



Q3-2023

Ransomware Report

October 2023





Table of Contents

Executive Summary	3
Quarterly Ransomware Outlook	6
Global Ransomware Threat Landscape	8
Microanalysis of Ransomware Activities	12
Ransomware Sectoral Impact	14
Weaponized Vulnerabilities of Q3-2023	16
Capricious Ransomware Techniques	18
Ransomware Threat Predictions	21
How to protect yourself from Ransomware Attacks	23
Cyble Vision – a Shield against Ransomware	25
References	26



Executive Summary

Cyble Research & Intelligence Labs (CRIL) closely monitors, tracks, and analyzes current and emerging ransomware threats across the globe. This report compendiously presents critical ransomware statistics and trends, major attacks, and common Tactics, Techniques, and Procedures (TTPs) observed in Q3-2023 to preempt the associated risks of the Ransomware Groups discussed herein.



This report encapsulates the following major findings from Q3-2023:

- **1,084** victims were publicly disclosed by ransomware groups, with United States (US) corporations continuing to be the most affected.
- Ransomware attacks have **doubled** on a Y-o-Y basis.
- The United Kingdom replaced Italy as the **second most** attacked country in this quarter.
- The majority of **high-income** organizations were targeted in the Professional Service, Construction, and IT & ITES sectors.
- The Healthcare sector witnessed **23% more** attacks in this quarter, to emerge amongst the most affected sectors.
- **LOCKBIT** claimed 5% fewer attacks compared to Q2-2023 but remained the most deplorable ransomware group, targeting 240 entities in Q3-2023.
- **8Base** emerged among the list of most active ransomware groups, with 84 listed victims in this quarter.
- The weaponization of vulnerabilities by ransomware groups reflects a shift towards Networking devices from previously observed exploitation of **Managed File Transfer** (MFT) applications.
- This quarter, we observed the emergence of **new ransomware groups** – Cactus, INC Ransom, Metaencryptor, ThreeAM, Knight, Cyclops Group, and MedusaLocker.



Total victims

1,084






Active Ransomware Groups

36 viz-a-viz 37 last quarter

Most Affected Countries (Top 5)

United States	530	▼ 7%
United Kingdom	67	-
Canada	46	▼ 18%
Germany	46	▼ 21%
France	37	▼ 8%

Most Active Ransomware Groups (Top 5)

				
LOCKBIT	CLOP	ALPHV	8Base	Play
240	174	96	84	62

Most Impacted Industry Sectors (Top 5)

Professional Services	150	▼ 19%	Construction	105	▼ 9%	IT & ITES	91	▼ 46%
Manufacturing	70	▼ 40%	Healthcare	96	▲ 23%			



Quarterly Ransomware Outlook

Cyble Research & Intelligence Labs identified 1084 ransomware victims in Q3-2023 compared to 1298 in Q2-2023 – a 16% decline. However, the attacks grew by 83% in this quarter as compared to Q1-2023 and doubled as compared to Q3-2022. This highlights the increasing menace of ransomware threats.



Our ransomware victim-to-country ratio data indicates that 60% of the victim organizations were primarily concentrated in 3 countries - **the United States (US), Italy, the United Kingdom (UK), and Canada.**

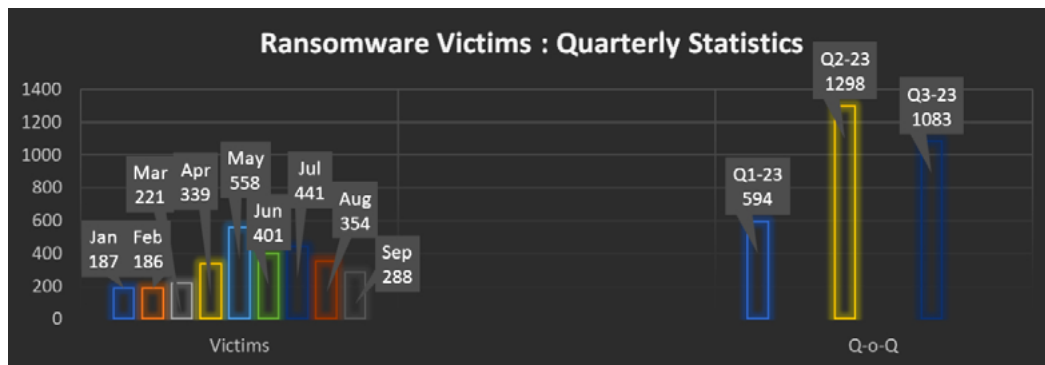
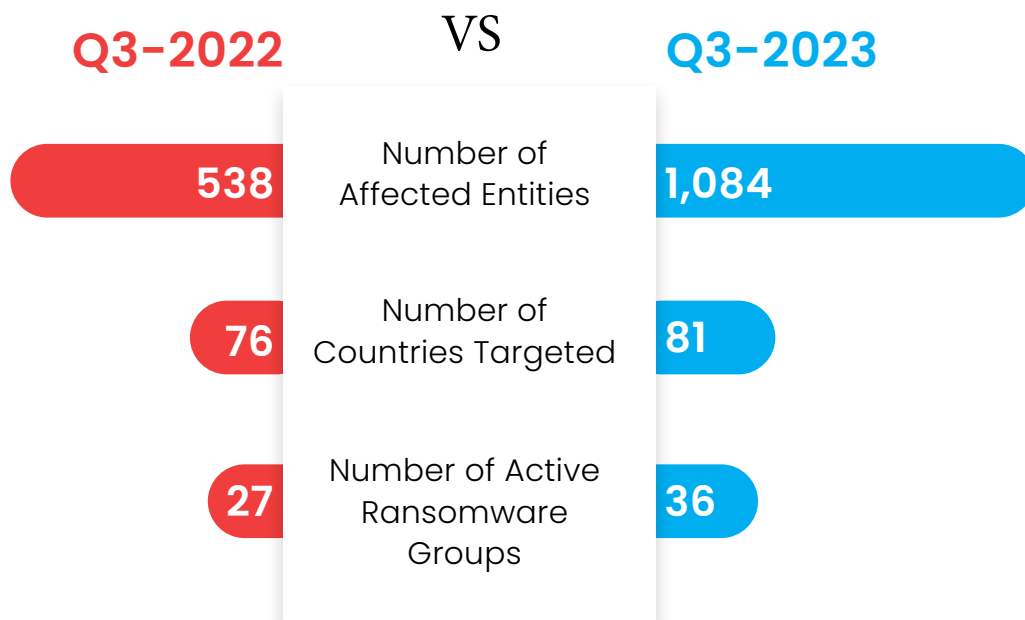


Figure 1: Comparative analysis of ransomware activities Q-over-Q

What has changed from Q2-2022 to Q2-2023?





Global Ransomware Threat Landscape

CRIL observed that the ransomware attack footprint decreased from **84 countries in Q2-2023** to **81 countries in the present quarter**.



The heightened vigor of these attacks against US entities has been an ongoing trend for the past few years and has persisted even in Q2-2023. Europe & CIS countries observed a significant spike of nearly 120% in ransomware attacks.



Figure 2: Global Distribution of Ransomware-Affected Organizations

Americas

The Americas was the most targeted region, with 624 ransomware victims this quarter, in contrast to 711 in Q2-2023. This region accounts for over 58% of ransomware victims disclosed publicly in Q3-2023. Canada was the second most targeted country in North America, while Mexico and Brazil were the most impacted countries in Latin America.



Ransomware attacks in the Americas have particularly impacted Professional Services. The BFSI sector has emerged among the 5 most affected sectors this quarter, besides IT & ITES, Manufacturing, and Construction. LOCKBIT, CLOP, ALPHV, 8Base, and Akira were the groups most actively involved in attacking the region, alongside 35 others.

Figure 3: Geographical distribution of Ransomware victims in the Americas



Europe & CIS

European organizations were the second most affected after the Americas, with 280 ransomware victims – a decrease of 34% from the previous quarter.

The United Kingdom replaced Italy with 67 victims to record the highest volume of ransomware attacks in the region. Germany had the second-highest victim count of 45, followed by France, with 37 reported incidents.



Professional Services replaced IT & ITES as the region's worst-hit sector. This quarter, we observed that ransomware groups also aggressively targeted Manufacturing, IT & ITES, and Construction sector entities in the region. LOCKBIT, CL0P, and NoEscape were the most active ransomware groups in this region.

Figure 4: Geographical distribution of Ransomware victims in Europe & CIS

Asia & Oceania

Asia and Oceania was the third most targeted region, with 107 victims alone. This quarter, IT & ITES was replaced by Construction as the most targeted sector, followed by Professional Services, Manufacturing, and Healthcare sectors. 24 ransomware groups were observed to be active in this region, **including LOCKBIT, ALPHV, 8Base, NoEscape, and CL0P, being the prominent ones.**



Australia and India emerged as the region's most targeted countries, similar to the last quarter.

Figure 5: Geographical distribution of Ransomware victims in Asia & Oceania



META

The Middle East, Turkey, and Africa (META) region **saw the lowest number of ransomware attacks at 73 victims**. While over 22 countries in this region were targeted, the majority of attacks were reported in Iran and Turkey, replacing South Africa and the United Arab Emirates from last quarter. **LOCKBIT** has consistently been the most active ransomware group in the region in Q3-2022. Over 14 ransomware groups are currently active in the region, with **Arvin Club** and **ALPHV** being the next most active ransomware groups. **Arvin Club** ransomware emerged in the ransomware scenes again after a prolonged gap to primarily target Iranian entities.



There is a sectoral shift in ransomware attacks towards Manufacturing and Education in the META region from earlier observed widespread attacks against BFSI and IT & ITES sectors.

Figure 6: Geographical distribution of Ransomware victims in META





Microanalysis of Ransomware Activities

The new ransomware groups identified this quarter were – **Cactus, INC Ransom, Metaencryptor, ThreeAM, Knight, Cyclops Group, and MedusaLocker.**



The figures below indicate a Quarter-over-Quarter comparative analysis of ransomware attacks by various groups. The data bars in Grey indicate the statistics of ransomware attacks by several ransomware groups in Q3-2023 in comparison to the previous quarters in 2023.

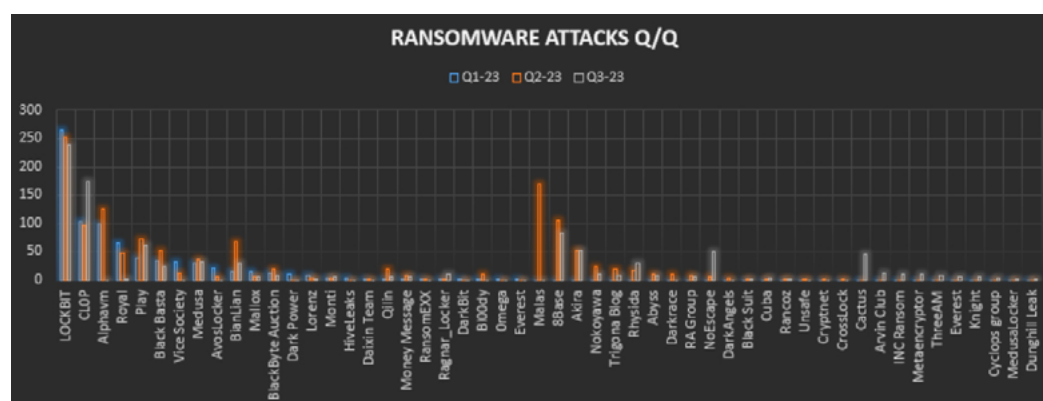


Figure 7: Ransomware activity in 2022

- LOCKBIT was the most active ransomware group, targeting 240 organizations in Q1-2023, a decrease of over 5% compared to Q2-2023. These affected entities were primarily from the Professional Services, Construction, Manufacturing, Education, and Consumer Goods sectors.
- CL0P ransomware group continued to mass-target several high-net-worth corporations vulnerable to MOVEit vulnerability, especially the organizations with businesses involved in the manufacturing of Operational Technology (OT) equipment, which is critical to several industries worldwide.
- Ransomware attacks by Ragnar Locker increased by 450% in this quarter. The sectoral attack footprint of the ransomware group expanded to Energy and Utilities, IT & ITES, and Professional Services. Incidentally and in contrast to other ransomware groups, Ragnar Locker was observed to be more oriented towards targeting the UK and France as compared to the US.
- Rhysida, a new ransomware group that emerged in Q2-2023, targeted 67% more organizations in Q3-2023 as compared to the previous quarter. Rhysida majorly targeted the Education, Government, and LEA entities from the US, the UK, and Spain.
- NoEscape ransomware group's activities alarmingly increased in this quarter. The new ransomware group that emerged into the ransomware screen with their sophisticated hybrid-cryptography method of encryption increased their attacks by over 600%, primarily across the US, Italy, and France. The group that operates a Ransomware-as-a-Service (RaaS) platform was evidently targeting the Services, Education, and Healthcare sectors in this quarter.



Ransomware Sectoral Impact

The sectoral impact in Q3-2023 was nearly identical to the previous quarter, and the trendline in the graph below highlights the highs and lows of attacks across different sectors in comparison to Q2 and Q1 2023. Professional Services continued to be the most targeted sector, with 150 victims, with a decrease of 20% compared to the previous quarter.



Construction replaced IT & ITES as the second most targeted sector, with 105 and 91 victims, respectively. As inferred from the number of victims and the continuing trend from Q3-2022, US-based businesses suffered the maximum ransomware-based breaches in the five most affected industrial sectors.

The Professional Services sector continued to be the most targeted sector by LOCKBIT and CL0P ransomware groups, followed closely by the IT & ITES and Construction sectors.

Considering the overall decline in ransomware attacks compared to the previous quarter in Q3-2023, there was a 20% decrease in attacks on the Professional Services sector, 9 % in attacks on the Construction sector, and a 45% decrease in the IT & ITES sector, compared to Q2-2023.

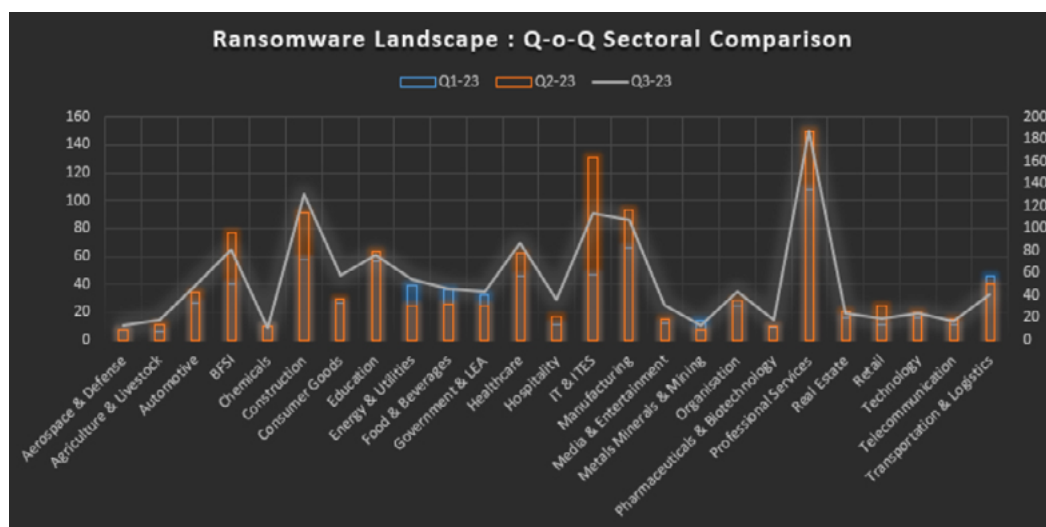
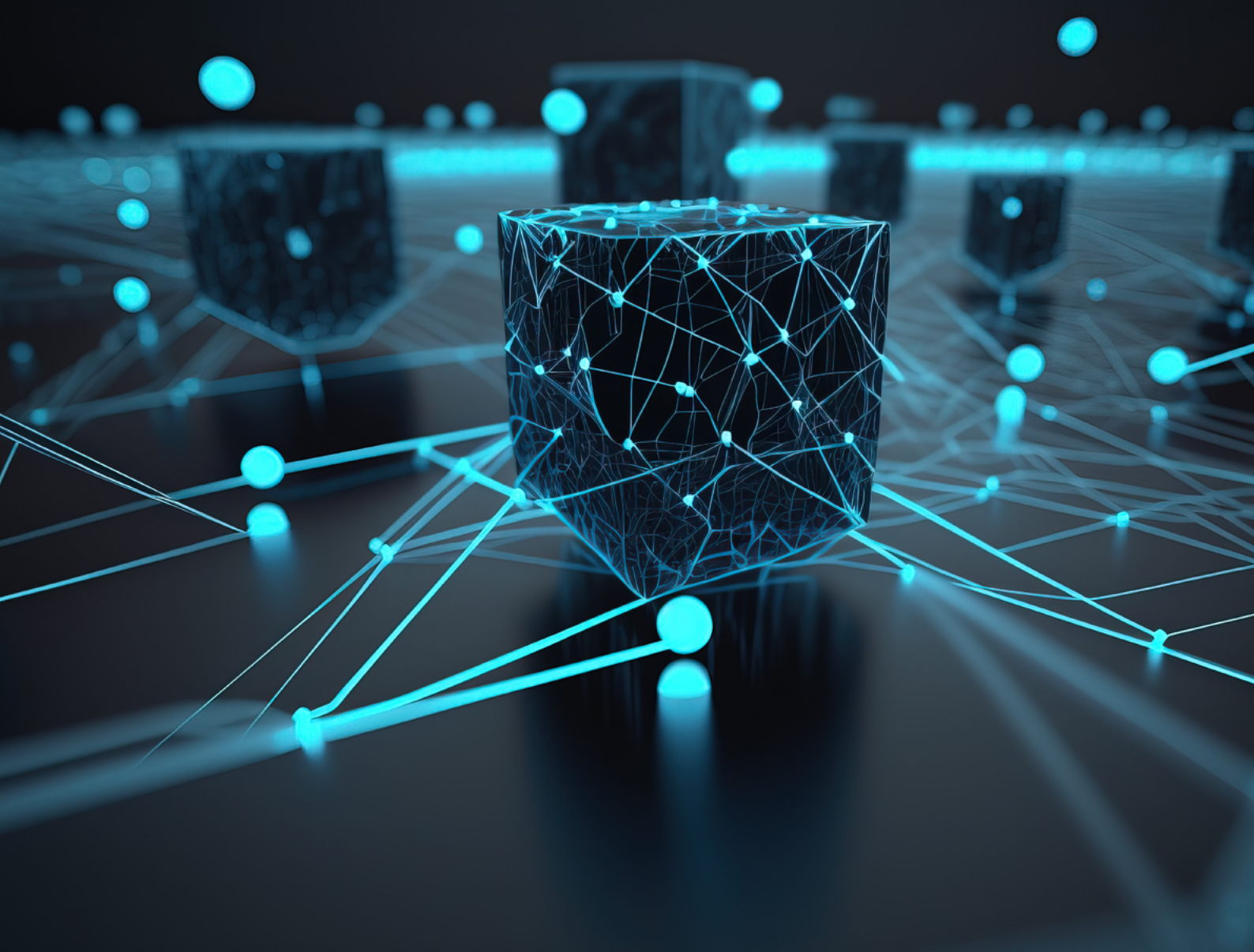


Figure 8: Q-o-Q Sectoral Comparison of Ransomware Landscape





Weaponized Vulnerabilities of Q3-2023

CVE-2023-36884

Microsoft has highlighted CVE-2023-36884, an Office and Windows HTML Remote Code Execution vulnerability. A targeted attack using specially crafted Microsoft Office documents was detected by a phishing campaign by Storm-0978, a Russian cybercriminal group known for ransomware and extortion operations. The group also developed and distributed the RomCom backdoor and deployed Underground Ransomware. A similar campaign was previously observed in June 2023, using CVE-2023-36884 to distribute a backdoor similar to RomCom, using a phishing site masquerading as legitimate software.



CVE-2023-3519

Threat Actors linked to the FIN8 hacking group were reported exploiting CVE-2023-3519 to compromise unpatched Citrix NetScaler systems. This cyber campaign involves domain-wide attacks targeting these systems. Analysis by Sophos X-Ops reveals a strong resemblance between the ongoing attacks and previous incidents using similar tactics. In mid-August, the TAs injected malicious code into the target system, distributing malware using BlueVPS Autonomous System Number and obfuscated PowerShell scripts. The attackers also deployed PHP webshells on compromised victim machines.

CVE-2023-20269

This vulnerability in Cisco ASA Software Release 9.16 or earlier allows attackers to exploit the improper separation of Authentication, Authorization, and Accounting (AAA) between remote access VPN and HTTPS management and site-to-site VPN features. The threat intelligence community reported that the threat actors were observed to be carrying out lateral movement and binary executions across vulnerable systems, resulting in the deployment and execution of ransomware binaries related to Akira or LockBit.

CVE-2023-32315

Hackers have been observed exploiting a vulnerability in Openfire messaging servers to encrypt servers with ransomware and deploy crypto miners. The flaw, identified as CVE-2023-32315, allows unauthenticated attackers to create new admin accounts on vulnerable servers. They install malicious Java plugins that execute HTTP requests. The flaw affects all Openfire versions from 3.10.0 to 4.7.4.

CVE-2023-27532

Cuba ransomware gang has targeted US and Latin American IT firms using CVE-2023-27532 to steal credentials from configuration files. The flaw affects Veeam Backup & Replication products. The FIN7 group has multiple affiliations with ransomware operations and has been actively exploiting this vulnerability.

CVE-2023-38831

A vulnerability in RARLAB's WinRAR versions before 6.23 allowed threat actors to create ZIP archives that could execute malicious code and carry various malware families. These weaponized ZIP archives were distributed in the wild and advertised in underground forums and Telegram channels. Open-source research identified multiple GitHub repositories hosting exploit generators for the vulnerability. AegisCrypter, a Threat Actor, offered to sell the WinRAR exploit for \$100, allegedly with an auto-download feature, and remain undetected by Windows Defender, Google Chrome, and Browser Edge.



Capricious Ransomware Techniques

Ransomware variants are adopting novel techniques to extort ransom and evade detection. Some of the new techniques that we observed in Q3-2023 were:



- “Grounding Conductor”, a new ransomware strain, specifically targets Windows operating systems. Despite not using a leak site for extortion, it encrypts files with a ransom note, compresses them into a ZIP archive, and adds a unique extension.
- Knight ransomware, aka Knight Lite, and a progression of Cyclops ransomware emerged in August 2023, along with their RaaS offering for Windows, Linux/ESXi, and macOS platforms. This ransomware variant also maintains a TOR-based leak site.
- Scarab ransomware is being distributed using a tool called Spacecolon, likely for breaching web servers or brute-force access. Its primary component is ScHackTool, while ScInstaller is a module for installing ScService, a backdoor that allows CosmicBeetle to execute commands, download payloads, and gather system data.
- The Cuba ransomware group has been observed to utilize a toolkit consisting of customized components and tactics. The first phase involves implementing BUGHATCH, a lightweight downloader that communicates with a command-and-control server to obtain a chosen payload. It also allows the operator to execute files or commands.
- A unique ransomware variant called “NoBit ransomware” was discovered, which focuses on file encryption using advanced algorithms. It includes features like geographic targeting, file type encryption, and ransom note file extensions.
- The Abyss Locker operators have developed a Linux encryptor targeting VMware’s ESXi virtual machine platform, targeting enterprises for improved resource management, performance, and disaster recovery. As businesses shift to virtual machines, ransomware gangs are creating encryptors to exploit this platform, encrypting all virtual servers on a device.
- ALPHV ransomware has released a Python crawler to synchronize leak posts and attachments with databases. The API could simplify the data extortion process, automating the extraction of old and newly created posts. However, the release may increase the risk of data being available to multiple threat actors and groups, as scammers have previously exploited this data for illicit purposes.
- SophosEncrypt, a new Ransomware-as-a-Service (RaaS) posing as Sophos, uses the company’s name for operations. The encryptor requests the ransomware affiliate to input a token, validate its authenticity, and provide additional information for device encryption.
- As observed from the Cyble Global Sensor Intelligence (CGSI) network, threat actors were quick in exploiting MOVEit vulnerability with a high possibility of automation to weaponize them. Threat actors exploited the same for targeting the Critical Infrastructure and Education sector in the United States.
- The lesser-known BI00dy ransomware group was observed to be exploring an exploit for CVE-2023-39143 - PaperCut NG/MF print management software.



Ransomware Groups Updating Their Variants

Yashma

CRIL discovered a new version of the Yashma ransomware, a 32-bit executable in.NET, rebranded as Chaos ransomware V5. It features an embedded batch file, allowing ransom notes to be retrieved from a GitHub repository, potentially obscuring the threat actor's identity.

Big Head

Researchers have discovered a ransomware strain called 'Big Head', spreading through deceptive online ads. The ransomware is a.NET binary that installs three AES-encrypted files, likely from a single operator, experimenting with attack optimization methods.

ArCrypter

ARCrypter ransomware, also known as ChileLocker, is a ransomware variant developed by Threat Actors that emerged in August 2022 after an attack on a Chilean entity. It targets organizations worldwide, targeting Windows and Linux systems, and has been observed to be active in the wild in Q3-2023.

Linux Variant of NIM-Based Ransomware

NIM, a cross-platform programming language, has been used by the Dark Power ransomware group to create ransomware variants, including "Kanti," to target cryptocurrency users by modifying encrypted file extensions and dropping ransom notes.

Activities Across Cybercrime Forums

Cybercrime Forums remained active for several ransomware groups in Q3-2023, a continuing trend observed from the last quarter.

Everest Ransomware Collaborates with Extortion Group

On September 02, 2023, the Everest Ransomware group made a post about targeting the SKF group along with a demand for ransom. A similar post was observed by CRIL on August 25, 2023, by Ransomed.vc, an extortion group that claimed to have compromised the same entity. This collaboration among these two groups was later confirmed by posts on their respective leak sites.

Extortion Group Affiliates Advertising on Underground Forums

In an underground forum, CRIL identified a threat actor under the alias 'Crime' aka BorisTulev, leaking partial data of some corporations. Upon correlating the names of these victim organizations with known breaches, we were able to establish the TA's link with the newly emerged extortion group - Ransomed, which had also advertised the name of the same business on their leak site for extorting them.

In another instance, we observed a new TA by the moniker 'pongo' advertising about their newly established extortion group - 'RansomCorp', and posted a separate thread on the forum to hire operators and affiliates for their extortion operations.



Ransomware Threat Predictions



As predicted in our previous report, the tactics employed in the recent surge of ransomware attacks towards organizations affected by the MOVEit vulnerability is noteworthy and a unique case wherein we witnessed large-scale and swift attacks across the globe, leveraging their internet exposures.



In the near future, similar campaigns may emerge by new ransomware groups who have already witnessed the impact and the benefit they can accrue by automating and mass exploiting such critical vulnerabilities. The distribution of custom scripts in underground cybercrime scenes and ease of access to open-source vulnerability scanners will be an added advantage in favor of such ransomware groups.



Social Engineering and the use of compromised user accounts, widely being auctioned in the underground for gaining an initial foothold into the networks of the targeted organizations, is likely to be the preferred technique that the ransomware groups will employ.



Considering the growth in ransomware attacks on the Construction sector, we anticipate an increase in attacks on organizations involved in the development of critical and strategic infrastructure development, especially across the US, Europe, and NATO allied countries.



As predicted about the growth in ransomware attacks on healthcare technology, we further anticipate a growth in such attacks in South America due to the anticipated growth of the industry in the region.



Ransomware attacks on the value chain of any industry have very high ensuing costs to resume or sustain the entire supply chain of various businesses. The ransomware groups have been particularly observed to be motivated to cause large-scale disruptions by launching supply chain attacks in 2023. The same technique is expected to be further expanded to target a plethora of small-medium companies involved in the production of machinery, automation equipment, robotics, and other ICS components employed by Critical Manufacturing, Automotive, Telecommunication, and Technology businesses.



Wide adoption of electric vehicles in the Automotive industry is likely to draw the attention of ransomware groups toward targeting the ancillaries supporting electric vehicle production and operations, such as companies involved in the production and installation of charging docks, applications supporting these operations, and technology providers of onboard diagnostic systems, operating system, Advanced Driver Assistance Systems (ADAS) and in-vehicle networks.



Ransomware groups can weaponize the following vulnerabilities in the coming quarters:

- CVE-2023-36845
- CVE-2023-39361
- CVE-2023-20900



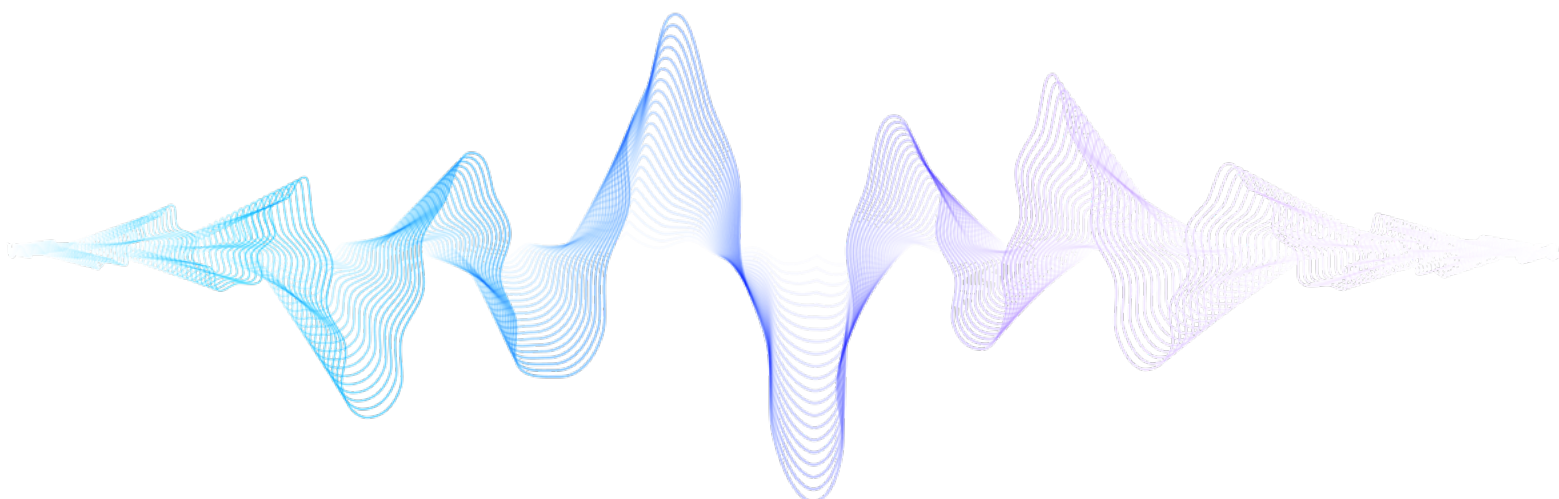
How to protect yourself from Ransomware Attacks

With Threat Actors and their TTPs increasing in sophistication and rapid adoption of new Ransomware techniques alongside the increasing use of Artificial Intelligence, the industry continues its search for the proverbial silver bullet to counter this potent cyber threat.



However, there are a few cybersecurity measures that we strongly recommend to organizations to reduce the likelihood of a successful attack:

- Define and implement a backup process and secure those backup copies by keeping them offline or on a separate network.
- Monitor darkweb activities for early indicators and threat mitigation.
- Enforce password change policies for the network and critical business applications or consider implementing multi-factor authentication for all remote network access points.
- Reduce the attack surface by ensuring that sensitive ports are not exposed to the Internet.
- Conduct cybersecurity awareness programs for employees, third parties, and vendors
- Implement a risk-based vulnerability management process for IT infrastructure to ensure that critical vulnerabilities and security misconfigurations are identified and prioritized for remediation.
- Instruct users to refrain from opening untrusted links and email attachments without verifying their authenticity.
- Deploy reputable anti-virus and internet security software packages on your company-managed devices, including PCs, laptops, and mobile devices.
- Turn on the automatic software update features on computers, mobiles, and other connected devices.





Cyble Vision – a Shield against Ransomware

From our quarterly reports, there are several clear patterns that we have established:

- Ransomware groups are continuously improving their tactics and going after more high-profile targets.
- Ransomware variants are becoming increasingly sophisticated and have achieved the capability to target and compromise even cyber-aware, large organizations and even National Critical Infrastructure.
- Even with the cybersecurity best practices in place, ransomware groups are finding new and innovative ways to compromise their intended targets, often bypassing these security measures.
- The rise in Ransomware-as-a-Service (RaaS) is worrying for individuals and entities of all sizes, as it empowers even non-technically sophisticated Threat Actors to carry out ransomware attacks against their target of choice.
- Increased scrutiny, regulations, governance, and law enforcement methods implemented against ransomware have caused Ransomware groups to evolve accordingly, adopting new ways to remain stealthier, establish persistence, and mask their activities from their victims and authorities.
- While following our recommendations mentioned in this article is a good first step to securing yourself and your organization against Ransomware attacks, it is by no means an air-tight solution that can guarantee cyber safety.

How can Vision help?

With a keen view into both the surface and deep web, Vision can keep you a step ahead of Ransomware operators.

- Through a keen Threat Analysis, Vision can help identify weak points in your organization's digital risk footprint and guide you on how to secure these gaps that ransomware groups could potentially exploit.
- Vision has the ability to scan your entire attack surface, extending to your vendors, partners, and third parties as well, giving you the ability to secure your entire supply chain and ecosystem from attacks.
- Being powered by AI allows Vision to scan vast quantities of data from all parts of the surface, deep and dark web, allowing real-time updates into Threat actor behavior.
- With a focus on Darkweb Monitoring, Vision can let you track Threat Actor patterns and actions on the Darkweb. From discussing a new variant to monitoring affiliate programs, you can stay one step ahead of Ransomware operators.

If you're interested in seeing how Vision can help secure your organization, reach out for a free demo with our cybersecurity experts [here](#).



References

[Hackers actively exploiting Openfire flaw to encrypt servers \(bleepingcomputer.com\)](#)

[Cuba ransomware uses Veeam exploit against critical US organizations \(bleepingcomputer.com\)](#)

[Under Siege: Rapid7–Observed Exploitation of Cisco ASA SSL VPNs | Rapid7 Blog](#)



Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the Darkweb. Its prime focus is to provide organizations with real-time visibility to their digital risk footprint. Backed by Y Combinator as part of the 2022 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Startups to Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, and India, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com

