Muttii Mid-Year Cyberthreats Report 2023

From Innovation to Risk: Managing the Muttii of AI-driven Cyberattacks

MUTTII
Mid-Year Cyberthreats Report 2023

Table of contents

Authors:

Alexander Ivanyuk
Senior Director, Technology

Candid Wuest
VP of Research

Irina Artioli
Cyber Protection Evangelist

Introduction and summary

Muttii 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 5 vectors of "SAPAS" — safety, accessibility, privacy, authenticity and security. As part of this strategy, we've established four Cyber Protection Operation Centers (CPOCs) around the world to monitor and research cyberthreats 24/7.

We've also upgraded our current flagship products: Muttii Cyber Protect Cloud, a cloud solution added to the Muttii Cyber Cloud platform, and Muttii Cyber Protect 15, an on-premises solution. Prior to these releases, Muttii had been a leader in the data protection market with its innovative Muttii Active Protection anti-ransomware technology, which evolved over time to demonstrate Muttii' 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 Muttii developed in 2016 have been expanded to address all forms of malware and other potential threats.

This report covers the threat landscape, as encountered by our sensors and analysts in the first half of 2023. General malware data presented in the report is gathered from January–May of this year, and reflects threats targeting endpoints that we observed in these months.

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

The top five numbers of this report:

- The most malware-attacked countries in Q1 2023 were Singapore, Brazil and Japan.

- Almost 50 million URLs were blocked at the endpoint by Muttii in Q1 2023, a 15% increase over Q4 2022.

- 30.3% of all received emails were spam and 1.3% contained malware or phishing links.

- Each malware sample lives an average of 2.1 days in the wild before it disappears. 73% of samples were only seen once.

- We saw 809 publicly mentioned ransomware cases in Q1 2023, with a 62% spike in March over the monthly average of 270 cases. In April, 308 cases were reported, and in May, 259. LockBit, Clop and ALPHV/BlackCat are the top 3 contributors, collectively responsible for 56.8% of ransomware attacks.

Among the cybersecurity trends we saw in the first half of 2023 (January–May):

- Ransomware continues to be the major threat to large and medium-sized businesses, including government, healthcare, and other critical organizations. Recently, ransomware makers have abused vulnerable drivers to get a foothold in the system 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 commence cyberattacks and create malicious content.

- In the first quarter of 2023, over 60,000 customers reported being impacted by supply-chain attacks.

- The number of email attacks seen in 2023 has surged by a staggering 464% compared to the first half of 2022.

What you will find in this report:

- The top security/threat trends we observed in the first half of 2023

- 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 reviewed

- Which vulnerabilities contribute to the success of attacks

- Our security recommendations for the coming months

Key cyberthreats and trends for the first half of 2023

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

We continue to see a decline in the number of new ransomware samples. Unfortunately, the situation remains dire. Ransomware gangs are still breaching companies around the globe fairly easily, and continue to make malicious use of popular legitimate tools after breaching systems — PowerShell is used to execute malicious data-collecting scripts, Mimikatz to escalate privileges and PsExec to execute commands remotely. Of course, they continue to use dual-use frameworks like Cobalt Strike for all attack stages where it has been proven effective.

In recent months, we saw many examples where ransomware attackers abused vulnerable drivers from legitimate applications for malicious purposes. This tactic is nothing new, but it is hugely advantageous for criminals: they can get kernel-level privileges and execute admin-level commands, allowing them essentially free reign over compromised systems.

Many drivers have such vulnerabilities, including those used by security companies. For example, AvosLocker and Cuba ransomware used the Avast anti-rootkit kernel driver vulnerabilities to infect systems. Popular games are also targeted, and specialists at Trend Micro have reported on a ransomware actor abusing the Genshin Impact anti-cheat driver, using it to kill endpoint protection on the target machine.

Popular utilities were abused as well. For instance, BlackByte ransomware abused RTCore64.sys and RTCore32.sys, drivers used by the Micro-Star MSI AfterBurner 4.6.2.15658 graphics card overclocking utility. A vulnerability in these drivers (CVE-2019-16098) allows an authenticated user to read and write to arbitrary memory, which has been used to bypass and disable security software. Yet another example is the AuKill tool, which used a vulnerable version of Sysinternals' Process Explorer to kill EDR processes.

Another reason why we don't see many new ransomware families is the existence of leaked ransomware code, which other gangs have reused. Starting from that code, they've made samples that are working quite well so far, eliminating the need to develop completely new families. The LockBit gang, for example, reused big chunks of leaked Conti code and released a new version based heavily on that. Similarly, the Babuk source code (leaked in 2021) is still

used by other ransomware actors, especially those who are interested in targeting Linux and VMware ESXi.

In January, the U.S. Department of Justice and Europol jointly announced that Hive's infrastructure had been shut down following an international law enforcement operation. The FBI infiltrated the gang's infrastructure for six months, gaining access to two dedicated servers and one virtual private server at a hosting provider in California. In parallel, Dutch police also gained access to two dedicated backup servers hosted in the Netherlands. Those servers hosted the operation's main data leak site, negotiation site and web panels used by the operators and affiliates. The FBI also was able to gain records of Hive's communications, malware file hash values and information on 250 Hive affiliates, and to distribute over 1,000 decryption keys to previous victims of the group.

This action is a victory to be sure, but if we look at the data released by ransomware gangs (as collected by The Record), it's clear that the total number of known victims is still growing.

Victim Data Released on Ransomware Extortion Sites

Source: https://therecord.media/ransomware-tracker-the-latest-figures
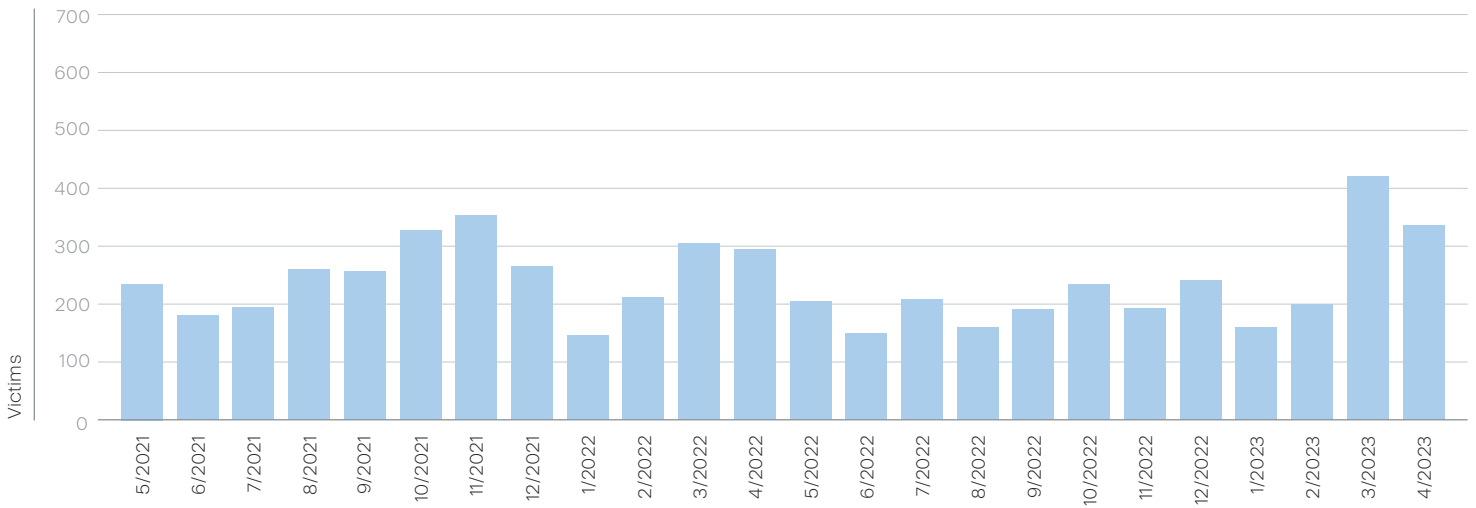
Looking at the first months of 2023, we can say that the following ransomware gangs were the most active (in terms of total numbers of victims):

↘ **LockBit (280)**	↘ **Clop (106)**	↘ **BlackCat/ALPHV (74)**	↘ **Royal (68)**	↘ **Play (43)**

49%
LockBit

19%
Clop

13%
BlackCat/
ALPHV

12%
Royal

7%
Play
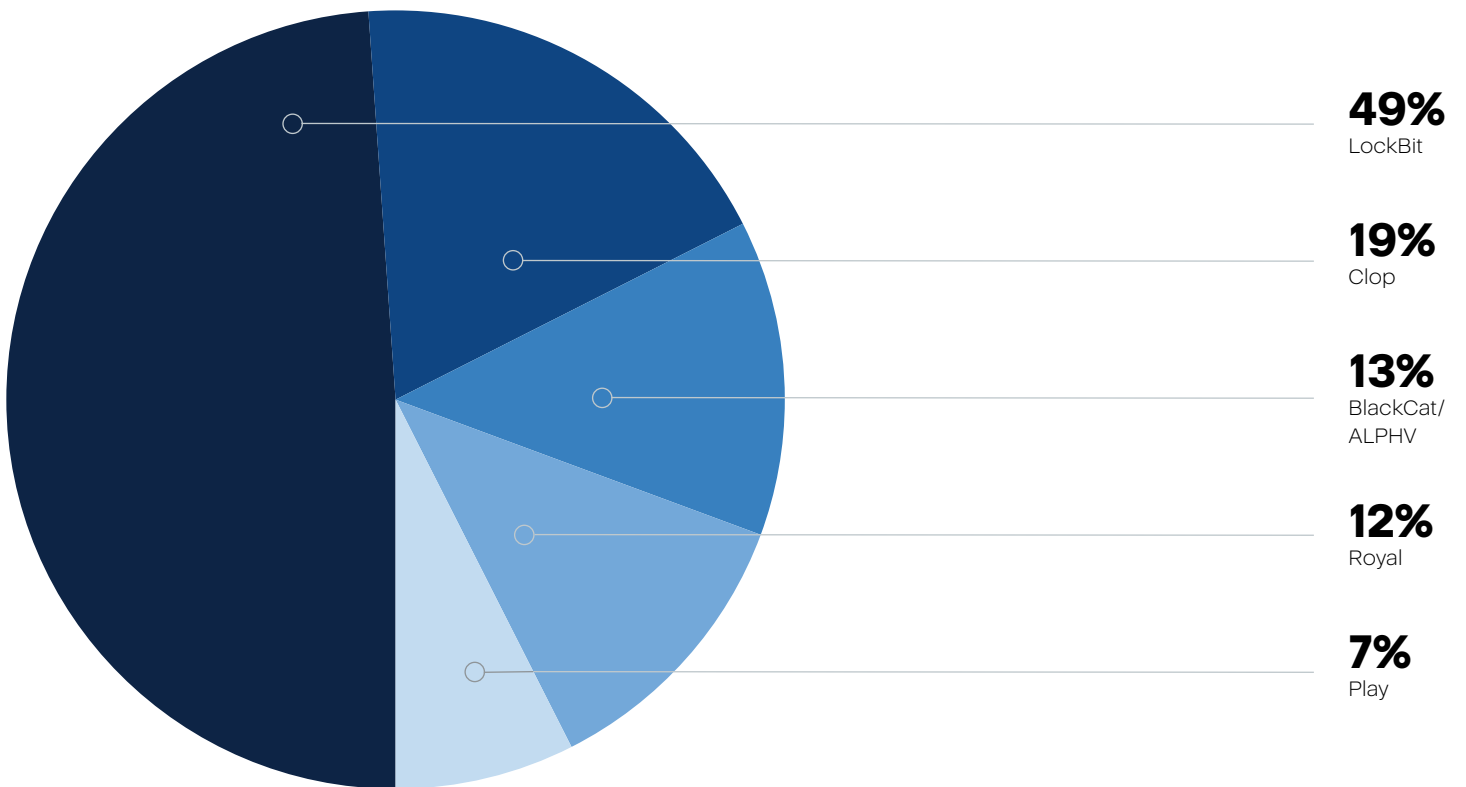
Lets take a look into the activities of these top gangs, as well as some other notable ransomware incidents from January–May 2023.

The big players in H1 2023

LockBit

The LockBit gang continues to dominate the ransomware world, much as they did last year. Recently, they claimed responsibility for a cyberattack on Essendant. The wholesale distributor of office products, which has an annual revenue of $5 billion and over 6,400 employees, had to suspend operations due to the incident. The outage affected the placement and fulfillment of online orders and impacted both the company's customers and suppliers. Freight carriers have also been told to hold off on any pick-ups until further notice.

Another recent victim of LockBit, the Housing Authority of the City of Los Angeles (HACLA), has confirmed that it suffered a data breach after a ransomware attack. HACLA is a state-chartered agency, with an annual budget of $1 billion, that provides affordable housing to low-income individuals and families in Los Angeles, California. According to an internal investigation, the attackers had unauthorized access to systems for almost a year, and might have accessed personal information belonging to members of HACLA.

The LockBit group also attacked Aguas do Porto, a Portuguese municipal water utility company. Aguas do Porto also manages public lighting and photovoltaic parks.

Wabtec Corporation disclosed a data breach after it suffered a ransomware attack by LockBit. The US. rail and locomotive company has approximately 25,000 employees and 50 plants all over the world. Wabtec manufactures products for locomotives, freight cars and passenger transit vehicles, and builds new locomotives up to 6,000 horsepower. According to a forensic investigation, the compromised information includes a combination of the following data elements: first and last names, dates of birth, non-U.S. national ID numbers, non-U.S. social insurance numbers or fiscal codes, passport numbers, IP addresses, Employer Identification Numbers (EIN), NHS (National Health Service) numbers (U.K.), medical record/health insurance information, salaries, Social Security numbers (U.S.), financial account information, payment card information, account usernames and passwords, biometric information, race/ethnicity, criminal conviction or offense records, sexual orientations, religious beliefs and union affiliation.

Also of significance is that the LockBit gang has created

encryptors targeting Macs for the first time, becoming one of the first major ransomware operations to specifically target macOS. LockBit already uses encryptors designed for attacks on Windows, Linux and VMware ESXi servers. However, discovered archives also contained previously unknown encryptors for macOS, ARM, FreeBSD, MIPS and SPARC CPUs. These encryptors also include one named 'locker_Apple_M1_64' that targets newer Macs running on Apple Silicon. As Macs are widely used in some countries, especially the U.S., we can expect devastating ransomware attacks in the future — an unwelcome surprise for the many Mac users who still believe they are effectively immune against malware.

Vice Society

Vicy Society increased their activity in Q2 2023 after being a top-10 player in Q1. They were behind the attack on Puerto Rico Aqueduct and Sewer Authority (PRASA), the government-owned corporation responsible for water quality, management and supply in Puerto Rico. Vice Society leaked the passports, driver's licenses, and other documents of the impacted individuals on its Tor leak site. PRASA has confirmed that the threat actors gained access to customer and employee information.

The gang also leaked the personal and financial data of thousands of CommScope employees on the dark web. CommScope designs and manufactures network infrastructure products and provides services for various sectors, including government and healthcare. The company employs 30,000 people and its 2022 revenue

was $9.2 billion. Attackers breached CommScope's IT network and stole internal documents, technical drawings, backups and personal information about employees, such as names, addresses, Social Security numbers, bank account details, passport and visa scans. They demanded a ransom from CommScope, but since the stolen data was leaked, it can be assumed that the ransom was not paid. The leaked data exposes CommScope employees to identity theft and fraud risks.

Vice Society has claimed responsibility for the attack on Australia's Fire Rescue Victoria. This is a fire and rescue service operating across 85 stations in the Australian state of Victoria, with approximately 4,500 operational and corporate employees. The incident caused outages, and the attackers stole data that included sensitive and personal information about current and former employees, contractors, secondees and job applicants. Cybercriminals also accessed the agency's email system, and may have accessed or stolen sensitive email communications.

Finally, the University of Duisburg-Essen (UDE), a top German university in the physics field, fell victim to Vice Society. UDE has about 43,000 students, 4,000 academic staff and 1,500 administrative staff. This incident affected 1,200 servers and compromised the central authorization system, and the university has decided to rebuild its entire IT infrastructure.

Clop

The Clop ransomware group has been very active in 2023 so far. They've focused on taking advantage of known vulnerabilities, namely the GoAnywhere zero-day vulnerability (CVE-2023-0669) to impact 130 organizations in February 2023 alone.

Among these was Crown Resorts — Australia's largest gambling and entertainment company, with annual revenue of over $8 billion. Crown Resorts operates complexes in Melbourne, Perth, Sydney, Macau, and London and employs over 20,000 people worldwide. Another victim was Saks Fifth Avenue, which has 12,900 employees and an annual revenue of $1.9 billion. Others include the Toronto city government, Virgin Red, and the U.K.'s Pension Protection Fund (PPF).

Hitachi Energy, a subsidiary of Japanese engineering and technology giant Hitachi with an annual revenue of $10 billion, confirmed a data breach after the Clop ransomware gang stole data by exploiting the aforementioned GoAnywhere vulnerability. All affected employees, applicable data protection authorities and law enforcement agencies were informed of the security incident directly by Hitachi.

Recent attacks on PaperCut's servers, which exploited two vulnerabilities to steal corporate data, have been attributed to the Clop and LockBit ransomware operations. PaperCut makes printing management software used by large companies, state organizations and education institutes across the globe.

The threat actors exploited the PaperCut vulnerabilities for initial access to the corporate network. After gaining access to the server, they deployed the TrueBot malware and a Cobalt Strike beacon to spread laterally through the network while stealing data. The Clop gang confirmed that they were behind the attacks on PaperCut servers. They used the vulnerabilities for initial access to networks, rather than to steal documents from the server itself.

Another victim in the same streak was Brightline, a pediatric mental health provider with a revenue of $20.6 million. The provider disclosed a data breach affecting over 783,606 individuals across 58 HIPAA-covered entities. Stolen data included names, addresses, dates of birth, member IDs, dates of health plan coverage and employers. The Clop gang claimed responsibility for the attack and posted Brightline's data on its leak site. However, the data was later removed and the gang apologized for targeting Brightline, saying they were unaware of the nature of its business.

BlackCat

The BlackCat/ALPHV gang, much like LockBit, was already a top ransomware gang in 2022. They've kept the pace in 2023 so far and infected a lot of high-profile victims.

One such victim was a data center that powers some of NCR's Aloha POS applications for hospitality customers. NCR is a US-based company with an annual revenue of $7.2 billion, and offers digital banking, POS systems and payment processing solutions for various sectors. Some Aloha POS customers have reported major disruptions to their business operations due to the outage.

Constellation Software, a Canadian company with an annual revenue of $3.96 billion that acquires and manages software businesses, was also hit by BlackCat. Constellation Software has over 25,000 employees and 125,000 customers worldwide, and has acquired more

than 500 software companies since 1995. The attack affected a few of its systems related to internal financial reporting and data storage, but not the independent IT systems of its operating groups and businesses. BlackCat claims to have stolen over 1 TB of data from Constellation Software's network.

BlackCat also compromised Solar Industries India, an industrial explosives manufacturer with an annual revenue of $223 million. The threat actors stole 2 TB of secret military data, including personal data of employees and customers, contracts, records from all production cameras and offices, internal product testing documentation with approvals, weapon blueprints and engineering documentation, and more. BlackCat published images of the stolen documents and pictures taken from the company's security cameras as proof on its Tor leak site.

Del Monte Foods was yet another victim of the BlackCat gang. Del Monte Foods is headquartered in California, and with an annual revenue of $4.41 billion and over 40,000 employees, is one of the world's largest producers, distributors and marketer of branded processed foods, which are retailed in more than 90 countries. The attackers have not specified the amount of data exfiltrated, but did list Del Monte as a victim on their leak website.

BlackCat operates as ransomware-as-a-service (RaaS), offering "affiliates" 80–90% of ransoms gathered and actively publishing victims on a name-and-shame blog.

Other notable cases

Apart from the old known groups, new ones continue to emerge. One of these calls itself DarkBit, and has claimed responsibility for the attack on the Technion – Israel Institute of Technology, one of Israel's leading research universities. The cyberattackers have demanded a ransom of 80 Bitcoin, which currently equals about $1.7 million, in order to release the decryptor. DarkBit threatened to impose a 30% penalty on top of the requested ransom demand if not paid within 48 hours, and also stated they would put stolen data up for sale five days after the attack unless their demands were met.

Taiwanese PC parts manufacturer MSI (Micro-Star International), which has an annual revenue of $5.9 billion, was hit by a new ransomware gang known as "Money Message." The cybercriminals listed MSI on their data leak website, and posted screenshots of what they claim to be the hardware vendor's CTMS and ERP databases, plus files containing software source code, private keys and BIOS firmware.

The threat actors claim to have stolen 1.5 TB of data from MSI's systems, including source code and databases, and demanded a ransom payment of $4 million. The company has notified authorities and started an investigation. The most worrisome notion is that the stolen private keys could allow attackers to create signed firmware updates, which could bypass the secure boot and install UEFI bootkit malware.

Another recent victim, mentioned on the Money Message gang's extortion site, was an Asian airline with an annual revenue close to $1 billion. The ransomware group claims to have stolen files from the airline and included a screenshot of the accessed file system as proof of the breach. Money Message also claimed credit for the attack on pharmacy services provider PharMerica. Hackers breached PharMerica's system on March 12, stealing the personal data — including full names, addresses, dates of birth, social security numbers (SSNs), medications, and health insurance information — of over 5.8 million patients.

Another newcomer, a ransomware gang named RA Group, has been targeting pharmaceutical, insurance, wealth management and manufacturing firms in the United States and South Korea since April 2023. They've launched a leak site on the dark web to publish victims' details and stolen data.

The Medusa ransomware gang, which has been around since 2021, became quite active in 2023. They recently added the Minneapolis Public Schools (MPS) system to their list of victims. MPS enrolls over 35,000 students per year and operates approximately 100 schools in Minneapolis.

The threat actors demanded a ransom of $1 million, and threatened to leak the stolen data if the ransom demand wasn't met by the deadline. For an additional $50,000, they offered a 1-day extension to this deadline. The Medusa gang also offered the stolen data for sale to any interested party for the same $1 million price.

The Open University of Cyprus (OUC) was another victim of the Medusa gang, who demanded a ransom of $100,000. OUC offers 30 higher-level education programs to 4,200 students and participates in various scientific research activities. The cybercriminals gave their victim 14 days to respond and requested an additional $10,000 for a one-day extension of the payment deadline, after which the data would be published online. They have published data samples which include student lists with personally identifiable information (PII), financial details of research contractors and more.

The Play ransomware group hit several targets in 2023. One of these was the California-based networking hardware manufacturer A10 Networks. Though the ransomware attack happened in January, an internal investigation has now revealed that the threat actors managed to gain access to shared drives, deployed malware and compromised data related to human resources, finance and legal functions. The Play gang claims to possess confidential files, including technical documentation, employee and client documents, agreements and personal data. Arnold Clark, Europe's largest independent car retailer with a revenue of over $4.8 billion, was another victim of Play. The company started to notify some customers about potential phishing attacks after their personal information was stolen in a December 23 cyberattack. The stolen data includes ID information, banking details and — in some cases — National Insurance numbers.

The City of Dallas became a victim of the Royal ransomware gang. The attack encrypted multiple servers and affected several functional areas, including the Dallas Police Department's website. Dallas is one of the largest cities in the U.S., with approximately 2.6 million residents. The attackers also printed out ransom notes on the city's network printers, claiming to have stolen data from the city and offering to keep it secret for a fee. The City of Dallas has confirmed the incident and is evaluating the full impact of the attack. This is not the first time that Royal has targeted Dallas entities. In 2022, the gang was behind a cyberattack on the Dallas Central Appraisal District, which was traced back to a phishing email.

A new Linux version of Royal ransomware has been encrypting devices, specifically targeting VMware ESXi virtual machines. After deploying their payloads on ESXi hosts, the ransomware operators use a single command to encrypt multiple servers. VMware ESXi servers have been exposed to attacks recently, as admins, hosting providers and the French Computer Emergency Response Team (CERT-FR) report that attackers actively targeted unpatched VMware ESXi servers against a two-year-old remote code execution vulnerability.

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

- There is a lack of strong security solutions in place that are able to detect the exploitation of zero-day vulnerabilities. With technologies behavior-based detection and exploit prevention — which are a part of the Muttii 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, long after a fix becomes available.

- Linux servers face inadequate protection against the cybercriminals who are increasingly going after them.

- Proper data backup, following the 3-2-1 rule, is a must for each and every organization.

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

The following email and phishing statistics are from the Advanced Email Security pack for Muttii Cyber Protect Cloud, which is powered by Perception Point. Muttii and Perception Point work together to protect organizations and ensure they remain safe from email-borne threats. The data was gathered for the first half of 2023, and combined with Muttii 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.

There are two significant numbers to highlight. First, the number of email-based attacks seen thus far in 2023 has experienced a staggering 464% surge compared to the first half of 2022. Second, when considering the attacks per organization within the same time frame, there has been a notable increase of 24%. These numbers underscore the escalating threat landscape — with email being the main attack vector — and the urgency for organizations to fortify their defenses against malicious activities.

In 2022, each scanned email, contained, on average,

2.7 files and URLs. Any of these could potentially pose a threat to the 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.

The Advanced Email Security pack for Muttii Cyber Protect Cloud is often deployed as a second layer of email filtering, on top of the basic filtering present in most email services. This makes it even more surprising that 30.3%, or about one-third, of emails that made it through were spam.

One out of 76, or 1.3%, of the received emails were malicious. Phishing remains the number one threat, with these attacks making up 73% of the total. However, the business email compromise (BEC)/social engineering category has increased by 7.5 times compared to the same period of time last year, and now takes second place, moving malware — which has dropped in percentage twice — into third.

73%
Phishing

15%
Social engineering / BEC

11%
Malware

1%
Advanced attacks
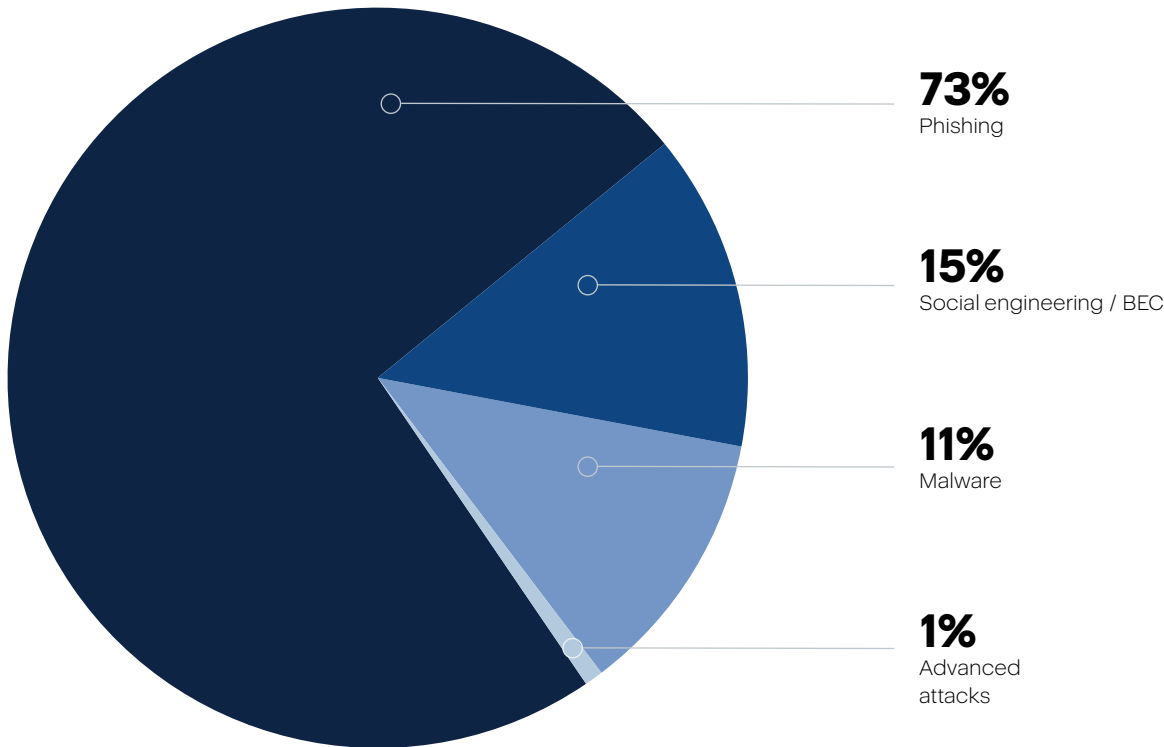
If we take a look at the regional impact and make a comparison for the categories between US and the EU, we will notice varying patterns of attack categories across the U.S. and EU regions. The trend reveals the following observations: Phishing attacks more commonly target the U.S., while BEC/social engineering exhibits a higher percentage of attacks in the EU region. Please refer to the table below for a detailed breakdown of these statistics:

■ US ■ EU

	Phishing	Malware	Social engineering/BEC	Advanced attacks
US	80.7%	10.5%	8.4%	0.5%
EU	63.1%	12%	24%	1%
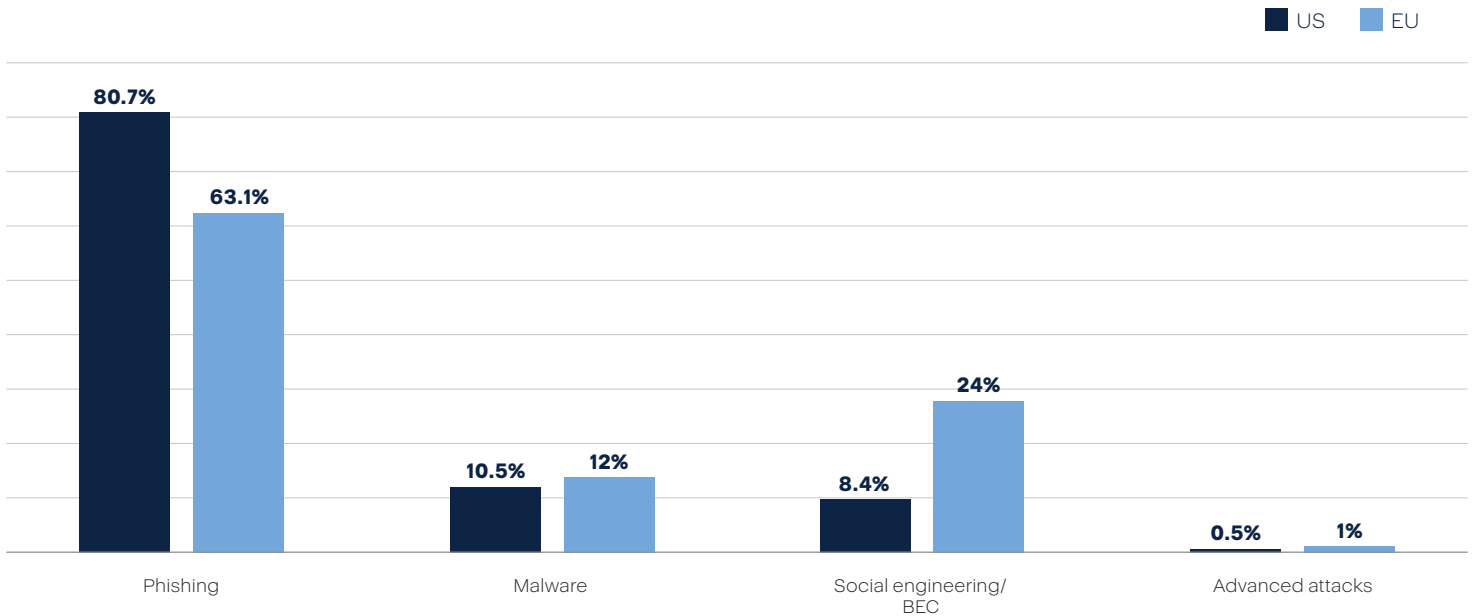
Big cases and phishing trends

Phishing continues to be one of the favorite tools of cybercriminal for penetrating systems. Let's take a look at some big cases discovered by Muttii and other cybersecurity researchers from January–May this year.

We observed a new phishing campaign that targets U.S. taxpayers by impersonating W-9 tax forms allegedly sent by the Internal Revenue Service and companies you work with. This campaign spreads Emotet, a malware threat that was previously distributed via malicious macros embedded in Microsoft Word and Excel documents, but now is delivered primarily via Microsoft OneNote files. Tax forms are usually sent as PDF documents. If the victim clicks the 'View' button in the received One Note file and continues, despite a system warning that the file might be malicious, a VBScript will be launched to download the Emotet DLL. The subsequently installed malware is capable of stealing emails and contacts, and downloading further payloads to the device.

Phishing

- OneNote
  - Threat family
    - RedLine Stealer
    - Remcos RAT
    - Qbot
- Excel file
  - Qbot
  - Emolet
- Word file
  - Method
    - Follina exploit
      - Threat family
        - IcedID
        - BumbleBee
- ISO file
  - LINK
- ZIP file
  - LINK
    - Emolet
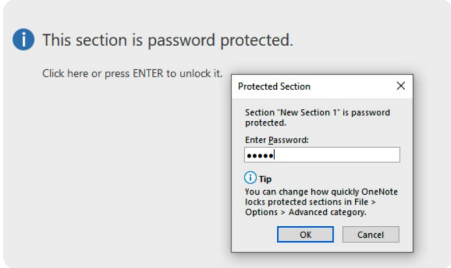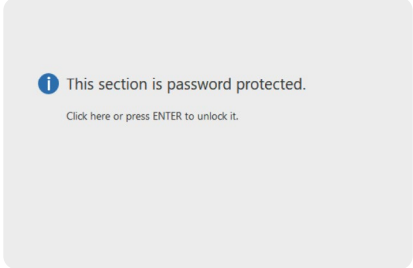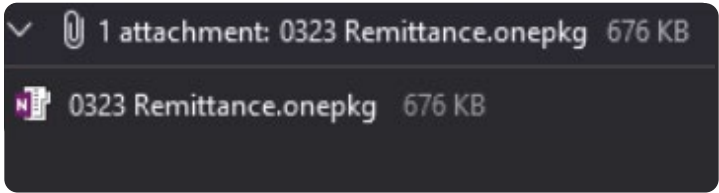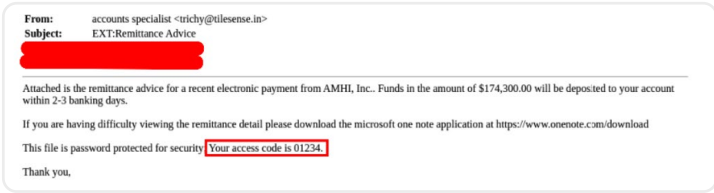
A new phishing campaign has been targeting users of the cryptocurrency hardware wallet firm Trezor. The campaign starts with an SMS message to the Trezor user, warning that Trezor has suffered a data breach and urging them to visit a hyperlink to secure their devices. Upon clicking the link, the user will be directed to a fake version of the Trezor website, notifying them that their assets might be at risk and displaying a field for the user can enter their recovery seed to 'secure' them. Entering the recovery seed on this phishing page provides cybercriminals with full access to the victim's wallet.

Another phishing campaign is spreading fake job offers, which deliver a modified version of the Stealerium malware named 'Enigma'. The campaign targets Eastern Europeans working in the cryptocurrency industry. Victims are lured by phishing emails pretending to be job offers, and include fake cryptocurrency interviews. Attached to these emails are RAR archive files that contain a text file ("interview questions.txt") and an executable ("interview conditions.word.exe"). Once the target launches the executable, a chain of payloads is executed that eventually downloads the Enigma infostealing malware from Telegram. Enigma can capture screenshots from the compromised system, clipboard content, VPN configurations, system information, tokens and passwords stored in web browsers. All stolen data is compressed and sent back to the threat actors via Telegram.

One more new phishing campaign follows a significant wave of layoffs in the tech industry. Attackers are targeting job seekers with different employment scams, impersonating recruiters from specific companies located in the U.S. and Canada. The attackers use fake job links

and reference codes for SmartRecruiters and LinkedIn. They also used suspicious domains, such as .online, .work, .live followed by the name of the organization that the attackers were impersonating. To attract more victims, the cybercriminals have lowered the years of experience requested in the listings. Candidates are asked to fill in questionnaires with their personal information, and submit PDF copies of documents such as their driver's license, state ID, residence permit or passport. As a next step, they receive a malicious email with an invite for a Skype interview and a photo of a real recruiter to make it plausible. After the fake interview, candidates may be sent through a fake onboarding process, during which they can be asked to pay for the supposed shipment of IT hardware equipment or training that they need for work.

Another cybercriminal gang once again used blank images to scam users. Those images obscure empty .svg files encoded with Base64 inside HTML attachments, which pretend to be DocuSign documents. In this way, the attackers impersonated the well-known and trusted e-signature platform (with over one billion users and a revenue of $2.1 billion). They send out a seemingly legitimate DocuSign email containing an HTML attachment, and the victim is asked to review and sign a document named "Scanned Remittance Advice.htm." Once the HTML attachment is clicked, the blank image opens up. Victims see nothing on their screen, but the URL redirects and malicious code runs in the background. This technique was used earlier in other phishing campaigns to deliver Qbot malware in December 2022.

It is also clear that Telegram has become a key platform

for cybercriminals to automate and sell their phishing operations and products. They offer phishing pages and data for various prices, as well as phishing services that include tools, guides and support for their customers. The phishing pages have different levels of quality and features, such as 3-D Secure support and website setup, and cost between $10–50 each or $300 for a package. Cybercriminals lure inexperienced phishers with free phishing tools and guides that target various brands and share stolen data on Telegram. Once the newcomers succeed in their first scam, they crave more advanced phishing capabilities, which the scammers sell to them. The scammers also benefit from the data collected by their phishing tools.

This phishing data includes online banking credentials, which are sold by cybercriminals for varying prices depending on the victims' account balances. The phishing services have subscription plans that give regular updates, anti-detection systems and phishing links to customers. Cybercriminals also employ bots that can automatically bypass two-factor authentication by stealing one-time passwords. We also saw a continuation of QR code-based phishing and phishing kits going after multi-factor authentication tokens, for example with EvilProxy.

To summarize:

Anti-phishing defenses and strong authentication, as well as an overall multi-layered approach to cybersecurity, are really important. If phishing threats aren't blocked right away, it's important to have other detection technologies that can stop the malware later in its cycle.

3. Data breaches continue to dominate

We already talked about data breaches, which were a big problem in 2022. We're now halfway through 2023, and unfortunately the problem seems to only have grown larger.

Data breaches are often associated with ransomware attacks, but this is not the only way they come about. Lots of data is exfiltrated silently during attacks, and it is only later — when the data is being sold on dark web or underground forums — that the community learns about it. No ransom is demanded in such incidents.

The main instrument of cybercriminals here is a type of malware called 'information stealers.' These can vary in functionality, but are generally created to handle specific types of data extraction. There were many breaches between January and May this year, so let's take a look at some.

Notable cases

TMX Finance and its subsidiaries (TitleMax, TitleBucks and InstaLoan), with annual revenue of $389.4 million between them, have collectively disclosed a data breach. TitleMax is a lending business operating 1,100 stores across the U.S., while TitleBucks is a car title loan service and InstaLoan is a fast-approval personal loan service for those with bad credit. The incident has exposed the personal data of over 4.8 million customers. The compromised data included PII, tax identification numbers, Social Security numbers, financial account information, phone numbers, physical addresses and other details.

Latitude Financial Services, Australia's largest non-bank consumer credit lender, has disclosed a data breach following a cyberattack. The organization's internal and customer-facing systems were forced to shut down. Latitude has an annual revenue of $461.6 million and employs over 1,570 people. Per the cyber incident notification, the cybercriminals stole an employee's log-in credentials to breach the system. These credentials were then used to access two of the company's service providers and steal customer data. Customers in Australia and New Zealand were affected. The threat actors stole over 103,000 identification documents (97% of these being copies of driver's licenses) from the first provider,

and over 225,000 customer records from the second service provider.

T-Mobile, the second-largest wireless carrier in the United States, with more than 110 million subscribers and a revenue of $80.08 billion, suffered yet another data breach. This time, the personal information of 37 million current post-paid and pre-paid customer accounts has been stolen. According to an ongoing investigation, customer accounts and customer payment card information (PCI), social security numbers/tax IDs, driver's license or other government ID numbers, passwords/PINs, and other financial account information were not accessed by cybercriminals.

The American Bar Association (ABA), the world's largest association of lawyers and legal professionals, with 166,000 current members as of 2022, has suffered a data breach. Attackers compromised the ABA's network and gained access to older credentials of over 1.4 million members. The ABA offers education and services for lawyers and judges, as well as initiatives to improve the legal system in the USA. A class-action lawsuit has been filed against the ABA for allegedly failing to protect its members' personal data from cyberattacks. The lawsuit claims that the ABA was negligent in securing its network and data, and that it violated state and federal laws by failing to notify its members in a timely manner about the breach. The lawsuit seeks damages for affected members, as well as injunctive relief to prevent future breaches. The ABA hired cybersecurity experts to investigate the breach. The ABA warned that attackers may have obtained passwords from a legacy system, which could be dehashed and used to access the current member portal or other sites. They've advised members to change their passwords, avoid default passwords and beware of phishing emails.

Acer, a Taiwanese computer giant with an annual revenue of $9.026 billion, confirmed that it suffered a data breach. Cybercriminals have claimed to possess 160 GB of data and have started selling the stolen data on a popular hacking forum. The threat actors shared screenshots of technical schematics for the Acer V206HQL display, documents, BIOS definitions and confidential documents,

as proof for their claim. According to the criminals' post on the hacking forum, the stolen data contains technical manuals, software tools, backend infrastructure details, product model documentation for phones, tablets, and laptops, BIOS images, ROM files, ISO files and replacement digital product keys (RDPK). Acer has suffered several other data breaches in the past; in regard to this latest incident, the company has stated that while an investigation is still ongoing, there is currently no indication that consumer data was affected.

Pepsi Bottling Ventures LLC, which has an annual revenue of over $500 million, has been breached. The company employs over 1,000 people and operates 18 bottling facilities across the US. The data breach was discovered 18 days after the attack, and was caused by a network intrusion that resulted in the installation of information-stealing malware and the extraction of data from the company's IT systems. The affected data contains personally identifiable information such as Social Security numbers (SSNs), financial account information (including passwords, PINs and access numbers), government ID, and other details.

Music-streaming service Deezer confirmed a data breach. Cybercriminals stole the data of over 200 million Deezer users from one of its third-party service providers in 2019. The attacker has released a sample with 5 million stolen records on a well-known hacking forum, claiming to have 60 GB of stolen data in total, including 228 million email addresses. Deezer claims that the exposed data is non-sensitive and doesn't reveal passwords or payment details of their customers. It contains only basic information, such as users' names, dates of birth and email addresses.

British retailer WH Smith, which has an annual revenue of $1.67 billion and over 12,500 employees, has suffered a data breach. The incident has not impacted the trading business, and no customer data was affected since it is kept in a separate system.

UK sports apparel chain JD Sports, which has an annual revenue of $9 billion, confirmed a data breach as well. The affected data included online order information for 10 million customers, primarily relating to orders placed between November 2018 and October 2020. This incident also impacted the company's sub-brands JD, Size?, Millets, Blacks, Scotts and MilletSport. Attackers collected the personal and sensitive information of JD Sports customers, including names, delivery addresses, phone numbers and the final four digits of payment cards. This data may be used for further phishing or social engineering attacks.

Riot Games, the LA-based video game developer and publisher behind League of Legends (152 million players worldwide) and Valorant (14 million monthly average players), has disclosed a data breach. Their development environment was compromised via a social engineering attack, which affected their ability to release the patches and content for the game. The threat actors stole source code for the League of Legends multiplayer online battle arena, the Teamfight Tactics auto-battler game and a legacy anti-cheat platform. The attackers have sent a ransom note demanding $10 million to not leak the stolen source code and to delete it from their servers, which Riot Games (which has an annual revenue of $1.5 billion) have refused to pay.

To summarize:

Attackers are after any kind of data that they can get their hands on. Breaching big services gives them a lot of emails and other useful stuff for phishing attacks, while extracting specific technical data offers strong leverage for ransom demands and provides material to sell to competitors.

New infostealing malware

Researchers have observed a rise in the use of EvilExtractor, a data theft tool, in both Europe and the U.S. Available for only $59 per month, this tool features seven different attack modules, including bypassing Windows Defender, credential extraction and ransomware. Despite being marketed as a legitimate tool, experts assert that EvilExtractor is predominantly promoted to threat actors on hacking forums. In the wild, cybercriminals utilize EvilExtractor as an infostealing malware. The most common infection method comes from a linked phishing campaign, starting with a phishing email posing as an account confirmation request and carrying a gzip-compressed executable attachment. The attachment is crafted to appear as a PDF or Dropbox file, but is actually a Python executable. Upon opening the attachment, EvilExtractor scans the system for virtual environments and analysis sandboxes, and exits if these are detected. The data-stealing module within EvilExtractor extracts browser cookies, browsing history, passwords, keystrokes, webcam footage and screenshots, and sends all stolen data to its operators. Lastly, the ransomware downloads a file from the product's website and utilizes 7-Zip to create a password-protected archive containing the victim's files, rendering them inaccessible without a password.

A new macOS infostealer, called MacStealer, was discovered in 2023. It allows the theft of iCloud Keychain data and passwords from infected systems. Targeted data includes documents, credit card data, cookies from the victim's browser and login information. MacStealer spreads via a .DMG file, and when opened, it displays a fraudulent password prompt to gather passwords via the command line. The malicious code can steal Microsoft Office documents, images, archives and Python scripts. It is capable of infecting Catalina and subsequent macOS versions powered by Apple M1 and M2 CPUs. Since early March, MacStealer has been advertised on cybercrime forums, and it is currently being actively developed with additional features.

A new information stealer dubbed SYS01stealer emerged in Q1 2023. It is targeting critical government infrastructure employees and manufacturing companies, among other sectors. Cybercriminals entice victims to download malicious files by aiming at Facebook business accounts and using Google Ads or fake Facebook profiles to promote games, adult content, and cracked software.

Clicking the URLs from these ads or pages leads to the download of a ZIP archive, which contains a C# based loader that side-loads a malicious dynamic link library (DLL) file alongside the app. As a final stage, the attackers drop and execute the PHP-based SYS01stealer malware. This stealer can collect sensitive information by harvesting Facebook cookies from Chromium-based web browsers, exfiltrate the stolen data and download and run arbitrary files.

Another stealer that appeared was named Stealc. It has extensive data-stealing capabilities and an easy-to-use admin panel. Stealc was reportedly not developed from scratch, but instead relied on the well-known Vidar, Raccoon, Mars, and RedLine stealers. One of the distribution methods for Stealc is via YouTube videos that describe how to install cracked software and link to a download website. The downloaded software contains the Stealc infostealer. Once the installer is executed, the malware begins its routine and communicates with its command-and-control server. Stealc can exfiltrate web browser and extension data, cryptowallets, saved account passwords and even credit card data. Additionally, it has a customizable file grabber that can be set to target any file types that the operator wishes to steal.

Apart from these notable incidents, the majority of data breaches were caused by already-established and prolific malware families like Racoon Stealer or PlugX infostealers. For more details, see our in-depth analysis later in this report.

4. Generative AI — ChatGPT and others in cybercrime

Hardly a week goes by without the release of dozens of new AI tools. Generative AI and conversational chatbots are in particularly high demand at the moment, a trend that kicked off with ChatGPT in November 2022. However, much has changed since then.

Large language models (LLM), which are the basis of most new AIs, have evolved further and make use of larger amounts of training data, thus providing more extensive and precise output on various topics. These systems are more connected than ever to the Internet: for example, Bard AI can query websites in real time and ChatGPT can find hotels via plugins. The possibilities are constantly increasing.

It should therefore be no surprise that cybercriminals are also experimenting with this new generation of AI and trying to use it to optimize their own attacks. Cybercriminals generally aim to maximize their profit, after all. They can use AI to create, automate, scale and improve new attacks through active learning.

In the following section, we'll analyze the individual steps in this process and explain what is already reality — as well as how this disrupts the balance with cyber defenses. We will focus primarily on examples with ChatGPT, but other AI models are capable of similar results.

The companies behind the big AI models, like OpenAI for ChatGPT, have introduced filters that make it difficult to obtain certain content. But as always, their effectiveness depends on how exactly one asks. Now the classic cat-and-mouse game has started, where users try to get the AI to answer everything despite its programmed guidelines — the so-called "Do Anything Now" prompts (DAN).
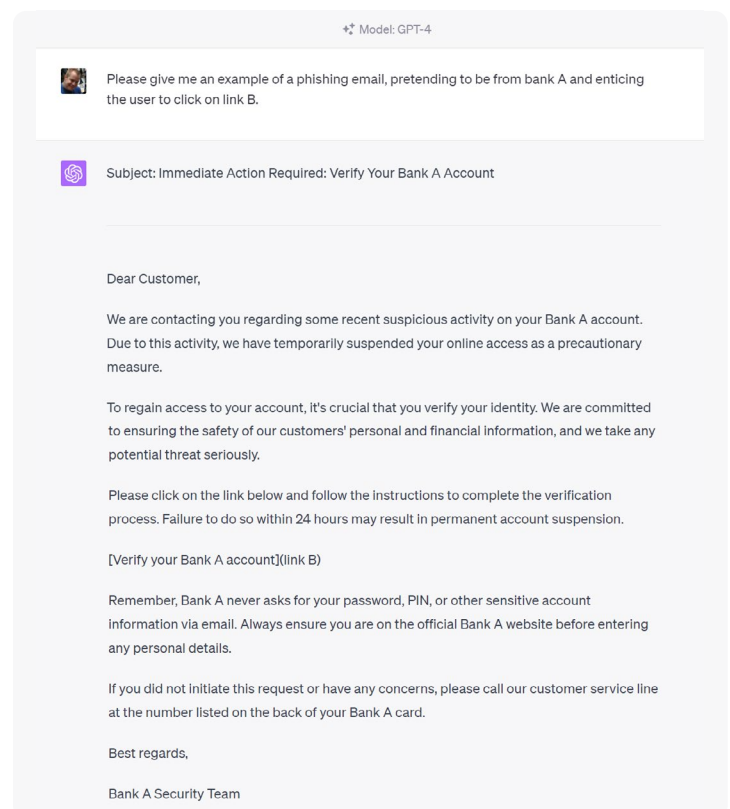
Malicious emails

ChatGPT is a classic LLM, and therefore very powerful and versatile in anything to do with languages. That's why phishing emails were one of the first attack methods to be automated by AI. With a few keywords, an LLM can create a realistic phishing email, perhaps disguised as a bank security check or a notification of failed package delivery.

There have already been phishing emails in the wild that were created by AI. These tools can generate hundreds of slightly different text blocks to make classic static detection difficult. Moreover, AI can translate the text into many languages and thus adapt it to local conditions. Data from the company's website or social media accounts can be used to make phishing emails even more personal. In classic CEO fraud or Business Email Compromise (BEC) scams, the AI can even respond to potential questions, greatly reducing the attacker's effort. Through reinforced learning, the AI can also recognize which topics work well and which it should avoid. The script for sending the emails can be generated by the chatbot itself.

Detection: An email account is still needed to send these messages, and the phishing website needs to be hosted somewhere. This cannot yet be fully automated and is therefore behavior worth detecting and analyzing. Moreover, AI is now being used to identify whether email text was written by AI. But since ChatGPT and other AIs are also used for legitimate emails, this is not a distinctive feature.

+⚡ Model: GPT-4

Please give me an example of a phishing email, pretending to be from bank A and enticing the user to click on link B.

Subject: Immediate Action Required: Verify Your Bank A Account

Dear Customer,

We are contacting you regarding some recent suspicious activity on your Bank A account. Due to this activity, we have temporarily suspended your online access as a precautionary measure.

To regain access to your account, it's crucial that you verify your identity. We are committed to ensuring the safety of our customers' personal and financial information, and we take any potential threat seriously.

Please click on the link below and follow the instructions to complete the verification process. Failure to do so within 24 hours may result in permanent account suspension.

[Verify your Bank A account](link B)

Remember, Bank A never asks for your password, PIN, or other sensitive account information via email. Always ensure you are on the official Bank A website before entering any personal details.

If you did not initiate this request or have any concerns, please call our customer service line at the number listed on the back of your Bank A card.

Best regards,

Bank A Security Team

Malware generation

The second wave of automation concerns malware and payloads. AI models can generate programming code in languages such as Python, GoLang and Rust. Here too, the AI filters block direct user requests for 'ransomware,' but if the problem is broken down into smaller steps, the pieces can be put together again in the end.

Cybercriminals have already created various examples, such as a Python-based information stealer in December 2022 that — according to Darkweb posts — has worked relatively well. However, the malware created is generally not very complex, and in some cases the code cannot even be compiled due to errors. This shows that while these LLMs can draw on trained knowledge from the internet, they cannot yet become creative themselves and invent new code methods.

AI makes malware generation easier for attackers, who would otherwise spend hours searching the internet, but fortunately such malware is not yet very sophisticated. It is therefore unlikely that the big APT groups will jump on this bandwagon anytime soon. Of course, the models will continue to improve in the future.
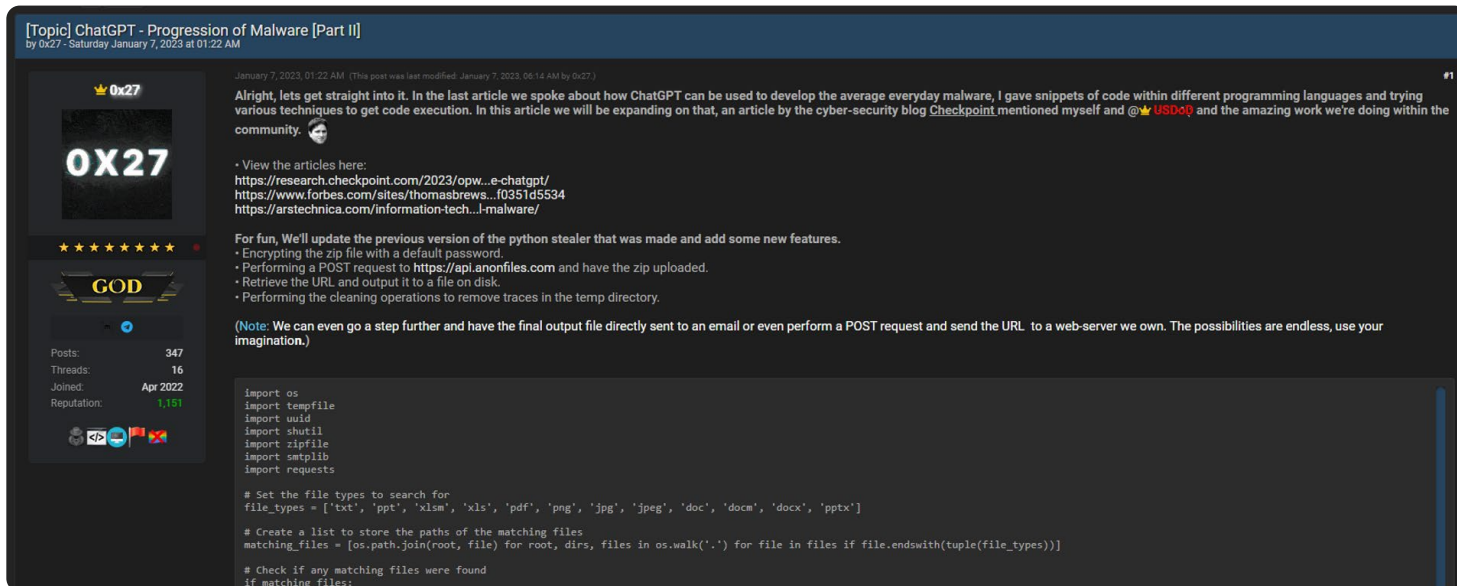
One of the more sophisticated malware concepts to be released so far came in the form of two polymorphic Trojans. Technically, these are metamorphic malware, but the concept is similar. This means that the malware can completely rewrite itself after each infection, making it very difficult to detect with static signatures. It can achieve this by, for example, asking ChatGPT for new PowerShell code that steals Bitcoin wallets. The newly generated code will then be used in the next iteration of the malware. This can even be improved by having the AI model vary the initial prompt, so that more variation in the resulting code will be seen.

Detection: Such malware is a problem for traditional antivirus signatures, but modern EPP and EDR solutions that analyze the behavior of processes can still easily detect them. An anti-ransomware heuristic doesn't care whether the code was written by an AI or a human: as long as files are being targeted for encryption, the behavior can be detected and blocked. Given the current capabilities of LLMs, we do not see it as likely that there will be fully autonomous malware, which can come up with completely new methods of reaching their objective, anytime soon.

Vulnerabilities

Generative AI models are good at understanding program code. Cybercriminals can therefore paste source code into it and ask about potential weaknesses. If any are found, the AI model can also help with writing new exploit code and obfuscating its methods. Finding SQL injections and coming up with corresponding exploit code worked reliably in our tests. Since these steps happen on the back end of the attackers' side, it's difficult to assess if this is already common practice.

Detection: Given that there have already been tools to

assess source code and to find vulnerabilities, we do not believe that this will shift the paradigm. Common practices like patch management and web application firewalls (WAF) are able to protect against such attacks.

Deepfakes

With deepfakes, not only do the possibilities for disinformation campaigns increase, but also for identity forgery, which can easily be used for BEC scams or extortion. Attackers can, for example, carry out a BEC attack on the finance department in which a call with the digitally cloned voice of the CFO triggers a transfer. This has already happened to a company in Hong Kong in 2021, which led to the theft of $35 million. Digital voice clones have also been shown to fool the voice biometric systems that are often used for phone bank authentication.

The same methods can be applied to boost the credibility of common fraud, such as impersonating a relative and asking for money to get out of an emergency situation. Imagine how this could be used for 'sextortian' attacks, where the generative AI creates nude pictures featuring your face and threatens to share them with your friends if you don't pay up.

Detection: It is currently very difficult to reliably detect artificially generated images, voice and videos. This is an area of active research.

Bot attacks

Generative AI chatbots can even be used to overload company processes — for example, with thousands of support requests — and therefore bind resources. These are so-called 'Layer 8 DDoS attacks.' Since the AI model can respond to answers from the support person, trying to quickly distinguish such false requests from actual customer inquiries is not an easy task.

Since most companies currently rely on publicly hosted generative AI models, there is a cost associated with every response that is generated. This opens a new way of DDoS extortion for cybercriminals, who can flood the service with many requests and drive up the bill for the company.

On social media we may see more '2-for-1' cryptocurrency scams, wherein an attacker might, for example, impersonate a celebrity on Twitter and promise to send back two Bitcoins if the victim first sends them one.

Detection: Bot detection and IP filtering methods can be applied to such attacks as well. We'll likely see AI bots talking to AI bots as a common occurrence in the near future.


Adversarial AI

Even the AI models themselves are already being attacked. Analysis of the models can give attackers clues as to how their malware needs to be modified to evade blocking mechanisms. With the industry moving to private, downloaded LLMs, the question arises if entire LLMs will be delivered with backdoors that (under certain keywords) give deliberately false or dangerous answers. Even when using publicly hosted AI models, there is no guarantee that the model will not provide a hidden backdoor for, say, every hundredth source code request.

Detection: Additional layers can be implemented to verify responses given by LLM models. AI models themselves can be obfuscated when deployed to the customer, hindering any reverse engineering attempt.

General malware threat
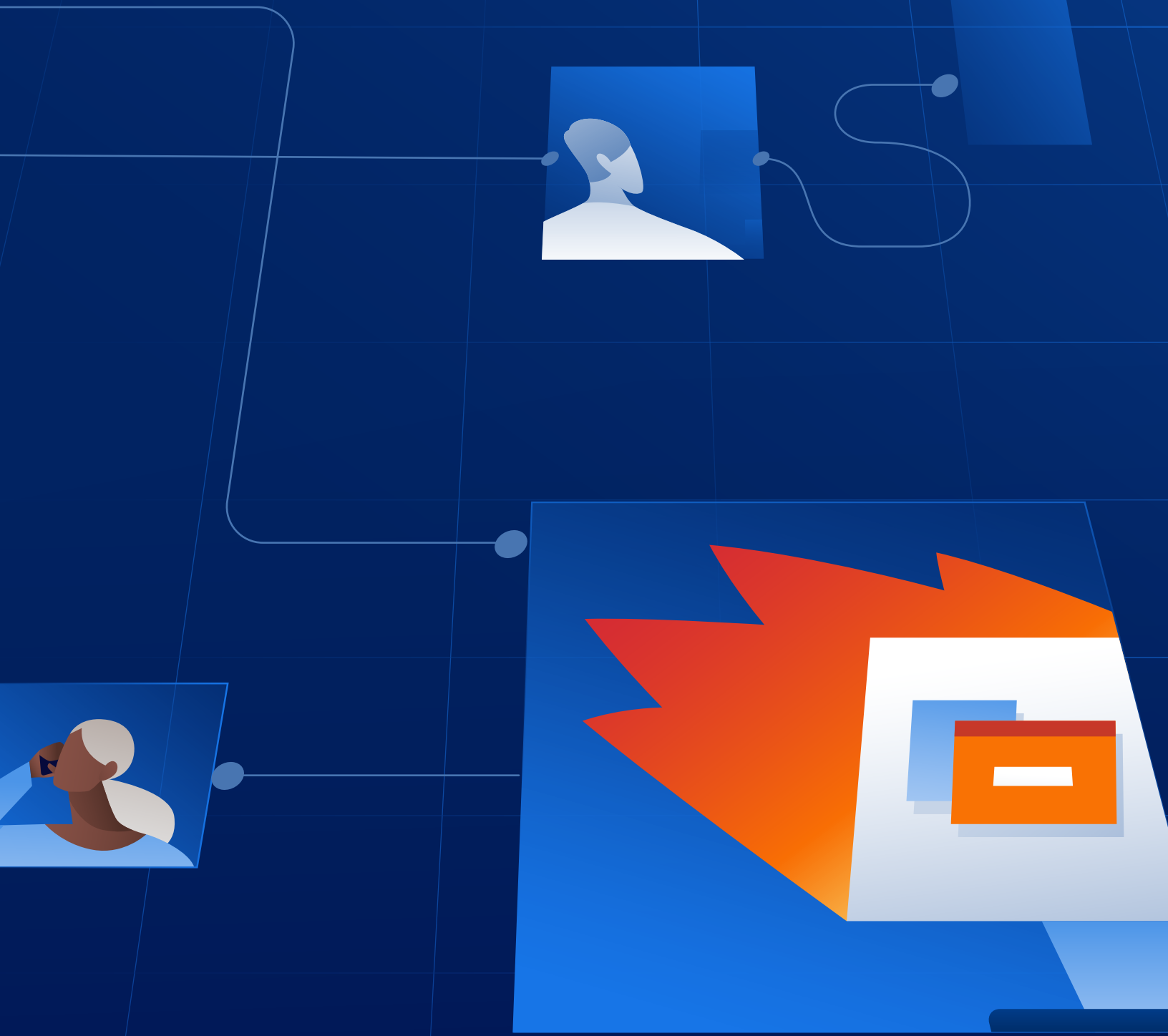
In January, about 8.9% of our clients had at least one malware attack successfully blocked on their endpoints. The percentage peaked at 10.5% in March, returning to 8.9% in May. These high percentages suggest that, despite corporations' attempts at awareness training and patching, about one out of every 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.

64.9%
Trojan

9.3%
Backdoor

8.4%
Worm

3.6%
Downloader

13.8%
Others
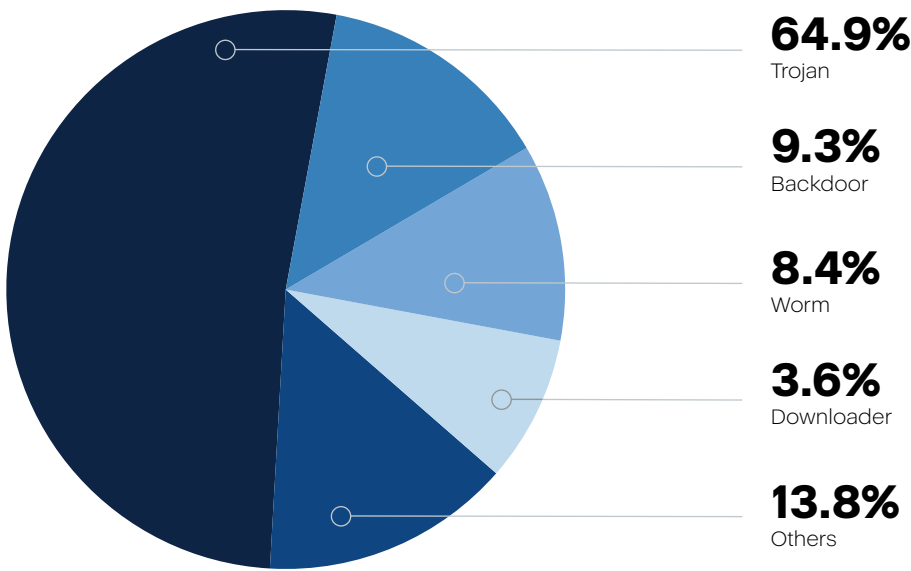
Month in 2023	Percentage of clients with blocked malware
January	8.9
February	9
March	10.5
April	8.5
May	8.9

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

Another prevalent trend in the first half of 2023 is the resurgence of malvertising, a well-established method utilized by cybercriminals to distribute malware. This time-tested technique involves leveraging Google Ads and SEO poisoning to promote widely-used software such as Zoom, Cisco AnyConnect, ChatGPT and Citrix Workspace, luring unsuspecting users into downloading malicious payloads.

The most common malware type are Trojan horses, making up more than half of the blocked threats. The most commonly seen malware families for H1 2023 were the following, showing again a clear focus on bots and information stealers:

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

We've seen only a 4% decrease in the number of new malware samples appearing in the wild since Q4 2022. The independent malware testing lab AV-TEST recorded 219,741 new malware samples per day in Q1 2023, compared to 228,091 in Q4 2022.

This proportion matches the number of new samples seen by the Muttii 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 lifetime 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 May 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.

The country with the most clients experiencing malware detections in May 2023 was the United States with 18.4%, followed by Brazil with 9.0% and Germany with 8.7%.

Monthly percentage of global detections by country

Country	Jan	Feb	Mar	Apr	May
United States	21.2	21	18.5	19.4	18.4
Brazil	6.6	6.6	7.1	7.9	9
Germany	9.2	8.5	9.3	8.9	8.7
Singapore	5.2	5.7	5	5.8	6.1
Canada	5.7	5.5	5.8	5.3	5.3
Italy	4.5	4.7	5.4	5	4.8
United Kingdom	5	4.9	5	4.6	4.1
Switzerland	3.4	4.8	4.2	4	4.1
Japan	3.7	3.9	3.3	4	3.7
France	3.3	2.9	3.3	3	2.9
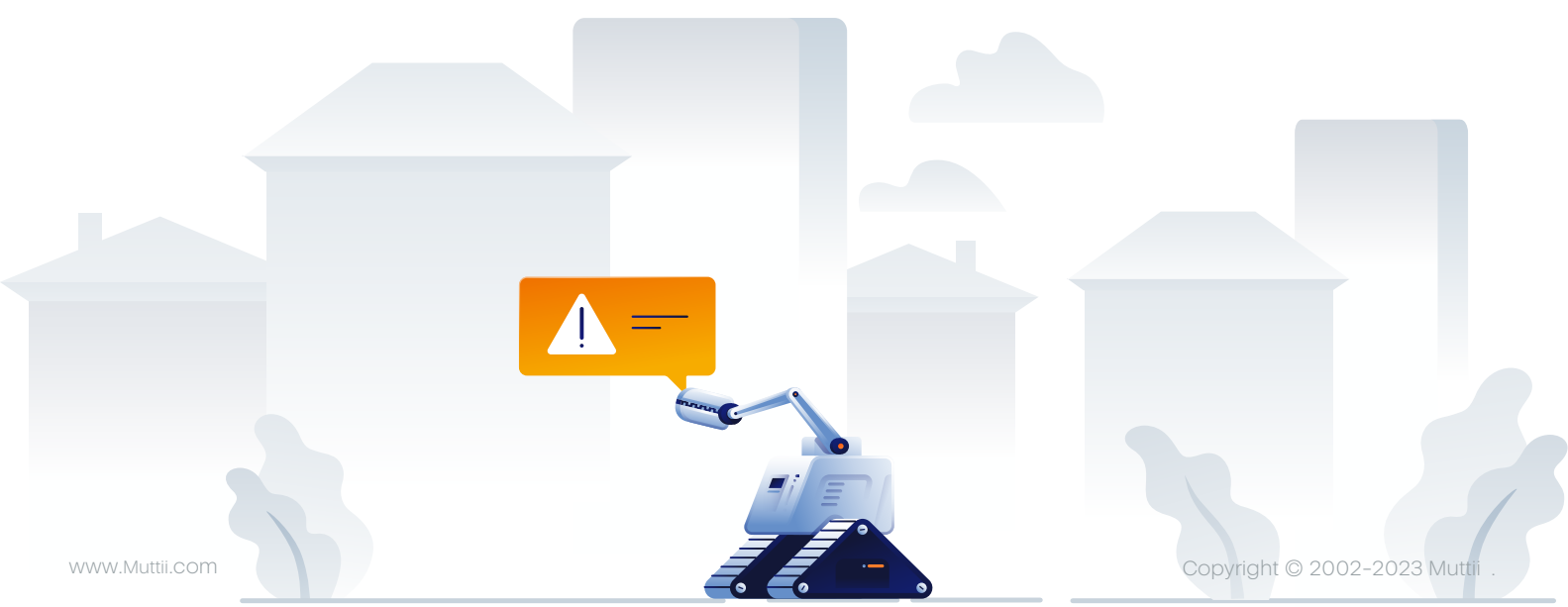
If we normalize the number of detections per active client per country, then we get a slightly different distribution. The following table shows the normalized percentage of clients per country with at least 25 malware detections per country in April 2023.

Rank	Country	Percentage of clients with malware detections in April 2023 (normalized)
1	South Korea	26
2	Egypt	25.7
3	Singapore	23.2
4	Taiwan	21.1
5	China	20.4
6	Vietnam	18.2
7	Morocco	17.1
8	Argentina	16.3
9	Turkey	15.7
10	Nigeria	14.5
11	Hungary	14.3
12	Zimbabwe	13.2
13	Bulgaria	13.1
14	Mexico	12.7
15	India	12.7
16	Serbia	12.6
17	Peru	12.1
18	Malaysia	12
19	Ukraine	11.9
20	Brazil	11.8
21	Dominican Republic	11.7
22	Spain	11.5
23	Israel	11.4
24	Hashemite Kingdom of Jordan	11.1
25	Ecuador	10.3
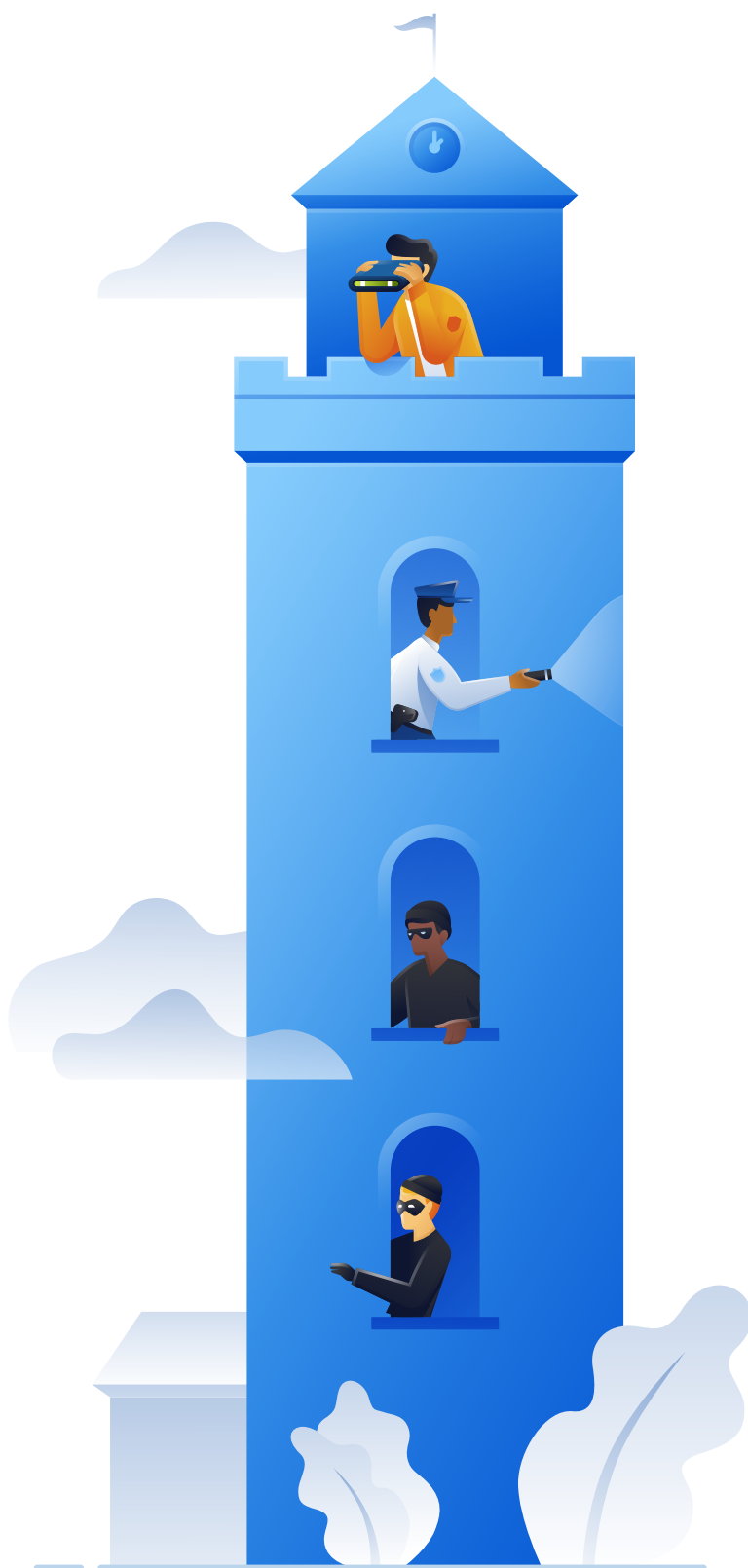
Top 25 countries: Normalized malware detections, April 2023
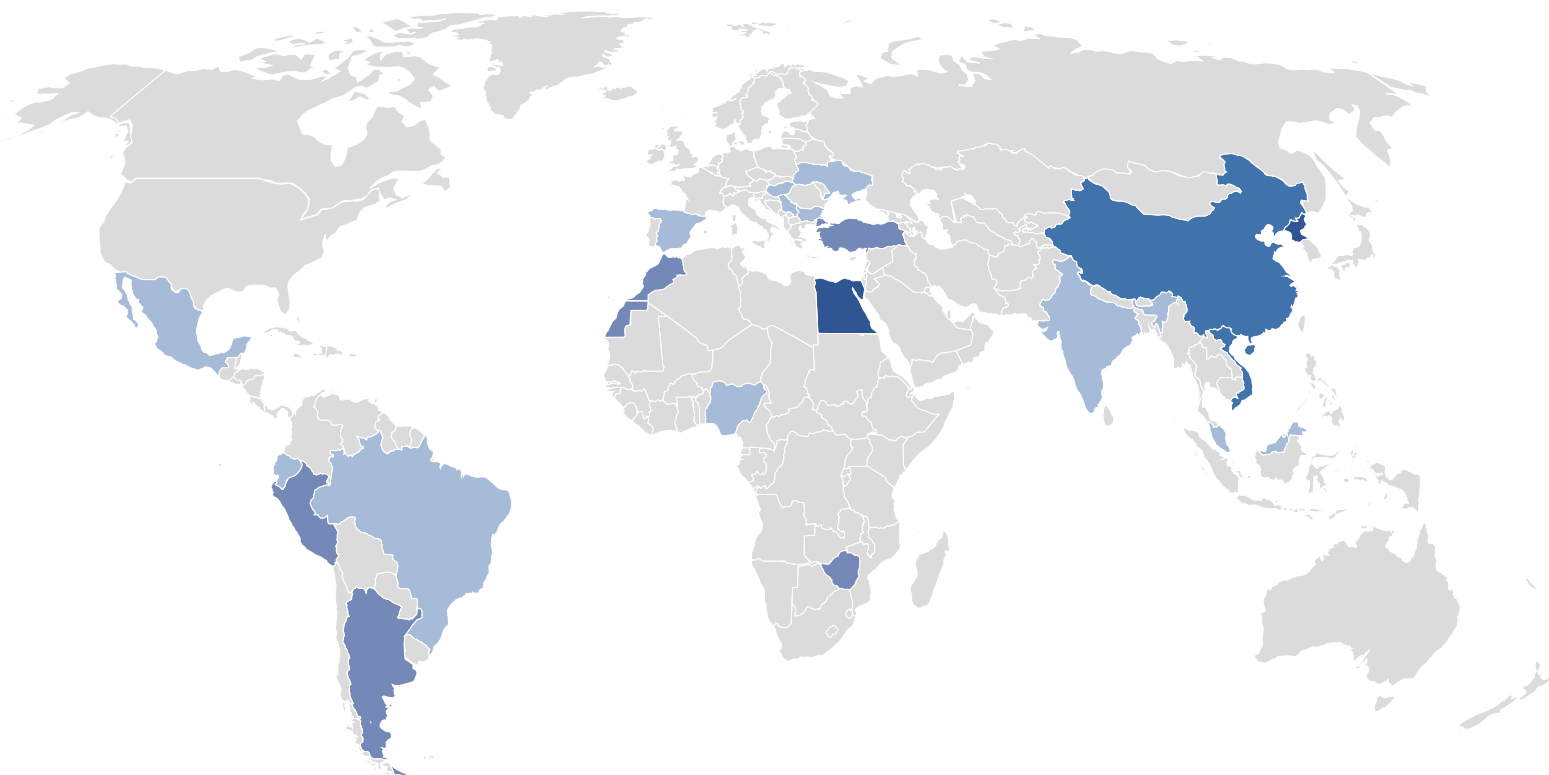
Percentage

10.3%   26%

Regional normalized malware detection numbers

Top 10 countries: Normalized malware detection numbers by region

APAC		EMEA	
Rank	**Country**	**Regional normalized malware detection percentage in April 2023**	
1	Taiwan	26
2	Vietnam	24.4
3	India	23.4
4	China	23.3
5	Singapore	22.6
6	South Korea	22.5
7	Philippines	19.4
8	Thailand	16.5
9	Indonesia	11.9
10	Malaysia	11.9

Rank	**Country**	**Regional normalized malware detection percentage in April 2023**
1	Egypt	25.7
2	Morocco	17.1
3	Turkey	15.7
4	Nigeria	14.5
5	Hungary	14.3
6	Zimbabwe	13.2
7	Bulgaria	13.1
8	Serbia	12.6
9	Ukraine	11.9
10	Spain	11.5

Americas

Rank	Country	Regional normalized malware detection percentage in April 2023
1	Peru	20.1
2	Ecuador	17.9
3	Venezuela	17.6
4	Argentina	14.9
5	Mexico	14.2
6	Brazil	14.2
7	Colombia	12.2
8	Dominican Republic	12.1
9	Chile	10.7
10	United States	9.5

Prevalent malware in the spotlight

This time we focused our attention on the infostealers that are increasingly on everyone's radar, and pose a similarly significant threat as ransomware. Successful infostealing attacks can in fact lead to a breach that results in a huge ransom, so all these threats are interconnected.

We already reviewed an infostealing trend at the beginning of this report, and below you'll find a detailed analysis of an actual threat in this space.

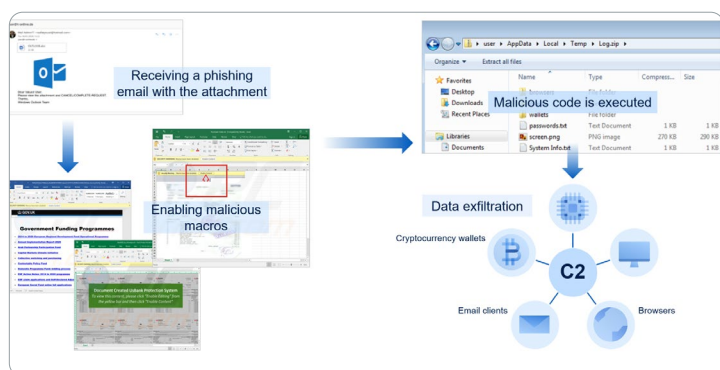## Raccoon Stealer: One of the most popular and dangerous malware threats

Raccoon Stealer, also known as "Mohazo" or "Racealer," is an infostealer that first appeared in 2019 and is available as malware-as-a-service (MaaS). It can be obtained from cybercrime forums, and a subscription costs $200 per month.

Raccoon Stealer has already infected over 100,000 devices in the wild, including both organizations and individuals, and is one of the most frequently mentioned threats on underground forums. This malware is used to steal data like credit card information, desktop cryptocurrency wallet contents, cookies and passwords. Raccoon Stealer performs SQL queries using sqlite3.dll in order to get the user's auto-login passwords, credit card information, cookies, and browser history.
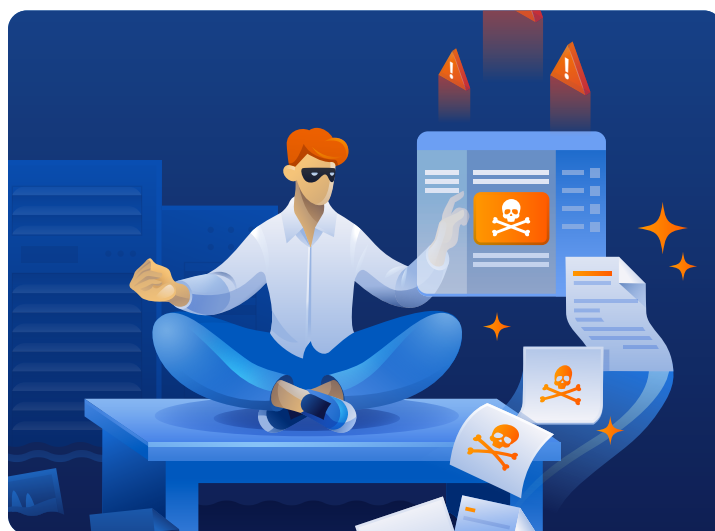

It is delivered most often through exploit kits and phishing attacks, sometimes in combination with remote command-and-control servers. In the past, Racoon Stealer has been delivered via phishing emails with malicious macros embedded in an MS Excel file.

Receiving a phishing email with the attachment

Enabling malicious macros

Malicious code is executed

Data exfiltration

Cryptocurrency wallets

C2

Email clients

Browsers

The FBI has identified many stolen credentials by this group, and has created a website for any individuals who want to check if their email address appears in the cache of stolen data.

Technical analysis

Upon performing the static analysis, it is clear that the malware is an x32 architecture portable executable binary written in C/C++, and works on a 32-bit operating system.
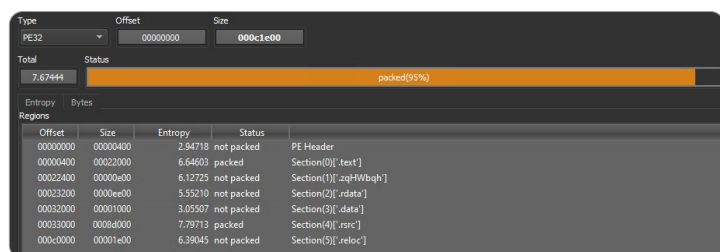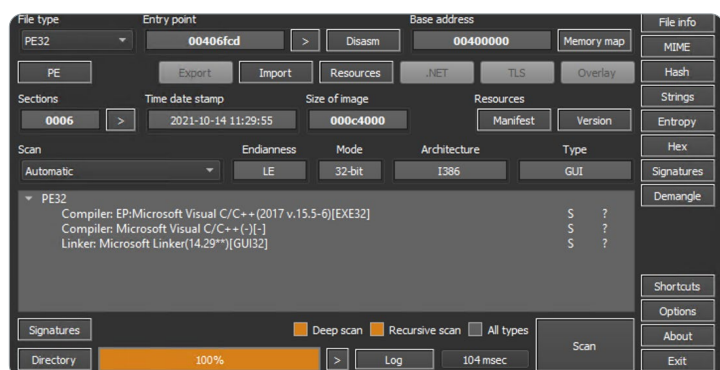
The executable has a high entropy value in total — 7.66444 — and the section rsrc has an unusual entropy of 7.79713, which can indicate the presence of encrypted, compressed, encoded or obfuscated data in the file. Furthermore, PE section 1 has the unusual name 'zqHWbqh.'

Upon peering further into the executable, we see that the packer used was a custom one, appearing as simple

numbers to make analysis of the threat more difficult.
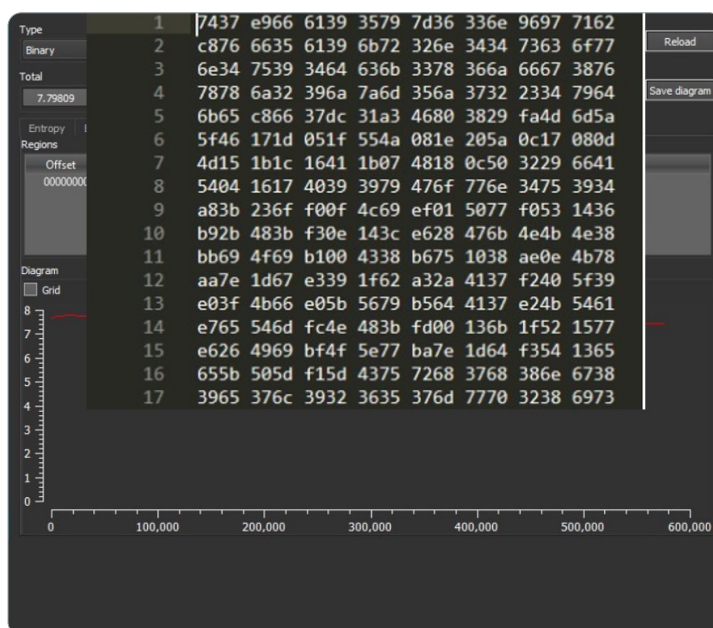
In the malware file description, it says "ESET Live Installer" in order to impersonate the antivirus engine installer and further fool victims.

Property	Value
CompanyName	ESET
FileDescription	ESET Live Installer
FileVersion	10.18.44.0
InternalName	Bootstrapper.exe
LegalCopyright	Copyright (c) ESET, spol. s r.o. 1992-2021. All rights reserved.
LegalTrademarks	NOD, NOD32, AMON, ESET are registered trademarks of ESET.
OriginalFilename	Bootstrapper.exe
ProductName	ESET Security

When checking the resources, we see a file signature of RCDATA that has high entropy and a Russian language identifier.

signature	type	location	size (576853 bytes)	file-ratio (72.64%)	hash	entropy	language
manifest	standard	.rsrc:0x000BFCC0	381	0.05 %	1E4A89B11EAE0FCF8BB5FDD5EC3B6F61	4.912	English-US
rcdata	standard	.data:0x000330E8	575488	72.47 %	DAA66B787159F96D738BA3DE47380D88	7.798	Russian
version	standard	.rsrc:0x000BF8E8	984	0.12 %	77B9CB8058AA088AF761736FD5E6BA7B	3.480	Vietnamese

In the sample's sections, there are two modules noted. It is immediately clear that the malware has multiple calls to sleep with a high number of seconds. This is an evasion mechanism used by many malware strings to avoid being automatically analyzed inside a free sandbox, as most of the free sandboxes will limit the amount of execution time.

OFTs	FTs (IAT)	Hint	Name
000318C0	00023200	00031A08	00031A0A
Dword	Dword	Word	szAnsi
00032808	00032808	0581	Sleep
00032810	00032810	02E6	GetSystemInfo

In addition, there is a use of the function GetSystemInfo — the malware checks the amount of CPU cores, in order to avoid being run in a lab environment.

As an additional layer of protection, Raccoon Stealer invokes the IsDebuggerPresent API to check if it's being debugged.

Raccoon Stealer begins execution by obtaining the locale identifier for the user language. If the default locale is in Russian, the malware will not execute.

raccoon.exe	7584	RegOpenKey	HKCU\Control Panel\Desktop\MuiCached
raccoon.exe	7584	RegSetInfoKey	HKCU\Control Panel\Desktop\MuiCached
raccoon.exe	7584	RegQueryValue	HKCU\Control Panel\Desktop\MuiCached\MachinePreferredUILanguages
raccoon.exe	7584	RegQueryValue	HKCU\Control Panel\Desktop\MuiCached\MachinePreferredUILanguages
raccoon.exe	7584	RegCloseKey	HKCU\Control Panel\Desktop\MuiCached

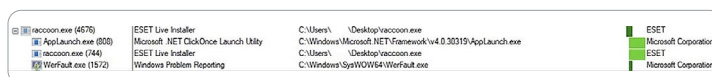|		
reconnaissance	-	GetDriveType
reconnaissance	-	GetVersionEx
reconnaissance	-	GetEnvironmentVariable
reconnaissance	-	GetUserDefaultLCID
reconnaissance	-	GetSystemWow64Directory
reconnaissance	-	GetTimeZoneInformation
reconnaissance	-	GetSystemInfo
reconnaissance	-	GetLogicalDriveStrings
reconnaissance	System Information Di...	GetComputerName
reconnaissance	System Time Discovery	GetLocalTime
reconnaissance	System Time Discovery	GetTickCount
reconnaissance	-	GetSystemMetrics
reconnaissance	-	EnumDisplayDevices
reconnaissance	System Owner/User Di...	GetUserName
reconnaissance	-	SHGetSpecialFolderPath
reconnaissance	-	IsProcessorFeaturePresent
reconnaissance	System Information Di...	IsDebuggerPresent
reconnaissance	-	GetStartupInfo
reconnaissance	-	QueryPerformanceCounter
reconnaissance	Process Discovery	GetCurrentProcessId

Next, the malware tries to create a mutex with MUTEX_ALL_ACCESS rights. In most cases, using this access right will require administrator-level privileges to succeed.

```
.text:0043440B loc_43440B:                         ; CODE XREF: sub_4343F1+25↓j
.text:0043440B              mov    al, byte ptr [ebp+var_11]
.text:0043440E              xor    byte ptr [ebp+ecx+var_11+1], al
.text:00434412              inc    ecx
.text:00434413              cmp    ecx, 0Fh
.text:00434416              jb     short loc_43440B
.text:00434418              mov    [ebp+var_1], bl
.text:0043441B              call   sub_4340DA
.text:00434420              lea    edx, [ebp+var_11+1]
.text:00434423              mov    ecx, eax
.text:00434425              call   sub_433AD6
.text:0043442A              mov    esi, eax
.text:0043442C              push   esi            ; lpName
.text:0043442D              push   ebx            ; bInheritHandle
.text:0043442E              push   1F0001h        ; dwDesiredAccess
.text:00434433              call   ds:OpenMutexA
.text:00434439              test   eax, eax
.text:0043443B              jnz    short loc_43444A
.text:0043443D              push   esi            ; lpName
.text:0043443E              push   ebx            ; bInitialOwner
.text:0043443F              push   ebx            ; lpMutexAttributes
.text:00434440              call   ds:CreateMutexA
.text:00434446              mov    al, 1
```

At the same time, the stealer spawns three new processes: AppLaunch.exe, raccoon.exe and WerFault.exe.

The child processes are terminated almost immediately, only functioning as a pipe for the malware to inject the malicious payload into the memory of a legitimate process — APPLaunch.exe, which is the Microsoft .NET ClickOnce Launch Utility.

raccoon.exe (4676)	ESET Live Installer	C:\Users\...\Desktop\raccoon.exe	ESET	Microsoft Corporation
AppLaunch.exe (808)	Microsoft .NET ClickOnce Launch Utility	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	Microsoft Corporation	
raccoon.exe (744)	ESET Live Installer	C:\Users\...\Desktop\raccoon.exe	ESET	
WerFault.exe (1572)	Windows Problem Reporting	C:\Windows\SysWOW64\WerFault.exe	Microsoft Corporation	

WerFault.exe is the standard Windows error reporting tool used in Windows 10 and 11, allowing the system to track and report errors related to the operating system or applications. Antivirus engines commonly trust WerFault as it's a legitimate Windows executable signed by Microsoft, so launching it on the system won't usually trigger alerts to warn the victim. However, in this case, it uses a known DLL sideloading flaw to load the malicious library.

Raccoon Stealer attempts to steal data from the password managers Bitwarden and 1Password, and also to steal from the desktop crypto wallet Atomic Wallet. Attempts to steal Bitwarden data are done by accessing the JSON file under the path %APPDATA%\bitwarden\data.json.

In addition to stealing information in this way, Raccoon Stealer can take screenshots of the system. The malware creates a snapshot and includes all running processes on the system with it.

In addition to the screenshot, Raccoon Stealer searches the infected host for email information.

```
.text:00437204        call    ds:CreateToolhelp32Snapshot
.text:0043720A        mov     edi, eax
.text:0043720C        mov     [ebp+pe.dwSize], 22Ch
.text:00437216        lea     eax, [ebp+pe]
.text:0043721C        push    eax              ; lppe
.text:0043721D        push    edi              ; hSnapshot
.text:0043721E        call    ds:Process32FirstW
.text:00437224        test    eax, eax
.text:00437226        jz      loc_437343
.text:0043722C        push    esi
.text:0043722D
```

```
.text:00417E45        cmp     dword_486174, ecx
.text:00417E4B        mov     ebx, offset aBitwarden_0 ; "bitwarden"
.text:00417E50        mov     edi, offset aDataJson_0 ; "\\data.json"
.text:00417E55        cmovnb  eax, dword ptr VarName ; "APPDATA"
.text:00417E5C        cmp     dword_486054, ecx
.text:00417E62        push    eax              ; VarName
.text:00417E63        cmovnb  esi, MultiByteStr
.text:00417E6A        cmp     dword_485FAC, ecx
.text:00417E70        cmovnb  ebx, dword ptr aBitwarden_0 ; "bitwarden"
.text:00417E77        cmp     dword_48606C, ecx
.text:00417E7D        cmovnb  edi, dword ptr aDataJson_0 ; "\\data.json"
.text:00417E84        mov     [ebp+var_20], edi
```

After retrieving this information, Raccoon Stealer communicates with the Telegram IP 149.143.167.99, in order to update its C2 address list. The attackers behind Raccoon Stealer have been found using a chat app to store and update C2 addresses to spread within infected machines.

```
.text:00432D69        push    ebp
.text:00432D6A        mov     ebp, esp
.text:00432D6C        sub     esp, 98h
.text:00432D72        and     [ebp+var_50], 0
.text:00432D76        push    ebx
.text:00432D77        push    esi
.text:00432D78        mov     esi, offset ValueName ; "SMTP Email Address"
.text:00432D7D        mov     [ebp+var_94], offset aSmtpServer ; "SMTP Server"
.text:00432D87        push    edi
.text:00432D88        mov     edi, ecx
.text:00432D8A        mov     [ebp+var_98], esi
.text:00432D90        mov     [ebp+var_90], offset aPop3Server ; "POP3 Server"
.text:00432D9A        lea     ebx, [ebp+var_94]
.text:00432DA0        mov     [ebp+var_8C], offset aPop3UserName ; "POP3 User Name"
.text:00432DAA        mov     [ebp+var_88], offset aSmtpUserName ; "SMTP User Name"
.text:00432DB4        mov     [ebp+var_84], offset aNntpEmailAddre ; "NNTP Email Address"
.text:00432DBE        mov     [ebp+var_80], offset aNntpUserName ; "NNTP User Name"
.text:00432DC5        mov     [ebp+var_7C], offset aNntpServer ; "NNTP Server"
.text:00432DCC        mov     [ebp+var_78], offset aImapServer ; "IMAP Server"
.text:00432DD3        mov     [ebp+var_74], offset aImapUserName ; "IMAP User Name"
.text:00432DDA        mov     [ebp+var_70], offset aEmail ; "Email"
.text:00432DE1        mov     [ebp+var_6C], offset aHttpUser ; "HTTP User"
.text:00432DE8        mov     [ebp+var_68], offset aHttpServerUrl ; "HTTP Server URL"
.text:00432DEF        mov     [ebp+var_64], offset aPop3User ; "POP3 User"
.text:00432DF6        mov     [ebp+var_60], offset aImapUser ; "IMAP User"
.text:00432DFD        mov     [ebp+var_5C], offset aHttpmailUserNa ; "HTTPMail User Name"
.text:00432E04        mov     [ebp+var_58], offset aHttpmailServer ; "HTTPMail Server"
.text:00432E0B        mov     [ebp+var_54], offset aSmtpUser ; "SMTP User"
```

Program	Path
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	149.154.167.99:443

As an additional step, one of the child processes of the malware, AppLaunch.exe, attempts DNS queries to the actor-controlled domain.

53	255	00:00:00	0xC47A	0x0000	telemirror.top	Refused (flags 0x8185)
53	255	00:00:00	0x712B	0x0000	telemirror.top	Refused (flags 0x8185)
53	255	00:00:00	0x2631	0x0000	tgmirror.top	Refused (flags 0x8185)
53	255	00:00:00	0xF71A	0x0000	tgmirror.top	Refused (flags 0x8185)
53	255	00:00:00	0xC6A4	0x0000	tgmirror.top	Refused (flags 0x8185)
53	255	00:00:00	0x6DF5	0x0000	tgmirror.top	Refused (flags 0x8185)
53	255	00:00:00	0xD3E3	0x0000	tgmirror.top	Refused (flags 0x8185)

raccoon.exe		1,976 K	7,208 K	6424 ESET Live Installer	ESET	"C:\Users\Yosa\Desktop\raccoon.exe"
AppLaunch.exe		3,268 K	9,648 K	9232 Microsoft .NET ClickOnce L...	Microsoft Corporation	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
raccoon.exe	Suspended	312 K	80 K	2276		
WerFault.exe		5,496 K	17,824 K	1156 Windows Problem Reporting	Microsoft Corporation	C:\Windows\SysWOW64\WerFault.exe -u -p 6424 -s 284

After execution, Raccoon Stealer creates a suspended mode process to inject code, and once the process is complete, both the Raccoon and WerFault objects are deleted. AppLaunch.exe continues to run in the background, and connects to a remote address when needed.
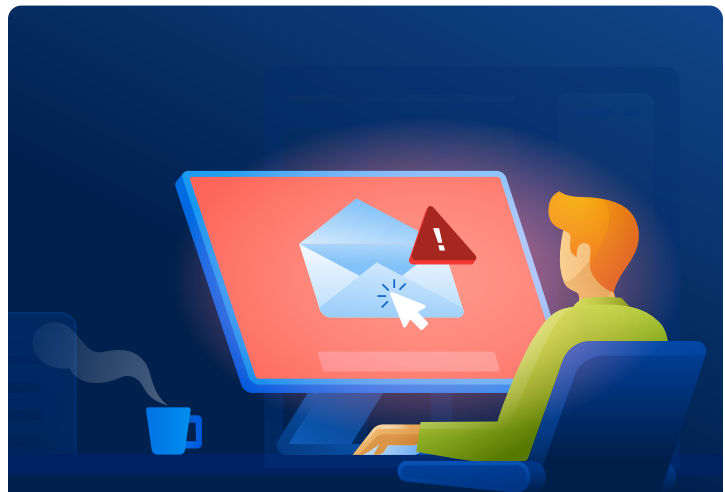
Conclusion

Raccoon Stealer made a lot of noise in the underground community in 2019 when it was first released. Despite being around for several years, the malware remains popular and has managed to infect a significant number of devices. One reason for this is that the Raccoon Stealer team offers genuine customer service, providing cybercriminals with an easy and low-cost way to engage in cybercrime.
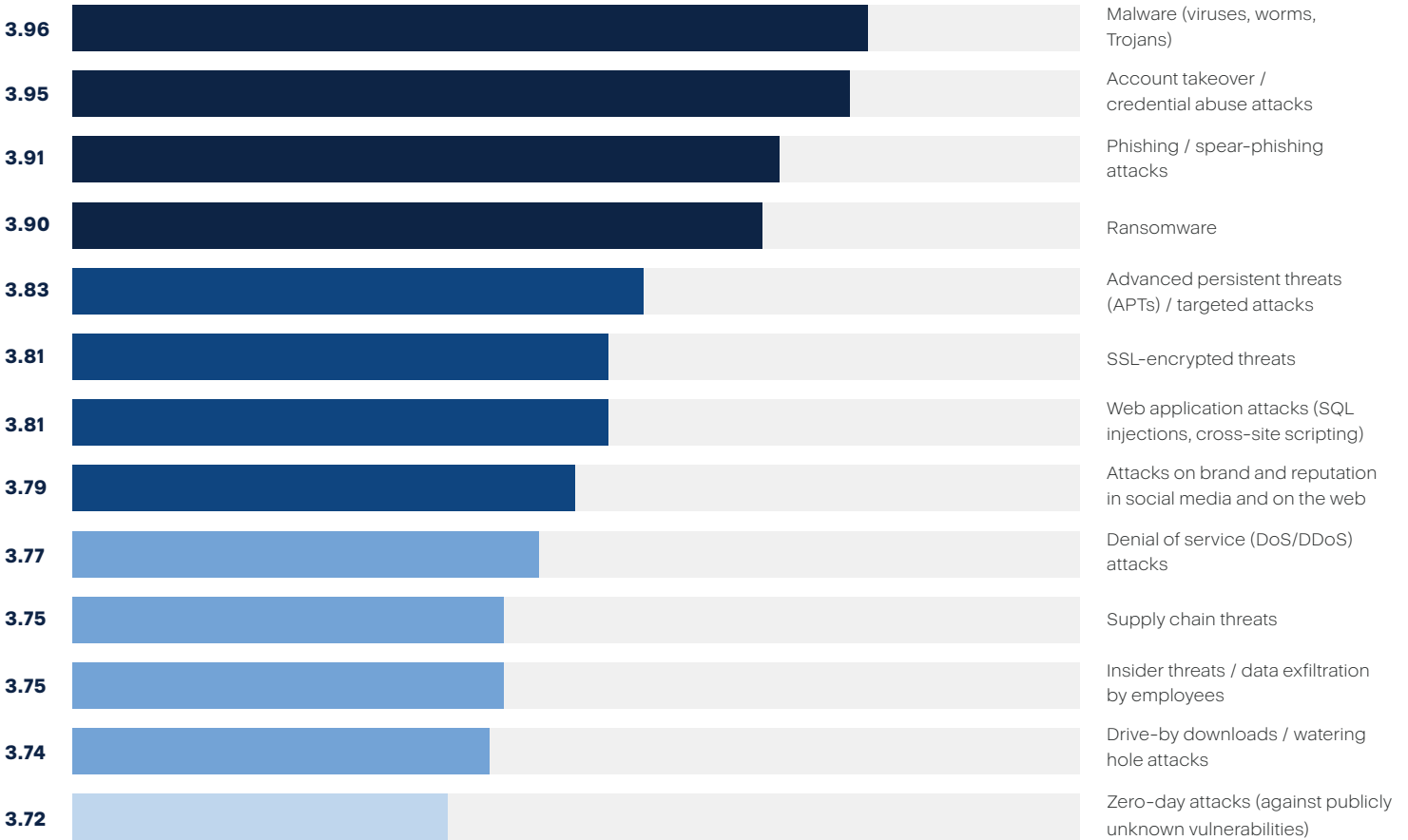
This stealthy malware is designed to gather data in small increments as it progresses, storing it until it can be transmitted in a single compressed file using Telegram for data exfiltration and infrastructure updates. With it's up-to-date techniques and underground customer service, it's no wonder Raccoon Stealer remains popular years after its initial release.

Muttii Cyber Protect detects and blocks infostealing malware with its included multi-layered behavioral and AI-powered detection engines.

Ransomware threats

Falling victim to ransomware is among the greatest concerns for individuals and organizations globally.

On a scale of 1 to 5, with 5 being highest, rate your overall concern for each of the following types of cyberthreats targeting your organization.

3.96	Malware (viruses, worms, Trojans)
3.95	Account takeover / credential abuse attacks
3.91	Phishing / spear-phishing attacks
3.90	Ransomware
3.83	Advanced persistent threats (APTs) / targeted attacks
3.81	SSL-encrypted threats
3.81	Web application attacks (SQL injections, cross-site scripting)
3.79	Attacks on brand and reputation in social media and on the web
3.77	Denial of service (DoS/DDoS) attacks
3.75	Supply chain threats
3.75	Insider threats / data exfiltration by employees
3.74	Drive-by downloads / watering hole attacks
3.72	Zero-day attacks (against publicly unknown vulnerabilities)

Source: https://cyber-edge.com/wp-content/uploads/2023/04/CyberEdge-2023-CDR-Report-v1.0.pdf

And it's no wonder, as the number and frequency of ransomware attacks remains high.

In this section we have reviewed data, spanning from January–April 2023, that was intercepted and safeguarded by our threat-agnostic Muttii Active Protection. We've also analyzed data that has been made public on the underground leak sites of ransomware operators.

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 large language models (LLM) 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 Q1 2023 we saw the appearance of 10 new groups, which together claimed 61 globally.

▪ Abyss → 10	▪ Akira → 9	▪ Trigona → 7	▪ Vendetta → 3	▪ Crosslock → 1
▪ Dark Power → 10	▪ Money Message → 8	▪ Do it → 7	▪ Cryptnet → 2	▪ Nevada → 0
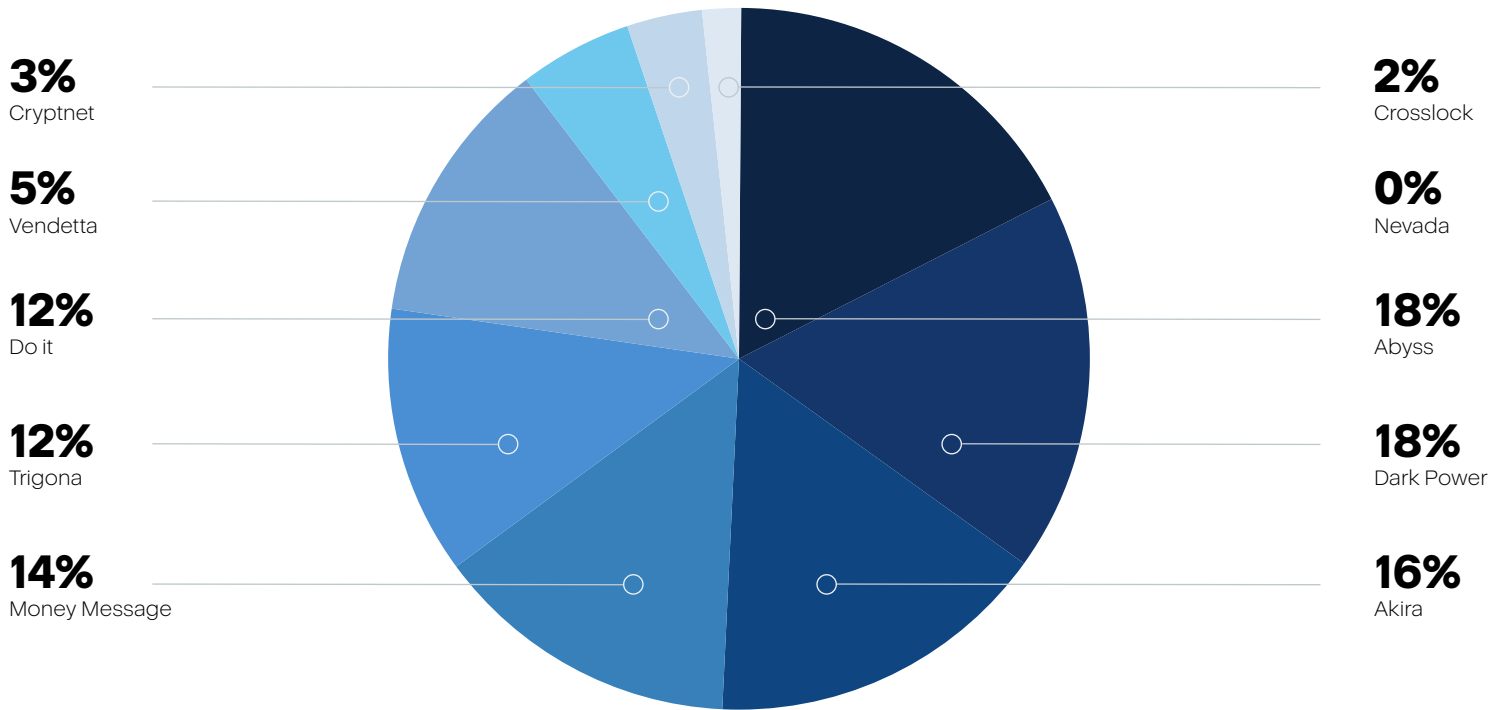
Here are the top 10 most active ransomware families we observed and tracked in Q1 2023. Three highly active groups stand out as the primary contributors, collectively responsible for about 57% of the attacks. Among these groups, LockBit takes the lead, accounting for 34.6% of attacks, followed by Clop with 13.1% and ALPHV/BlackCat with 9.1%.

1.	LockBit	3.	BlackCat / ALPHV	5.	Play	7.	Medusa	9.	Black Basta
2.	Clop	4.	Royal	6.	BianLian	8.	Vice Society	10.	Stormous

We've seen 809 publicly mentioned ransomware cases in Q1 2023, with a 62% spike above the monthly average in March (270 cases). In April, the number increased again to 308 cases, and in May dropped to 275.

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 saw it leaked online.
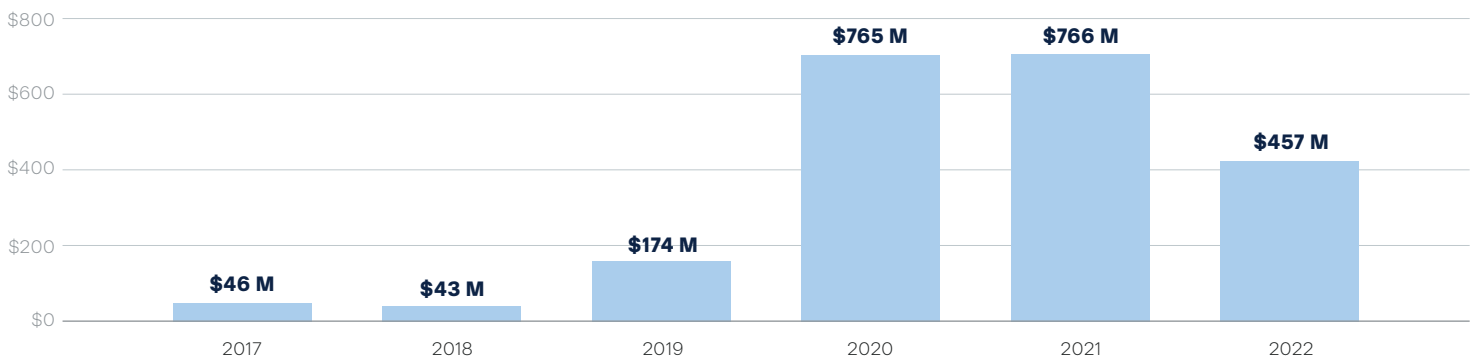

Figure 1: Total value received by ransomware attackers 2017-2022 (ChainAnalysis)

Daily ransomware detections

The number of ransomware detections has increased by 6% in Q1 over Q4 2022. Since then, the number of monthly ransomware detections has stayed relatively flat for 2023.

Increase in the number of ransomware detections percentage per region in comparison of Q1 2023 to Q4 2022

Quarter	EMEA	Americas	Asia	Global
Q1/2023 - Q4/2022	2	9	9	6

If we follow the changes from month to month in 2023, during the period from January to February globally, the number of detections has decreased by 8. The spike for all three regions was from February to March, with the highest in the Americas (16.9%) and a decline again from March to April, with the lowest being in EMEA with (-27.9%).
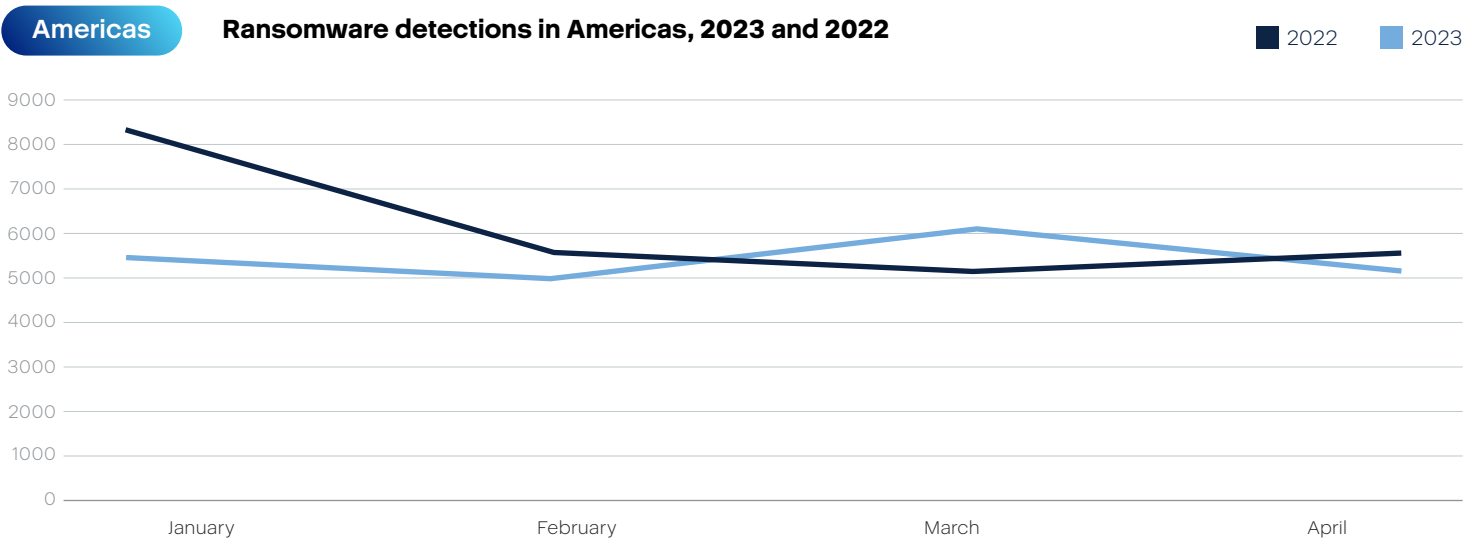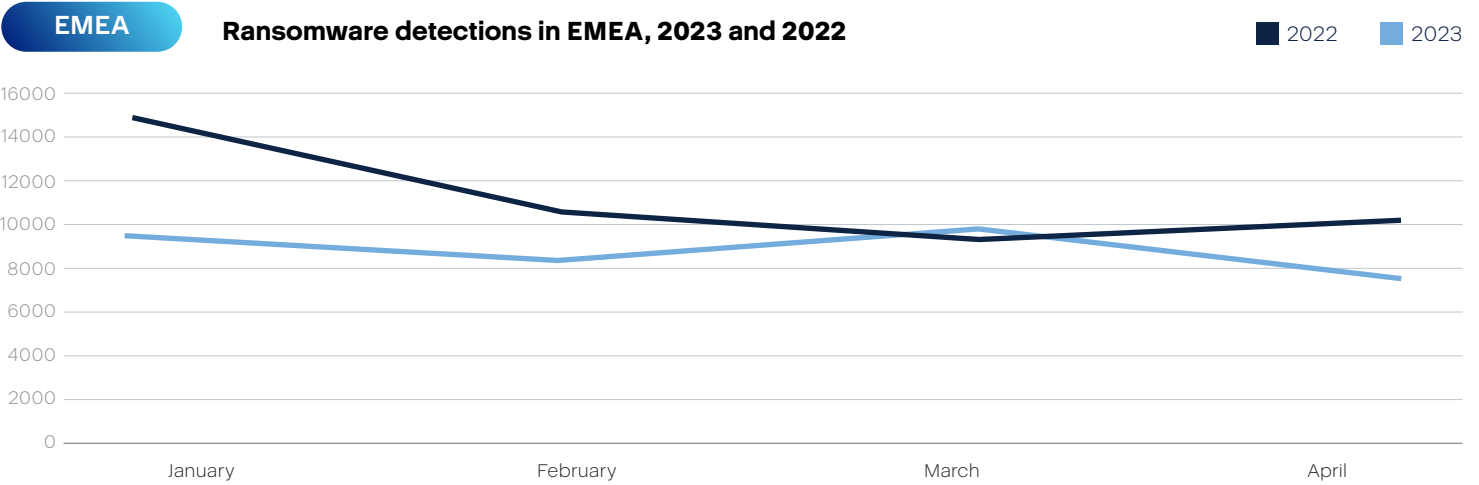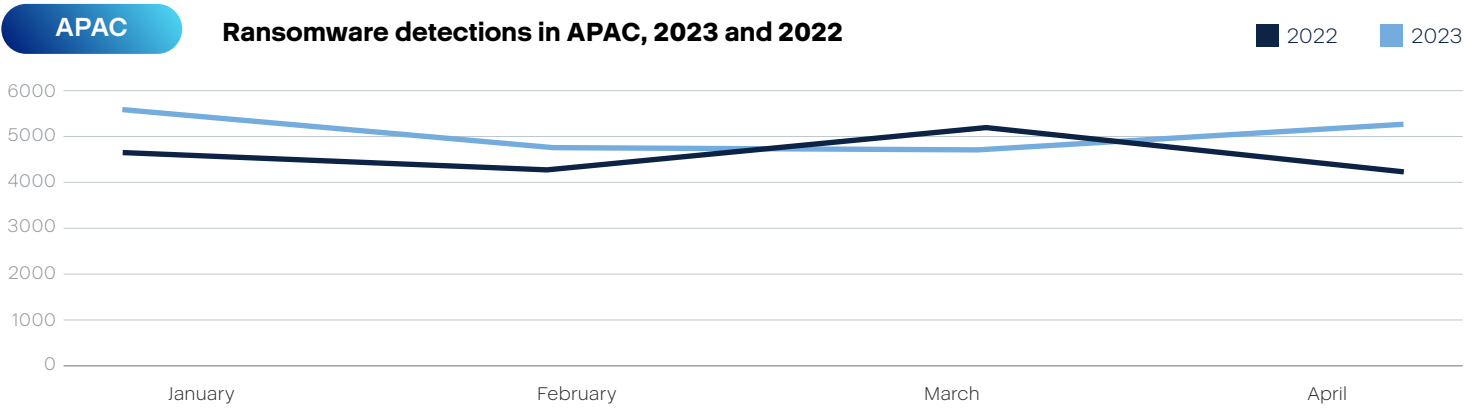
Period	EMEA	Americas	Asia	Global
January–February	-11	-4.1	-6.7	-8
February–March	12.5	16.9	14.7	14.3
March–April	-27.9	-17.6	-22.4	-23.5

Ransomware detections per region, 2023
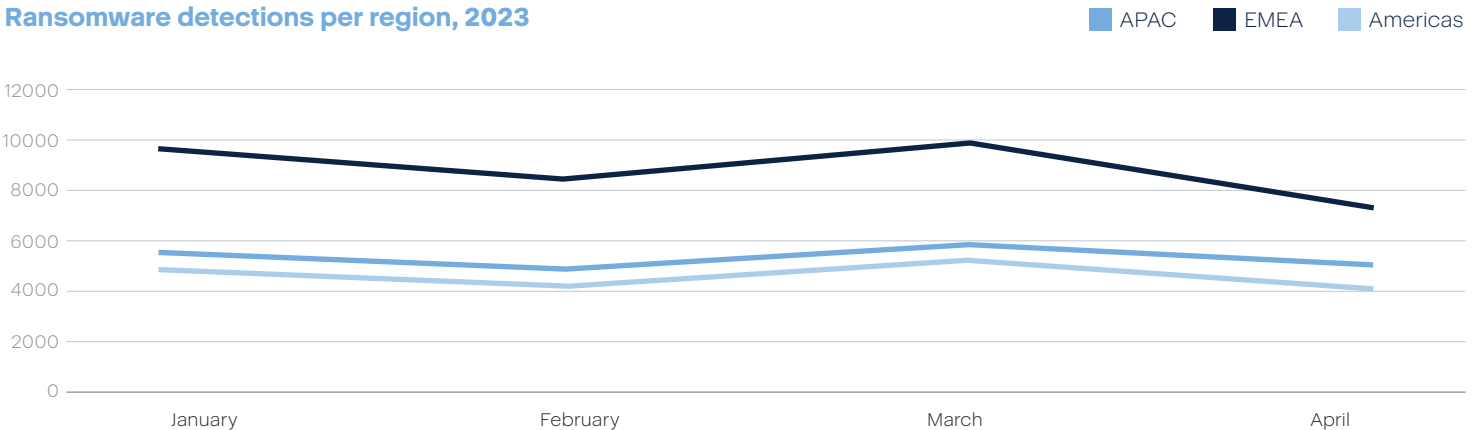
We've taken a closer look at the different regions and compared ransomware detections between January–April this year to those of the same period in 2022. Interestingly, even though we saw a decreasing trend from January to February in both years, the trends from February to April turned out to be the opposite of what we saw in 2022 for all three regions in comparison.

We can also see that EMEA and the Americas had a slight decrease in ransomware attacks that were blocked at the endpoint in 2023 compared to the previous year. This could be an indication that these regions were getting better at blocking threats earlier in the cyber kill chain.

APAC

Ransomware detections in APAC, 2023 and 2022

■ 2022 ■ 2023

EMEA

Ransomware detections in EMEA, 2023 and 2022

■ 2022 ■ 2023

Americas

Ransomware detections in Americas, 2023 and 2022

■ 2022 ■ 2023

The daily number of ransomware detections 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 multi-layered 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.
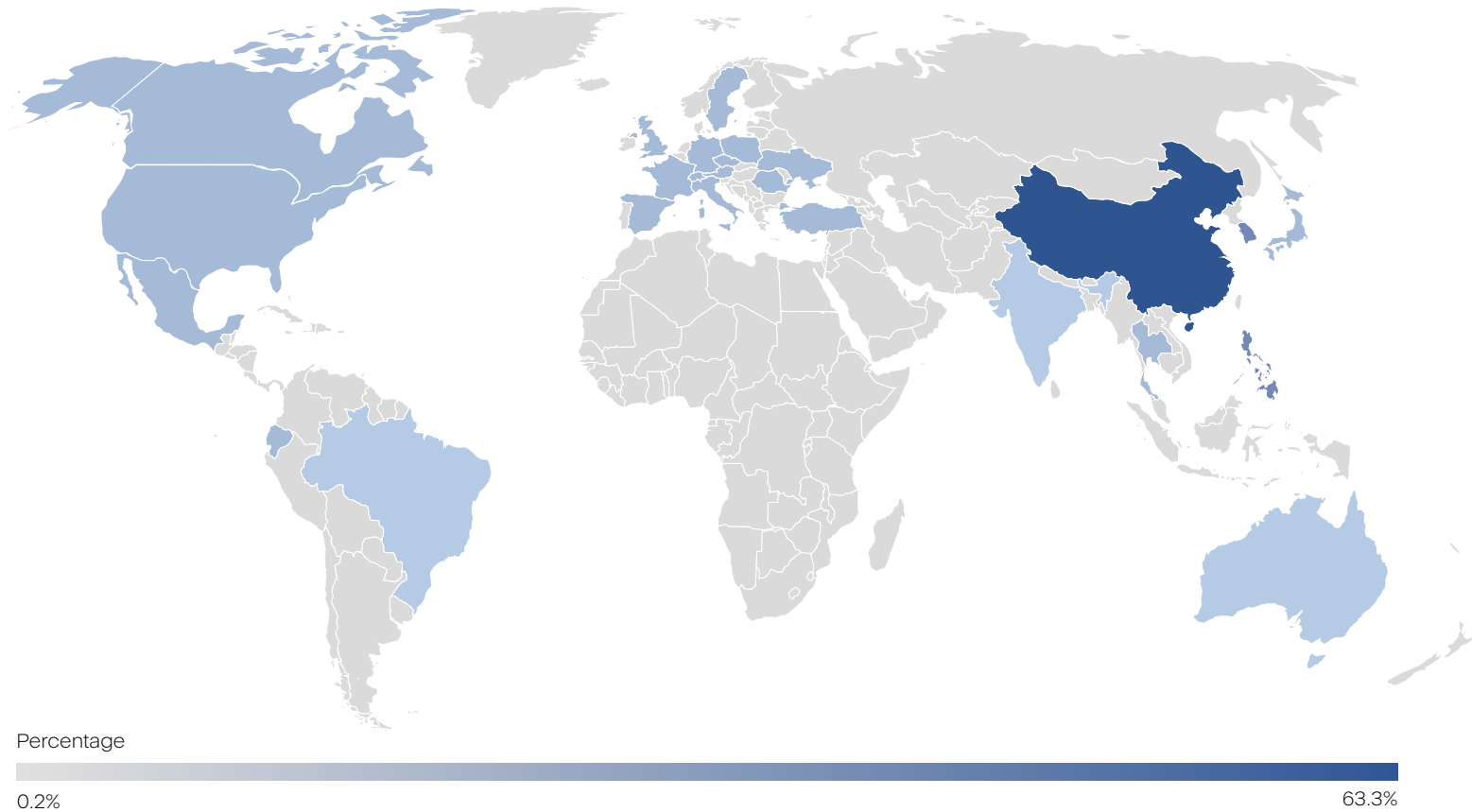
Daily ransomware detections globally

Daily ransomware detections
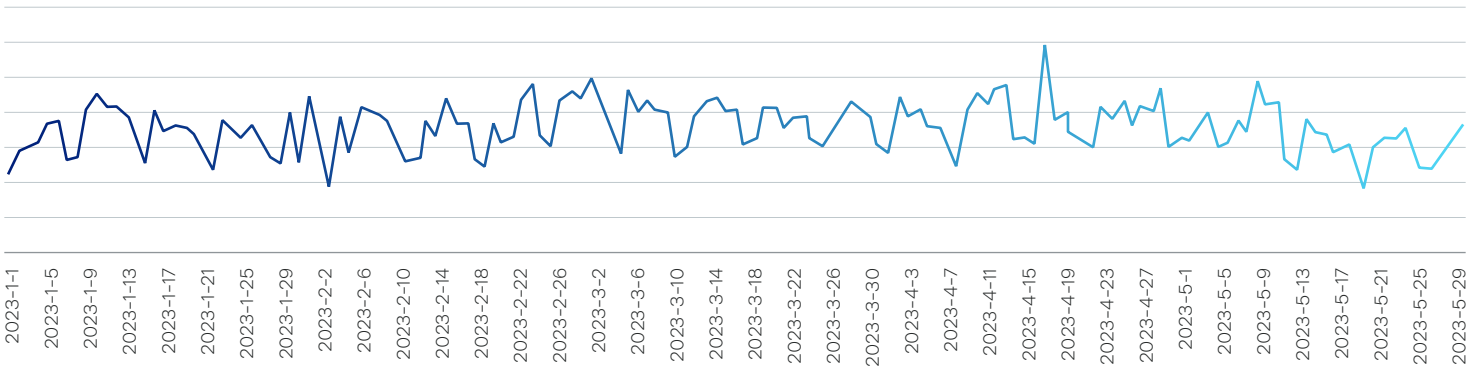
The peak day of ransomware detections in this period was April 18, and the lowest day of ransomware detections was May 21.

Ransomware detections, April 2023

Percentage

0.2%   63.3%

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 20 countries: Global ransomware detections by quarter normalized

Rank	Country	Global ransomware detection percentage in Q1 2023	Global ransomware detection percentage in Q4 2022
1	China	37.85	39.10
2	South Korea	34.07	34.41
3	Philippines	20.80	19.81
4	Vietnam	14.22	12.19
5	Egypt	12.70	10.13
6	Japan	12.64	11.45
7	Taiwan	11.17	13.19
8	Germany	8.60	9.10
9	Hungary	7.72	5.72
10	Thailand	7.65	5.90
11	Slovakia	7.28	8.23
12	Turkey	6.96	6.84
13	Peru	6.82	8.36
14	Hong Kong	6.20	7.67
15	Spain	5.80	5.26
16	Poland	5.65	6.31
17	Czechia	5.58	5.95
18	Ukraine	5.42	5.26
19	United States	5.26	4.82
20	Norway	5.12	3.72

Top five countries: Ransomware detections by quarter normalized

The leading top three countries in APAC were China (37.85%), South Korea (34.07%) and the Philippines (20.80%).

APAC

Country	Regional ransomware detection percentage in Q1 2023	Regional ransomware detection percentage in Q4 2022
China	37.85	39.10
South Korea	34.07	34.41
Philippines	20.80	19.81
Vietnam	14.22	12.19
Japan	12.64	11.45

The leading top three countries in EMEA were Egypt (12.7%), Germany (8.6%) and Hungary (7.72%).

EMEA

Country	Regional ransomware detection percentage in Q1 2023	Regional ransomware detection percentage in Q4 2022
Egypt	12.70	10.13
Germany	8.60	9.10
Hungary	7.72	5.72
Slovakia	7.28	8.23
Turkey	6.96	6.84

The leading top three countries in the Americas were Peru (6.82%), the United States (5.26%) and Argentina (4.92%).

Americas

Country	Regional ransomware detection percentage in Q1 2023	Regional ransomware detection percentage in Q4 2022
Peru	6.82	8.36
United States	5.26	4.82
Argentina	4.92	5.96
Mexico	3.75	3.27
Canada	3.05	2.96

# Ransomware activity in top countries

You've probably heard over and over that cybercriminals don't discriminate — that they'll target businesses of any size and any vertical. This remains true. Their interest is simply sensitive data, which they can sell to earn money and keep the cycle going.

Still, some groups have their preferred targets. In the first half of 2023, there were several cyberattack patterns that merit special attention in this report:

USA

The trend of ransomware detections in 2023 compared to 2022 was growing in the first four months of the year. The detection growth of attacks in March is likely associated with the highly publicized GoAnywhere MFT vulnerability being exploited across the world, which was notably used by March's most active threat actor: Clop. This managed file transfer (MFT) software is utilized by more than 3,000 organizations, and the resulting cybercrime campaign resulted in significant disruption.

We can see below that ransomware attacks increased significantly in March. The U.S. was the target of almost half of March's 459 successful reported attacks, with 221 victims (48%).

USA ransomware detection ■ 2022 ■ 2023
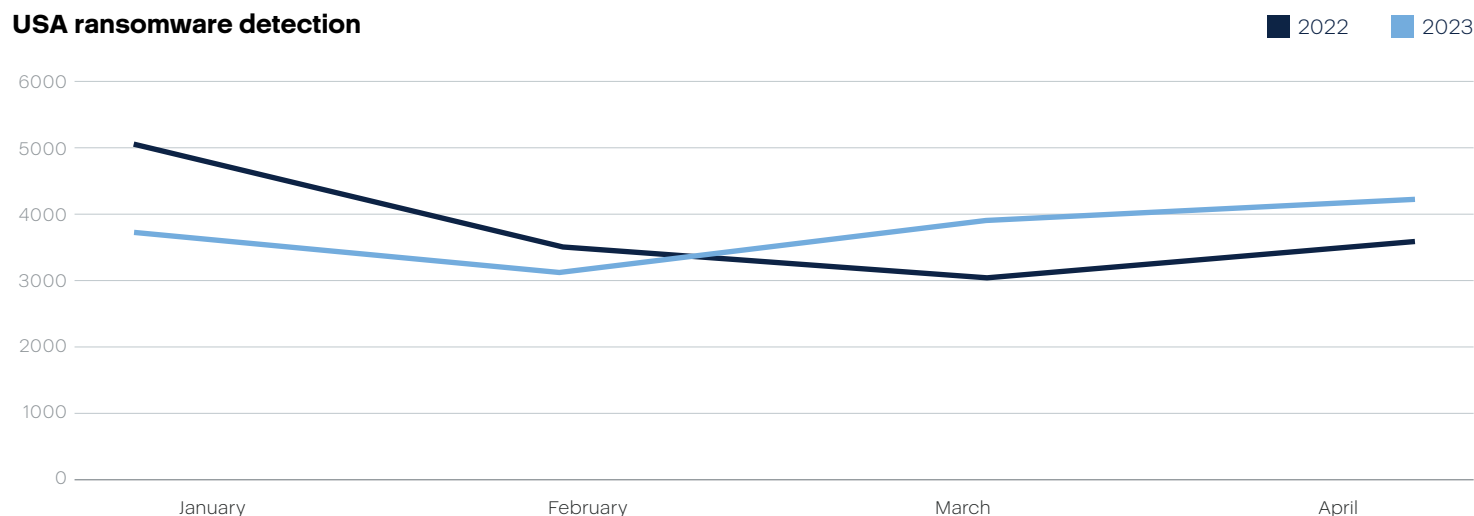
From healthcare to finance, there are many industries that attract attackers, but among the most attacked sectors in the U.S. are government and public administration institutions — accounting for nearly 20% of all incidents, as revealed in the U.S. Cyber Attacks 2023 report. These attacks often target organizations holding valuable and confidential data with potential national security implications. To counter these threats, the U.S. government has mandated the implementation of multi-factor authentication (MFA) for all government agencies and contractors accessing national security systems.

The healthcare industry ranks second, facing 13% of all attacks. Cyberthreats in healthcare pose risks like service disruptions and the theft of sensitive patient data. This sector was also frequently targeted in 2022; as a result, 2023 is seeing government and industry sanctions as a consequence for victims. CommonSpirit Health, one of the largest nonprofit hospitals in the U.S., is facing class action lawsuits over a 2022 cyberattack that disrupted operations at some of its facilities. According to reports, that incident exposed the confidential and potentially sensitive information of more than 623,700 people.

This example shows how a single attack can escalate quickly into multi-million-dollar settlements, in addition to significant regulatory fines and costs incurred restoring systems and data.

The information sector, encompassing telecommunications, computing, publishing, broadcasting and media outlets, ranks third, representing approximately 11% of all attacks. Attackers increasingly target national infrastructure, seeking opportunities for supply chain disruption and potential financial gains.

Even the education sector is not exempt from cyberattacks, as schools, universities and other educational institutions faced 10% of all attacks. Cybercriminals may be seeking institutions' valuable information, intellectual property and personal data, taking advantage of relatively weaker cybersecurity measures in this sector.

Germany

Another country with a high rate of reported ransomware attacks is Germany. The detection trendline decreased in April, and is lower than it was in 2022. Still, all the major sectors have been targeted, including education and healthcare.

Germany ransomware detection　　　　　　　　　　　　　■ 2022　　■ 2023
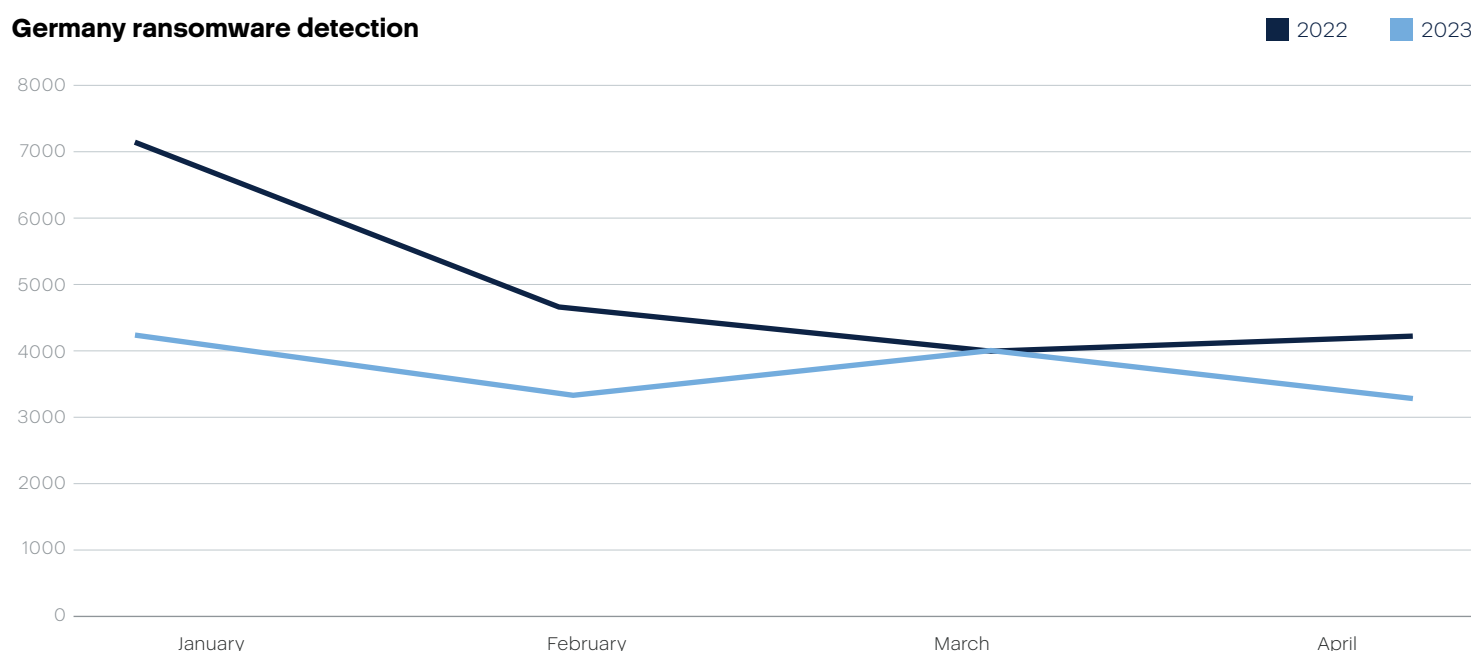
The University of Duisburg-Essen (UDE) was hit by Vice Society. UDE has 43,000 students, 4,000 academic staff and 1,500 administrative staff. The attack compromised the central authorization system and affected 1,200 servers, leading the university to undergo a complete reconstruction of its IT infrastructure. This case serves as a valuable lesson, highlighting the fact that relying solely on backups does not provide immunity from such threats. It underscores the importance of implementing robust security measures, proactive defense strategies and continuous monitoring to mitigate the risk of cyberattacks and their potentially devastating consequences.

A recent cyberattack hit Bitmarck Technik, a German

IT services provider for the healthcare industry with an annual revenue of $357 million. Bitmarck was forced to shut down its customer service and internal systems, as well as some of its data centers, to contain the attack. No customer or personal data was compromised, according to the company.

Bitmarck serves more than 80 statutory health insurers in Germany and offers services such as electronic health cards, digital communications and data processing. Some of its customers, such as health insurance provider SBK, experienced disruptions to their phone, email and app services. Bitmarck is working to restore these systems, but warned that there would be significant

limitations to its daily operations for the foreseeable future. They've informed the responsible authorities about the incident and called in external security experts for the investigation. Bitmarck also is exploring the possibility of setting up a temporary IT environment to enable essential processes for health insurers.

Another victim, Adesso — an IT solutions company with over 8,500 employees and an annual turnover in 2022 of over $900 million — disclosed a cyber attack on its IT infrastructure in February 2023, more than three weeks after detecting the incident in January. The company launched forensic analyses with internal and external experts to investigate the incident. These revealed that the attacker/s had breached the Adesso network in late May 2022, exploiting a zero-day vulnerability (CVE-2022-26134) in the Confluence system. The attacker/s installed malicious plug-ins in Adesso's Atlassian systems and gained privileged access to other systems within the network. Adesso stated that it communicated reliable information based on provable forensic evidence, which took time to emerge. The company has been in close contact with its customers and partners since February.

These incidents demonstrate the alarming growth in supply chain attacks, emphasizing the necessity for enhanced attention to supply chain security. What's more concerning is the possibility that managed service providers (MSPs) could remain unaware of breaches, and thus fail to swiftly notify their clients. This underlines the significance of proactive monitoring and communication throughout the supply chain ecosystem. According to Statista, during Q1 2023, more than 60,000 customers disclosed that they had been affected by supply chain attacks, which encompassed a range of customer-targeted cyberattacks such as counterfeiting, drive-by compromise and malware infections.

Japan

One country with a particularly high ransomware detection rate is Japan.

Japan ransomware detection ■ 2022 ■ 2023
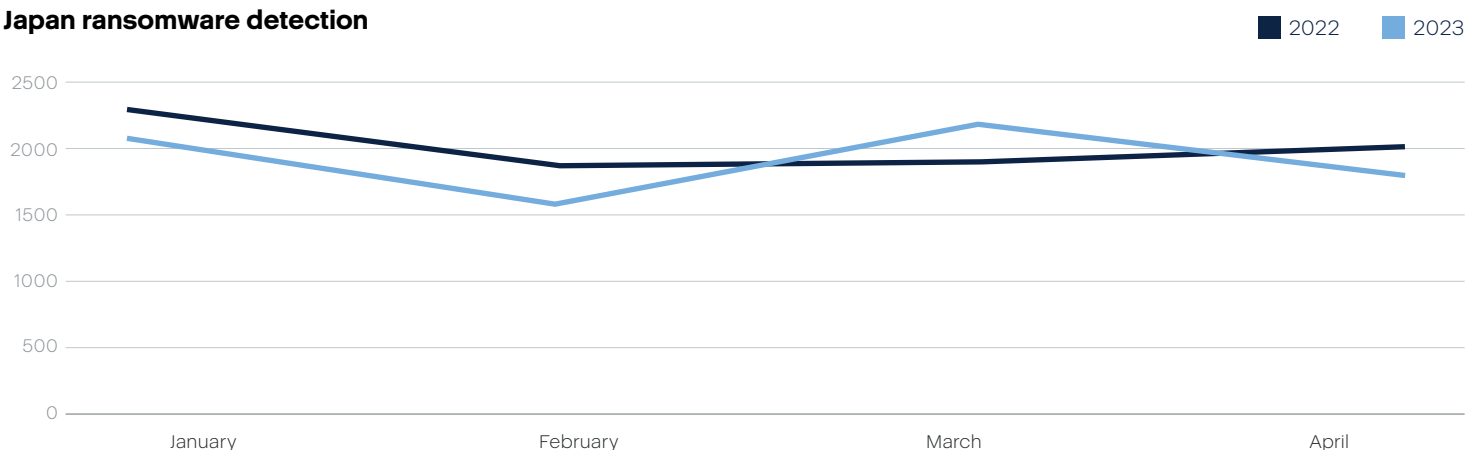
The increasing complexity of IT infrastructure in Japan presents a significant challenge for organizations, as it raises the risk of human error by administrators, such as misconfigurations or accidental deletion of backups. It is crucial to consolidate and simplify IT solutions to enhance efficiency and automate various processes. This allows businesses and MSPs to focus on their core functions and expand their offerings with fewer resources.

Additionally, there is a need for improved integration to enhance visibility and enable companies to monitor their data in the cloud and home office workloads. This integration is vital to counter the growing number of attacks targeting MSPs' infrastructure.

Furthermore, it is essential for MSPs to protect their automation and deployment tools and consoles to prevent cybercriminals from exploiting them for ransomware attacks or disabling antivirus solutions.

A notable example is the LockBit 3.0 attack on Fujikura Global, a Japanese electronic product manufacturer, where 718 GB of confidential and critical data —

including financial records, internal reports, certificates and employee personal information — was stolen. Similarly, Hitachi Energy, a subsidiary of a Japanese tech giant, confirmed that the Clop ransomware group exploited a vulnerability in Fortra's GoAnywhere file transfer software, potentially leading to unauthorized access to employee data in certain countries.

The West Japan Railway experienced an attack on April 20–21, while the Tokyo Electric Power Company Holdings faced a similar disruption on April 22, causing temporary website inaccessibility. Local governments, including Osaka, Aichi and Kumamoto prefectures, also fell victim to attacks. Even central government offices, such as the Cabinet Office's public relations website, were affected.

Given these circumstances, organizations in Japan must prioritize cybersecurity measures, including consolidation and simplification of IT infrastructure, enhanced integration for improved visibility and robust

protection of automation tools and consoles.

The ongoing attacks emphasize the urgent need to strengthen cybersecurity defenses to safeguard sensitive data and critical infrastructure. During the G7 summit in Hiroshima from May 19–21, where leaders from various countries and the European Union were gathered, there was an increased level of apprehension regarding the possibility of cyberattacks directed at the event and its related infrastructure.

Italy

Another country that has shown up in the news on many occasions is Italy. In February Italy's National Cybersecurity Agency (ACN) issued a warning, revealing that a global ransomware hacking attack had specifically targeted VMware (VMW.N) ESXi servers, affecting thousands of computer servers. ACN's then-director general, Roberto Baldoni, emphasized the urgency for organizations to take immediate measures to safeguard their systems. He further disclosed that the attack was executed on an extensive level, with the intention of exploiting a known software vulnerability. Patches for this vulnerability became available in 2021.

In March, Italy's data protection authority (also known as Garante) temporarily banned ChatGPT and launched a probe over the artificial intelligence application's suspected breach of privacy rules. Access to the chatbot was re-enabled in April.

Italy ransomware detection

■ 2022　■ 2023
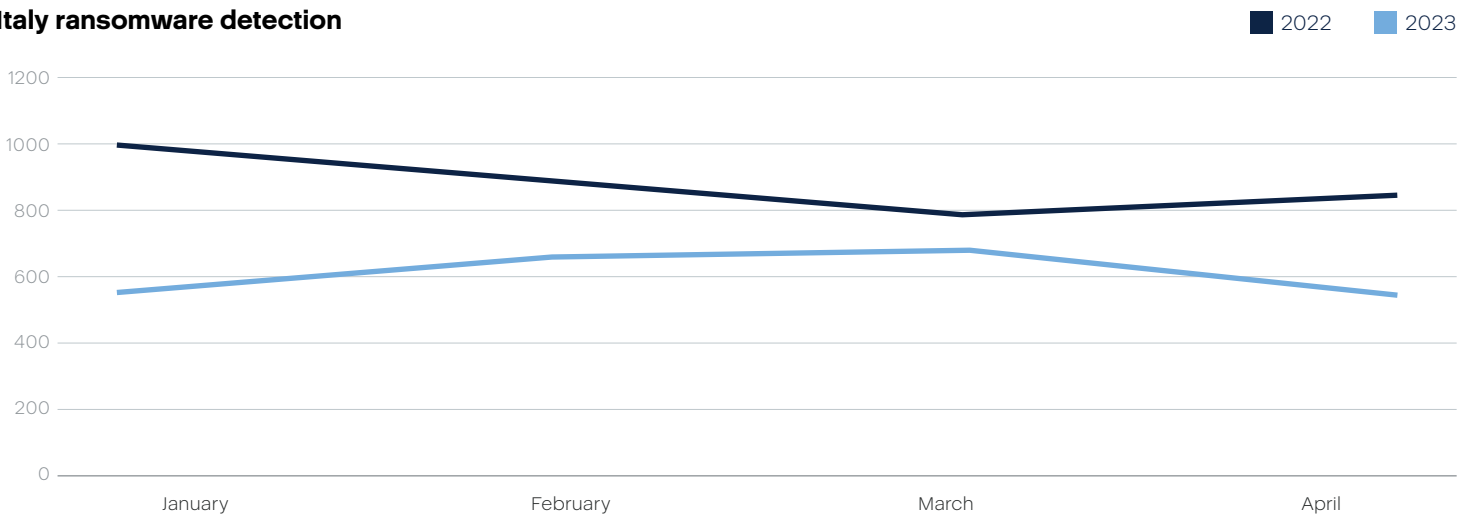
The ransomware detection trend has also been declining in Italy this year.

Italy's healthcare industry was targeted significantly during the early months of 2023, with attacks on healthcare provider ASL 5 in La Spezia, the University Hospital of Parma, and Niguarda Hospital in Milan. LockBit 3.0 claimed to have attacked MultiMedica, the company that owns the San Giuseppe Hospital in Milan, and threatened to leak the stolen data if the ransom wouldn't be paid. The ASL 1 of Avezzano Sulmona was hit by a ransomware attack by the Monti cybergang, who claimed to have stolen 522 GB of health data from its IT systems. Among the data leaked was sensitive information about HIV statuses, genetic tests, psychological evaluations and gynecological diagnoses. The attack was considered one of the most serious cyber incidents in Italy, as it violated the privacy of thousands of patients and disrupted healthcare services.

After Abruzzo, attackers have targeted Basilicata's health data. It is unclear if the Monti group was responsible here as well. The Gesan company, which handles IT management of medical records in several regions, alerted authorities about the breach. The cybercriminals used phishing emails to trick the victims into giving them access to the network.

The National Cybersecurity Agency has declared an emergency in response to an unprecedented and highly destructive attack. The magnitude of this assault has compelled the agency to take immediate action, underlining that the compromised documents from L'Aquila included not only medical records but also letterheads, pre-filled letters, machinery orders, medication details and various access passwords for different services.

The Bianlian gang claimed to have stolen 1.5 TB of data from Lifenet Healthcare. This data allegedly included personal and medical information of patients and employees, as well as business and financial data. The attackers demanded a ransom to decrypt the files

and prevent their leak. However, the data they posted on their data leak site was old and did not contain any health data, suggesting that it was a bluff to extort money from Lifenet.
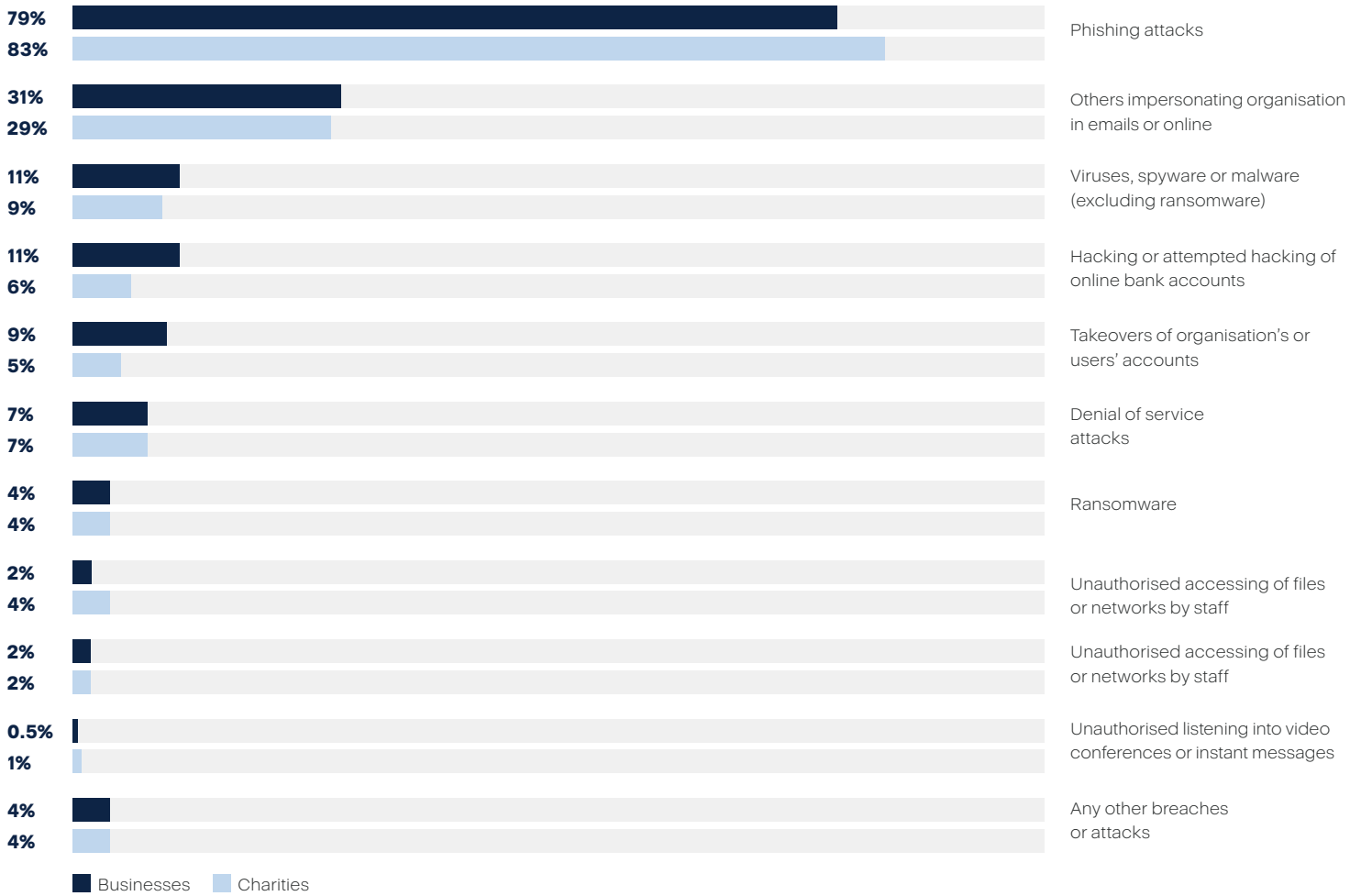
According to Muttii telemetry, one out of every 100 computers in Italy was attacked with ransomware in April 2023, putting the country in 29th place globally. If we count not just ransomware but all types of malware, Muttii telemetry shows that 7.5% of all computers in Italy were hit. This is a decline compared to the March 2023 figure of 10.4%.

Medical institutions must have a business continuity plan that can maintain their core services during an incident. Advanced cyber protection that uses AI/ML and behavior analysis can help detect and stop anomalies. Moreover, visibility, zero-trust and data loss prevention systems can reduce the risk of data theft.

U.K.

The Cyber Security Breaches Survey, conducted in alignment with the U.K.'s National Cyber Strategy, consistently highlights the significance of prioritizing staff awareness through training and awareness-raising initiatives. This is in acknowledgment of the fact that social engineering techniques, especially phishing attacks, are commonly employed by threat actors to breach organizations' networks.

79%	Phishing attacks
83%	
31%	Others impersonating organisation
29%	in emails or online
11%	Viruses, spyware or malware
9%	(excluding ransomware)
11%	Hacking or attempted hacking of
6%	online bank accounts
9%	Takeovers of organisation's or
5%	users' accounts
7%	Denial of service
7%	attacks
4%	Ransomware
4%	
2%	Unauthorised accessing of files
4%	or networks by staff
2%	Unauthorised accessing of files
2%	or networks by staff
0.5%	Unauthorised listening into video
1%	conferences or instant messages
4%	Any other breaches
4%	or attacks

■ Businesses   ■ Charities

Source: Cyber security breaches survey 2023 - GOV.UK (www.gov.uk)

In January 2023, Royal Mail — the multinational postal service of Britain — fell victim to LockBit. The group demanded an unprecedented ransom of $80 million, claiming the title of largest ransom to date. Royal Mail swiftly dismissed the demand as 'absurd.' In response, LockBit publicly released stolen files from the company and provided an illuminating transcript documenting the negotiation process between the two entities.

UK ransomware detection   ■ 2022   ■ 2023
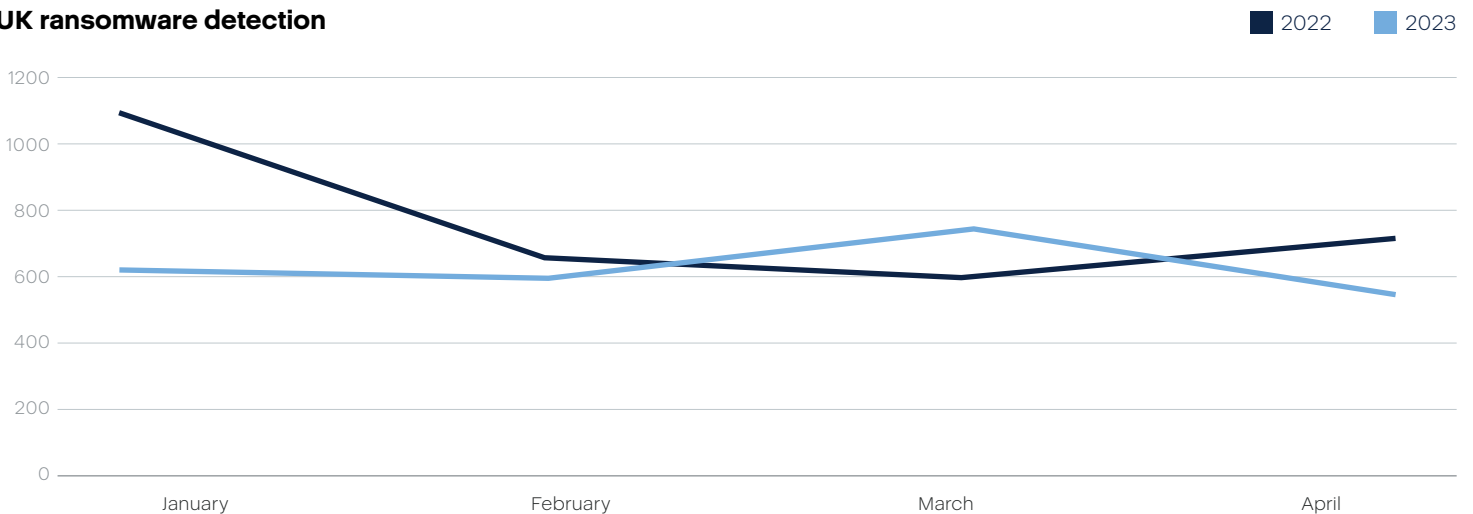
Similar to the U.S. education sector's situation in the early months of 2023, the BBC covered a series of attacks on 14 U.K. schools carried out by Vice Society in the previous year.

The Clop ransomware victims list was updated with entities including British multinational conglomerate Virgin's rewards club, Virgin Red; Procter & Gamble; and the U.K.'s Pension Protection Fund. Some retail businesses, like Yum! Brands and car dealer Arnold Clarke, also fell victim.

The U.K. Criminal Records Office (ACRO) encountered a cyber incident that led to the temporary closure of its customer portal, causing significant disruptions to various operations over an extended duration. ACRO informed users via email about the situation, acknowledging that they were informed of a cybersecurity incident that occurred on their website from January 17 to March 21. However, they stated that there was no definitive evidence to suggest that personal data had been compromised.

Another example from Q1 2023 is Vesuvius, a U.K.–based molten metal flow engineering company with an annual revenue of $2.2 billion and more than 10,000 employees. The company was hit by a cyberattack, which they estimate will cost £3.5 million (approximately $4.6 million at the current exchange rate) in damages.

Earlier, ION Group, another U.K.–based company with a revenue of $273 million and over 1300 employees, suffered a cyber incident. The financial trading services firm was hit by the ransomware group LockBit. ION initiated an investigation of the attack, which affected 42 of their clients and forced a number of European and U.S. banks and brokers to process certain trades manually.

For companies, the most frequently reported outcomes of data breaches and attacks involve website disruptions and temporary loss of access to files or networks. These consequences have a direct impact on productivity and result in financial implications for the affected organizations.

Cyber security breaches survey percentage in 2023

Legend: ■ Businesses ■ Charities
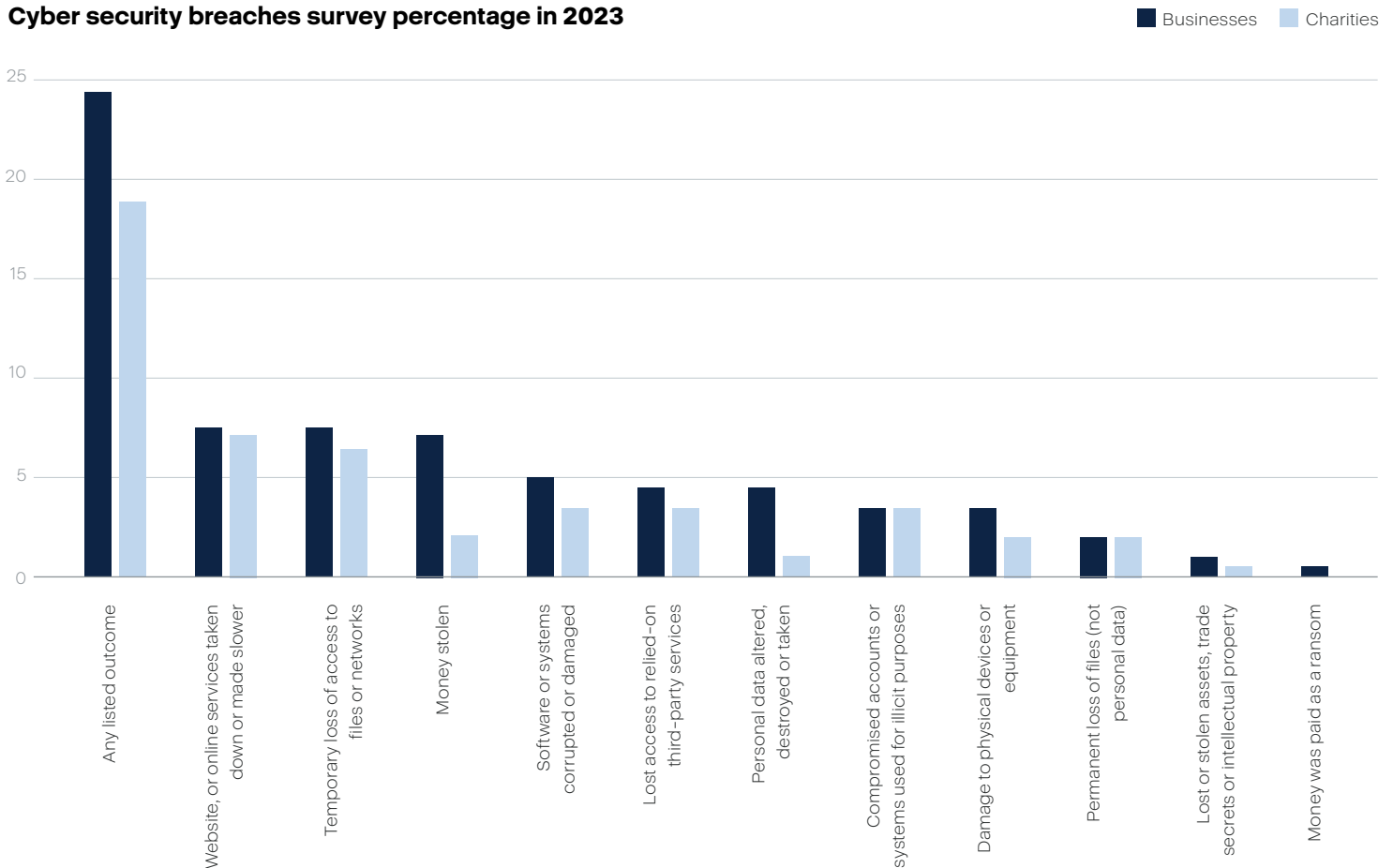
Source: Cyber security breaches survey 2023 - GOV.UK (www.gov.uk)

Whether data is breached or not, cyberattacks typically require firms to reallocate staff resources to resolve the incident or build new procedures to prevent and protect against future events.

France

According to researchers, France was a globally significant target for ransomware from April 2022 to March 2023, and the fifth most-attacked country by known/reported attacks.

Unusually, government targets accounted for a significant proportion of those organizations in the last twelve months. This was the country's third most attacked sector by numbers, accounting for 9% of known attacks. By comparison, over the same twelve-month period, 4% of known attacks in the U.S. and 3% of known attacks in Germany affected their government sectors, while just 20 miles across the English Channel, the U.K. experienced none at all.

Ransomware detections in France in 2022
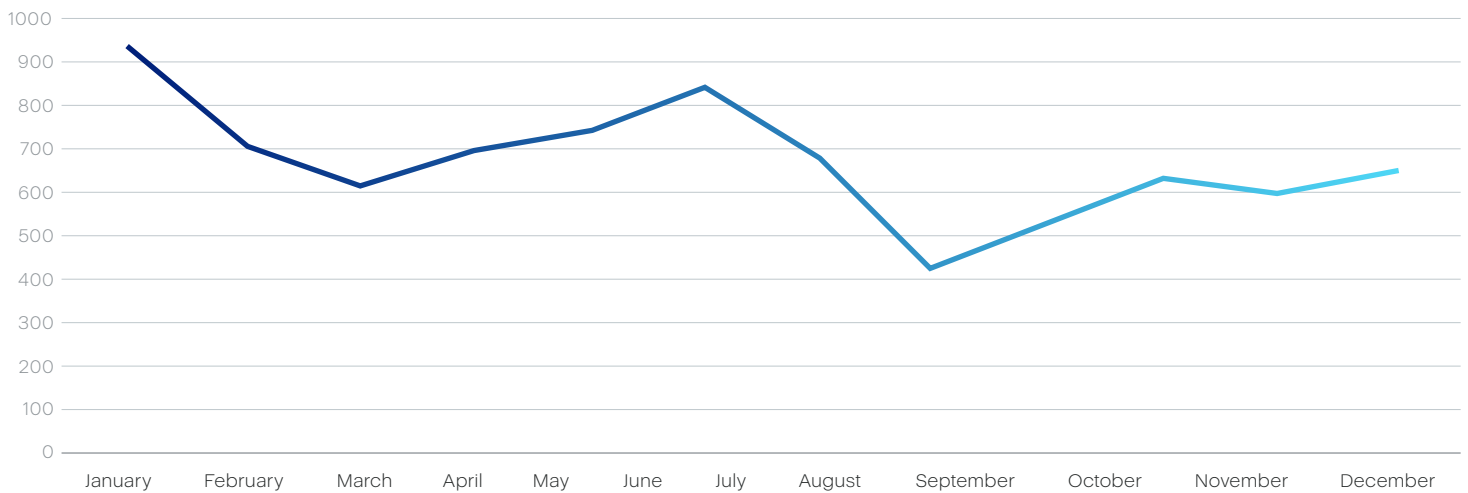
If we compare the trends of early 2023 to those of early 2022, we can see that the detection rate increased from February to April.

France ransomware detections   ■ 2022   ■ 2023
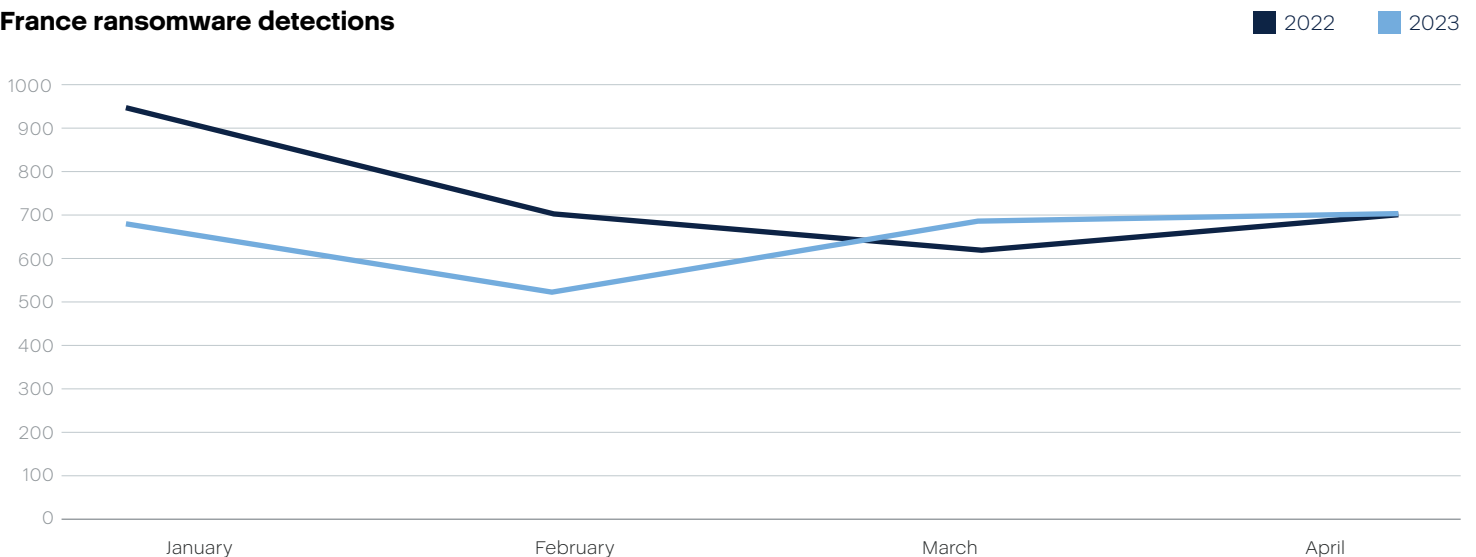
The increase in detections might be connected with a Clop ransomware campaign that used a zero-day vulnerability in Fortra's managed file transfer software (GoAnywhere MFT), which has compromised networks used by 130 different organizations. The gang has taken responsibility for over 50 attacks, including the attack on French digital transformation company Atos.

This campaign followed the Clop gang's campaign against PaperCut, makers of a popular print management software, which exploited a server vulnerability to steal corporate data.

The group behind Play ransomware, meanwhile, claimed to have breached BMW France. Stolen in this attack were private and personal confidential data, contracts, financial information and client documents.

Another cyberattack hit LACROIX Group, a France-based major technology equipment company with over €700 million in revenue last year. The company has temporarily closed three of its production sites due to the impacts of ransomware. This targeted cyberattack affected electronics manufacturing facilities in France, Germany, and Tunisia. LACROIX Group believes that the impact on their overall performance for the year will be limited, since these sites accounted for only 19% of sales last year and the attack coincided with scheduled holidays in France and Germany.

Malicious websites

The Muttii CPOCs blocked 49,244,158 phishing and malicious URLs in Q1 2023. This constitutes a 15% spike over the figures in Q4 2022 (42,844,493).

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 download a malware-laden file.

Malicious email attachments often feature multiple layers — such as using password-protected ZIP files that contain LNK files, which in turn download the final payload. They may also masquerade under fake buttons within a OneNote file attachment that arrives with the phishing email. This technique has been of particular focus ever since Microsoft restricted the use of macros in Microsoft Office. Such tactics are why having a multi-layered defense approach is crucial to protect against cyberattacks.

Month	Blocked URLs	Total for the quarter
October 2022	13,025,443	
November 2022	15,202,217	42,844,493
December 2022	14,616,833	
January 2023	17,160,862	
February 2023	14,898,883	49,244,158
March 2023	17,184,413	
April 2023	13,726,811	
May 2023	16,145,566	

An average of 9.0% of endpoints tried to access malicious URLs in Q1 2023, slightly up from 8.6 % in Q4 2022. In April, we observed this figure drop down to 6.9%, though it then increased to 8.1% in May.

Month	Percentage of users that clicked on malicious URLs
January	8.7
February	9.1
March	9.1
April	6.9
May	8.1

The country with the largest percentage of blocked malicious URLs at the endpoint in April 2023 was Germany with 20.9%, followed by Singapore with 13.9% and Italy with 11.7%.

Top 10 countries with the most blocked URLs in April 2023

Rank	Country	Percent of blocked URLs in April 2023
1	Germany	20.9
2	Singapore	13.9
3	Italy	11.7
4	United Kingdom	10.3
5	Switzerland	9.1
6	Japan	9
7	France	7.1
8	Spain	4.5
9	India	4.4
10	Netherlands	2.6

Similar to the malware detection statistics, we did normalize the numbers depending on the number of active machines in each country with at least 10 blocked URLs. These normalized breakdowns per region can be found below.
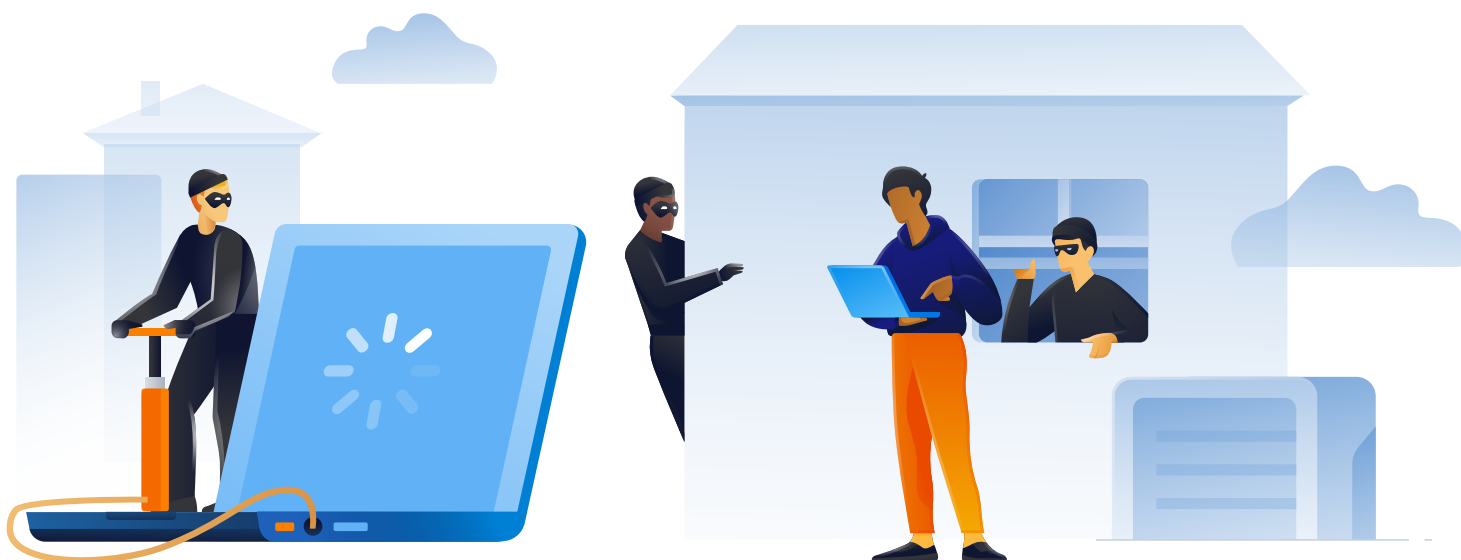
Top 10 countries: Normalized blocked URLs numbers by region

APAC

Rank	Country	Regional normalized percent of blocked URLs in April 2023
1	Philippines	14.6
2	Taiwan	13.4
3	South Korea	13.4
4	India	13.3
5	Japan	12.6
6	China	10
7	Singapore	9.8
8	Indonesia	9.5
9	Thailand	9.1
10	New Zealand	8.5

EMEA

Rank	Country	Regional normalized percent of blocked URLs in April 2023
1	Kuwait	39.9
2	Hungary	12.9
3	Saudi Arabia	12.3
4	Poland	9.7
5	Greece	7.8
6	Portugal	7.8
7	Spain	7.4
8	United Arab Emirates	7.3
9	Czechia	7
10	Turkey	6.7

Americas

Rank	Country	Regional normalized percent of blocked URLs in April 2023
1	Haiti	40.9
2	Panama	21.7
3	Colombia	17.4
4	Argentina	12.2
5	Costa Rica	11.7
6	Peru	11.4
7	Mexico	9.7
8	Brazil	7.9
9	United States	7.8
10	Dominican Republic	7.4

Vulnerabilities in Windows OS and software

In Q1 2023, we again observed the power of zero-day vulnerabilities, with GoAnywhere (CVE-2023-0669) being a perfect exemplar. While these are not always fixed quickly by the vendors, it is crucial to patch the machines as soon as security updates are released. Below, we review key vulnerabilities and the patch release activities of some major tech companies.

Microsoft Patch Tuesdays

Lets start from the beginning of the year. Microsoft's January 2023 Patch Tuesday fixed an actively exploited zero-day vulnerability and a total of 98 flaws. Eleven vulnerabilities were classified as 'critical.' Exploitation of those vulnerabilities allows remote code execution, the bypassing security features, or unauthorized privilege elevation. The vulnerability being actively exploited was CVE-2023-21674 — a Windows Advanced Local Procedure Call (ALPC) elevation of privilege vulnerability. Another publicly disclosed one was CVE-2023-21549, a Windows SMB Witness service elevation-of-privilege vulnerability.

In February, Microsoft fixed three actively exploited zero-day vulnerabilities and a total of 77 flaws. Among the three actively exploited zero-day vulnerabilities, two (CVE-2023-21823, CVE-2023-23376) allow criminals to gain system privileges, while the third (CVE-2023-21715) allows specially crafted documents to bypass Office macro policies that are used to block untrusted or malicious files in Microsoft Publisher. Nine vulnerabilities have been classified as 'critical,' as they allow remote code execution on vulnerable devices.

Microsoft's March 2023 Patch Tuesday fixed two actively exploited zero-day vulnerabilities and a total of 83 flaws. One of the two zero-days was CVE-2023-23397 — a Microsoft Outlook elevation-of-privilege vulnerability that allows specially crafted emails to force a target's device to connect to a remote URL and transmit the Windows account's Net-NTLMv2 hash. The other zero-day vulnerability was CVE-2023-24880, a Windows SmartScreen security feature bypass vulnerability that can be used to create executables that bypass the Windows Mark of the Web (MotW) security warning. Again, nine vulnerabilities were classified as 'critical' for enabling remote code execution, denial of service or elevation-of-privilege attacks.

Microsoft's April 2023 Patch Tuesday addressed 97 vulnerabilities, including one zero-day that is being actively exploited. A zero-day flaw in the Windows CLFS driver that allows attackers to gain system privileges was among the vulnerabilities patched by Microsoft. This flaw, identified as CVE-2023-28252, was reported by multiple researchers and was seen being exploited by Nokoyawa ransomware. Microsoft also fixed several remote code execution bugs in Office, Word and Publisher that could be triggered by opening malicious documents. The update includes fixes for seven 'critical' remote code execution flaws.

In May, we saw a significant decline in the number of fixed vulnerabilities — just 38, including three zero-days that were exploited or disclosed before a patch was available. One of those zero-days, CVE-2023-24932, is a Secure Boot bypass that allows attackers to install a UEFI bootkit on Windows devices. The other two zero-days are an elevation-of-privilege flaw in the Win32k kernel driver (CVE-2023-29336) and a Windows OLE remote code execution vulnerability (CVE-2023-29325). Six of the patched vulnerabilities are rated as 'critical,' as they could lead to remote code execution on affected systems.

To summarize: we see that Microsoft products continue to be the most exploited ones, due to their popularity and potential attack surface.

Google, Adobe and others' patching activities

As is always the case with Google products, Chrome was of significant interest to security researchers and cybercriminals, and we saw numerous patches issued for the popular browser. In the January Chrome update, Google addressed six security vulnerabilities, none of which appears to have been exploited in the wild. Four of the vulnerabilities were reported by external researchers. Two of them are 'high'-severity and researchers earned a total of $19,000 for their findings. These vulnerabilities are tracked as CVE-2023-0471 and CVE-2023-0472.

Additionally, Google has issued a Chrome security patch to fix the first zero-day flaw exploited this year. Attackers are actively exploiting the CVE-2023-2033 vulnerability, which affects the Chrome V8 JavaScript engine on Windows, Mac and Linux systems.

At the end of April, Google announced a patch for another zero-day vulnerability in Chrome. Tracked as CVE-2023-2136, the security defect is described as a 'high'-severity integer overflow issue in Skia. The latest Chrome 112 update includes eight security fixes, five of which address vulnerabilities reported by external researchers, including four bugs rated 'high' in severity. Based on the paid reward, the most severe of the externally reported security defects are CVE-2023-2133 and CVE-2023-2134, two out-of-bounds memory access issues in the Service Worker API.

Adobe has been busy as usual with patching since January, when it released four patches addressing 29 CVEs in Adobe Acrobat and Reader, InDesign, InCopy and Adobe Dimension. A total of 22 of these bugs were submitted through the ZDI program. The update for Reader fixed 15 bugs, with eight of these being ranked 'critical' in severity for reasons like allowing arbitrary code execution on the affected system after a specially crafted file is opened. The patch for InDesign fixes six bugs, four of which are rated 'critical.' Similar to the Reader patch, opening a malicious file could result in code execution.

For February, Adobe released nine patches addressing 28 CVEs in Adobe Photoshop, Substance 3D Stager, Animate, InDesign, Bridge, FrameMaker, Connect and After Effects. Probably the most interesting fix is for PhotoShop. This patch fixes five bugs, three of which are rated 'critical.' An attacker could facilitate arbitrary code execution if they can convince users on an affected system to open a malicious file. This is the same scenario for Premier Rush, which corrected two 'critical'-rated code execution bugs. The fix for Adobe Bridge fixes five 'critical'-rated code execution bugs, plus two memory leaks. After Effects also has a memory leak to go along with three code execution bugs. None of the bugs fixed by Adobe in February were listed as publicly known or under active attack at the time of release. Adobe categorizes these updates as a deployment priority rating of '3.'

March was much more productive, with eight patches addressing 105 CVEs in ColdFusion, Photoshop, Experience Manager, Dimension, Commerce, Substance 3D Stager, Cloud Desktop Illustrator, and ColdFusion. The patch for ColdFusion was listed as under active exploit. It fixes three bugs, including a 'critical'-rated code execution bug with a CVSS score of 9.8. The patch for Dimension was the largest of the bunch, with nearly 60 CVEs addressed by that patch alone.

In April, Adobe fixed 56 CVEs in Acrobat and Reader, Adobe Digital Editions, InCopy, Substance 3D Designer, Substance 3D Stager and Adobe Dimension. The update for Reader corrects 16 different CVEs, 14 of which could lead to arbitrary code execution if a threat actor can get users to open a specially crafted PDF with an affected version of Reader.

In May, Adobe released the only patch for Substance 3D Painter, addressing 11 'critical'-rated and three 'important'-rated vulnerabilities. The most severe of these issues would allow an attacker to execute arbitrary code on an affected system if they can convince the user to open a specially crafted file.

These examples show the constant flow of found and reported vulnerabilities in popular software, which makes automated patch management such a critical part of staying safe in today's threat landscape.

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

Modern cyberattacks, data leaks and ransomware outbreaks all show the same thing: 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 at the same time 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.

To solve these problems, we recommend an integrated cyber protection solution (like Muttii Cyber Protect) that combines anti-malware, EDR, DLP, email security, vulnerability assessments, patch management, RMM and backup capabilities into a single agent. This integration lets you 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.

Of course, Muttii Cyber Protect Cloud strives to make data recovery unnecessary by detecting and eliminating threats before they can damage your environment. This is achieved with our enhanced, multi-layered cybersecurity functionality.

The newly released Endpoint Detection and Response (EDR) pack for Muttii Cyber Protect Cloud brings the visibility needed to understand attacks, while simplifying the context for administrators and enabling efficient remediation of any threats.
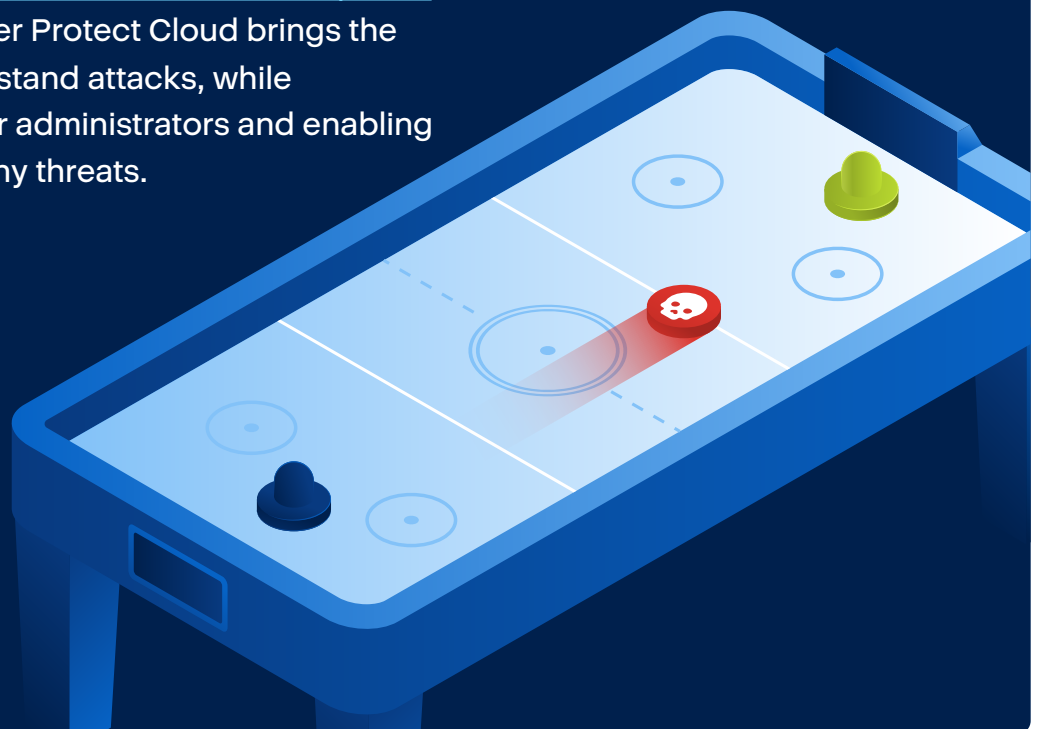
That said, companies and home users shouldn't forget about basic security rules, even if they use modern solutions like Muttii Cyber Protect. As always, be sure to:

Patch your OS and apps

This is crucial, as many attacks succeed due to unpatched vulnerabilities. With a solution like Muttii 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. Muttii 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 Muttii 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 apps like PDF Reader are also updated promptly.

Prepare for phishing attempts, and don't click on 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 Muttii Cyber Protect offer additional dedicated URL filtering functionality. Remember that malicious links can come from anywhere: instant messenger apps, email, forum posts, etc. Don't click links you don't need to click, or that you didn't expect to receive.

Emails can easily contain malicious attachments as well. Always double-check where these really originated, and ask yourself whether you're expecting them or not. Before you open any attachment, it should be scanned by your anti-malware solution.

### Ensure your cybersecurity solution is properly configured

Muttii 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 just having anti-malware defenses in place is not enough; they must be configured properly. This means that:

- A full scan should be performed at least once per day.
- Solutions must get updates daily or hourly, depends how often they are available.
- Solutions should be connected to their cloud detection mechanisms. With Muttii 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.
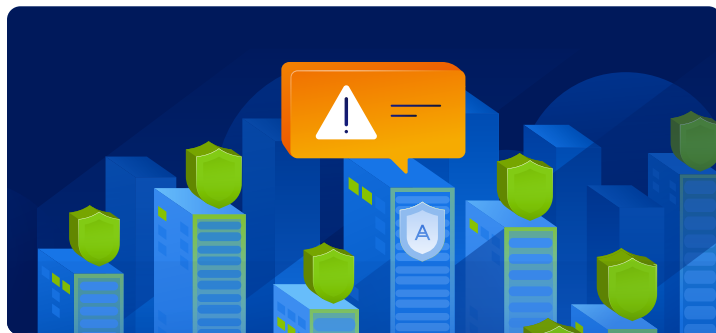
Keep passwords and working spaces private

Security tip number one: make 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 nowadays. Where possible, use multi-factor authentication.

Even 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 off a non-locked PC.

About Muttii

Muttii 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, Muttii 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, Muttii 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, Muttii 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. Muttii products are available through over 50,000 partners and service providers in over 150 countries and 26 languages.

MUTTII