CYBLE

Q1-2023
Ransomware Report

TABLE OF CONTENTS

EXECUTIVE SUMMARY **3**

QUARTERLY RANSOMWARE OUTLOOK **6**

GLOBAL RANSOMWARE THREAT LANDSCAPE **7**

MICROANALYSIS OF RANSOMWARE ACTIVITIES **12**

RANSOMWARE SECTORAL IMPACT **14**

EVOLVING RANSOMWARE THREAT PROFILE **17**

WEAPONIZED VULNERABILITIES OF Q1-2023 **20**

CAPRICIOUS RANSOMWARE TECHNIQUES **22**

RANSOMWARE THREAT PREDICTIONS **26**

HOW TO PROTECT YOURSELF FROM RANSOMWARE ATTACKS **27**

REFERENCES **28**

ABOUT US **30**

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 Q1-2023 to preempt the associated risks of the Ransomware Groups discussed herein.

The first quarter of 2023, as predicted by CRIL, witnessed an unprecedented rise in ransomware attacks. Flagitious groups like LOCKBIT, CL0P, and Alphavm orchestrated these huge blobs in the ransomware threat landscape. Joining the foray Royal and Play ransomware groups persisted in an execrable manner.

As prognosticated by us last quarter, the CL0P ransomware group quickly weaponized the GoAnywhere Managed File Transfer (MFT) zero-day vulnerability and claimed to encrypt the data of **105 organizations across 22 countries**. Reports suggest that over **130 organizations were targeted by CL0P** in this zero-day attack.

In a coordinated operation, Law Enforcement Agencies (LEA) obliterated the Hive ransomware group that had been nefariously expanding its operations since June 2021. The FBI, with LEAs from Germany and Netherlands, initially infiltrated the ransomware group's operations and provided decryption keys to nearly 1,300 victim organizations around the globe. Subsequently, they seized the entire infrastructure of Hive, rendering them ineffective.

The massive surge in ransomware attacks dwindled the supply chain security of the Manufacturing, Technology, Energy, Healthcare, and Food & Beverages sectors. Further, CRIL observed a peculiar rise in attacks on industries involved in Integrated Control Systems (ICS) supply chains, opening Pandora's box for future attacks on Critical Infrastructure.

As speculated in the previous year, this increase in ransomware attacks has not spared even small corporations. We saw a surge in demand for cyber insurance in the US and Europe. The heightened cyber risk adding to business risks has pushed the cyber insurance costs by nearly **100% from last year**.

EXECUTIVE SUMMARY

THIS REPORT ENCAPSULATES THE FOLLOWING MAJOR FINDINGS FROM Q1-2023:

- 783 victims were publicly disclosed by ransomware groups, with United States (US) corporations continuing to be the most affected.
- The United Kingdom (UK) and France witnessed a steep increase of 81% and 50%, respectively, in ransomware attacks.
- The majority of high-income organizations were targeted in the Manufacturing, Energy & Utilities, and BFSI sectors.
- The BFSI, Healthcare, and Education sectors suffered over 30% more attacks in Q1-2023 as compared to Q4-2023.
- LOCKBIT claimed 86% more attacks and remained the most deplorable ransomware group, undermining the cyber integrity of 265 entities in Q1-2023.
- We observed the emergence of new ransomware groups – Dark Power, DarkB!t, MortalKombat, Money Message, and Nevada in this quarter.
- CL0P ransomware group has compromised over 100+ organizations by exploiting the high-severity zero-day vulnerability, CVE-2023-0669, GoAnywhere MFT.
- Magniber ransomware was reported exploiting the Windows SmartScreen Security Feature Bypass Vulnerability (CVE-2023-24480), confirming our predictions from Q4-2022 that ransomware groups may resort to exploiting more zero-days.
- Capricious techniques of ransomware groups in Q1-2023 provide further insights into their operations and indications about the evolving ransomware threat landscape in the year ahead.

EXECUTIVE SUMMARY

Total victims - 783

Active Ransomware Groups - 25

viz-a-viz **29 last quarter**

MOST AFFECTED COUNTRIES (TOP 5)

35% ▲

United States - **344**

81% ▲

United Kingdom - **58**

15% ▲

Canada - **37**

50% ▲

France - **27**

24% ▲

Germany - **26**

MOST ACTIVE RANSOMWARE GROUPS (TOP 5)

265

105

99

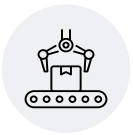
67

40

MOST IMPACTED INDUSTRY SECTORS (TOP 5)

Professional Services - 109

53% ▲



Manufacturing - **67**

13% ▲

Construction - **58**

18% ▲

Education - **57**

31% ▲

IT & ITES - **47**

=

QUARTERLY RANSOMWARE OUTLOOK

CRIL identified 783 ransomware victims in Q1-2023 compared to 594 in Q4-2022 – a 32% growth in attacks Quarter-over-Quarter (Q-over-Q) and 47% Year-over-Year (Q1-2022).

Our ransomware victim-to-country ratio data indicates that over **50% of the victim organizations** were primarily concentrated in 3 countries - **the United States (US), the United Kingdom (UK), and Canada.**

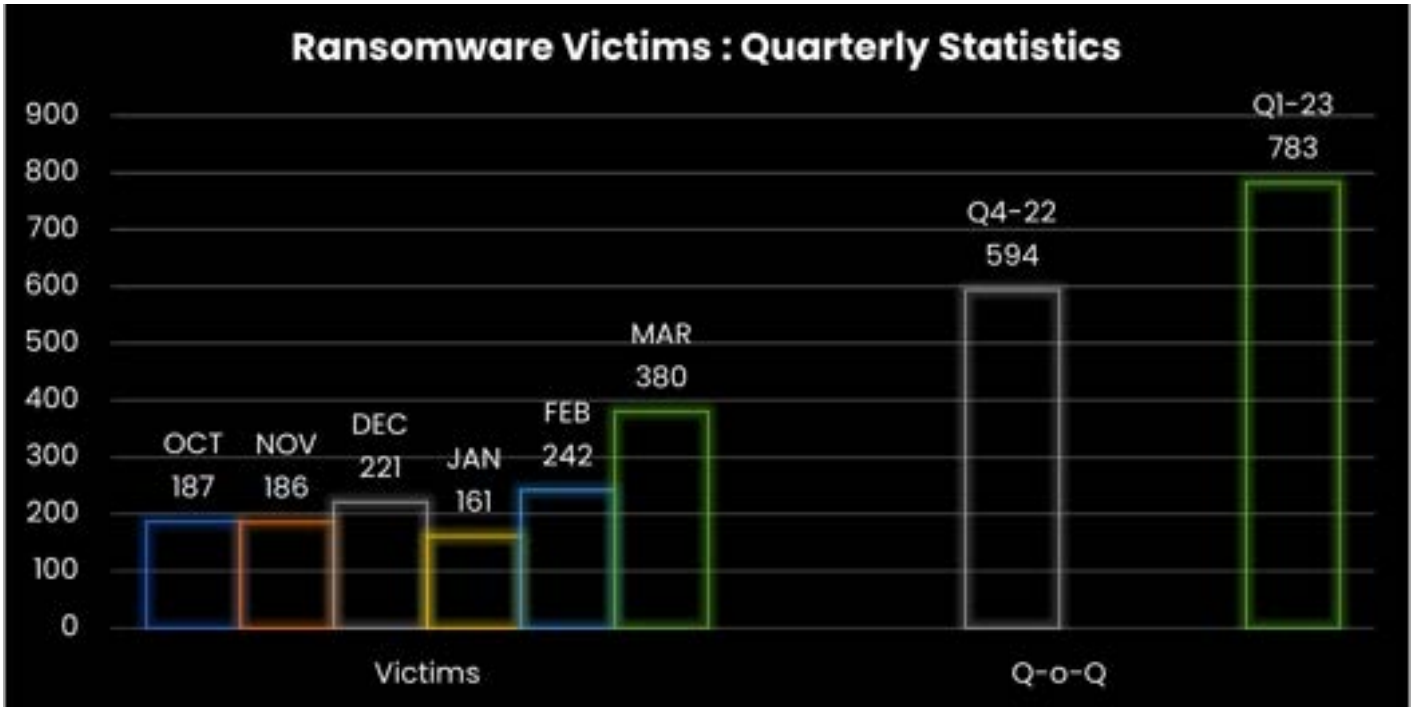
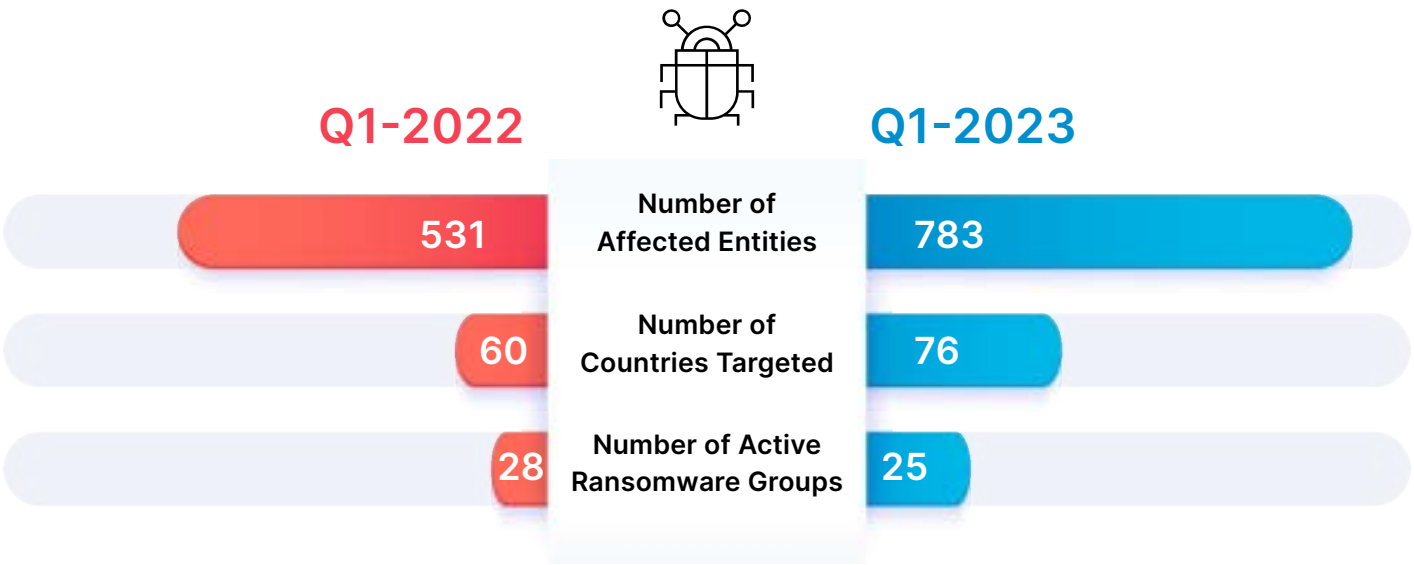


Figure 1 - Comparative analysis of ransomware activities Q-over-Q

WHAT HAS CHANGED FROM Q1-2022 TO Q1-2023



GLOBAL RANSOMWARE THREAT LANDSCAPE

CRIL observed that the ransomware attack footprint grew from 69 countries in Q4-2022 to 76 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 Q1-2023. As predicted, ransomware attacks engulfed more and more entities in Asia & Oceania than ever before.

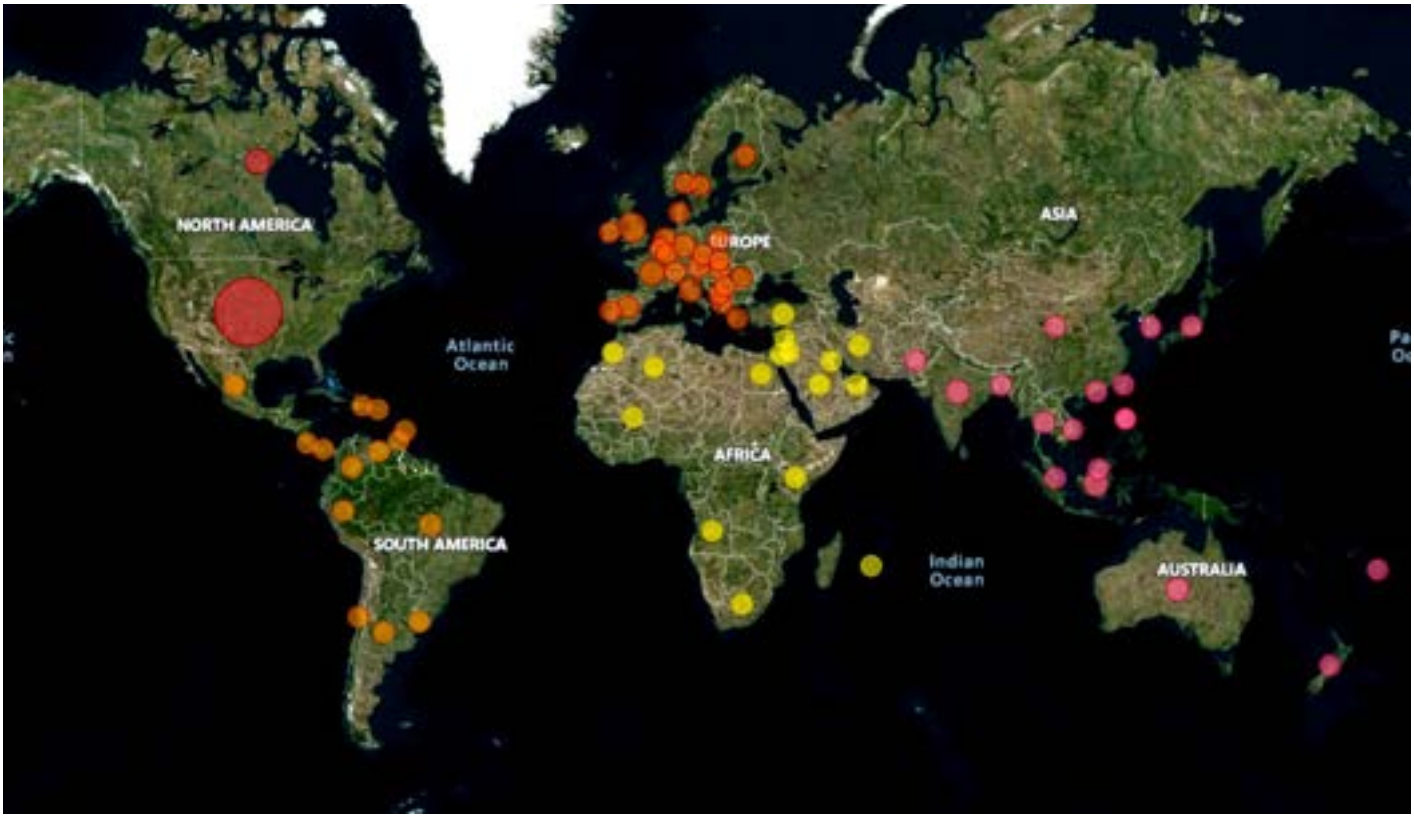


Figure 2: Global Distribution of Ransomware-Affected Organizations

GLOBAL RANSOMWARE THREAT LANDSCAPE

AMERICAS

The Americas was the most targeted region, with over 430 ransomware victims this quarter, in contrast to 300, in Q4-2023. This region accounts for over 54% of ransomware victims disclosed publicly in Q1-2023. 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 Q1-2023.

Figure 3: Geographical distribution of Ransomware victims in the Americas

Ransomware attacks in the Americas have particularly impacted Professional Services. The Healthcare sector has emerged to be among the 5 most affected sectors this quarter, besides Construction, Education, and Manufacturing. LOCKBIT, CL0P, ROYAL, ALPHV, and Black Basta were the groups most actively involved in attacking the region, alongside 16 other groups.

GLOBAL RANSOMWARE THREAT LANDSCAPE

EUROPE & CIS

European organizations were the second most affected after the Americas, with 195 ransomware victims – an increase of 32% from the previous quarter. The United Kingdom suffered the highest volume of ransomware attacks, with 58 victims. France replaced Germany to record the second highest number at 27, and Germany with 26 reported incidents.

The figure below showcases the geographical distribution of major ransomware activities across Europe and the CIS region in Q1-2023.

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

Professional Services continued to be the worst-hit sector in the region. This quarter, we observed that ransomware groups also aggressively targeted Manufacturing and IT & ITES, a shift from previous attempts to target the Transportation & Logistics sector. Apart from these, Construction and Education remained the most affected sectors in this region. LOCKBIT, CL0P, ALPHV, ROYAL, and Play were particularly nefarious in this part of the world.

GLOBAL RANSOMWARE THREAT LANDSCAPE

ASIA & OCEANIA

Asia & Oceania was the third most targeted region, with 115 victims alone at the beginning of the year. This quarter, ransomware attacks primarily focused on Manufacturing, Energy & Utilities, IT & ITES, Professional Services, and Healthcare. In this region, 18 ransomware groups were observed to be active, **including LOCKBIT, Alphavm, CL0P, and Medusa being the prominent ones.**

Indonesia and India emerged as the region's most targeted countries, replacing Australia and Taiwan.

The figures below reflect the distribution of major ransomware activities across this region in Q1-2023.

COUNT OF VICTIMS

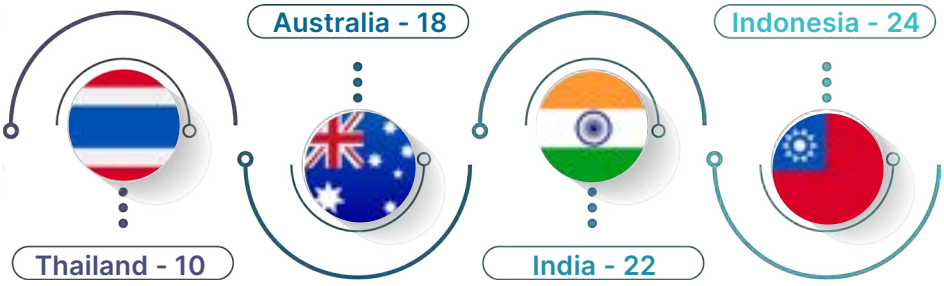


Figure 5: Geographical distribution of Ransomware victims in Asia & Oceania

GLOBAL RANSOMWARE THREAT LANDSCAPE

META

The Middle East, Turkey, and Africa (META) region **saw the least number of ransomware attacks.** While over 17 countries in this region were targeted, the majority of attacks were reported in Turkey and the United Arab Emirates, followed by Israel.

Figure 6: Geographical distribution of Ransomware victims in META

LOCKBIT has consistently been the most active ransomware group in the region from Q3-2022. There are over 8 ransomware groups active in the region, with CL0P and Dark Power being the next most active after LOCKBIT.

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

MICROANALYSIS OF RANSOMWARE ACTIVITIES

CRIL observed 25 active ransomware groups this quarter.

New ransomware groups identified this quarter were – Dark Power, DarkBit, and Money Message. The other two newly discovered ransomware groups MortalKombat and Nevada, have not disclosed their victims publicly. Further, we observed nil activities from previously active ransomware groups – Bully Gang, Cuba, LV, Nokoyawa, Onyx, Putin Team, Quantum Blog, Relic, REvil, and Unsafe in Q1-2023.

NEW RANSOMWARE GROUPS OBSERVED TO BE ACTIVE IN Q1-2023

- DARKBIT
- DARK POWER
- MONEY MESSAGE
- MORTALKOMBAT
- NEVADA

The figures below indicate a comparative analysis of ransomware attacks by various gangs Quarter-over-Quarter.

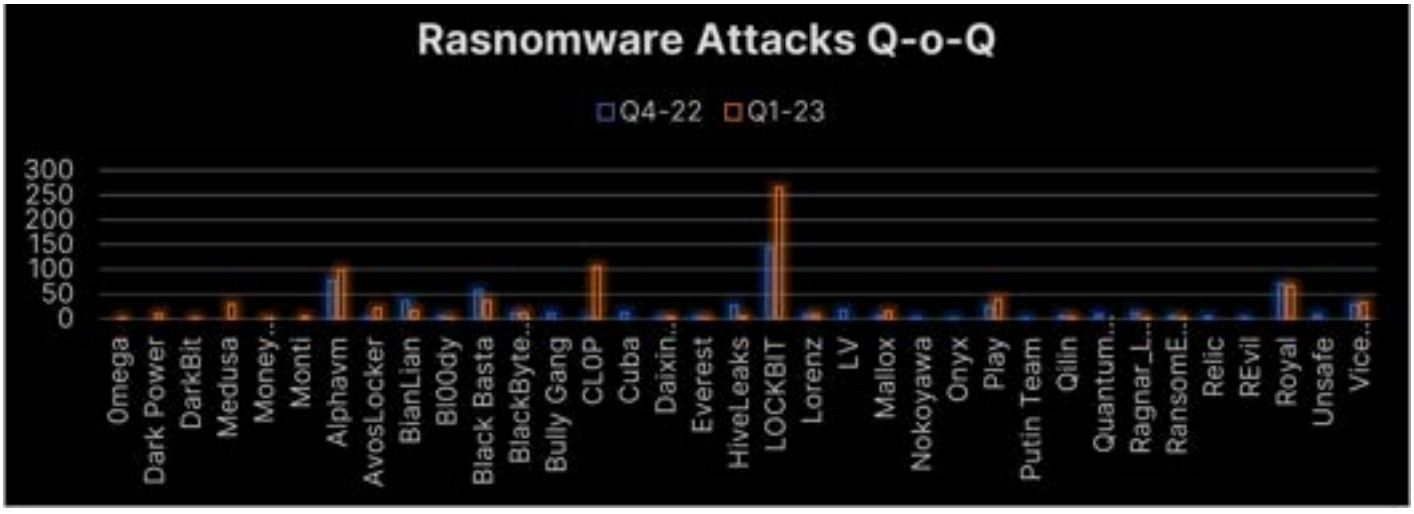


Figure 7: Ransomware attacks Quarter-over-Quarter

MICROANALYSIS OF RANSOMWARE ACTIVITIES

- LOCKBIT was the most active ransomware group, targeting 265 organizations in Q1-2023, an increase of over 86% compared to Q4-2022. These affected entities were primarily from the Professional Services, Construction, Manufacturing, Transportation & Logistics, and Government & LEA sectors.
- Since its emergence, LOCKBIT has disclosed the highest number of victims ever in a single quarter.
- LOCKBIT's 34% of victims had the highest number of victims from the US, followed by more attacks in France, the United Kingdom, and Canada; similar to Q4-2022, when LOCKBIT was highly prevalent in the United States and had most of its victims from there.

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

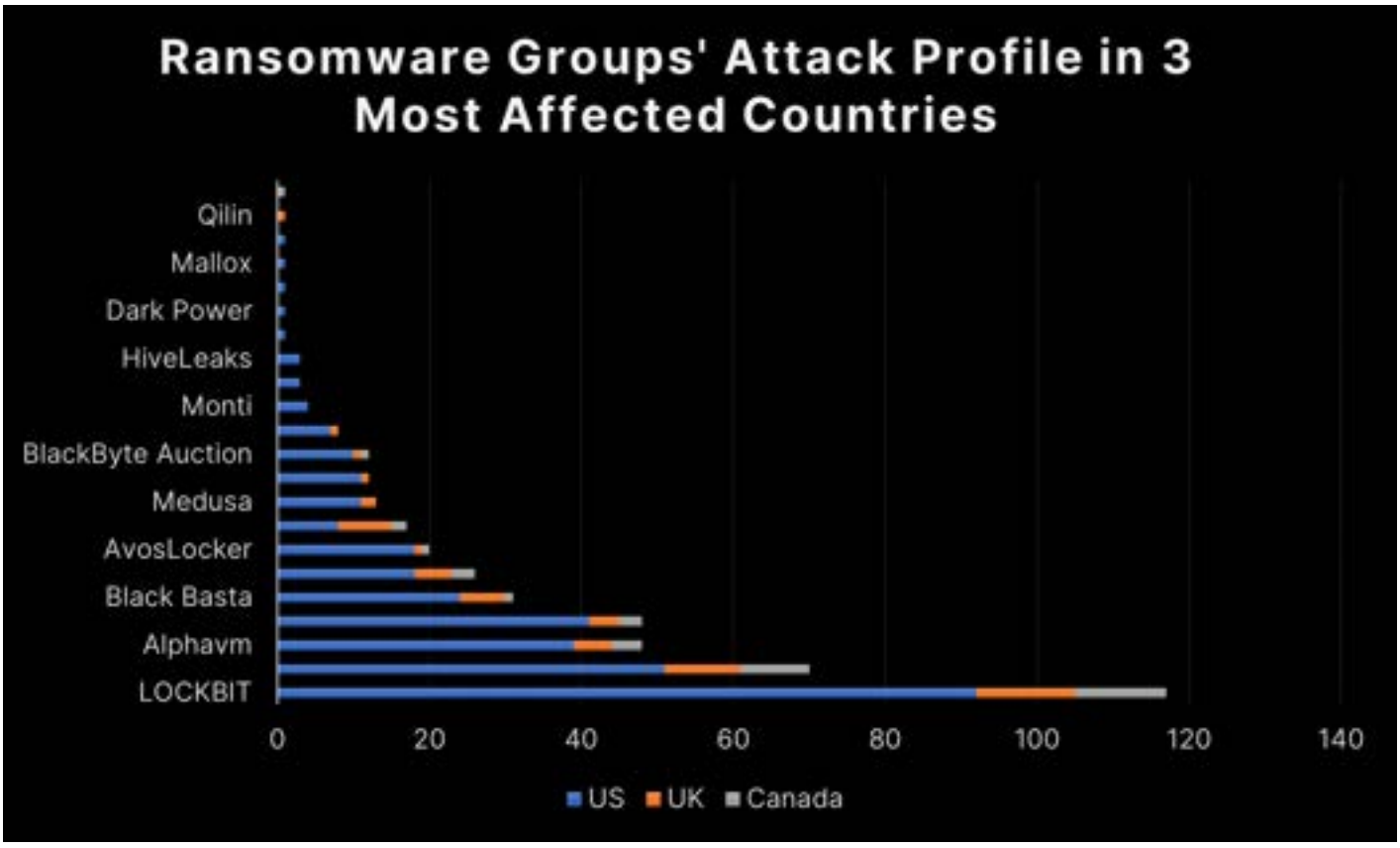


Figure 8: Ransomware Group's attack profiles in the 3 most affected countries

RANSOMWARE SECTORAL IMPACT

CRIL observed a slight change in the Ransomware group's sectoral attack footprint in Q1-2023. **The Education sector,** which had earlier replaced Healthcare in Q4-2022 to emerge in the 5 most-affected sectors, **moved to the fourth position replacing IT & ITES in Q1-2023.** LOCKBIT, Alphavm, Play, and Royal were observed to primarily target this sector in the first quarter of 2023.

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.

LOCKBIT has been actively targeting US companies in the **Professional Services, Manufacturing, and Construction sectors.**

In Q1-2023, there was **a 53% increase in attacks on the Professional Services sector** compared to Q4-2022.

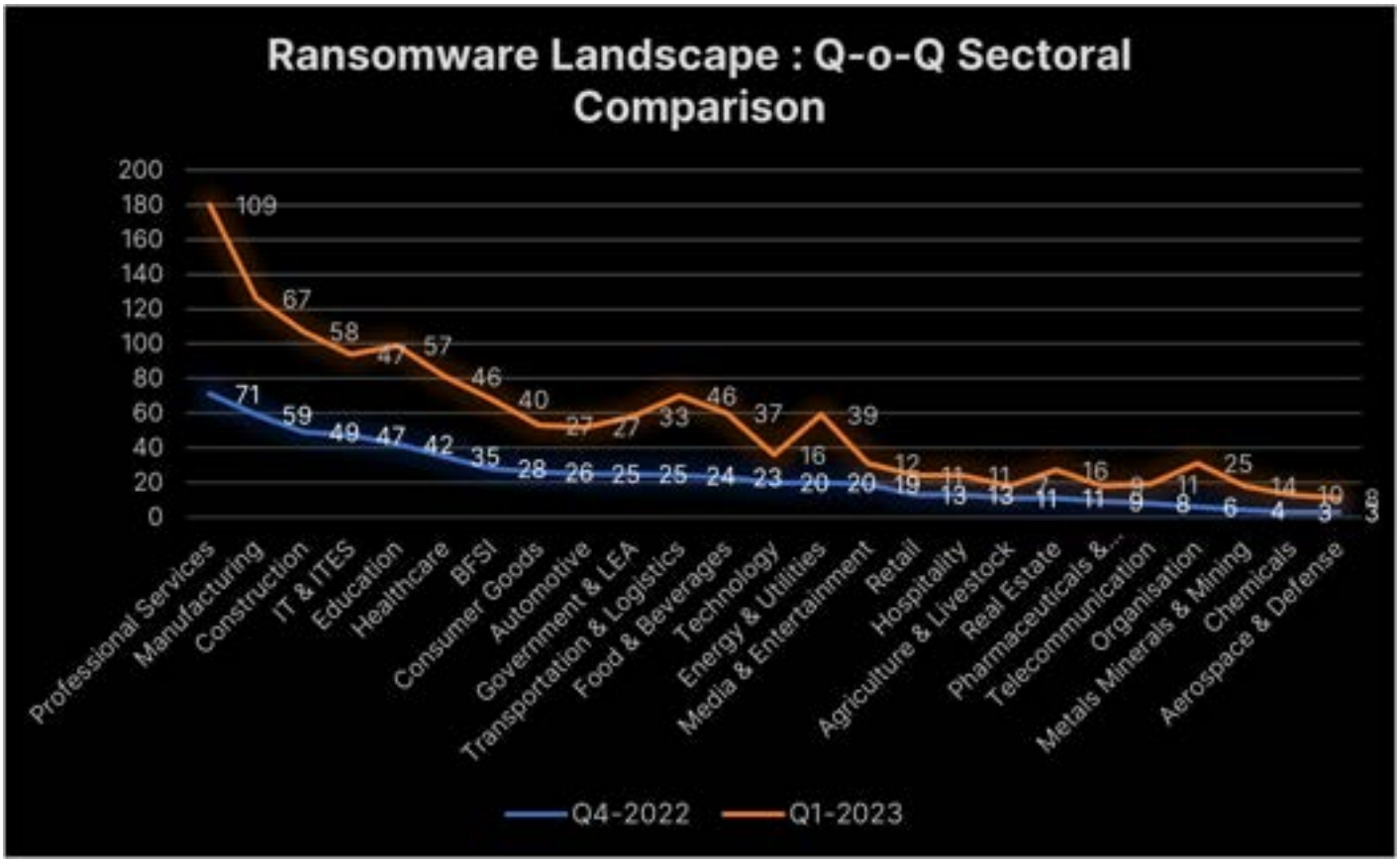


Figure 9: Ransomware Landscape : Q-o-Q Sectoral Comparison

RANSOMWARE SECTORAL IMPACT

In Q1-2023, the countries that were adversely affected in the five most targeted industries were:

PROFESSIONAL SERVICES	MANUFACTURING	CONSTRUCTION	IT & ITES	EDUCATION
United States	United States	United States	United States	United States
United Kingdom	United Kingdom	United Kingdom	Germany	United Kingdom
Canada	France	Germany	India	Australia
Germany	Germany	Canada	Turkey	Brazil
Italy	Singapore	Australia	Spain	Germany

RANSOMWARE SECTORAL IMPACT

REPEATED RANSOMWARE ATTACKS IN Q1-2023:

- A Canadian Transportation & Logistics service provider suffered an attack from the Royal Ransomware Group in January 2023, earlier compromised by the AvosLocker ransomware group in June 2022
- A US-based Risk and Compliance Solutions service provider, earlier targeted by Daixin Team in January 2023, was compromised by LOCKBIT in February 2023
- Mallox targeted an Indian conglomerate in January 2023, which was earlier targeted by XING LOCKER in April 2021
- Royal ransomware group targeted a Germany-based Manufacturer in February 2023, which was previously attacked by Grief in October 2021
- A US retail company was targeted by LOCKBIT in February 2023 and earlier by Marketo in May 2021
- LOCKBIT targeted a US-based Manufacturer of Drilling & Testing Equipment in February 2023 and earlier by Pysa ransomware group in June 2021
- LOCKBIT targeted a Thailand-based Airline company in February 2023, which was previously targeted by Alphavm in November 2022
- A city institution in the US was targeted twice in March 2023 but by different groups – LOCKBIT and Play
- A Taiwanese Real Estate company was targeted again by LOCKBIT in March 2023. The group had earlier targeted the same entity in October 2021
- Royal attacked an Australia-based Home Loan provider targeted by Vice Society in March 2023 and December 2022
- AvosLocker targeted a Law-firm based in the US in March 2023, which Black Basta previously targeted in December 2022
- A US-based College previously targeted by Quantum Blog in January 2022 was compromised by Vice Society in March 2023
- A Brazil-based Cloud Computing and IT Outsourcing company was compromised by LOCKBIT in March 2023 and by Grief in September 2021

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 attack.

Cyble Research & Intelligence Labs worked on profiling new ransomware groups in Q1-2023 to forewarn our readers about their activities in the evolving ransomware threat landscape.

DARKBIT

DarkBit ransomware group is understood to be ideologically aligned in selecting their victims. The DarkBit Ransomware, compiled as a Go binary, targets Windows operating systems and employs multithreading for its encryption process.

Figure 10: DarkBit's Tor Website

EVOLVING RANSOMWARE THREAT PROFILE

MORTALKOMBAT

MortalKombat ransomware is a variant of the Xorist family of ransomware that was initially detected in January 2023 and provides a builder tool for TAs to personalize the malware. Xorist has been decryptable at no cost since 2016. According to security analysts, this specific ransomware is not particularly advanced since it also targets system files and applications, which are usually avoided to prevent the system from becoming unstable, thereby reducing the probability of a successful Ransomware attack.

However, reports suggest that TAs are employing MortalKombat ransomware along with the Laplas Clipper in a new campaign targeting corporations in the US, UK, Turkey, and the Philippines.

MONEYMESSAGE

Observed during March 2023, Money Message is a newly discovered ransomware strain that has victims worldwide. The group is capable of encrypting network shares, and its approach to target network shares resembles that of the Maze and Petya ransomware groups.

Researchers observed that the group uses the C++ language for the encryptor. An embedded JSON file decides on an encryption method for a gadget. It utilizes a double extortion technique to target its victims, which involves exfiltrating the victim's data before encrypting it.

The group has already targeted several high-profile organizations, including billion-dollar companies. This impact is further highlighted in a recent incident when the group demanded a ransom of USD 500,000.

MIMIC RANSOMWARE

Mimic is a new strain of ransomware that was discovered by security researchers. It targets Russian and English-speaking users and was first observed in June 2022. The ransomware abuses the APIs of a legitimate tool called "Everything", which is a Windows filename search engine developed by "Voidtools". Mimic is equipped with multiple capabilities, such as deleting shadow copies, terminating multiple applications and services, and using the "Everything32.dll" functions to identify files that are to be encrypted. Mimic shares similarities in its code with the Conti ransomware, whose source code was made public in March 2022.

EVOLVING RANSOMWARE THREAT PROFILE

BLACKSNAKE RANSOMWARE

CRIL discovered BlackSnake ransomware in this quarter, based on the Chaos ransomware source code. The developers of this ransomware added a clipper module directly into the file to target cryptocurrency users, which is a departure from the usual approach of having a separate file for the clipper. The ransomware code reveals that the TAs of this ransomware intend to exclude systems located in Azerbaijan or Turkey, indicating their probable affiliation.

DARK POWER RANSOMWARE

Dark Power emerged in the ransomware scene in January 2023 and utilized the Nimcrypto library to conduct its cryptographic operations, with the specific algorithm used for encryption being AES CRT. Moreover, the ransomware disables other backup and anti-malware services, ultimately increasing the likelihood that the victim will pay the demanded ransom.

NATIONAL HAZARD AGENCY (NHA)

The new ransomware group emerged from the shadows of LOCKBIT ransomware group and was reported in March this year. The NHA uses the LOCKBIT builder and as per reports on social media, was allegedly initiated by a LOCKBIT affiliate going by the moniker 'Bassterlord'. Bassterlord aka FishEye claimed training the new ransomware group members to pave way for their exit from LOCKBIT. Basserlord had been a prominent initial access broker before becoming a ransomware affiliate.

WEAPONIZED VULNERABILITIES OF Q1-2023

WINDOWS SMARTSCREEN SECURITY FEATURE BYPASS VULNERABILITY (CVE-2023-24880)

CVE-2023-24880, discovered on February 15, 2023, allows an attacker to evade Mark of the Web (MOTW) defenses by using malicious files that induce a loss of integrity and availability of security features such as Protected View in Microsoft Office, which rely on MOTW tagging.

CVE-2023-24880 coexists with CVE-2022-44698, discovered in December 2022, highlighting another Windows SmartScreen security feature bypass, this time using malformed initialed JavaScript files.

Magniber ransomware was also reportedly exploiting the Windows SmartScreen Security Feature Bypass Vulnerability (CVE-2023-24480), using malicious MSI files signed with a specific Authenticode signature to bypass this security feature.

Magniber is considered a successor of Cerber ransomware and has been active since the second half of 2017. The group has expanded its attack footprint from South Korea to other Asian and a few European countries. It has been reported to be particularly active since the start of 2023.

CVE-2023-0669

Published on February 06, 2023, CVE-2023-0669 is a pre-authentication command injection vulnerability targeting GoAnywhere MFT. An attacker can leverage the flaw to remotely execute code on vulnerable instances of GoAnywhere MFT.

The **CL0P** ransomware group has been observed to have compromised over 100 organizations by exploiting this high-severity zero-day vulnerability.

CVE-2022-47986

Published on February 17, 2023, CVE-2022-47986 targets IBM Aspera Faspex, an application used by multiple organizations, allowing employees to quickly exchange files. A remote attacker can leverage this vulnerability to execute arbitrary code on the system caused by a YAML deserialization flaw.

IceFire ransomware was reported to be exploiting CVE-2022-47986 to target Linux-based systems.

WEAPONIZED VULNERABILITIES OF Q1-2023

CVE-2021-21974

Published on February 24, 2023, CVE-2021-21974 is a heap-overflow vulnerability in VMware ESXi. The vulnerability can be leveraged by a Threat Actor (TA) residing within the same network segment as ESXi, who has access to port 427 and may be able to trigger the heap-overflow issue in OpenSLP service resulting in Remote Code Execution.

ESXiArgs ransomware was reported to be exploiting CVE-2021-21974 to target unpatched ESXi servers.

CVE-2021-31207, CVE-2021-34473, CVE-2021-34523

Published in 2021, these three vulnerabilities have a CVSS v3 score of 7.2, 9.8, and 9.8, respectively, and target the Microsoft Exchange Server.

Researchers discovered that Ransomware groups, including Hive, Babuk or Babyk, and AvosLocker, actively exploited critical flaws and vulnerabilities.

OWASSRF FLAW (INCLUDING CVE-2022-41080 & CVE-2022-41082)

Discovered in December 2022, the OWASSRF flaw is exploited by leveraging a chain of vulnerabilities, including CVE-2022-41080 and CVE-2022-41082, to enable RCE through Outlook Web Access.

The flaw is actively exploited exploitation by both **Cuba and Play** ransomware groups to compromise organizations.

CVE-2021-27877, CVE-2021-27876, CVE-2021-27878

These three vulnerabilities, published on March 1, 2021, target Veritas Backup Exec, a data protection software product that supports virtual, physical, and cloud platforms.

Researchers discovered that ALPHV/BlackCat ransomware affiliates leveraged the high-severity flaw to establish initial access to the target network.

CAPRICIOUS RANSOMWARE TECHNIQUES

Ransomware variants are adopting novel techniques to extort ransom and evade detection. Some of the new techniques that we observed in Q1-2023 were:

BIANLIAN FOCUSES ON EXTORTION

BianLian emerged in July 2022 and has targeted numerous prominent organizations. Recently, the ransomware group has altered its approach from encrypting victims' files to exclusively extracting data from compromised networks and using it for extortion purposes. This change in strategy could be due to a drop in ransom payments. To economize their operations, the group is focusing on extorting their victims.

CATB RANSOMWARE PERFORMING DLL HIJACKING

CatB Ransomware is persistently observed using DLL hijacking via Microsoft Distributed Transaction Coordinator (MSDTC) to extract and execute ransomware payloads and avoid detection.

The CatB ransomware is distributed in the form of two DLLs, with the first one being a dropper DLL that conducts initial evasive checks and then drops and executes the second DLL. This second DLL, in turn, contains the actual ransomware payload.

LORENZ ADOPTS NOVEL EXTORTION TECHNIQUE

Ransomware groups continuously modify their extortion techniques to pressure their victims into paying the ransom. During this quarter, CRIL observed the Lorenz ransomware group adopting advanced extortion tactics, quite similar to the one adopted by LOCKBIT and ALPHV in 2022.

On their leak site, the Lorenz ransomware group was observed to be mentioning domain names similar to the victim's domain name. Upon visiting these domains, we observed that they reflect the company's compromised data and reveal information about the negotiations between the group and the victim organization.

In one such instance on January 10, 2023, the Lorenz ransomware group apparently also contacted the victim's clients and employees regarding the ransomware attack.

Figure 11: Excerpt from Lorenz leak site highlighting the mirrored domain and leaked negotiations chat

CAPRICIOUS RANSOMWARE TECHNIQUES

RANSOMWARE GROUPS UPDATING THEIR VARIANTS

LOCKBIT

As contemplated in the Q4-2022 report, the LOCKBIT ransomware group adopted a newer version known as 'LOCKBIT Green' after its LOCKBIT 3.0 (aka LOCKBIT Black) builder was leaked, and their source codes were revealed to Canadian LEA following an arrest of its Russian affiliate in Ontario.

LOCKBIT Green uses a new encryptor based on the leaked Conti ransomware group's source code. The newly adopted encryption algorithm is ChaCha20, the same as the one used by Conti.

The group's members were also observed to be bragging about the same in an underground forum.

Figure 12: LOCKBIT discussing its variants on an Underground Forum

BlackByte

BlackByte has been offering Ransomware-as-a-Service (RaaS) since July 2021 and employs the Double Extortion technique. The Construction sector is the primary target of BlackByte Ransomware, followed by the Manufacturing and Retail sectors. The previous iterations of the BlackByte Ransomware were created using the programming languages Go and .NET. However, the latest variant of BlackByte Ransomware, known as BlackByteNT, was compiled using VC++ (Visual C++). The switch may have been made to enhance the malware's performance and to evade detection.

Alphavm

Alphavm, also known as ALPHV-ng, BlackCat, and Noberus, was first identified in November 2021 and is a ransomware-as-a-service (RaaS) threat group that targets businesses worldwide.

On February 21, 2023, ALPHV informed their affiliates of a new product update, BlackCat 2.0 Sphynx. The group claimed that a new technique had been added to mask the encryption process leading to the optimization of detection by Antivirus software.

CAPRICIOUS RANSOMWARE TECHNIQUES

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.

Royal Linux Variant Targets ESXi Servers

Royal ransomware was first identified in early 2022 and utilized RaaS from BlackCat and Zeon ransomware to target Windows machines. Since adopting new and unique code, Royal has become the most widespread ransomware group surpassing LOCKBIT for the first time.

Subsequently, in this quarter, CRIL came across a Linux sample of Royal ransomware targeting ESXi servers by employing multithreading encryption. The ransomware uses a combination of RSA and AES encryption algorithms for its encryption.

CL0P Launches Flawed Linux Variant

In early-2023, the CL0P ransomware group was observed targeting Linux machines through its new variant. The Linux variant of the ransomware is not significantly different from the Windows variant, as the underlying logic remains the same.

The ELF binary of the ransomware appears to target the folders associated with the Oracle database, which is not commonly seen in Linux ransomware files. The new variant of this ransomware has a flawed encryption algorithm that allows for the effortless recovery of encrypted files.

IceFire Linux Variant

IceFire malware operators, previously known for exclusively targeting Windows systems, have broadened their scope to include Linux as a potential target. While previous reports suggested that IceFire primarily targeted technology companies, the latest attacks have been directed toward organizations within the Media and Entertainment sectors.

The Linux version of IceFire ransomware was observed to be targeting CentOS hosts that were running a vulnerable version of IBM Aspera Faspex file server software.

CYBERCRIME FORUMS

Cybercrime Forums remained an active hub for several ransomware groups in Q1-2023, a continuing trend observed from the last quarter.

Qilin

CRIL observed that the Qilin Ransomware operators were looking to hire affiliates in a cybercrime forum. The group has had relatively sporadic activities since its discovery in Q3-2022. Previously it claimed to have compromised six organizations in October 2022, and this quarter, it claimed to have compromised three.

CAPRICIOUS RANSOMWARE TECHNIQUES

Agenda ransomware, also known as Qilin, is believed to operate on a Ransomware-as-a-Service model. **The ransomware was initially coded in GoLang, but a recent variant has also been observed using Rust binaries.**

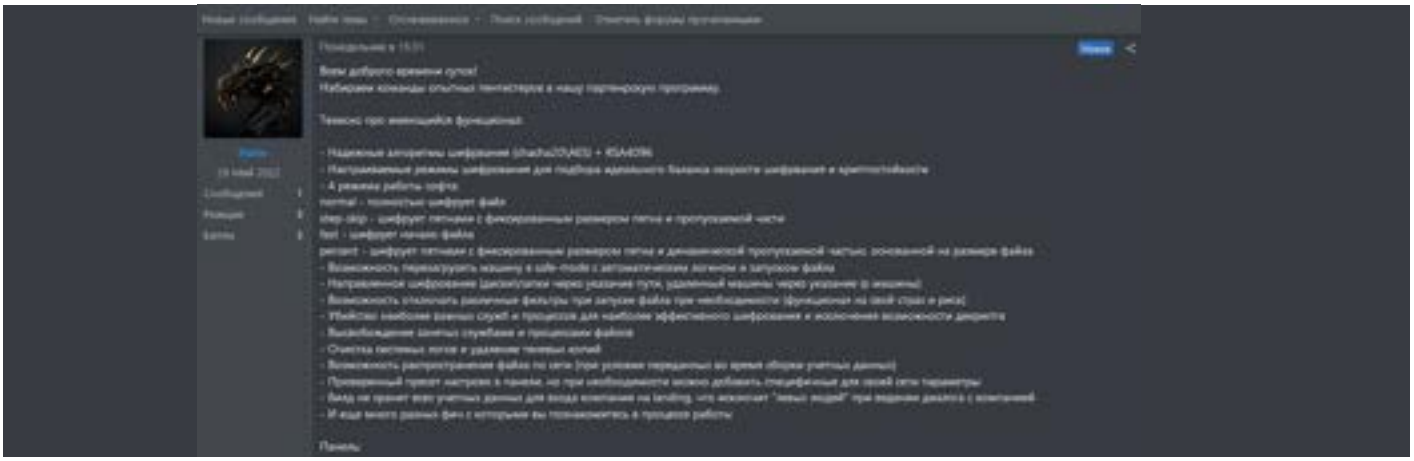


Figure 12: Qilin ransomware group's recruitment post on an underground forum

Nevada RaaS

The threat actors behind the Nevada Ransomware-as-a-Service (Raas) have been actively promulgating their services through a Russian cybercrime forum.

On December 10, 2022, the TA "nebel" announced a new project in a post and invited new affiliates to join. The Nevada Ransomware offers highly competitive and attractive terms, with a commission of 85% for partners that can increase to 90% based on time and progress.

Recently, the project operators made significant improvements to the locker for Windows and Linux/ESXi and provided new builds to their affiliates, which experts in malware intelligence have analyzed. Multiple updates to the locker in January indicate that the project is actively being developed with strong support.

Feud in AvosLocker Ransomware Group

A disgruntled coder of ransomware group AvosLocker and a member of the Russian cybercrime forum from 2020, under the moniker 'ExitQ', took their conflict with the group to the forum, claiming that they were locked out of the ransomware group's affiliate panel. The AvosLocker affiliate claimed that the administrators had locked their access to the panel while it was still negotiating USD 2 Million ransom with the victim organization. To counter the situation, another member of AvosLocker named 'lightbulb' posted proof to debunk ExitQ's claims.

All the group chatter revealed that most AvosLocker members and administrators are English speakers. The affiliates are responsible for end-to-end operations for a particular victim, including negotiations. After exfiltration of the data, the data is stored on that particular affiliate's own storage, which is then decrypted using the AvosLocker affiliate panel. An affiliate is also responsible for publishing the victim's name on AvosLocker's data leak site.

RANSOMWARE THREAT PREDICTIONS FOR 2023

- As highlighted in our previous reports, the role of Initial Access Brokers (IAB) is critical to Ransomware Landscape. We envisage that more conventional threat actors will likely venture into the IAB crime model due to its sheer profitability.
- Considering the trend from Q1-2023, we anticipate an increase in ransomware attacks on Asian and South American nations as the economy continues to grow in the region, leveraging a lucrative target for Ransomware victims. These regions often still depend on relatively outdated infrastructure and need sustained efforts to enhance their cybersecurity posture.
- We may observe a growth in ransomware attacks on the value chain of the Telecommunications industry, particularly in the field of Satellite Communications. We may also see ransomware groups trying to exploit associated vulnerabilities associated with critical infrastructure.
- Ransomware groups are likely to further streamline their operations using AI. They can leverage AI to reduce the process of gaining an initial foothold in the victim's infrastructure, develop exploits and frequently customize their tools for exploiting critical vulnerabilities to target mass victims. Further, ransomware groups' phishing and social engineering tactics will likely get more deceptive and harder to detect.

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

CVE-2023-23397	CVE-2021-39144	CVE-2023-23397	CVE-2023-23397
CVE-2023-23397	CVE-2023-23397	CVE-2023-23397	CVE-2023-23397

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 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

Quarterly Cyber Insurance Update: February 2023 (wsj.com)

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

https://blog.talosintelligence.com/new-mortalkombat-ransomware-and-laplas-clipper-malware-threats/

https://www.bleepingcomputer.com/news/security/alphv-ransomware-exploits-veritas-backup-exec-bugs-for-initial-access/

https://www.bleepingcomputer.com/news/security/cisa-orders-agencies-to-patch-exchange-bug-abused-by-ransomware-gang/

https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-321a

https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/

https://www.rapid7.com/blog/post/2023/03/28/etr-active-exploitation-of-ibm-aspera-faspex-cve-2022-47986/

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

https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/

https://twitter.com/vxunderground/status/1640932106229497859?s=46&t=ZbrTUzg8ztA-cALLQ8S_NJg

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