

Q4-2022

Ransomware Report



TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
QUARTERLY RANSOMWARE OUTLOOK	6
• WHAT HAS CHANGED FROM Q4-2021 TO Q4-2022	6
GLOBAL RANSOMWARE THREAT LANDSCAPE	7
• AMERICAS	7
• EUROPE & CIS	9
• ASIA & OCEANIA	10
• META	11
MICROANALYSIS OF RANSOMWARE ACTIVITIES	12
RANSOMWARE SECTORAL IMPACT	14
EVOLVING RANSOMWARE THREAT PROFILE	16
• ROYAL	16
• PLAY	17
• QILIN	17
• RELIC	18
• MALLOX	18
• PUTIN TEAM	19
• NOKOYAWA	19
CAPRICIOUS RANSOMWARE TECHNIQUES	20
• INTERMITTENT ENCRYPTION	20
• DATA WIPERS	20
• OVERCOMING ENTRY BARRIERS	21
• ZERO DAYS	21
• RDP	21
• LOCKBIT V4 OR REBRAND?	22
• SUPPLY CHAIN ATTACKS	23
• CYBERCRIME FORUMS	23
• AUSTRALIAN HEALTHCARE ENTITY RANSOMWARE ATTACK LINKED TO TA RADAR	23
• ENDURANCE RANSOMWARE	23
RANSOMWARE THREAT PREDICTIONS FOR 2023	24
HOW TO PROTECT YOURSELF FROM RANSOMWARE ATTACKS	25

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 Q4-2022 to preempt the associated risks of the Ransomware discussed herein.

Ransomware activities in Q4-2022 steadily rose, in contrast to the drop we had observed in the previous quarter. Although Ransomware continues to be a formidable threat, we witnessed a **100 percent increase in high-net-worth companies targeted in Q4 as compared to Q3-2022**.

As speculated in our [Q3-2022 report](#), **multiple small-medium scale industries fell victim to supply chain attacks** executed by ransomware groups. Notable incidents include LOCKBIT ransoming multiple businesses in New Zealand after exploiting Mercury IT and asserting the same on their leak site. Similarly, the Play ransomware group targeted multiple Swedish entities operating in the Transportation and Logistics sector by attacking their common IT service provider.

It is well known that the REvil ransomware group's leak site was taken down in Q1-2022 after the arrest of REvil affiliates. Incidentally, in October 2022, Australia-based Medibank was allegedly targeted, and surprisingly, the claim was made on REvil's leak site.

Initial speculations indicated that REvil had returned, but the perpetrators claimed to be an affiliate of REvil, ALPHV (Blackcat), and Hive Ransomware groups. These could be lesser-known threat actors or affiliates trying to garner attention by alleging themselves as members of well-known ransomware groups.

In our [Q1-2022 ransomware report](#), we anticipated the **emergence of new ransomware groups based on the leaked source code of Conti ransomware**. This prediction was validated in Q4-2022 with the emergence of several [new ransomware families](#), including Putin Team, BlueSky, ScareCrow, and Meow, which were based on the leaked Conti source code.

This year, we witnessed prominent ransomware families shifting towards using **Rust or GoLang-based binaries**, with **several new strains such as RansomEXX, Play, and Qilin** adopting this trend in Q4-2022. This shift towards cross-platform languages was comprehensively envisaged in our [Q2-2022 Ransomware Report](#).

EXECUTIVE SUMMARY

THIS REPORT ENCAPSULATES THE FOLLOWING **MAJOR FINDINGS** FROM Q4-2022:



594 victims were publicly disclosed by ransomware groups, with United States (US) corporations continuing to be the most affected



While Services & Manufacturing sectors were worst hit, we witnessed a significant increase of attacks towards Education sector. The BFSI sector appeared more resilient towards ransomware attacks in 2022



Royal ransomware was the most active ransomware group in Q4-2022 in the US, replacing LOCKBIT. This drop in the victim count of LOCKBIT could be attributed to the recent arrest of one of their affiliates in Canada



LOCKBIT was the most active ransomware group this quarter. However, the victim count and stature of the organizations targeted by the ransomware group has declined since July 2021



We monitored several new players on the ransomware scene in Q4-2022 - Royal, Play, Qilin, Putin Team, Mallox, and Nokoyawa



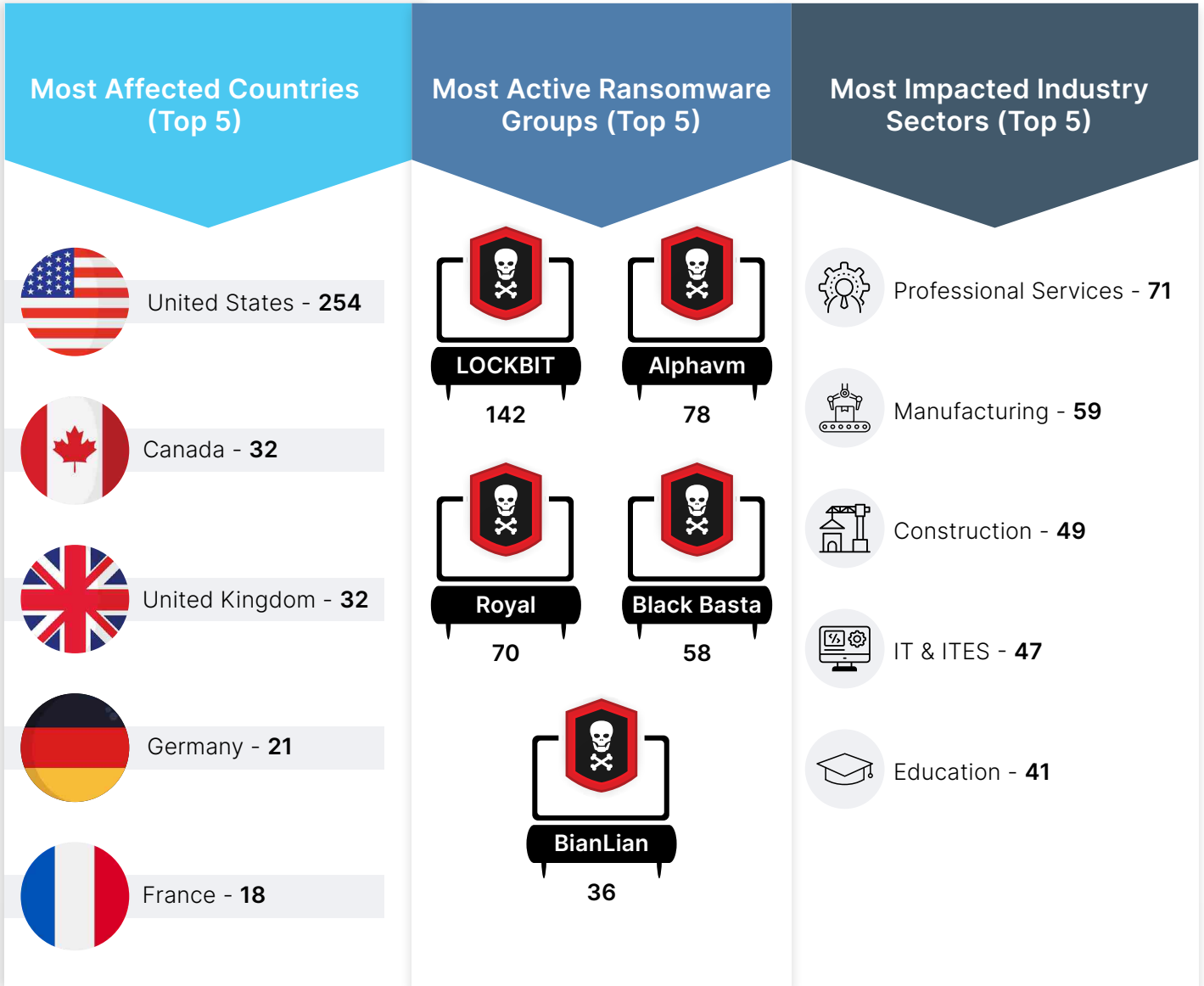
This quarter, multiple ransomware groups were observed adopting intermittent encryption to speed up the encryption process and evade detection

Our analysis of the Q4-2022 ransomware threat landscape led us to infer that ransomware groups might invest in exploiting more zero days in forthcoming attacks. In the future, ransomware groups may target large entities with strategic importance and significant contribution to their country's economy.

EXECUTIVE SUMMARY

Total victims - **594**

Active Ransomware Groups - **29**



QUARTERLY RANSOMWARE OUTLOOK

“CRIL identified 594 ransomware victims in Q4-2022 compared to 538 in Q3 – a 10% Quarter-over-Quarter (Q-over-Q) increase and a 28% decrease from the same time period last year (Q4-2021).”

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.**

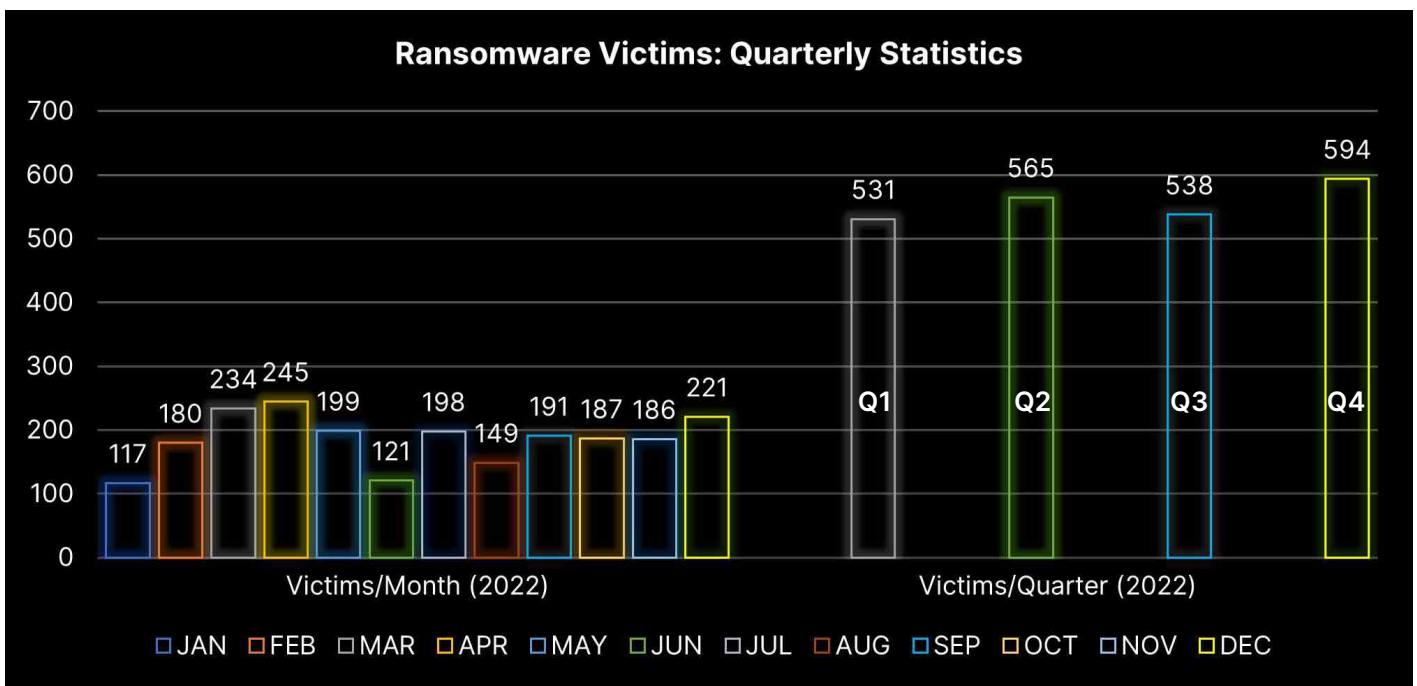
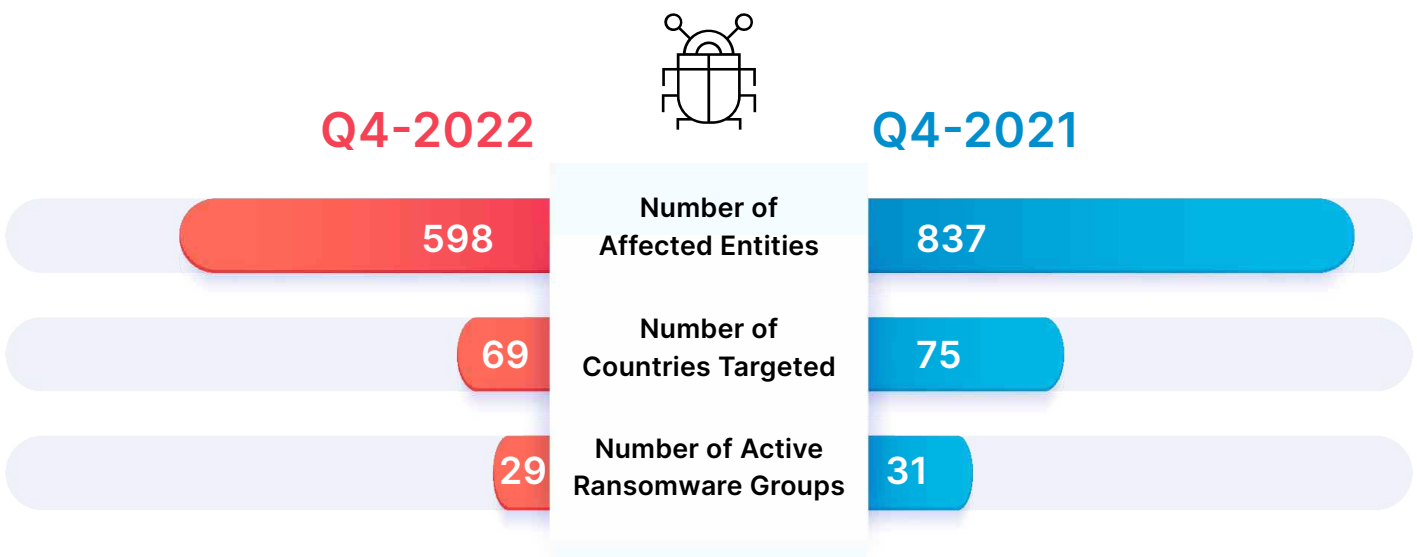


Figure 1: Comparative analysis of ransomware activities Q-over-Q

WHAT HAS CHANGED FROM Q4-2021 TO Q4-2022



GLOBAL RANSOMWARE THREAT LANDSCAPE

“In Q4-2022, we observed ransomware activities in 69 countries – a 9% Q-o-Q decline from previously observed 76 countries in Q3.”

Ransomware attacks are becoming increasingly common worldwide, with no particular region or industry being immune to them. Earlier, we observed that the Commonwealth of Independent States (CIS) was relatively less prone to ransomware attacks. However, since the outbreak of the Russia-Ukraine conflict, multiple new groups have been spotted executing attacks on such nations as well.

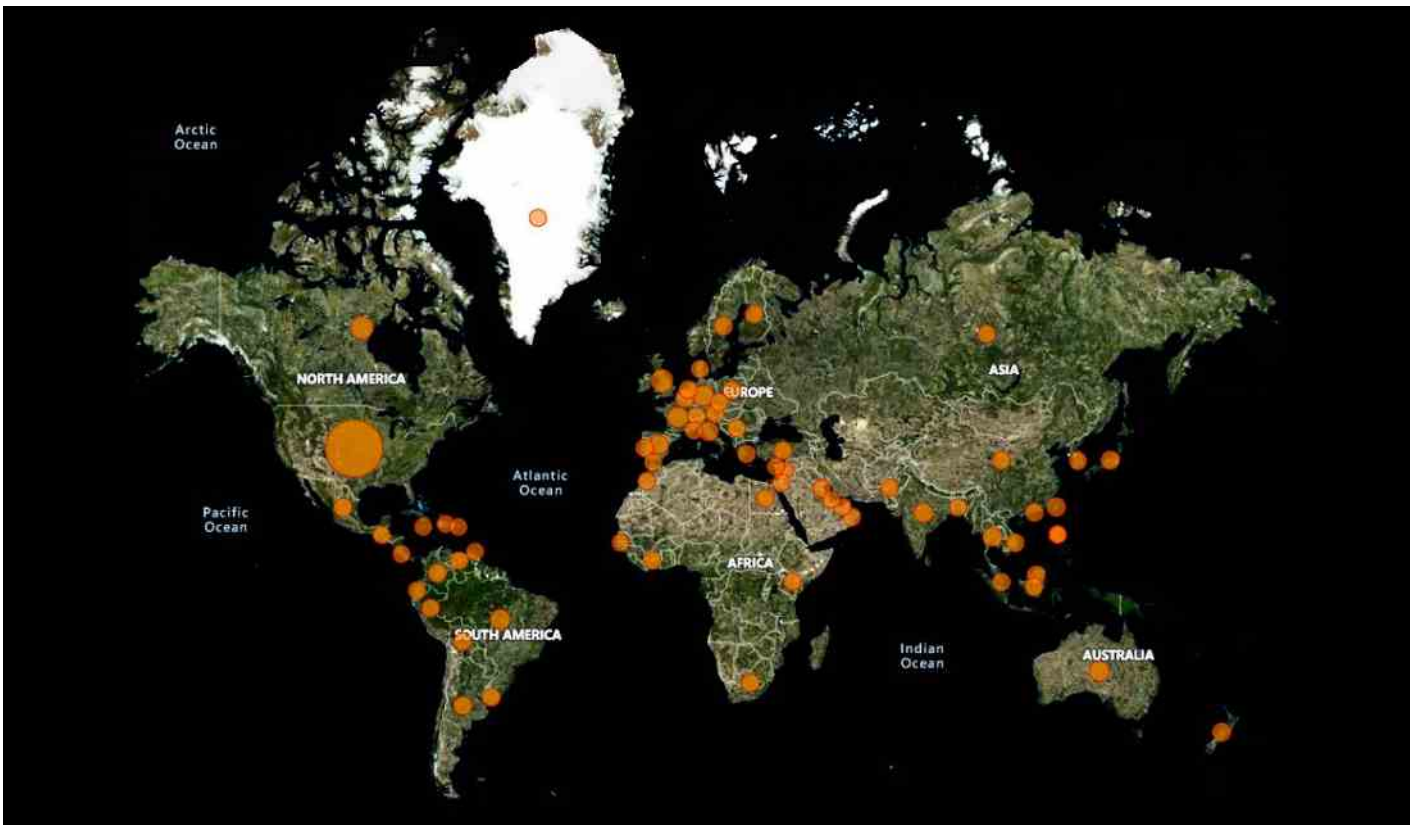




Figure 2: Global Distribution of Ransomware-Affected Organizations

AMERICAS

The **Americas was the most targeted region, with over 300 ransomware victims**. This region accounts for over 50% of ransomware victims disclosed publicly in Q4-2022.

A snapshot of the ransomware landscape in the region is as follows:

NORTH AMERICA	LATAM
 <ul style="list-style-type: none"> • US: 254 • Canada: 32 	 <ul style="list-style-type: none"> • Brazil: 16 • Mexico: 7 • Colombia: 5

GLOBAL RANSOMWARE THREAT LANDSCAPE

The US and Canada suffered the most ransomware attacks due to a combination of factors, including high levels of technology adoption, relatively valuable data, high ransom demands, and huge attack surfaces. These countries have many businesses and organizations that handle sensitive data for various other global organizations and are susceptible to ransom demands to restore their systems.

The strong cyberinfrastructure in these countries may also make it more difficult for ransomware attackers to carry out an attack successfully. Still, it could also make it more appealing to attackers because the **payoff is likely much higher if they can successfully execute a ransomware attack.**

The figure below showcases the geographical distribution of major ransomware activities across this region in Q4-2022.



Figure 3: Geographical distribution of Ransomware victims in the Americas

Ransomware attacks in the Americas have particularly impacted the Professional Services, Manufacturing, IT and ITES, Education, and Construction sectors, with LOCKBIT, ROYAL, and ALPHV being the most active groups in the region, alongside 25 other, less active groups.

GLOBAL RANSOMWARE THREAT LANDSCAPE

EUROPE & CIS

Europe was the second most ransomware-affected region, with 147 ransomware victims. Of the listed countries, the United Kingdom had the highest recorded instances of ransomware attacks, with 32 victims. Germany had the second highest number at 21, and France had 18 reported cases. **There were also ransomware victims disclosed from Russia, something that has rarely been seen to this point.**

The figure below showcases the geographical distribution of major ransomware activities across Europe and the CIS region in Q4-2022.



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

Construction, Professional Services, Transportation & Logistics, and Education were the most affected sectors in this region. LOCKBIT, Play, Alphavm, and Vice Society were particularly nefarious in this part of the world.

GLOBAL RANSOMWARE THREAT LANDSCAPE

ASIA & OCEANIA

Asia & Oceania was the third most targeted region, with sectors like Professional Services, Construction, Manufacturing, Technology, and IT & ITES being the most adversely impacted by ransomware attacks.

In this region, 19 ransomware groups were observed to be active, **including LOCKBIT, Alphavm, BianLian, and Play, being the prominent ones.**

The figures below reflect the distribution of major ransomware activities across this region in Q4-2022.

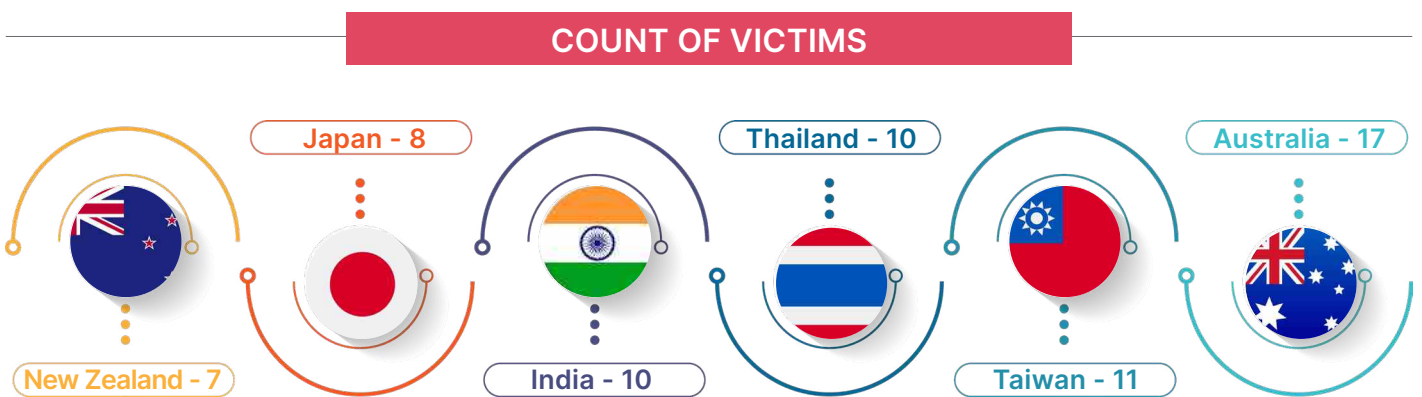


Figure 5: Geographical distribution of Ransomware victims in Asia & Oceania

GLOBAL RANSOMWARE THREAT LANDSCAPE

META

The Middle East, Turkey, and Africa (META) region **saw the least number of ransomware attacks**. While over 10 countries in this region were targeted, the majority of attacks were reported in Lebanon, with other countries such as Oman, Turkey, South Africa, Ivory Coast, Israel, United Arab Emirates, Kuwait, and Bahrain experiencing relatively fewer attacks.



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 12 ransomware groups active in the region, with Vice Society and ALPHV being the next most active after LOCKBIT. Entities from the Hospitality, IT & ITES, Education, and Construction sectors suffered the most attacks in the META region.

MICROANALYSIS OF RANSOMWARE ACTIVITIES

“CRIL covered the activities of 29 ransomware groups in Q4-2022, rising from 26 in Q3-2022.”

Other **new ransomware groups** identified this quarter and highlighted as red bars in the graph below were - **Royal, Play, Bully Gang, Unsafe, Qilin, Relic, Mallox, Putin Team, and Nokoyawa**. Further, we observed nil activities from previously active ransomware groups – **CHEERS, Onyx / VSOP, IceFire, LILITH, Omega, and Red Alert** in Q4-2022. These groups are likely to be operating under different aliases to avoid Law Enforcement scrutiny after their attacks in Q3-2022.

NEW RANSOMWARE GROUPS OBSERVED TO BE ACTIVE IN Q4-2022



MICROANALYSIS OF RANSOMWARE ACTIVITIES

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

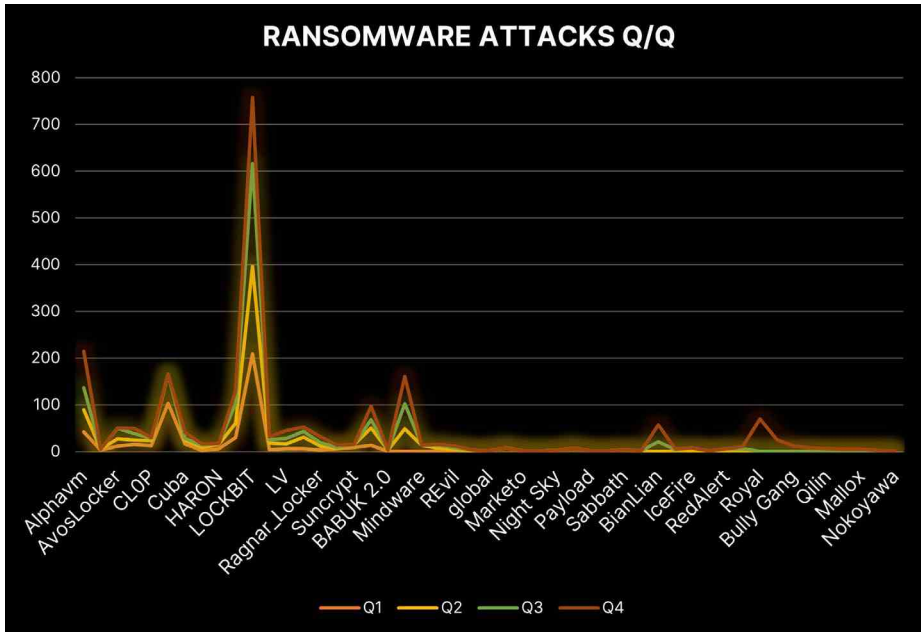


Figure 7: Ransomware activity in 2022

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

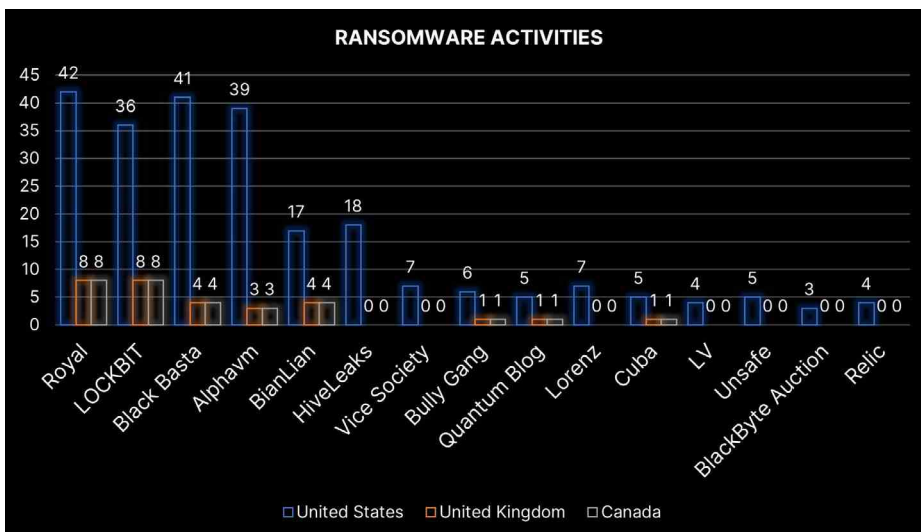


Figure 8: Ransomware Activity in the three most affected countries

- LOCKBIT was the most active ransomware group, targeting 142 organizations in Q4-2022, a decline of over 35% compared to Q3. These affected entities were primarily from the Professional Services, Construction, Manufacturing, Consumer Goods, and BFSI sectors
- Since July 2021, this is the lowest number of victims disclosed by LOCKBIT ransomware
- LOCKBIT had the highest number of victims in countries such as Australia, France, the United Kingdom, and Taiwan. Previously, LOCKBIT was highly prevalent in the United States and had most of its victims there. However, in Q4-2022, Royal ransomware overtook LOCKBIT in terms of victim numbers in the US

RANSOMWARE SECTORAL IMPACT

Ransomware groups mostly had a similar sectoral attack surface in Q4-2022, as observed in Q3-2022, except **Education replaced the Healthcare organizations to emerge in the 5-most affected sectors**. 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.

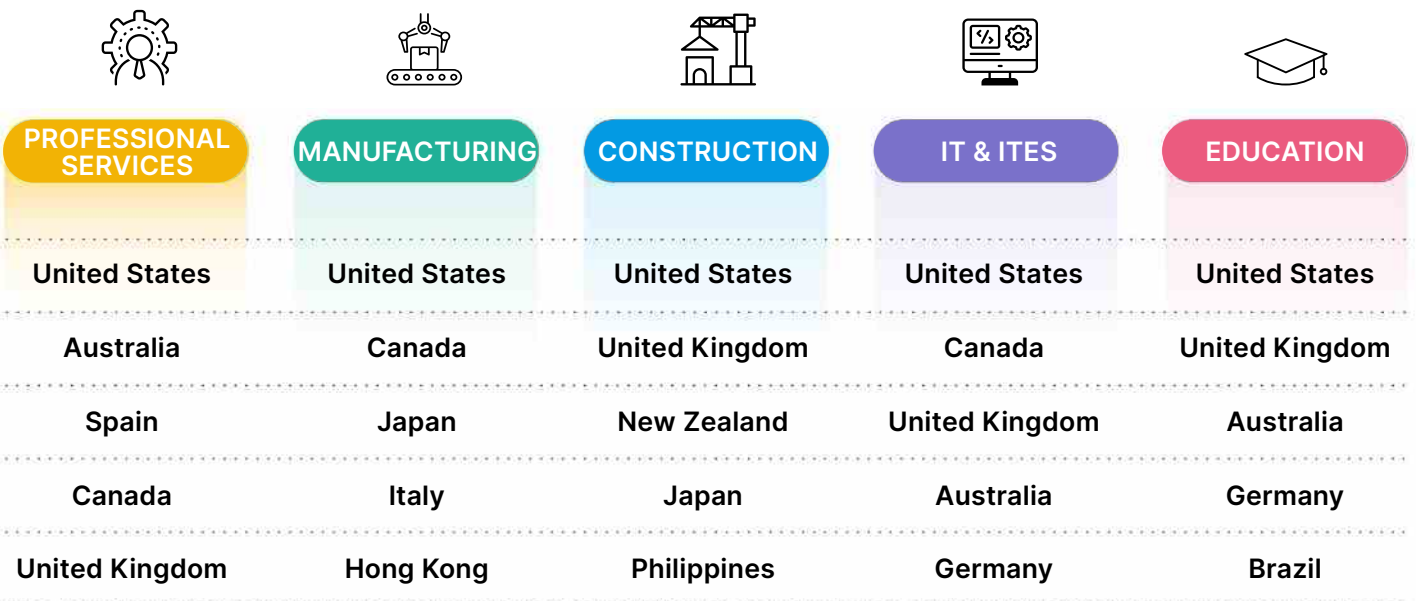
LOCKBIT has been actively targeting US companies in the **Services, Manufacturing, and Construction sectors**.

In Q4-2022, there was a **68% increase in attacks on the Education sector** compared to Q3-2022. Vice Society, Hive Leaks, and BianLian have primarily targeted the Education sectors in the last quarter of 2022.

We observed that the countries known for their niche sectoral capabilities often have those sectors worst affected due to Ransomware attacks. For instance, Taiwan, known for its Technological prowess, had the highest number of victims in the sector. In contrast, Germany’s automotive sector, the German economy’s strength, was worryingly targeted.

In the Middle East and Turkey, the hospitality industry had the highest number of victims, suggesting that ransomware groups may not just be targeting industries at random but are instead targeting industries contribute significantly to a country’s Gross Domestic Product (GDP).

In Q4-2022, the five most targeted industries by ransomware groups were:



RANSOMWARE SECTORAL IMPACT

REPEATED RANSOMWARE ATTACKS IN Q4-2022:

- A US-based Healthcare service provider, earlier targeted by LOCKBIT in September 2022, was compromised by the Everest ransomware group in October 2022
- A Construction company from the United Kingdom was targeted by LOCKBIT in February 2022 and BlackByte in October 2022
- Vice Society targeted another US-based Healthcare entity in November 2022, which was previously attacked by LOCKBIT in July 2021
- A Consumer Goods company from the US was targeted twice in December 2022 by Hive Leaks & Alphavm.
- Vice Society first targeted a Professional Services company in the US in November 2022, which was subsequently hit by Alphavm in December 2022
- A French Transportation & Logistics service provider became a victim of the REvil ransomware group in February 2021 and was targeted again by the Unsafe ransomware group in December 2022



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 usually 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.

EVOLVING RANSOMWARE TOOLKITS ARE MODIFYING THE CURRENT RANSOMWARE THREAT LANDSCAPE:

- Exmatter, a data exfiltration tool used by the Alphavm ransomware group, has now added data-wiping capabilities
- The BlackByte ransomware group has also started using a new data exfiltration tool called Exbyte, written in Go
- The RansomEXX group has rebranded as “RansomEXX2” and released a new payload written in Rust targeting Linux systems
- Additionally, the ViceSociety ransomware group has adopted the PolyVice payload, which uses a robust encryption scheme to encrypt victims’ data quickly

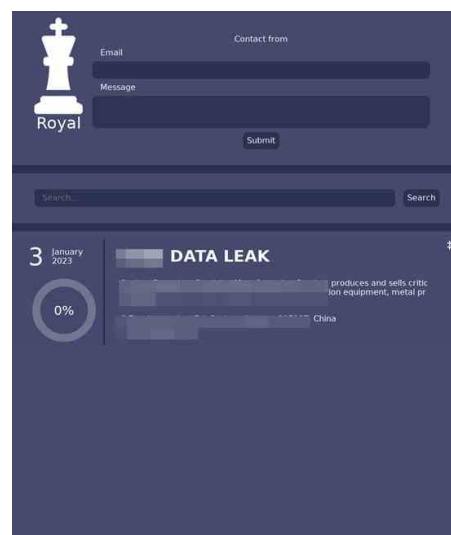
“Cyble Research & Intelligence Labs worked on profiling new ransomware groups in Q4-2022 to forewarn our readers about their activities in the dynamic ransomware threat landscape.”

ROYAL

Royal ransomware was one of the most active groups in Q4-2022. It has been active since January 2022 and was known as “Zeon” before rebranding itself in September 2022.

It is understood to be run by experienced cybercriminals with a history of involvement with the Conti group. Unlike many other ransomware operations, Royal does not offer its services to affiliates but instead operates as a private group.

Initially, the group used encryptors from other ransomware operations, such as BlackCat. After rebranding, however, they began using a new encryptor to generate ransom notes under their current name.



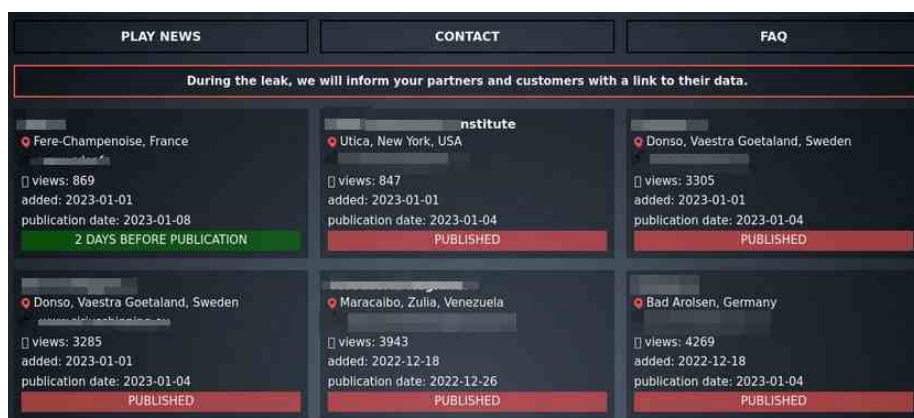
EVOLVING RANSOMWARE THREAT PROFILE

PLAY

Play ransomware is a relatively new group that has been targeting companies primarily in **Latin America** but is slowly establishing a global presence with victims in **Europe and the Commonwealth of Independent States**.

“This group has been observed using a hybrid cryptography scheme of RSA and AES to encrypt files and is highly obfuscated with various anti-analysis techniques. Play ransomware has also been spotted exploiting zero-day vulnerabilities and other weaknesses for initial access, such as “ProxyNotShell.”

Despite the lack of code overlap with other ransomware groups, the group’s identified Tactics, Techniques, and Procedures (TTPs) resemble those of the Nokoyawa and Hive ransomware families.

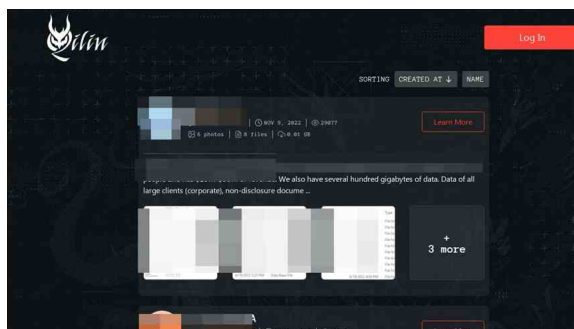


QILIN

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.”

This variant lacks some of the features found in the original binaries but can terminate the Windows AppInfo process and disable User Account Control (UAC).

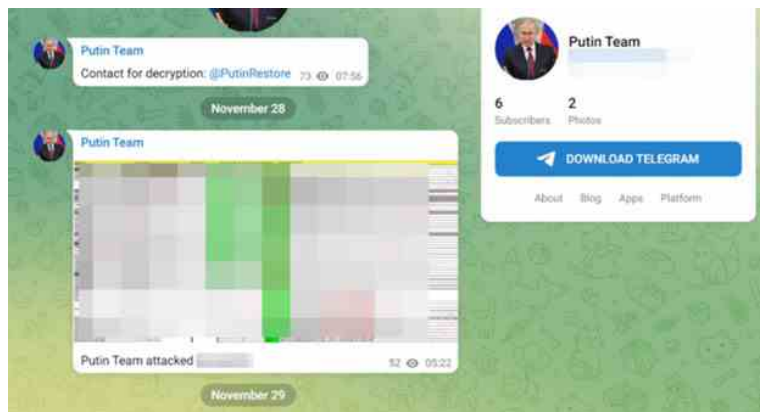


EVOLVING RANSOMWARE THREAT PROFILE

PUTIN TEAM

CRIL recently discovered a new ransomware group called “Putin Team”, which is believed to have used altered versions of the leaked Conti ransomware source code to create its own ransomware binaries. The group claims to be of Russian origin, but there is no evidence thus far to confirm this.

Putin Team uses a Telegram channel to disclose information about its victims and has posted details of two victims so far.



NOKOYAWA

Nokoyawa is a Windows-based ransomware that was first identified in February 2022. The group behind this uses double extortion technique to target its victims.

“The latest version of Nokoyawa is written in the Rust programming language and uses Curve25519 and Salsa20 encryption algorithms.”

Previously, it was written in C and used ECC with SECT233R1 and Salsa20 for file encryption.

Reports have noted that the Rust-based version of Nokoyawa 2.0 allows the threat actors to have runtime flexibility through a configuration parameter passed via the command line.

NOKOYAWA Leaks

We have collected companies that don't worry about their customers!

Nexon Asia Pacific

Nexon is headquartered in Sydney, New South Wales... [Read](#)

CAPRICIOUS RANSOMWARE TECHNIQUES

Ransomware variants are adopting novel techniques to extort ransom and evade detection. Some of the new techniques that we observed in Q4-2022 were:

INTERMITTENT ENCRYPTION

“Multiple ransomware groups use intermittent encryption to speed up the encryption process and make their ransomware more difficult to detect. Intermittent encryption was first observed with the LockFile ransomware in mid-2021 and, since then, has been adopted by several prominent ransomware groups, including PLAY, Qilin, Black Basta, and ALPHV.”

The technique allows these groups to operate stealthily and evade normal detection methods. This technique involves partially or only encrypting certain parts of files, making it harder for security systems to detect the intrusion. Intermittent encryption is used to increase the speed of the attack and reduce the chances of being detected and stopped.

Ransomware detection systems often use statistical analysis and tools to measure the intensity of input/output operations or compare versions of a file to identify attacks.

However, intermittent encryption, which only partially encrypts files or certain parts of them, is a “lighter” process that can evade these detection tools. This is because it does not affect the intensity of input/output operations as much as complete file encryption does.

DATA WIPERS

Data wipers are malicious software programs that are designed to delete or erase data from a computer or other device. Ransomware, on the other hand, encrypts a victim’s files and demands a ransom from the victim to restore access.

“Recently we observed that ALPHV ransomware added data wiper capabilities, followed by Project Relic ransomware, reported to be stealing, encrypting, and deleting sensitive files.”

The data-wiping capabilities of ransomware allow attackers to delete the victim’s data if the ransom is not paid. This technique instills added pressure on the victim to pay the ransom, fearing the permanent loss of their encrypted data. Further, this technique can disrupt business operations and lead to financial losses.

CAPRICIOUS RANSOMWARE TECHNIQUES

OVERCOMING ENTRY BARRIERS

ZERO DAYS

In the fourth quarter of 2022, many major ransomware attacks involved using zero-day vulnerabilities to gain initial access to networks. Previous large-scale attacks, such as the REvil attack on Kaseya VSA and the Accellion FTA attack by Lorenz ransomware, also took advantage of zero-days. The exploitation of zero-days can allow threat actors to launch attacks on a large scale.

In the second quarter of 2022, the LOCKBIT ransomware group even launched a bug bounty program, offering bounties ranging from \$1000 to \$1 million for reporting vulnerabilities. This indicates that ransomware groups are actively seeking out systems with zero-days or unpatched vulnerabilities.

In the first week of December 2022, the US cloud computing company Rackspace experienced a Microsoft Exchange outage and later revealed that a ransomware attack had been responsible. The Play ransomware group was found to be behind the attack and had used a zero-day exploit dubbed "OWASSRF" to bypass Microsoft's ProxyNotShell URL rewrite mitigations and likely target a critical flaw [CVE-2022-41080](#), allowing for remote privilege escalation on Microsoft Exchange servers.

The attackers were also able to gain remote code execution on vulnerable servers by exploiting the [CVE-2022-41082](#) vulnerability, which had been previously abused in ProxyNotShell attacks.

RDP

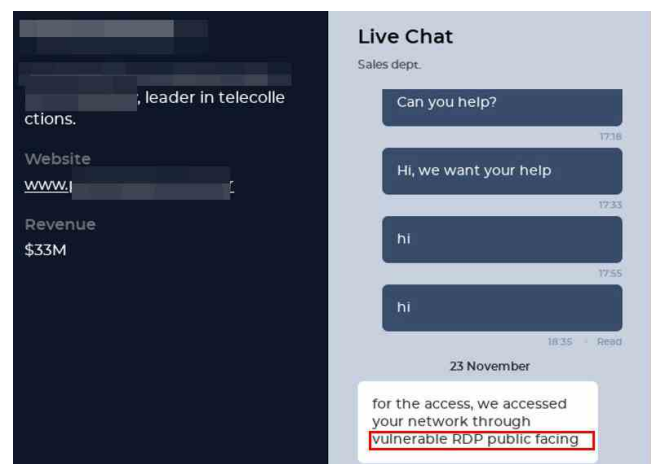
An exposed RDP port on the internet could lead to a major security incident. Threat actors can easily scan the internet for systems with exposed RDP ports and then attempt to gain access using stolen credentials or vulnerabilities.

Once access is gained, Threat Actors (TAs) can access the system, steal sensitive data, and potentially spread malicious programs such as ransomware to other network systems.

Intelligence gained from Cyble Global Sensor Intelligence (CGSI) indicates a surge in the number of RDP exploitation attempts in the past few months. Over 4,783,842 exploitation attempts were made in Q4-2022, with a peak in exploitation attempts being observed in September-end and mid-November.

CRIL carried out an investigation and found multiple ransomware groups targeting open RDP to gain initial access to corporate networks.

The figure below shows the exploitation of RDP mentioned by Hive ransomware.



CAPRICIOUS RANSOMWARE TECHNIQUES

LOCKBIT V4 or REBRAND?

On October 26, 2022, a Russian national was arrested in Ontario, Canada. According to Europol, this individual was a high-value target due to their involvement in numerous high-profile ransomware cases and is known for attempting to extort victims with ransom demands ranging from €5 to €70 million.

During the arrest, Canadian law enforcement officers discovered evidence linking the individual to the LOCKBIT ransomware group:

- The screenshots of Tox exchanges with the public-facing representative of the group (LOCKBITSupp)
- Instructions on how to deploy the LOCKBIT malware
- The malware's source code
- Photographs of a computer screen showing login credentials for various platforms belonging to employees of a Canadian company that LOCKBIT had attacked in January 2022

After this incident, LOCKBIT ransomware might launch a new version (v4) or rebrand. This arrest can also make a few affiliates of LOCKBIT take a bid, as they might want to keep their operations under the radar of law enforcement agencies.

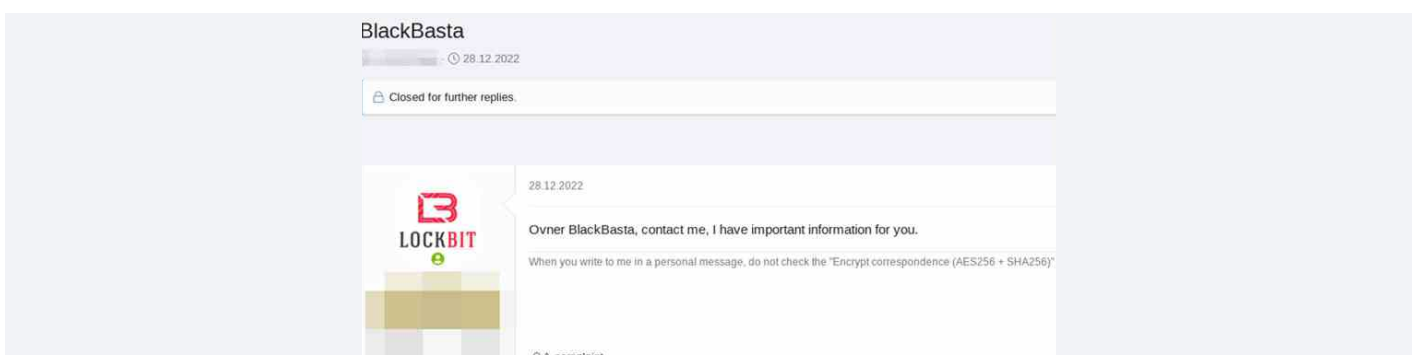
Incidentally, in Q4-2022, LOCKBIT reported the least number of victims since July 2021. They used to have the highest number of victims in the United States quarter-over-quarter since their launch, **but in Q4-2022, they had significantly lower incidences of observed attacks.**

LOCKBIT ransomware might rebrand or launch a new version to avoid detection and prosecution. If a criminal group uses a pseudonym or alias, it can be more difficult for law enforcement to trace their activities back to their real identity. Another reason for changing identity could be to gain access to new resources or opportunities.

Recently, the admin of LOCKBIT ransomware posted a message on a cybercrime forum for the owner of BlackBasta ransomware to contact him. There are multiple reasons for this post, but it's possible that these groups may want to collaborate in the future or there's some information disclosure attributed to them.

The leak site of BlackBasta ransomware has been down for multiple weeks, and the reason is still unknown.

The figure below shows the post made by the ransomware group.



CAPRICIOUS RANSOMWARE TECHNIQUES

SUPPLY CHAIN ATTACKS

In Q3-2022, we predicted that ransomware groups' supply chain attacks could catastrophically impact various entities. In one such case, LOCKBIT compromised a New Zealand-based IT & ITES entity providing cloud services, which enabled the group to attack various other organizations, including government organizations.

Considering the magnitude of such attacks and the profitability of efforts, this exploitation technique is likely to be adopted by other ransomware groups in 2023.

CYBERCRIME FORUMS

CRIL predicted in Q3-2022 that the cybercrime forums might see an influx of marketing activity by Ransomware Groups or their affiliates. There were instances where the affiliates were also observed to be marketing accesses and data sales on popular underground forums.

A few of these instances are listed below:

AUSTRALIAN HEALTHCARE ENTITY RANSOMWARE ATTACK LINKED TO TA RADAR

At the end of December, TA RADAR was selling alleged data from Australia-based dental clinic Dental One on BreachForums. The TA is a self-proclaimed ransomware group.

The TAs shared a screenshot of the folder-tree of stolen data while mentioning that 500 GB of data from the servers of the Craigieburn-based clinic, consisting of customers' Protected Health Information (PHI), invoices, reports, scans, online forms, important documents, etc. were compromised.

Dental One operates 5 clinics in Melbourne. CRIL predicted that the extent of the attack may not be limited to Craigieburn clinic and can affect the other four clinics in Melbourne - Lower Templestowe, Epping North, Richmond - Victoria Gardens, and Reservoir.

Our observation turned out to be true: within a few days, Alphavm, aka Black Cat Ransomware Group, announced targeting Dental One and leaked 6 GB of data.

The screenshot shared by the group is similar to what TA RADAR shared on their forum post, but our analysis suggests that the attack impacted all five clinics.

We envisage TA RADAR to be associated with Alphavm through their affiliate program and subscribing to Alphavm's Ransomware-as-a-Service (RaaS), or the TA could be advertising the sale of the victim organization's data in cybercrime forums, a trend adopted by some prominent ransomware groups like Everest and LOCKBIT to put further pressure and extort ransom.

ENDURANCE RANSOMWARE

TA IntelBroker on BreachForums self-proclaims themselves to be Endurance Ransomware Group. Initially, a one-member group emerged in October 2022 and was even observed hiring affiliates. Ironically, they were also observed to be seeking help from C# developers to add a list of enhancements in the existing malware (Endurance) developed by the TA.

The TA has allegedly breached several US government organizations and also offers Ransomware-as-a-Service (RaaS) on the forum. Open research results revealed a GitHub page belonging to the TA, which included the source code of the Endurance-Wiper. The malware is written in C# using the .NET framework. However, the effectiveness of their ransomware remains doubtful.

RANSOMWARE THREAT PREDICTIONS FOR 2023



In the recent past, we observed several ransomware builders and source codes had been leaked. TAs can perform mass scanning of vulnerable services, such as RDP, and then use leaked builders or ransomware source code to execute these attacks. An attacker with moderate skills can also execute such attacks. Considering this, we may see **a surge in ransomware attacks from unknown and less sophisticated ransomware groups.**



As we highlighted the growing use of Data Wipers among Ransomware Groups, **we assess that if equipped with a data exfiltration tool, future data wipers have the potential to replace ransomware.** The execution of ransomware is more complex and time/resource-consuming than data wipers, as data wipers only need to destroy data. TAs can exfiltrate the data and store it on a remote server. After exfiltration, they can execute a data wiper, leaving the victim with no data. Then they can ask the victim to pay for the exfiltrated data. In this case, the ratio of Attack/Ransom earned could be higher than in a traditional ransomware attack.



Initiatives such as OpenAPI to democratize AI for noble developments are also gaining a lot of attention from cybercriminals. Novice cybercriminals are **using the newly launched ChatGPT tool to develop and refine their malicious tools and encryption techniques**, streamline their operations and perform more targeted attacks on High-Value Targets using minimum resources at hand.



Henceforth, CRIL will likely observe more hacktivist groups launch ransomware and extortion attacks for monetary and political gains.



We also anticipate an increase in ransomware attacks against Infrastructure-as-a-Service providers in 2023, as cloud adoption grows among several small and medium enterprises.



Cyber insurance providers are increasingly getting overwhelmed due to the sheer quantum of claims from ransomware victims' organizations. The insurers are anticipated to constrict the underwriting and make the claims process more stringent. The insurance companies are preparing to implement policies that necessitate the insured entity to harden their cybersecurity infrastructure, without which the claims could be rejected. Insurance companies are likely to use cybersecurity companies' services to test the security adoptions of the companies approaching for insurance, renewals, and even before settling claims. This will also help bring down the increasing cyber insurance premium for companies with hardened security frameworks.

HOW TO PROTECT YOURSELF FROM RANSOMWARE ATTACKS

With Threat Actors and their TTPs increasing in sophistication and rapid adoption of new Ransomware techniques, the industry is still searching 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



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 Start-ups 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

