CYBLE

Q2-2023 Ransomware Report

July 2023

Table of Contents

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 Q2-2023 to preempt the associated risks of the Ransomware Groups discussed herein.

This report encapsulates the following major findings from Q2-2023:

- 1,298 victims were publicly disclosed by ransomware groups, with United States (US) corporations continuing to be the most affected.
- Italy and Germany witnessed a steep increase of 294% and 119%, respectively, in ransomware attacks.
- The majority of high-income organizations were targeted in the Professional Service, IT & ITES, and Construction sectors.
- As predicted, IT & ITES and BFSI emerged within the 5-most impacted sectors in this quarter.
- We observed the emergence of over 20 new ransomware groups in Q2-2023, a significant spike of 30% in the formulation of new ransomware groups compared to Q1-2023.
- LOCKBIT claimed 5% fewer attacks compared to Q1-2023 but remained the most deplorable ransomware group, targeting 252 entities in Q2-2023.
- CL0P ransomware group, after targeting numerous organizations with GoAnywhere vulnerability in Q1-2023, continued to mass exploit MOVEit vulnerability in Q2-2023.
- Capricious techniques of ransomware groups in Q2-2023 provide further insights into their operations and indications about the evolving ransomware threat landscape in the year ahead.

Total victims

1,298

Active Ransomware Groups

37 viz-a-viz **25** last quarter

Most Affected Countries (Top 5)

United States	569	▲ 65%
Italy	71	▲ 294%
United Kingdom	70	▲ 21%
Germany	57	▲ 119%
Canada	56	▲ 51%

Most Active Ransomware Groups (Top 5)

LOCKBIT	Malas	ALPHV	CLOP	Play
252	171	127	97	74

Most Impacted Industry Sectors (Top 5)

Professional Services	186	▲ 71%	IT & ITES	164	▲ 249%	Manufacturing	117	▲ 75%	
BFSI	96	▲ 140%	Construction	115	▲ 98%				

Quarterly Ransomware Outlook

CRIL identified 1,298 ransomware victims in Q2-2023 compared to 783 in Q1-2023 – a 66% growth in attacks Quarter-over-Quarter (Q-over-Q) and 130% increase Year-over-Year (Q2-2022).

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

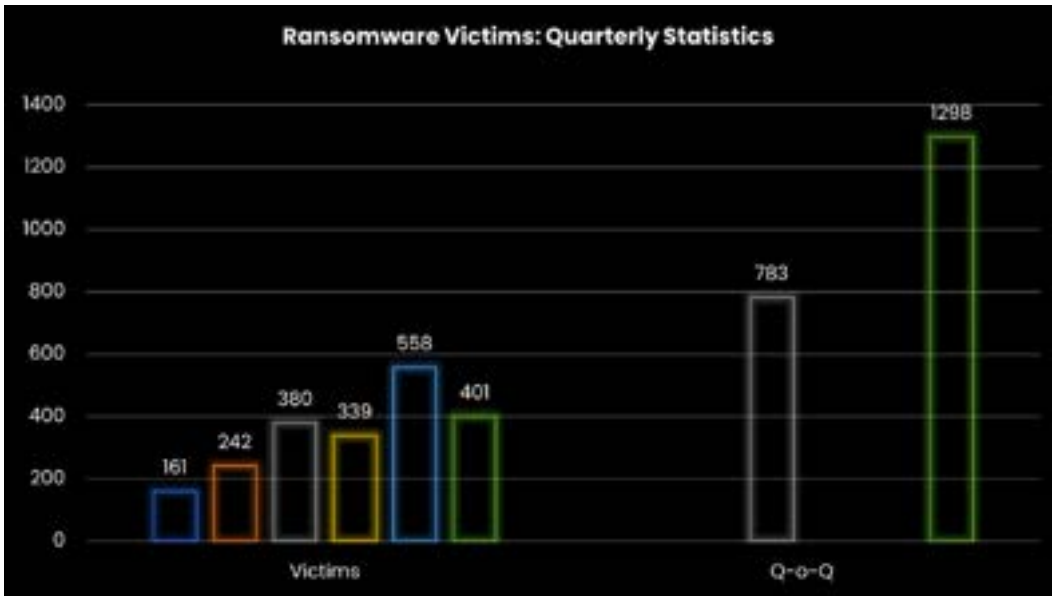
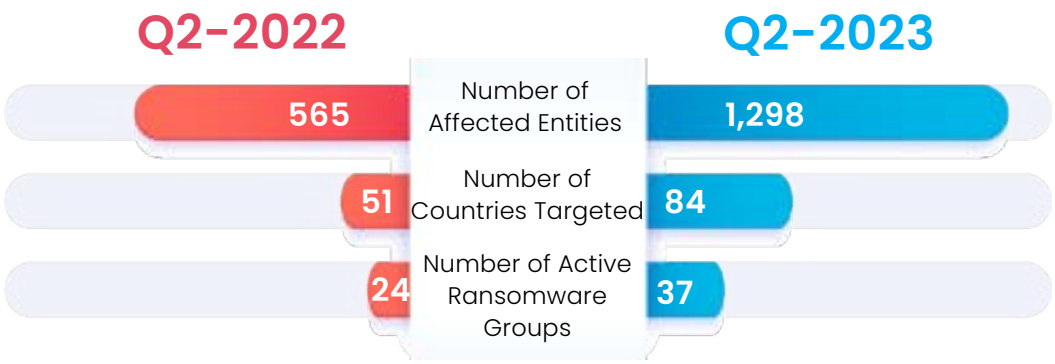


Figure 1: Comparative analysis of ransomware activities Q-over-Q

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



Global Ransomware Threat Landscape

CRIL observed that the ransomware attack footprint grew from 76 countries in Q1-2023 to 84 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

Americas was the most targeted region, with 711 ransomware victims this quarter, in contrast to 430, in Q1-2023. This region accounts for over 80% of ransomware victims disclosed publicly in Q2-2023. We also observed a growth in attacks on South American organizations compared to the previous quarter. A snapshot of the ransomware landscape in the region is as follows:

The figure below showcases the geographical distribution of major ransomware activities across this region in Q2-2023.

Ransomware attacks in the Americas have particularly impacted the Professional Services sector. The Construction sector has emerged among the 5 most affected sectors this quarter, besides IT & ITES, Manufacturing, and Healthcare. LOCKBIT, ALPHV, 8Base, CLoP, and Akira were the groups most actively involved in attacking the region, alongside 30 others.

Figure 3: Geographical distribution of Ransomware victims in the Americas

Europe & CIS

European organizations were the second most affected after the Americas, with 427 ransomware victims – an increase of 120% from the previous quarter. Italy replaced the United Kingdom to record the highest volume of ransomware attacks in the region, with 71 victims. The United Kingdom had the second-highest victim count of 70, followed by Germany with 57 reported incidents.

The figure below showcases the geographical distribution of major ransomware activities across Europe and the CIS region in Q2-2023.

IT & ITES replaced Professional Services as the region's worst-hit sector. This quarter, we observed that ransomware groups also aggressively targeted the Professional Services and Manufacturing sectors, a shift from previous attempts to target the Construction sector. Apart from these, Transportation was also one of the most affected sectors in this region. Malas, LOCKBIT, Play, CLoP, and 8Base were particularly nefarious in this part of the world.

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

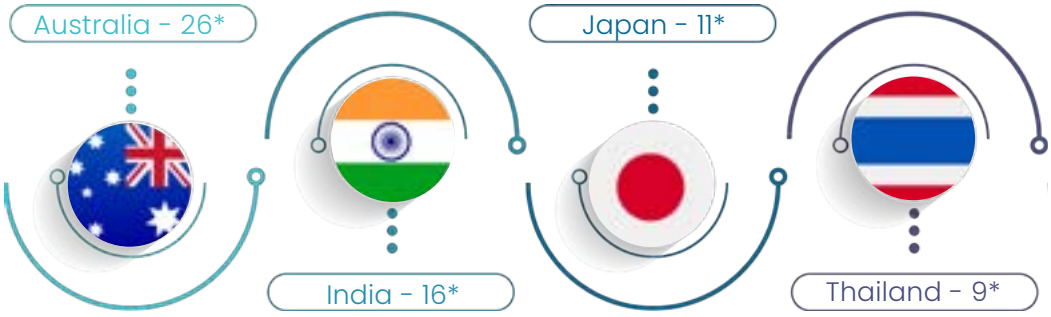
Asia & Oceania

Asia & Oceania was the third most targeted region, with 112 victims alone. This quarter, the sectoral impact of ransomware attacks has completely shifted focus to IT & ITES, BFSI, Professional Services, Construction, and Manufacturing sectors. While in Q1-2023, Manufacturing, Energy & Utilities, IT & ITES, Professional Services, and Healthcare were the most targeted. In this region, 24 ransomware groups were observed to be active, including **LOCKBIT, ALPHV, 8Base, BianLian, and Malas being the prominent ones.**

Australia and India emerged as the region's most targeted countries, replacing Indonesia as the most targeted country from the last quarter.

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

The figures below reflect the distribution of major ransomware activities across Asia & Oceania in Q2-2023.



***Count of Victims**

META

The Middle East, Turkey, and Africa **(META) region saw the least number of ransomware attacks.** While over 20 countries in this region were targeted, the majority of attacks were reported in South Africa and the United Arab Emirates. **LOCKBIT** has consistently been the most active ransomware group in the region from Q3-2022. Over 12 ransomware groups are active in the region, with **ALPHV and 8Base** being the next most active after LOCKBIT.

There is a sectoral shift in ransomware attacks towards BFSI and IT & ITES in the META region from earlier seen widespread attacks against the Healthcare and Food & Beverages sectors. At the same time, Organization and Professional Services remained among the most targeted sectors in the region.

Figure 6: Geographical distribution of Ransomware victims in META

Microanalysis of Ransomware Activities

New ransomware groups identified this quarter were – Dark Race, Dunghill, La Piovra, Trigona, NoEscape, Akira, Rancoz, BlackSuit, RA Group, Malas, CryptNet, Rhysida, 8Base, Obsidian ORB, Buhti, Rorschach, Cylance, CROSSLock, RTM Locker, and Cactus.

The figures below indicate a Quarter-over-Quarter comparative analysis of ransomware attacks by various groups. The data bars in orange indicate the rise in ransomware attacks in Q2-2023.

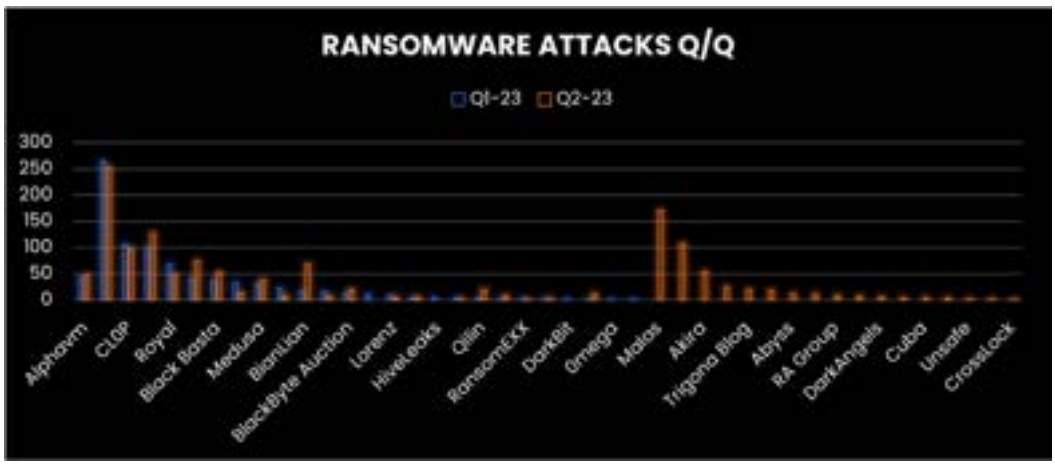


Figure 7: Ransomware attacks Quarter-over-Quarter

- **LOCKBIT was the most active ransomware group, targeting 252 organizations in Q2-2023, a decrease of over 5% compared to Q1-2023. These affected entities were primarily from the Professional Services, Manufacturing, Construction, BFSI, and IT & ITES sectors**
- **LOCKBIT's 37% of victims had the highest number of victims from the US, followed by Canada and the United Kingdom, similar to Q1-2023**

The figure below showcases the activity of prevalent ransomware groups in most impacted nations, including the United States, the United Kingdom, and Canada.

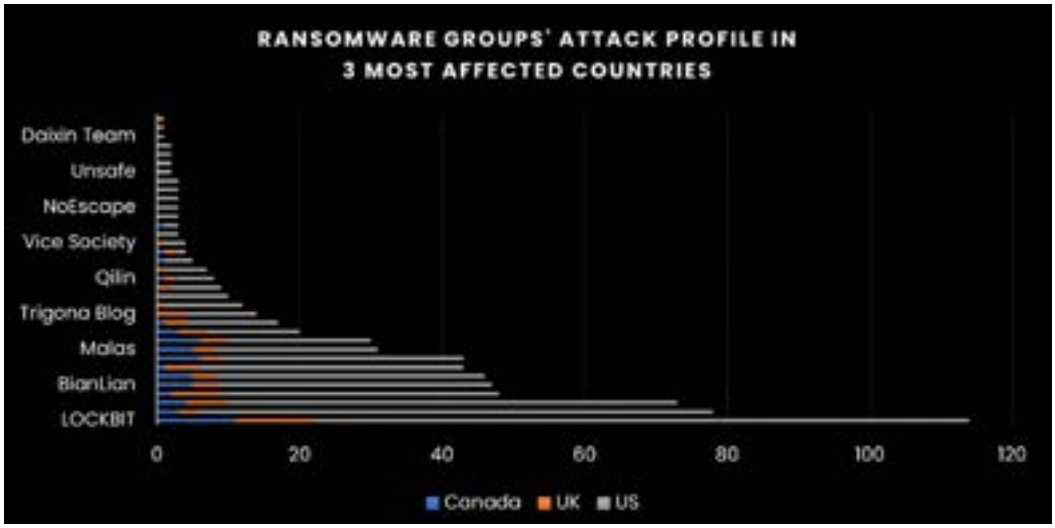


Figure 8: Ransomware Activity in the three most affected countries (US,UK & Canada)

Ransomware Sectoral Impact

CRIL observed a few significant crests and troughs in the Ransomware group's sectoral attack footprint in Q2-2023. As predicted earlier, the IT & ITES sectors climbed up to emerge as the second most targeted sectors in Q2-2023, a three-point jump in attacks on the sector from the previously reported fifth-most sector. IT & ITES was most targeted by the Malas ransomware group.

While BFSI was fifth among the 5-most targeted sectors in Q2-2023, as predicted earlier, CL0P was particularly observed to be targeting this sector.

As inferred from the number of victims and the continuing trend from Q2-2022, US-based businesses suffered the maximum ransomware-based breaches in the five most affected industrial sectors. Notably, Italian corporations in the 5-most hit sectors were equally targeted.

The Professional Services sector was vigorously targeted by Malas and 8 Base ransomware groups, while LOCKBIT continued to claim maximum victims from-Manufacturing and Construction sectors.

In Q2-2023, there was a 70% increase in attacks on the Professional Services sector, 105 % in attacks on the IT & ITES sector, and a 140% increase on the BFSI sector, compared to Q1-2023.

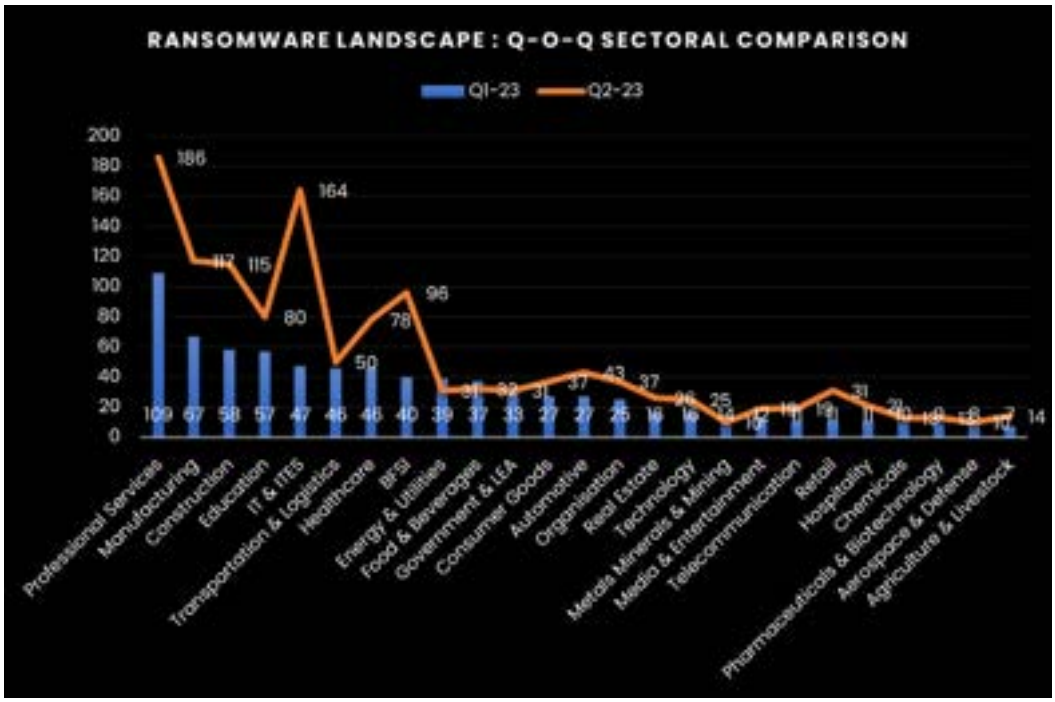


Figure 9: Q-o-Q Sectoral Comparison of Ransomware Landscape

In Q2-2023, the countries that were adversely affected in the five most targeted industries were:

PROFESSIONAL SERVICES	IT & ITES	MANUFACTURING	CONSTRUCTION	BFSI
United States	United States	United States	United States	United States
United Kingdom	Italy	Italy	Italy	United Kingdom
Italy	Spain	Germany	Canada	Australia
Brazil	Canada	United Kingdom	Germany	India
Canada	United Kingdom	Canada	United Kingdom	Italy

Repeated Ransomware attacks in Q2-2023

— French Digital Automation and Energy Management company suffered an attack from the CL0P Group in June 2023, earlier compromised by the LOCKBIT ransomware group in December 2021.

— A German Transportation & Logistics service provider, earlier targeted by LOCKBIT in June 2022, was compromised by CL0P in June 2023.

— A Government entity in Colombia, was targeted twice in May 2023 by LOCKBIT and Medusa.

— Qilin targeted a Japanese Electronics manufacturer in April 2023, which was previously attacked by LOCKBIT in November 2021.

— Vice Society targeted Malaysia-based University twice in May 2023 and earlier in May 2022.

— A US-based IT & ITES company was targeted by CL0P in June 2023 and earlier by the Conti ransomware group in March 2022.

— CL0P repeatedly targeted UK-based Energy company. The initial breach was in March 2021, and the recent one in June 2023.

— A Professional Services firm in the US was targeted by the Monti Ransomware group in March 2023 and by ALPHV in April 2023.

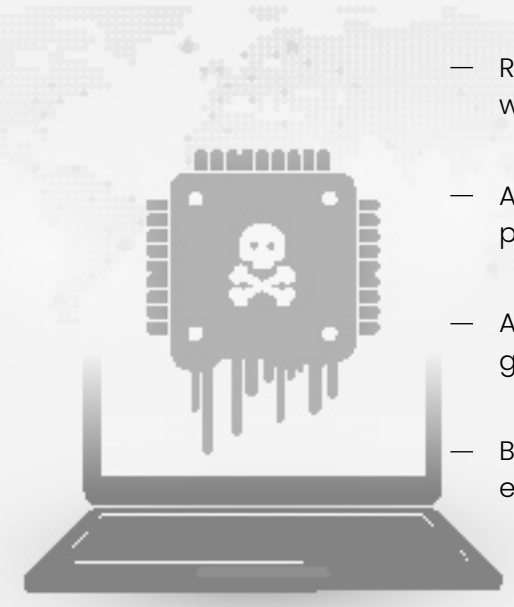
— A Germany-based ship-building company was targeted by RansomEXX in April 2021 and recently targeted by BianLian in April 2023.

— REvil attacked a US-based energy provider in June 2021. The company was again targeted by Unsafe in April 2023.

— ALPHV and Play groups targeted a Spain-based software solutions provider, in April and May 2023, respectively.

— A Canada-based Newsprint Company was targeted by Rhysida and Play groups in June 2023.

— BianLian and ALPHV compromised a US-based construction and engineering solutions provider, in June 2023.



Evolving Ransomware Threat Profile

The profile of ransomware attacks has evolved over time. Initially, ransomware attacks were relatively unsophisticated and targeted individual users. However, as the profitability of ransomware attacks increased, attackers began to target organizations, businesses, and even governments, which are typically willing to pay larger ransoms to restore access to their critical systems and data.

Ransomware attacks have now become more targeted and customized, with attackers conducting detailed research on their targets before launching an attacks.

Cyble Research & Intelligence Labs worked on profiling new ransomware groups in Q2-2023 to forewarn our readers about their activities in the evolving ransomware threat landscape.

NoEscape Ransomware

During May 2023, threat actor 'N0_Esc4pe' was observed offering Ransomware-as-a-Service (RaaS) dubbed 'NoEscape'. The ransomware for the affiliate is developed entirely in C++, and the actor claims that the malware was created from scratch without using any third-party resources.

The technical features of the RaaS indicated that it allows its operators to leverage the triple extortion technique to extort their victims. The primary feature included the malicious build supporting ChaCha20 and RSA encryption algorithm.

It is a hybrid-cryptography method that sophisticated ransomware groups use to encrypt files and protect their keys. The technique encrypts all the ChaCha20 keys with a global ChaCha20 key before encrypting this global key with its RSA-2048 public key.

Akira Ransomware

Akira ransomware, discovered in April 2023, exfiltrates and encrypts their data using a double-extortion technique. The ransomware utilizes the "Microsoft Enhanced RSA and AES Cryptographic Provider" libraries to encrypt the victim's machine.

Figure 10: Akira ransomware group leak site

Rancoz Ransomware

The Rancoz ransomware group shares similarities with Vice Society ransomware. The threat actors behind the ransomware group employ double extortion techniques to maximize their chances of receiving payment from victims. The ransomware deletes Shadow Copies, removes values in the Windows Registry related to Remote Desktop Connection, deletes the default Remote Desktop Protocol (RDP) configuration file, and erases all Windows event logs. Rancoz ransomware employs a combination of symmetric and asymmetric encryption techniques to encrypt files securely. It uses the NTRUEncrypt algorithm for asymmetric encryption, and for symmetric encryption, it uses the ChaCha20-Poly algorithm.

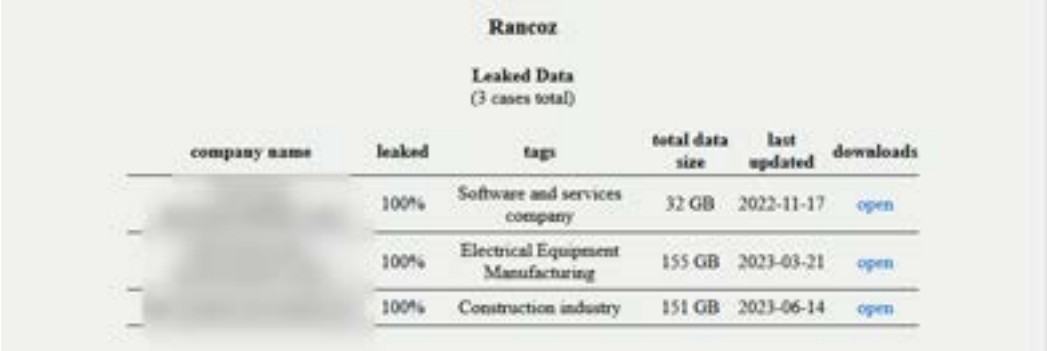


Figure 11: Rancoz ransomware group leak site

BlackSuit Ransomware

BlackSuit ransomware targets both Windows and Linux operating systems. According to observations made by researchers, the code of the Linux variant of BlackSuit has been found to share similarities with the Royal ransomware. The ransomware applies the AES algorithm to encrypt files.

Figure 12: BlackSuit ransomware leak site

RA Group Ransomware

RA ransomware group emerged in April 2023. The RA group appears to be utilizing leaked source code from Babuk ransomware for their double extortion attacks. The ransomware binary utilized by the group is coded in C++ and shares Babuk's mutex name. The ransomware executable employed by RA Group utilizes the curve25519 cryptography scheme and the hc-128 algorithm from the eSTREAM cipher for encryption purposes. It is important to note that this encryption process selectively encrypts specific portions of the source file's content rather than the entire file.

Figure 13: RA Group leak site

MalasLocker Ransomware

The cybersecurity community reported about a new ransomware group called MalasLocker in May 2023. The ransomware group has been targeting the Zimbra server to steal emails and encrypt files since May 2023. The Spanish-speaking ransomware group has leaked emails of over 170 organizations, mainly from Italy, Russia, and the United States. However, instead of requesting a ransom payment, the threat actors insist on donating to a charitable cause to provide an encryptor and prevent data leaks.

The ransomware group's Base64 encoded section within the ransom note reveals an Age encryption tool header relatively rarely seen among ransomware groups. Further, the MalasLocker ransomware group is observed to target non-Windows devices that suggest similar tactics as that of AgeLocker ransomware discovered in 2020 and the QNAP campaign of 2022.

Figure 14: Malas Ransomware leak site

CryptNet Ransomware

CryptNet ransomware was reported to be discovered in April 2023. The ransomware is written in .NET and uses obfuscation techniques with Eziriz's .NET Reactor. After removing the obfuscation, it becomes apparent that CryptNet is similar to the Chaos ransomware family and the latest variant, Yashma. These similarities include encryption methods, the ability to disable backup services, and deleting shadow copies. It seems that CryptNet has streamlined the code from Yashma to enhance the performance of file encryption.

Rhysida Ransomware

Rhysida ransomware is a 64-bit binary and targets Windows operating systems. This ransomware uses multiple threads to process files and directories. The Rhysida ransomware employs a combination of RSA and AES algorithms to encrypt files.

Figure 15: Rhysida ransomware leak site

8Base ransomware

8Base Ransomware group discovered in May 2023 is known to be active since April 2023. The group employs a double extortion technique and publishes their victim names on Tor-based leak sites and Telegram channel. The group is observed to be particularly targeting Brazilian entities besides other nationality organizations. Another peculiar tactic observed among the ransomware group is carrying supply chain attacks on IT & ITES organizations and their clients.

Figure 16: 8 Base ransomware leak site

Obsidian ORB Ransomware

Obsidian ORB shares a similarity with Chaos ransomware. It is based on a 32-bit PE binary complied using .NET. The ransomware employs the "Microsoft Enhanced RSA and AES Cryptographic Provider" libraries to encrypt files less than 2 MB on the victim's machine. It overwrites the larger than 2 MB files with random data rendering them forever inaccessible. Notably, this ransomware employs a distinctive ransom payment method, demanding that the victims pay the ransom via gift cards.

Buhti Ransomware Group

Buhti Ransomware group, aka Blacktail, is known to employ leaked code from the LOCKBIT and Babuk ransomware families to target Windows and Linux machines, respectively. Initially recognized for its focus on Linux systems in February 2023, Buhti has more recently drawn the attention of security researchers as evidence suggests its attempts to compromise Windows computers within compromised networks. The ransomware group uses a wide variety of tools such as Cobalt Strike, Meterpreter, Sliver, AnyDesk, and ConnectWise.

Rorschach Ransomware

Cyble Research & Intelligence Labs (CRIL) discovered a unique ransomware strain called Rorschach, deployed using a signed component of a commercial security product. The threat actor responsible for Rorschach is unaffiliated with known ransomware groups and has autonomous behavior, self-propagation, and rare functionalities. The developers have combined effective features from other ransomware variants, raising the bar for ransom attacks and self-propagation. Rorschach highlights the need for robust cybersecurity measures and continuous monitoring and analysis of ransomware samples to keep up with evolving threats.

Cylance Ransomware

Researchers have discovered a new ransomware called Cylance that can target Linux and Windows operating systems. The ransomware enables Windows privileges for the current process, allowing restricted actions such as debugging, modifying security settings, and restoring files. The Linux variant uses ChaCha Stream Cipher for encryption, a variant of the Salsa20 encryption algorithm. After encryption, the ransomware appends the ".Cylance" extension to the encrypted filename. This ransomware appears to be in the developmental stage, as little information is currently available regarding its victims.

CrossLock Ransomware

CrossLock, a new ransomware strain, was discovered by CRIL. It employs double extortion techniques, encrypting and exfiltrating data from victims' systems. Threat actors have written the ransomware using the Go programming language, which offers benefits such as compiling a single codebase for different operating systems. CrossLock also employs Event Trace bypass techniques to avoid detection by security systems. The ransomware also performs actions to reduce data recovery chances and increase attack effectiveness.

RTM Locker

Researchers have revealed the methods used by "Read The Manual" (RTM) Locker, a growing cybercriminal gang. RTM Locker operates as a private Ransomware-as-a-Service provider, targeting unscrupulous attacks to generate unlawful profits. The gang relies on third-party affiliates who must follow strict regulations. Their primary objective is to operate discreetly and avoid media coverage, aiming to earn revenue while remaining anonymous. The gang communicates through encrypted notifications in English and Russian, excluding the CIS region. RTM Locker uses encryption techniques to maximize damage and executes the ransomware with the required privileges, resulting in a User Account Control (UAC) prompt.

Cactus

The Cactus ransomware group has been operating since March 2023, exploiting security vulnerabilities in VPN appliances to gain initial entry into commercial entities' networks. They use a VPN server and service account to pivot inside the network, a pattern observed in all incidents. The group encrypts its ransomware binary for protection, using a batch script to retrieve the encryptor binary using 7-Zip. To enable file encryption, the group requires a unique AES key embedded as a hardcoded HEX string, which effectively encrypts the ransomware and bypasses antivirus and network monitoring tools. The ransomware also alters file extensions, using .CTS0 before and .CTS1 after encryption. After gaining access to the victim's network, the group establishes persistent access through a scheduled task and employs SoftPerfect Network Scanner to search for relevant targets.

Weaponized Vulnerabilities of Q2-2023

CVE-2023-27350

The Bl00dy Ransomware group, LOCKBIT ransomware group, and Buhti ransomware group have been observed to be exploiting PaperCut MF & NG vulnerability (CVE-2023-27350) to target thousands of exposed instances of companies, schools, and government agencies around the world.

MOVEit Transfer Critical Vulnerability (CVE-2023-34362)

During June 2023, the CL0P ransomware group, on their leak site, published a note confirming that they have exploited Progress MOVEit Transfer SQL Injection Vulnerability (CVE-2023-34362) and exfiltrated the data of several enterprises. The note also mentioned communication email IDs for those companies affected by their attacks, to contact them by June 14, with other instructions to negotiate.

The announcement was backed by early threat intelligence data that revealed the CL0P ransomware was exploiting an undisclosed SQL injection vulnerability found in Progress Software's Managed File Transfer (MFT) solution called MOVEit Transfer. The vulnerability allowed them to infect internet-facing MOVEit Transfer web applications with a web shell called LE0MURLOOT. Subsequently, the web shell was employed to pilfer data from the underlying MOVEit Transfer databases.

CL0P ransomware has been previously attributed to carrying out zero-day exploits against Accellion File Transfer Appliance (FTA) devices in 2020 and 2021, as well as Fortra/Linoma GoAnywhere MFT servers in early 2023.

After the incident, the US government announced a bounty of USD 10 Million on any information about the CL0P ransomware group.

CVE-2023-28252

Researchers observed that the Nokoyawa ransomware gang was exploiting CVE-2023-28252 in their attacks after the announcement of this vulnerability in April 2023.

Capricious Ransomware Techniques

Ransomware variants are adopting novel techniques to extort ransom and evade detection. Some of the new techniques that we observed in Q2-2023 were:

Vice Society Employs new PowerShell Script

The Vice Society ransomware group has developed a new PowerShell script to automate stealing data from compromised networks, primarily targeting backups for double extortion. This tactic leverages corporate and customer data to persuade victims to pay the ransom, avoid publishing sensitive information, and receive decryption services.

ALPHV Affiliate UNC4466 Targets Exposed Veritas Backup Exec Installations

The cybersecurity community has discovered a new affiliate of the ALPHV ransomware group, identified as UNC4466, which is targeting Veritas Backup Exec installations that are publicly accessible. They use vulnerabilities such as CVE-2021-27876, CVE2021-27877, and CVE-2021-27878 to gain unauthorized access to the victims' systems.

Previous investigations of ALPHV ransomware attacks have shown that they were primarily executed using stolen login credentials. However, the recent attack by the UNC4466 group suggests a shift towards opportunistically taking advantage of known vulnerabilities.

Hypervisor Jackpotting

The practice of "hypervisor jackpotting," which is progressively gaining traction among various ransomware gangs, involves attacking VMware ESXi hypervisors with ransomware to scale up such attacks.

Recently researchers observed a new Ransomware-as-a-Service (RaaS) operation called MichaelKors, which provides affiliates with ransomware binaries targeting Windows and ESXi/Linux systems.

New Rorschach Ransomware Implements Fast Encryptor

A unique ransomware variant, Rorschach, has emerged in the ransomware threat landscape. The ransomware spreads automatically when executed on a Domain Controller (DC) while simultaneously erasing the affected machines' event logs. Moreover, this ransomware is highly adaptable, relying on its built-in configuration and numerous optional arguments, enabling it to modify its behavior per the operator's requirements.

Rorschach ransomware uses a fast hybrid-cryptography scheme combining curve25519 and eSTREAM cipher hc-128 algorithms to encrypt a portion of the original file content. Rorschach's hybrid-cryptography scheme routine is suspected to be borrowed from the leaked source code of Babuk ransomware. Rorschach's encryption routine is not only fast but also implements effective thread scheduling via I/O completion ports.

The list of languages Rorschach uses to halt the malware is similar to that of LOCKBIT, and LOCKBIT also inspires the I/O Completion Ports thread scheduling method. Additionally, the final renaming of encrypted files is done using the same method as in LOCKBIT v2.0.

Money Message Suspected to be Leveraging Stealer Logs

Money Message ransomware was discovered in March 2023. After analyzing ransomware binaries, we noticed they contained admin credentials in the configuration, which were then used to target network resources. Based on this, we suspect the threat actors might leverage stealer logs in their operation.

Trigona Ransomware Deployed via Compromised Microsoft SQL Servers

Threat actors are installing Trigona ransomware by exploiting vulnerable and publicly accessible Microsoft SQL (MS-SQL) servers, which results in the encryption of all the files present on them. TAs exploit easy-to-guess login credentials through brute-force or dictionary attacks to gain unauthorized access to MS-SQL servers.

Ransomware Using AuKill Tool to Disable EDR

The AuKill defense evasion tool takes advantage of an old version of the driver utilized by Microsoft's Process Explorer version 16.32. This method is often called a "Bring Your Vulnerable Driver" (BYOVD) attack. AuKill incapacitates EDR (Endpoint Detection and Response) processes, allowing the tool to deploy either ransomware or a backdoor onto the targeted system.

AuKill tool has been utilized in at least three ransomware incidents to disable the target's security measures and execute the ransomware. Two of these incidents occurred in January and February, where the attackers deployed Medusa Locker ransomware after employing the AuKill tool. In another incident in February, the tool was utilized just before deploying LOCKBIT ransomware.

Ransomware Groups Updating Their Variants

Alphv/BlackCat

CRIL discovered a new defense evasion capability in Alphv/BlackCat Ransomware. The updated kernel driver, signed by Microsoft, was used to manipulate, halt, and terminate processes on targeted endpoints. The attackers used a known driver, but Microsoft signed an alternative driver. The group exploited this vulnerability to gain high-privilege access to the Windows operating system and exploit enhanced protection through Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) technologies. To evade detection and maintain offensive capabilities, TAs continue to use rootkits, which conceal malicious code, subvert defenses, and operate covertly. Rootkits can obscure complex targeted attacks, undermining defenses before launching payloads within victim environments.

Mallox

Mallox ransomware has begun to use the ".malox" file extension, using BatLoader to deploy the ransomware binary. This method eliminates the need for a downloader and injects the ransomware payload into a batch script, injected into "MSBuild.exe", without saving it on disk. This modification suggests that the Mallox ransomware group is actively modifying its tactics, techniques, and procedures to enhance evasiveness and maintain its malicious activities.

The Proliferation of Linux Variants

Recently, several organizations have adopted cloud computing and virtualized environments, leading to a rise in ransomware attacks targeting Linux and cloud systems. In addition to this attack, an upsurge of various types of Linux malware targeting virtual machines has also been observed.

Akira

Initially focused on Windows systems, Akira Ransomware expanded its target range to include a Linux 64-bit variant in May 2023. Upon execution, the Akira ransomware loads a pre-determined list of file extensions and RSA public key that it intends to target and encrypt.

Trigona New Linux Variant

Trigona ransomware emerged in October 2022 and has been active since its inception. It targets compromised MSSQL servers using brute force methods, and a Linux version of Trigona was discovered in May 2023, showing similarities to its Windows counterpart. Trigona is believed to be associated with CryLock ransomware due to similarities in tools, tactics, and procedures. The highest number of Trigona ransomware detections occurred in the United States, India, Israel, Turkey, Brazil, and Italy.

The primary targets of Trigona attacks were the Technology and Healthcare industries. Trigona exploits ManageEngine vulnerability CVE-2021-40539 and uses previously compromised accounts from network access brokers.

Activities Across Cybercrime Forums

Cybercrime Forums remained active for several ransomware groups in Q2-2023, a continuing trend observed from the last quarter.

Cyclops

The Cyclops Ransomware operators were offering an information stealer malware in early June, which had the capability to infect all the major operating systems. Cyclops is a Go-based stealer designed to capture details such as OS and device information and extract files of interest. The group advertised itself on forums offering to sell the malware, as described in the figure below.

Figure 17: Cyclops admin post

CRIL subsequently observed that the group's website went live with the names and compromised data of the three victims listed.

NoEscape Ransomware

CRIL discovered threat actor 'N0_Esc4pe' offering Ransomware-as-a-Service (RaaS) dubbed 'NoEscape' on an underground forum. The ransomware is developed in C++ and uses the triple-extortion technique to extort victims. The actor also offers a special service for DDoS/Spam for USD 500k, which can be used to pressurize targeted companies for payouts. The ransom is demanded after spreading throughout the network, and criminals may sell stolen data or publish it online. The actor does not work in Commonwealth of Independent States (CIS) countries, suggesting a possible origin from Russia or CIS. The actor seeks affiliates with an undisclosed hiring mechanism and provides a TOX address for contacting them about the RaaS.

Figure 18: TA N0_Esc4pe's advertisement on the forum

Threat Actors Affiliated to Nebula Ransomware Advertise RaaS and Sells Compromised Access

A threat actor (TA) operational on the now-defunct Exposed forum was observed to be selling access to a Japanese telecommunication company. In their previous activities, the TA was observed to be hiring members for their Nebula ransomware group.

Figure 19: Nebula Ransomware Group member selling compromised access

Ransomware Groups Leverage New Underground Forum for Recruitments and Data Sale

As predicted in our previous report, the ransomware groups were observed advertising the hiring of affiliates and offering their RaaS on the now-defunct 'Exposed' forum. Medusa, Nebula, Providence Worldwide, and an unnamed RaaS provider had posted different requirements for language competencies in Rust, GoLang & C, to offering 70% as payouts.

Notably, most of these groups encouraged company employees to join them as Initial Access Brokers or provide insider information. All of them have provided alternate secured communication channels for communication.

We also observed the BlackByte ransomware group promoting the sale of compromised data and leaking sample data. The forum administrators promoted these services by adding a distinct sub-forum for Ransomware. This is a new tactic adopted by the administrators to upmarket their forum. Similar activity began in now-defunct BreachForums in Sep 2022 and XSS, which was previously strictly restricted by their forum administrators.

Ransomware Threat Predictions

- Governments worldwide are tightening the noose on the ransomware groups to prevent financial and data loss in their industries. Despite that, the proliferation of new ransomware groups remains challenging for businesses to safeguard their operations. Even governments are adopting stricter regulations for such incident reporting on affected organizations. Ransomware groups may use this situation to adopt new extortion techniques, thereby pressuring the affected entity to pay the ransom. Hence, considering the increase in number of ransomware attacks, we anticipate an increase in ransomware payments in 2023.

- We may observe a growth in ransomware attacks on businesses providing critical services related to Energy and Transportation & Logistics sectors.

- As predicted earlier about the increase in weaponization of the latest vulnerabilities by ransomware groups, we have observed that ransomware groups have been quick to mass exploit vulnerabilities such as GoAnywhere and MOVEit, just after their announcement and before the security teams are able to patch those vulnerabilities. This indicates automation of reconnaissance operations for identifying potential victims.

- This also validates our predictions from Q1-2023 that ransomware groups will quickly adopt AI to automate their operations. Further aggressive use of AI is anticipated for reverse engineering the security patches of critical vulnerabilities to promptly exploit more Zero-days.

- As witnessed a pause in the ransomware operations of LOCKBIT in the later part of this quarter, we anticipate similar tactics being adopted by other prevalent ransomware groups to reorganize their groups, improve their variants or adopt new techniques to facilitate their adoptions and evade detection by LEA.

- Since the emergence of new ransomware groups is on a new high due to the disintegration of old ransomware groups, we may witness further increased activity in the ransomware landscape. We have observed that the operational security practiced by the new groups is relatively low. Also, the governments and LEA are promoting bounties for apprehending persistent ransomware groups. Therefore, we may witness an increase in takedowns of ransomware groups.

- Related to the above, the ransomware groups are also expected to employ other detection evasive techniques such as restricting the use of leak sites and realigning their activities under new identities.

- During Q2, we observed that threat actors had highlighted the significance of vulnerabilities affecting Managed File Transfer software products by weaponizing critical flaws like CVE-2023-34362 to exfiltrate organizations' confidential data. Therefore, there is a strong likelihood that threat actors will actively seek for and exploit new vulnerabilities or flaws affecting such technologies.

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

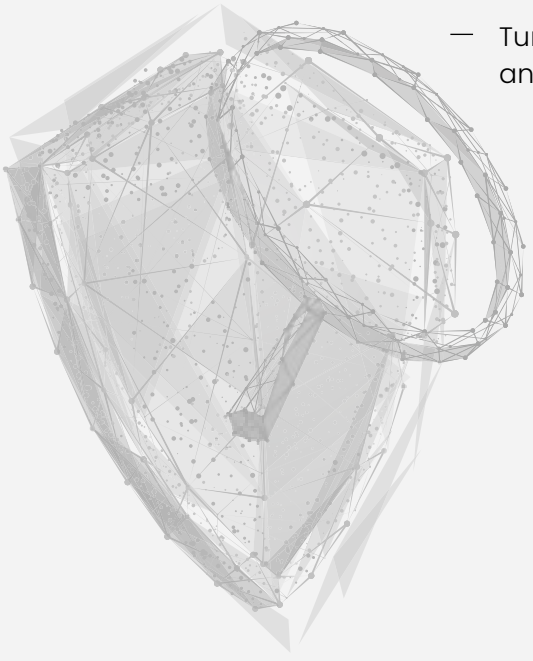
  - CVE-2023-28311
  - CVE-2023-23376
  - CVE-2023-20867
  - CVE-2023-21554
  - CVE-2023-27997

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 reputed 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.



References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-131a

https://www.cisa.gov/sites/default/files/2023-06/aa23-165a_understanding_TA_LOCKBIT.pdf

https://www.bleepingcomputer.com/news/security/windows-zero-day-vulnerability-exploited-in-ransomware-attacks/

https://www.crowdstrike.com/blog/hypervisor-jackpotting-lack-of-antivirus-support-opens-the-door-to-adversaries/

https://thehackernews.com/2023/05/inside-qilin-ransomware-affiliates-take.html

https://thehackernews.com/2023/05/new-michaelkors-ransomware-as-service.html

https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-2nd-2023-whodunit/

https://www.bleepingcomputer.com/news/security/new-qbot-email-attacks-use-pdf-and-wsf-combo-to-install-malware/

https://research.checkpoint.com/2023/rorschach-a-new-sophisticated-and-fast-ransomware/

https://www.mandiant.com/resources/blog/alphv-ransomware-backup

https://www.bleepingcomputer.com/news/security/microsoft-sql-servers-hacked-to-deploy-trigona-ransomware/

https://twitter.com/Unit42_Intel/status/1653760405792014336

MalasLocker ransomware targets Zimbra servers and demands charity donations (https://www.bleepingcomputer.com/news/security/malaslocker-ransomware-targets-zimbra-servers-demands-charity-donation/)

MalwareHunterTeam on Twitter: “Looks is another new ransomware gang: Rhysida. https://twitter.com/malwrhunterteam/status/1658829565215604738

ABOUT US

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