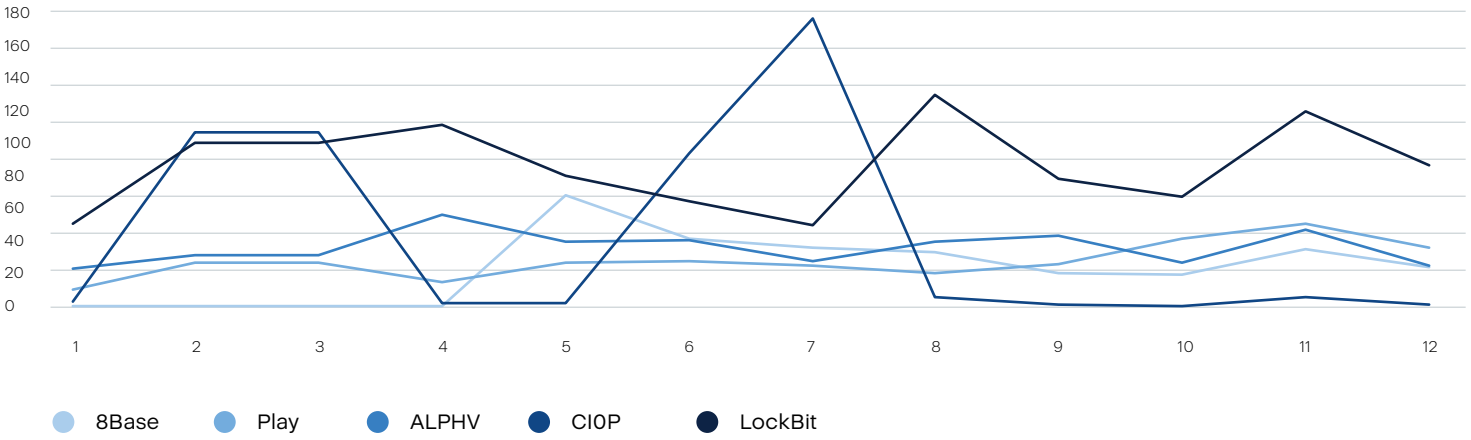
# Key cyberthreats and trends in H2 2023

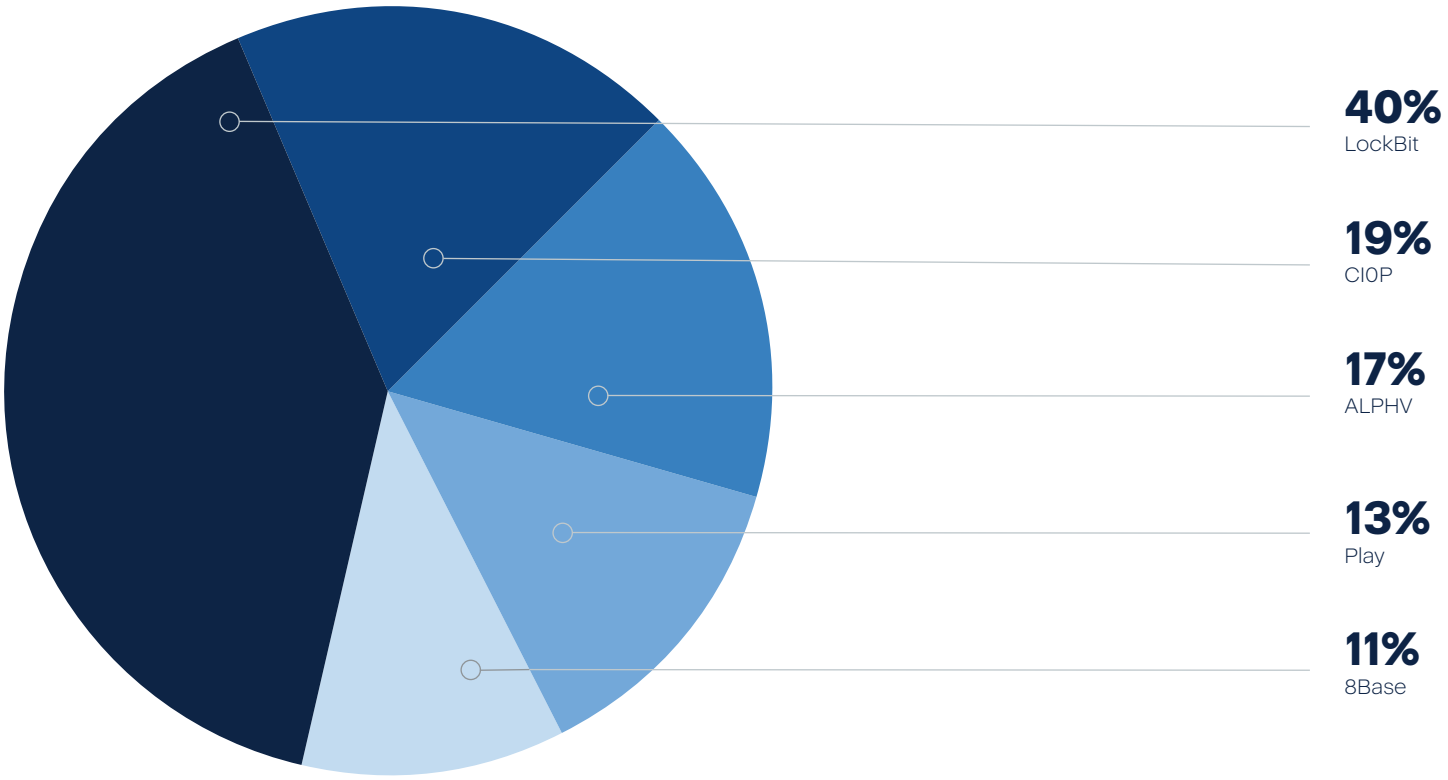
# 1. Ransomware variants continue to decrease, but businesses are still losing data and money

Looking back at 2023, the following ransomware gangs were the most active in terms of total numbers of victims:

**LockBit (1,000)** **CI0P (487)** **BlackCat / ALPHV (415)** **Play (322)** **8Base (269)**

### Top 5 ransomware gangs per month, number of victims



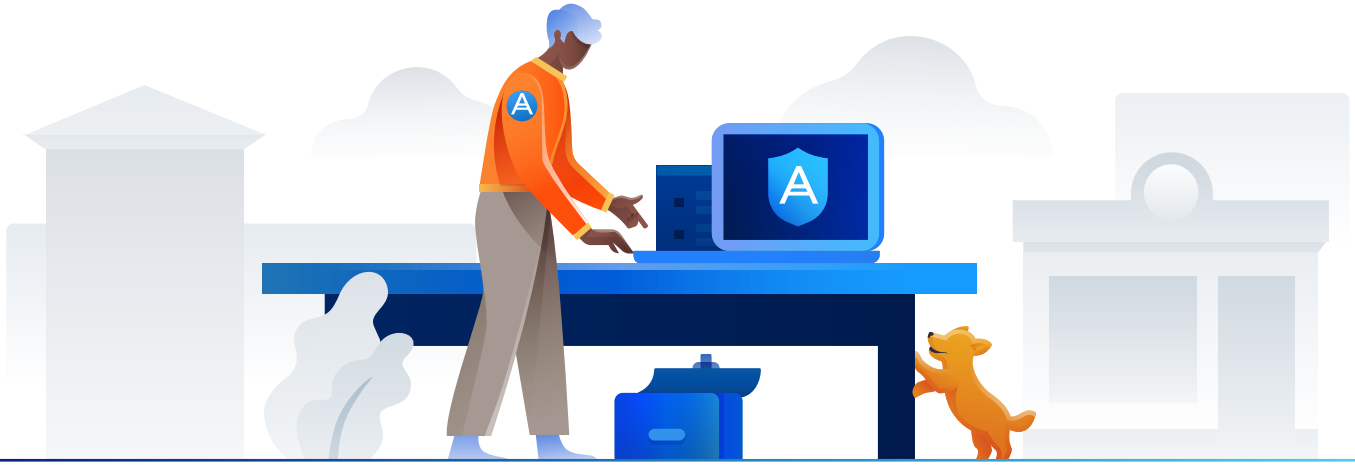
The BlackCat / ALPHV gang, much like LockBit, was already a top ransomware gang in 2022. They kept up the pace in 2023 and infected a large number of high-profile victims. In December 2023, the U.S. Department of Justice (DOJ) revealed that the U.S. Federal Bureau of Investigation (FBI), in collaboration with international law enforcement agencies, successfully breached the ALPHV ransomware operation's servers, allowing the FBI to monitor activities and obtain decryption keys. This operation saved approximately $68 million in ransom payments by helping 500 victims recover their files for free. Despite the ALPHV gang's attempt to regain control of its data leak site, the FBI's access led to back-and-forth control of the URL. This prompted the gang to relax restrictions for affiliates, enabling them to target any organization except those in the Commonwealth of Independent States. According to the FBI, ALPHV affiliates compromised more than 1,000 entities, demanded more than $500 million, and received nearly $300 million in ransom payments.

## Lets take a look into the activities of these top gangs, as well as some other notable ransomware incidents from July – December 2023.

**U.S. / manufacturing sector / Dark Angels**

Johnson Controls International, with $26.6 billion in annual revenue, fell victim to a Dark Angels ransomware attack that encrypted numerous company devices, including VMware ESXi servers, severely disrupting operations of the company and its subsidiaries. The multinational conglomerate specializes in industrial control systems, security equipment, air conditioning and fire safety equipment, employing a workforce of 100,000 across its corporate operations and subsidiaries, including York, Tyco, Luxaire and more. The Dark Angels ransomware gang demanded a $51 million ransom payment for a decryption key and the deletion of 27 terabytes of stolen data.

Active since May 2022, Dark Angels infiltrates corporate networks, exfiltrates data for double extortion and encrypts all network devices upon accessing the Windows domain controller. They initially employed encryptors based on Babuk ransomware's source code leak, but they began using a Linux encryptor similar to Ragnar Locker's in 2021.



### U.S. / manufacturing sector / ALPHV

The ALPHV ransomware group claimed responsibility for an attack on Clarion, a global manufacturer of car audio and video equipment. Clarion is widely known for its car navigation systems and for providing components to automakers such as Suzuki, Toyota, Subaru, Ford, Volkswagen, Proton and Peugeot.

### U.S. / hospitality sector / Scattered Spider

Caesars Entertainment, the largest U.S. casino chain with an extensive loyalty program, revealed that it paid a ransom to prevent the online exposure of customer data stolen in a recent cyberattack. The breach involved the theft of Caesars' loyalty program database, which contains customer driver's license and social security numbers. An 8-K form filed with the U.S. Securities and Exchange Commission (SEC) disclosed that Caesars is still investigating the extent of sensitive information accessed by the attackers, but stated that no member passwords, PINs, bank account details or payment card information were compromised.

Although Caesars did not explicitly link the attack to a specific cybercriminal group, a Bloomberg report suggests the involvement of Scattered Spider (also known as UNC3944 and 0ktapus), a financially motivated threat group active since at least May 2022. Scattered Spider employs various tactics, including social engineering, multifactor authentication fatigue and SMS credential phishing to pilfer user credentials and infiltrate target networks.

### U.S. / hospitality sector / ALPHV

Similar to the Caesar's ransomware attack, an affiliate of the BlackCat / ALPHV ransomware group attacked MGM Resorts International, forcing the hospitality and entertainment company to shut down its IT systems. The cybercriminals claimed to have infiltrated MGM's infrastructure, encrypted more than 100 ESXi hypervisors and exfiltrated data from the network. They maintained access to some of MGM's infrastructure and demanded a ransom to avoid further attacks. Personal information, including social security numbers, driver's license numbers and customer names were among the data stolen. In October, MGM informed the U.S. Securities and Exchange Commision that it lost around $100 million as a result of the attack, suggesting that MGM paid the ransom.

### Spain / government sector / LockBit

The LockBit cybercrime gang attacked the city council of Seville, disrupting municipal services and demanding a $1.5 million ransom, which the council refused to pay. While the attack was initially mistaken for an internal systems failure, the attackers encrypted networks and threatened to expose stolen data.

### Israel / health care sector / Ragnar Locker

The Ragnar Locker ransomware group claimed responsibility for an attack on Israel's Mayanei Hayeshua Medical Center, publishing their admission on their data leak site and threatening to release 1 TB of stolen data. The cyberattack disrupted hospital operations and new patient care.

The threat actors stated they didn't encrypt devices to avoid medical equipment malfunctions, but they did steal data, including sensitive medical records and drug prescriptions. Ragnar Locker published 420 GB of the allegedly stolen data and threatened to release more if the ransom was not paid.

### U.S. / health care sector / Rhysida

The Rhysida ransomware group claimed responsibility for an attack on Prospect Medical Holdings, a U.S. health care company with 16 hospitals and 166 outpatient care clinics. Multiple hospitals under Prospect Medical Holdings, spanning several states, experienced computer system disruptions that led to ER closures and ambulance diversions. Rhysida claimed to have accessed a database containing 500,000 social security numbers, corporate documents and patient records, and demanded a 50 Bitcoin ransom ($1.3 million).

### U.S. / health care sector / LockBit

The LockBit ransomware group claimed an attack on Varian Medical Systems and threatened to release the medical data of cancer patients. Varian Medical Systems, a health care company owned by Siemens Healthineers and specializing in oncology software, generates $3 billion in annual revenue and operates in two segments: oncology systems and imaging components.

### Japan / manufacturing sector / ALPHV

The BlackCat / ALPHV ransomware group claimed responsibility for breaching Japanese watchmaker Seiko's network and exposing the stolen data on their leak site. Seiko employs roughly 12,000 people and has an annual revenue that surpasses $1.6 billion.

### U.S. / education sector / NoEscape

Hawai'i Community College, part of the University of Hawai'i (UH) with over 50,000 students, suffered a ransomware attack and shut down IT systems to prevent the malware strain from spreading. The NoEscape ransomware gang threatened to publish 65 GB of stolen data unless a ransom was paid, prompting UH to negotiate with the cybercriminals to protect the data. After determining that approximately 28,000 individuals' data might have been compromised, UH made the difficult decision to pay the ransom to safeguard their sensitive information.

### Canada / manufacturing sector / Akira

Yamaha's Canadian music division confirmed a cyberattack after two separate ransomware groups claimed responsibility. Yamaha Canada

was first listed as a victim of BlackByte. Later, Akira ransomware also included Yamaha Canada on its leak site.

Yamaha Canada Music, a wholly owned subsidiary of Yamaha Corporation, a Japanese manufacturing giant with revenue of $3.34 billion, promptly implemented measures to contain the attack and collaborated with external specialists and IT teams to prevent significant damage.

**Poland / medical / RA Team**

ALAB Laboratories, a prominent player in Poland's medical laboratory sector, experienced a major cyberattack orchestrated by the relatively unknown cybercriminal gang, RA Team. The gang disclosed snippets of the pilfered data on its blog, including results from over 50,000 medical studies. RA Team claims to have extracted 246 GB of data, including lab reports, customer details, legal papers, financial information and business contracts.

**U.K. / insurance / LockBit**

Sabre Insurance, a U.K. motor insurance firm, fell victim to a ransomware attack that led to a data breach, with the accessed information characterized as "noncritical" and linked to archived data. Preliminary investigation results indicate that the breach originated from an IT management company that provided technical services to Sabre. LockBit claimed responsibility, posting six images as proof on its leak site and demanding $900,000 in exchange for the destruction and download of the compromised data.

**Japan / U.S. / entertainment / Rhysida**

Sony, the parent company of Insomniac Games, experienced a data breach after being hit by the Rhysida ransomware gang. Rhysida has since leaked developer passports, internal emails, personal information and more. Also leaked to the dark web were internal screenshots from a Wolverine game that is still in development, including annotated screenshots and character art of Marvel characters.

**Japan / Germany / financial / Medusa**

Toyota Financial Services (TFS), with revenue of $4.6 billion, issued a warning to customers regarding a data breach that exposed sensitive personal and financial information. TFS, a global subsidiary of Toyota Motor Corporation operating in 90% of Toyota's car markets, confirmed unauthorized access to its systems in Europe and Africa in November. The Medusa ransomware group demanded an $8 million payment within 10 days of the breach for data deletion. Toyota took certain systems offline to contain the breach, impacting customer services. The breach affected divisions like Toyota Kreditbank GmbH in Germany, compromising data such as full names, addresses, contract details, lease-purchase information and IBANs.

**Italy / MSP / LockBit**

Italian cloud service provider Westpole, specializing in digital services for public administration, suffered a significant cyberattack affecting its customer, PA Digitale, disrupting services for 1,300 public administrations, including 540 municipalities. The attack, attributed to LockBit 3.0 ransomware, led to manual operations in several municipalities, impacting salary payments. While the Italian cybersecurity agency recovered data for over 700 entities, restoring the remaining 1,000 public administrations remains challenging, raising concerns about Westpole's ability to fully recover and fulfill obligations to affected public administrations.

### U.S. / Australia / manufacturing / Hunters International

Austal USA, a shipbuilding company with $1.585 billion in annual revenue and more than 4,300 employees, confirmed a cyberattack in December. Hunters International, a recent ransomware-as-a-service operation, claimed responsibility for the attack. As a contractor for the U.S. Department of Defense (DOD) and the Department of Homeland Security (DHS), the Australian-based company specializes in high-performance aluminum vessels. Its American subsidiary, Austal USA, under contract for U.S. Navy programs, including building $360 million worth of Independence class littoral combat ships, stated that it quickly mitigated the incident, involving regulatory authorities like the FBI and NCIS. While no personal or classified information was accessed, Hunters International threatened to release more stolen data, including compliance documents and finance details. Hunters International denies theories of its affiliation with the Hive gang, asserting a focus on data theft for extortion rather than encryption.

### U.S. / MSP / ALPHV

Confirmed through leaked screenshots of stolen data, IT services and business consulting firm HTC Global Services acknowledged a cyberattack by the ALPHV ransomware gang. Despite not posting an official statement on their website, HTC issued a brief announcement on Twitter, assuring active investigation and resolution efforts to safeguard user data integrity. The cyber incident, which exposed passports, contact lists, emails and confidential documents, is speculated to have exploited the Citrix Bleed vulnerability, particularly affecting HTC's business unit and CareTech.

### Germany / finance / energy / Cl0P

Deutsche Bank AG, one of the largest banks in the world, with total assets of $1.5 trillion and $6.3 billion in annual net income, confirmed that a data breach occurred with one of its service providers. The breach is likely associated with a data theft attack by the Cl0P ransomware group exploiting a

MOVEit Transfer vulnerability. The incident resulted in the exposure of customer data in Germany for those who utilized the service provider's account-switching service in 2016, 2017, 2018 and 2020.

Siemens Energy, a Munich-based energy technology company with $32 billion in annual revenue, also confirmed a data breach in the Cl0P ransomware data-theft attacks exploiting a zero-day vulnerability in the MOVEit Transfer platform.

### U.S. / services / Cl0P

Maximus, a U.S. government services contractor, disclosed a data breach in which attackers stole the personal data of 8–11 million individuals during recent MOVEit Transfer data theft attacks. With a presence in the U.S., Canada, Australia and the U.K., Maximus employs 34,300 people and has about $4.25 billion in annual revenue,

The breach occurred due to a zero-day flaw in the MOVEit file transfer application, which is known to be widely exploited by the Cl0P ransomware gang. Despite immediate isolation of the affected environment, the attackers had access to compromise a significant number of individuals.

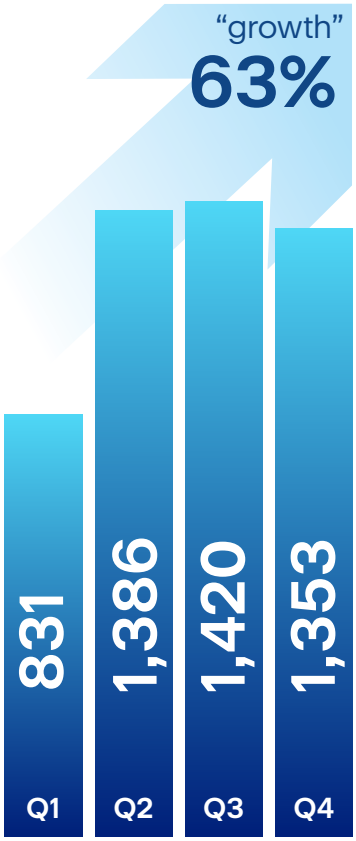
The Cl0P ransomware group is behind one of the biggest attacks in 2023. In the span of just three months, the MOVEit vulnerability, exploited on May 27, 2023, wreaked havoc. By the end of 2023, it impacted more 2,600 organizations and 85 million individuals, with a financial toll exceeding approximately $9.93 billion — equivalent to the annual revenue of a midsized Fortune 500 company. The exploited MOVEit vulnerability, rooted in an SQL injection flaw enabling remote code execution, allows unauthorized users to gain remote access to the MOVEit server environment without authentication, enabling attackers to deploy webshells or malicious scripts on MOVEit servers.

## MOVEit cyberattack — Affected organizations

(as of December 20, 2023)

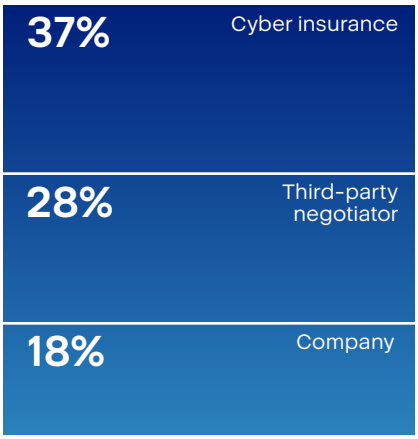
| | |
|---|---|
| U.S. | 2,290 |
| Canada | 152 |
| Germany | 40 |
| U.K. | 25 |
| Puerto Rico | 12 |
| Netherlands | 10 |
| Switzerland | 9 |
| Ireland | 6 |
| Australia | 6 |
| Austria | 4 |

# Ransomware statistics

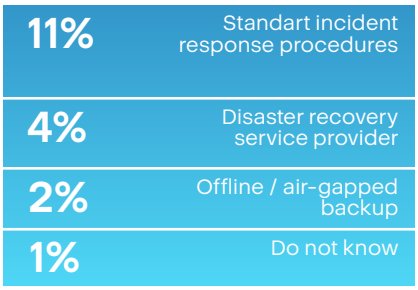



## Ransomware victims

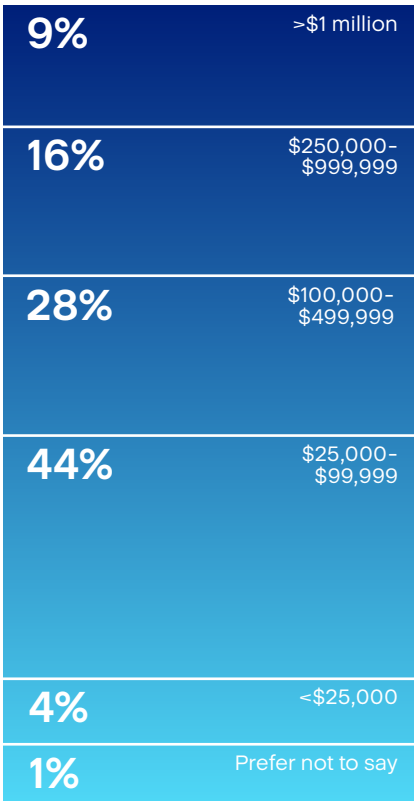
**Who paid the ransom?**




**How services were restored when the ransom was not paid**




## Ransomware remediation




## Ransomware payouts

www.splunk.com/en_us/newsroom/press-releases/2023/ciso-research-reveals-90-of-organizations-suffered-at-least-one-major-cyber-attack-in-the-last-year-83-report-ransomware-payments.html

**There were hundreds of other cases, 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 Cloud 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.
- Linux servers face inadequate protection against the cybercriminals who are increasingly exploiting them.
- Proper data backup, following the 3-2-1 rule, is a must for all organizations. Immutable backup space can often be the last line of defense.
- Attackers often manage to gain domain administrative rights and then uninstall security tools.

# 2. Attacks on MSPs are not slowing down

Managed service providers (MSPs) and managed security service providers (MSSPs) have become indispensable allies to businesses seeking robust IT infrastructure and cybersecurity. However, their utility and central position in the digital supply chain have also turned them into attractive targets for cybercriminals. As Acronis focuses on MSP and MSSP clients, we want to delve into the reasons MSPs and MSSPs are under constant attack, looming future threats, and defense strategies to mitigate risks.

## Cybercriminals put a bullseye on MSPs and MSSPs

MSPs and MSSPs offer centralized services to numerous businesses, from SMBs to large corporations. The scaling capabilities and efficiencies that make them a business asset also make them a single point of failure — an opportunity for cybercriminals to exploit multiple entities through a single attack. Additionally, MSPs often have elevated privileges in their clients' environments to perform regular maintenance, monitor security and manage IT resources, which, if compromised, can leave the door open for widescale IT disasters.

It's not easy to filter specific attacks on MSPs or MSSPs, as many of the stories never make it to the public or are listed as generic attacks against the end clients. A recent high-profile breach of Microsoft cloud email accounts belonging to multiple U.S. government agencies resulted in 60,000 emails being stolen from 10 U.S. State Department accounts. In September, Microsoft disclosed that it had identified additional flaws that enabled the China-linked threat actor Storm-0558 to compromise the cloud email accounts.

According to Microsoft, one flaw caused an Azure Active Directory key used in the compromise to be improperly captured and stored in a file following a Windows system crash. Another flaw resulted in the key not being detected. MSPs and MSSPs use Azure and its services extensively, and these service providers could very well become victims of similar attacks. Many service providers would not have been able to detect illegal access to their clients' emails due to lack of visibility.

## Why MSPs and MSSPs are attractive targets

### Centralized access

MSPs and MSSPs hold the keys to multiple kingdoms. They manage the IT and security infrastructure for multiple clients, providing cybercriminals with numerous potential victims through one point of penetration. A successful breach could grant access to valuable data from multiple organizations contained within a service provider's networks.

### Broad impact potential

With access to a wide array of clients, attackers can launch more extensive ransomware campaigns, data breaches and espionage efforts. The attack surface is expansive, and the impact is substantial when considering the number of businesses that could be affected by a single breach at an MSP or MSSP.

### Resource constraints

Though they handle IT operations and security, MSPs often work with limited resources — this is especially true of smaller service providers. Cybercriminals rely on the notion that not all MSPs have the state-of-the-art

security layers required to defend against sophisticated attacks, making them softer targets compared to larger corporations with dedicated security teams.

### Insider threats

Most cyberattacks include a human element. With numerous employees having access to high-level permissions across client systems, the risk of insider threats at an MSP or MSSP, whether malicious or accidental, increases significantly.

## Future threats to anticipate

The digitization trajectory and the reliance on MSPs and MSSPs continue to rise. Similarly, the spectrum of threats is evolving. Ransomware and phishing attacks remain prevalent, but more advanced tactics like supply chain attacks, AI-driven attacks and state-sponsored incursions are likely to intensify.

MSPs should brace themselves for threats unique to their operations, including "island hopping," in which attackers use an MSP's infrastructure to attack clients, as well as "credential stuffing," which exploits an MSP's broad access to systems.

## Protective measures and preventative strategies

### Adopt a zero trust security model

MSPs should consider the principle of "never trust, always verify." Implementing zero trust security measures involves strict identity verification for every person and device attempting to access resources within a network, regardless of whether they sit within or outside of the network perimeter.

### Enhance monitoring and detection

Continuous and comprehensive monitoring of network traffic, user behaviors and anomaly detection can provide early warnings of potential breaches. Investing in extended endpoint detection and response (XDR), security information and event management (SIEM) systems, and machine learning-based solutions can lift some burdens off technical staff and provide more advanced analysis. For smaller MSPs, managed detection and response (MDR) services — which Acronis provides with Advanced Security + EDR — are a must.

### Regularly update and patch infrastructure

Cybercriminals often exploit known vulnerabilities that have yet to be patched by MSPs. Ensuring that all systems, applications and components are updated is a critical step in the battle against cyberattacks.

### Educate staff and cultivate a security-first culture

Human error remains one of the greatest vulnerabilities in any organization. Regular training on current threats, phishing prevention and the importance of a cautious approach to all communications can significantly reduce the risk of breaches.

### Multifactor authentication (MFA)

Implementing MFA in MSP and MSSP environments is a must. It is a critical layer of security that makes it harder for attackers to gain access, even if they have obtained credentials.

### Develop and practice incident response plans

Having a strategic and tactical response plan for when incidents do occur is crucial. Regularly practicing these plans through simulations can ensure readiness and minimize damage if an actual breach occurs.

## What MSPs should pay attention to

Running an MSP or MSSP safely and successfully also requires additional security measures. Here are just a few:

### Regulatory compliance and data privacy

Keeping abreast of changes in regulations and ensuring compliance not only improves security but also protects MSPs and MSSPs from legal repercussions in the event of a breach.

### Insider risk management

Reducing the number of employees with access to high-level permissions, implementing a solid onboarding and offboarding process and routinely auditing user activity can help mitigate insider risks.

### Client security requirements

Service providers must understand and manage the unique security needs of different clients. Customized security postures tailored to the specific operational and regulatory landscapes of clients can help MSPs and MSSPs provide better defense.

## Conclusions and recommendations

The cybersecurity landscape is riddled with dangers. As MSPs and MSSPs continue to be the bedrock upon which businesses operate and secure themselves, they must also elevate their security measures. This means not only preparing defenses against present threats but also forecasting and inoculating against future challenges. A collaborative approach that includes engaging with cybersecurity communities to share threat intelligence, adopting innovation in security practices, and relentlessly pursuing the highest security standards is fundamental for MSPs and MSSPs navigating the volatile threat landscape.

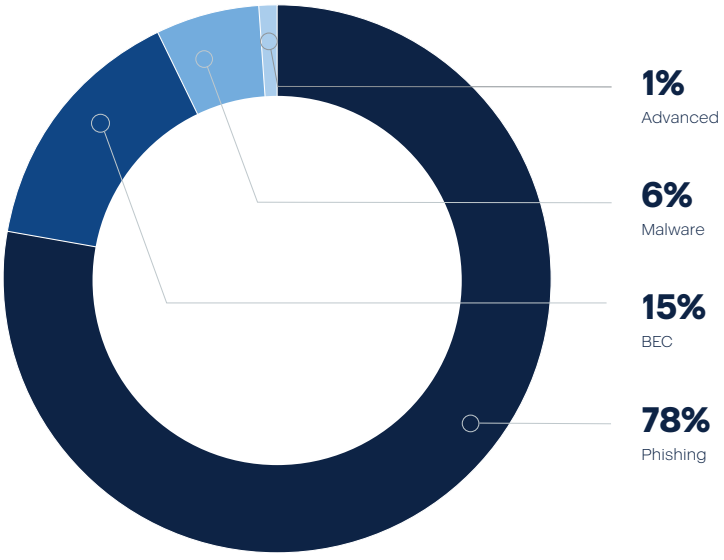
As cybercriminals refine their methods, the adage "the best defense is a good offense" could not be more pertinent. For MSPs and MSSPs, it is crucial to strike a balance between robust defensive measures and proactive threat hunting to provide the secure operational framework their clients rely on. This will not only ensure their survival but will also fortify the digital security landscape against the relentless tides of cyberthreats.

# 3. Phishing and malicious emails remain the main vectors of infection

The following 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 from email-borne threats. The data was gathered for the second half of 2023 and combined with Acronis telemetry data for malware and URL blocks on the endpoints.

The overall number of email-based attacks detected in 2023 increased 222% compared to the second half of 2022, while the number of attacks per organization within the same time frame increased 54%. These statistics underscore the escalating threat landscape — with email being the main attack vector — and the urgency for organizations to fortify their defenses against malicious activities.

The not surprising fact is that 91.1% of organizations have already faced AI-enhanced phishing.




**8 out of 10 emails are phishing emails**

In 2023, each scanned email contained, on average, 2.7 files and URLs. Any of these could potentially pose a threat to an organization. And as expected, in 2023 we've observed a 15% increase in the number of files and URLs per scanned email. 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.

One out of 76, or 1.3%, of received emails were malicious in H2 2023. Phishing was the number one email threat, representing 78% of malicious emails. Business email compromise (BEC) / social engineering, however, increased from 3% to 15% compared to the same period last year, making it the second most common email threat. Malware, the third most common email threat, represented 6% of malicious emails, down from 18% in H2 2022.

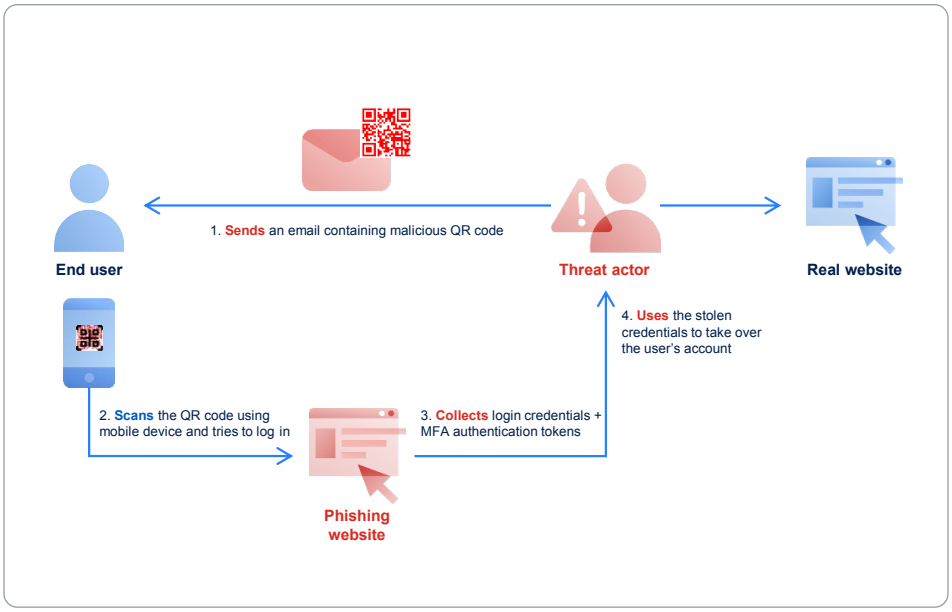
## Phishing examples and trends

Phishing remains a preferred tactic for cybercriminals seeking to infiltrate systems, with notable cases identified by Acronis and other cybersecurity researchers during the second half of 2023. Additionally, quishing, a new form of phishing that utilizes QR codes, introduces new challenges where QR code-based attacks are harder to detect. The simplicity and effectiveness of QR code exploitation, coupled with users' distraction on mobile devices, make it an attractive avenue for attackers to embed malicious URLs, initiate phishing attacks and exfiltrate data. As quishing gains traction, individuals and organizations are urged to exercise caution, scrutinize codes for alterations and employ security measures to mitigate the evolving risks posed by QR code exploits.

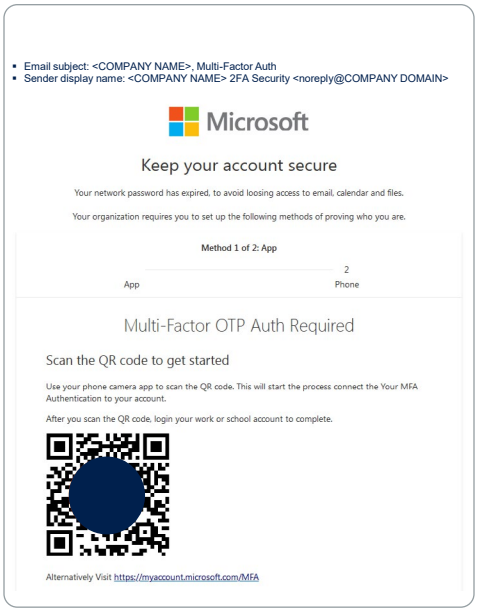
The number of quishing attacks showed that one out of eight emails with a QR code is malicious. In the second half of 2023, 15% of all emails that contain QR codes were quishing attacks.

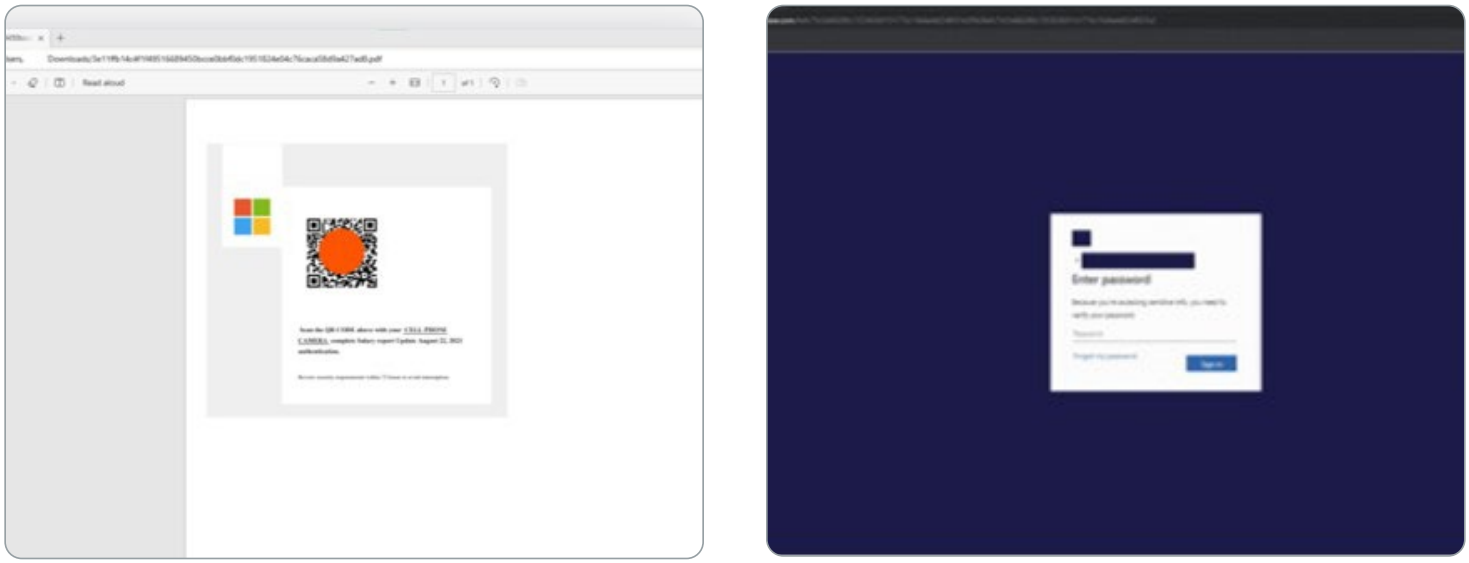
A recent quishing campaign targeted multiple recipients across various organizations. Impersonating Microsoft 365 via email, threat actors notified end users that their "network password" had expired. Users were prompted to scan a QR code with their mobile camera to enable a purported MFA method for their Microsoft account. The phishing emails were highly targeted, with email subjects and senders carefully tailored to the target company. Featuring a single image containing text, logos and the QR code, the emails lacked any textual data in the body. Individuals falling victim to the scam would be directed to a deceptive Microsoft-themed page designed acquire their account credentials through a fake login.

**Example 1. Scan and type your password**




**Example of phishing email with QR code**

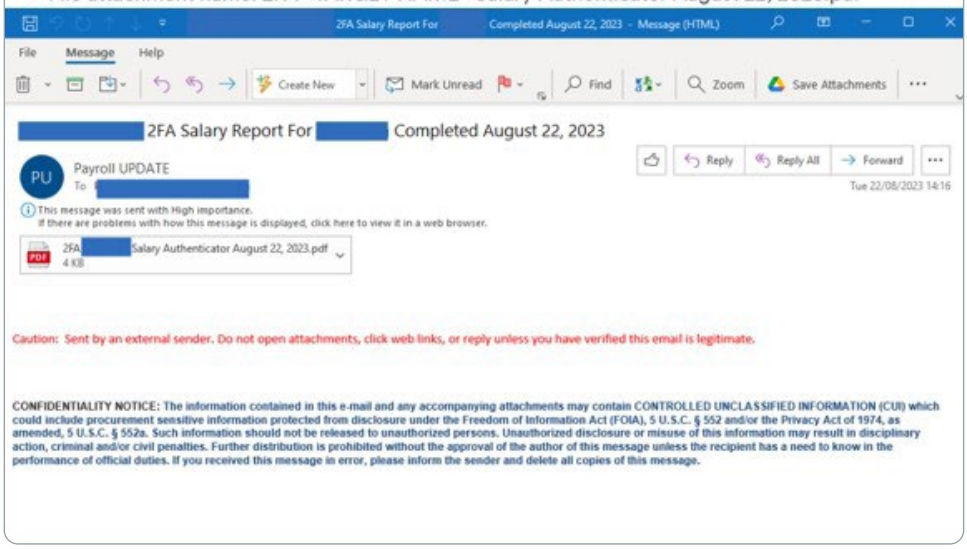


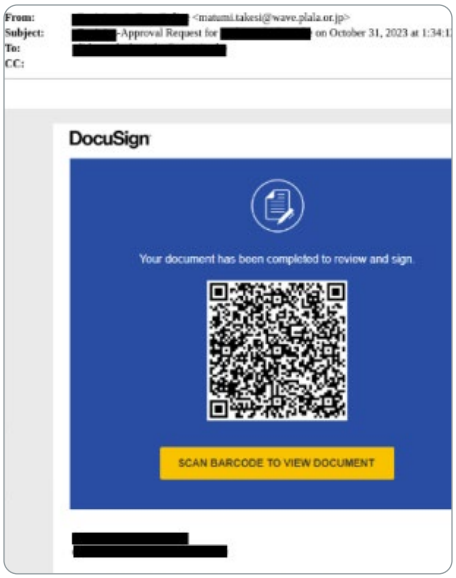


**Example 2. Quishing with QR code in PDF**

In below quishing example, a malicious QR code is concealed within a PDF attachment. The threat actor lures recipients with a phishing email purporting to be related to salary and payroll — a common social engineering tactic. In the PDF, the user is asked to scan the QR code to authenticate their Microsoft account and complete a "salary report."

- Email subject: <COMPANY NAME> 2FA Salary Report For <TARGET NAME> Completed August 22, 2023
- Sender display name: Payroll UPDATE
- File attachment name: 2FA <TARGET NAME> Salary Authenticator August 22, 2023.pdf




**Example 3. Malicious QR code in DocuSign approval request**

Anti-phishing defenses and strong authentication, as well as an overall multilayered approach to cybersecurity, are critical to fighting email-based attacks. If phishing threats aren't blocked at the time of delivery, it's important to have other detection technologies in place that can stop the malware later in its cycle. This so-called shift-left paradigm has grown in importance in cybersecurity.

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.

# 4. Data breaches continue to dominate

In 2023, the cybersecurity landscape continued to be marred by significant data breaches, affecting a variety of sectors and highlighting the relentless threat posed by cybercriminals. Despite the advancements in security products and controls, attacks have persisted, bringing to the fore the evolving nature of cyberthreats. As noted in our mid-year 2023 report, data breaches are often associated with ransomware attacks, but this is not the only way data is breached. Data is often exfiltrated silently during attacks and later sold on the dark web or underground forums.

The main instruments of data exfiltration are information stealers. Their functionality varies, but they are generally created to handle specific types of data extraction. Some information stealers contributed to both large and small incidents we observed in the second half of 2023. The number of data breaches increased toward the end of the year and included significant data leaks. We recorded more than 1,500 incidents, but this number represents only publicly disclosed cases. The number of breached records (and the record roughly can be connected to a user / human here) exceeded six billon, with the FarkBeam leak alone representing nearly four billion records.

Let's examine some cases from midsummer. In July, a cybersecurity researcher reported a data breach at

Indonesian Immigration Directorate General affected more than 34 million Indonesian citizens. The leaked data included passport data, including full names, passport numbers, expiration dates, dates of birth and gender. The leaked data probably included National Identity Community Identity Card (NIKIM) information, a digital identity used to secure electronic passports containing personal data such as names, addresses and identity numbers. The Indonesian Immigration Directorate General disputed the nature of the data leaked online.

Also in July, U.S.-based health care giant HCA Healthcare experienced a data breach that impacted 11 million patients. HCA said the data appears to have been stolen from an external storage location exclusively used to automate the formatting of email messages. The dataset includes PII such as patient names, home addresses, phone numbers, dates of birth and gender.

In August, the Electoral Commission of the U.K. fell victim to a data breach. This complex attack involved unauthorized access to internal emails, its control system and copies of electoral registers, which contain voter data. The accessed data included the names and addresses of U.K. voters registered between 2014 and 2022, including those registered as overseas voters. The exact number of people impacted wasn't communicated, but it's estimated that the register for each year includes details of about 40 million individuals.

In September, DarkBeam, a U.K.-based cybersecurity company, was breached as a result of mishandling sensitive data. The breached data contained 16 collections, each housing 239,635,000 records. More than 3.8 billion records were breached, including pairs of login credentials — email addresses and passwords — from previously reported and unreported data breaches. DarkBeam had collected this information to alert its customers in case of a data breach. In the hands of cybercriminals, the breached data can be used to target others or break into associated accounts.

In October, 23andMe, a DNA testing company, experienced a significant data breach that revealed still existing vulnerabilities in the protection of sensitive genetic and personal information. Genetic data itself was not stolen. The breach exposed personal information, including names, birth years, sex and details about

genetic ancestry results. Initially, a hacker announced the breach, publishing the data of one million 23andMe users of Ashkenazi Jewish descent and another 100,000 users of Chinese descent. He later published records of four million more general accounts. In December, 23andMe confirmed that the breach was much worse: 5.5 million users were affected.

In terms of scale, the 23andMe breach was nothing compared to the Indian Council of Medical Research (ICMR) breach the same month, which affected 815 million Indian residents. Personal data was exfiltrated from the ICMR's Covid-testing database and offered for sale on the dark web.

The exfiltrated data included full names, ages, genders, addresses, passport numbers and Aadhaar numbers (12-digit government identification numbers). We do expect many identity theft cases and forged passports after such an incident.

**The data breaches of 2023 reinforce several critical cybersecurity tenets:**

- **Continuous monitoring and assessment**: Organizations must invest in real-time threat detection and routine system audits to identify vulnerabilities early and respond rapidly to potential breaches.
- **Robust defense mechanisms**: Businesses and organizations must deploy a multifaceted security strategy that includes end-to-end encryption, firewalls, intrusion prevention systems and secure access management.
- **Regulatory compliance and best practices**: Adhering to data protection regulations such as GDPR and HIPAA is not optional. Compliance ensures a basic security standard is in place while protecting the organization from potential legal penalties.
- **Employee training and awareness**: Human error remains a significant contributor to data breaches. Regular training on security best practices is essential to empower employees to act as the first line of defense.
- **Incident response planning**: Having a tested incident response plan in place is crucial for minimizing the damage caused by a breach. Quick and decisive actions can mitigate risks and restore operations faster.

The numerous data breaches of 2023 serve as a reminder of the continuous risks in our connected world. As cyberthreats evolve, so must our defenses. By learning from these incidents, organizations can better prepare themselves to protect their most valuable assets: their data and their customers' trust.

# 4. The AI menace: Cybercriminals embrace malicious AI-based tools for corporate attacks

AI promises a future of efficiency and breakthrough innovations; however, just as technology has evolved to aid and augment human capabilities, so too has its potential for misuse. In recent years, a darker side of AI has emerged, wherein cybercriminals exploit intelligent tools to scale up sophisticated attacks on corporate entities. And the public release of ChatGPT one year ago escalated the threat.

## The rise of malicious AI-based cyberattacks

The adoption of machine learning and AI by cybercriminals has led to the development of highly sophisticated attack methodologies. AI's ability to learn and adapt makes it a potent tool for executing attacks that can evade standard detections and countermeasures. The result is a significant shift in the threat landscape, challenging companies to rethink their security strategies.

# AI-powered threats

### 1. Spear phishing and AI-generated social engineering attacks

Using AI, cybercriminals can automate custom phishing campaigns that are incredibly convincing. Natural language processing (NLP) tools can now draft phishing emails that mimic the tone, style and vocabulary of genuine communications from trusted sources. Likewise, AI algorithms can analyze an individual's online behavior to tailor deceptive messages that the recipient is more likely to trust and act upon.

### 2. Deepfake technology for impersonation

Deepfake technology uses AI to create convincing audio and video forgeries. Cybercriminals leverage this technology to impersonate senior executives in CEO fraud attacks, tricking employees into transferring funds or disclosing sensitive information. Such AI-altered content is becoming increasingly difficult to distinguish from authentic media, upping the ante for corporate security teams.

### 3. Automated exploit development

AI systems can rapidly analyze software and systems for vulnerabilities faster than human cybersecurity teams. Automated testing tools powered by AI can identify zero-day vulnerabilities which can then be exploited before companies have time to patch and protect against them.

### 4. Adaptable malware

Malware typically has a static behavior pattern, making it detectable by traditional security solutions. However, with the integration of AI, malware can now dynamically adjust its operations to evade detection, learn from environmental interactions or even deactivate if it detects a sandbox environment.

### 5. AI-powered botnets

Cybercriminals are using AI to create more autonomous botnets that can optimize their attack patterns in real time. These botnets are harder to detect and shut down because they constantly evolve and seek new vulnerabilities in systems to exploit.

# Case studies: AI abuse in cyberattacks

Only a few years ago, the infamous "DarkSide" ransomware group reportedly utilized AI-based translation services to localize ransom messages, improving their efficacy in non-English-speaking countries.

Cybercriminals abuse generative AI services like ChatGPT but also have developed malicious AI tools such as WormGPT and FraudGPT, which are marketed on illicit web forums with claims they leverage unique large language models (LLMs) especially developed for criminal purposes. The tools are being

offered often on a subscription basis. They're similar to popular LLMs but without guardrails and are trained on data selected to enable attacks, which is hard to confirm but still can be the case.

WormGPT, developed in 2021, is an AI module based on the GPTJ language model, and is already being used in BEC attacks and for other nefarious uses. Users can simply ask the service to write an email purporting to come from a bank that's designed to trick the recipient into divulging their login credentials. WormGPT then produces a unique and usually grammatically perfect email that's far more convincing than what most attackers could write on their own.

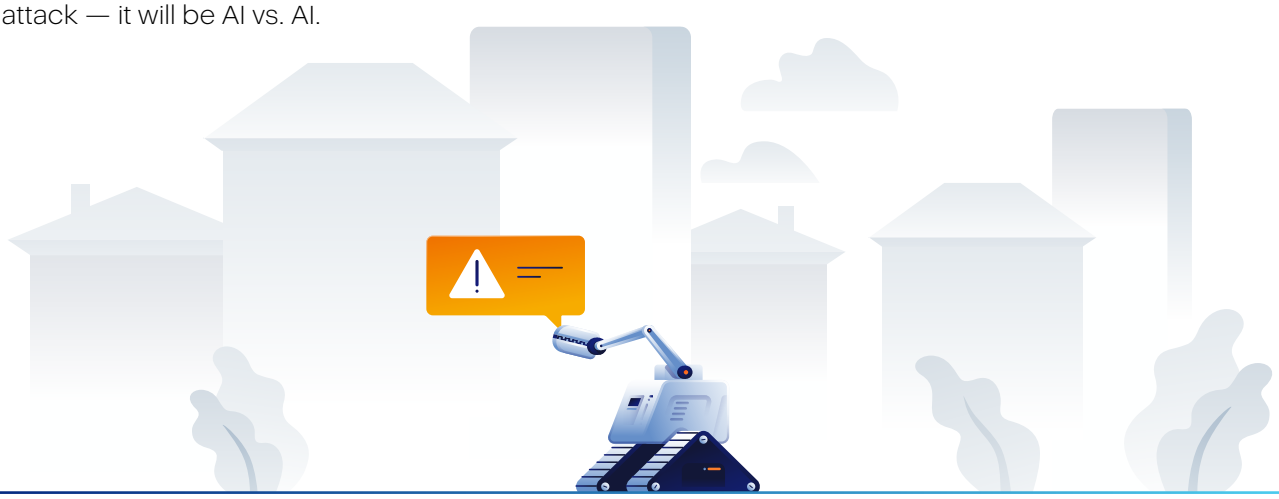
WormGPT inspired other similar tools, most prominently FraudGPT — a tool similar to WormGPT and used to create malicious content, such as phishing emails and cracking tools, or to conduct hostile activities, such as carding. Other malicious AI tools include DarkBERT, DarkBART and ChaosGPT. Developed by a South Korean company called S2W Security and trained on dark web data, DarkBERT is designed to combat cybercrime, but like ChatGPT, it is now being exploited for malicious purposes.

Another example of malevolent AI usage is the Mylobot botnet, that incorporates various evasion tactics and exhibits the potential for further adaptation based on AI integration, highlighting the shift towards intelligent malware development. Needless to say, Mylobot is currently quite active and not easy to detect by security products.

# The future: A new cybersecurity arms race

As AI tools become more sophisticated, so must the defense mechanisms against them. The cybersecurity sector is now in an arms race with malicious actors, each side using increasingly advanced AI to outwit the other. Companies must be prepared to engage in a continuous process of learning and evolving their security protocols to outpace the adaptive nature of malicious AI. This includes efficient and automated threat protection and recovery. As in some incidents, there will not be enough time for a human analyst to react to the attack — it will be AI vs. AI.

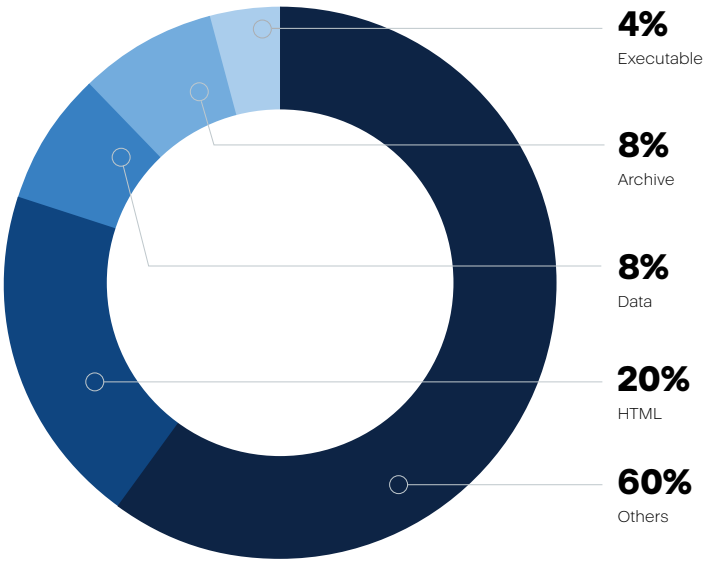
While it's imperative to develop technologies that can identify and defend against these advanced threats, equal importance must be given to establishing a corporate culture of security awareness, one that is prepared to face adversaries armed with AI. As we advance into an era in which AI capabilities will only expand, remaining vigilant and adaptable in the face of these intelligent threats will be the cornerstone of corporate cybersecurity.



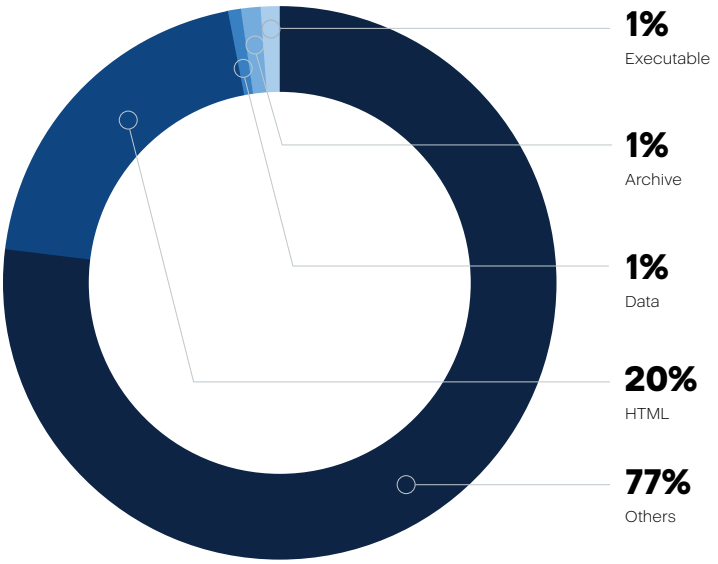
# 2

# General malware threats

In January, about 8.9% of our customers had at least one malware attack successfully blocked on their endpoints. Malware attacks peaked at 18.3% in October and declined to 13.5% in December. These high percentages suggest that, despite corporations' attempts at awareness training and patching, about one 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.




Malware types detected in the last two weeks of May 2023 (source: av-test.org)




Windows file types detected in the last two weeks of December 2023 (source: av-test.org)

| Month in 2023 | Percentage of clients with blocked malware |
|---|---|
| January | 8.9% |
| February | 9.0% |
| March | 10.5% |
| April | 8.5% |
| May | 8.9% |
| June | 10.5% |
| July | 12.4% |
| August | 12.9% |
| September | 16.3% |
| October | 18.3% |
| November | 17.9% |
| December | 13.5% |

The most common malware type is the Trojan Horse, making up more than half of the blocked threats. Below is a list of the most commonly seen malware families for H2 2023, with a clear focus on bots and information stealers:

- RedLine Stealer
- Remcos
- Agent Tesla
- njRAT
- FormBook
- Lumma
- Vidar
- Emotet
- Raccoon Stealer
- Smoke Loader

Since Q4 2022, we've seen a 50% increase in the number of new malware samples appearing in the wild. The independent malware testing lab AV-TEST recorded 219,741 new malware samples per day in Q1 2023, compared to 162,430 in Q4 2023.

This proportion matches the number of new samples seen by the Acronis CPOCs. This decrease could be the result of some spikes at the end of last year as well as more targeted distribution methods of malware — for example, through malware droppers and distribution networks.

The average lifespan of a malware sample in June 2022 was a mere 2.3 days, after which it disappeared and was never seen again by us. In December 2023, 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, 73% were seen only once across our customer base.

Singapore, Spain and UAE were among the focus countries with the most customers experiencing malware detections in December 2023.

Our security teams did numerous malware analyses during the second half of the year, but we would like to focus on a CustomLoader campaign. CustomerLoader was first spotted in June 2023 delivering different payloads to its targets. It is a .NET loader that obtained its name by the 'custom' string in its C&C communication. It probably works as malware as a service, offering its capabilities to other threat actors. At the time of analysis, it's been mostly used by infostealers and remote access trojans. In this campaign, CustomLoader used a .LNK file to bring the DuckTail infostealer to the victim's machines. DuckTail is a Vietnam threat group that became active in May 2023. It delivers malicious files to victims using phishing job offerings on Linkedin. Threat actors target users that are working in digital marketing, advertising and business, because of their value of their accounts on the underground forums.

As you can see, this is an advanced malware that can devliver various payloads. You can learn more about DuckTail by reading our full analysis, and find further malware analysis blogs at our Cyber Protection Operation Center.

## Key features of CustomLoader:

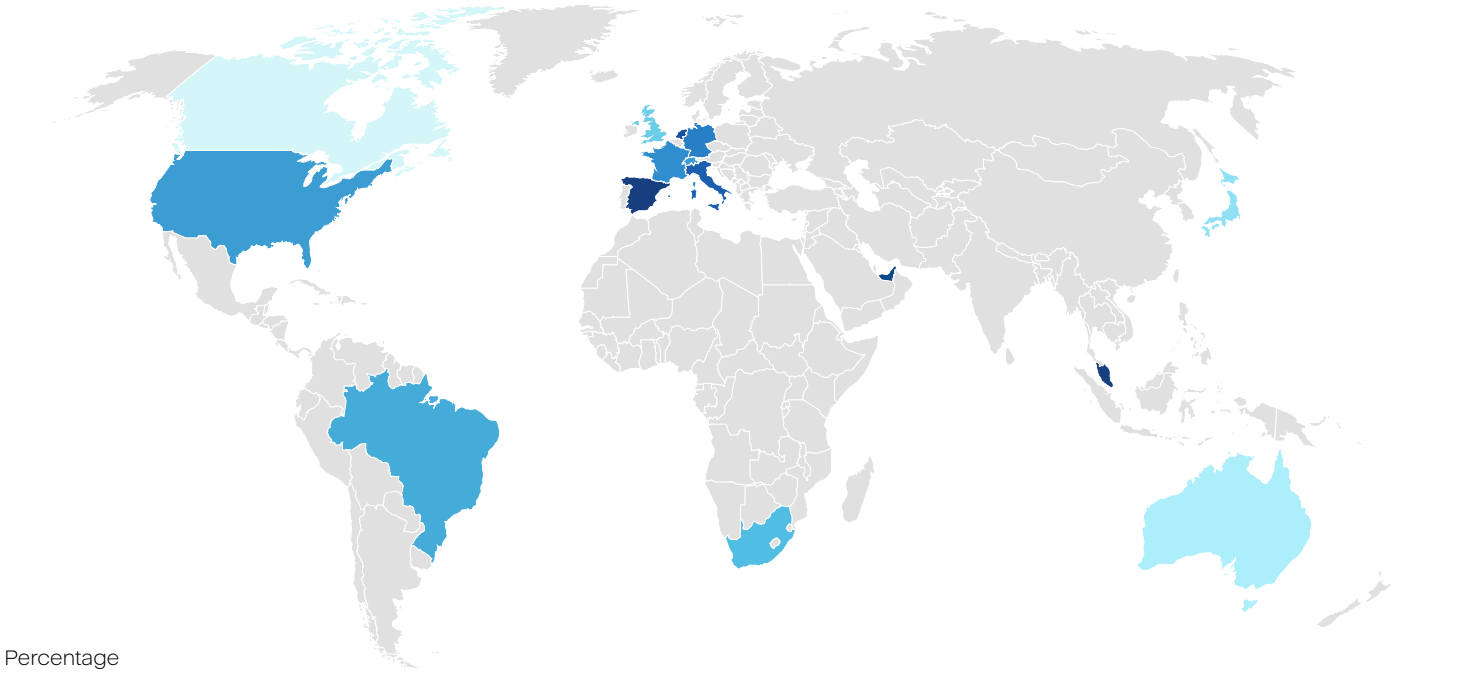
- Comes to victims as .lnk file which executes encoded command.
- Downloads C\C++ application, which drops a lot of .NET files.
- One of the .NET files extracts one more executable file.
- Last executable loads payload to the memory.
- Steals browser data.
- Uses Telegram API to exfiltrate data.

Although the main threat families in downloader, infostealer and ransomware did evolve in functionality, we haven't seen many new techniques. However, we occasionally see new threat methods, including the Go-based NKAbuse malware. It uses the New Kind of Network (NKN), which is a relatively new, decentralized, peer-to-peer network protocol leveraging blockchain technology. This allows the malware to communicate stealthily. The threat focuses on Linux and IoT devices and acts as a backdoor and DDoS tool.

## Monthly percentage of global detections by country

| Country | Detection rate in November | Detection rate in December | Normalized detection rate in December |
|---|---|---|---|
| Australia | 1.8% | 1.4% | 15.2% |
| Brazil | 10.2% | 8.6% | 22.3% |
| Canada | 5.5% | 4.7% | 9.2% |
| France | 3.6% | 4.3% | 21.0% |
| Germany | 8.4% | 8.0% | 21.6% |
| Italy | 5.6% | 6.1% | 23.4% |
| Japan | 2.8% | 2.5% | 16.6% |
| Netherlands | 1.2% | 1.5% | 27.6% |
| Singapore | 5.3% | 6.1% | 55.6% |
| South Africa | 1.2% | 1.2% | 18.0% |
| Spain | 2.8% | 3.1% | 41.3% |
| Switzerland | 3.6% | 3.6% | 20.2% |
| United Arab Emirates | 0.8% | 1.0% | 28.6% |
| United Kingdom | 4.5% | 4.5% | 17.3% |
| United States | 17.8% | 16.2% | 18.2% |

## Top 25 countries: Normalized malware detections, December 2023



If we normalize the number of detections per active client per country, then 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 December 2023.

**Top 10 countries: Normalized malware detections**

| Rank | Country | Percentage of clients with malware detections in December 2023 |
|---|---|---|
| 1 | Namibia | 74.5% |
| 2 | Bahrain | 59.6% |
| 3 | Serbia | 58.3% |
| 4 | Egypt | 56.3% |
| 5 | Singapore | 55.6% |
| 6 | Sri Lanka | 54.8% |
| 7 | Israel | 47.7% |
| 8 | Finland | 43.6% |
| 9 | South Korea | 42.4% |
| 10 | Republic of Moldova | 41.8% |

# Ransomware threats

Given the persistently high number and frequency of attacks, falling victim to ransomware is among the greatest concerns for individuals and organizations globally. Our ransomware data from July to December 2023 reveals the global rate of ransomware detections blocked / detected by our threat-agnostic Acronis Active Protection. Additionally, we have analyzed data made public on the underground leak sites of ransomware operators.

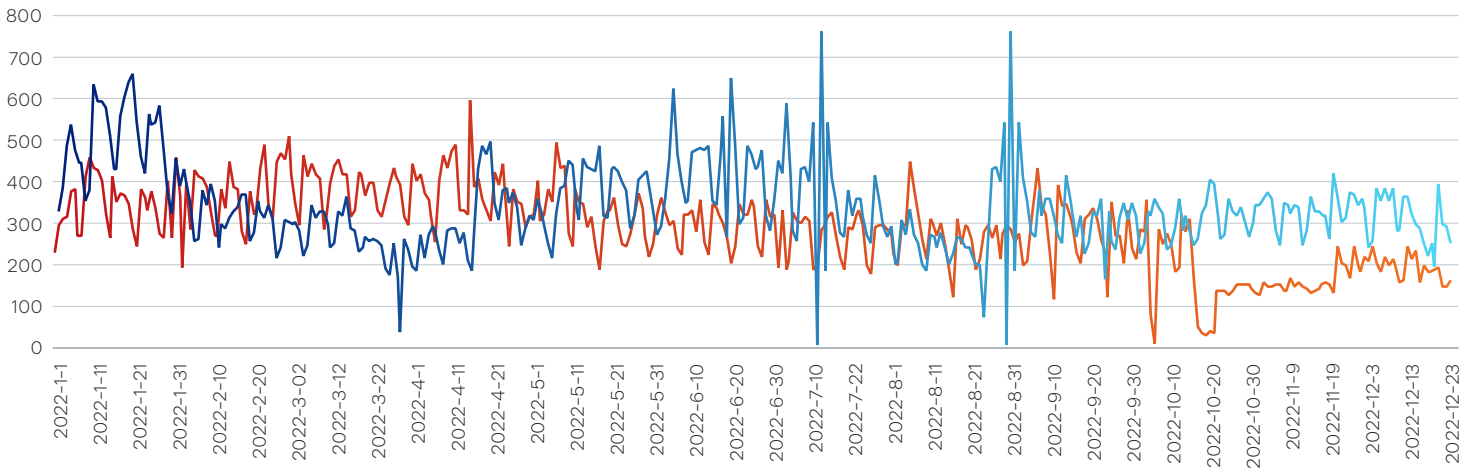
The situation is compounded by a significant increase in data breaches. These breaches often provide a treasure trove of sensitive information that can be exploited in ransomware attacks, further escalating the risk and impact. Moreover, the availability of LLMs like ChatGPT has enabled cybercriminals to automate and scale their attacks. This advancement in technology has not only increased the frequency of attacks but also expanded the ransomware market by introducing more players. Consequently, the landscape of ransomware threats is becoming more complex and challenging to navigate.

## Daily ransomware detections

The number of ransomware detections has decreased by 43% in Q4 2023 over Q4 2022. Since then, the number of monthly ransomware detections has stayed relatively flat for 2023.

The daily number of ransomware detections also appears to be relatively stable, with no significant spikes recently and a slight upward trend overall. This reinforces the importance of maintaining high resilience through the implementation of a multilayered cyber protection solution, 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**



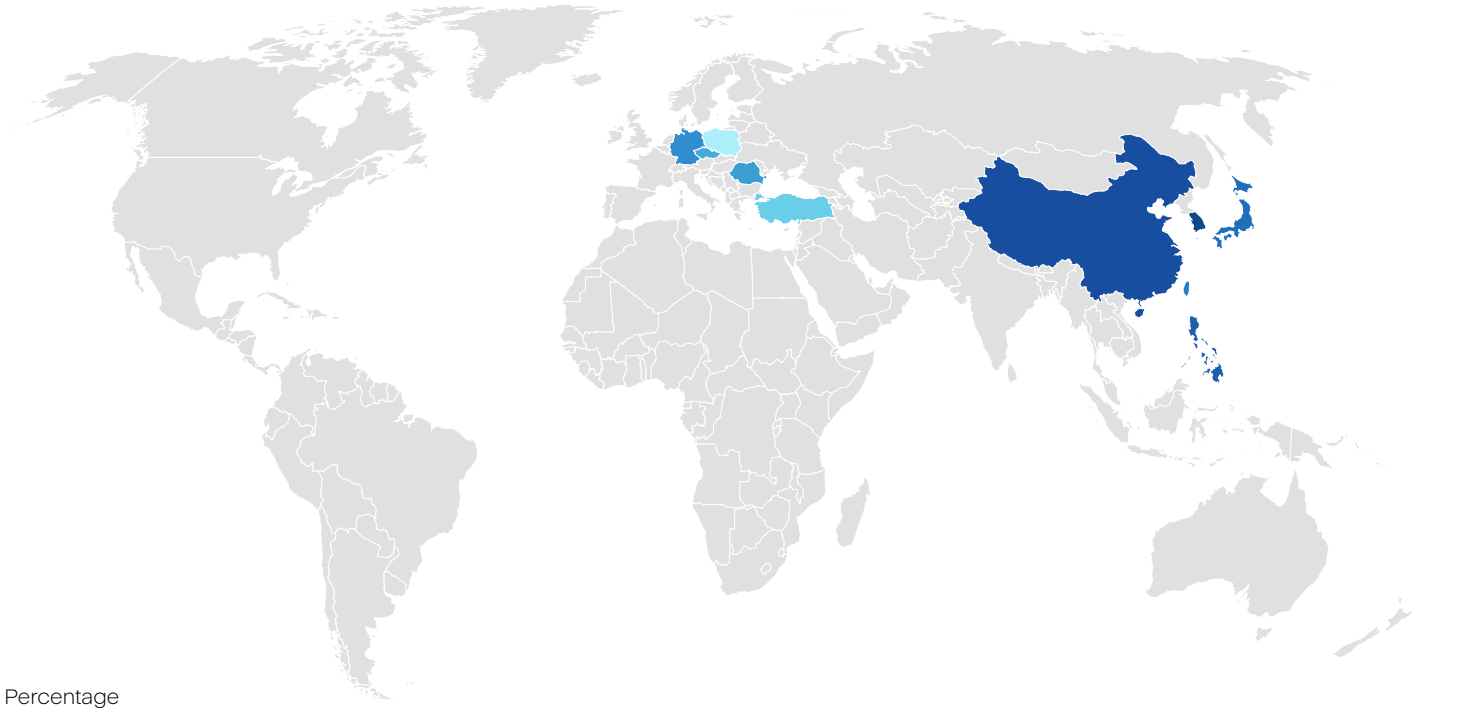
Ransomware detections peaked on April 18, while October 16 saw the lowest number of detections.

In the below chart, 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.

### Top 10 countries: Global ransomware detections by quarter, normalized

| Rank | Country | Global ransomware detection percentage in Q3 2023 | Global ransomware detection percentage in October 2023 | Global ransomware detection percentage in November 2023 |
|---|---|---|---|---|
| 1 | South Korea | 45.2% | 10.4% | 13.3% |
| 2 | China | 26.6% | 7.8% | 9.6% |
| 3 | Philippines | 18.9% | 6.8% | 7.3% |
| 4 | Japan | 13.9% | 3.1% | 4.2% |
| 5 | Taiwan | 10.7% | 3.4% | 3.3% |
| 6 | Germany | 9.3% | 2.4% | 2.9% |
| 7 | Romania | 7.7% | 1.9% | 2.8% |
| 8 | Czechia | 6.8% | 1.9% | 1.8% |
| 9 | Turkey | 4.9% | 1.9% | 1.9% |
| 10 | Poland | 5.3% | 1.8% | 1.5% |

### Top 25 countries: Normalized malware detections, November 2023



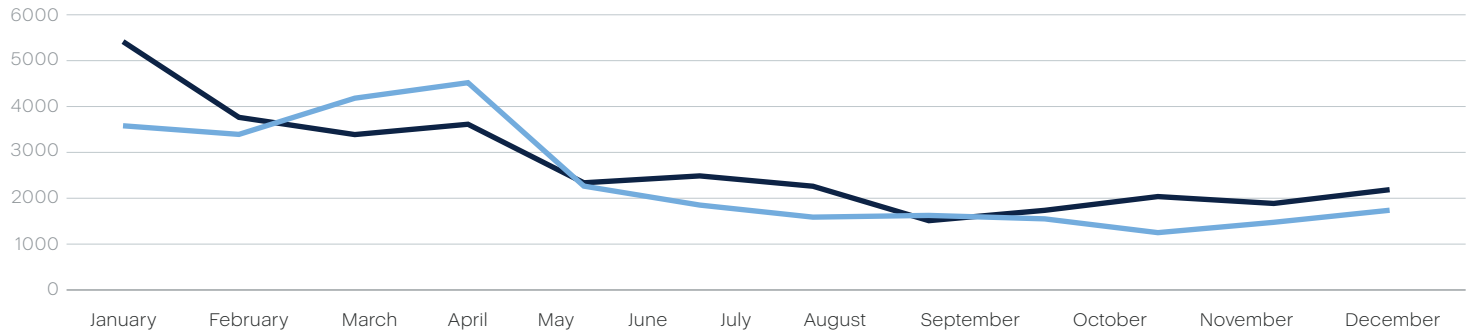
# Ransomware activity in focus countries

Cybercriminals don't discriminate — they target businesses of all sizes and in all industries.

Still, some groups have their preferred targets. In the second half of 2023, there were several cyberattack patterns that merit special attention in this report. The following graphs compare the monthly ransomware detections at the endpoint month over month.

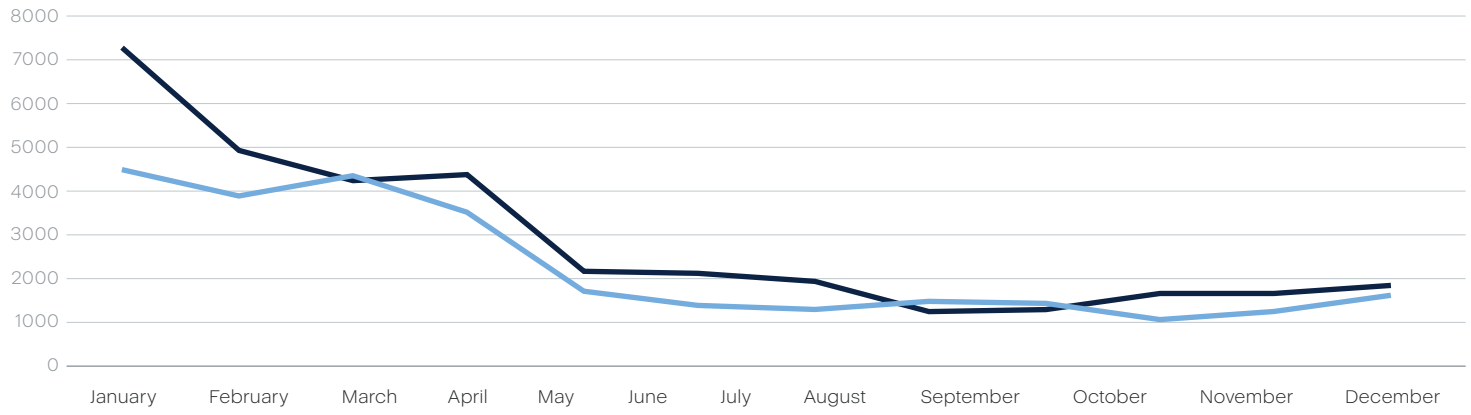
**U.S.**

**U.S. ransomware detections**



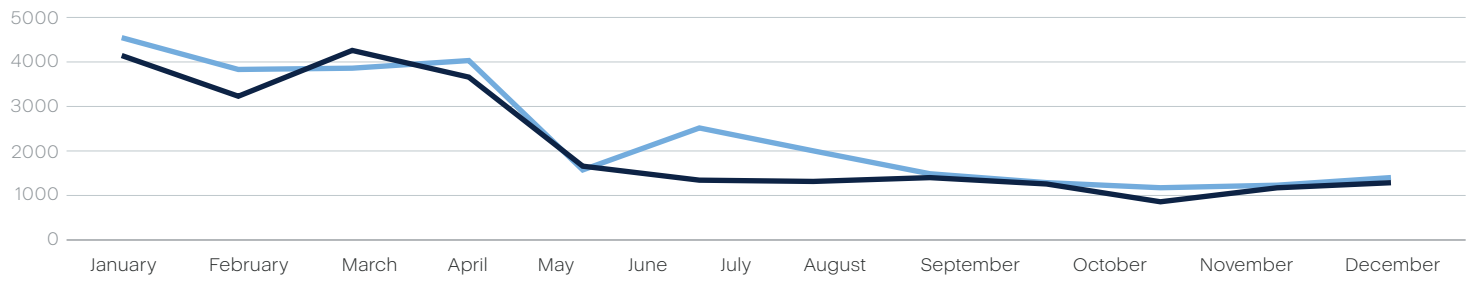

**Germany**

**Germany ransomware detections**



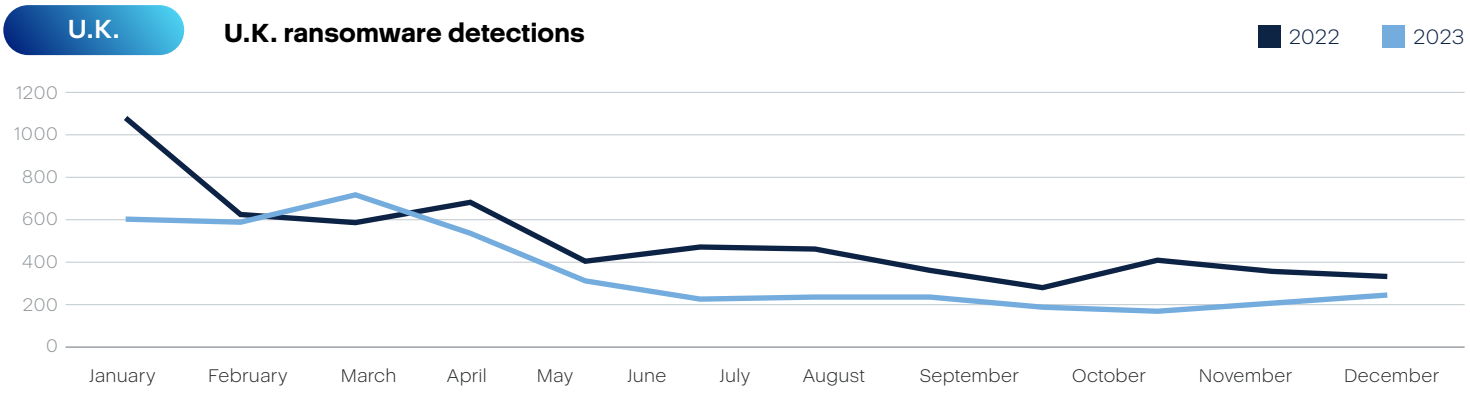

**Japan**

**Japan ransomware detections**



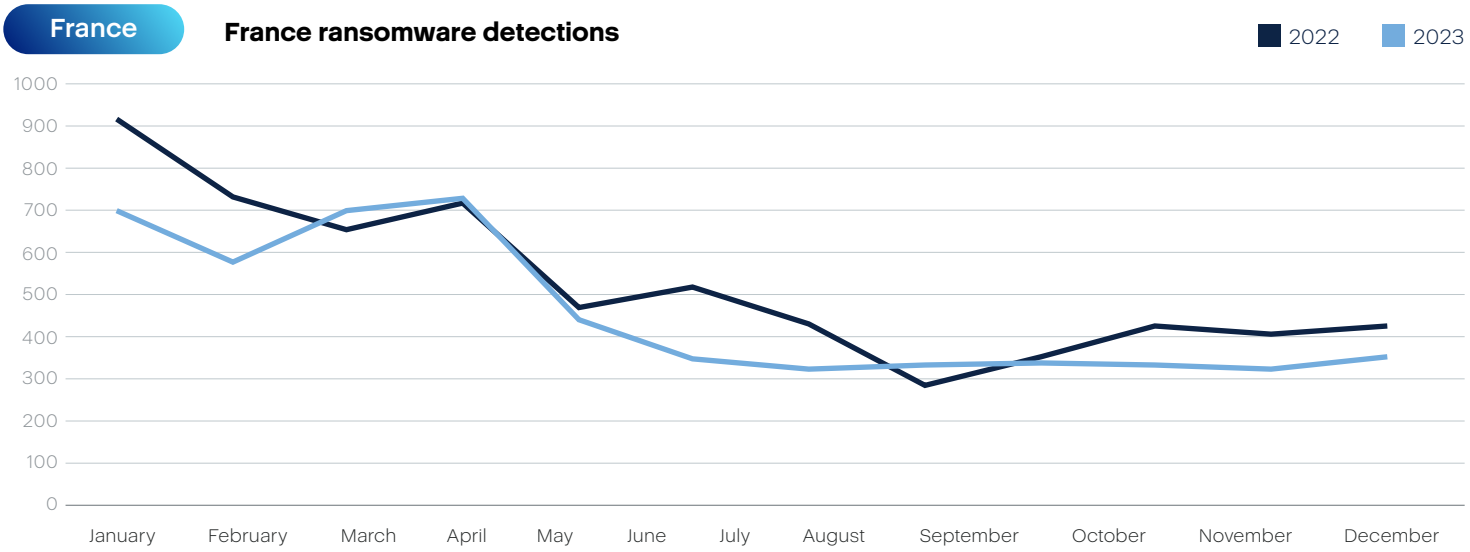
U.K.

**U.K. ransomware detections**



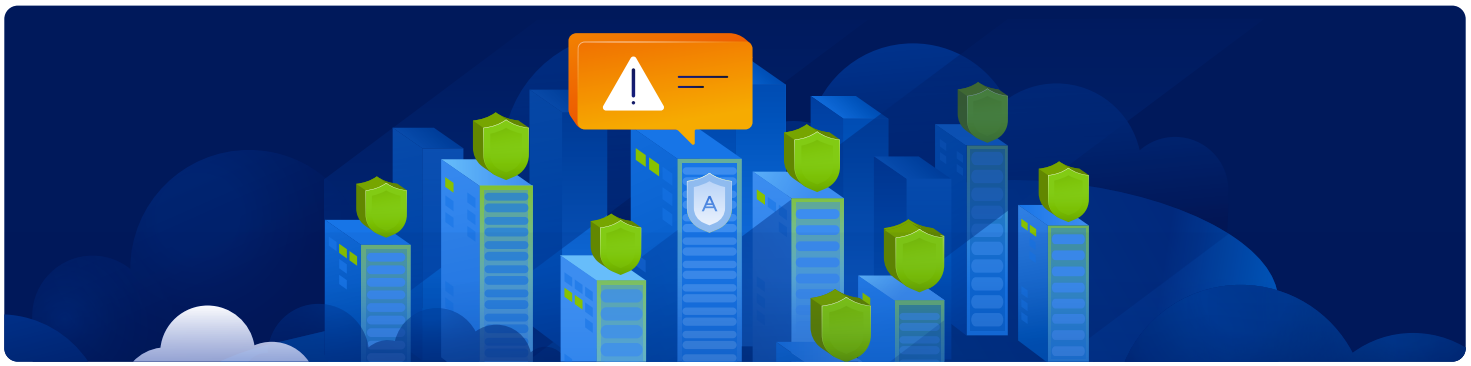

France

**France ransomware detections**




# Malicious websites

Acronis CPOCs blocked 27,292,197 phishing and malicious URLs in Q4 2023. This constitutes a 2% decrease compared to Q3 2023 (27,822,009). Despite improvements in email filtration and security software, cybercriminals persist in using malicious URLs to compromise systems, eluding basic defenses. These deceptive URLs, cleverly embedded in seemingly legitimate emails, still manage to deceive users — more than 30% of phishing emails successfully entice users to open them. Malicious email attachments, employing techniques like password-protected ZIP files and fake buttons within OneNote file attachments, underscore the need for a multilayered defense approach to effectively thwart evolving cyberhreats.



| Month | Blocked URLs | Total for the quarter |
|---|---|---|
| January | 17,160,862 | |
| February | 14,898,883 | 49,244,158 |
| March | 17,184,413 | |
| April | 13,726,811 | |
| May | 16,145,566 | 48,283,485 |
| June | 18,411,108 | |
| July | 16,591,252 | |
| August | 7,137,168 | 27,822,009 |
| September | 4,093,589 | |
| October | 3,897,113 | |
| November | 10,003,042 | 27,292,197 |
| December | 13,392,042 | |

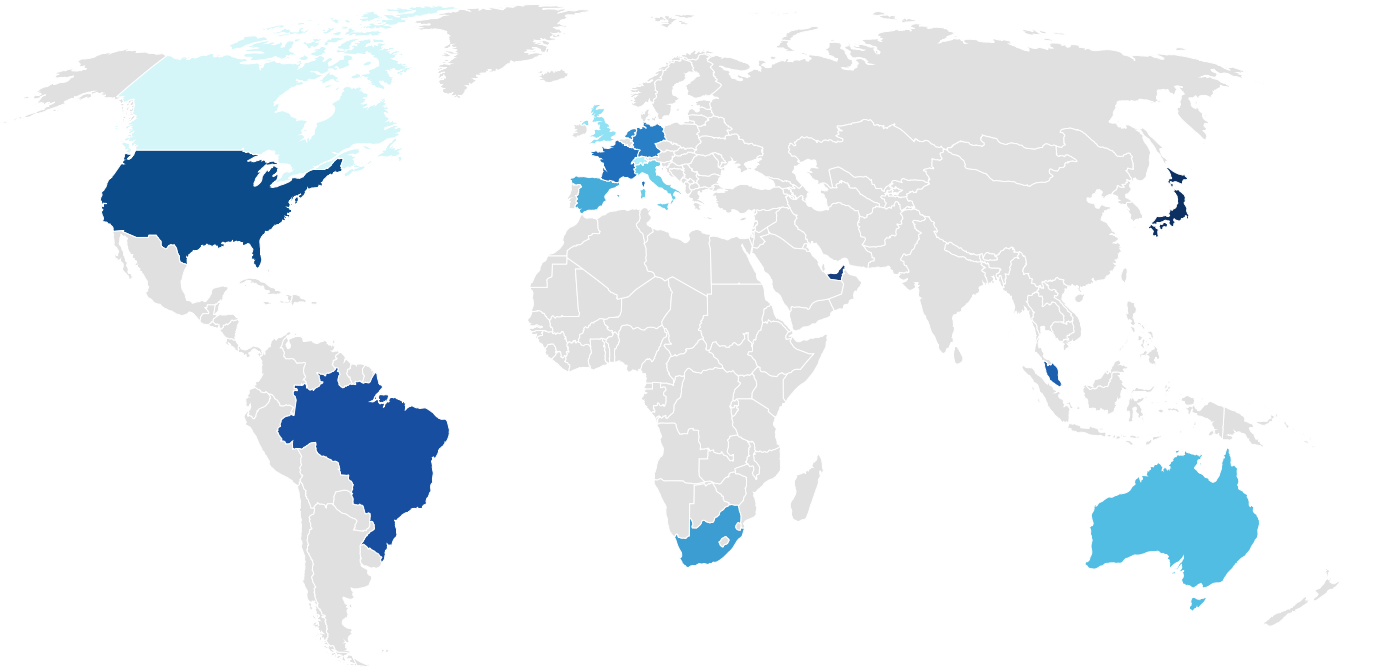
An average of 15.7% of endpoints tried to access malicious URLs in Q4 2023, up from 8.6% in Q4 2022. In September, it spiked 17%, but then dropped to 15.8% in December.

| Month | Percentage of users that clicked on malicious URLs |
|---|---|
| January | 8.7% |
| February | 9.1% |
| March | 9.1% |
| April | 6.9% |
| May | 8.1% |
| June | 13.3% |
| July | 16.1% |
| August | 16.8% |
| September | 17.0% |
| October | 15.8% |
| November | 16.0% |
| December | 15.3% |

Among the focus countries, the country with the largest percentage of blocked malicious URLs at the endpoint in December 2023 was Japan with 21.2%, followed by United Arab Emirates with 18.7% and the United States with 18.2%.

## Focus countries with the blocked URLs in December 2023

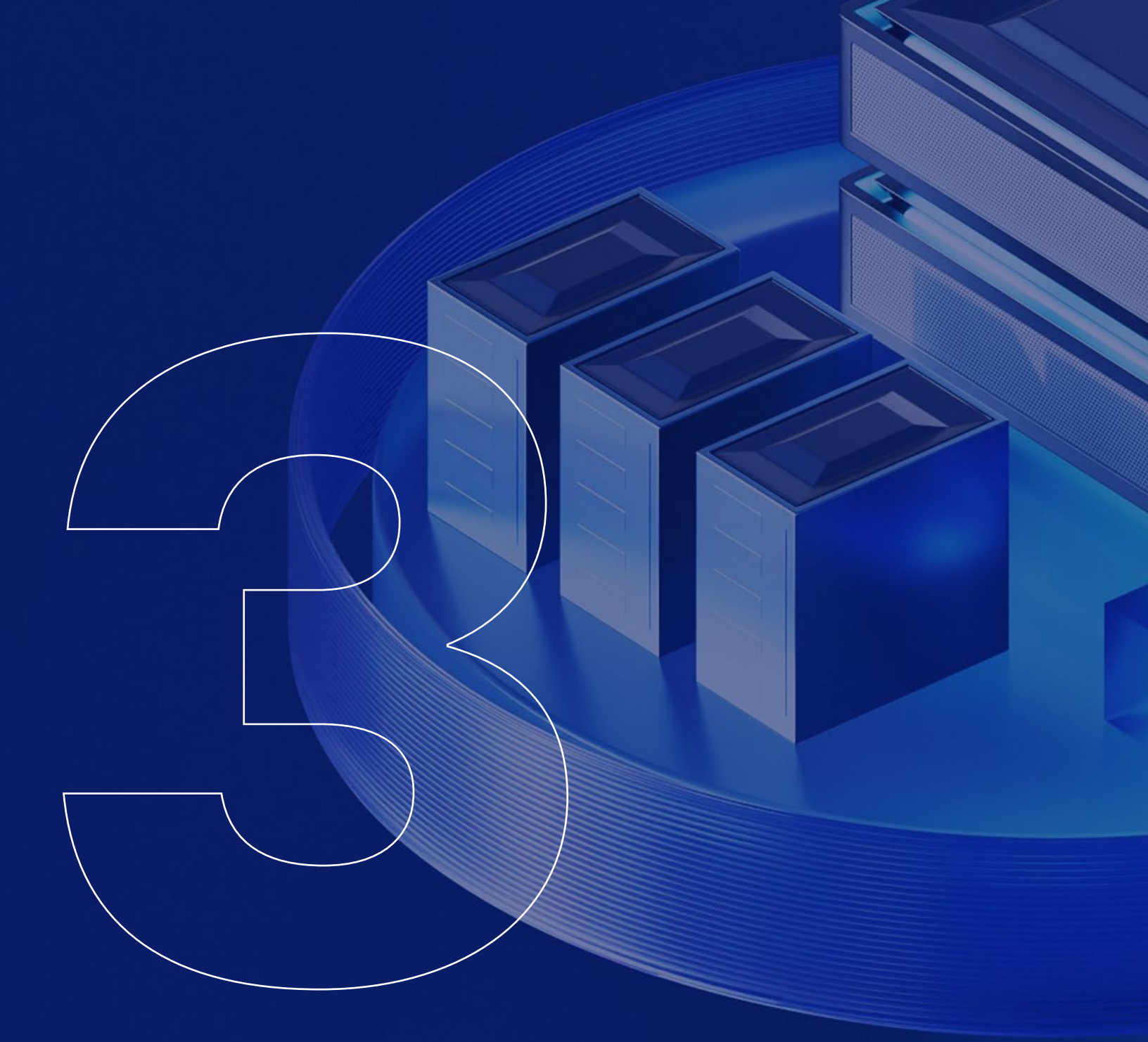
| Rank | Country | Percentage of blocked URLs in December 2023 |
|---|---|---|
| 1 | Japan | 21.2% |
| 2 | United Arab Emirates | 18.7% |
| 3 | United States | 18.2% |
| 4 | Brazil | 17.6% |
| 5 | Singapore | 17.3% |
| 6 | France | 17.2% |
| 7 | Germany | 16.4% |
| 8 | Netherlands | 15.0% |
| 9 | South Africa | 14.7% |
| 10 | Spain | 13.4% |
| 11 | Australia | 13.1% |
| 12 | Italy | 12.9% |
| 13 | United Kingdom | 11.3% |
| 14 | Switzerland | 10.2% |
| 15 | Canada | 5.1% |



Percentage

5.1% 21.2%

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



# 33

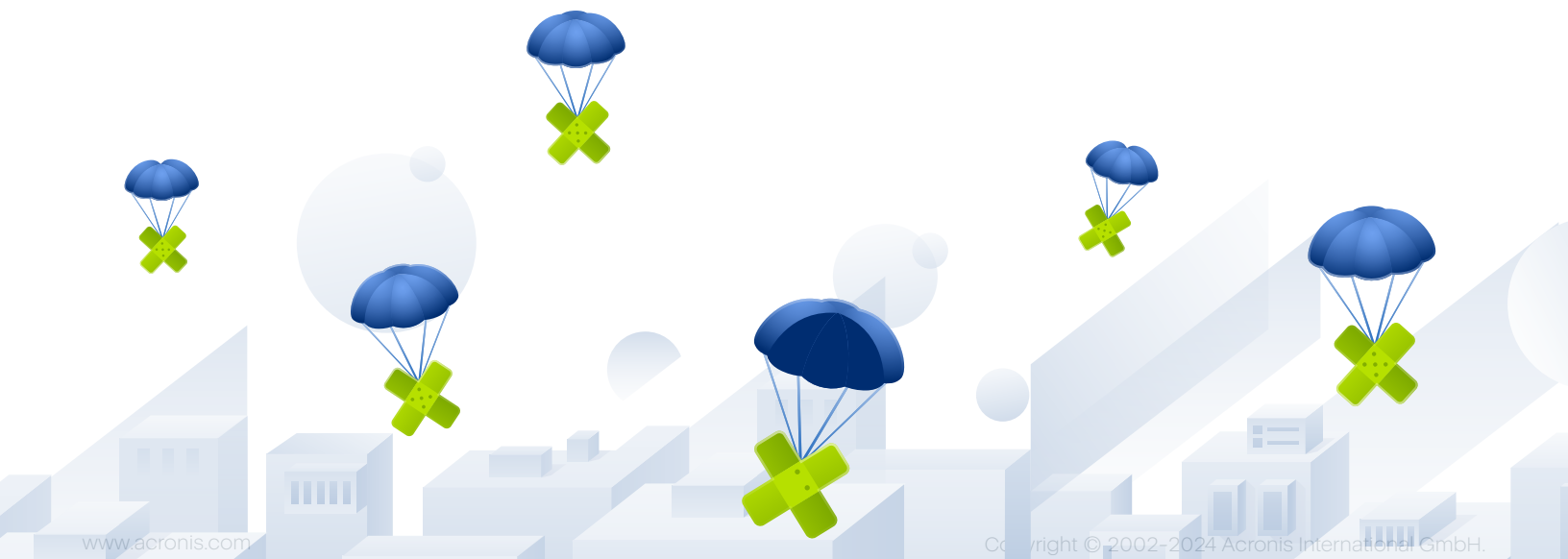
# Vulnerabilities discovered in products of key software vendors

The latter half of 2023 was marked by a significant surge in cybersecurity threats, with a range of vulnerabilities and zero-day exploits affecting products from major software providers such as Microsoft and Google. As threat actors become more inventive in their approach, it's imperative to stay abreast of the latest patches and security advisories. In this section, we explore several critical Patch Tuesday releases from Microsoft, alongside Google's response to newfound flaws, detailing the technical aspects and potential impact of these vulnerabilities.

# Microsoft Patch Tuesdays

July was a particularly intense month, with Microsoft addressing 132 flaws, including six zero days, marking it as a critical point for cybersecurity practitioners. Let's take a look at three of the vulnerabilities:

- CVE-2023-32046: Windows MSHTML Platform Elevation of Privilege Vulnerability. Exploited privilege elevation vulnerability in Windows MSHTML that was exploited by opening a specially crafted file through email or malicious websites. Additionally, by exploiting the Windows SmartScreen Security Feature Bypass Vulnerability (CVE-2023-32049), threat actors could prevent the display of the Open File — Security Warning prompt if victims downloaded or opened files from the Internet.
- CVE-2023-36874: Windows Error Reporting Service Elevation of Privilege Vulnerability. Actively exploited an elevation of privileges flaw that allowed threat actors to gain administrator privileges on the Windows device.
- CVE-2023-36884 Office and Windows HTML Remote Code Execution Vulnerability. Microsoft released guidance on a publicly disclosed, unpatched Microsoft Office and Windows zeroday that allows remote code execution using specially crafted Microsoft Office documents. But, an attacker would have to convince the victim to open the malicious file. This vulnerability was exploited by the RomCom hacking group, previously known to deploy the Industrial Spy ransomware in attacks. The ransomware operation later rebranded under the name Underground, where they continue to extort victims. The threat actors are also linked to the Cuba ransomware operation.



An August release saw updates for 87 flaws, including two actively exploited flaws and 23 remote code execution vulnerabilities. One of the zero days (CVE-2023-36884) received a Defense in Depth update to mitigate a flaw under active attack. Another zero day (CVE-2023-38180) is a denial-of-service vulnerability in .NET and Visual Studio.

**An additional six vulnerabilities, described below, are rated as critical:**

CVE-2023-29328 and CVE-2023-29330 are Critical remote code execution vulnerabilities affecting Microsoft Teams. The vulnerability would allow an attacker to execute code on a system remotely when a victim joins a malicious Teams meeting. What is alarming is that no special privileges are necessary for a successful attack.

Another important update was pushed to Microsoft Office to patch a previously disclosed, unpatched vulnerability (CVE-2023-36884). According to Microsoft, installing this update will stop the attack chain that leads to the exploitation of the Windows Search Security Feature Bypass Vulnerability.

In September, Microsoft responded to two zero-day vulnerabilities, along with 59 additional flaws affecting a range of products. One of the zero days had already been exploited in the wild, making the patch a critical update for affected users. The urgency of the situation was underscored by the diverse nature of the vulnerabilities addressed and which impacted Microsoft's operating systems, Office applications, web browsers and more. The aggregate of these flaws comprised privilege escalation, remote code execution (RCE), information disclosure and denial of service, each with varying degrees of severity.

The zero days included the Elevation of Privilege Vulnerability in Microsoft Streaming Service Proxy (CVE-2023-36802), which allowed attackers to gain SYSTEM privileges. The Microsoft Word Information Disclosure Vulnerability (CVE-2023-36761) can be used to steal NTLM hashes when opening a document, including in the preview pane. Later, NTLM hashes can be cracked or used in NTLM Relay attacks to gain access to the account.

Microsoft's October updates were reflective of an ongoing commitment to securing systems against an evolving array of threats. According to the Microsoft Security Response Center (MSRC), the focus was on mitigating risks associated with remote code execution, denial of service and elevation of privilege. This batch patched 104 flaws, including three actively exploited zero-day vulnerabilities.

CVE-2023-36563 Microsoft WordPad Information Disclosure Vulnerability can be used to steal NTLM hashes when opening a document in WordPad. According to Microsoft, an attacker could take control of an affected system simply by logging in and running a specially crafted application. The second vulnerability was in Skype for Business, the vulnerability was classified as an Elevation of Privilege bug.

The CVE-2023-44487 vulnerability led to a new zero-day DDoS attack technique called HTTP/2 Rapid Reset that has been actively exploited since August and which broke all previous records of rps (rapid resets). This attack abuses the HTTP/2's stream cancellation feature to continuously send and cancel requests, overwhelming the target server / application and imposing a DoS state. Microsoft's mitigation steps in the advisory are to disable the HTTP/2 protocol on your web server.

November's Patch Tuesday saw Microsoft address 58 vulnerabilities, including five zero days. The updates were wide reaching, targeting issues within Windows, Microsoft Office, Edge browser and more. The three critical flaws fixed are an Azure information disclosure bug, an RCE in Windows Internet Connection Sharing (ICS) and a Hyper-V escape flaw that allows the executions of programs on the host with SYSTEM privileges.

CVE-2023-36025 Windows SmartScreen Security Feature Bypass Vulnerability is an actively exploited flaw that allows a malicious internet shortcut to bypass security checks and warnings. According to Microsoft, an attacker would be able to bypass Windows Defender SmartScreen checks and their associated prompts.

Lastly, a recent December Patch Tuesday was less productive: 34 vulnerabilities, including a single zero-day vulnerability and three critical remote code execution (RCE) vulnerabilities. CVE-2023-20588 describes a potential information disclosure due to a flaw in certain AMD processor models. AMD states that a divide-by-zero on these processor models could potentially return speculative data. The vulnerability was patched at the OS level in all supported versions of Windows, even as far back as Windows Server 2008 for Azure-hosted assets participating in the Extended Security Update (ESU) program.

# Adobe patch work

## In July, Adobe released security updates to address 15 vulnerabilities in Adobe InDesign and Adobe ColdFusion. Out of 15 vulnerabilities, three were rated as critical and could lead to arbitrary code execution and security feature bypass.

Four security advisories were released in August to address 37 vulnerabilities in Adobe Acrobat and Adobe Reader, Adobe Commerce, Adobe Dimension and Adobe XMP Toolkit SDK. Out of 37 vulnerabilities, 19 were rated as critical and could lead to arbitrary code execution, memory leak and security feature bypass.

In September, Adobe released three security advisories to address five vulnerabilities in Adobe Acrobat and Adobe Reader, Adobe Connect and Adobe Experience Manager. One was a zero-day vulnerability CVE-2023-26369 in Adobe Acrobat and Adobe Reader. It was actively exploited and led to arbitrary code execution.

In October, Adobe released three security advisories to address 13 vulnerabilities in Adobe Bridge, Adobe Commerce and Adobe Photoshop — eight were of critical severity: successful exploitation may result in arbitrary code execution, privilege escalation and security feature bypass.

November was more fruitful, with 14 security advisories to address 66 vulnerabilities — 34 being critical — in Adobe ColdFusion, Adobe RoboHelp Server, Adobe Acrobat and Reader, Adobe InDesign, Adobe Photoshop, Adobe Bridge, Adobe FrameMaker Publishing Server, Adobe InCopy, Adobe Animate, Adobe Dimension, Adobe Media Encoder, Adobe Audition, Adobe Premiere Pro and Adobe After Effects.

The previous updates stood in stark contrast to December, when Adobe released nine security advisories to address 212 vulnerabilities in Adobe Prelude, Adobe Illustrator, Adobe InDesign, Adobe Dimension, Adobe Experience Manager, Substance3D Stager, Substance3D Sampler, Substance3D After Effects and Substance3D Designer. Adobe Experience Manager has received the largest number of security updates (185) for important and moderate severity vulnerabilities, 13 of which were of critical severity.

# Google security updates

While Google focuses much of its patching on its Android operating system, which we do not cover in our security reports, Google takes significant steps to make their Chrome browser more secure. For example, July's Chrome 115 update fixed 20 security vulnerabilities, four of which were rated as having a high impact. CVE-2023-3727 and CVE-2023-3728 are use-after-free bugs in WebRTC.

Six of the flaws were listed as having a medium severity, and none of the vulnerabilities were known to have been used in real-life attacks. Even so, we know that Chrome is a highly targeted platform and needs to be updated regularly. In August, Google pushed Chrome 116 to patch 26 vulnerabilities, eight of which are rated as having a high impact. The most serious issues include CVE-2023-2312, a use-after-free bug in Offline, and CVE-2023-4349, a use-after-free flaw in Device Trust Connectors. Just a few days later, Google released the first of its more regular weekly security updates, patching five flaws. The four vulnerabilities rated as having a high impact include two use-after-free bugs and two out-of-bounds memory access issues.

October continued at a similar pace: 20 security fixes were released for Chrome browser, including one patch for a flaw rated as critical. In November, Google Chrome encountered seven zero-day vulnerabilities, prompting a critical update, including an emergency patch for an issue already being used in real-life attacks. CVE-2023-6345 is an already exploited flaw that is an integer overflow issue in Skia, an open source, 2D-graphics library. The six other flaws fixed by Google and rated as having a high impact include CVE-2023-6348, a type-confusion bug in Spellcheck, and CVE-2023-6351, a use-after-free issue in libavif.

What is more interesting is that Google specializes in discovering and mitigating hardware vulnerabilities as well. Two of the most notable were disclosed in August, when Google researchers discovered Downfall (CVE-2022-40982) and Zenbleed (CVE-2023-20593) vulnerabilities affecting Intel and AMD CPUs, respectively. Hardware vulnerabilities are usually much harder to patch and can be devastating if left unattended.

In November, Google's information security engineering team discovered Reptar (CVE-2023-23583), a new CPU vulnerability that impacts several Intel desktop, mobile and server CPUs. The vulnerability is related to how redundant prefixes are interpreted by the CPU. If exploited successfully, the vulnerability leads to bypassing the CPU's security boundaries. In a multitenant virtualized environment, the exploit on a guest machine causes the host machine to crash, resulting in a denial of service to other guest machines running on the same host. Additionally, it could potentially lead to information disclosure or privilege escalation.

# Conclusion

The revelations of the second half of 2023 emphasize the neverending cat-and-mouse game between cybersecurity professionals and threat actors. The frequency and severity of the vulnerabilities discovered serve as a reminder of the criticality of consistent system updates and proactive security measures.

Systems administrators and IT professionals must remain vigilant, ensuring timely application of security patches and adherence to best practices in defense. By shedding light on the specific vulnerabilities, the industry can better equip itself against the threats posed by ever more creative adversaries, ultimately fortifying the digital landscape against unforeseen attacks.

# Predictions for 2024

### AI-driven phishing attacks

We expect to see a rise in phishing attacks powered by generative AI. These attacks will utilize AI to create highly convincing fake messages and personalized scenarios, deceiving users into divulging even more sensitive information.

### Phishing beyond email

Traditional email phishing will evolve into communication platforms like Microsoft Teams. Attackers will exploit these platforms for phishing attempts, catching users off guard. The trend of QR code-based phishing and stealing of web session tokens to bypass MFA authentication will continue.

### Deepfake exploitation

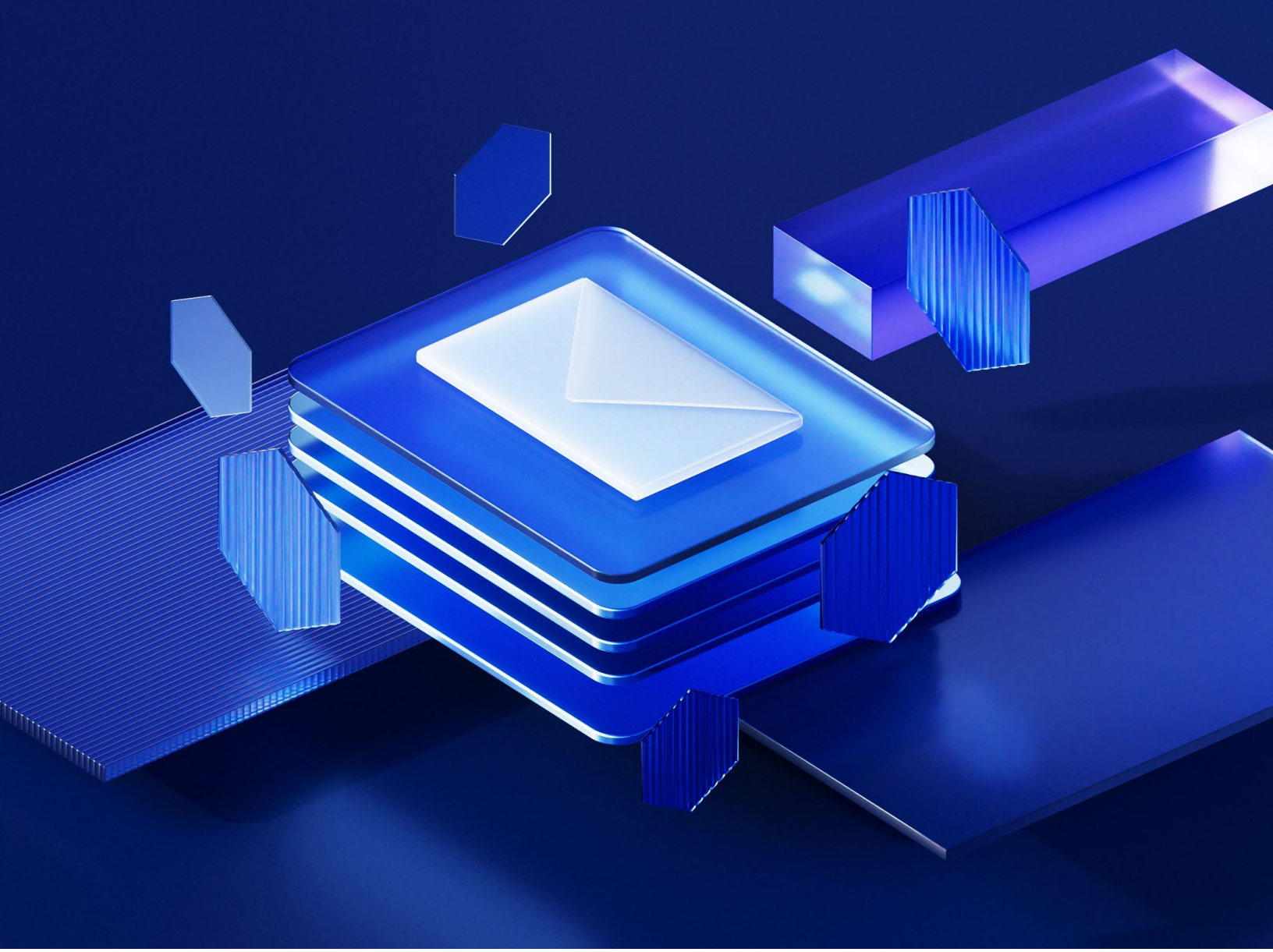
AI generated deepfakes will become prominent tools for cybercriminals. These hyper-realistic fake videos or audio recordings will be used to manipulate individuals or public opinion, potentially causing significant harm. AI-generated deepfakes are especially increasing in business email compromise (BEC) scams and extortion threats.

### Attacks on AI models

Cybercriminals will conduct attacks against AI models, but the costs to conduct such attacks currently outweighs the benefits for the majority. The number of techniques to attack AI models is increasing, as has been listed on the MITRE ATLAS matrix; and these more frequent attack techniques are stealing the API keys and reselling them or increasing the operational costs for companies by forcing AI systems to overwork.

### Automated cyberattacks

AI will not only enhance the sophistication of attacks but also their volume and frequency. Automated cyberattacks will become more prevalent, allowing attackers to strike multiple targets simultaneously with minimal effort. This will lead to AI vs. AI scenarios, which will require AI automated defense in order to react quickly enough to mitigate the attacks.



### Disabling security solutions

Trends like “bring your own vulnerable driver” will continue to target security solutions directly. Attackers will aim to disable EDR systems to carry out their malicious activities undetected. In many cases, a simple uninstalling of the solution will still go unnoticed by the IT department.

### Identity provider and MFA bypasses

Multifactor authentication (MFA) and centralized identity providers will become prime targets for attackers, as breaching these systems can give attackers access to a wide array of resources. We expect an increase in the usage of phishing-resistant MFA combined with ZTA solutions.

### Human errors due to complexity and stress

The increasing complexity of IT systems and stress on the individuals who manage them will lead to more human errors. The growing availability of AI copilots helps to soften the skills gap, but the complexity of integrating all the data sources correctly will still be challenging. Such errors can open doors for further cyberattacks.

### Living off your infrastructure

Attackers will increasingly use ‘living off the land’ strategies, exploiting legitimate tools and services of MSPs or performing supply chain attacks to gain access to multiple targets through a single breach. If no suitable tools are found, then legitimate software packages will be deployed to support the attackers’ objectives.

5

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

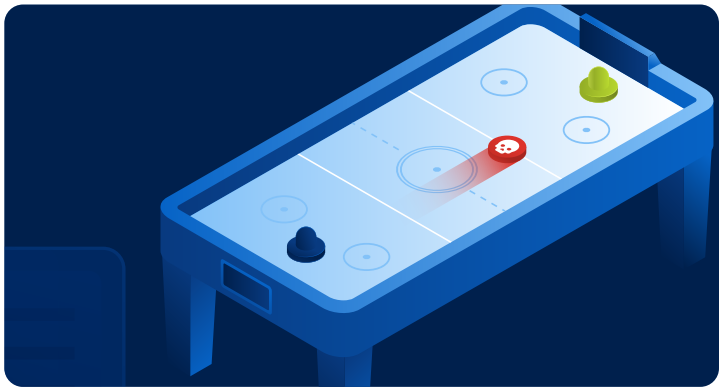
Modern cyberattacks, data leaks and ransomware outbreaks all reveal the same thing: the current approach to cybersecurity is failing, and failure is the result of weak technologies, heightened complexity and human mistakes caused by clever social engineering tactics.

Backup is essential for when cybersecurity solutions fail. At the same time, backup solutions can be compromised or disabled, and often perform slowly, causing significant financial losses due 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.

To solve these problems, we recommend an integrated cyber protection solution that combines anti-malware, EDR, DLP, email security, vulnerability assessments, patch management, RMM and backup capabilities into a single agent. This integration enables you to maintain optimal performance, eliminate compatibility issues and ensure rapid recovery: If a threat is missed or detected while your data is being altered, the data will be restored from a backup immediately. 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.



Endpoint Detection and Response (EDR) for Acronis Cyber Protect Cloud 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 sure 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 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 multifactor authentication.

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. Also 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. 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 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 on 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 on 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 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 ensure that the license is legitimate if you're using a paid version from a security vendor.

# About Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions powered by AI. With advanced anti-malware powered by cutting-edge machine intelligence and blockchain based data authentication technologies, Acronis protects any environment — from cloud to hybrid to on premises — at a low and predictable cost.

Founded in Singapore in 2003 and incorporated in Switzerland in 2008, Acronis now has more than 2,000 employees and offices in 34 locations worldwide. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, and top-tier professional sports teams. Acronis products are available through over 50,000 partners and service providers in over 150 countries and 26 languages.

Acronis

Learn more at
acronis.com