LOGPOINT

END OF THE YEAR REPORT:

THE CYBERSECURITY ROLLERCOASTER OF 2023

Written by:

Bibek Thapa Magar
Anish Bogati
Swachchhanda Shrawan Poudel

www.logpoint.com

TABLE OF CONTENTS

ABOUT THE REPORT

This report offers an in-depth retrospective of cybersecurity in 2023, a year marked by unyielding cyberattacks. It delves into the pervasive presence of ransomware, data breaches, and vulnerabilities that besieged the digital landscape. Providing a comprehensive foundation with facts, data, and insightful infographics, this report unveils a chilling timeline of major cyber-attacks that defined the year's security breaches.

Enter a landscape where cybercrime took on new forms. AI fueled an arms race between defenders and attackers, and the accessibility of "Cybercrime-as-a-service" and "Ransomware-as-a-service" democratized potent cyber weaponry. No sector was immune—healthcare and all critical infrastructure—all became battlegrounds in digital warfare.

The report meticulously dissects ransomware's relentless grip on crucial infrastructure, financial giants, and mobile platforms, demanding hefty ransoms. New attack vectors emerged, leveraging deepfakes, AI-powered bots, sophisticated malware, and overwhelming conventional detection methods—even nation-states engaged in cyber warfare, amplifying the shadowy landscape.

Yet, amidst this darkness, the report illuminates a path forward—a call for vigilance, preparedness, and robust defense strategies. Collaboration, innovation, and prioritization of cybersecurity can reclaim the digital realm, fostering a future where innovation reigns supreme over-exploitation.

EXECUTIVE SUMMARY

Cybercrime took a massive toll on the digital world in 2023, with persistent ransomware assaults and increased data breaches in industries including finance and healthcare. The distinction between attacks driven by AI and human intelligence is becoming more hazy as ransomware, which has increased by 42%, targets critical infrastructure and demands millions of dollars. Sensitive data and identity information were exposed in a surge of breaches, and a delayed containment and identification process increased the risks.

Vulnerabilities exceeded 29,000 by 2023, setting new benchmarks for vulnerability levels. Because of "Cybercrime-as-a-Service," technology enabled speedy exploitation and increased the power of even untrained threat actors. Current tactics that employ AI chatbots, deepfakes, and SEO poisoning are more complicated and challenge established security protocols.

Financial and critical infrastructure sectors were particularly affected, as destructive DDoS attacks and nation-state cyberwarfare targeted them. Therefore, for a robust digital future, it is essential that stakeholders work together, play proactive defense, and conduct ongoing monitoring.

Bibek Thapa Magar
Logpoint Security Research

Bibek Thapa Magar is a certified ethical hacker focusing on adversarial attack simulation, detection engineering, and threat hunting. He currently works as a Security Researcher with the Logpoint Security Research team.

Anish Bogati
Logpoint Security Research

Anish Bogati is a security researcher with a passion for understanding adversaries' tradecraft and malware. Staying current with the latest threats and understanding their targeting strategies, Anish specializes in crafting analytics for swift identification and counteraction of network threats.

Swachchhanda Shrawan Poudel
Logpoint Security Research

Swachchhanda Shrawan Poudel is a cybersecurity professional specializing in purple teaming, reverse engineering, and malware analysis. Currently a Security Researcher at Logpoint Security Research, he leads the Emerging Threat Protection initiative. His focus includes detection engineering, threat hunting, and remediation, with a special passion for crafting effective detection rules, threat reports and playbooks.

KEY FINDINGS

1. Many global operations were conducted by the Federal Organizations throughout the world. The result of which was the takedown of Notorious ransomware gangs like **Alphv** and **Hive**.
2. Phishing tactics transformed with deepfakes, Phishing-as-a-Service (PhaaS), and AI-driven chatbots, complicating detection methods.
3. The global average **cost of a data breach** was USD 4.45 million.
4. Initial Access Brokers (IABs) introduced a "cybercrime-as-a-service" model on the dark web which helped to lower the entry barriers for attackers.
5. A total of 147 new ransomware/malware were discovered this year. Four of which made it to the top ten ransomware of 2023 and 2 made it to the top six of the list.
6. 2023 saw 5,613 ransomware attacks, which was a 42% increase compared to 2022. In total 373 ransomware groups were active this year.
7. Lockbit3 was the most prevailing ransomware this year with a staggering 954 total victims throughout this year.
8. CVE count surged from 5,187 to 29,065 in a decade, with a 16% increase in 2023, mostly in high-risk CVSS scores. 5109 CVEs were in the critical risk zone (9+).
9. Over 84% of confirmed Known Exploited Vulnerabilities resided in the high-critical zone, demanding immediate mitigation.
10. Dominant ransomware groups like LockBit3, Clop, and AlphV persisted while emerging threats gained traction.
11. Hyper-volumetric DDoS attacks surged, targeting financial institutions, retailers, and critical infrastructure.
12. Unpatched vulnerabilities, especially zero-day exploits, posed significant risks due to rapid exploitation.

LETTER FROM CISO

In 2023, the cybersecurity landscape saw profound shifts. Threat actors continued to evolve, employing sophisticated attack techniques to launch targeted attacks. Ransomware evolved into a more targeted and damaging adversary. Artificial intelligence, both a tool for defense and a weapon for attackers, has become an integral part of cyber operations. Phishing attacks reached a new subtlety, thanks to AI. While the cloud security concerns intensified, the supply chain compromise and innovative malware strains continued to challenge conventional cybersecurity measures. Also, the emergence of quantum computing compelled a reevaluation of encryption strategies.

Further, geopolitical tensions intensified the cybersecurity landscape, particularly in the Russia-Ukraine and Israel-Hamas conflicts. The year also saw an ongoing challenge in data breaches, with a record-high **average cost of data breaches** reaching $4.45 million. Several factors contributed to that amount, including ransomware, phishing, malware, supply chain compromises, and zero-day exploits. Some of the noteworthy incidents, such as those involving DarkBeam (3.8 billion records), Okta (50 billion records impacting 100% of customers), T-Mobile (37 million records), 23andMe (6.9 million records), Duolingo (2.6 million records), and **Discord.io** (760,000 records), underscore the global cybersecurity challenges and highlight the importance of robust cybersecurity measures.

While cyber threats and breaches pose challenges, the key to adequate security is establishing a solid foundation through a comprehensive approach. Simply tossing point solutions here and there won't suffice; the true magic lies in consolidation. Logpoint Converged SIEM seamlessly integrates SIEM, SOAR, UEBA, and EDR capabilities into a unified platform, eliminating the need for multiple solutions and vendors. Logpoint leverages cutting-edge technologies for centralized monitoring, end-to-end security, alert prioritization, insider threat detection, comprehensive threat response, compliance checking, and more. This positions Logpoint as a versatile cybersecurity solution. Moreover, Logpoint Converged SIEM provides:

- Threat intelligence
- Pre-built use cases
- Correlation rules
- Alerts
- and, playbooks that can be easily customized to suit individual environments and business needs.

Also, our **emerging threat reports** and blog posts are very well received by the international security community. These resources cover the entire spectrum of threats, including Indicators of Compromise, TTPs, MITRE ATT&CK mapping, and detection rules, empowering organizations in their proactive threat-hunting activities.

As the threat landscape evolves, so must our defenses. Organizations can tackle many cyber challenges by keeping updated on emerging threats, leveraging advanced technologies, and taking security measures. Logpoint remains committed to helping businesses on this journey, providing the tools and expertise needed to prosper in ever-changing cyberspace.

Roshan Pokhrel
Logpoint, CISO

WORDS FROM OUR HOD

Cybersecurity in 2023 was indeed a rollercoaster ride, as the threat landscape continued to evolve and expand in terms of speed, sophistication, and impact and the GenerativeAI took the cyber world by storm and once again ignited the renewed call worldwide for responsible AI. The stretched Russia-Ukraine conflict, the Middle East situation, and the upcoming US elections at the doorstep paint the picture bleak. However, there are some silver linings in the **cloud**. The gradual adoption of zero trust, increasing cyber awareness, and unprecedented coordination between law enforcement agencies, authorities, and cyber communities across borders to bring down or significantly disrupt various bad actors and their infrastructures such as the Hive ransomware, Snake malware, Qbot infostealer and many other infamous actors provide some hope and new avenues for international collaboration.

I personally feel, that despite new and legacy challenges, defensive security will thrive in 2024. The need for cybersecurity will remain a top priority for organizations and individuals alike. Being at the top of the **hype cycle** and gathering so much attention throughout 2023, Generative AI is likely to capture heavy investments in research and development in cybersecurity solutions this year. In addition to that, some interesting push towards **crypto agility** with the expected release of more **PQC standards** is likely to drive some industry leaders towards post-quantum security plans. With NIS2 going full swing this year, the pursuit of protecting critical infrastructure will continue in a more focused and coordinated way paving way for the OT security to new heights.

As a part of our responsibilities, the Logpoint Security Research team will continue developing and evaluating new features and techniques for detecting, preventing, and responding to such cyber threats. Devising end-to-end solutions against emerging threats and their timely delivery to our customers will be our paramount focus. I am confident, that our multi-pronged approach to protect our customers through extended EDR capabilities and cloud-native offerings will gain momentum this year in addition to our ease-of-use and quality initiatives.

Basudev Raut
Logpoint, HoD, Security Research

A RECAP ON 2023

In 2023, the cybersecurity scene saw increased sophisticated cyberattacks and data breaches, similar to previous years. With the rise of AI, defenders were able to come up with new concepts and techniques to stay ahead in the game. But the adversaries had the same access. With which they were able to craft malicious and novel artifacts to bypass the defenses.

Data is the most valued asset these days. So attackers are lurking towards getting their hands on the data. Ransomware and data breaches were some of the top profitable cybercrimes for threat actors. September's **DarkBeam data breach** was one of the year's major stories. The most extensive data breach of the year involved a misconfigured Elasticsearch and Kibana interface that revealed an astounding 3.8 billion records. Forget about financial organizations getting hit by ransomware, we even saw a Swedish church **Svenska Kyrkan** getting hit by ransomware, postponing funerals. These kinds of incidents show the need for robust data security procedures for all types of organizations.

Throughout the year, the digital world saw numerous threats, including CVE exploits, zero-days, supply chain attacks, info-stealers, and rampant ransomware activities. Among the many highlights, **Cybercrime-as-a-Service** also gained popularity this year. It enabled the less technically proficient opponents to launch attacks with greater ease. Threat actors came up with sophisticated strategies, significantly affecting a large number of organizations. Notable trends included- the emergence of new threat actors, splintering from existing groups, and the evolution of malware families. Rebranding is one strategic response to global takedowns that certain threat actors have undertaken. We have covered them through our **blogs and reports** throughout the year and also offered means of addressing them with our consolidated security platform, **Logpoint Converged SIEM**.

Threat Actors Takedown

Amid the proliferation of various threat actors and malware families, notable successes have been in countering cyber threats in 2023. Through collaborative efforts involving multiple government entities, access to the servers of a significant threat actor was achieved, resulting in the removal of all victims' data and the shutdown of their servers.

Operating as a **Ransomware-as-a-Service** provider, Hive and its affiliates have been responsible for launching ransomware attacks on critical sectors such as healthcare and energy globally, accumulating a victim list exceeding 200 between 2022 and 2023.

Since late July 2022, **the FBI** has successfully penetrated Hive's computer networks, obtaining decryption keys and offering them to victims globally. This proactive approach prevented victims from succumbing to a ransom demand totaling **$130 million**. Since gaining access to Hive's network, the FBI has supplied over 300 decryption keys to thwart ongoing attacks against Hive victims. Moreover, more than 1,000 additional decryption keys were distributed to prior victims of Hive.

In a coordinated effort in January 2023 involving the FBI, German law enforcement, and the Netherlands National High Tech Crime Unit, control of the servers and websites utilized by Hive for communication was seized. This strategic move disrupted Hive's capacity to launch attacks and extort victims, marking a significant blow to their operations.

QBot, or Qakbot or Pinkslipbot, has been a modular information stealer since 2007. Initially recognized as a banking Trojan, it has also served as a loader malware. Notably, investigators have traced that the Qakbot team has received approximately $58 million in ransoms paid by victims from October 2021 to April 2023. Besides, it is also one of the top malware families observed in MalwareBazaar.

In a **collaborative effort** known as Operation '**Duck Hunt**', led by the Justice Department and the FBI with international cooperation, significant strides were made in dismantling QBot and its associated botnet infrastructures. This operation resulted in the seizure of more than **$8.6 million** in cryptocurrency representing illicit profits. Furthermore, as part of the operation, the Qakbot malicious code was eradicated from victim computers to prevent further harm to their systems and networks.

The Ragnar Locker Ransomware group faced a coordinated international takedown led by Europol and Eurojust. This **international effort** resulted from a comprehensive investigation conducted by the French National Gendarmerie in collaboration with law enforcement authorities from Czechia, Germany, Italy, Japan, Latvia, the Netherlands, Spain, Sweden, Ukraine, and the United States of America.

Although not a Ransomware-as-a-Service operation, they had a documented list of 120+ victims dating back to 2022. This group conducted high-profile attacks on critical infrastructure worldwide.

According to Europol, from October 16 to 20, joint operations took place in Czechia, Spain, and Latvia, where a prime suspect of the Ragnar locker group was arrested, and in the following days, more suspects were interviewed. Finally, the leading ransomware developer was arrested and was presented before the Paris Judicial Court at the end of the operation week. Simultaneously, the ransomware's infrastructure was seized in the Netherlands, Germany, and Sweden. In Sweden, the associated Tor data leak website was taken down.

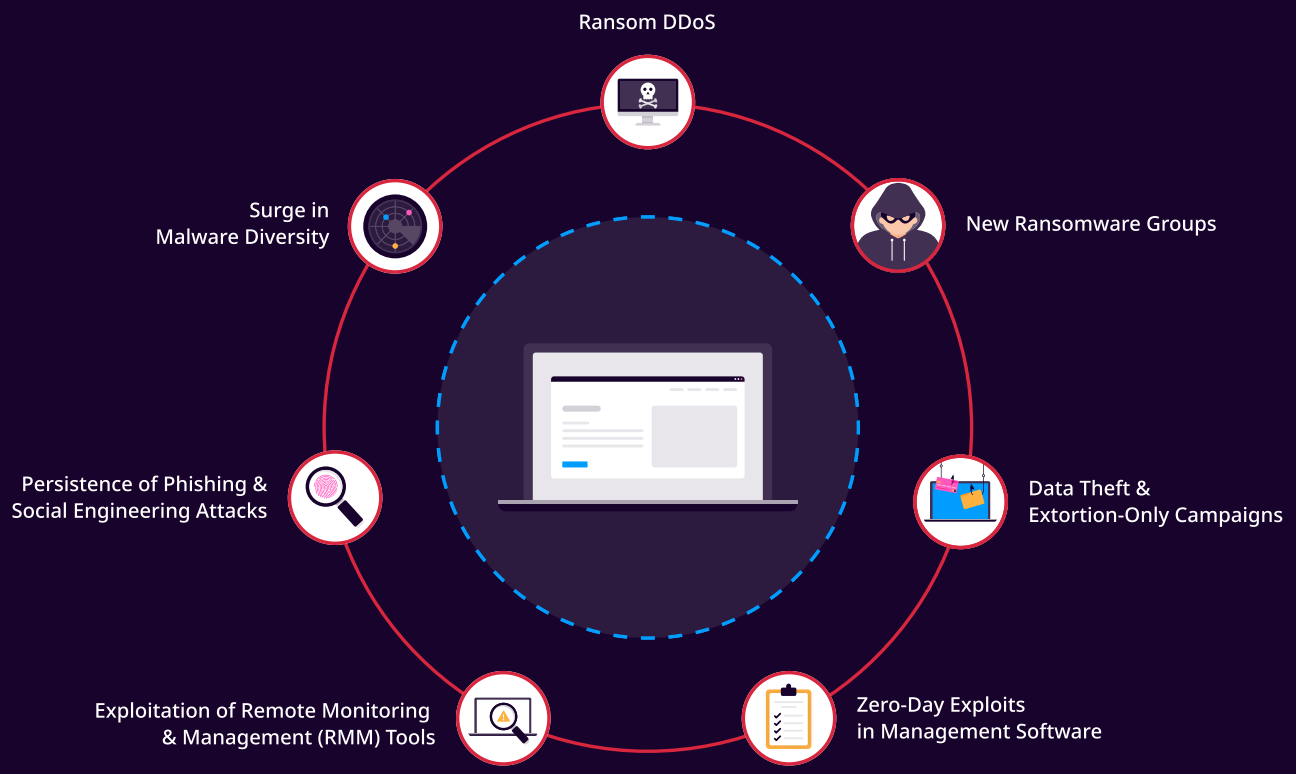
Alphv, a.k.a BlackCat, Noberus, was active since November 2021 and was one of the most active ransomware groups until December. They operated as a Ransomware-as-a-Service model and targeted both Windows and UNIX. As of September 2023, Alphv collected almost **$300 million** from around 1,000 victims. Through the joint cyber operation of the FBI and other law enforcement agencies from multiple countries, they were able to seize the AlphV server. There had been back and forth between the AlphV team hosting the new leak site and the Federal organization taking them over. Despite efforts, the affiliates' activities persist, with some victims' data being posted on new leak sites and others on alternative platforms. However, the FBI created a decryption tool enabling relevant authorities to provide decryption keys to more than 500 victims. Additionally, they successfully averted numerous ransom payments, saving victims approximately **$68 million** by supplying decryption keys for data recovery.

Global Operations

In the span of six months from July to December 2023, Interpol conducted **Operation HAECHI IV**, targeting seven categories of cyber-enabled scams, including voice phishing, romance scams, online sextortion, investment fraud, money laundering associated with illegal online gambling, business email compromise fraud, and e-commerce fraud. Concurrently, Interpol's global law enforcement initiative against internet-based financial crimes resulted in the arrest of nearly 3,500 individuals and the seizure of assets valued at around $300 million across 34 nations. Additionally, collaborative efforts between Filipino and Korean authorities, led by Korea's National Police Agency, culminated in the apprehension of a notable online gambling criminal in Manila. This two-year pursuit involved blocking 82,112 suspicious bank accounts and confiscating $199 million in physical currency and $101 million in virtual assets as part of the operation.

The Central Office for Combating Cybercrime (ZIT) and the Federal Criminal Police Office (BKA) have taken control of the **Kingdom Market** server of the darknet marketplace. This marketplace, operating on the dark web, facilitated the trade of drugs, malware, and counterfeit documents and IDs. The **BKA** suspects the operators of **Kingdom Market** of engaging in the commercial operation of an illicit trading platform on the Internet and the unauthorized trafficking of narcotics.

Unique Aspects of 2023



In the threat landscape, various unique aspects of cyberattacks were observed:

1. **Ransom DDoS:** Adversaries no longer use DDoS to disrupt the workflow, now they are leveraging DDoS to extort ransom from the targets. It is relatively easier for attackers to conduct. There is no hassle of infiltrating the system and getting past the defenses. Knowledge of the target URL or IP address would suffice.
2. **New Ransomware Groups:** The rise of new ransomware groups, such as Akira, Medusa, and Rhysida, marked a distinctive trend. Although new to the scene, they successfully accumulated a significant number of victims by the end of the year. Notably, some of these groups functioned as Ransomware as a Service (RaaS), enabling affiliates to operate freely and contributing to the growing list of victims.
3. **Data Theft and Extortion-Only Campaigns:** In 2023, some attackers escalated data theft and pursued extortion-only campaigns. Clop, in particular, caused widespread damage by exploiting multiple vulnerabilities, gaining unauthorized access, and exfiltrating data. Rather than encrypting the data, these attackers opted for ransom demands or threats of public exposure.
4. **Zero-Day Exploits in Management Software:** Experiencing a notable uptick, threat actors like Clop have actively set their sights on management software such as managed file transfer (MFT), IT Service Automation, and Print Management software, aiming to infiltrate a large number of organizations utilizing these products. Threat actors exploited multiple zero-days in GoAnywhere, MOVEit, PaperCut, and SysAid.
5. **Exploitation of Remote Monitoring and Management (RMM) Tools:** Remote Monitoring and Management (RMM) tools, crafted for the remote monitoring and administration of IT systems, pose a dual challenge by providing administrators with efficiency while acting as potential gateways for malicious exploitation. Tools like Anydesk and ScreenConnect are increasingly exploited by adversaries to circumvent defense mechanisms, ensuring persistent access to systems.

6. **Persistence of Phishing and Social Engineering Attacks:** Despite advancements in cybersecurity, phishing and social engineering attacks remained a persistent threat in 2023. Attackers used fake emails, websites, and phone calls, and even messaged the victims to trick them into revealing sensitive information or installing malicious software.
7. **Surge in Malware Diversity:** There has been a significant rise in utilizing multiple malware categories this year, with a notable increase in loader and proxy malware. To fulfill specific objectives, adversaries have increasingly turned to various malware variants, like SmokeLoader, SystemBc, and Socks5Systemz. This includes encrypting traffic to C2 to evade network-based detection.

These unique aspects highlight the dynamic and complex nature of the cyber threat landscape in 2023 and urge businesses and organizations to stay vigilant and informed about the latest trends and best practices for cybersecurity.

Commonalities with Previous Years

The threat landscape exhibits high continuity with previous years. Many threat actors persist, either rebranded or split into new groups. The tactics and techniques mainly employed mirror those from earlier periods. The exploitation of vulnerabilities for initial access remains constant, with the only variation being in the specific vulnerabilities targeted and exploited. Adversaries persist in pursuing consistent objectives, including infiltration, evasion of defenses, sustained access, and the retrieval of sensitive data, employing similar techniques as the previous year. Also, some adversaries' goals to achieve specific objectives, such as causing damage to victims or initiating the breakdown of infrastructures, remain the same.

The cyber threat landscape is expected to remain complex and challenging. A proactive approach needs to be adopted by organizations in cybersecurity, continuously assessing risks, implementing robust security controls, and staying informed about the latest threats and trends. By taking these steps, organizations can minimize their cyberattack exposure and protect their valuable data and assets.

Timeline of major attacks in 2023

Please click on the headlines to read more

JANUARY
- Royal Mail ransomware attack
- T-Mobile data breach
- NFT Investments phishing attack

FEBRUARY
- Zero-day exploitation in GoAnyWhere
- Dish Network ransomware attack
- U.S. Marshals Service ransomware attack
- RailYatri data breach
- People Connect data breach

MARCH
- Lapsus$ cyberattacks
- AT&T data breach
- Latitude Financial data breach
- Trojanized 3CX Desktop Applications

APRIL
- German wind turbine manufacturer Nordex cyberattack
- Vastaamo data breach
- Leaked Pentagon documents
- A ransomware incident at Americold

MAY
- US govt contractor ABB ransomware attack
- Luxottica data breach
- Indonesia's BSI Bank data leak
- Norton Healthcare data leak

JUNE
- Oregon, Louisiana state IDs stolen
- Genworth Financial Data Breach
- TSMC Ransomware attack
- Shell ransomware attack

JULY
- Estee Lauder data breach
- Microsoft hack sees emails stolen from US agencies
- Israeli Oil Refinery attack
- Delta Dental 7 million individuals impacted after MoveIt zero day exploitation

AUGUST
- UK Electoral Commission
- Discord data leak
- Data compromised following MOVEit attack
- Salesforce Email Service Zero-Day Exploited

SEPTEMBER
- MGM Resorts cyber attacks
- DarkBeam data leak
- Motel One ransomware attack

OCTOBER
- Largest Indian Data Leak
- Airbnb Data Breach
- CDW Corporation ransomware attack
- Israel-Hamas cyber conflict
- Facebook's official page was hacked
- A breach in Okta's customer support management system
- Mr.Cooper 14.7 million customers' data exposed

NOVEMBER
- Kubernetes Secrets leak
- McLaren Health Care data breach
- Toyota hit by Medusa ransomware
- Idaho National Nuclear Lab Data breach
- Henry Schein ransomware attack
- LoanCare's more than 1.3 million individual data breach

DECEMBER
- VF Corporation
- Xfinity 36 million customers' data breach
- Yakult Australia 95 GB data leak after a breach
- GTA 5 source code leaked
- EasyPark Data Breach

The digital realm in 2023 resembled a battlefield, with cyberattacks raining down on diverse targets. While headlines screamed "ransomware rampage," the story goes deeper. From crippling healthcare systems to exposing millions of data, these digital onslaughts cast a wide net, leaving no sector unscathed.

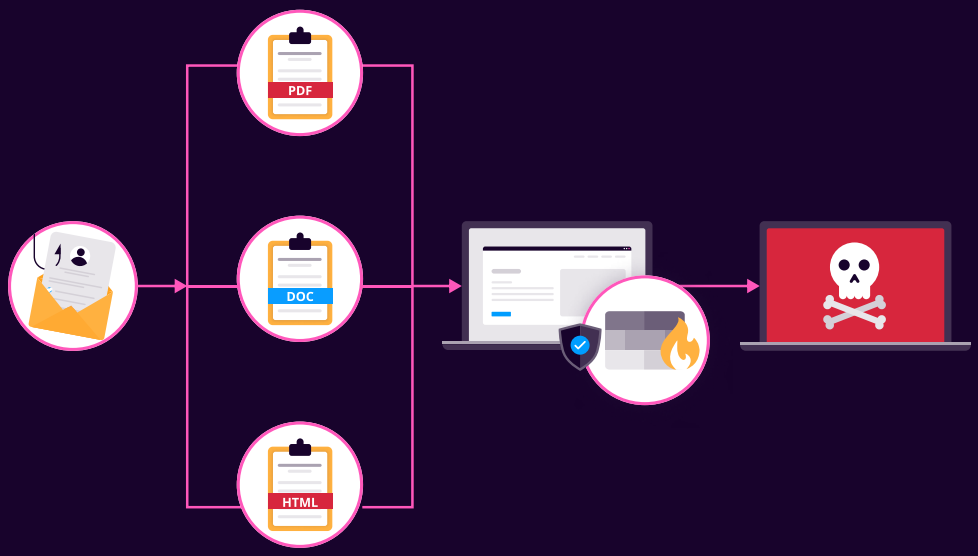
Ransomware, the reigning menace, demonstrated its omnipresence and devastating reach. Critical infrastructure bore the brunt, with the **US Marshals Service**, **Dish Network**, and **Liverpool NHS Hospital** falling victim early in the year. The grip tightened as energy giants such as Suncor and **TSMC**, alongside **Toyota**, faced a similar fate. These attacks sent a sobering message: no sector stood immune to this evolving threat.

The year also bore witness to an unsettling surge in data breaches. **T-Mobile** and **Royal Mail's** January ordeals served as preludes to the widespread exposure of millions of users' information in attacks on Latitude Financial, Lapsus$'s audacious targeting of tech giants, and massive breaches at **Airbnb**, **23andMe**, and **CDW Corporation**. The compromise of sensitive medical data during attacks on **McLaren Health Care** and the **Idaho National Nuclear Lab** further heightened data privacy and security concerns.

Beyond the visible chaos, a deeper layer of cyber warfare unfolded. **Leaked Pentagon documents** hinted at potential espionage, while attacks on **Estee Lauder** spotlighted the rising threat of intellectual property theft. **Tesla's** data breach and assaults on government contractors underscored the potential for widespread disruption and economic harm.

This multifaceted threat transcended borders, encapsulated by global incidents like the most significant Indian data leak and the Israel-Hamas cyber conflict. Even renowned brands like **VF Corporation** and **Xfinity** succumbed to attacks, underscoring the vulnerability across diverse industries and critical services.

WHAT TOOK THE SPOTLIGHT THIS YEAR?



Initial Access Payloads

As **macros from the internet are blocked by default**, the use of malicious macros-enabled office documents has been significantly reduced. However, office files like Word and Excel exploit vulnerabilities such as **CVE-2017-11882** and **CVE-2017-0199**. Delivery mechanisms such as PDF Droppers, CVE-2017-11882, and HTML Smuggling have become popular.

PDF Droppers

A PDF dropper is a carrier for malware or other form of payload. PDF files are widely used and trusted for sharing documents. Many users need more thought to open PDFs, making them an attractive vector for attackers. Attackers embed malicious payloads within the PDF file to exploit vulnerabilities in PDF readers or employ social engineering tactics. They may prompt victims to act by clicking on links within the PDF document, leading to the execution of embedded malicious code or redirecting users to malicious sites. For instance, a PDF could deceive users into clicking what appears to be a harmless link, only to turn them to malicious sites for downloading payloads or delivering attached malicious content. PDF droppers are versatile because they can carry various types of malicious payloads. They are not limited to a specific format, allowing threat actors to use them to deliver various malware, such as loaders, stealers, ransomware, or other malicious software.

CVE-2017-11882

CVE-2017-11882 is an old Microsoft Office Memory Corruption Vulnerability located within Equation Editor, facilitating remote code execution upon exploitation. Since it is not a recent vulnerability, a patch has been available since November 2017. Nevertheless, due to the negligence or persistent delay in organizations and individuals adopting the practice of patching or upgrading their software to the latest versions, adversaries frequently leverage the CVE-2017-11882 exploit to gain initial access to the victim system. From the phishing intelligence report of Cofense, which ranked among the top five payload delivery mechanisms during the first three quarters of 2023, CVE-2017-11882 remains significant. This suggests that it will likely maintain its position in the top 5 list during the fourth quarter as well and in upcoming times, given the abundance of payloads available in **MalwareBazaar**.

HTML Smuggling

One of the most used file types for phishing is an HTML file. It is leveraged to perform HTML Smuggling, which utilizes the capabilities of HTML5 and JavaScript, which are supported by every modern web browser.

HTML Smuggling operates by deceiving a target into opening a malicious HTML file, often delivered through phishing emails. Once opened, the victim's web browser loads a payload containing malicious JavaScript code hidden within the HTML file. Attackers craft a payload that uses JavaScript to create a malicious file dynamically from existing code. As a result, when the browser executes this JavaScript, it discreetly places the fully-formed payload on the victim's system. Through this manipulation of JavaScript, attackers exploit the user's trust, implementing their malicious agenda.

Unlike any other methods, payloads are locally built into the system using this technique. As a result, many of the security controls in place are bypassed.

Mark of the Web Bypass

A security feature known as "Mark of the Web" (MOTW) functions as a warning label for files downloaded from the internet, aiding your computer in identifying potential risks. Whenever a file is downloaded from the internet, an Alternate Data Stream file, "Zone.Identifier," is created, which contains the relevant identifier number, i.e., 3. Below is the list of identifiers

Description	ZoneId
File from local system	0
File from local intranet	1
File from trusted sites	2
File from Internet	3
File from Restricted sites	4

These zone identifiers help security features like Windows Defender SmartScreen recognize that the file originated from the internet, triggering necessary precautions such as warning users to deny the program's execution.

Sneaky attackers find ways to get around these protections, like using container files such as `.iso`, and `.vhd`. ISO files are container files that are an exact copy of a CD or DVD. A virtual hard disk (VHD) is a disk image file format for storing a hard drive's contents. These attackers create an ISO or VHD file with their payload files inside the container files. When a user downloads a container file, MOTW (Mark of the Web) functions appropriately, assigning a relevant Zone Identifier, set to 3. However, since an ISO file is a container, including it in the system is simple. The files use a different file system called Optical File System. MOTW works differently than intended since it is only supported in NTFS. Besides, VHD files can be configured to support another file system instead of NTFS so that MOTW can be bypassed.

Loaders

Adversaries heavily rely on Malware Loaders to discreetly deploy their obfuscated payloads in the system. These Loaders are highly confusing and are designed to circumvent defense mechanisms and establish connections to Command and Control (C2) servers. Their versatility allows customization for maintaining persistence or escalating privileges based on the configuration.

Directly deploying primary payloads, such as remote agents, beacons, or customized malware, escalates the risk of detection. To minimize this risk, adversaries favor using malware loaders due to their extensive botnet infrastructure, enabling seamless payload distribution without the threat of Network Security Controls blocking C2 addresses.

In the event of detecting adversaries' primary payloads or intrusion attempts, there is a substantial likelihood of the malware undergoing analysis by Blue Teamers and Threat Intelligence Analysts. As a result, threat actors have to work on creating new malware variants, which will be cumbersome and time-consuming.

Below are the top loaders uploaded in **any.run**

1. SmokeLoader
2. PrivateLoader
3. DbatLoader
4. GCleaner
5. HijackLoader

InfoStealer

Infostealers play a crucial role in identity theft and are often available as Stealer as a Service for threat actors. Despite their relatively affordable prices, they present a significant threat by targeting a broad spectrum of users.

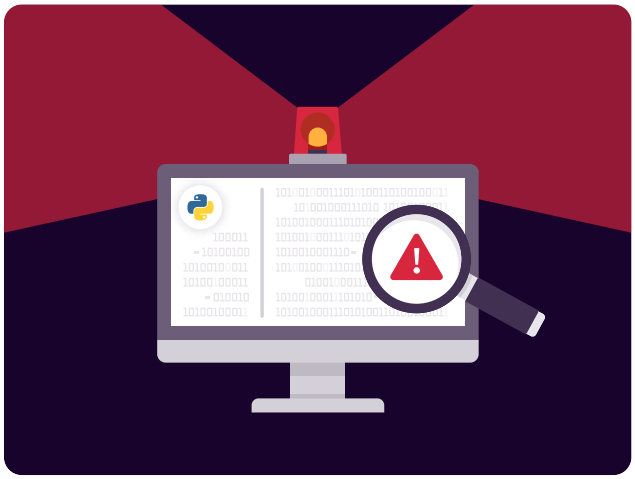
They are distributed primarily via phishing and cracked applications. Once an infostealer infiltrates a system, it carries out its intended purpose, typically involving the theft of sensitive data and credentials from various sources like the system itself, application configuration data, web browsers, e-wallets, and mail clients. The stolen information is then transmitted out of the compromised system.

Several well-known infostealers, including RedlineStealer, AgentTesla, Vidar, Amadey, and Formbook, have gained notoriety. These stealers actively search for sensitive data within the system. Some stealers target specific types of sensitive data, such as **Ducktail** Infostealer, which primarily targets Facebook business accounts. Threat actors employ these stealers to extract system information, user data, and credentials from victim systems, utilizing various techniques and leveraging legitimate platforms such as Discord and Telegram for exfiltration.

Many known breaches have occurred due to InfoStealer, such as the **Uber hack** and the **Airbus data breach** after an employee system was infected. In another case, Russian threat actors were deploying **GraphSteel** infostealer on the Ukrainian government's system. Also, in the recent **3CX supply chain attack**, adversaries dropped infostealer, i.e., ICONICSTEALER, which specifically targeted application configuration data and web browsers.

Malicious Packages

A malicious package constitutes a type of malware distributed in the guise of an open-source package and uploaded to a package repository like PyPI or NPM. It aims to target unsuspecting developers or companies who install and execute these packages inadvertently. These malevolent packages can facilitate a range of attacks, including unauthorized access, the divulgence of confidential information, excessive consumption of computing resources, and, in some cases, the destruction or manipulation of data. This technique aims explicitly at developers as its primary audience, posing a potential threat to the final product created by those utilizing such packages.



Typically, these malicious packages masquerade as authentic ones, employing dependency confusion and typosquatting tactics. As a result, if users accidentally install a malicious package due to typos or encounter a bug in the development environment that fails to differentiate between a local package in a software build and a package with the same name in a public software repository, it leads to the download and execution of malicious payloads into the system. Sometimes, these packages are also falsely advertised as legitimate, pretending to carry out specific tasks while intending harm. An **example** is the VMConnect module uploaded by adversaries to resemble the legitimate vConnector. Some of the **packages observed** were configured with PowerShell script to drop other payload stages. And others can be loaded with **infostealers** and configured according to adversaries' requirements.

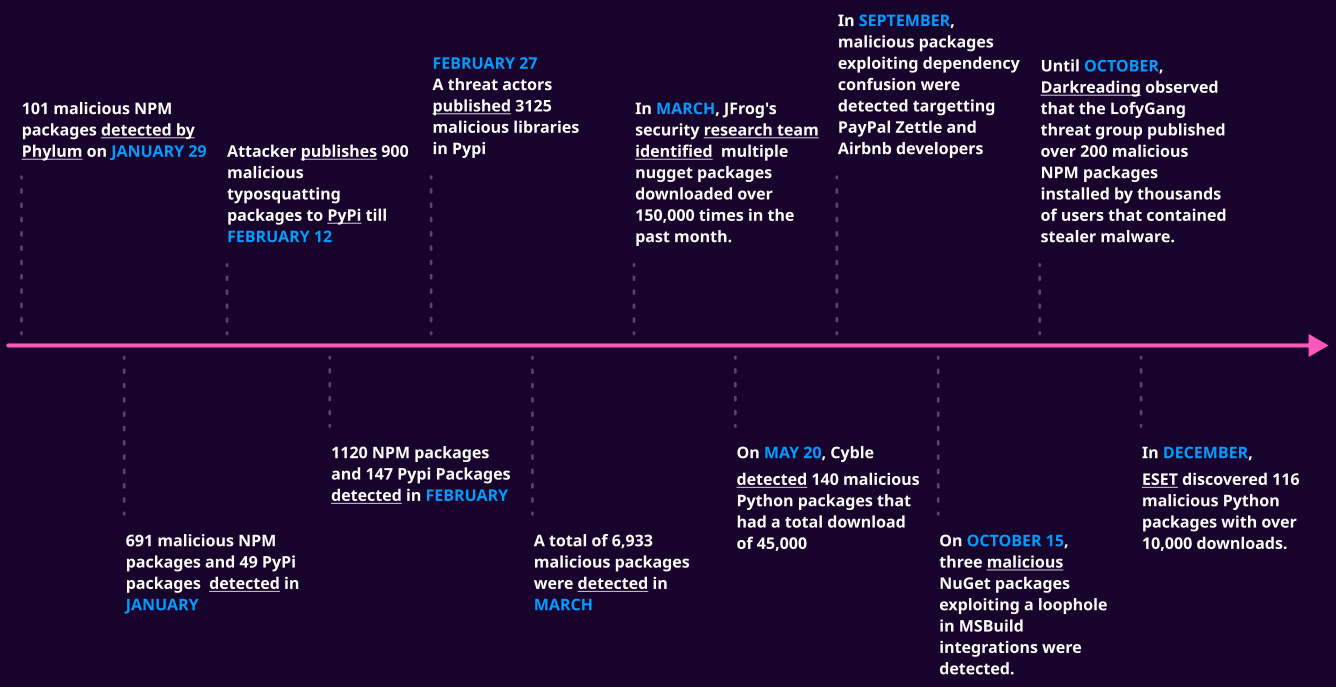
One of the earliest **research** studies published by **Nikolai Tschacher** demonstrated the risk of typosquatting programming language package managers by publishing **214** unique typo packages on PyPi, NPM, and RubyGems, which got 92 average installations per package.

In November 2022, **Sonatype** detected and blocked over 101,000 malicious packages uploaded to the open-source repositories.

Moving forward in December 2022, after the collaborative effort between **Checkmarx** and **Illustria**, it was **discovered** that a combined total of 144,294 malicious packages were generated. Among these, 136,258 were published on NuGet, 7,824 on PyPi, and 212 on NPM.

Crafty attackers find ways to get around these protections, like using container files such as `.iso`, and `.vhd`. ISO files are container files that are an exact copy of a CD or DVD. Whereas virtual hard disk (VHD) is a disk image file format for storing the entire contents of a hard drive. What these attackers do is create an ISO or VHD file with their payload files inside the container files. When a user downloads a container file, MOTW (Mark of the Web) functions properly, assigning a relevant Zone Identifier, set to 3. However, because an ISO file, being a container, can easily integrate into the system, and the files use a different file system called Optical File System, MOTW doesn't work as intended since it's only supported in NTFS. Besides VHD files can be configured to support another file system instead of NTFS so, MOTW can be bypassed.

2023 Stats for malicious package



LOOKING BACK AT THE THREAT LANDSCAPE

Cybercriminals have persistently advanced and employed increasingly sophisticated techniques to evade traditional security measures. These tactics encompass leveraging social engineering, exploiting unpatched vulnerabilities, and targeting critical infrastructure. The situation highlights the need for organizations to invest in advanced security solutions and stay informed about the latest cyber threats.

Ransomware Evolution

Ransomware has evolved a lot since its introduction from a mere floppy disk demanding a few hundred dollars. Today, it's a **billion-dollar** industry and is still growing. According to **Sophos**, the average ransom demand reached a staggering **$1.4 million**, almost double that of 2022, i.e. **$812,380**. Additionally, the percentage of organizations making larger ransom payments has grown compared to 2022, **with 40% now acknowledging payments of $1 million or beyond**, contrasting with the mere 11% reported in the previous year. It has grown to be a separate industry, and even if the ransomware group shuts down, they come up with rebranding or are recruited by some other groups to continue their actions. Every year, threat actors develop novel techniques to get past the defenses and cause a massive loss to the victim. Besides direct attacks, adversaries also use supply-chain attacks to get into the victim's environment and infect them.

In 2023, Ransomware-as-a-service (RaaS) was a popular business model where ransomware developers sold their malware to other cybercriminals who then used it to launch attacks. **Ransomware targeting cloud services is growing as more organizations move their data to the cloud**. Ransomware attackers were increasingly targeting IoT devices due to their lack of security. **Ransomware targeting mobile devices was also a growing trend as more people used their smartphones and tablets for work**.

Ransomware attacks have evolved to include supply-chain attacks, where adversaries exploit vulnerabilities in the supply chain to infect victims. RaaS is making the launch of ransomware attacks accessible to people with little technical knowledge and few dollars in their pocket. **Pre-built and easy-to-use ransomware kits and tutorials are readily available on the dark web, making it relatively easier for aspiring cybercriminals to get into the business**. This "democratization" of ransomware has amplified the threat landscape and encouraged cyber criminals to participate in cybercrime.

Ransomware has gradually developed its methods of making the ransom payment undeniable. Multiple extortion techniques have been employed to get the demanded ransom out of the victims. **Irrespective of the sensitivity, they are targeting even critical sectors like healthcare and education for their financial gain and only backing down once they get the demanded ransom**.

AI-powered ransomware threats are also on the rise. Adversaries are leveraging AI to automate vulnerability scanning and negotiating ransom. **In their extortion videos, they also use Gen-AI to create sophisticated artifacts and deepfakes**.

Ransomware attacks are no longer just the domain of petty criminals. **Nation-states increasingly use ransomware as a cyber warfare tool, targeting critical infrastructure and government agencies**.

According to the available data, 9 more active ransomware groups exist than last year. As of December 10, 2023, there are 1254 new ransomware victims this year, a 31.79% increase in ransomware victims. **March 9, 2023, saw the highest number of victims, with 182 affected that day**.

Phishing Metamorphosis

Phishing has been a lifelong headache for organizations. It has existed since the beginning and is constantly morphing into newer ways to deceive end users. It has been exploiting the weakest link in the cybersecurity realm i.e. “Human”. **742.9 million phishing emails** have been sent to inboxes in the first half of 2023 alone, a staggering 54% increase compared to the same period in 2022.

They put aside traditional attack techniques like spear phishing, vishing, and whaling. Attackers are coming up with even more sophisticated techniques like **Deep fakes** - for instance, **"Imagine a video message where your CEO asks you to send him some confidential documents with a sense of urgency prompting you to act quickly."** Almost all of us will act accordingly without thinking. This has become a reality today. With the advent of AI deepfakes, adversaries are exploiting their capabilities to deceive people. It has become the most chilling realism in the game.

Phishing-as-a-Service (PhaaS) has also democratized the attack. Pre-built phishing kits and tutorials are readily available and easy to use. Lesser technically sound people are also getting encouragement to get into the business. It has allowed anyone to launch sophisticated phishing attacks with ease. Not just that, AI chatbots like ChatGPT can also be used to generate content that can mimic the tone and style of the legitimate sender to fool the victims, thereby increasing the chance of being affected.

Apart from the conventional attacks, **‘Quishing’ has entered the fray**. It is a form of phishing that uses QR codes to trick users into providing personal information, downloading malware, or visiting phishing websites. These work uniquely and bypass the traditional measures. They cannot be read until rendered, and even after being rendered, they cannot be identified by only looking at them. The previously known "hover and see the link" won't work here.

With the rise of Vishing, Phishing has even further evolved into a hybrid phishing technique. i.e., **"callback phishing"**. It is also known as **"BazaarCall".** It is an advanced spearphishing technique threat actors use to gain initial access to the system. It works in multiple stages. At first, they gain the victim's trust by sending seemingly legitimate and clean emails containing some information. They then instruct the victims to expect a callback or encourage them to contact the given number through which they manipulate the victim, get their way in, or infect them.

Threat actors are further using **SEO Poisoning** for their malicious activities, like the delivery of malware or data theft. Although Search engines are advanced enough to block the typo-squatted or keyboard-stuffed malicious sites, Adversaries use other techniques like SEO cloaking, Website hijacking, and URL redirection to compromise the victims.

Gen-AI: The double-edged sword

Since the introduction of ChatGPT, it has been a lifesaver for developers and content creators. Not only that, but it has been helpful to security analysts as well. **Different vendors are adding it as a feature** in their security products. However, it has become a double-edged sword, empowering adversaries with malware development, advanced phishing, and automated zero-day exploit discovery.

Gen-AI carries so much potential and has been exploited by adversaries to the next level. Its capability, called **voice cloning**, is scary because it can imitate a voice and replicate gestures with a few seconds of audio. Since it is indistinguishable from the actual person, vishing is even more effective, and victims easily fall for it.

Phishing 101 was to look for writing patterns and grammatical and spelling mistakes in the email or message. But gone are the days because AI can easily mimic a person's language and writing pattern, and it can be indistinguishable from a real one without any flaws. The language barrier no longer remains the issue. The written content and the language in a **video** can be easily changed. The end victim cannot identify whether they are interacting with the actual person or the adversary. Deep fakes are the next big thing, which we talked about earlier.

It has helped developers to generate secure code. However, it can also be used to create novel and evasive malware variants on the adversarial side. Imagine AI churning out millions of malware samples, each slightly different, making traditional antivirus software obsolete. AI automation to search for software vulnerabilities can help adversaries discover zero-day exploits before developers or security vendors can patch them. This gives attackers a critical window of opportunity to launch devastating attacks.

Gen-AI is still evolving, and with all these **capabilities**, It has become difficult for an average person or even a technically sound person to differentiate between normal and fraudulent activities.

War influence

In recent times, the battleground has expanded beyond physical territories into the realm of cyberspace. The Russia-Ukraine conflict vividly illustrates this shift, but it's not an isolated incident. The current situation with Israel and Hamas further emphasizes this evolution. In 2023, warfare has significantly contributed to the surge in cybercrime, with nation-states and their proxies engaging in extensive data breaches. They've targeted military intelligence, economic strategies, and critical infrastructure blueprints.

The tactics employed by adversaries have evolved beyond traditional breaches. They're weaponizing disinformation through fake news, social media manipulation, and even hacking news channels. The aim is precise: eroding public trust, influencing elections, and sowing discord.

Within the threat landscape, classified documents have been exploited to disrupt diplomatic relations and expose national security vulnerabilities. Conflict zones have become fertile ground for cybercriminals, where attacks and thefts are rampant. The ongoing strife in Ukraine, for instance, has witnessed a surge in cybercriminal activities, affecting both combatants and civilians alike.

The correlation between war and cyber threats has birthed a new breed of attacks involving sophisticated malware and intricate strategies. The Russia-Ukraine conflict is a testament to this, showcasing both sides' development of intricate cyber offensives. 2023 has furthered this trend, witnessing the emergence of novel malware and innovative attack methodologies.

Cloud Security

The digital landscape is undergoing a monumental shift, with businesses and organizations of all sizes migrating to the cloud. Cloud services have revolutionized how organizations access and utilize computing resources. Due to numerous benefits, organizations are moving towards the cloud. These services provide flexibility and cost efficiency allowing businesses to scale resources based on demand, optimize costs, and foster collaboration among geographically dispersed teams.

However, Cloud security has become a severe issue. With the mass adoption of cloud service, the attack surface is growing larger and is getting harder to manage. Sensitive data in the cloud means an equal need for security postures, as the consequences might be devastating.

Identity, credentials, access, and key management have become an issue. Improper management leads to the credentials falling into the wrong hands and, finally, to data breaches and system compromise. Not only that but insecure interfaces and APIs are also an issue. A small mistake from the employees can result in multiplied damage. A simple misconfiguration caused by simple human error can cause much damage to the organization.

Cloud-native malware is on the rise as well. These are specially designed for cloud environments and can be sophisticated and challenging to detect and remove.

Cloud services pose a greater risk of data breaches. Adversaries, if successful in exploiting vulnerabilities to get access to the cloud services or by other means, can result in data theft and misuse. Insiders with access to the resources can access, tamper, or steal sensitive data and misuse cloud resources. Although it can be intentional or unintentional, it poses a severe risk.

Supply chain attacks are also on the rise, as adversaries exploit third-party software or hardware vulnerabilities to get into the victim machine. Further, cloud jacking is also a rising issue in cloud security where adversaries misuse the cloud services. Not only that, but accidental cloud data disclosure has also become a severe issue. Exposing databases to the public internet remains an issue. Those databases further have weak passwords or do not require any authentication, making them easy targets for threat actors. Also, service and security misconfiguration is another common issue resulting in an intrusion on the cloud.

Zero Days

Zero-days are the flaws in software or hardware, unknown to the vendor or the public, that attackers can exploit to gain unauthorized access, steal data, or wreak havoc. These are treated as valuable objects in the dark web. A typical vulnerability in a regular application is not a big deal, but imagine a zero-day in most popular appliances used by high-profile entities. It can unlock a wonderful playground for adversaries. These zero-days are bought and sold on the dark web for millions of dollars, and the organization will remain oblivious. Organizations pay an excellent reward for vulnerability, but the same can be sold in the dark market for even more money.

Last year (2023), was no stranger for zero days. In May, **vulnerabilities** were discovered in MOVEit Transfer and MOVEit Cloud and disclosed publicly. Within 48 hours, mitigation and patch were released. However, during that time frame, the Clop ransomware group already exploited this vulnerability, which affected millions of customers.

As seen from the incident, the **Time-to-Exploit** window is narrowing. Even in a small timeframe, attackers can cause more damage. After it is known to the public, it goes to being n-Day. But still, many need to be made aware, and some are difficult to apply patches to. So they still get exploited in the wild and act as zero days.

Attackers are also coming up with variants of the previously disclosed vulnerabilities and weaponizing them as their zero days.

DDoS

The world saw a significant amount of DDoS attacks this year as well. Year after year, the attackers are developing new ways to launch powerful, sophisticated DDoS attacks against multiple targets. Banks and other financial institutions, including online retailers, which rely heavily on online transactions, are often targeted by adversaries, which can cause vast amounts of economic damage. These attacks cause businesses to lose revenue due to downtime and lost productivity. Not only that, but it damages the company's reputation and erodes the customer's trust as well. Attackers often use DDoS as a diversionary tactic to launch other cyberattacks.

Killnet and **AnonymousSudan** were the most active groups conducting large attacks in the first quarter. Hyper-volumetric DDoS attacks were on the rise, it peaked above **71 million requests per second** (rps) — which exceeded Google's previous world record of 46M rps by 55%. These attacks leverage a new generation of botnets, which can be as much as **5000 times** stronger than the traditional botnets comprised of IoT devices. Adversaries have also used DDoS as a third option for extortion. However, it is not always necessary to compromise the internal systems to threaten the victims to extort ransom. In peak business hours, adversaries often threaten businesses to provide ransom payments to avoid or stop the ransom DDoS attack. These kinds of activities occur during black Fridays or Christmas when the sales are at their maximum.

There was a massive surge in SPSS-based, DNS amplification, and GRE-based DDoS attacks. DNS laundering attacks are also rising because they are relatively hard to deflect or stop. In this kind of attack, harmful and malicious traffic appears legitimate, making it harder for victims to distinguish between legitimate and malicious traffic.

Data Breaches

According to the **Cost of a data breach** report by IBM, **“the global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.”** It also mentions that due to such violations, 51% of organizations are further investing in their security posture to fortify their defenses. This report also says that only 1 out of 3

organizations could detect their system breach by themselves. 2 out of three organizations had third parties or attackers informing them about the breach. And such a situation cost them a million more than when the internal team detected it. IBM has also observed that with investment in IR planning and testing, organizations were able to save 1.49 million.

Data breaches have become a singular motive of adversaries. In the case of ransomware attacks, they also exfiltrate data to hold the second level of extortion for the ransom payment. Unlike traditional breaches, adversaries implement supply chain attacks to compromise multiple vendors to amplify their attack and maximize the damage. The data breach doesn't only cost the data. Instead, it costs the victims a loss of reputation, customers, and regulatory fines. It creates instead a ripple effect. All the victims in the supply chain are affected.

Data breach not only affects the organizations. It involves the end users equally, not just their information. It has been seen that most organizations transfer the cost to customers, increasing the prices of services and products.

Supply Chain attacks

Supply chain attacks are cyberattacks that exploit the trust between a software publisher and a software user. The attackers compromise the software publisher's code or website and inject malicious code into the software packages distributed to the users. The malicious code can perform various actions, such as stealing data, installing backdoors, or launching further attacks.

In 2023, cybercriminals were even more sophisticated when infiltrating **supply chains** to damage or steal from businesses. **According to a report by Cybersecurity Ventures**, some of the most common supply chain attack methods and approaches included social engineering, phishing, stolen credentials, CI/CD pipeline compromise, vulnerability exploitation, and open-source component targeting.

There were several high-profile supply chain attacks in 2023. For example, In December 2022, **PyTorch** Framework was targeted in supply chain attack. In February 2023, **Applied Materials** was hit by a supply chain attack. In March 2023, **3CX** was targeted by a supply chain attack. In June 2023, **MOVEit** was hit by a supply chain attack. In September/October 2023, **JetBrains** was also targeted by a supply chain attack. In October 2023, **Okta** was hit by a supply chain attack.

Additionally, the exploitation of malicious packages to target open-source repositories like PyPI and NPM has witnessed a growing trend as vectors for deploying malware via supply chain attacks, specifically aimed at developers.

One of the platforms that is often targeted by supply chain attacks is PyPI (Python Package Index), which is a repository of open-source Python software. PyPI hosts over 300,000 packages, some of which may contain malicious code or vulnerabilities. According to some recent reports [1,2,3,4], attackers have abused PyPI packages for supply chain attacks in 2023 by using various techniques, such as:

- Embedding PowerShell scripts in the `setup.py` file of the packages, which can execute arbitrary commands on the user's system.
- Incorporating obfuscated code in the `init.py` file of the packages, which can download and run a malicious executable file from a suspicious URL.
- Using `test.py` scripts to bundle malicious code into Python packages can be executed by importing them into other Python programs.

A Double Supply Chain Attack

In 2020, despite the discontinuation of X_TRADER, users could still download the software. However, unknown to users, malicious actors sponsored by North Korea had compromised the setup file. The file harbored multiple payloads and was signed with the trading platform certificate, constituting a financially motivated attack as part of their **Operation AppleJeus**.

According to **3CX**, one of their employees downloaded and installed a trojanized version of the **X_TRADER** software on the system. The X_TRADER installation application was implanted with malware and was signed with the trading technologies certificate. After the execution of the malicious installer, threat actors were able to gain access to the victim system and were successful in retrieving credentials from the 3CX employee's system. Among the credentials, adversaries retrieved the 3CX organization VPN credentials of the employee. After infecting the employee system, adversaries could access the organization's network through a VPN.

After access to the 3CX Network, the adversaries could move laterally and gain access to the Windows and macOS build environments of 3CXDesktopApp. According to the **Mandiant**, after gaining access to the build server, adversaries were able to successfully implant a backdoor of the 3CXDesktopApp for both Windows and MacOS. Also, the Application was verified, and Microsoft even signed the Windows version implant.

When the ECX Electron application is updated the malicious version is installed. After the update, the legitimate DLLs containing backdoor implants from threat actors are dropped and executed, further dropping other stages of implants and payloads.

Initial Access Brokers

A new class of intermediaries has emerged in the shadowy underworld of cybercrime: **Initial Access Brokers** (IABs). Operating like dark web real estate agents, they facilitate the sale of access to compromised networks and systems, making cyberattacks a neatly packaged commodity. This **"cybercrime-as-a-service"** model has shattered the old paradigm, lowering the technical barrier to entry and dramatically elevating the risk for all organizations. Gone are the days when sophisticated skills were a prerequisite for cybercrime. With IABs, access is just a click and a hefty ransom away.

This shift has profound consequences. Skilled hackers can now focus on their expertise – exploiting stolen credentials or deploying malware – while others purchase pre-breached access, democratizing cybercrime and amplifying its frequency.

The evolving IAB landscape presents dangers and challenges for law enforcement. The anonymity of these brokers makes them elusive targets. International cooperation and advanced investigative techniques are essential to dismantle their networks and hold bad actors accountable.

Looking ahead, the IAB model is poised to evolve further. We can expect increased specialization, the emergence of "cybercrime brokers" offering comprehensive attack packages, and even the chilling possibility of "security marketplaces" where vulnerabilities are traded openly.

GLOBAL ATTACK PATTERNS THIS YEAR

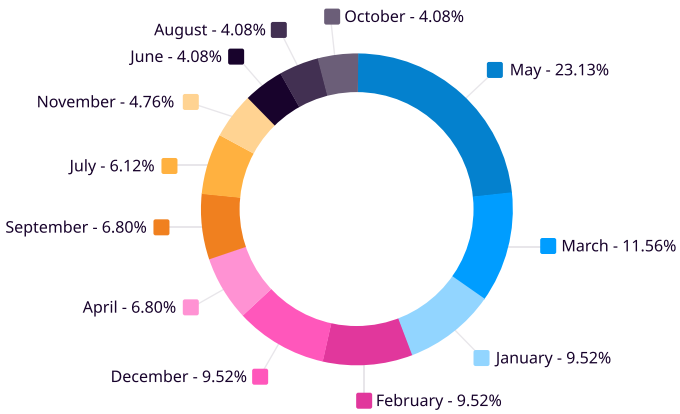
Ransomware

2023 witnessed a relentless surge in ransomware attacks across the globe, leaving a trail of crippled systems, stolen data, and substantial financial losses. Gone are the days of targeted takedowns; attackers now wield sophisticated tools and employ multi-pronged strategies, making no sector immune. Healthcare facilities, critical infrastructure, and even small businesses have become unfortunate targets, facing extortion demands that can reach millions.

Stats of New Ransomware/Malware Discovered in 2023

In 2023, the discovery of new malware and ransomware followed an uneven trajectory, with a noticeable surge in May (34) compared to other months. While the first half saw a relatively consistent average of 14 monthly discoveries, the second half dipped significantly, with June, July, and August averaging just 6. Overall, 145 new threats were identified throughout the year, highlighting the ever-present cyber threat landscape and the need for constant vigilance

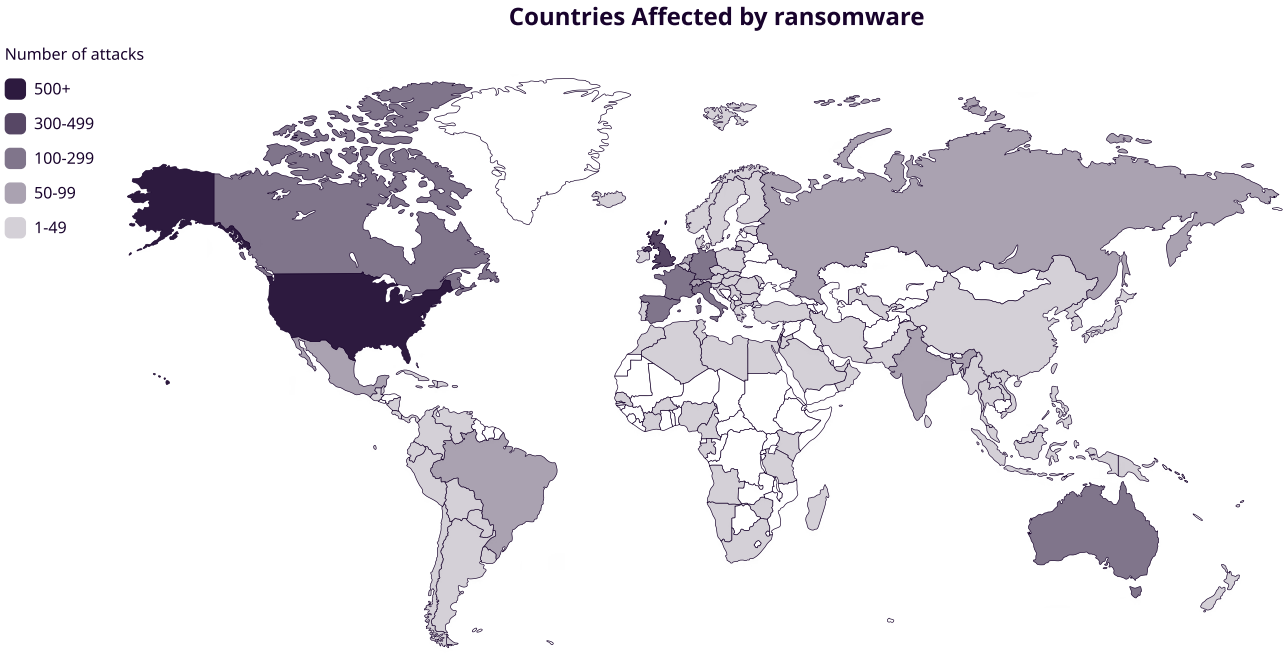
Stats of New Ransomware/Malware Discovered in 2023



Source: Cyber Management Alliance

The cyber threat landscape in 2023 was marred by a dramatic escalation in ransomware incidents, culminating in a **staggering 5,613 attacks.** This disturbing figure represents a **42% surge** compared to the **3,941 incidents** documented in 2022. Equally concerning is the marked expansion in active ransomware groups, rising from 61 in 2022 to **78 in 2023**. This **28% increase** underscores cyber threats' evolving and complex nature, demanding greater vigilance and adaptability from organizations globally.

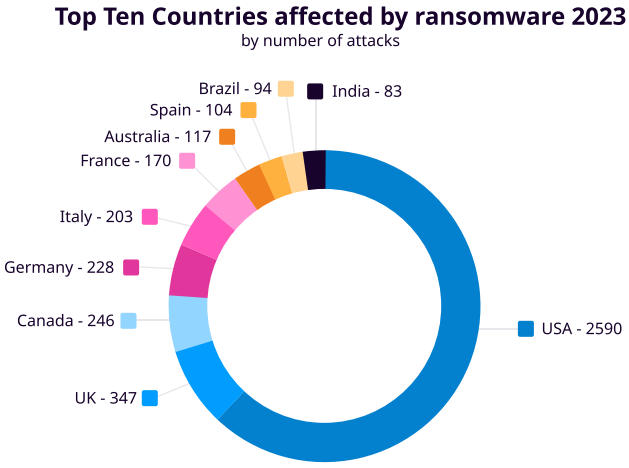
There have been a total of **5,613 ransomware attacks this year.** Among the total number of victims, some were affected once, twice, and thrice. We have referenced **Ransomfeed** for the report to collect and analyze the data. Here is the breakdown:



Global Ransomware attack pattern
Source: Ransomfeed

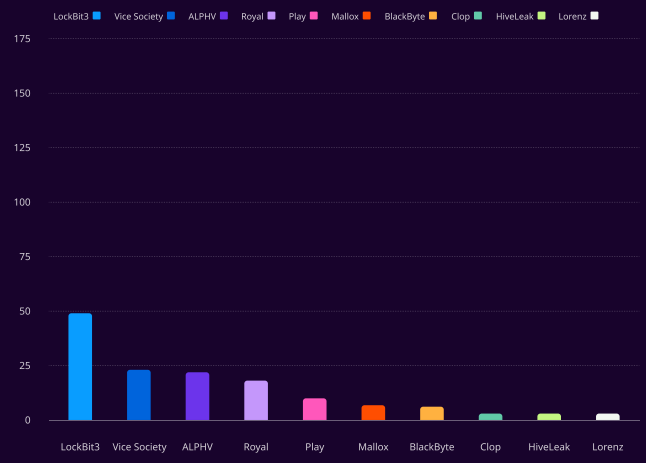
The US is the global ransomware epicenter, with 2590 victims - nearly 44% of the total attacks worldwide. This translates to over 10 times the number suffered in the UK (347) and over 30 times more than India (83). Following the US is a tightly packed group: Canada (246), Italy (203), and Germany (228) share the grim podium. Notably, these top 6 countries account for almost 60% of all documented ransomware victims globally.

The uneven distribution paints a troubling picture, with diverse nations across varied development levels suffering under this cyber scourge. Even major economies like China (41) and Japan (45) see significant numbers of victims, highlighting the widespread reach and adaptability of ransomware gangs.

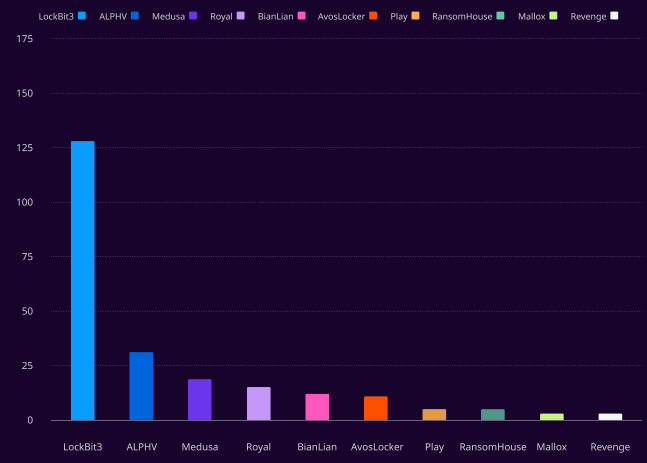


Source: Ransomfeed

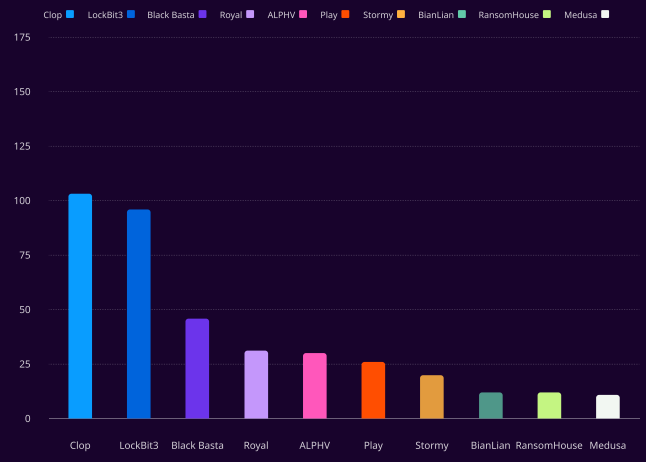
Top 10 Ransomware Groups in January 2023



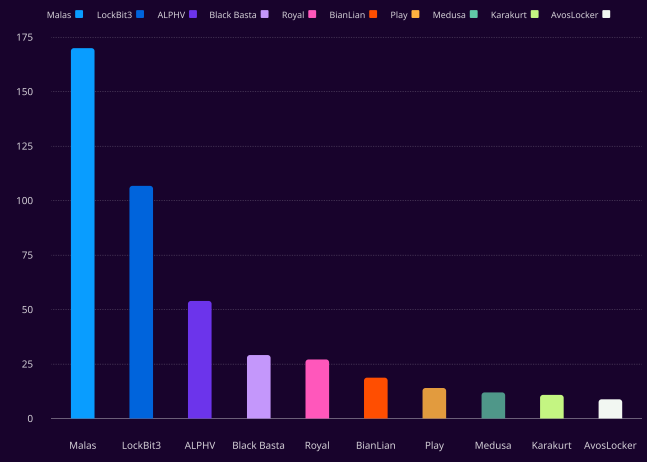
Top 10 Ransomware Groups in February 2023



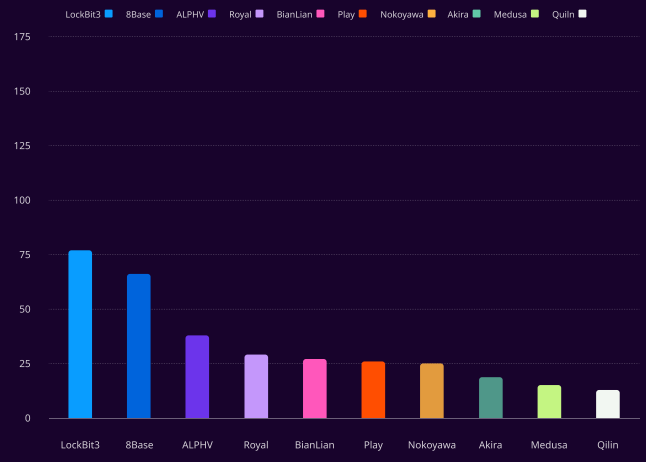
Top 10 Ransomware Groups in March 2023



Top 10 Ransomware Groups in April 2023



Top 10 Ransomware Groups in May 2023

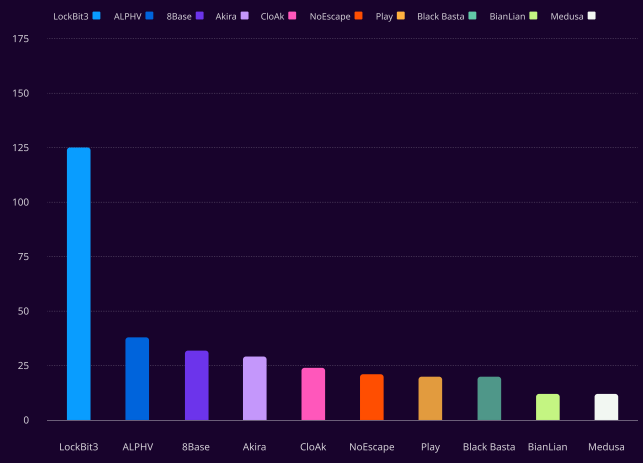


Top 10 Ransomware Groups in June 2023

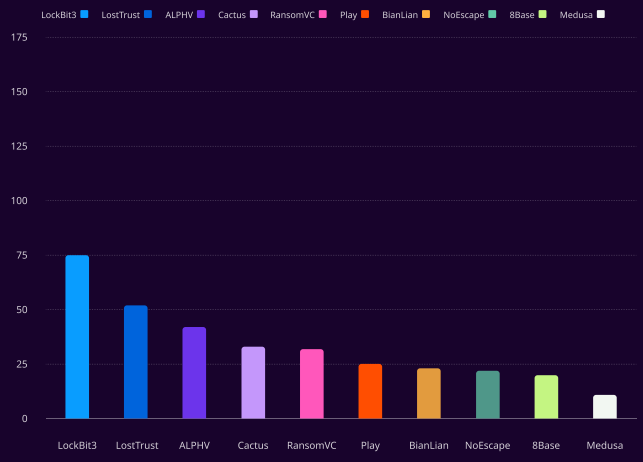
Source: Ransomfeed

Top 10 Ransomware Groups in July 2023

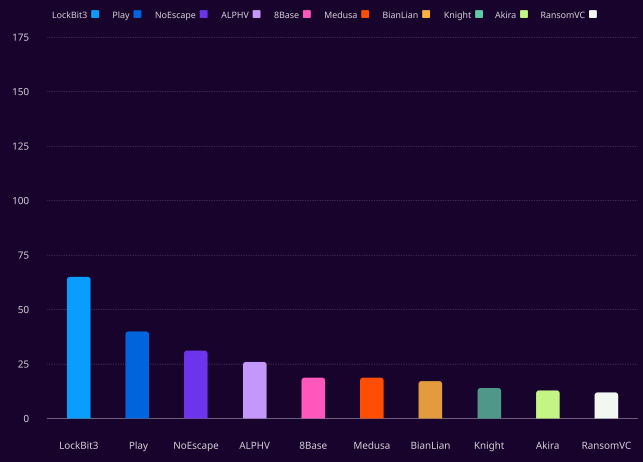
Top 10 Ransomware Groups in August 2023



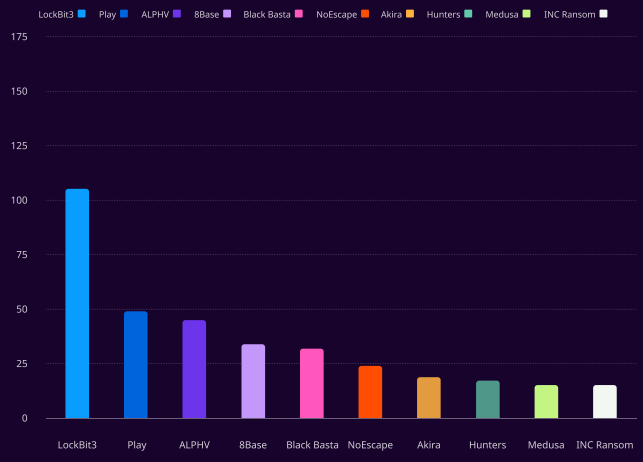
Top 10 Ransomware Groups in September 2023



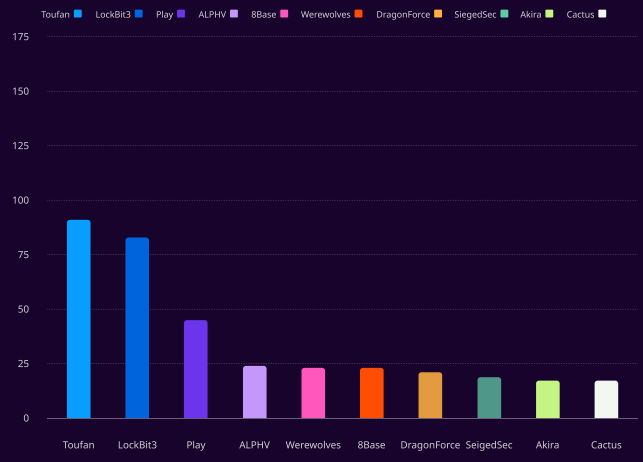
Top 10 Ransomware Groups in October 2023



Top 10 Ransomware Groups in November 2023



Top 10 Ransomware Groups in December 2023

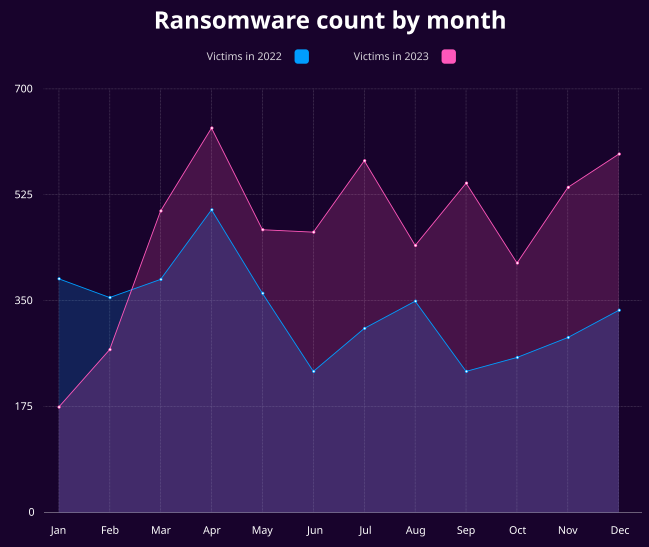


Source: Ransomfeed

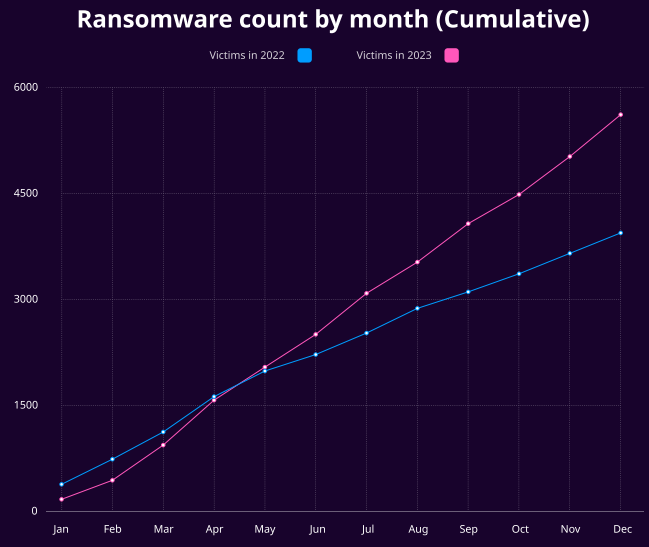
The above graph paints a grim picture of the ransomware landscape, with **Lockbit3** reigning supreme over seven of the twelve months, its consistent presence totaling a staggering **954** victims annually. However, the spotlight shifts briefly in **March** and **July**, when **Clop** surges with **103** and **170** victims, respectively, showcasing its opportunistic potential. Similarly, **Malas** roars in **April** with a peak of **170** victims. Notably, **Alphv** maintained a steady presence in the top 3 for seven months, racking up **321** victims, while **8base** remained a constant nuisance for five months, claiming **242** victims.

But it's not just established players dominating the scene. **Play** made a notable mark in **October**, **November**, and **December**, racking up **40**, **49**, and **35** victims, respectively, demonstrating its emerging threat potential. The scene gets even more enjoyable with the appearance of **LostTrust** in **September**, who debuts with **52** victims, and **NoEscape** in **October**, who joins the party with **31** victims. These newcomers and **Toufan**, **werewolves**, **Dragonforce**, **Siegedsec**, **Akira**, and **Cactus** warrant close attention as they pose potential future threats.

December brings a new twist to the ransomware landscape with the emergence of **Toufan**, which takes the top spot with **91** victims. **Lockbit3** remains a significant threat, but werewolves, Dragonforce, and Siegedsec closely follow it. These new groups and established players will keep security researchers busy in the coming months.

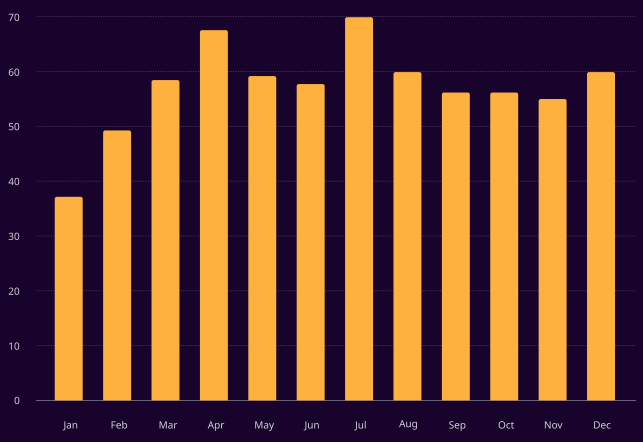


Source: Ransomfeed



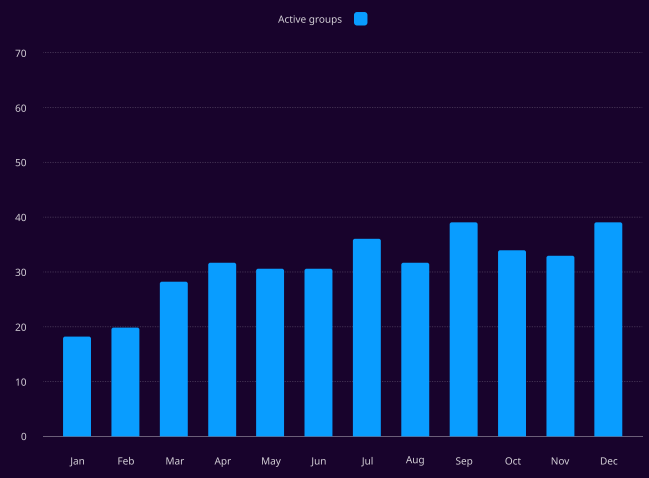
Source: Ransomfeed

Total number of countries affected by ransomware throughout the year



Source: Ransomfeed

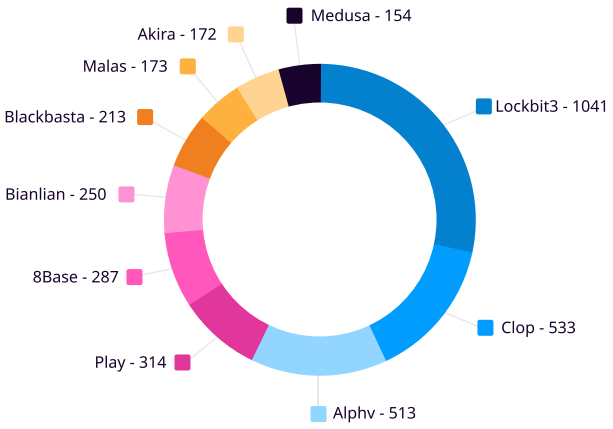
Active Ransomware Groups throughout the year



Source: Ransomfeed

Ransomware surged in 2023, with victim counts tripling from January's 174 to a dizzying peak of 635 in April across 67 countries. Though attack groups danced between 18 and 39, victim counts stayed consistently high, dipping only briefly in May and June. July witnessed a resurgence; even November, with fewer active groups, ensnared a concerning 537. December, however, saw a chilling rise, with **both victim counts (591) and functional groups (39) nearing year highs.**

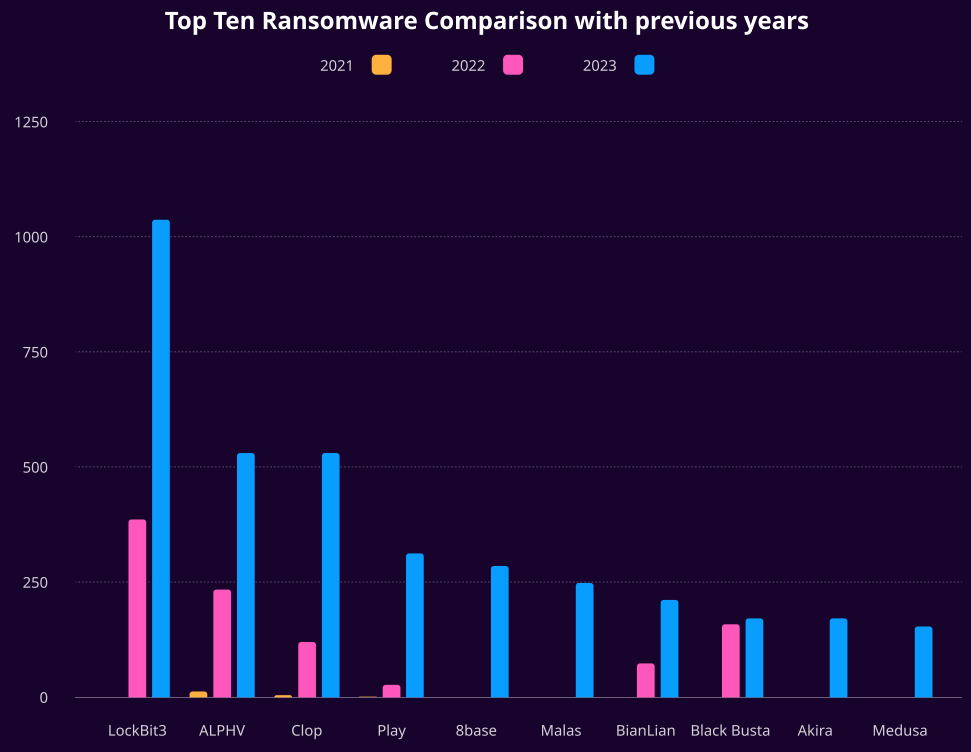
Top ten ransomware of 2023



Source: Ransomfeed

LockBit3 remained the unchallenged kingpin with **1,041** victims this year, followed by established names like **Clop** (533 victims) and **AlphV** (513 victims). These familiar actors continued their reign of terror, leaving a trail of destruction in their wake.

However, the landscape was not static. Rising stars like **Malas** (173 victims) and **Akira** (172 victims) emerged as significant threats, demonstrating the adaptability of the ransomware ecosystem. Notably, **8base**, which rose to prominence in the latter half of 2023, secured the 5th spot with **287** victims, showcasing its rapid ascent in the threat landscape.

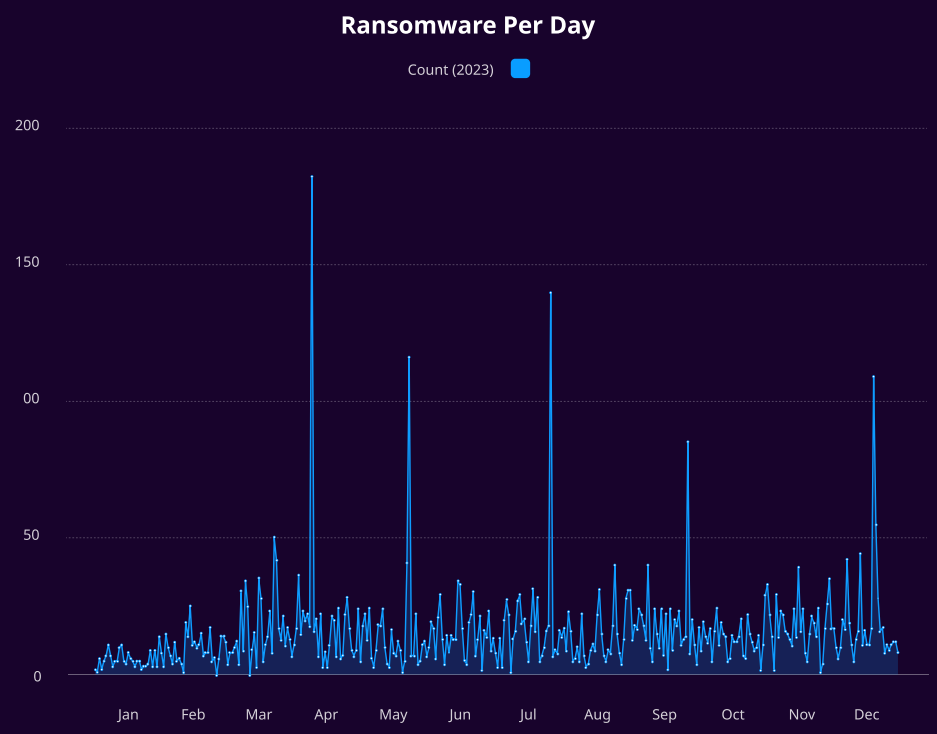


Source: Ransomfeed

Established players like **LockBit3** maintained dominance, significantly escalating victim counts from **389 in 2022** to **1041 in 2023**, representing a **167.35% increase**. AlphV and Clop also remained formidable threats within the top 5 despite experiencing minor fluctuations in victim counts.

The emergence of new contenders was evident. Play underwent a remarkable surge, escalating from 26 victims in 2022 to 314 in 2023, marking the **most substantial percentage increase (1115.38%)** among the top ten. Additionally, 8base emerged as a new threat, securing the 5th spot with 287 victims in 2023, signifying the rapid evolution of the ransomware landscape.

Previously unknown groups made an appearance. Malas debuted with 250 victims in 2023, underscoring the continual influx of new actors posing emerging threats. Similarly, Akira joined the scene with 172 victims in 2023. Bianlian and BlackBasta, prominent in 2022, experienced a decline in victim count in 2023, hinting at potential shifts in tactics or targets. Meanwhile, Medusa maintained a presence below the top ten but consistently posed a threat in 2023, illustrating the enduring risk from established less prominent groups.



Source: Ransomfeed

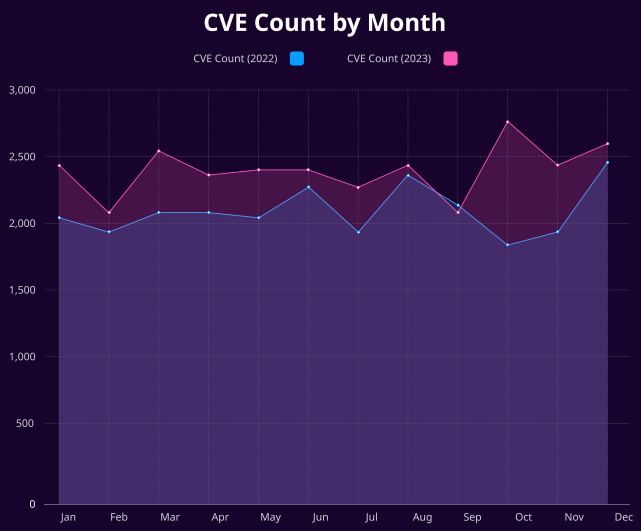
The 2023 ransomware landscape unfolds like a chilling thriller, punctuated by sudden jolts of victim counts. April 9th stands alone, a sentinel of fear with its staggering 182 victims, likely signifying a significant data breach or a particularly ruthless targeted attack. May 23rd, July 26th, September 26th, and December 19th follow with numbers ranging from 85 to 116, hinting at potential coordinated campaigns exploiting specific vulnerabilities.

For further stats: Ransomware.live

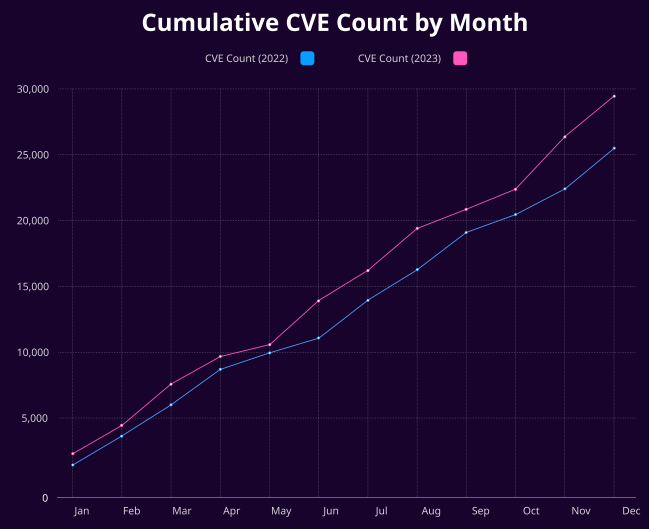
CVE

Over the past decade, the cyber landscape has been marked by a relentless surge in vulnerabilities, with the Common Vulnerabilities and Exposures (CVE) list mirroring this alarming trend, and since 2013, reported vulnerabilities have nearly tripled, from just over 5,000 to a staggering 29,065 in 2023. This upward trajectory shows no signs of slowing down. In the last three years, we've witnessed exponential growth, with the number of vulnerabilities increasing. 2023 is a stark testament to this, breaking all previous records with a staggering 16% increase from 2022, pushing the total to a record-breaking 29,065.

Source: CVEdetails



Source: CVEdetails



Source: CVEdetails

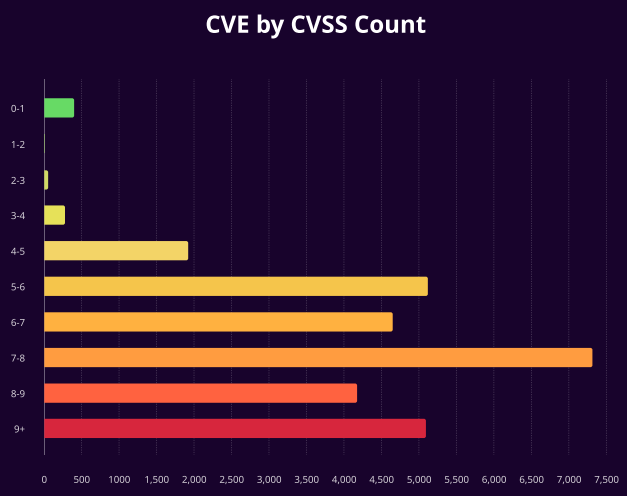
Examining the monthly breakdown of CVE counts in 2023 reveals a worrying trend. While September and November saw minor dips compared to 2022, with 2157 and 2483 vulnerabilities, respectively, the remaining months witnessed a concerning surge. October emerged as the champion of vulnerability inflation, boasting a staggering **45.5% increase**, pushing the count from 1850 in 2022 to 2701 in 2023. March wasn't far behind, witnessing a **24.1% rise**, with reported vulnerabilities jumping from 2059 to 2559. These significant spikes underscore the need for organizations to be particularly vigilant during these periods and prioritize patching critical vulnerabilities promptly.

The cumulative CVE count paints an even grimmer picture. The gap between 2022 and 2023 figures widened steadily as the year progressed. By December, the cumulative count in 2023 stood at a staggering 2677, compared to 2421 in 2022, representing a **10.6% increase**. This sustained rise in vulnerabilities reaffirms the importance of proactive vulnerability management practices. Organizations must invest in robust scanning tools, prioritize timely patching, and implement adequate security best practices to stay ahead and mitigate potential risks.

A closer look at the 2023 CVE data reveals a landscape dominated by **high and critical vulnerabilities**, demanding immediate attention from organizations. Nearly **half (49.4%)** of all reported vulnerabilities fall within the **CVSS score ranges of 6 to 9**, signifying a substantial risk for exploitation and potentially severe consequences if left unaddressed.

Among these, a particularly alarming statistic emerges: **17.74%** of vulnerabilities in 2023 scored **9 or higher** on the CVSS scale, placing them in the **highly critical** category.

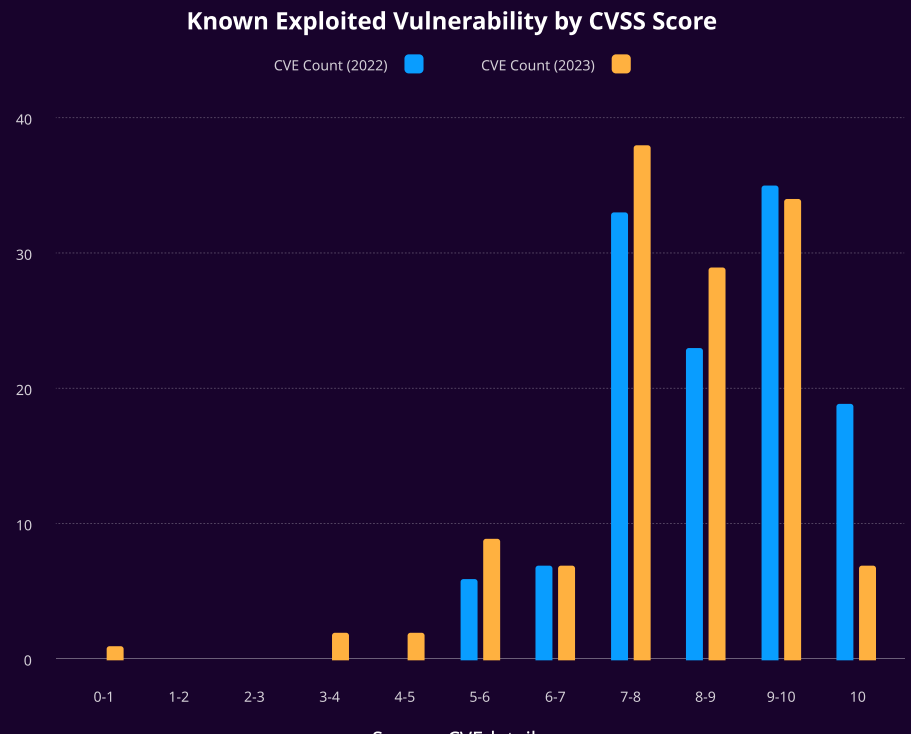
While the focus should undoubtedly be on the high and critical vulnerabilities, we shouldn't neglect the **17.72%** of vulnerabilities in the **5-6 CVSS range**. Though classified as "medium" severity, these vulnerabilities still pose significant threats. They should be addressed as part of a comprehensive security strategy.



Source: CVEdetails

Known exploited Vulnerabilities

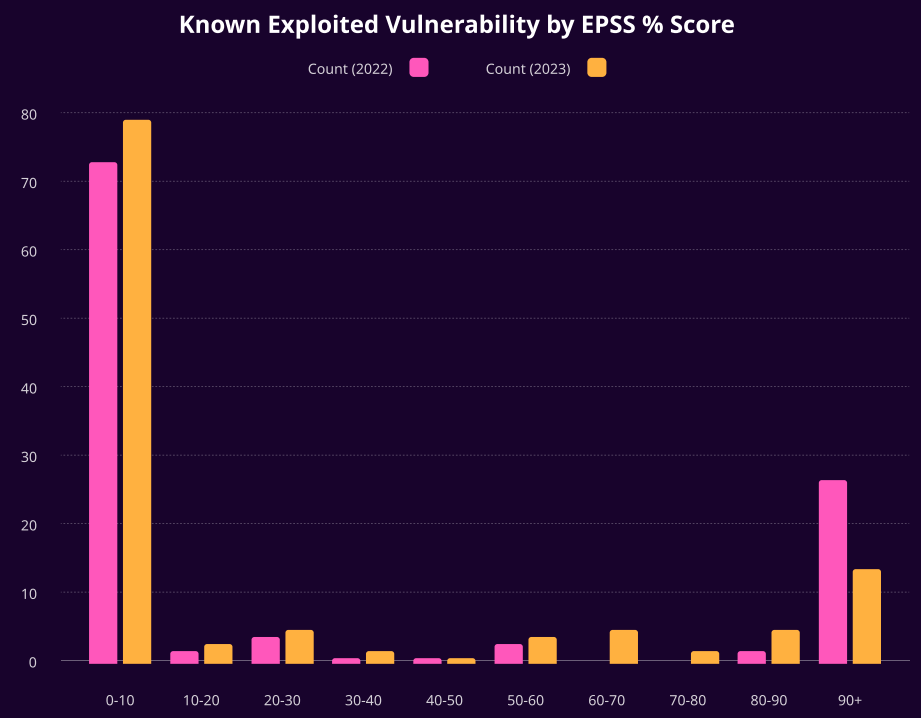
CVSS scores highlight the potential impact, but real threats require evidence. **Known exploited vulnerabilities (KEVs)** have been used in the wild, guiding organizations to prioritize patching based on actual attacks, not just theoretical risk. Tracking KEVs, gathered from diverse sources, is crucial for focused security efforts against immediate dangers.



Source: CVEdetails

Out of 29,065 reported vulnerabilities in 2023, only 129 (less than 1%) are confirmed as **known exploited vulnerabilities (KEVs)**. A concerning trend emerges: Over 108 CVEs out of 129 KEVs, nearly 84%, fall into the high-critical severity zone (CVSS above 7), starkly contrasting with the low-severity zone. High-severity vulnerabilities saw a notable increase, with 38 in the 7-8 range and 34 in the 9-10 range.

Comparing the trends between 2022 and 2023 reveals intriguing insights. The medium-high (5-6) CVSS range witnessed a dramatic 50% increase in KEVs, rising from 6 in 2022 to 9 in 2023. Meanwhile, KEVs in the high (7-8) and critical (8-9) ranges remained relatively stable at 38 and 29, respectively. However, the number of KEVs with the highest essential (10) CVSS score slightly decreased from 19 in 2022 to 7 in 2023. Despite this dip, vigilance remains crucial as these vulnerabilities pose a significant threat. In 2022, attackers primarily targeted high and critical vulnerabilities, leaving lower ranges untouched. Overall, the number of exploited vulnerabilities was slightly higher in 2023 (129) compared to 2022 (115).

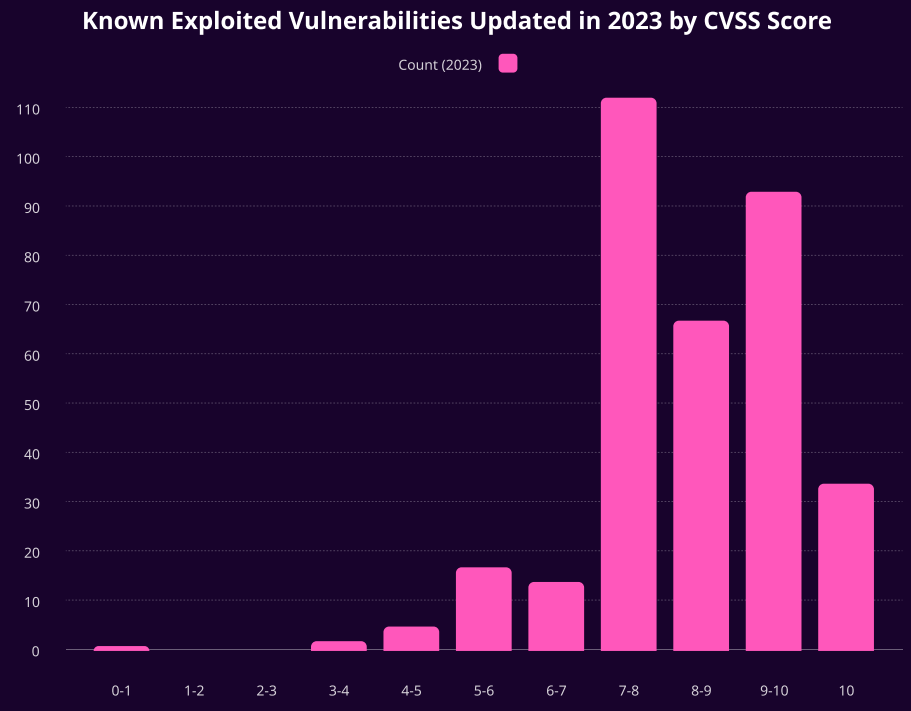


Source: CVEdetails

The **EPSS (Exploit Prediction Scoring System)** score evaluates the likelihood of exploiting a vulnerability. It's a metric used to gauge the vulnerability's susceptibility to exploitation based on various factors.

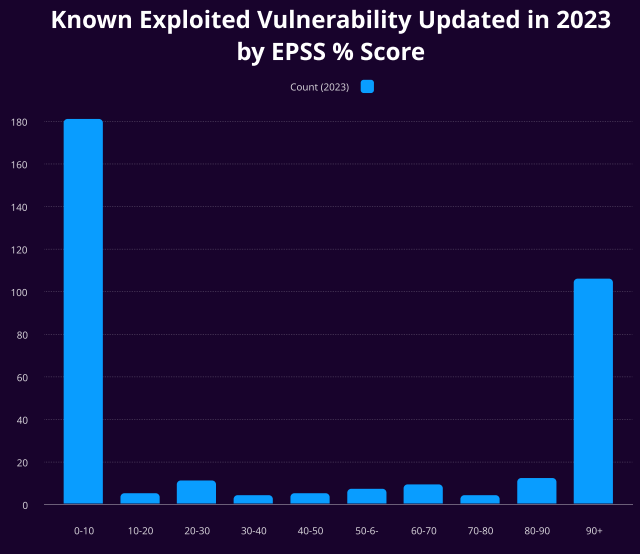
The **landscape of 2023's exploited vulnerabilities** paints a concerning picture when viewed through Exploit Prediction Scoring System (EPSS) scores. While **most of the CVE (61%) were deemed unlikely to be exploited (EPSS 0-10%)**, a disturbing **nearly 19% CVE lurked in the highest exploitation probability range (EPSS above 90%)**. Almost one in five known exploited vulnerabilities posed a **grave immediate threat** requiring urgent patching and mitigation.

Comparing the 2022 and 2023 data, we see a mixed bag of trends across the different EPSS ranges. In the highest EPSS range (90+), there was a significant decrease in vulnerabilities from 37 in 2022 to 24 in 2023, a drop of over 10%. This positive trend suggests that fewer high-risk vulnerabilities are being exploited. In the lowest EPSS range (0-10), we saw a slight vulnerability increase from 73 in 2022 to 79 in 2023. This is not a significant concern, as these vulnerabilities are unlikely to be exploited. For the remaining, there were relatively minor changes.



Source: CVEdetails

While 2023 witnessed updates across the full spectrum of known exploited vulnerabilities, a chilling majority lurks in the shadows of high-to-critical severity. Nearly 89% huddle within the 7-10 CVSS range, with 111 alone occupying the high-severity 7-8 band. These potent threats demand immediate attention and mitigation, lest they exploit existing systems. The remaining 12% paint a less alarming picture, occupying lower severity tiers. While vigilance is still crucial, addressing these threats allows for a more measured approach to patching and mitigation.



Source: CVEdetails

Known Exploited Vulnerability Updated in 2023 by EPSS Score

This section presents statistical data following updates to CVEs once they have been assigned.

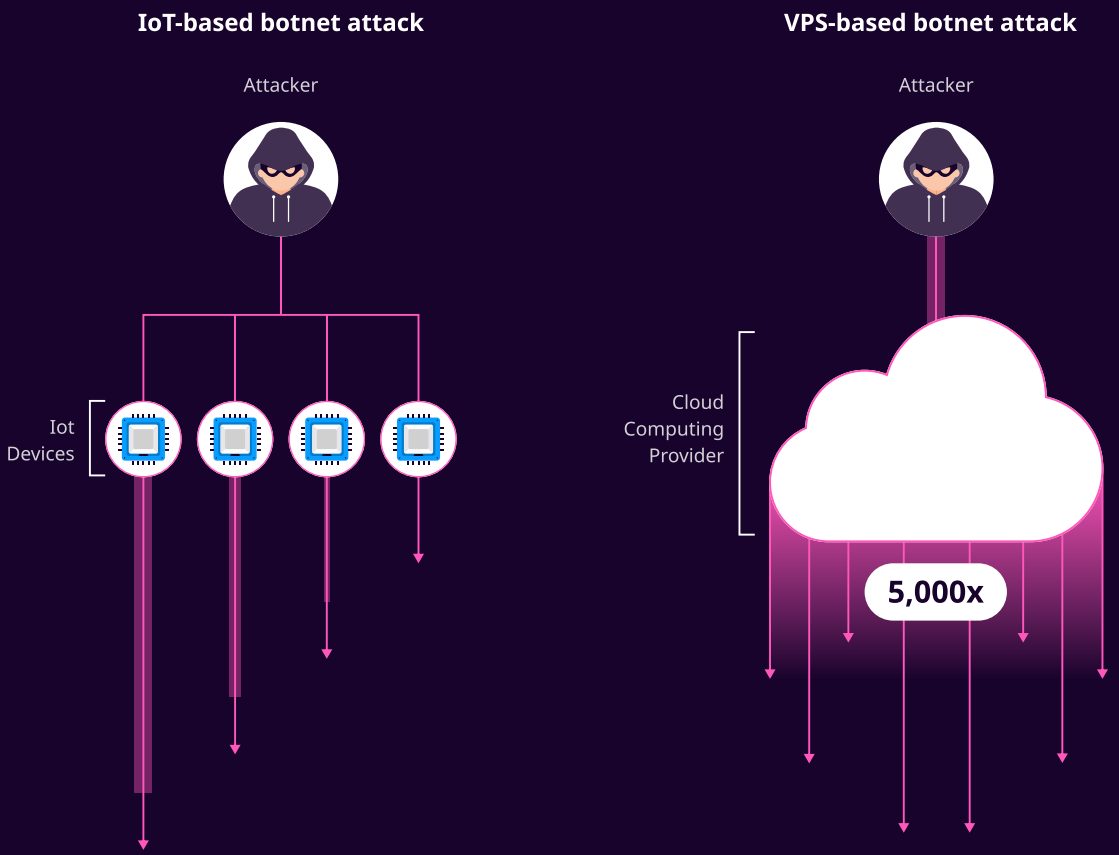
While a reassuring 53% (181 vulnerabilities) slumber in the low-exploitation zones (0-10% EPSS), a chilling 31% (106 vulnerabilities) lurk in the shadows of near-certain exploitation (above 90% EPSS). Adding to the concern, another 35% (122 vulnerabilities) hover in the high-probability range (above 70% EPSS), signifying their significant susceptibility to exploitation. Only the remaining 18% reside in the moderate zone (10-70% EPSS), presenting a somewhat lower, yet still present, risk.

DDoS

DDoS (Distributed Denial-of-Service) attacks are malicious connection attempts from multiple systems across the world to flood a website and render it unavailable to legitimate users. DDoS leads to revenue loss due to website downtime, operational disruptions, and customer churn. It also tarnishes the brand image and degrades customer trust.

2023 observed massive DDoS traffic volumes, exceeding previous records. Hacktivist groups and cybercriminals are increasingly launching targeted attacks against specific industries, such as cryptocurrency companies, non-profit organizations, and broadcast media. DNS-based attacks are becoming more popular, as they can be difficult to mitigate and amplify attack traffic. Ransom DDoS attacks are relatively more straightforward for adversaries to conduct and are on the rise. UDP laundering has also become a stealthy weapon of choice for attackers. This technique cloaks harmful traffic within the innocent guise of regular UDP datagrams, making it a nightmare to identify and filter out. The expertise requirement is relatively lower, and only the knowledge of IP/URL would suffice. Attackers are seen to threaten or attack the victims mostly on special occasions like Black Friday, Thanksgiving, and such days where the damage to victims would be more significant.

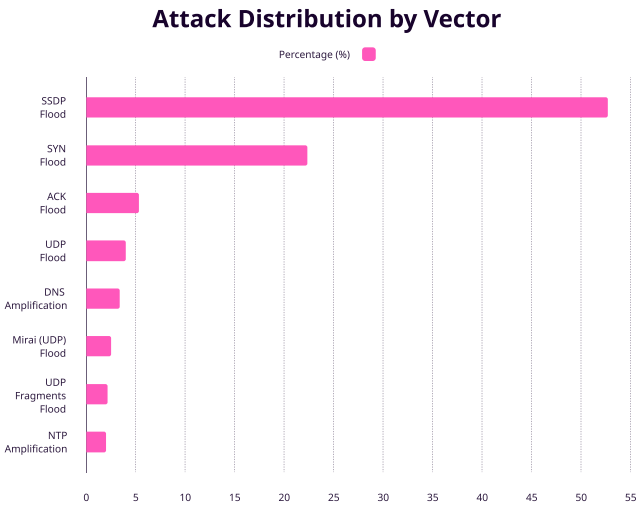
Hyper-volumetric attacks are on the rise that leverages a new generation of botnets comprised of Virtual Private Servers (VPS) instead of Internet of Things (IoT) devices, which can be as much as **5000 times** stronger than the traditional botnets comprised of IoT devices.



Source: Cloudflare

Here are some important aspects of 2023:

1. Attackers are leveraging powerful botnets to launch massive attacks, exceeding previous records. According to Cloudfare, 2023 saw DDoS attack peaking 201 million requests per second.
2. Hacktivist groups and cyber criminals are increasingly focusing on specific industries. Cryptocurrency companies saw a 600% rise in attacks, while non-profit organizations and broadcast media were also targeted. Gaming and gambling industries are also the top targets of attackers.
3. Deliberately engineered and targeted DNS attacks are becoming more common, making them harder to mitigate.
4. Affordable DDoS-for-hire services through underground marketplaces facilitated attacks even for less technical individuals or groups with malicious intent. This democratized access to DDoS capabilities posed a significant threat to smaller businesses and individuals lacking robust security measures.



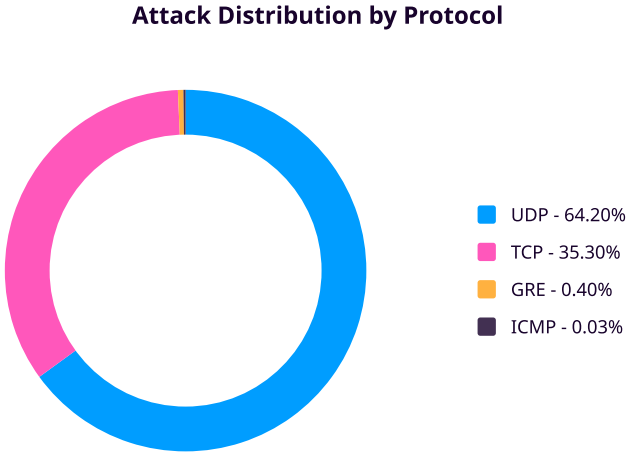
Source: Cloudflare Radar

Attack distribution by Vector

Among the multiple vectors used for the Network layer attacks, SSDP Flood, SYN Flood, ACK Flood, and UDP Flood dominate the top 4 positions - constituting a staggering 85.65% of all attacks globally. SSDP Flood reigns supreme, claiming a whopping 53.25% of the pie, while SYN Flood and ACK Flood take sizable bites with 22.32% and 5.93%, respectively. UDP Flood follows at a slightly smaller distance with 4.15%.

Network Layer attacks distribution by Protocol

2023 shows the dominance of **UDP (User Datagram Protocol)** in network layer attacks, accounting for a whopping **64.2%** of the total. Following it, the **TCP (Transmission Control Protocol)** trails behind at **35.3%**. Unlike TCP, UDP is connectionless, making it significantly faster and more efficient for sending large data bursts. **GRE (Generic Routing Encapsulation)** protocol encapsulates other protocols within itself, potentially adding another layer of complexity to attack analysis. Its low representation of **0.4%** might indicate specialized use cases for DDoS attacks. The minimal presence of **ICMP (Internet Control Message Protocol 0.03%** could be due to its relative inefficiency compared to UDP floods.



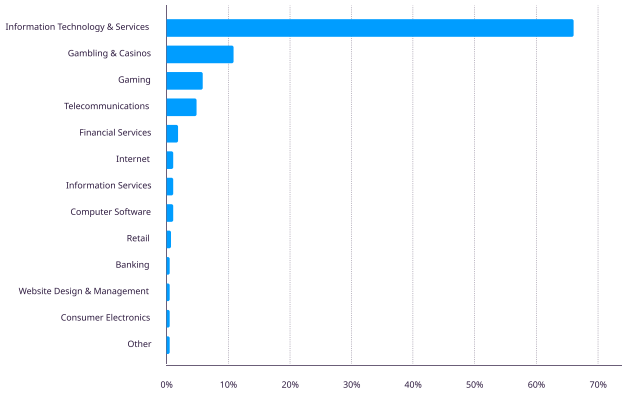
Source: Cloudfare Radar

Network Layer attacks distribution by Industry

Information Technology and Services (IT&S) takes the lead in attracting DDoS attacks, grabbing **66.82%** of the assault pie. This hefty slice is no surprise, considering IT&S handles sensitive data and critical infrastructure, making it a prime target for disruption. Chasing after IT&S at a distant second is **Gambling & Casinos** with **11.36%**. Rounding out the top three is **Gaming** with **6.42%**. Its reliance on online connectivity and competitive nature make it another lucrative target for malicious actors.

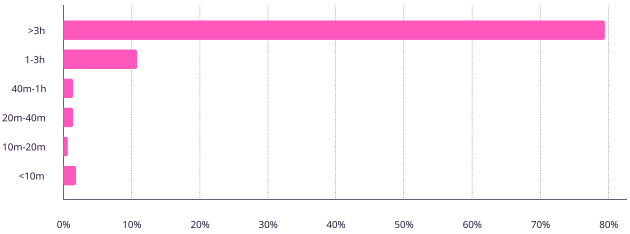
These three industries combined account for a colossal **84.6%** of DDoS attacks, highlighting a concentrated focus on sectors heavily reliant on online services and vulnerable to significant disruptions.

Network Layer attacks distribution by Industry



Source: Cloudfare Radar

Network Layer attacks distribution by Duration



Source: Cloudfare Radar

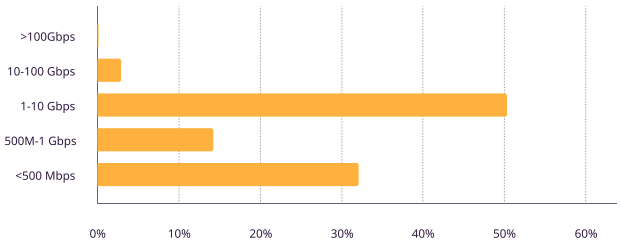
Network Layer attacks distribution by Duration

Almost **80% of attacks extend beyond 3 hours**, depicting persistent, long-term assaults to inflict maximum damage. **11% of attacks lasted 1-3 hours**, showcasing a blend of duration and intensity. However, only **9%** of the attacks were short bursts. Among these, almost **3%** lasted for less than 10 minutes.

Network Layer attacks distribution by Bit rate

DDoS attacks unleash data deluges of varying sizes, aiming to drown online targets. A **miniscule 0.008%** unleashes **digital tsunamis exceeding 100 Gbps**, threatening even the mightiest infrastructure. **3.1%** are **powerful attacks** between 10-100 Gbps, causing widespread mayhem. The **vast majority (50.66%)** are **persistent** in the 1-10 Gbps range, flooding smaller targets over time. Smaller deluges of 500 Mbps-1 Gbps (13.73%) and under 500 Mbps (32.5%) act like **relatively more minor attacks seemingly harmless.**

Network Layer attacks distribution by Bit rate

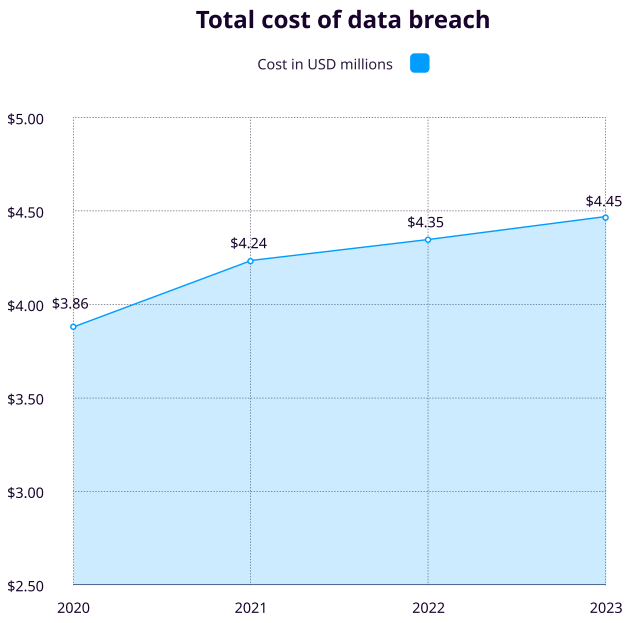


Source: Cloudflare Radar

Data Breach

Data breaches are no longer a silent threat lurking in the shadows. In 2023, they've become a global headline-grabbing reality, exposing millions of records and posing a significant threat to individuals and businesses. Critical infrastructure sectors like healthcare, finance, and energy face higher-than-average data breach costs, i.e., an average cost of **$5 million per breach**, significantly higher than other industries. Unlike others, these breaches have more severe financial consequences.

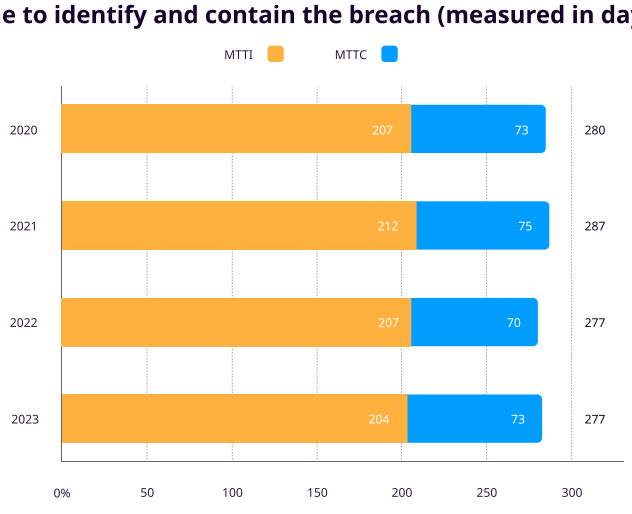
Over half of organizations increase their security investments following a breach, recognizing the importance of beefing up defenses.



Source: IBM

IBM's "**Cost of Data Breach**" report highlights an escalating trend in the average cost of data breaches, reaching a peak of $4.45 million in 2023, a record-breaking figure. This surge reflects a consistent upward trajectory in breach-related expenses over four years. Here are some of the highlights from the report:

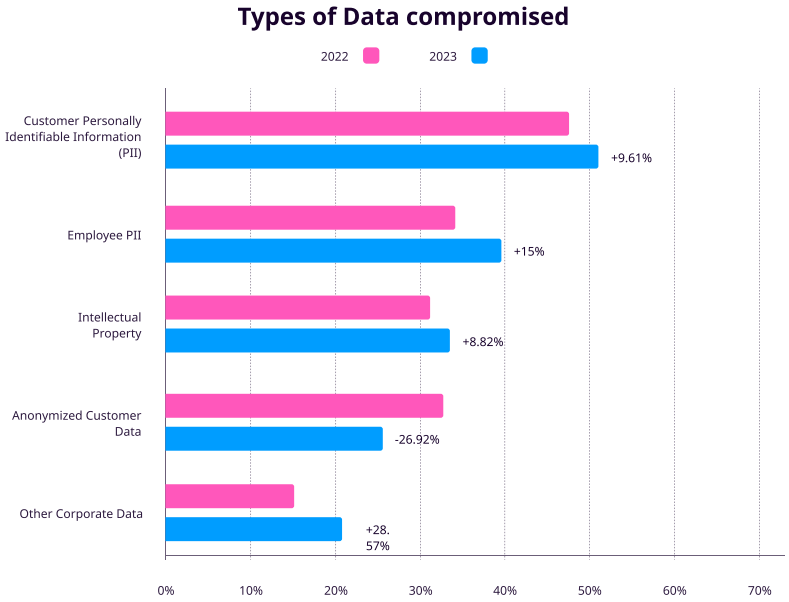
1. It takes an average of 277 days for organizations to detect and contain a data breach, showcasing the time lapse from intrusion to resolution.
2. **Organizations with tailored automated response playbooks for ransomware neutralized threats 16% faster, resolving attacks in only 68 days compared to an average of 80 days.** Utilization of security AI and automation techniques can detect and contain breaches a remarkable 108 days faster.
3. Software supply chain attacks contribute to 12% of data breaches, highlighting this as a significant threat source.
4. Incorporating threat intelligence into security measures results in breaches being identified 28 days earlier, highlighting the significant acceleration in breach detection through this method.
5. Organizations equipped with an Incident Response (IR) team and regularly tested IR plans detect breaches 54 days earlier than those lacking these preparations.



Source: IBM

Often, attackers infiltrate our systems unnoticed, lurking in the shadows while we remain unaware of their presence. They silently navigate our networks, probing vulnerabilities and potentially accessing sensitive data or compromising security. This lack of visibility into their activities within our systems underscores a critical challenge in cybersecurity: the time taken to detect and contain these breaches.

Organizations have undergone a gradual shift in their response times to breaches. In 2020, the average time to identify a violation stood at 207 days. However, in 2021, this duration slightly increased to 212 days before dropping back to 207 days in 2022. Encouragingly, 2023 marked a decrease to 204 days, continuing the downward trend. Conversely, the containment duration was reported at 73 days initially, spiked to 75 days in 2021, and then dropped to 70 days in 2022, signifying a fluctuating pattern. However, there was a subsequent increase to 73 days in 2023, hinting at a potential upward trend in breach containment. Overall, while the time to identify and contain breaches remained consistent in 2022 and 2023, there were notable fluctuations in these durations across the four years.

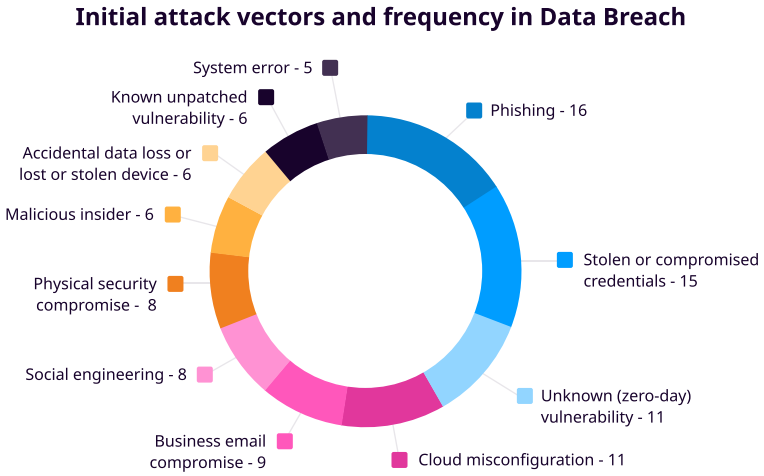


Source: IBM

Across various data breach categories in 2023, a discernible trend emerged. Customer Personally Identifiable Information (PII) breaches surged from 47% in 2022 to 52% in 2023, marking a significant 9.61% increase. Similarly, Employee PII breaches climbed notably from 34% to 40%, representing a 15% rise. Intellectual Property breaches experienced a modest uptick from 31% to 34%, reflecting an 8.82% increase. In contrast, breaches linked to Anonymized Customer Data witnessed a considerable decline, dropping from 33% in 2022 to 26% in 2023, signifying a substantial decrease of 26.92%. This reduction might represent enhanced security measures or improved anonymization techniques organizations adopt. Conversely, breaches related to Other Corporate Data surged from 15% to 21%, indicating a notable 28.57% increase.

Initial attack vectors and frequency in Data Breach

Data breaches' frequency and associated costs vary significantly across different initial access vectors. Phishing attacks have the highest occurrence, constituting 16% of breaches and carrying a substantial cost of **$4.76 million**, showcasing their prevalence and significant financial impact. Malicious insider breaches, representing 6% of incidents, incurred the highest price at $4.90 million, underscoring their financial implications despite a lower frequency. Stolen or compromised credentials, accounting for 15% of breaches, incurred costs of **$4.62 million**, highlighting their substantial role in breach occurrences and their financial implications.



Source: IBM

LOGPOINT COVERAGE

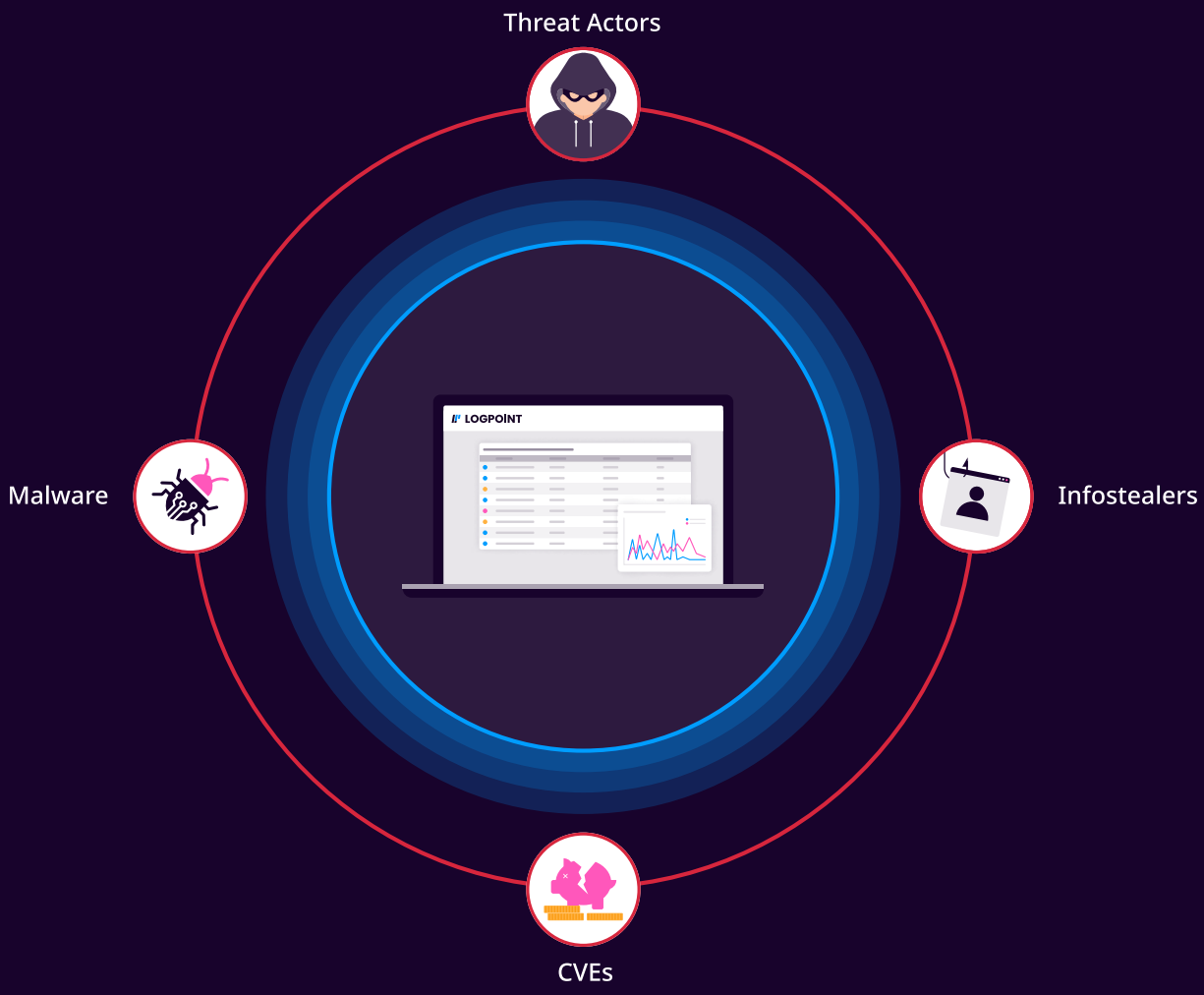
What Logpoint Uncovered in Global Security 2023?

In 2023, Logpoint Security Research extensively addressed various threats, exploring emerging techniques employed by threat actors across multiple domains. The comprehensive analysis covered a spectrum of malware families, including Coin-Miners, InfoStealers, Loader Malware, and Ransomware. Furthermore, the investigations delved into numerous instances where critical vulnerabilities (CVEs) were exploited on a large scale, along with incidents related to supply chain attacks.

We also delved into additional techniques exploited by threat actors, not mentioned in the sections below. We specifically address a technique used at an alarming rate for phishing, namely **Quishing.** Another noteworthy method is HTML Smuggling, already described in this report in the initial access payload section. Additionally, there was a guidance blog related to **Detecting and Responding to Compromises in Azure AD through AAD Connect.** We also furnished guidelines for the detection and automatic response to malicious **OneNote attachments**.

The list of covered contents and relative blog references are below.

The covered contents are organized into distinct categories to enhance comprehension, and they are as follows:



CVE

CVE-2023-23397

The security flaw There had been back and forth between the AlphV team hosting the new leak site and the Federal organizations taking over them. However, the affiliates continue to attack organizations and look for alternating leak sites to host data. CVE-2023-23397, discovered in Microsoft Outlook, allows unauthorized NTLM credential theft when exploited. It's important to note that Outlook on the web and Microsoft 365 remained immune to this exploit since they do not support NTLM authentication. This vulnerability is exploited through zero-click attacks, wherein adversaries craft malicious emails to exploit the identified weakness.

CVE-2023-29059

It designates a vulnerability within the 3CX DesktopApp, where a malicious backdoor has been clandestinely inserted into its code, suspected to be the work of North Korean threat actors. Notably, this security concern affects versions 18.12.407 and 18.12.416 of the Windows 3CX DesktopApp and DesktopApp Electron for macOS application with versions 18.11.1213, 18.12.402, 18.12.407, and 18.12.416.

MoveIT zero Day

Multiple vulnerabilities in MOVEit Transfer tracked as **CVE-2023-34362**, **CVE-2023-35036**, and **CVE-2023-35708** were found, which, when chained for exploitation, grant unauthorized access to the system and aid the escalation of privileges. The Clop Group was behind the active exploitation of this vulnerability.

CVE-2023-28252

It is a privilege escalation vulnerability present in the Common Log File System. Specifically, it is identified as an out-of-bounds write (increment) vulnerability, exploitable during attempts to extend a metadata block within the system. According to **Kaspersky**, this vulnerability is exploited by manipulating a base log file. Following the successful exploitation, which grants system privileges, threat actors have been observed deploying the Nokoyawa Ransomware.

CVE-2023-27350

PaperCut, a widely used print management software, was vulnerable to a critical exploit, CVE-2023-27350, with a CVSS score of 9.8. This vulnerability allows threat actors to execute arbitrary code (RCE) remotely. Another high-severity vulnerability, CVE-2023–27351, with a CVSS score of 8.2, has been reported in PaperCut products. Both CVEs were exploited by chaining authentication bypass vulnerability.

CVE-2023-36884

With a significant rating of 8.8, CVE-2023-36884 is identified as a high-severity Office and Windows HTML Remote Code Execution Vulnerability. Storm-0978 has exploited this vulnerability to orchestrate a targeted phishing campaign, focusing on individuals and countries supporting Ukraine.

CVE-2023-38831

It is an arbitrary code execution vulnerability on WinRAR, having a CVSS score of 7.8. The exploitation of this vulnerability occurs when extracting a ZIP archive using WinRAR, which includes both a harmless file and a folder sharing the identical name as the benign file. When WinRAR attempts to remove the soft file, a bug in the WinRar causes the files inside the folder to be executed.

CVE-2023-42793

CISA, in collaboration with international partners, has detected cyber actors affiliated with the Russian Foreign Intelligence Service (SVR) exploiting CVE-2023-42793. This vulnerability enables an unauthenticated malicious actor to remotely execute arbitrary code on the TeamCity server and has a CVSS score of 9.8.

CVE-2022-42475

A critical vulnerability was detected in FortiOS SSL-VPN in December 2022, a heap-based buffer overflow issue identified as CVE-2022-42475 with a CVSS score of 9.4. Chinese APTs took advantage of this flaw in January 2023. They were found exploiting it by using their specially crafted malware, tracked as BOLD MOVE, to control the vulnerability in FortiOS SSL-VPN.

OWASSRF

OWASSRF combines CVE-2022-41080 and CVE-2022-41082, enabling attackers to attain remote code execution (RCE) through Outlook Web Access (OWA). Similar to ProxyNotShell, OWASSRF utilizes SSRF for exploitation. The key distinction lies in the exploitation strategy. While ProxyNotShell leveraged the AutoDiscover endpoint for CVE-2022-41040, OWASSRF employs the OWA frontend endpoint to exploit CVE-2022-41080. Play ransomware groups were detected exploiting this vulnerability.

MOVEIt

MOVEIt is a Managed File Transfer(MFT) from Progress Software. This is the second MFT service provider targeted by Clop this year. Multiple vulnerabilities in MOVEit Transfer were discovered and, when exploited, granted unauthorized access to the system. By chaining the bugs, adversaries achieved code execution with local administrator privileges, using the relevant service's privileges. **Clop** orchestrated this attack, with the initial exploitation attempt dating back to July 2021. In 2023, the exploitation continued, starting as early as May 27th. According to **Konbriefing**, about 2602 organizations had been the victims of supply chain attacks, and the number of impacted individuals whose data were exfiltrated is tremendously high, i.e., between 78 and 83 million. Some of the victim organizations were managed service providers. As a result, threat actors could gain access to the multiple organizations that the MSP was working with. From data taken from **emisoft**, the top 5 most impacted invidious were from the following organizations.

Organization	Individuals Affected Count
Maximus	11.3 million
Welltok	8.4 million
Louisiana Office of Motor Vehicles	6 million
Alogent	4.5 million
Colorado Department of Health Care Policy and Financing	4 million

InfoStealers

AgentTesla

Initially identified as a remote administrator tool written in the .NET framework, AgentTesla has evolved significantly since its establishment in 2014. It has expanded its capabilities, becoming an Info Stealer and securing a position in the top 10 list on MalwareBazaar as of December 2023. AgentTesla can harvest data from multiple applications, such as mail clients, browsers, and local files.

Redline Stealer

RedLine Stealer, as its name suggests, is an InfoStealer that was **first seen around March 2020**. It is a powerful data collection tool capable of extracting login credentials from various sources, including web browsers, FTP clients, email apps, Steam, instant messaging clients, and VPNs. It can collect data from browsers, chat logs, local files, and cryptocurrency wallet databases. Besides, it can collect information regarding the victim's systems.

Ransomware and Threat Actors

Royal Ransomware

First seen in January 2022, there are at least 211 confirmed victims of the Royal group. Besides phishing, the group uses Google ads to guide users to forums, posts, and blog comments to make victims download and execute the payload. They also used "Callback" phishing, a similar technique the Conti leveraged.

Hive Ransomware

Discovered in June 2021, Hive is ransomware that operates on the Ransomware-as-a-Service model. The FBI, CISA, and HHS revealed that the Hive group and its affiliates targeted over 1,300 businesses worldwide. They managed to secure nearly $100 million in ransom before collaborative efforts led to the seizure of their servers in January 2023.

Play ransomware

Emerging in June 2022, Play ransomware remains active, targeting high-profile victims. The Name Play was given as it appends the ".PLAY" extension to a file after encryption. Employing Big Game Hunting tactics, it predominantly focuses on organizations with substantial revenue. As of December, it ranks among the top 10 groups with the most victims every month. They bypassed ProxyNotShell mitigations by exploiting OWASSRF vulnerability to gain initial access.

Gamaredon

Starting its operations in June 2013, Gamaredon has conducted numerous cyberattacks against Ukraine, targeting government services and critical infrastructure. The group aims to pilfer sensitive information and disrupt the country's operations. Gamaredon was detected employing info-stealer malware known as GammaLoad and GammaSteel. These custom-made malware variants act as information-stealing implants capable of exfiltrating specific file types, capturing user credentials, and taking screenshots of the victim's computer.

EsxiArgs Ransomware

A ransomware campaign was started by threat actors that targeted the VMware ESXi hypervisor, which exploited a relatively old vulnerability in ESXi tracked as CVE-2021-21974. After exploiting those vulnerabilities to gain access, threat actors deployed a customized ransomware payload, tracked as EsxiArgs Ransomware. The encryption was deployed on more than 120 ESXi servers.

Nokoyawa Ransomware

Nokoyawa ransomware surfaced in March 2022, focusing on Windows environments and exhibiting notable similarities in its attack chain with Hive. Threat actors were observed exploiting CVE-2023-28252 to elevate privileges on Microsoft Windows servers associated with small and medium-sized enterprises and deploying Nokoyawa ransomware.

Vice Society

The group primarily directs its efforts toward educational institutions, notably impacting one of the biggest school systems, the Los Angeles Unified School District, an entity that oversees many schools. Unlike many others, Vice Society employs various malware families for encryption. Their activities paused around July 2023, but there are suspicions that they have rebranded themselves as a new threat group called Rhysida.

BianLian

Bianlian stands out as one of the top 10 ransomware groups in 2023. Since its emergence in June 2022, it has targeted a significant number of victims, reaching a total of 350 known cases. The group is notorious for exploiting vulnerabilities in Remote Desktop Protocol (RDP) and Virtual Private Network (VPN) systems for initial access to targeted systems. Additionally, Bianlian employs storage service providers like Mega to exfiltrate data from their victims.

Lockbit Ransomware

LockBit functions on the Ransomware-as-a-Service (RaaS) model, making it the preferred option for threat actors seeking to unleash ransomware. In 2022, LockBit claimed the title of the most widely deployed ransomware variant globally, and it continues to maintain its prominence in 2023. This enduring presence is attributed to a substantial number of affiliates and the decline of its competitors.

8base Ransomware

8base Group is another group from our list that earned a spot on the top 10 ransomware groups in 2023, with a tally of at least 280 known victims recorded until December. The group initiated its activities in March 2022. However, it was not until May 2023 that a notable surge in group operations became apparent. Since then, the 8base group has maintained an active presence, consistently mentioning their victims on their leak site.

Akira Group

Emerging in March 2023, the Akira group swiftly ascended to become one of the leading ransomware groups this year. By August of the same year, they were actively exploiting a vulnerability in Cisco ASA VPNs, recognized as CVE-2023-20269. This exploit granted them unauthorized access to the network.

APT-29

APT-29, a.k.a The Dukes, Cozy Bear, or Nobelium, is a prominent cyber espionage group linked to Russia's Foreign Intelligence Service (SVR). APT-29 is known to use the HTML Smuggling technique and ISO images to deliver their payload initially. APT-29 was behind one of the biggest supply chain attacks, i.e., the SolarWinds supply-chain attack in 2020. They are also known for conducting sophisticated and cyber espionage activities against governments and non-governmental organizations, businesses, think tanks, and other high-profile targets.

Cactus

The Cactus ransomware campaign has been active since March, focusing on big game hunting. They are known to exploit vulnerabilities in VPN appliances and public-facing applications and perform malvertising to gain initial access. They are known to deploy a batch script that executes 7-zip to extract the ransomware binary and deletes the artifacts before executing the payload.

Rhysida

Rhysida is a newly emerged ransomware group that surfaced in May 2023, operating on a Ransomware-as-a-Service model. Several reports have presented evidence of the infamous ViceSociety group transitioning into Rhysida. Since May, they have displayed data from 78 known victims on their leak site.

Other Malware Families

Crypto-Miners

Crypto miners are malware designed to hijack a computer's processing power to mine cryptocurrency, such as Bitcoin or Monero. Once deployed, they use the infected system's resources to perform complex mathematical calculations to solve a blockchain puzzle and earn cryptocurrency for the attacker. This process consumes significant computational resources, leading to system slowdowns and increased energy consumption for the victim.

Snake Malware

Snake, previously known as "Uroburos," stands out as an advanced cyber-espionage tool crafted by the Ryazan-based FSB group "Turla" for sustained intelligence gathering on high-value targets. This sophisticated malware, active since 2004, exhibits stealth and modularity, enabling it to operate covertly in networks. Snake employs custom communication protocols with encryption and fragmentation techniques to enhance security and avoid detection. Its internal technical architecture allows the integration of new components effortlessly, ensuring smooth interoperability across various host operating systems like Windows, MacOS, and Linux.

LOGPOINT ANALYTICS

Alerts Coverage for 2023

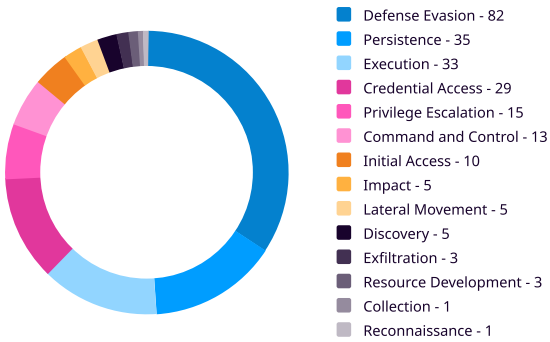
We have dedicated ourselves to creating, updating, and maintaining analytics throughout the year. In terms of alerts, we have incorporated numerous distinctive detection rules. Below are the statistics for the alerts we have added and updated.

Total Alerts added: 228

Total alerts updated: 274

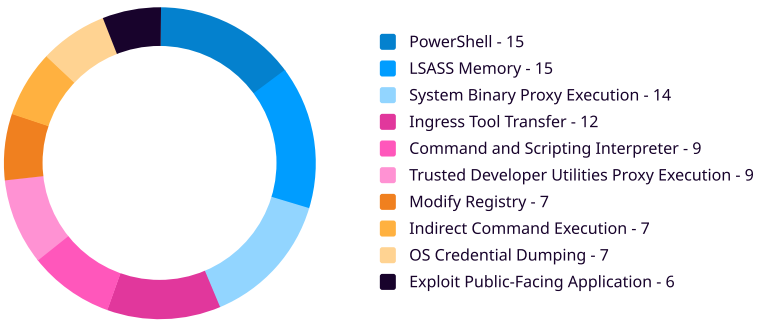
Stats on Newly Added Windows Alerts

New Alerts' Tactics Coverage



Adversaries emphasize defense evasion, employing various strategies to achieve their objectives. It is logical for the highest number of our created alerts to fall under this tactic. Subsequently followed by Execution, Persistence, Credential Access, Privilege Escalation, Command and Control, Initial Access, Impact, Lateral Movement, Discovery, Exfiltration, Resource Development, Collection, and Reconnaissance.

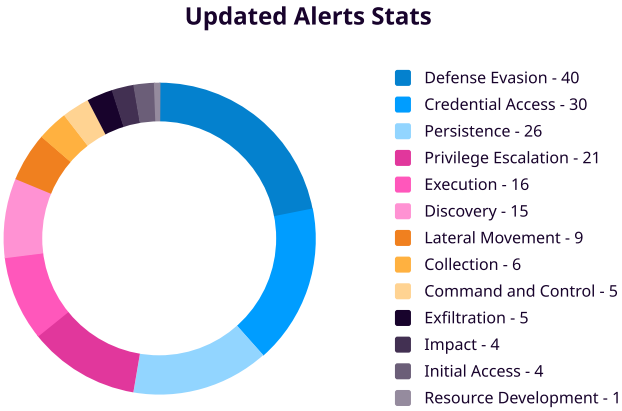
New Alerts' Top 10 Technique Coverage



Among various techniques, most of the newly created alerts fall under PowerShell as it is the most frequently utilized for execution and defense evasion. Following PowerShell, the list of top 10 techniques includes LSASS Memory, System Binary Proxy Execution, Ingress Tool Transfer, Command and Scripting Interpreter, Trusted Developer Utilities Proxy Execution, Modify Registry, Indirect Command Execution, OS Credential Dumping, and Exploit Public-Facing Application.

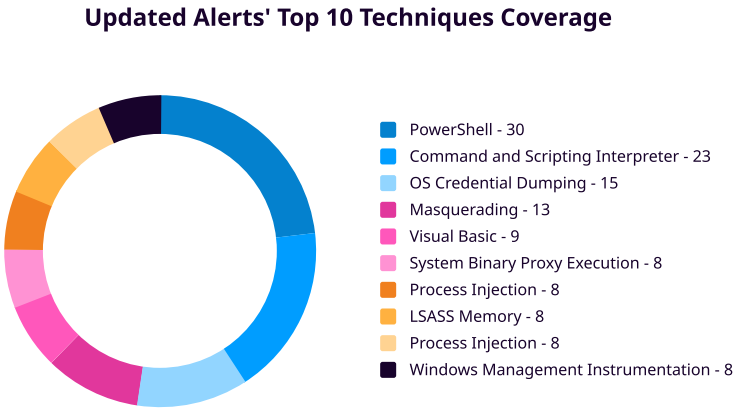
Updated Alerts Stats

Not only the addition of new alert rules but, for the improvement of detection we have also updated the existing alert rules making them even more reliable. Among these alert rules, the highest number of alert rules fall under Defense Evasion followed by Credential Access, Persistence, Privilege Escalation, Execution, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact, Initial Access, Resource Development.



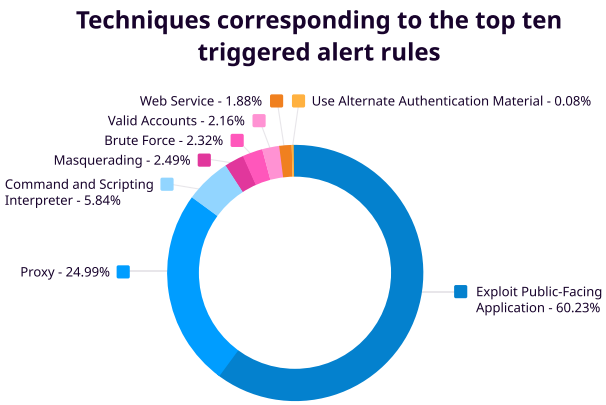
Updated Alerts' Top 10 Techniques Coverage

Again, most of the updated alerts fall under PowerShell techniques, followed by Command and Scripting Interpreter, OS Credential Dumping, Masquerading, Visual Basic, System Binary Proxy Execution, Process Injection, LSASS Memory, Process Injection, Windows Management Instrumentation in the top 10 list.



Top 10 Triggered Alert Rules

1. Default Possible SQL Injection Attack
2. Suspicious PowerShell Parameter Substring Detected
3. Default Blocked Inbound Traffic followed by Allowed Event
4. Possible Botnet Connection-Outbound Spam
5. Renamed Binary Detected
6. Default Brute Force Attack Attempt - Multiple Unique Sources
7. Mitre - Initial Access - Valid Accounts - Off Hour Logon
8. Threat Intel Connections with Suspicious Domains
9. Suspicious PowerShell Invocation Based on Parent Process
10. Possible Pass the Hash Activity Detected



Alert rules in Logpoint Converged SIEM are triggered to notify users whenever any significant events occur. It might be a suspicious activity or an abnormal activity that is happening within the organization. And so far in 2023, We have observed these above top ten alert rules that were triggered mostly. So, Looking at them, almost half of them were triggered due to proxy connection. We also observed that almost 14% of them were triggered due to the usage of command and script interpreters to execute suspicious commands, scripts, or binaries and that almost 7% of them were triggered due to some form of data manipulation like file overwrite.

LESSONS LEARNED

In the digital age, cyberattacks are a severe threat to scale organizations. In 2023, we witnessed various devastating and sophisticated cyberattacks affecting multiple industries and organizations, including governments, businesses, hospitals, and media outlets. Some of the learning after reflection of 2023 cybersecurity trends are:

- **Ransomware is still a significant challenge**: Ransomware is malware that encrypts the victim's data and demands ransom for its decryption. Ransomware attacks have increased in frequency and severity in 2023. Adopting Multiple Extortion techniques by ransomware has made them even more disastrous and successful. Some notable ransomware attacks in 2023 include **The Guardian Cyber Attack**, **Toronto SickKids**, and **Kaseya**. These attacks have caused not only financial damage but also reputation loss. Organizations must implement robust backup and recovery strategies to prevent or mitigate ransomware attacks, educate employees on spotting phishing emails and malicious attachments, and avoid paying for ransomware.
- **Nation-state actors are becoming more aggressive**: Nation-state actors are hackers supported by governments who engage in cyberattacks for political or strategic reasons. In 2023, we witnessed increased cyber warfare between countries like Russia and Ukraine, North Korea, and South Korea. These attacks targeted critical systems, stole important information, spread false information, and tried to influence people's thoughts. Nation-state actors also use cyberattacks to help their friends or partners in conflicts worldwide. To stay safe, organizations should improve their cybersecurity, watch for strange activity on their networks, and work with others to share information and good security practices.
- **The complexity of Cloud security is becoming more challenging**: Cloud computing offers many benefits for organizations, such as scalability, flexibility, cost-efficiency, and innovation. However, cloud security also poses new challenges and risks for organizations that rely on cloud services or platforms. **In 2023, we saw an increase in cloud-based attacks that exploited vulnerabilities in cloud providers' systems or applications.**

PREDICTIONS FOR 2024

Cybersecurity is a dynamic and evolving field, and everything that happens in information technology and computer science directly affects the cybersecurity landscape. The rise of generative AI has caused ripples in various fields, including cybersecurity. Geopolitical reasons have also been significant stimuli for the cyber landscape since the internet has become a thing worldwide. In 2023, conflicts such as those between Ukraine-Russia and Israel-Hamas significantly shaped the cyberspace landscape. Cyberattacks influenced by geopolitical reasons will also be prominent in the coming years. Here are some of the predictions of the cybersecurity landscape, especially cyber-attacks, threat actors, attack vectors, strategies, malware, and ransomware in 2024.

Cybersecurity is a dynamic and evolving field. Every development in information technology and computer science directly impacts the cybersecurity landscape. Geopolitical factors have also been significant drivers of the cyber landscape ever since the advent of the internet. In 2023, conflicts such as those between Ukraine-Russia and Gaza-Hamas significantly shaped the cyberspace landscape. Cyberattacks influenced by geopolitical reasons will remain prominent in the coming years. Here are some predictions of the cybersecurity landscape in 2024, focusing on cyber-attacks, threat actors, attack vectors, strategies, malware, ransomware, and more:

- AI will revolutionize **everything and everyone — for better and for worse**. There's a higher chance of cyber attacks being more dangerous because threat actors will use smart AI tools to find weaknesses in important areas. With more AI tools around, there are more ways for cyber threats to happen, making systems easier to break into. To stay safe, companies must use AI to defend against these cyber threats.
- In 2024, session hijacking is expected to be a notable cyber threat as more organizations move to **passwordless access management from passwords to MFA**. However, some may still encounter data breaches due to weak password protections. The rise of passwordless authentication could lead to occasional credential theft when insecure backup options like passwords are used. Recognizing the complexity of current IT and security setups, many enterprises will likely streamline their technology through consolidation to simplify operations and enhance security.
- Malware and APT group activities will become more sophisticated and stealthy, using AI and ML to evade detection and analysis. They will also target more devices and platforms, such as mobile phones, smart home devices, IoT devices, cloud services, and web browsers. **They will also leverage zero-day exploits and supply chain attacks to compromise critical infrastructure and systems.**
- Ransomware will continue to be a major threat, with more groups launching new variants and campaigns. Ransomware will also use AI to generate more unique encryption keys, avoid detection by security tools, and extort victims with multiple extortion techniques. **Ransomware will also target more sectors and regions, such as healthcare, education, government, media, entertainment, gaming, finance, energy, transportation, manufacturing, retail, hospitality, and tourism.**
- Hacktivism will increase in frequency and intensity, using cyberattacks to expose corruption, injustice, human rights violations, environmental issues, and political agendas. Hacktivists will also use cyberattacks to disrupt or sabotage critical services or facilities that support their causes or enemies. **Hacktivists will also use cyberattacks to spread misinformation or propaganda through social media or deepfake technology.**
- Adversaries will target cloud systems to utilize their resources for malicious purposes. For example, **GPU farming** is a technique that uses GPUs (graphics processing units) to mine cryptocurrencies or perform other tasks in the cloud. As more businesses and services move to the cloud, it becomes a more attractive target for cybercriminals. They may seek to exploit vulnerabilities in cloud software, hijack user accounts, or use the cloud's computing power for their ends, such as cryptocurrency mining or launching further attacks.

- Gartner Inc., a prominent research and advisory firm for IT professionals and executives, reveals its top **eight cybersecurity predictions for 2023-2024**. These forecasts include half of CISOs adopting human-centric design practices in their cybersecurity programs; comprehensive privacy regulations covering the majority of consumer data; 10% of large enterprises implementing a thorough zero-trust program; ongoing national significance of election security; increased use of AI-driven security solutions for automated threat detection and incident response; widespread adoption of zero-trust architecture; the persistent threat of ransomware for many global organizations; and the growing sophistication and targeting of socially engineered tactics to deceive individuals into compromising their devices or personal information.
- Phishing attacks will become more sophisticated and targeted, using generative AI and large language models to create convincing and personalized messages that can bypass traditional security measures. **These attacks also leverage voice chatbots, VR/MR headsets, and QR codes to deliver malware or steal sensitive data.**
- As evident from the cases of MoveIt and Papercut, adversaries swiftly transitioned to data exfiltration after initial access. This implies that threat actors will likely exploit vulnerabilities to acquire remote access and promptly initiate data exfiltration, preceding the need for a ransomware attack.
- Adversaries find crypto exchange hacks very profitable, as the increasing numbers show. In 2021, around 3.3 billion worth of cryptocurrency was stolen. This number went up to over 3.8 billion in 2022 and then dropped to about **2 billion in 2023**. These trends indicate that crypto exchange breaches remain appealing to adversaries, posing an ongoing threat. It implies that attackers focus on these breaches for the big money they can make, making them a major target for cyberattacks compared to other areas.

CONCLUSION

In a landscape of ever-evolving threats, adversaries tirelessly innovate and come up with new ways to circumvent existing defenses. With every fix or mitigation, new evasion tactics emerge, showcasing the adaptability of threat actors. Vulnerabilities will endlessly be introduced in applications due to continuous revision of the existing code base, and some vulnerabilities remain concealed but only until adversaries or researchers discover them. Technology is ever-evolving, and with each evolution comes an opportunity for both defenders and attackers. The competition will remain perpetual among defenders and attackers. Many external factors such as geopolitical tensions and conflicts can fuel the rise of cyber attacks. The day for defenders to rest can hardly be imagined. So, Organizations must always keep up with the ever-evolving threat landscape, stay updated with the latest defensive methodologies, diligently monitor adversary activities in the wild, and fortify their defenses with robust, multi-layered strategies

At Logpoint, we remain vigilant look out for potential threats, and closely monitor emerging risks. Through proper dissection and thorough analysis in our labs, we continuously work on providing top-notch analytics and automated responses via the Logpoint Converged SIEM platform. We consistently and closely monitor emerging threats, update our analytics, or develop new ones to address novel techniques.

As customers and individuals, you can stay informed by staying up-to-date with our latest **blogposts** providing insights into the latest threats. These posts may include hunting and detection mechanisms, response strategies, and sometimes prevention techniques to help you stay safe and ahead in the game.

ABOUT LOGPOINT

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats.

By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats.

Logpoint offers SIEM, UEBA, and SOAR technologies in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more.

Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company.

For more information visit **www.logpoint.com**