CYBLE

Q1-2022 Ransomware Report

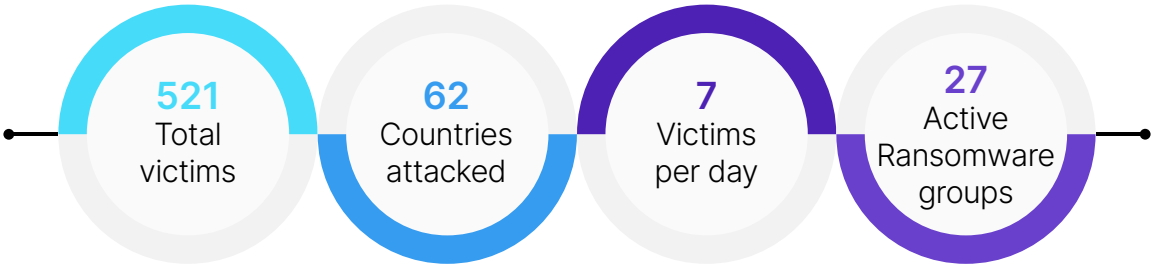
View Report >

Table of Contents

Executive Summary

Cyble Research Labs closely monitors, tracks, and analyzes current and emerging ransomware threats across the globe. This report covers critical ransomware statistics and trends, major attacks, and common Tactics, Techniques, and Procedures (TTPs) observed in the First Quarter of 2022.

Q1 2022 Ransomware Highlights:



Top 3 Ransomware groups:

ALPHV

42 - Victims

14 - Countries Attacked

Conti

103 - Victims

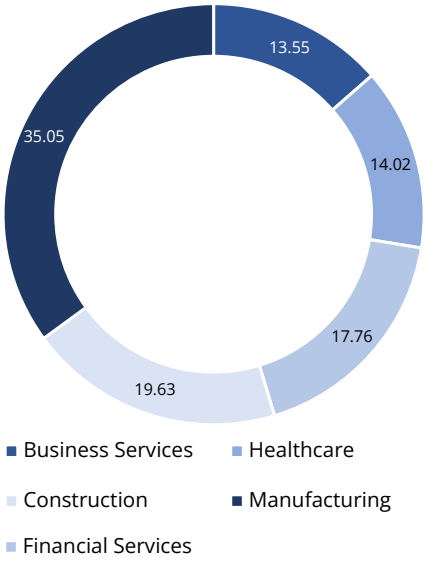
20 - Countries Attacked

LOCKBIT

209 - Victims

43 - Countries Attacked

Most attacked industries:



Most targeted countries:

Top 10 Ransomware groups:

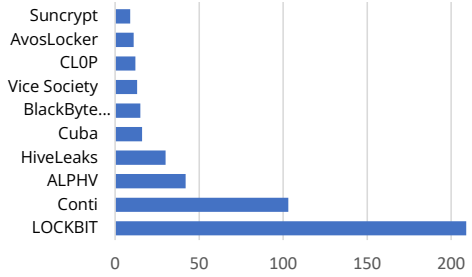


Figure 1: Main Highlights

Cyble Research Labs identified 521 ransomware victims in Q1 2022 – a 37% decline over Q4 2021.

LOCKBIT was the most active ransomware gang in Q1, with 209 victims, mostly from the Manufacturing, Financial Services, and Construction industries.

62 countries worldwide were observed being hit by Ransomware attacks. The United States, United Kingdom, and Italy emerged as the most targeted regions by Ransomware groups - accounting for well over half the total attacks.

Executive Summary

Q1-2022 saw the emergence of two new ransomware groups Pandora Leaks and Night Sky. These groups are suspected to be operating on the Ransomware-as-a-Service (R-a-a-S) model. The Pandora Leaks ransomware group is possibly a rebrand of ROOK ransomware.

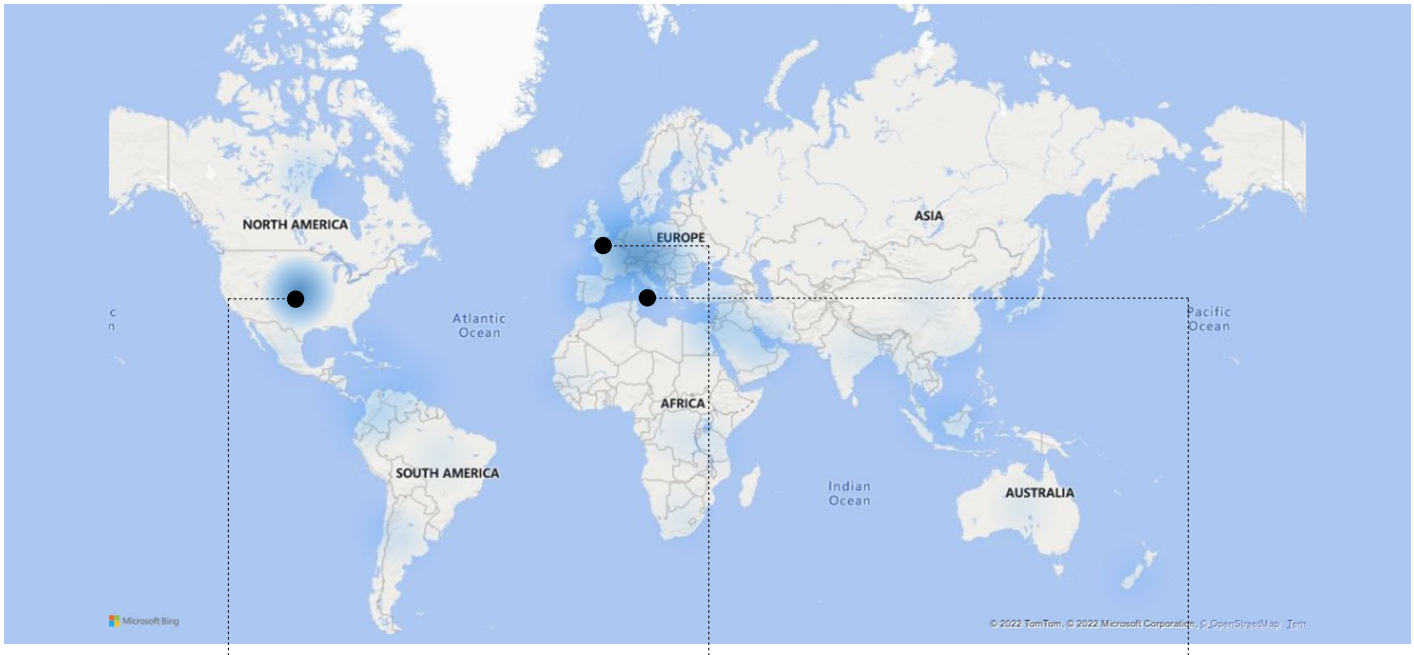
Q1 2022 turned out to be a nightmare for certain ransomware groups. In Jan 2022, 15 members of the REvil ransomware group were arrested by Federal Security Service (FSB) in Russia. Due to the Russia-Ukraine conflict in Feb 2022, we observed internal strife between Conti ransomware group members. This led to the disclosure of their chats, ransomware source code, and internal structure.

Figure 2 showcases the geographical distribution of major ransomware activities across the globe in Q1-2022.

37% Decline in ransomware activities

New Ransomware groups:

- Pandora Leaks
- Night Sky



United States	United Kingdom	Italy
Most active ransomware group: • LOCKBIT Most targeted industries: • Manufacturing • Education • Financial Services	Most active ransomware group: • LOCKBIT Most targeted industries: • Construction • Business Services • Retail	Most active ransomware group: • LOCKBIT Most targeted industries: • Manufacturing • Government • Retail

Figure 2: Ransomware Activities

LOCKBIT 2.0 was the most active ransomware group in the last quarter, followed by Conti and ALPHV ransomware. LOCKBIT and Conti have remained the most active ransomware groups over the past year.

Cyble Research Labs tracked the activities of 27 active ransomware groups in Q1 – 2022 as listed below:

LOCKBIT				
HARON	Sabbath	Vice Society	RansomEXX	Ragnar_Locker
Conti	CL0P	LV	Lorenz	Cuba
Grief	XING LOCKER	Moses Staff	Everest	Rook
AvosLocker	BlackByte Auction	ALPHV	Quantum Blog	Arvin Club
Marketo	Ragnar_Locker	Suncrypt	Pandora Leaks	Payload
ENTROPY HALL OF FALL				

Figure 3: Active Ransomware groups

Nearly all the ransomware groups covered in this report use the double/triple extortion method and steal data before encrypting it. Now more than ever, organizations need to implement robust data backup and restoration capabilities following an attack to recover their data and operational capability.

In the Russia-Ukraine conflict so far, we witnessed certain Threat Actors encrypting victims' systems but did not ask for ransom. These TAs did not exfiltrate the victim's data either, highlighting how politically motivated TAs use such malware strains to carry out their attacks.

Ransomware groups typically use strong encryption algorithms such as AES-256 to prevent the breaking of ciphers. Additionally, we have observed most ransomware groups deleting shadow files to further inhibit data recovery.

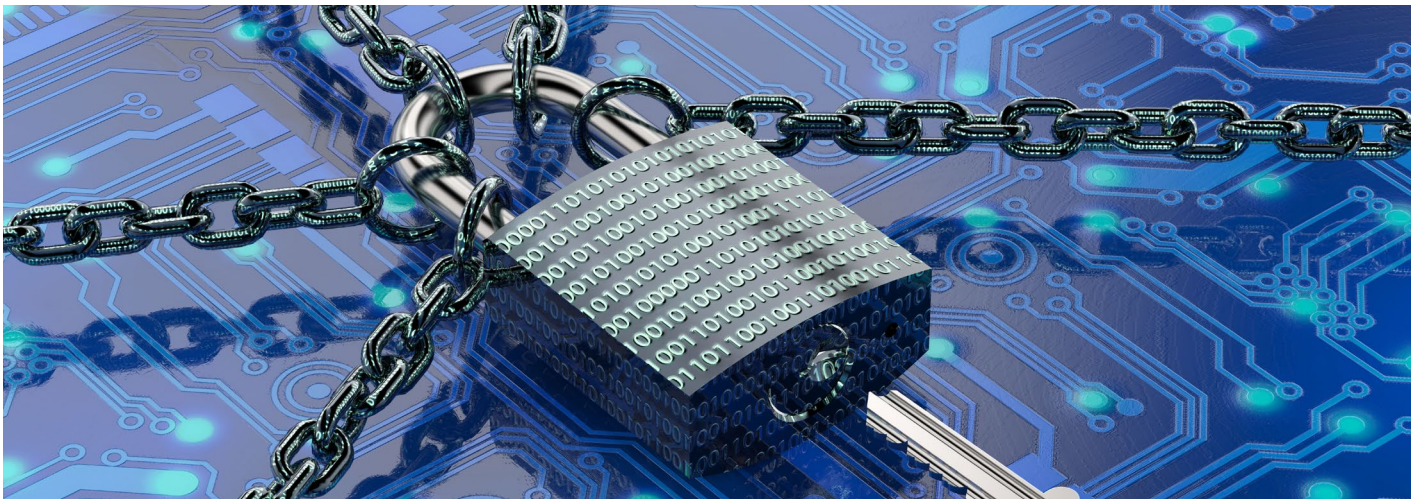


Figure 4 shows the common TTPs used by Ransomware groups. One of the standard techniques that multiple ransomware groups use is Inhibiting System Recovery (T1490). This technique deletes shadow files, and ransomware groups additionally adopt various obfuscation techniques for stealth.

Technique ID	Technique Name
T1486	Data Encrypted for Impact
T1490	Inhibit System Recovery
T1027	Obfuscated Files or Information
T1112	Modify Registry
T1083	File and Directory Dicovery
T1135	Network Share Discovery
T1059	Command and Scripting Interpreter
T1134	Access Token Manipulation
T1548	Abuse Elevation Control Mechanism
T1562	Impair Defenses

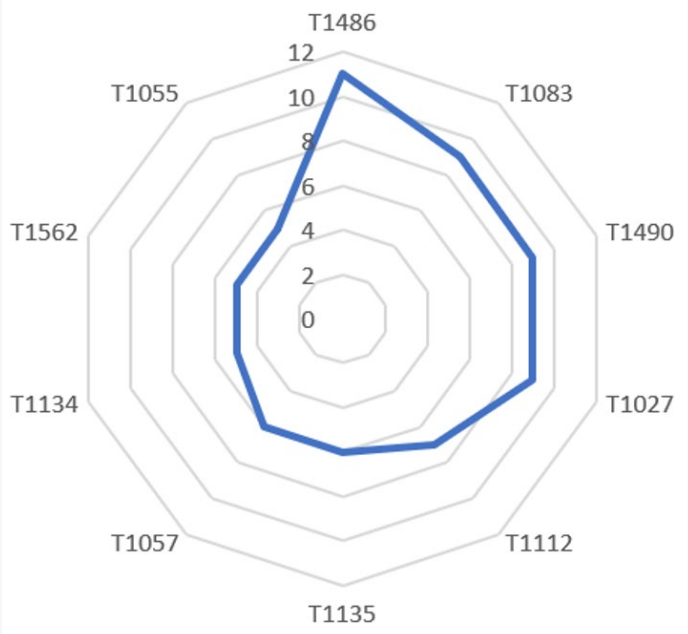


Figure 4: Common TTPs

The figure below shows the top 15 ransomware groups in Q1 2022. LOCKBIT and Conti are the only ransomware groups that have been aggressively carrying out their operations over a long period.

ALPHV, Cuba, and Suncrypt ransomware groups had a surge in ransomware victims in Q1 2022 by over 100% compared with their activities in Q4 2021. Certain ransomware groups like Sabbath, Pysa, and Grief were less prevalent than in Q4 2021.

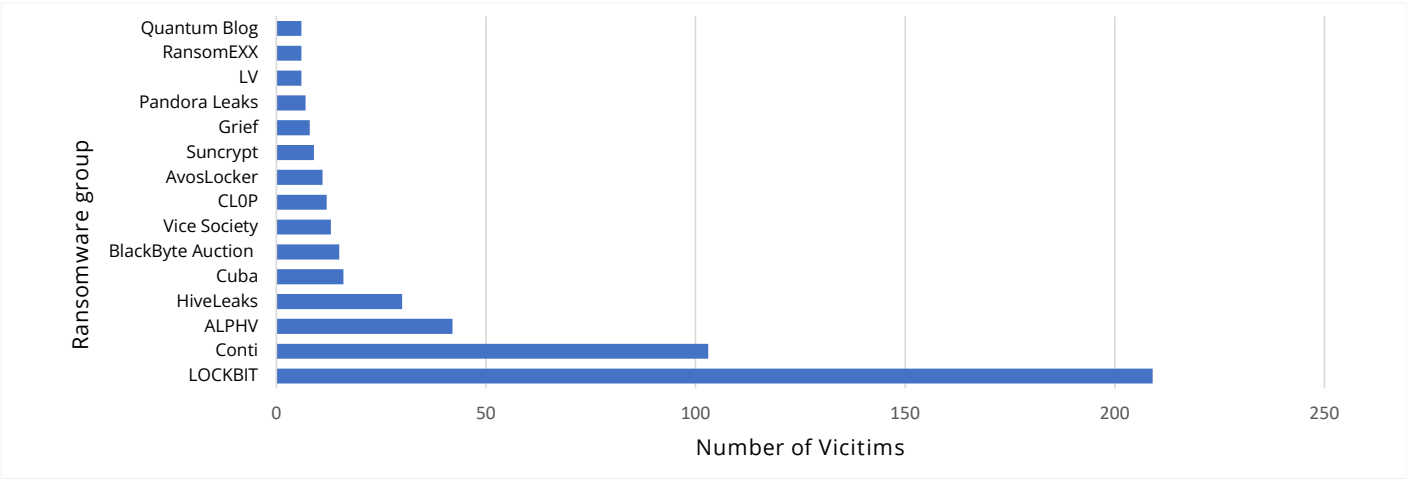


Figure 5: Top 15 ransomware groups

Ransomware groups attacked **62 countries in Q1 2022**, including:

- United States
- United Kingdom
- Italy
- Germany
- Canada
- France
- Spain
- Switzerland
- China
- Netherlands
- Brazil
- India
- Mexico
- Australia
- Austria
- Argentina
- Turkey
- Sweden
- United Arab Emirates
- Japan
- Colombia
- Singapore
- Belgium
- Denmark
- Lebanon
- New Zealand
- Finland
- South Korea
- South Africa
- Indonesia
- Hongkong
- Kuwait
- Thailand
- Venezuela
- Senegal
- Costa Rica
- Luxembourg
- Europe
- Malaysia
- Israel
- Bangladesh
- Saudi Arabia
- Barbados
- Serbia
- Dominican Republic
- Slovenia
- Tanzania
- Chile
- Tunisia
- Congo
- Unidentified
- Bahrain
- Bahamas
- Czech Republic
- Egypt
- Hungary
- Portugal
- Romania
- Ecuador
- Norway
- Poland
- Jordan

Figure 6: Heat Map

Over the past year, the United States is still the most targeted country,. Switzerland, Argentina, Netherlands, Austria, Mexico, and Italy had Quarter-on-Quarter (QoQ) increase in ransomware attacks. Out of 62 countries attacked, over 40% of victims were from the United States.

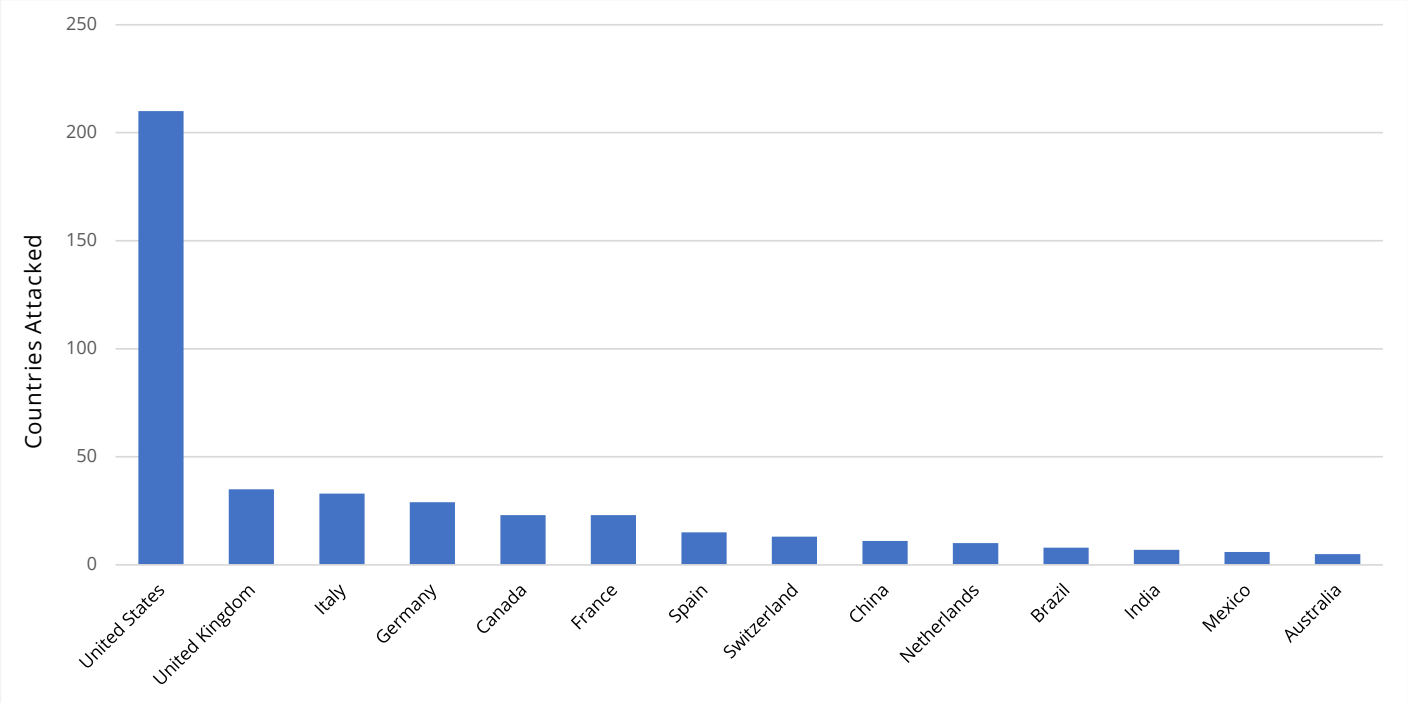


Figure 7: Top 14 most targeted countries

Q1 2022 witnessed an increase in the number of attacks on organizations working in the Financial Services, Insurance, and Pharmaceutical industries. Though the number of victims observed in the Automotive sector in Q1 2022 was less than in previous quarters, major players in this industry were impacted by ransomware attacks. The figure below shows the top 10 industries targeted by ransomware groups.

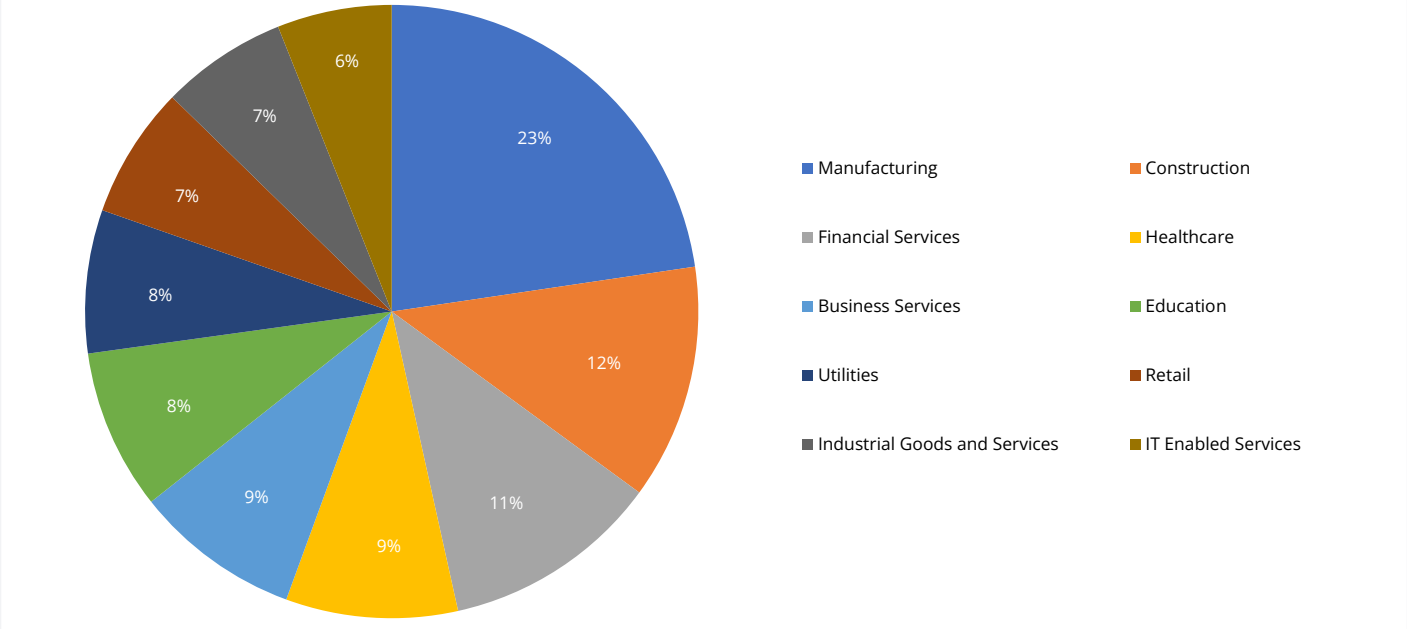


Figure 8: Top 10 most targeted industries

Spotlighted Ransomware Attacks in Q1

In Q1 2022, Conti, LOCKBIT, and ALPHV groups were behind the major ransomware attacks.

The figure below showcases the timeline of ransomware activities in Q1 2022.

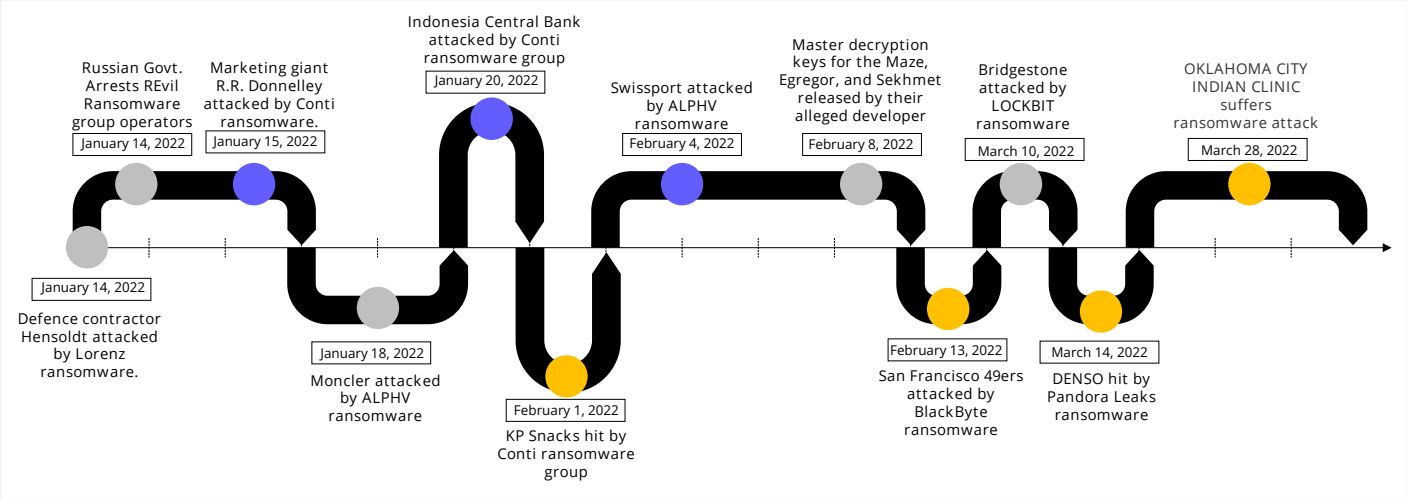


Figure 9: Timeline of ransomware activities

1. HENSOLDT Holding Germany:

This company was attacked by Lorenz ransomware in December 2021, and the incident was disclosed in January 2022. The Threat Actor exfiltrated over 200GB of data in this attack. Hensoldt is a multinational defense contractor headquartered in Germany. The Lorenz ransomware group has been active since April 2021. It tends to follow the double extortion method - in addition to demanding a ransom; they threaten to sell/leak the exfiltrated data.

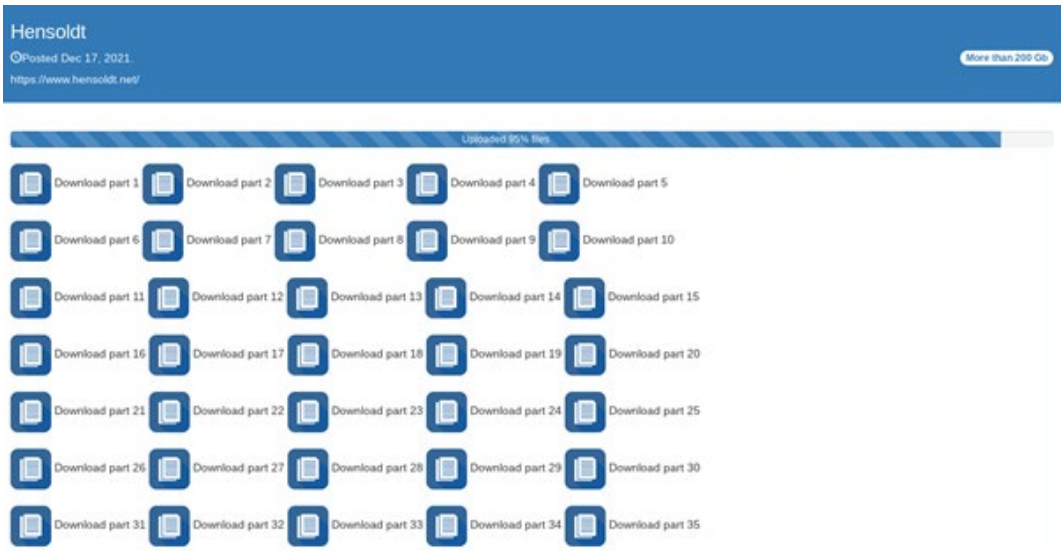


Figure 10: Lorenz ransomware leak site

2. RR Donnelly:

RR Donnelly is a significant player in the Media industry headquartered in the United States. Also known as RRD, it provides marketing and business communications-related services. RRD was attacked by Conti ransomware in January 2022. Conti ransomware has been working on the Ransomware-as-a-Service model and has been active since late 2019. It is suspected that the victim organization paid the ransom as the post made by Conti ransomware on their leak site regarding RRD was removed within 2-4 days.

3. Bank of Indonesia:

The Bank of Indonesia is the central bank of the Republic of Indonesia. It was attacked by Conti ransomware on January 20, 2022. Over 350GB data has been exfiltrated by the TA. During our analysis, we found that this data is from over 200 systems and contains sensitive information about the infrastructure of the Bank of Indonesia. Confidential documents and customers data may be leaked in the future.

Figure 11: Conti ransomware leak site

4. Swissport:

Swissport International Ltd. is an aviation services company that provides airport ground, lounge hospitality, and cargo handling services at 285 airports in 45 countries across the globe. ALPHV/BLACKCAT attacked Swissport on February 4, 2022. The TA claims to have exfiltrated over 1.5 TB of data. ALPHV is a new ransomware group active since Q4 2021, operating on the Ransomware-as-a-Service model.

Spotlighted Ransomware Attacks in Q1

Figure 12: ALPHV ransomware leak site

5. San Francisco 49ers:

The San Francisco 49ers are an NFL team based in the San Francisco Bay Area. The team is ranked as the sixth-most valuable NFL franchise on Forbes' list at $4.5 billion. On February 13, 2022, the San Francisco 49ers were attacked by BlackByte ransomware. The BlackByte ransomware group has been active since Q3 2021. The group has leaked over 8GB of the victim's data on their leak site.

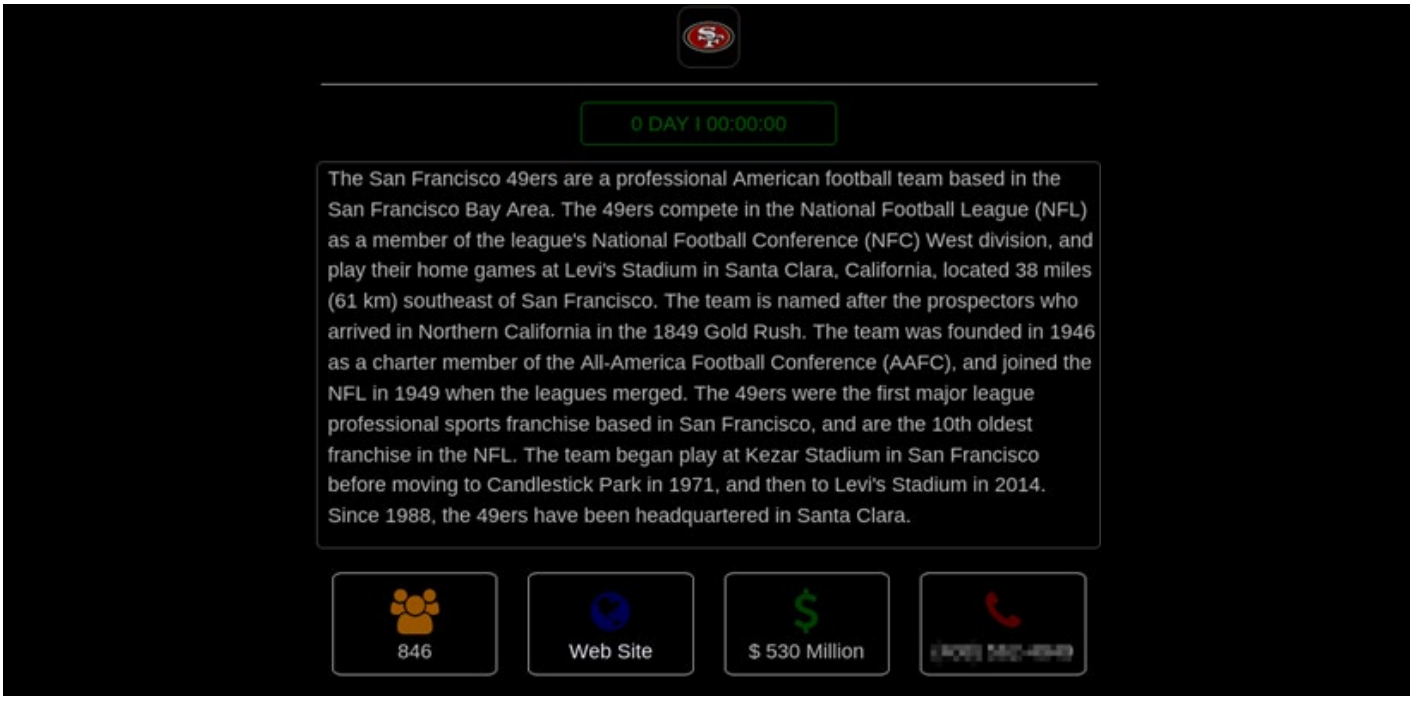


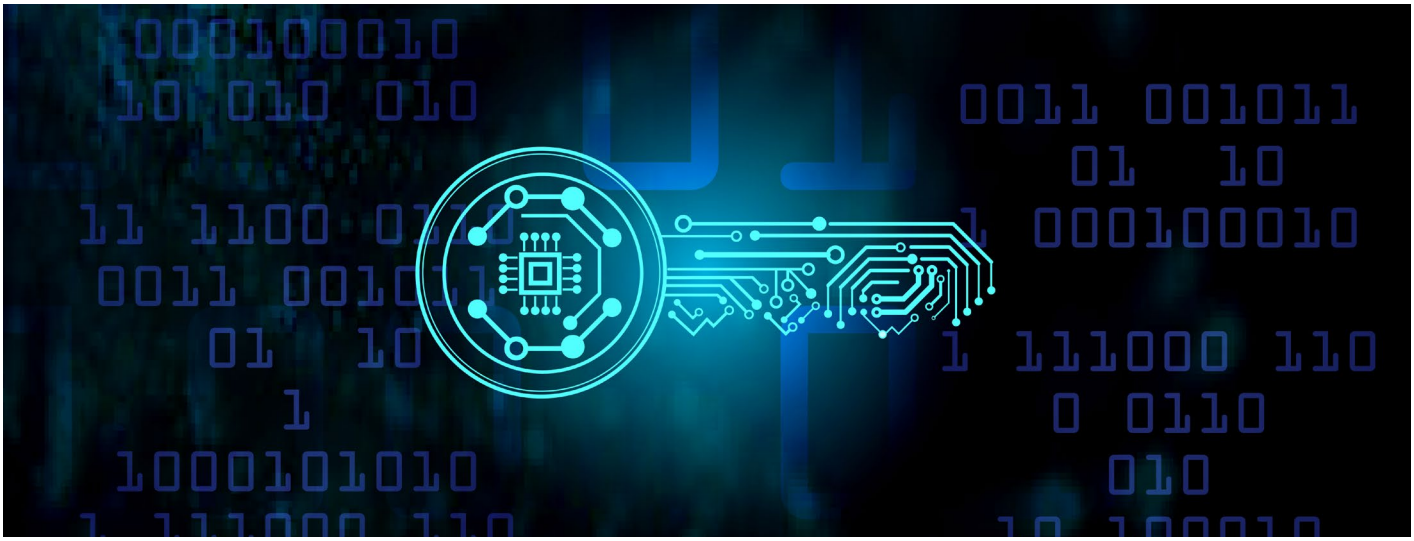
Figure 13: BlackByte ransomware leak site

Spotlighted Ransomware Attacks in Q1

6. Bridgestone Americas:

Bridgestone Americas, Inc. is a subsidiary of Bridgestone Corporation. They provide sustainable mobility and advanced solutions worldwide. On March 10, 2022, the LOCKBIT Ransomware Group attacked Bridgestone Americas. LOCKBIT ransomware group is operating on the Ransomware-as-a-Service model. As shown in the figure below, the TA has leaked the stolen data on the extortion site.

Figure 14: Lockbit ransomware leak site



Night Sky ransomware:

The Night Sky is another ransomware group that uses double extortion to target its victims. The group was discovered on January 1, 2022. The group had 2 victims mentioned on their leak site, both from Asian countries. Some researchers claim that this group originated from China. After January 2022, their leak site went down. It is tricky to comment on whether the group is still operational based on the current scenario.

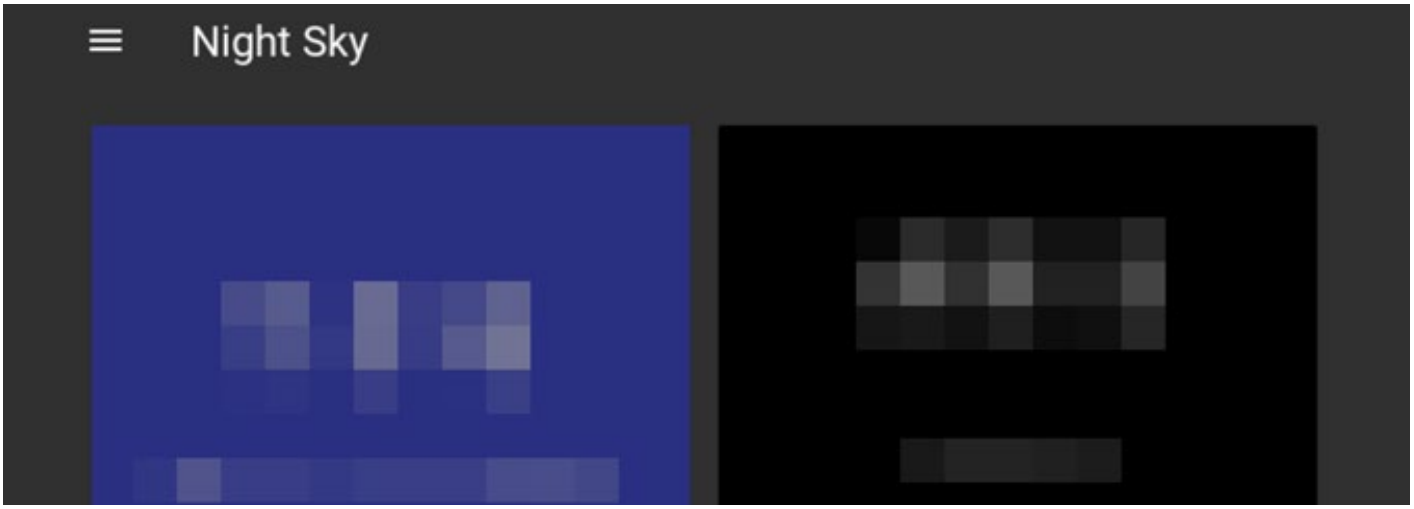


Figure 15: Night Sky ransomware leak site

Pandora Leaks ransomware:

Pandora ransomware came into the spotlight in March 2022 after targeting some high-profile victims on its leak site. The ransomware group announced its first victim on February 21 2022, and has posted around seven victims at the time of publishing this report. Cyble Research Labs' in-depth analysis of this ransomware group concluded that there is a high possibility that Pandora is a rebrand of Rook ransomware. Over 50% of its victims are headquartered in the United States, and the rest in Japan. The majority of the group's victims are from the Financial Services industry, with one high-profile victim from the automotive industry.

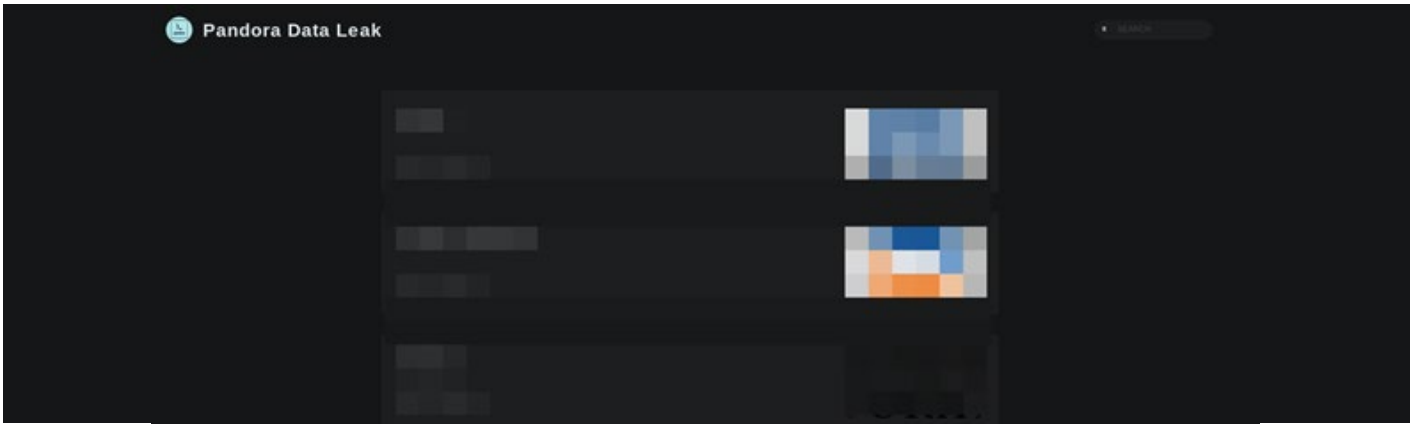


Figure 16: Pandora ransomware leak site

Ransomware taking a jab at NAS devices

Network Attached Storage, abbreviated as NAS, is a storage device connected to a network used to create backups and retrieve files from remote locations. Researchers determined that ransomware such as DeadBolt, eCh0raix, and qlocker targeted NAS devices.

It's suspected that TAs are gaining initial access to these devices by either exploiting unpatched vulnerabilities or targeting unsecured Internet-facing NAS instances. According to a report, around 5000 instances of QNAP NAS devices were infected with this malware in January 2022 alone. The figure below shows the devices impacted with DeadBolt ransomware recently.

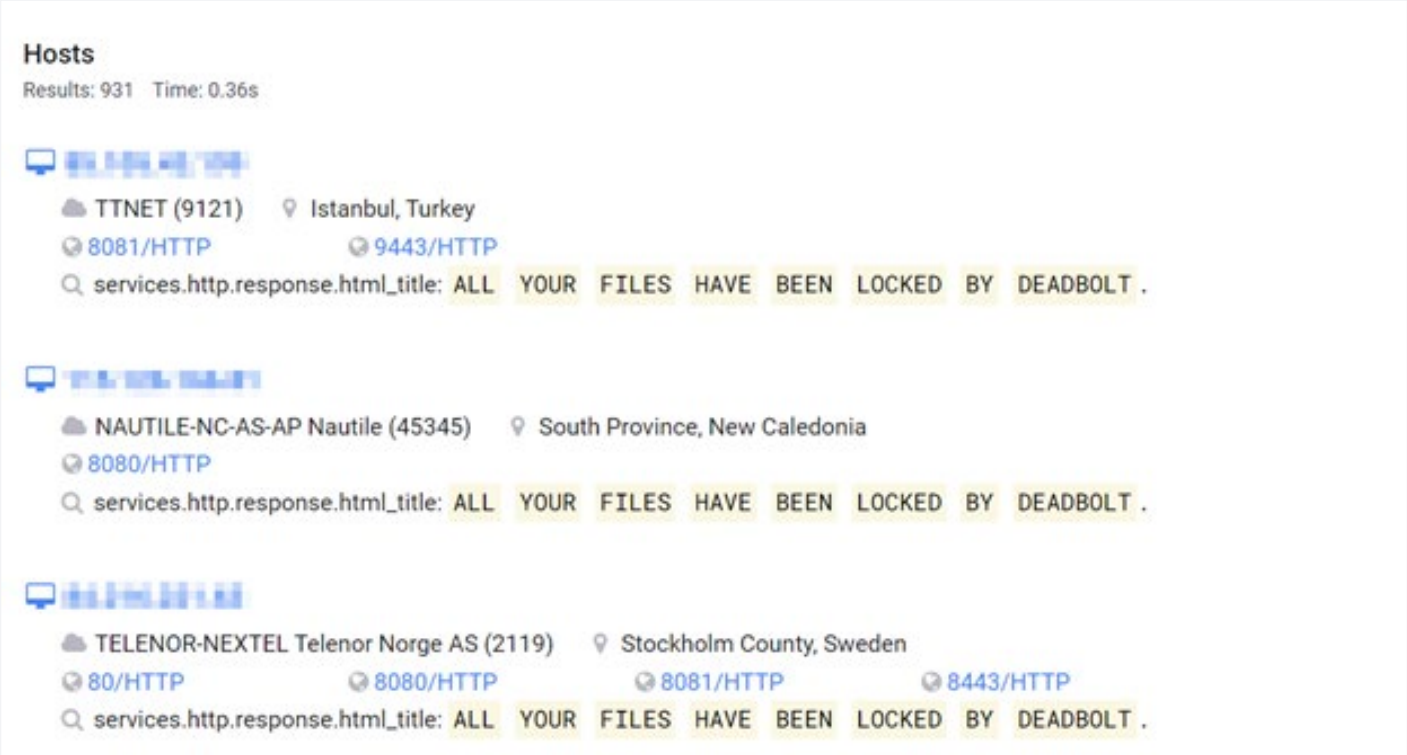


Figure 17: Censys search results for NAS devices impacted with Deadbolt ransomware

In Q1 2022, DeadBolt ransomware was observed attacking multiple vendors of NAS devices which, including QNAP and ASUSTOR. The TA behind this ransomware demands 50 Bitcoin (BTC) as a ransom for the master decryption key (which can be used to decrypt data of all victims) and claims to be targeting zero days in both QNAP and ASUSTOR based devices.

Darkweb Insights and Incidents impacting ransomware operations

Increased scrutiny and action by Law Enforcement Agencies

Q1 2022 started with the arrest of 15 alleged members of the REvil ransomware group by the FSB, the principal Russian security agency, which surprised the entire cybersecurity industry. It's suspected that several ransomware group members have their roots in Russia and do not attack organizations based out of Russia. As per the TA's belief, they were loyal to their motherland, which would insulate them from Law Enforcement. Clearly, this was not the case.

Russia is often called a haven for cybercriminals. After FSB arrested REvil members, we witnessed a decline in attacks by most ransomware groups, highlighting that these operations might be forcing ransomware operators to narrow their targeting scope.

At the end of January, one of NetWalker ransomware's affiliates was sentenced to 7 years in prison in Canada and was arrested in 2021. The Justice Department stated that the NetWalker affiliate earned over $27M through ransomware operations.

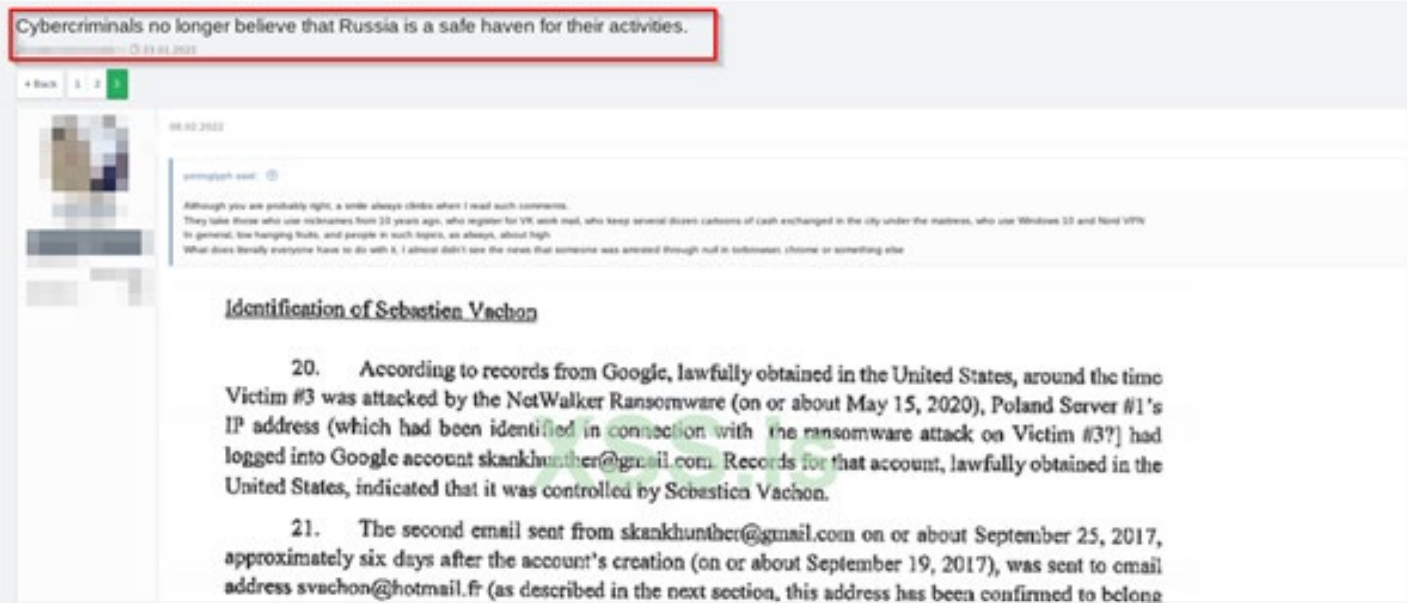


Figure 18: Darkweb chatter

Yaroslav Vasinskyi, a REvil affiliate behind the Kaseya ransomware attack, was also extradited to the United States at the beginning of March 2022.

Darkweb Insights and Incidents impacting ransomware operations

How has the Russia-Ukraine conflict affected Ransomware operations?

As the Russia-Ukraine conflict escalated, many Threat Actors voiced their views and sided with either Russia or Ukraine. Consequently, politically motivated and hacktivist groups also started jumping into the cyberwar. We have observed similar cyberwarfare activities from ransomware groups on both sides of the conflict.

Conti announced its full support for the Russian Government, as shown in the figure below.

Figure 19: Conti Statement on Russia Ukraine war

One of the TAs based out of Ukraine didn't agree with Conti's support towards the Russian Government and decided to leak its internal Jabber chats and ransomware source code. Researchers were able to identify a lot of Personally Identifiable Information (PII) belonging to Threat Actors.

This leak revealed that Conti operated like a corporation and had around 100 individuals on its payroll. Certain findings also indicated that Conti's Leader might be associated with FSB. Using these findings, researchers were able to identify recent TTPs and active infrastructure.

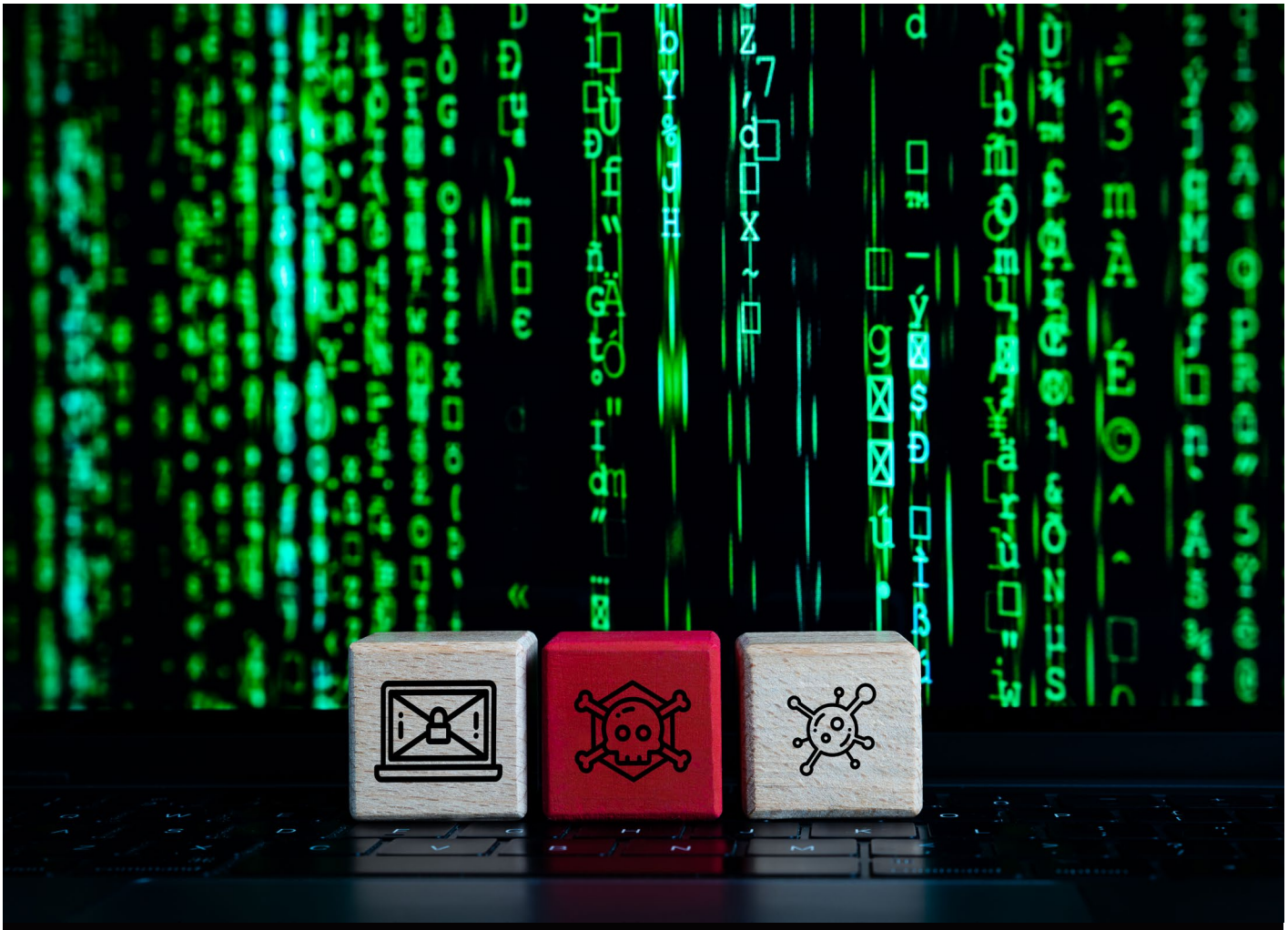
These findings assisted multiple organizations in fine-tuning their detection of such threats. Due to this leak, Conti lost its affiliates, but Conti is still active, and in the future, we could expect some rebrands and updated TTPs.

Ransomware Collaborations

Ransomware collaborations are a matter of concern as resources from multiple groups can be utilized to carry out attacks. Conti's leaked Jabber data also provided insights about their collaboration with other ransomware groups. We also came across an instance in which HARON/MIDAS and ALPHV ransomware posted the same victim on their leak site with the same data as shown in the figure below. The modus operandi for this attack is unclear so far. However, there are chances that these groups are associated or working together.

Figure 20: Possible association between two ransomware groups

Future Predictions



We may witness increased ransom amounts demanded by ransomware groups as Law Enforcement agencies are actively taking down Threat Actors involved with Ransomware activities. TAs might thus try to reduce the scope of attacks and increase ransom to maintain a Risk-Reward balance.

We might see multiple rebrands coming in the future, as rebranding is one of the techniques used by TAs so that they don't remain highlighted for a long time.

Other TAs can use Conti's leaked data to create a new ransomware group. Recently, a group named NB65 was observed operating with Conti's modified source code. Other TAs might repurpose the leaked code for their uses as well.

How to protect yourself from Ransomware Attacks

With Threat Actors and their TTPs increasing in sophistication, 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
- 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 and contractors
- 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 wherever possible and pragmatic

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 2021 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, Dubai and India, Cyble has a global presence.

To learn more about Cyble, visit www.cyble.com