CYBLE

Q3 – 2022

Ransomware Report

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Ransomware Threat Landscape in Q3-2022 witnessed a subtle shift indicating a growing awareness of the prevention of ransomware-related crime among organizations. Cyble Research and Intelligence Labs (CRIL) investigated the ransomware attacks in Q3 to connect dots across various ransomware activities and further mitigate the risk of these attacks.

Despite an economic slowdown, enterprises are increasing their spending on resilient cybersecurity infrastructure and ransomware insurance. However, these remain trifling and are found wanting for a cyber security strategy that encompasses not just technology but also the various essence of the human element.

The cybersecurity incidences in the last quarter portray a lack of implementation of cybersecurity hygiene in patching vulnerabilities, data governance policies, misconfigured cloud infrastructure, and complacent access management, to name just a few among the long list of "don'ts" that were prevalent in Q3.

Q3-2022 witnessed numerous upshots in the ransomware threat landscape. Prominent ransomware groups have shifted their tactics from targeting large businesses to small-medium scale industries. Smaller businesses have relatively limited cybersecurity resources and budgets but are still a critical link to the value-chain that might aid ransomware groups in infiltrating large business networks via numerous techniques.

It has been observed that small businesses cannot afford the ransoms, yet ransomware groups are monetizing their exploits by selling such data leaks - partially or in their entirety - on popular cybercrime forums. CRIL has observed an uptick in such activities and subsequently enumerated them in this report.

Ransomware operators continue to evolve with new extortion techniques, further elaborated in detail in this report. Though these are observed every quarter, and a single logic cannot attribute to these variations, the common factor remains declining ransom payouts, which explains the variation that we have observed in Ransomware group's TTPs.

CRIL corroborated incidences from darkweb and underground forums about ransomware groups experiencing DDoS (Distribute Denial of Service) attacks on their leak sites to prevent them from leaking victim data. Even in such instances, ransomware groups took refuge in cybercrime forums to maintain their hegemony.

In our Q2-2022 report, our predictions of increased adoption of unconventional programming languages such as Rust and Go by ransomware groups were validated with the emergence of a new ransomware 'BianLian' based on the Go language in Q3.

As a result of the present geopolitical tensions between China and Taiwan, there has been an increase in ransomware activities and other cyberattacks on Taiwanese entities. Taiwan-based corporations are imperative to the global supply chain, especially in Technology, IT, and Manufacturing sectors. However, the ransomware groups that were swayed into targeting organizations based on their geopolitical value in the Russia-Ukraine conflict at the start of the year were gradually aligning themselves in Q3 towards East/South-East Asian countries. We expect this trend to continue for the foreseeable future, alongside the conventional cherry-picking of victims.

QUARTERLY RANSOMWARE OUTLOOK

Cyble Research & Intelligence Labs (CRIL) 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 Third Quarter of 2022.

- Total victims: **538**
- Active Ransomware Groups: **26**

MOST AFFECTED COUNTRIES

United States	France	United Kingdom	Germany	Canada
220	32	28	25	19

MOST ACTIVE RANSOMWARE GANGS

LOCKBIT	BlackBasta	Alphavm	HiveLeaks	AvosLocker
220	54	47	43	22

TOP 5 IMPACTED INDUSTRY SECTORS

- Professional Services
- Construction
- Manufacturing
- IT & ITES
- Healthcare

QUARTERLY RANSOMWARE OUTLOOK

CRIL identified 538 ransomware victims in Q3-2022 compared to 565 in Q2 – a **4.7% decline** Quarter-over-Quarter (Q-over-Q). Our ransomware victim-to-country ratio data indicates that over 50% of victim organizations were primarily concentrated in 3 countries - the United States (US), France, and United Kingdom (UK).

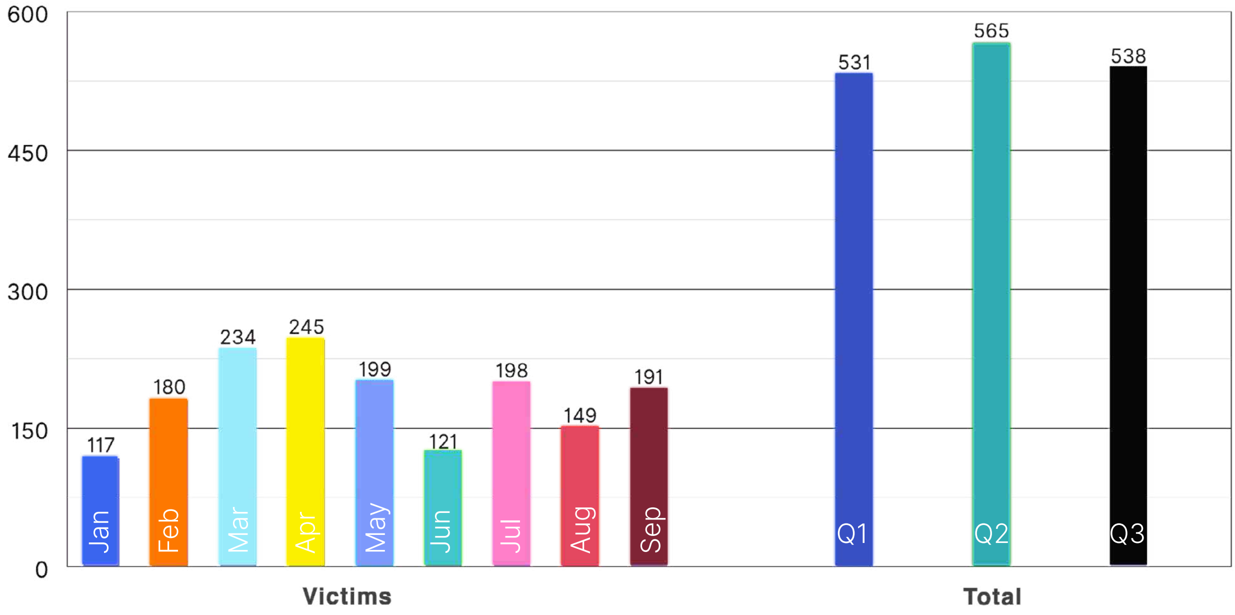


Figure 1 – Comparative analysis of ransomware activities Q-over-Q

GLOBALIZED RANSOMWARE THREAT LANDSCAPE

In Q3-2022, we observed ransomware activities escalating to 76 countries – a **50% Q-o-Q rise** from what we previously observed (50 countries).

Both the above observations indicate the growing scope of ransomware group activities in other countries, particularly those with relatively lower cybersecurity spending or where data protection policies are less prevalent.

The US was the most affected nation due to ransomware activities, but we have observed a downward trend in the victim count from 227 in Q2 to 220 in Q3. Similarly, in Q2, 40 organizations based out of Germany were affected, which reduced to 25 in Q3-2022. France has replaced Germany as the second most affected country in this quarter. UK organizations remained the third most widely targeted but with a slight decrease from the previous quarter (29 in the previous quarter compared to 28 in Q3).

In the **Americas**, alongside the US and Canada, we observed Brazil, Mexico, and Colombia also being targeted.

Europe was the second most ransomware-affected region, with 172 ransomware victims. Besides Germany, 16 Italian organizations were plagued by ransomware, with 14 in Spain.

The **Middle East, Turkey & Africa (META)** was the least affected region, while in **APAC and Oceania – Australia, Taiwan, and India** witnessed an increase in ransomware incidents.

The figure below showcases the geographical distribution of major ransomware activities across the globe in Q3-2022.

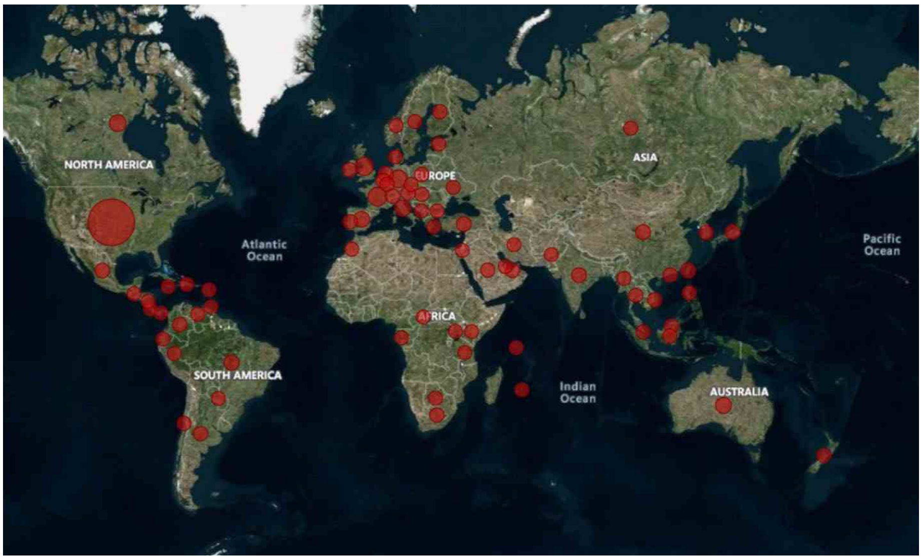


Figure 2 – Geographical distribution of Ransomware Activity

Traditionally, **LOCKBIT** has been the **most active ransomware group** in 2022 and remained so in Q3-2022, with 220 victims. LOCKBIT is closely trailed by Black Basta and ALPHV ransomware groups, respectively. **Black Basta** replaced ALPHV in Q2-2022 as the **second most active ransomware group**.

MICROANALYSIS OF RANSOMWARE ACTIVITIES

LOCKBIT was peculiarly observed to have changed its tactics from targeting multi-million dollar organizations to small-scale entities.

A new ransomware group by the moniker 'BianLian' surfaced in Q3 and maliciously affected over 20 organizations. BianLian is among the top 10 active ransomware groups observed in Q3-2022. Onyx ransomware surfaced in Q2-2022 and rebranded itself under the name 'VSOP' in Q3.

CRIL covered activities of 26 ransomware groups in Q3-2022, which rose from 25 in Q2-2022. Other **new ransomware groups** identified this quarter and highlighted in yellow in the graph below were - **0mega, Diaxin Team, IceFire, LILITH, RedAlert, and Bl00dy.**

Further, we observed nil activities from previously active ransomware groups – **ArvinClub, Suncrypt, BABUK 2.0, and Mindware** in Q3-2022.

The figures below indicate the comparative analysis of ransomware attacks by various groups in Q-over-Q.

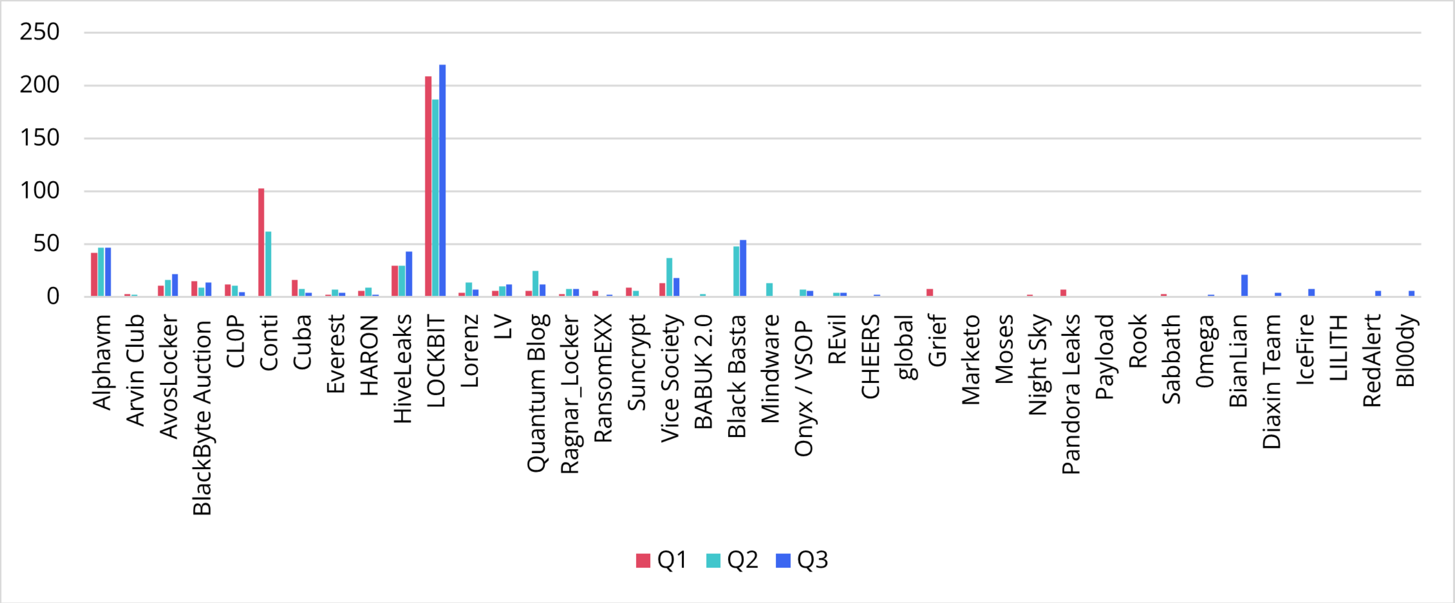


Figure 3 – QoQ Ransomware Attack Trends

MICROANALYSIS OF RANSOMWARE ACTIVITIES

LOCKBIT targeted 220 organizations in Q3-2022, a **17% rise compared to Q2**, primarily from the Professional Services, Manufacturing, and Construction industries. LOCKBIT was also the most active group with the highest number of victims in the top three ransomware-affected countries – 70 in the US, 28 in France, and 5 in the UK.

Incidentally, LOCKBIT was more inclined to victimize German corporations compared to the previous quarter; in Q3, we observed them disproportionately targeting French corporations instead. Other active ransomware groups that primarily target US organizations were Black Basta, HiveLeaks, and Alphavm.

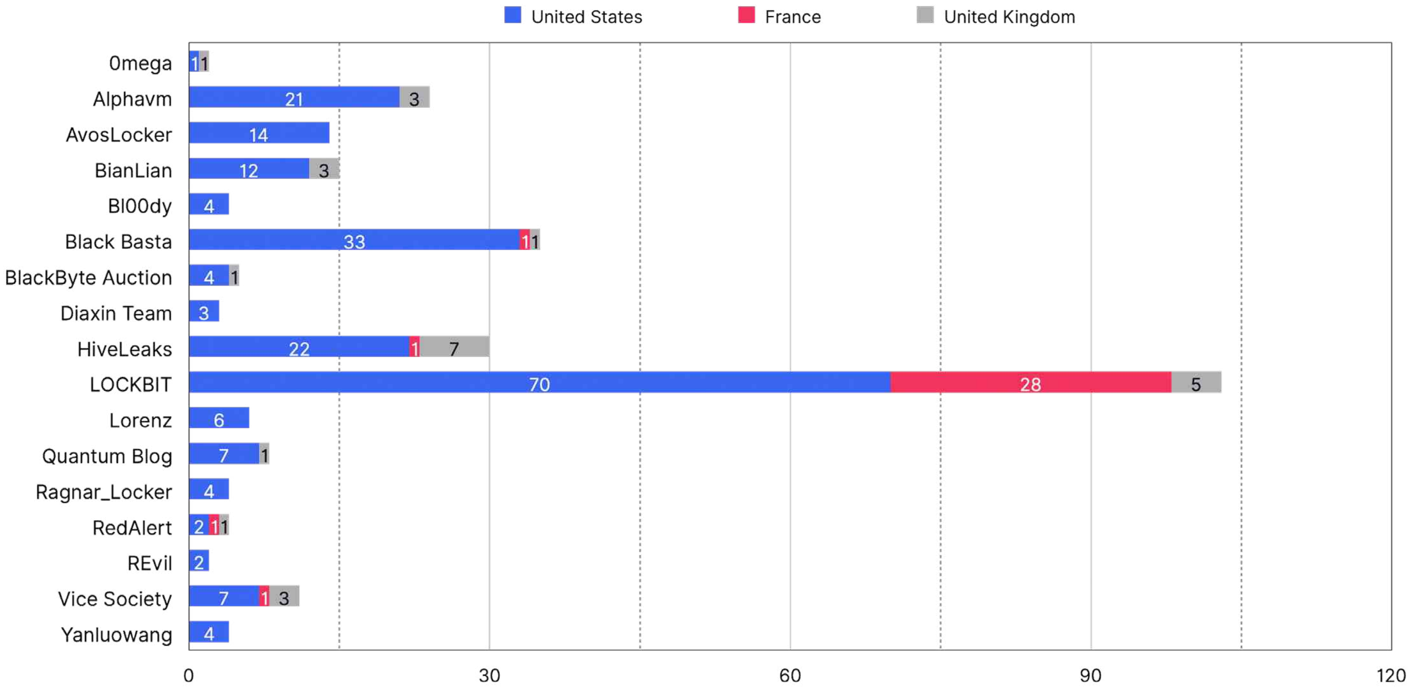


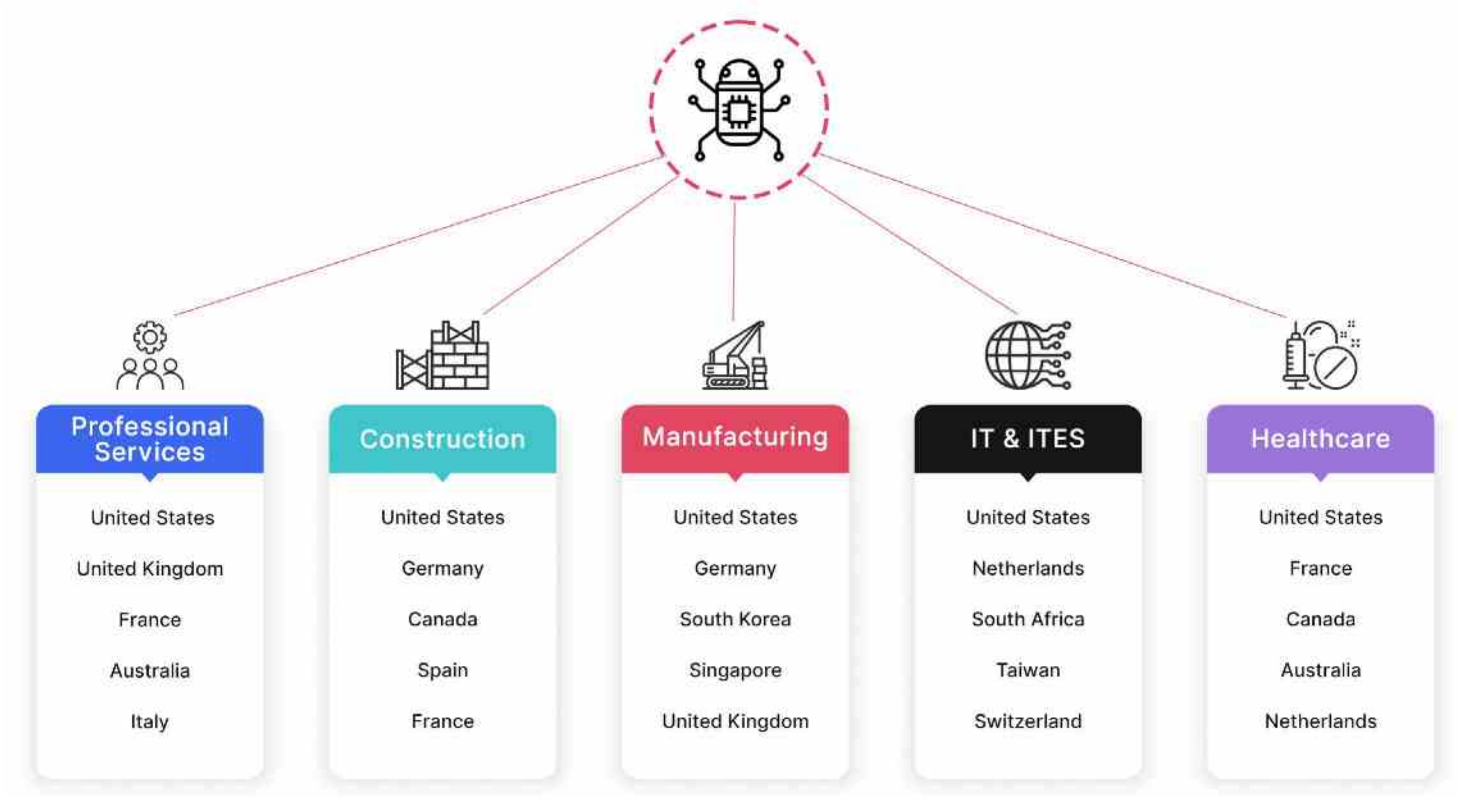
Figure 4 – Distribution of Ransomware Attacks for the 3 most affected nations

RANSOMWARE SECTORAL IMPACT

Ransomware groups mostly had a similar sectoral footprint in Q3-2022, as observed in Q2-2022, except the IT & ITES replaced the Government & LEA organizations to emerge in the 5-most affected entities. We can infer from the number of victims and continuing trends from Q2-2022, that US-based businesses suffered the highest number of ransomware incidents in the five most affected industrial sectors.

LOCKBIT vigorously attacked French companies from the Services, Construction & Healthcare sectors. South Korea and Singapore-based Manufacturing entities were the newly-observed victims in the sector. As highlighted earlier in this report, Taiwanese multinational corporations from the IT & ITES sectors were disproportionately targeted to disrupt their entire value chain.

In Q3, the five most targeted industries by ransomware groups were:



Professional Services	Construction	Manufacturing	IT & ITES	Healthcare
United States	United States	United States	United States	United States
United Kingdom	Germany	Germany	Netherlands	France
France	Canada	South Korea	South Africa	Canada
Australia	Spain	Singapore	Taiwan	Australia
Italy	France	United Kingdom	Switzerland	Netherlands

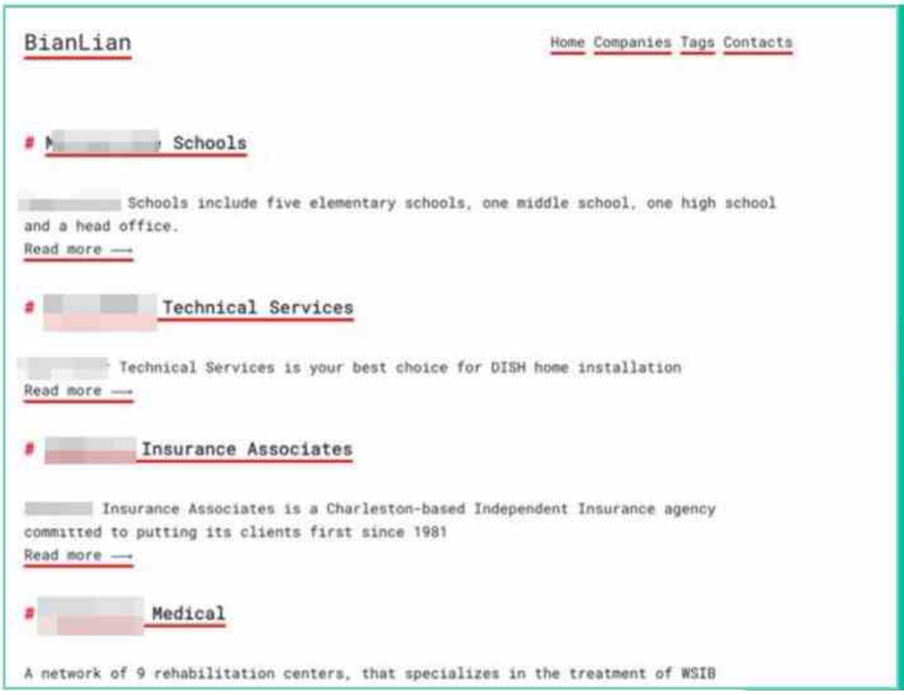
Figure 5 – Five most targeted industries by ransomware groups

EVOLVING RANSOMWARE THREAT PROFILE

Cyble Research & Intelligence Labs worked on profiling new ransomware groups in Q3-2022 to forewarn our readers about their activities in the dynamic ransomware threat landscape.

BianLian

BianLian ransomware has cross-platform functionalities, making reverse engineering more difficult.



BianLian

[redacted] Schools

[redacted] Schools include five elementary schools, one middle school, one high school and a head office.

Read more ⟶

[redacted] Technical Services

[redacted] Technical Services is your best choice for DISH home installation

Read more ⟶

[redacted] Insurance Associates

[redacted] Insurance Associates is a Charleston-based Independent Insurance agency committed to putting its clients first since 1981

Read more ⟶

[redacted] Medical

A network of 9 rehabilitation centers, that specializes in the treatment of WSIB

Ransomware Group : BianLian

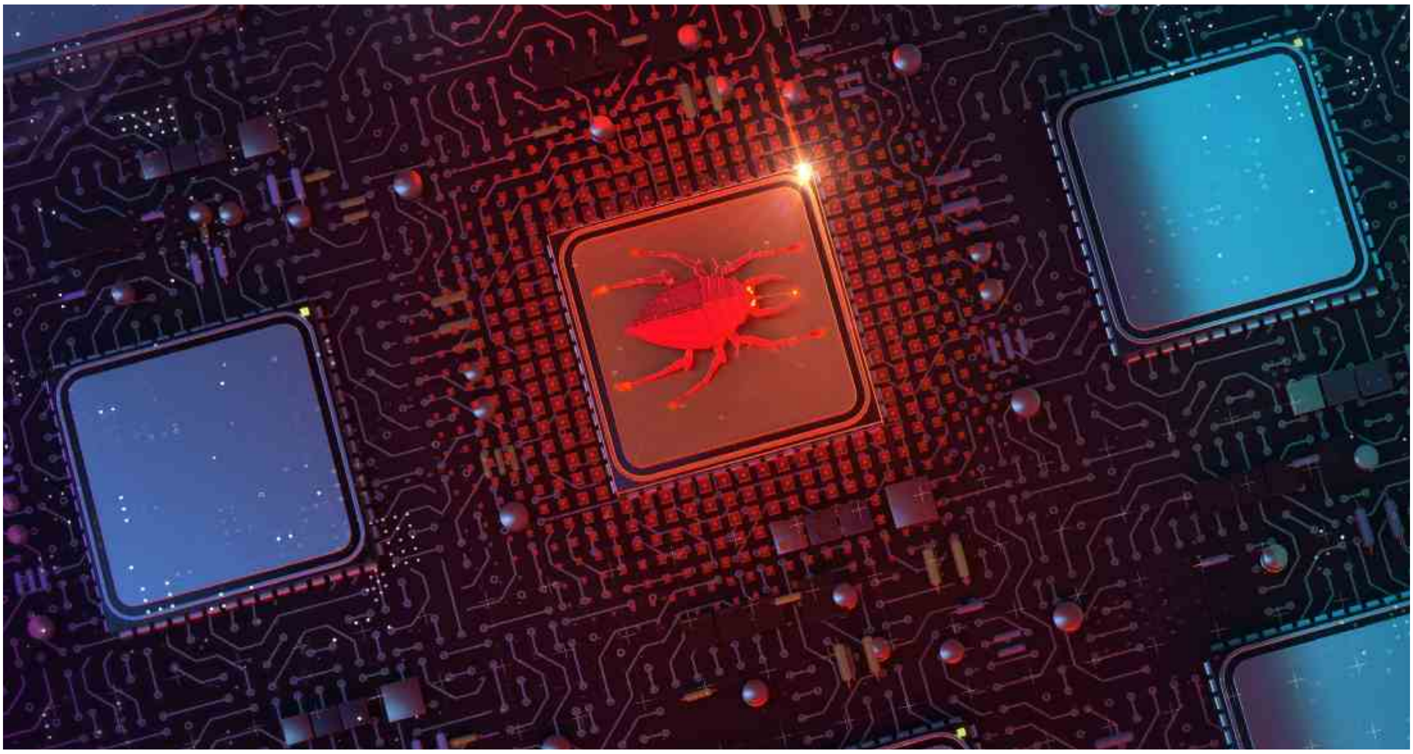
Programming Language: GoLang

Total Countries Targeted: 6

Total Victims: 21

Most targeted Industries: Manufacturing, Media & Entertainment, Healthcare

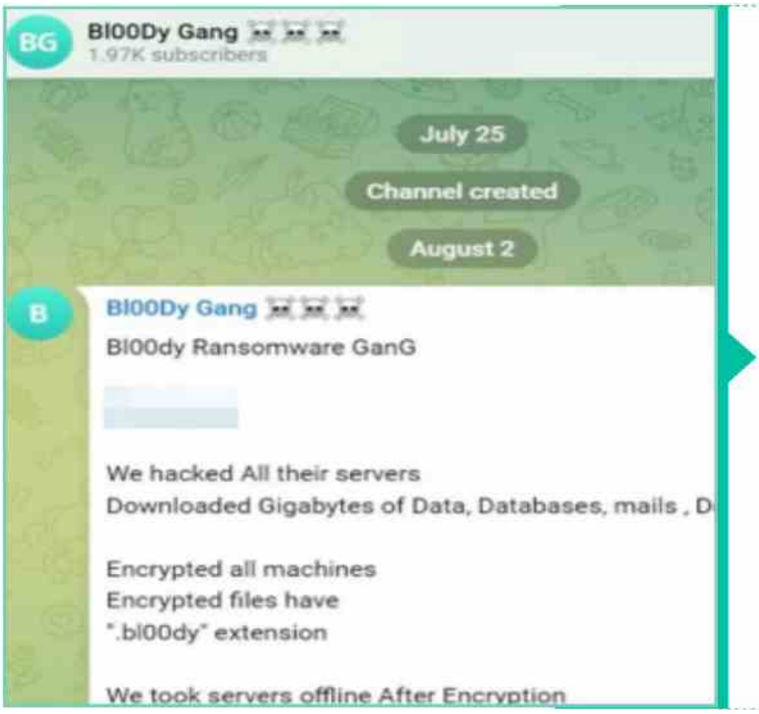
Most Targeted Countries: United States, United Kingdom, Australia



EVOLVING RANSOMWARE THREAT PROFILE

Bl00dy

Bl00dy ransomware is a new ransomware group that uses Telegram to post details of its victims. The group migrated from its earlier C/C++ coded payload to the leaked builder of LOCKBIT 3.0 ransomware. Upon execution, the ransomware would encrypt files on the victim's machine and appends the extension of encrypted files as ".bl00dy."



BlOODy Gang ☠☠☠
1.97K subscribers

July 25

Channel created

August 2

BlOODy Gang ☠☠☠

Bl00dy Ransomware GanG

We hacked All their servers
Downloaded Gigabytes of Data, Databases, mails , D

Encrypted all machines
Encrypted files have
".bl00dy" extension

We took servers offline After Encryption

Ransomware Group : Bl00dy

Programming Language: Using Different Payloads, possibly from leaked builders.

Total Countries Targeted: 3

Total Victims: 6

Most targeted Industries: Consumer Goods, Professional Services

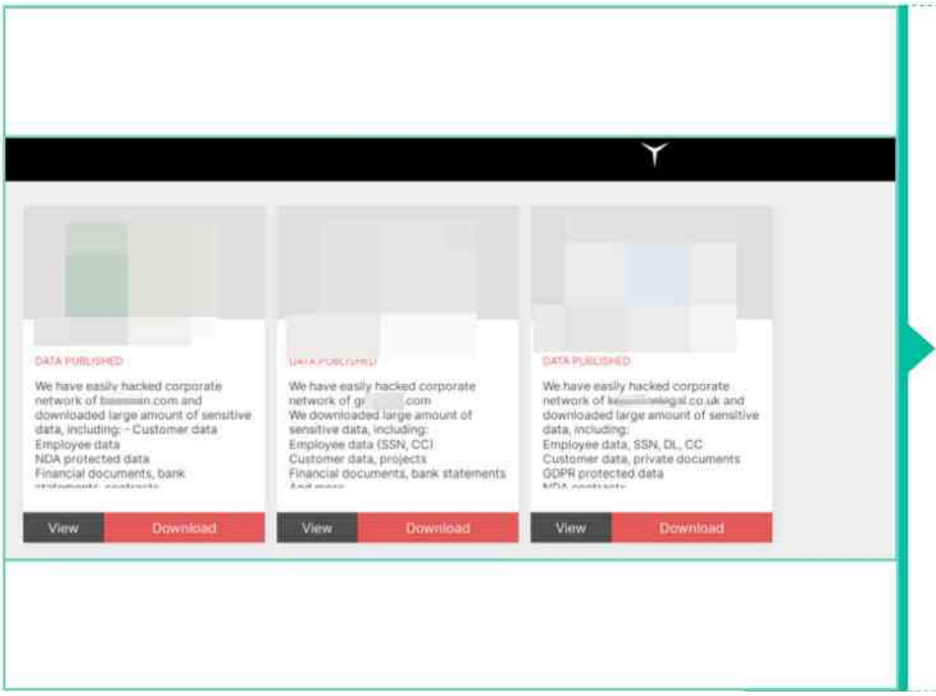
Most Targeted Countries: United States, Russia, Ukraine

EVOLVING RANSOMWARE THREAT PROFILE

RedAlert Ransomware

RedAlert or N13V is a new ransomware strain that targets both Windows and Linux VMWare ESXi servers on corporate networks. The ransomware stops all running virtual machines and encrypts any file related to virtual machines, such as virtual disks.

RedAlert Ransomware was named after a string with the same name in the ransom note, but threat actors named their campaign "N13V". RedAlert only accepts ransom payments in Monero(XMR), which is atypical for ransomware groups.



DATA PUBLISHED

We have easily hacked corporate network of [redacted]n.com and downloaded large amount of sensitive data, including: - Customer data
Employee data
NDA protected data
Financial documents, bank statements, contracts

DATA PUBLISHED

We have easily hacked corporate network of gr[redacted].com
We downloaded large amount of sensitive data, including:
Employee data (SSN, CC)
Customer data, projects
Financial documents, bank statements
And more

DATA PUBLISHED

We have easily hacked corporate network of k[redacted]egal.co.uk and downloaded large amount of sensitive data, including:
Employee data, SSN, DL, CC
Customer data, private documents
GDPR protected data
NDA contracts

Ransomware Group : RedAlert or N13V

Programming Language: C/C++

Total Countries Targeted: 5

Total Victims: 6

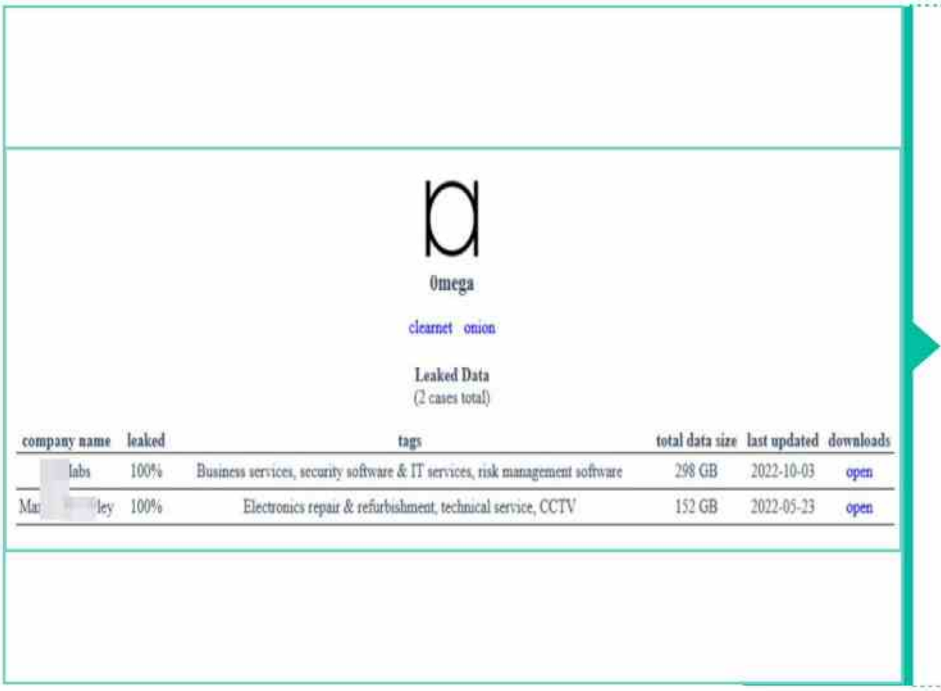
Most targeted Industries: BFSI, Construction, IT & ITES

Most Targeted Countries: United States, United Kingdom

EVOLVING RANSOMWARE THREAT PROFILE

0mega Ransomware

0mega ransomware came into the limelight around the first week of July 2022. This ransomware strain has disclosed details of two victims and targets organizations using double extortion techniques. The ransomware appends the files with the ".0mega" extension and creates ransom notes named "DECRYPT-FILES.txt."



0mega

clearnet onion

Leaked Data
(2 cases total)

company name	leaked	tags	total data size	last updated	downloads
[redacted]labs	100%	Business services, security software & IT services, risk management software	298 GB	2022-10-03	open
Ma[redacted]ley	100%	Electronics repair & refurbishment, technical service, CCTV	152 GB	2022-05-23	open

Ransomware Group : 0mega

Programming Language: Not Available

Total Countries Targeted: 2

Total Victims: 2

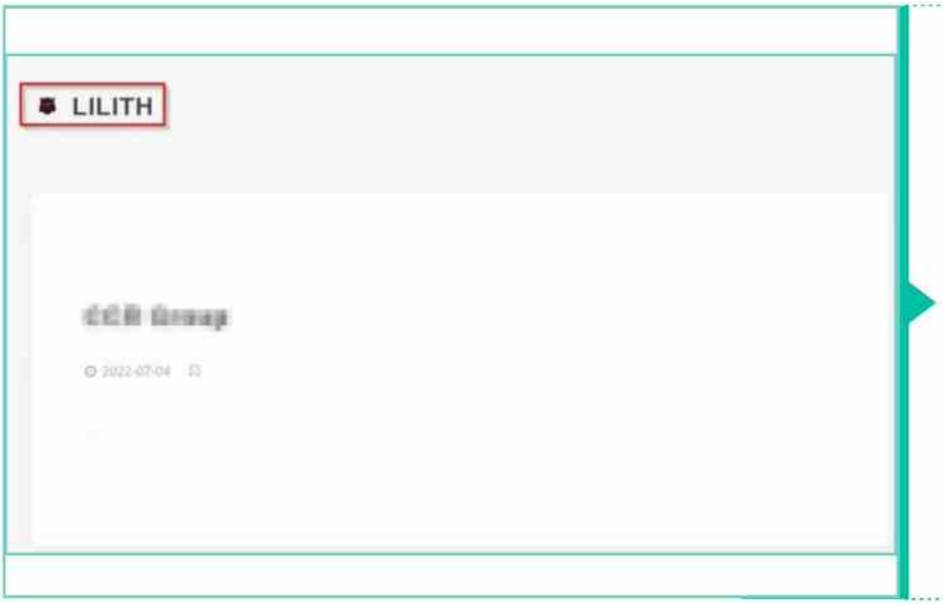
Most targeted Industries: IT & ITES, Professional Services

Most Targeted Countries: United States, United Kingdom

EVOLVING RANSOMWARE THREAT PROFILE

Lilith Ransomware

Since its emergence in July 2022, Lilith Ransomware has posted details of a single victim, and their leak site is down. Lilith ransomware encrypts files on the victim's machine and appends the extension of encrypted files as ".lilith."


LILITH

[redacted]

2022-07-04

Ransomware Group : Lilith

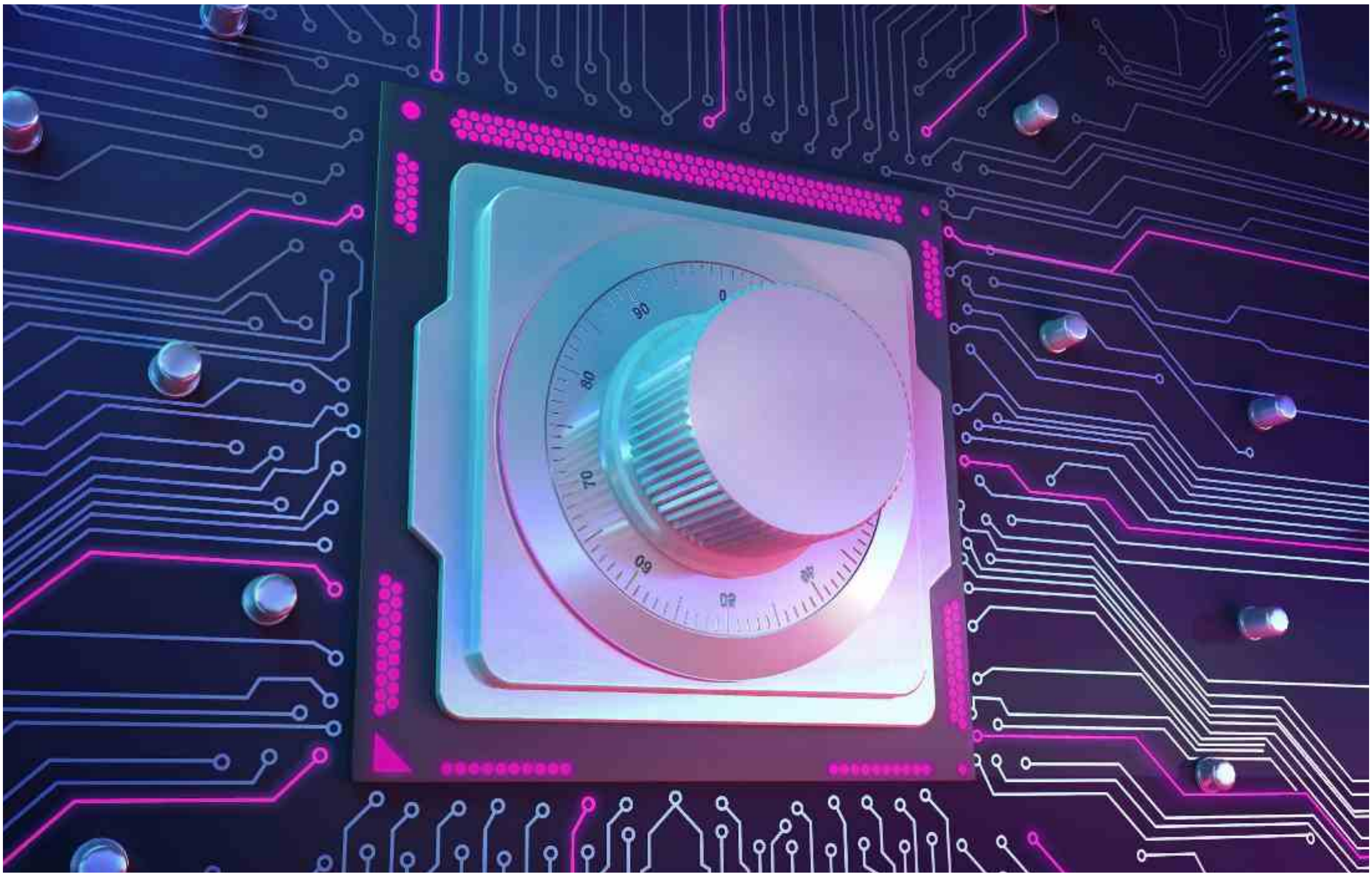
Programming Language: C/C++

Total Countries Targeted: 1

Total Victims: 1

Most targeted Industries: Telecommunication

Most Targeted Countries: Turkey

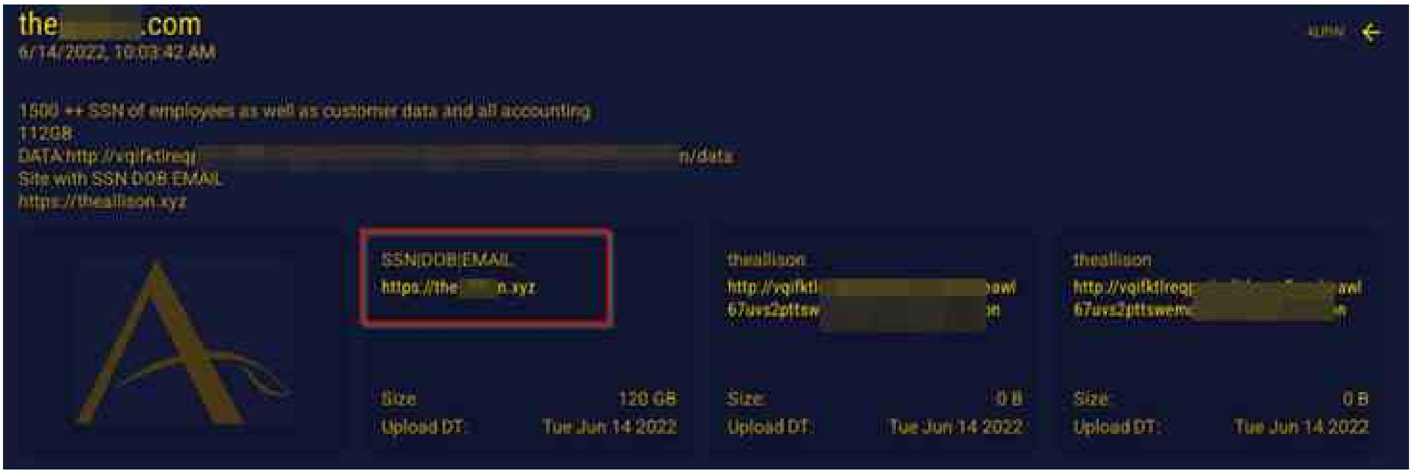


CAPRICIOUS RANSOMWARE TECHNIQUES

Spoofed Domains

Besides following the usual modus operandi of extortion where the ransomware groups encrypt the victim's data and then leak the exfiltrated data on their leak site, we are witnessing certain ransomware groups trying to go a few steps beyond in the extortion of their victims.

ALPHV ransomware created a spoofed domain of their victims in July 2022 and used it to leak the breached data.



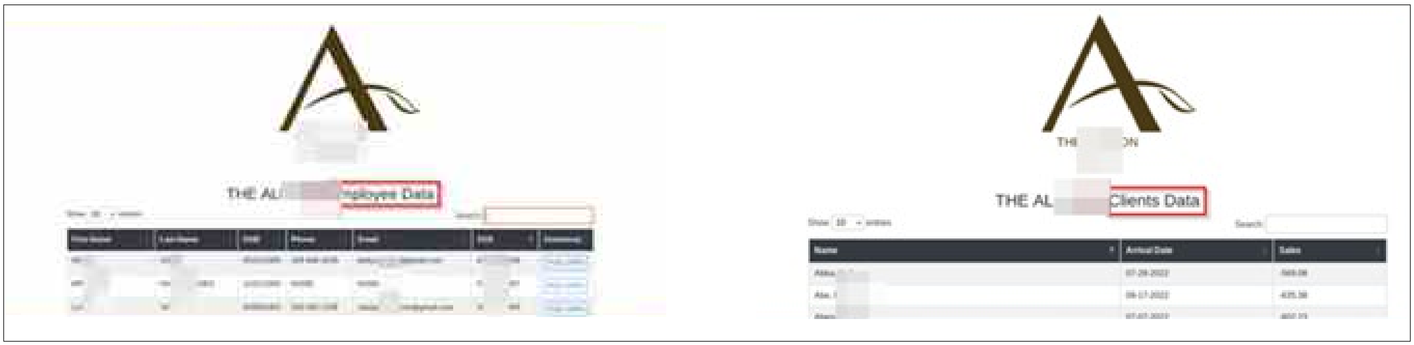
the[redacted].com
6/14/2022, 10:03:42 AM

1500 ++ SSN of employees as well as customer data and all accounting
112GB
DATA:http://vqifktlreq[redacted]n/data
Site with SSN DOB EMAIL
https://theallison.xyz

SSN|DOB|EMAIL https://the[redacted]n.xyz	theallison http://vqifktl[redacted]awl 67uvs2pttsw[redacted]n	theallison http://vqifktlreqp[redacted]awl 67uvs2pttswem[redacted]n
Size: 120 GB	Size: 0 B	Size: 0 B
Upload DT: Tue Jun 14 2022	Upload DT: Tue Jun 14 2022	Upload DT: Tue Jun 14 2022

Figure 6 – Screenshot of ALPHV's spoofed domain

Anyone can search for records available on this spoofed domain. The figure below shows the leaked records of employee data, including First Name, Last Name, Date of Birth, Phone, Email, and SSN of the victim organization's employees. The client data contains Name, Arrival Date, and Sales data.



THE AL[redacted]nployee Data

THE AL[redacted] Clients Data

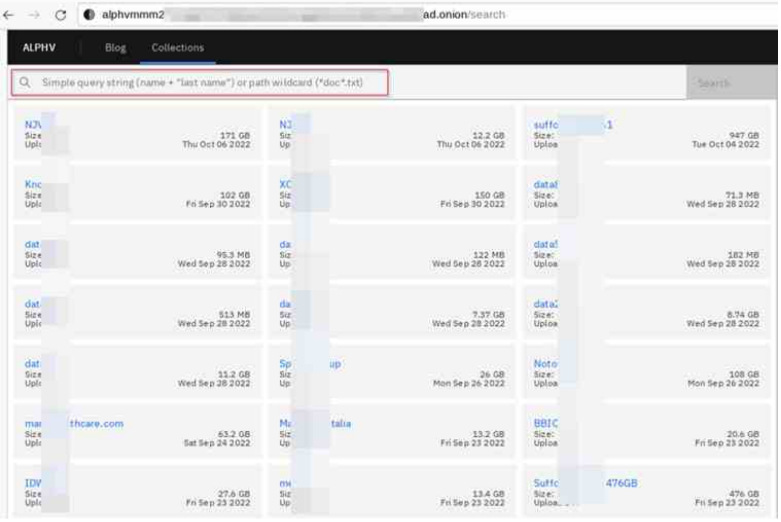
Name	Arrival Date	Sales

Figure 7 – Excepts of searchable data from ALPHV's spoofed domains

CAPRICIOUS RANSOMWARE TECHNIQUES

Searchable Database

The ALPHV ransomware group went ahead with a new extortion technique in late July by creating a tool called "ALPHV Collections" to search for keywords in leaked databases. The group hosts this searchable database on their leak site. ALPHV Collections is capable of performing string-based searches in the entire dataset.



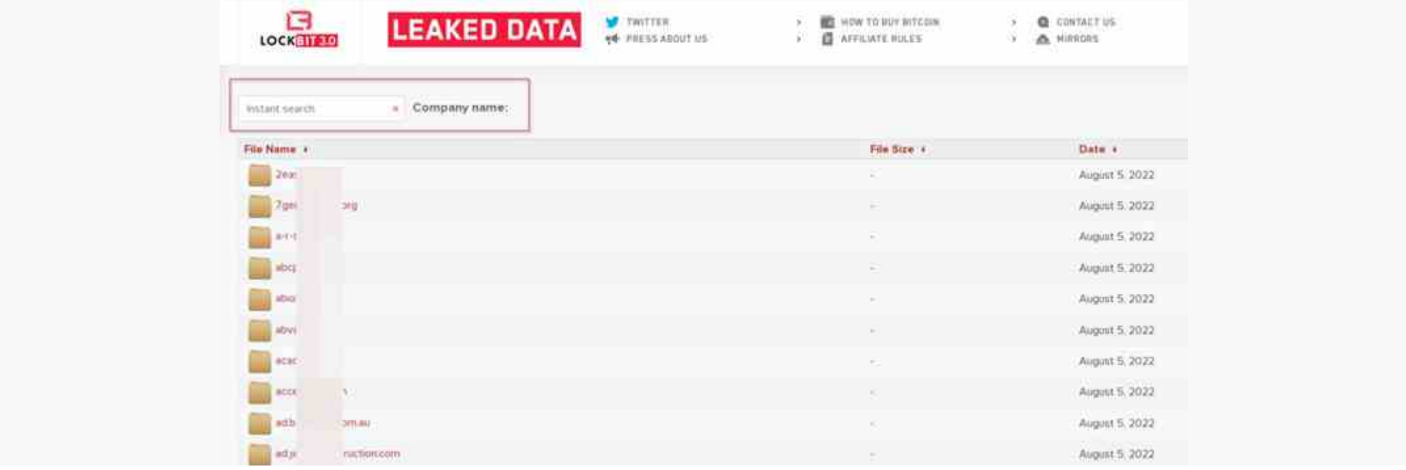
Simple query string (name + "last name") or path wildcard (*doc*.txt)

NJ\ Size Upl 171 GB Thu Oct 06 2022	NJ Siz Up 12.2 GB Thu Oct 06 2022	suffo 1 Size: Uploa 947 GB Tue Oct 04 2022
Knc Size Upl 102 GB Fri Sep 30 2022	XC Siz Up 150 GB Fri Sep 30 2022	data! Size: Uploa 71.3 MB Wed Sep 28 2022
dat Size Upl 95.3 MB Wed Sep 28 2022	da Siz Up 122 MB Wed Sep 28 2022	data! Size: Uploa 182 MB Wed Sep 28 2022
dat Size Upl 513 MB Wed Sep 28 2022	da Siz Up 7.37 GB Wed Sep 28 2022	data: Size: Uploa 8.74 GB Wed Sep 28 2022
dat Size Upl 11.2 GB Wed Sep 28 2022	Sp up Siz Up 26 GB Mon Sep 26 2022	Noto Size: Uploa 108 GB Mon Sep 26 2022
mar thcare.com Size Upl 63.2 GB Sat Sep 24 2022	M talia Siz Up 13.2 GB Fri Sep 23 2022	BBIC Size: Uploa 20.6 GB Fri Sep 23 2022
IDV Size Upl 27.6 GB Fri Sep 23 2022	m Siz Up 13.4 GB Fri Sep 23 2022	Suffc 476GB Size: Uploa 476 GB Fri Sep 23 2022

Figure 8 – Snapshot from ALPHV's searchable data index

Since rebranding itself and initiating a new leak site, we observed that LOCKBIT 3.0 is continuously adopting new techniques to remain a potent threat to its victims.

In August 2022, LOCKBIT ransomware created a dedicated site for hosting the leaked data of their victims. But LOCKBIT only provides a search operation based on the victim organization's name. The figure below shows the site created by LOCKBIT ransomware.



Instant search × Company name:

File Name	File Size	Date
2ea	-	August 5, 2022
7ge org	-	August 5, 2022
a-r-t	-	August 5, 2022
abc	-	August 5, 2022
abo	-	August 5, 2022
abv	-	August 5, 2022
acac	-	August 5, 2022
acc s	-	August 5, 2022
adb om.au	-	August 5, 2022
adj ruction.com	-	August 5, 2022

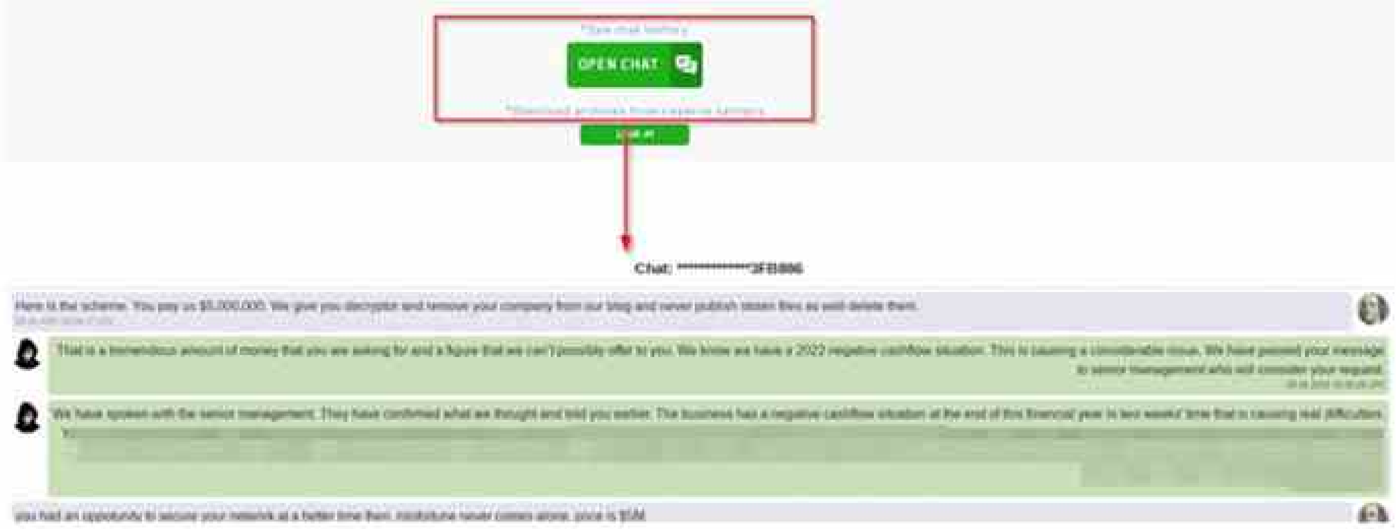
Figure 9 – LOCKBIT's leaked data search portal

CAPRICIOUS RANSOMWARE TECHNIQUES

LOCKBIT Blows Gaff on a Victim

LOCKBIT ransomware released a conversation with one of its victims on their leak site to intimidate them into paying a ransom. These chats mainly contain the negotiations between the ransomware group and their victims.

This was the first time we observed LOCKBIT using this technique. Earlier, we had observed the Conti ransomware group adopting this technique.



Chat: ************3FB886

Here is the scheme. You pay us $5,000,000. We give you decryptor and remove your company from our blog and never publish stolen files as well delete them.

That is a tremendous amount of money that you are asking for and a figure that we can't possibly offer to you. We know we have a 2022 negative cashflow situation. This is causing a considerable issue. We have passed your message to senior management who will consider your request.

We have spoken with the senior management. They have confirmed what we thought and told you earlier. The business has a negative cashflow situation at the end of this financial year in two weeks' time that is causing real difficulties. [illegible]

you had an opportunity to secure your network at a better time then. misfortune never comes alone. price is $5M

Figure 10 – Leaked conversation between LOCKBIT and a victim

Educational Institutes Under Siege

In Q3-2022, over 25 educational institutions were targeted by ransomware groups. Vice Society, AvosLocker, and LOCKBIT were the top three ransomware groups targeting this sector.

Incidentally, all Vice Society ransomware victims are from the United States and the United Kingdom. CISA also reported that the education sector, especially kindergarten through twelfth grade (K-12) institutions, had been a frequent target of ransomware attacks.

The impact of these attacks ranges from restricted access to networks and data, delayed exams, and canceled school days. Additionally, they also gained unauthorized access and stole personal information of students and staff.

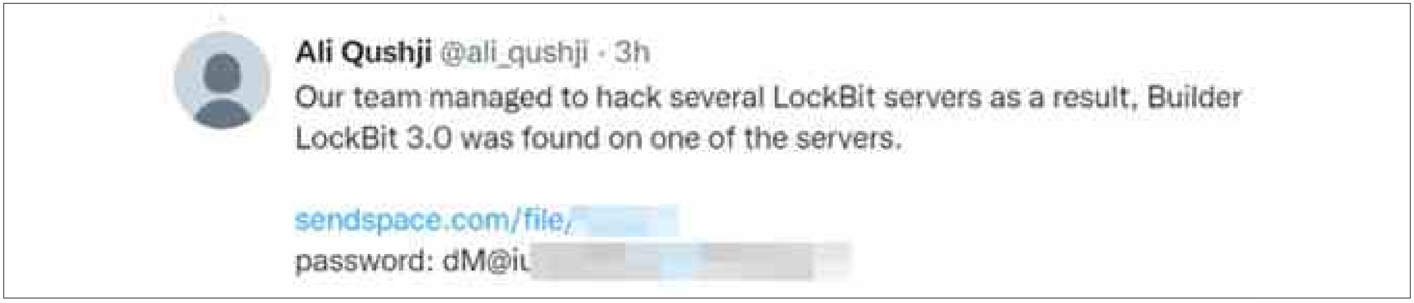
One of the recent victims of Vice Society ransomware includes Los Angeles Unified School District (LAUSD). LAUSD is a public school district in Los Angeles, California and is the largest public school system in California (in terms of the number of students) and the second largest public school district in the United States.

During the 2020-21 school year, LAUSD schooled 664,774 students. Over 500GB of data was exfiltrated in this attack, containing sensitive information such as Social Security Numbers, passport details, student psychological assessments, and other information.

CAPRICIOUS RANSOMWARE TECHNIQUES

Another Ransomware Builder Leaked

Cyble Research and Intelligence Labs (CRIL) came across a newly registered Twitter user claiming that their team managed to hack several LOCKBIT servers and acquired a builder of LOCKBIT 3.0 ransomware, also known as "LOCKBIT Black." This user has leaked the alleged builder for free on Twitter.



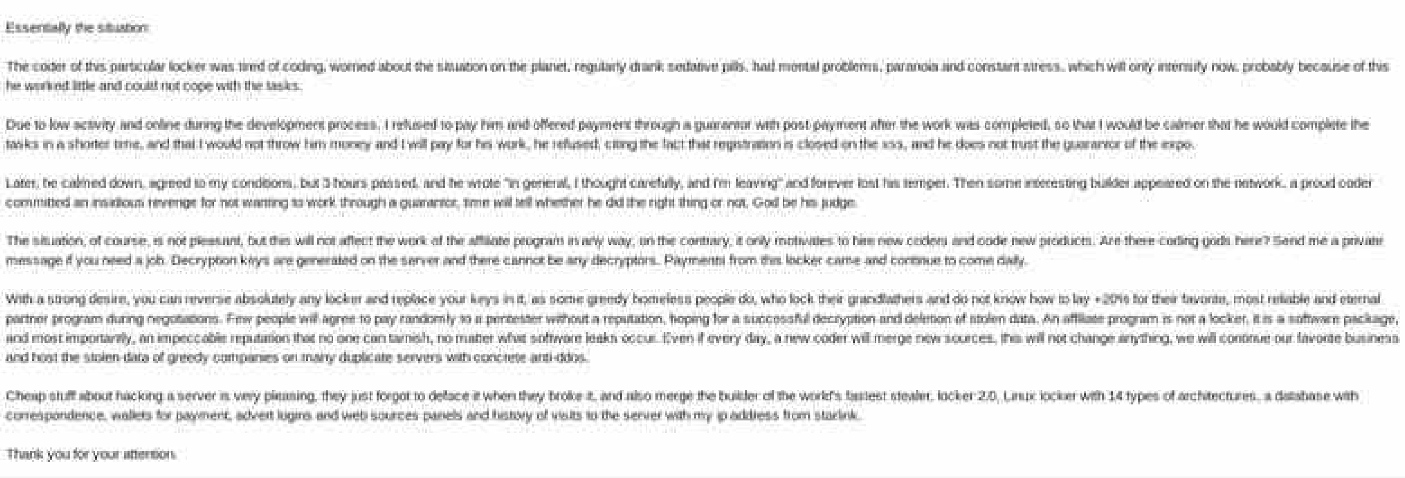
Ali Qushji @ali_qushji · 3h

Our team managed to hack several LockBit servers as a result, Builder LockBit 3.0 was found on one of the servers.

sendspace.com/file/[redacted]
password: dM@iu[redacted]

Figure 11 – Alleged leak of LOCKBIT Builder

But later, an operator of LOCKBIT ransomware on a cybercrime forum posted that a developer of LOCKBIT ransomware leaked the builder.



Essentially the situation:

The coder of this particular locker was tired of coding, worried about the situation on the planet, regularly drank sedative pills, had mental problems, paranoia and constant stress, which will only intensify now, probably because of this he worked little and could not cope with the tasks.

Due to low activity and online during the development process, I refused to pay him and offered payment through a guarantor with post-payment after the work was completed, so that I would be calmer that he would complete the tasks in a shorter time, and that I would not throw him money and I will pay for his work, he refused, citing the fact that registration is closed on the xss, and he does not trust the guarantor of the expo.

Later, he calmed down, agreed to my conditions, but 3 hours passed, and he wrote "in general, I thought carefully, and I'm leaving" and forever lost his temper. Then some interesting builder appeared on the network, a proud coder committed an insidious revenge for not wanting to work through a guarantor, time will tell whether he did the right thing or not, God be his judge.

The situation, of course, is not pleasant, but this will not affect the work of the affiliate program in any way, on the contrary, it only motivates to hire new coders and code new products. Are there coding gods here? Send me a private message if you need a job. Decryption keys are generated on the server and there cannot be any decryptors. Payments from this locker came and continue to come daily.

With a strong desire, you can reverse absolutely any locker and replace your keys in it, as some greedy homeless people do, who lock their grandfathers and do not know how to lay +20% for their favorite, most reliable and eternal partner program during negotiations. Few people will agree to pay randomly to a pentester without a reputation, hoping for a successful decryption and deletion of stolen data. An affiliate program is not a locker, it is a software package, and most importantly, an impeccable reputation that no one can tarnish, no matter what software leaks occur. Even if every day, a new coder will merge new sources, this will not change anything, we will continue our favorite business and host the stolen data of greedy companies on many duplicate servers with concrete anti-ddos.

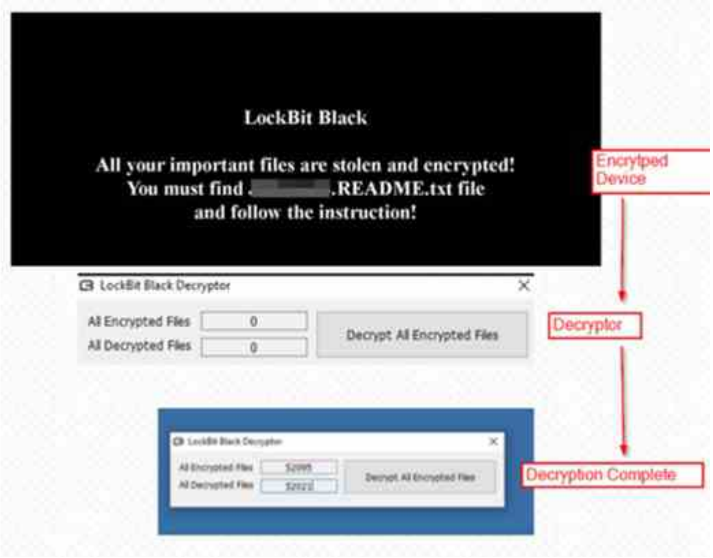
Cheap stuff about hacking a server is very pleasing, they just forgot to deface it when they broke it, and also merge the builder of the world's fastest stealer, locker 2.0, Linux locker with 14 types of architectures, a database with correspondence, wallets for payment, advert logins and web sources panels and history of visits to the server with my ip address from starlink.

Thank you for your attention.

Figure 12 – Post made by a LOCKBIT operator on a cybercrime forum

CAPRICIOUS RANSOMWARE TECHNIQUES

We tested both the ransomware payload and decryptor generated using the builder. The binary was able to encrypt files, and the decryption process was successful using the decryptor. These types of leaks can lead to the emergence of new ransomware groups.



LockBit Black

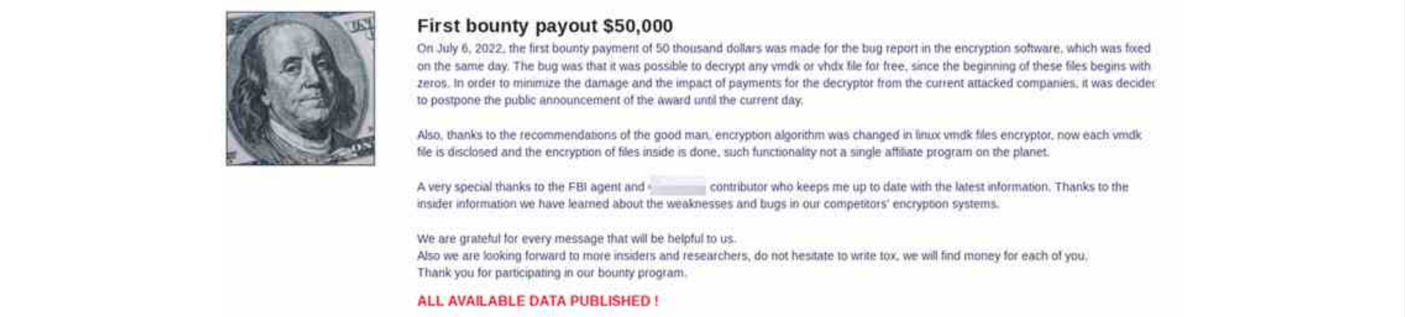
All your important files are stolen and encrypted!
You must find .[redacted].README.txt file
and follow the instruction!

Figure 13 – Ransomware encryption and decryption phases

LOCKBIT Bounty Payout

After the release of LOCKBIT 3.0, LOCKBIT launched a bug bounty program as well. This ransomware group started to pay bounties ranging between USD 1,000 - 1 million for any bug found in their products or compromising their real identities. Recently the LOCKBIT ransomware group announced the payment of USD 50,000 as its first bounty.

The operator of LOCKBIT ransomware stated, "An individual reported a bug in the encryption software of the Linux platform. The bug was that it was possible to decrypt any vmdk or vhdx file for free since the beginning of these files begins with zeros. In order to minimize the damage and the impact of payments for the decryptor from the current attacked companies, it was decided to postpone the public announcement of the award until the current day."



First bounty payout $50,000

On July 6, 2022, the first bounty payment of 50 thousand dollars was made for the bug report in the encryption software, which was fixed on the same day. The bug was that it was possible to decrypt any vmdk or vhdx file for free, since the beginning of these files begins with zeros. In order to minimize the damage and the impact of payments for the decryptor from the current attacked companies, it was decided to postpone the public announcement of the award until the current day.

Also, thanks to the recommendations of the good man, encryption algorithm was changed in linux vmdk files encryptor, now each vmdk file is disclosed and the encryption of files inside is done, such functionality not a single affiliate program on the planet.

A very special thanks to the FBI agent and [redacted] contributor who keeps me up to date with the latest information. Thanks to the insider information we have learned about the weaknesses and bugs in our competitors' encryption systems.

We are grateful for every message that will be helpful to us.
Also we are looking forward to more insiders and researchers, do not hesitate to write tox, we will find money for each of you.
Thank you for participating in our bounty program.

ALL AVAILABLE DATA PUBLISHED !

Figure 14 – LOCKBIT advertising their first bounty in a post

CAPRICIOUS RANSOMWARE TECHNIQUES

Bring Your Own Vulnerable Driver (BYOVD)

Bring Your Own Vulnerable Driver (BYOVD) is an attack technique where attackers with administrative privileges try to exploit the legitimate signed vulnerable drivers on the victim's system. Recently, BlackByte ransomware was spotted using this technique to disable EDR.

The ransomware group was exploiting CVE-2019-16098, which allows an authenticated user to read and write to arbitrary memory and could lead to privilege escalation.

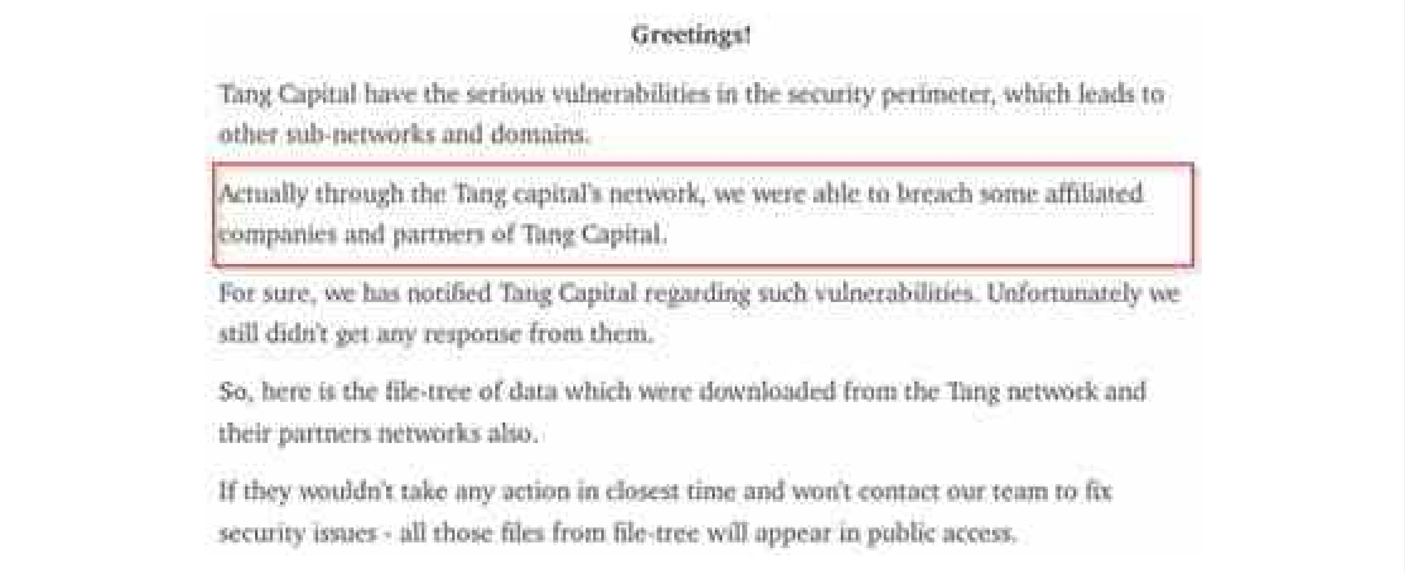
This indicates that TAs will not necessarily lookout for zero-days to execute attacks, and it is thus essential to patch existing vulnerabilities without delay.

Ransomware Attacks Compounding Risks of Supply Chain Attacks

With advancements in technology and accessibility, devices are connected to the internet faster than ever before, expanding an organization's attack surface significantly. Exploding amount of data is shared every second, and it becomes essential to secure the resources involved.

Ransomware poses great risks to the supply chain. Ransomware groups can earn a mint using supply chain attacks, as attacking a single organization could compromise multiple organizations, as we witnessed in the Kaseya incident.

Recently Ragnar_Locker also claimed credit for a supply chain attack that they executed.



Greetings!

Tang Capital have the serious vulnerabilities in the security perimeter, which leads to other sub-networks and domains.

Actually through the Tang capital's network, we were able to breach some affiliated companies and partners of Tang Capital.

For sure, we has notified Tang Capital regarding such vulnerabilities. Unfortunately we still didn't get any response from them.

So, here is the file-tree of data which were downloaded from the Tang network and their partners networks also.

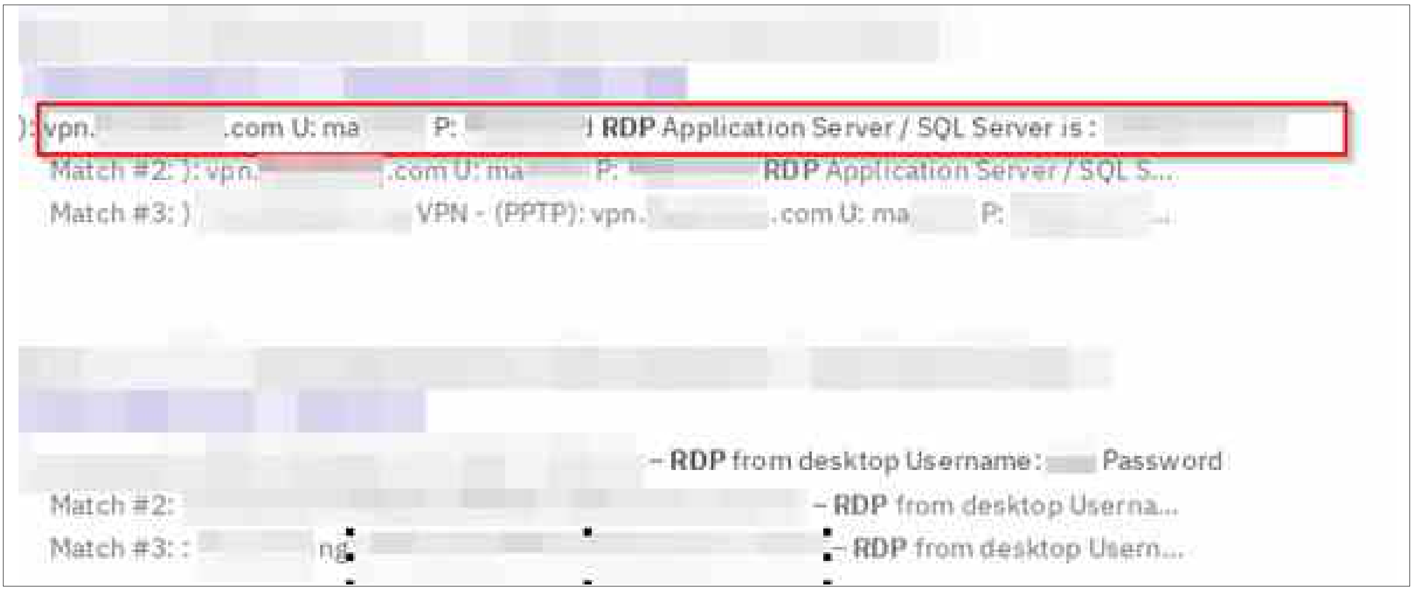
If they wouldn't take any action in closest time and won't contact our team to fix security issues - all those files from file-tree will appear in public access.

Figure 15 – Post made by the Ragnar_Locker ransomware group

CAPRICIOUS RANSOMWARE TECHNIQUES

The data exfiltrated in a ransomware attack can contain sensitive information such as login credentials. Using ALPHV collections, anyone can search for strings such as RDP credentials. This search operation is performed on the data exfiltrated from the systems of ransomware victims.

TAs can easily leverage this tool for targetting other companies, and it can also result in supply chain attacks. The figure below shows the search results on ALPHV Collections. It also highlights how having visibility on exposed databases can help prevent such attacks.



```
[redacted]
): vpn.[redacted].com U: ma[redacted] P: [redacted] RDP Application Server / SQL Server is : [redacted]
  Match #2: ): vpn.[redacted].com U: ma[redacted] P: [redacted] RDP Application Server / SQL S...
  Match #3: ) [redacted] VPN - (PPTP): vpn.[redacted].com U: ma[redacted] P: [redacted]...

[redacted]
[redacted] – RDP from desktop Username: [redacted] Password
  Match #2: [redacted] – RDP from desktop Userna...
  Match #3: : [redacted] ng: [redacted] – RDP from desktop Usern...
```

Figure 16 – Exposed victim data on ALPHV leak site

CYBERCRIME FORUMS SHELTERING RANSOMWARE GROUPS

During the Quarter, we observed several TA dumping or advertising ransomware victim data on popular cybercrime forums for sale. Ransomware groups broadcast this data from their newly created aliases or profiles on popular cybercrime forums, which cannot be coherently attributed to any ransomware groups.

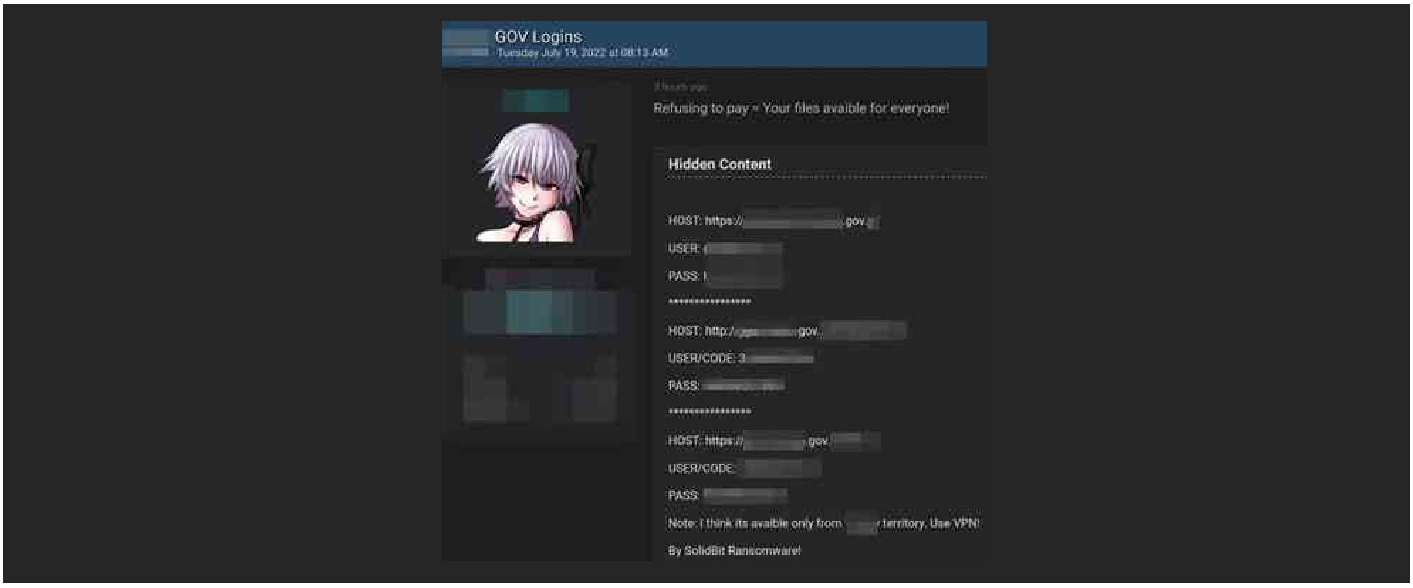
Alternatively, these could be the affiliates of these ransomware groups and probably tasked to market their exploits on cybercrime forums as the ransom payments decline further in this quarter. Interestingly these cybercrime forums have been averse to such affiliates since May 2021 and forbade any attempt to sell or leak the data of ransomware victims.

Some of the related activities observed by CRIL are:

- A TA was observed trading 10 TB of alleged to be previously undisclosed ransomware victim data for other data leaks
- A possible alias of Everest ransomware group with the moniker 'Everest' on a popular cybercrime forum was observed dumping an Italy-based Energy & Utilities company's data announced to be targeted just a week ago.
- Another TA posted access details of the Turkish Government's portals that were ransomed in the recent past.

Login Credentials

SolidBit ransomware does not have a leak site and was seen using cybercrime forums to extort its victims. For extorting their victims, the SolidBit ransomware released the login credentials of multiple Government departments of a Country for extorting their victim, as shown in the figure below. Using these credentials, other TAs can also access victims' networks.



[redacted] GOV Logins
[redacted] Tuesday July 19, 2022 at 08:13 AM

3 hours ago

Refusing to pay = Your files avaible for everyone!

Hidden Content

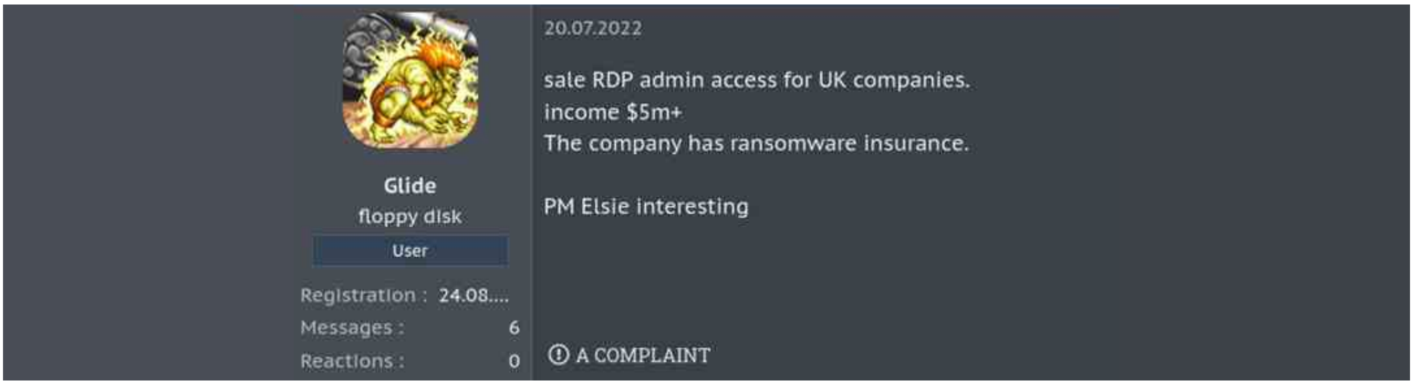
HOST: https://[redacted].gov.[redacted]
USER: [redacted]
PASS: [redacted]
****
HOST: http://[redacted]gov.[redacted]
USER/CODE: 3[redacted]
PASS: [redacted]
****
HOST: https://[redacted].gov.[redacted]
USER/CODE: [redacted]
PASS: [redacted]
Note: I think its avalble only from [redacted] territory. Use VPN!
By SolidBit Ransomware!

Figure 17 – Leaked Credentials of Ransomware victims on a cybercrime forum

CYBERCRIME FORUMS SHELTERING RANSOMWARE GROUPS

Safeguarding business interests with Ransomware Insurance has become a growing trend amongst firms. However, it seems that the Initial Access Broker (IAB) is advertising the sale of access of networks to ransomware-insured organizations to ransomware groups on cybercrime forums.

This technique may have been adopted towards possible fruitful negotiations with the insurers rather than the victims, as the latter may still resist paying the ransom.



Glide
floppy disk
User

Registration : 24.08....
Messages : 6
Reactions : 0

20.07.2022

sale RDP admin access for UK companies.
income $5m+
The company has ransomware insurance.

PM Elsie interesting

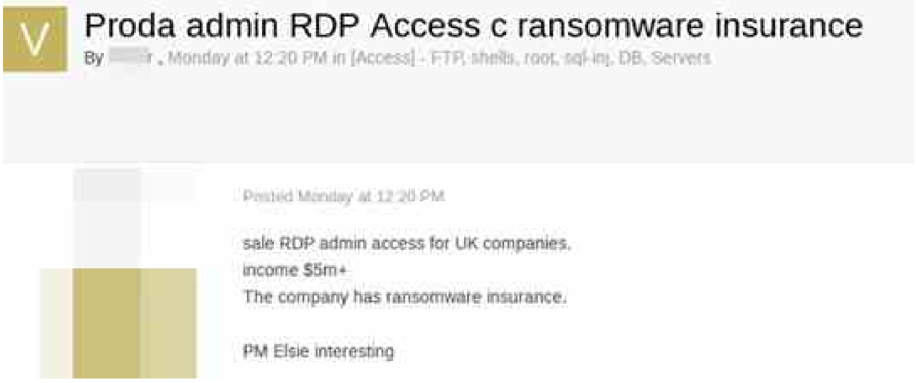
ⓘ A COMPLAINT

Figure 18 – TA selling network access while highlighting that the company has Ransomware Insurance

Betting on Cyber Insurance

Cyber Insurance enables organizations to claim coverage for recovering from cyber attacks. To recover from a ransomware attack, a victim organization might end up paying millions of dollars. Since more organizations are now investing in cyber insurance, threat actors have also begun to target such organizations. The figure below shows a TA selling access to an organization and mentions that the victim has ransomware insurance.

There are multiple reasons for victims not paying the ransom; one is a lack of capital. An organization with cyber insurance can thus become a lucrative target for TAs. TAs can leverage this to earn by settling a negotiation because there are chances that the victim might get insurance cover.



Proda admin RDP Access c ransomware insurance

By [redacted]r , Monday at 12:20 PM in [Access] - FTP, shells, root, sql-inj, DB, Servers

Posted Monday at 12:20 PM

sale RDP admin access for UK companies.
income $5m+
The company has ransomware insurance.

PM Elsie interesting

Figure 19 – Impact in Q3 RW groups act – Amount paid or penalties paid

FUTURE PREDICTIONS

There’s a high possibility that LOCKBIT ransomware might shift to a triple extortion technique which includes the following pattern.

encryption → Data Leak → DDoS (Distributed Denial of Service)

LOCKBIT ransomware might DDoS their victims who failed to pay the ransom. This will enable TAs to create more downtime for the victim organization. In future attacks, we might see multiple new ransomware groups using leaked LOCKBIT 3.0 builder.

Based on statistical analysis, **we may see a decrease in ransomware attacks in Q4 2022.**

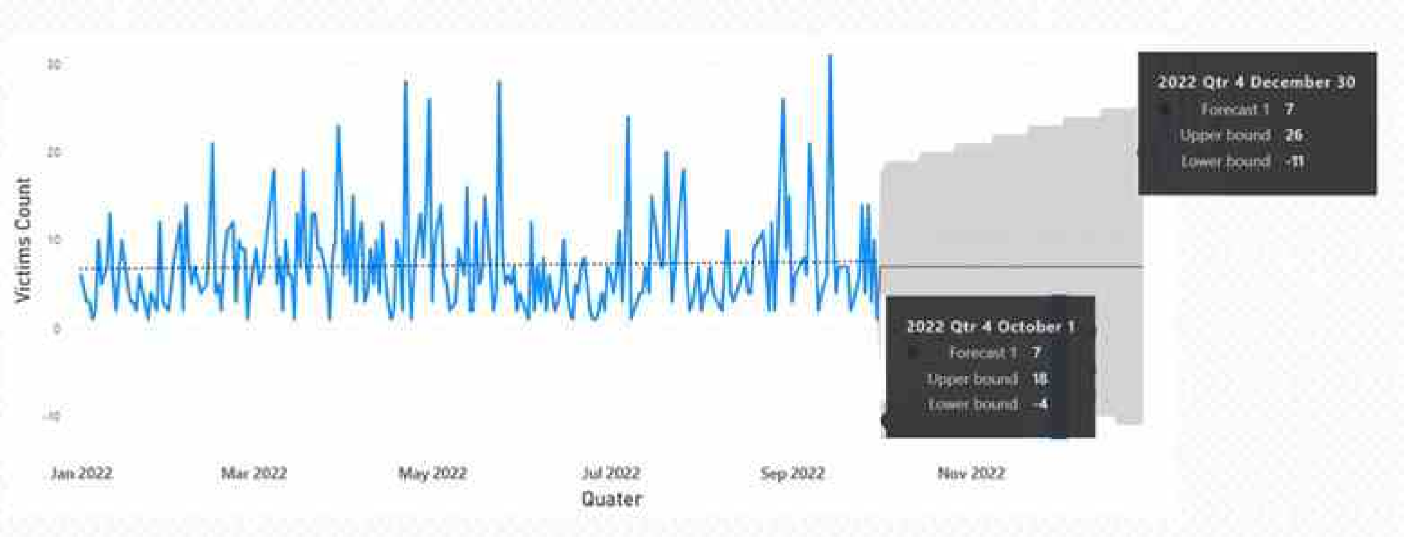


Figure 20 – Forecast for Q4-2022

Supply Chain attacks can become a lucrative technique for TAs, as they can impact multiple victims in a single attack. The creation of searchable databases as an extortion technique can also aid TAs in executing such attacks. Several times, ransomware victims have repeatedly refused to pay the TA’s ransom demand, leading TAs to try and adopt different extortion techniques.

Even though this has been attributed several times before, we presume more politically aligned ransomware groups will align with APTs in the coming months as the ransom payout shrinks and to enhance their prowess in the ransomware space. Earlier, APT groups such as DEV-0401 (China) and APT42 (Iran) were repeatedly observed using ransomware for financial gains.

Iran-Linked APT 42 has been accused of conducting over 30 cyber espionage campaigns against activists and those the state considers dissidents. They are also widely suspected of operating on behalf of the Islamic Revolutionary Guard Corps (IRGC)’s Intelligence Organization (IRGC-IO). Researchers reported that the DEV-0401 was seen deploying LockFile, AtomSilo, Rook, Night Sky, and Pandora ransomware.

HOW TO PROTECT YOURSELF FROM RANSOMWARE ATTACKS

With Threat Actors and their TTPs constantly 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
- 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 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 package 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 into 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