Lockbit 3.0 – Ransomware group launches new version

blog.cyble.com/2022/07/05/lockbit-3-0-ransomware-group-launches-new-version/

July 5, 2022

"Lockbit Black" actively targeting BFSI Sector

LockBit ransomware is currently one of the most popular and active ransomware groups in the wild. This ransomware variant was first detected in September 2019 and used by Threat Actors (TAs) to target multiple sectors and organizations worldwide. The TAs behind LockBit operate under the Ransomware-as-a-Service (RaaS) business model.

In the figure below, we have prepared a breakdown of the industries targeted by the LockBit ransomware. As per our investigation, we determine that over 1/3rd of the ransomware gang's victims are from the BFSI sector, followed by the Professional Services sector.

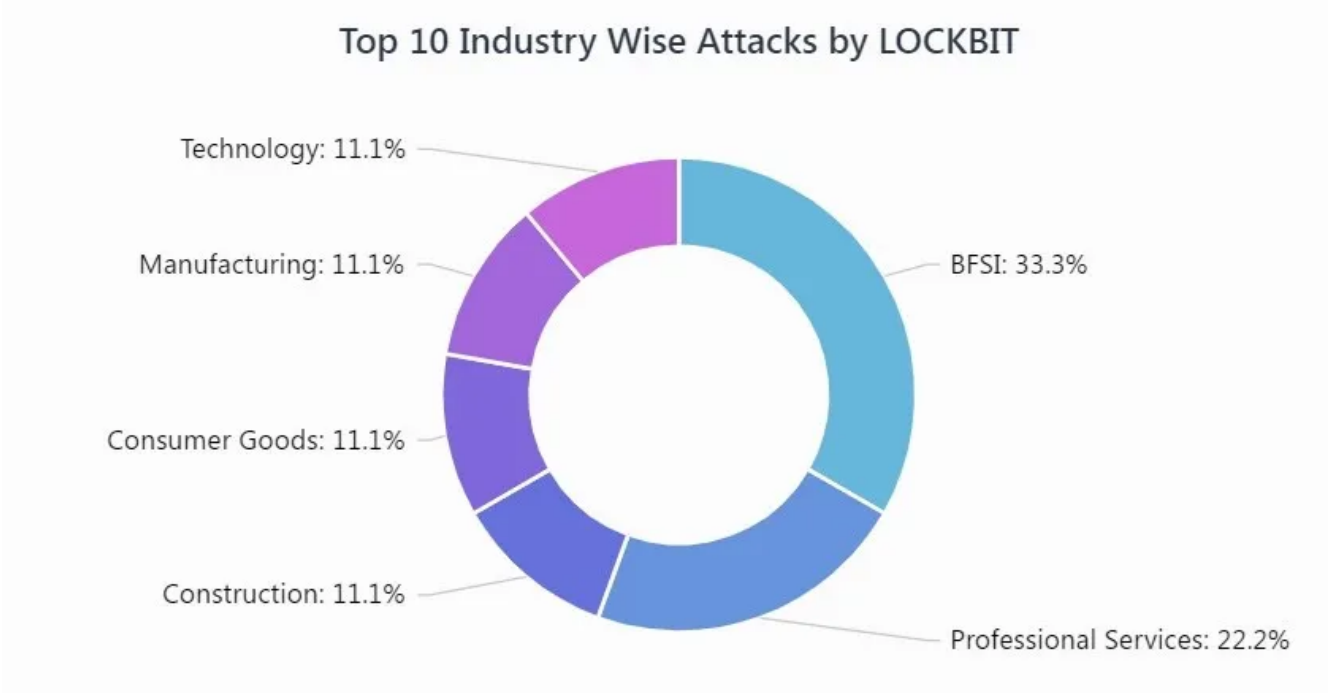


Figure 1 – Industries Targeted by the LockBit Ransomware

In August 2021, LockBit 2.0 ransomware was analyzed by Cyble Research Labs. In March 2022, the TAs behind LockBit announced that LockBit 3.0 would be released shortly. Last week, the TAs updated their leak site with information about their latest version and its features (shown below).

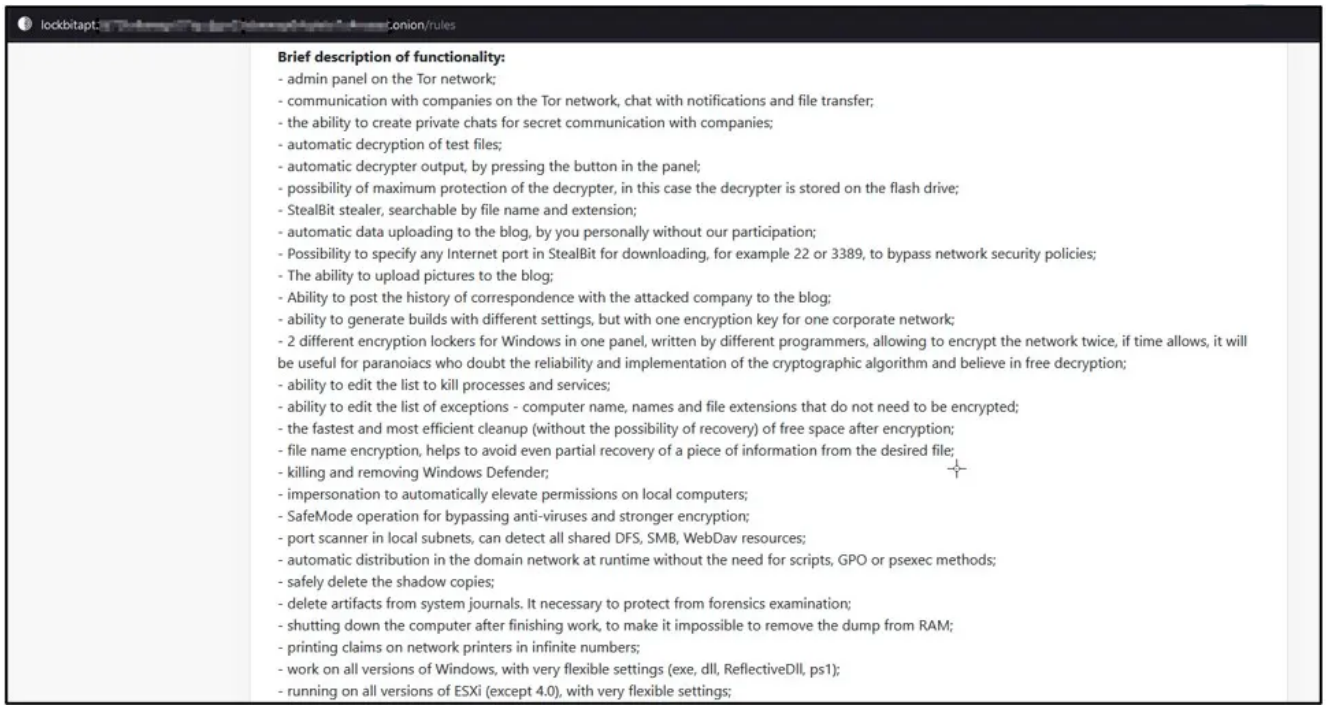


Figure 2 – LockBit 3.0 Ransomware Functionalities

While searching for the latest LockBit 3.0 sample, Cyble Research Labs came across a Twitter post wherein a researcher mentioned that a new version of ransomware named “LockBit 3.0” (also referred to as “LockBit Black”) is now active in the wild.

LockBit 3.0 encrypts files on the victim’s machine and appends the extension of encrypted files as *“HLJkNskOq.”*

LockBit ransomware requires a key from the command-line argument “-pass” to execute. The below figure shows the process chain of the LockBit ransomware file.

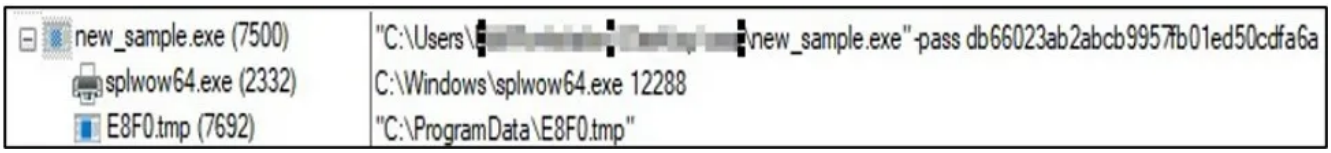


Figure 3 – LockBit 3.0 Ransomware Process Tree

Technical Analysis

The sample hash (SHA256), ***80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce***was taken for this analysis.

Based on static analysis, we identified that the ransomware is encrypted and decrypts the strings and code during runtime.

The ransomware resolves its API functions dynamically, as shown below.

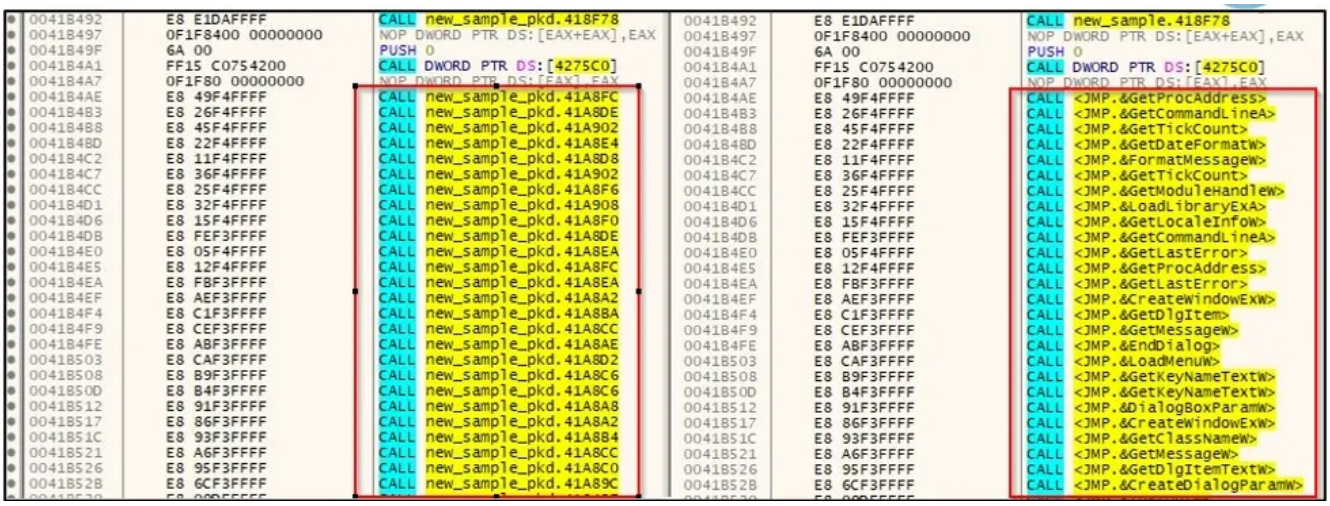


Figure 4 – Resolved API functions of LockBit 3.0

After that, it creates a mutex to ensure that only one instance of malware is running on the victim’s system at any given time.

The malware exits if the mutex is already present. The below figure shows the created mutex name.

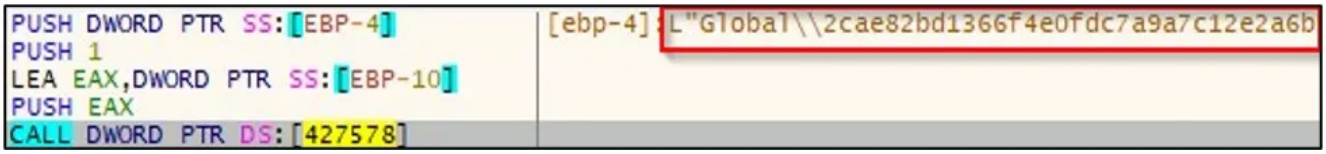


Figure 5 – Mutex Creation

The ransomware creates multiple threads using the *CreateThread()* API to perform several tasks in parallel for faster file encryption, as shown in Figure 6.

Each thread is responsible for querying system information, getting drive details, ransom note creation, getting file attributes, deleting services, file search, encryption, etc.

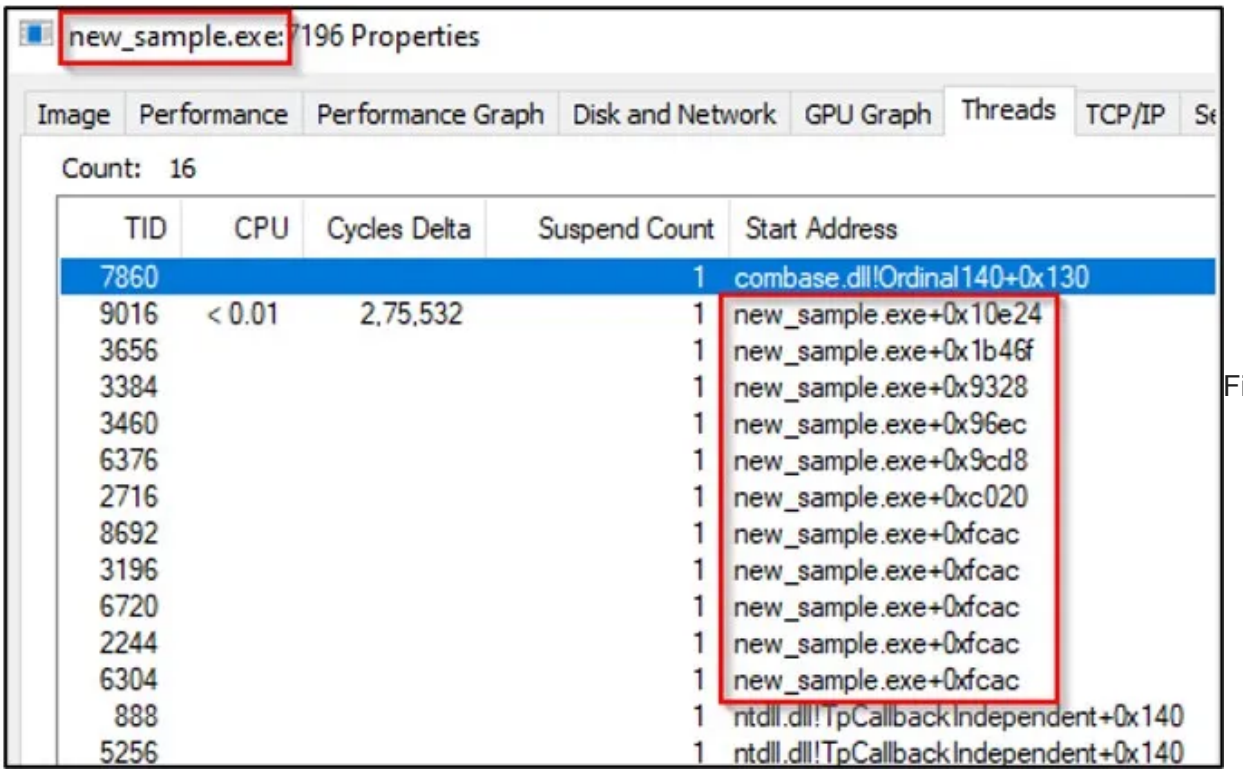


Figure 6 – Multiple Thread Creation

Before encrypting the files, the ransomware uses the *WMI* query to enumerate Volume Shadow copies using the command *"select * from Win32_ShadowCopy"*.

It then deletes the copies using *"Win32_ShadowCopy.ID,"* as shown in Figure 7.

The ransomware performs this operation to prevent any attempts at system restoration after encrypting the files.

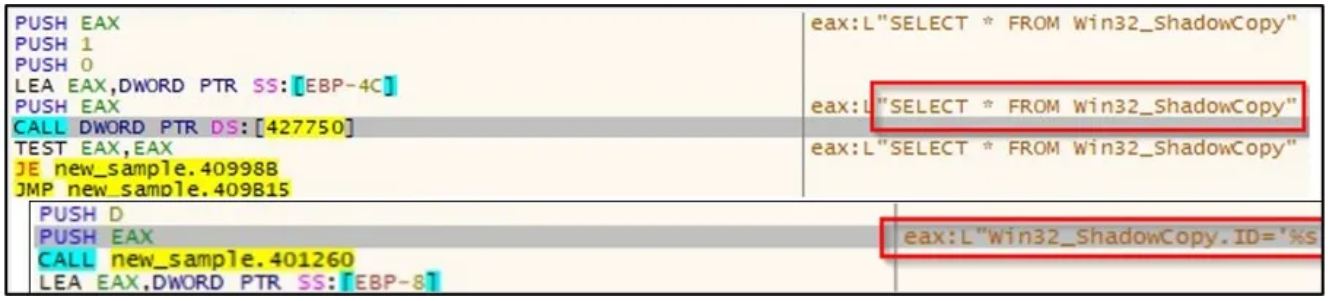


Figure 7 – Delete ShadowCopy

LockBit 3.0 ransomware deletes a few services to encrypt the files successfully. To delete these services, the ransomware calls the *OpenSCManagerA()*API to get the service control manager database access.

After gaining access, the ransomware enumerates the services and fetches the service names from the victim's machine.

It then checks for the presence of these services and deletes them if they are actively running on the victim's machine. The below image shows the list of some service names targeted by ransomware.

Background Intelligent Transfer Service	RAS Asynchronous Media Driver
Windows Bind Filter Driver	AsyncMac
bindflt	AssignedAccessManager Service
Base Filtering Engine	AssignedAccessManagerSvc
BitLocker Drive Encryption Service	Adaptec SAS/SATA-II RAID Storport's Miniport Driv
BDESVC	arcsas
bcmfn2 Service	AppX Deployment Service (AppXSVC)
bcmfn2	AppXSvc
BasicRender	AppvVfs
BasicRender	AppvVfs
BasicDisplay	AppvVemgr
BasicDisplay	AppvVemgr
Background Activity Moderator Driver	AppvStrm
QLogic Network Adapter VBD	AppvStrm
b06bdrv	Microsoft App-V Client
ActiveX Installer (AxInstSV)	AppVClient
AxInstSV	App Readiness
Cellular Time	AppReadiness
autotimesvc	Application Management
Windows Audio	AppMgmt
Audiosrv	Smartlocker Filter Driver
Windows Audio Endpoint Builder	applockerfltr

Figure 8 – List of Services for Deletion

After deleting the services, the ransomware drops two files named "*HLJkNskOq.ico*" and "*HLJkNskOq.bmp"* in the *%programdata%* location.

The ransomware creates a *"DefaultIcon"* registry key for the extension "*HLJkNskOq"* shown in the figure below.This operation changes the icons of the encrypted files, which have the extension "*HLJkNskOq."*

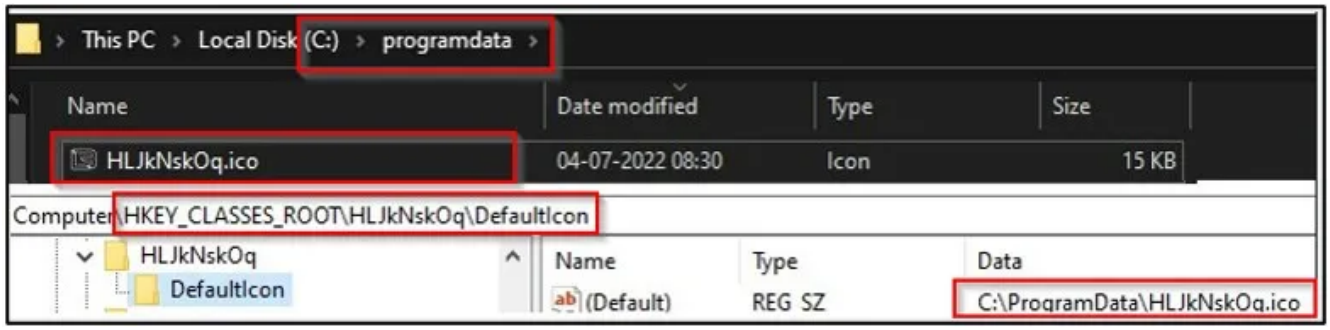


Figure 9 – Registry Modification of Default Icon

Before initiating the encryption process, the ransomware drops the below ransom note in multiple folders with the file name *"HLJkNskOq.README.txt."*

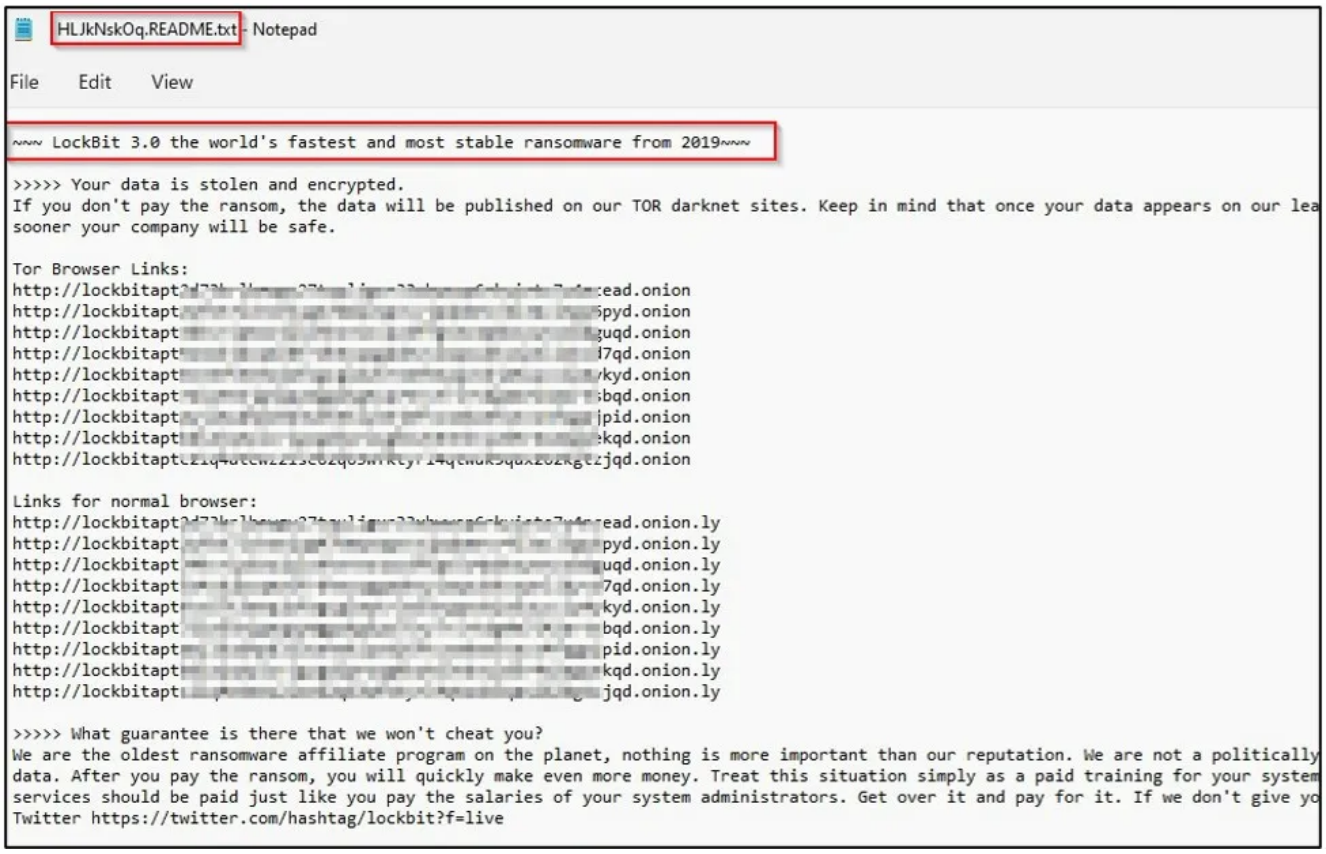
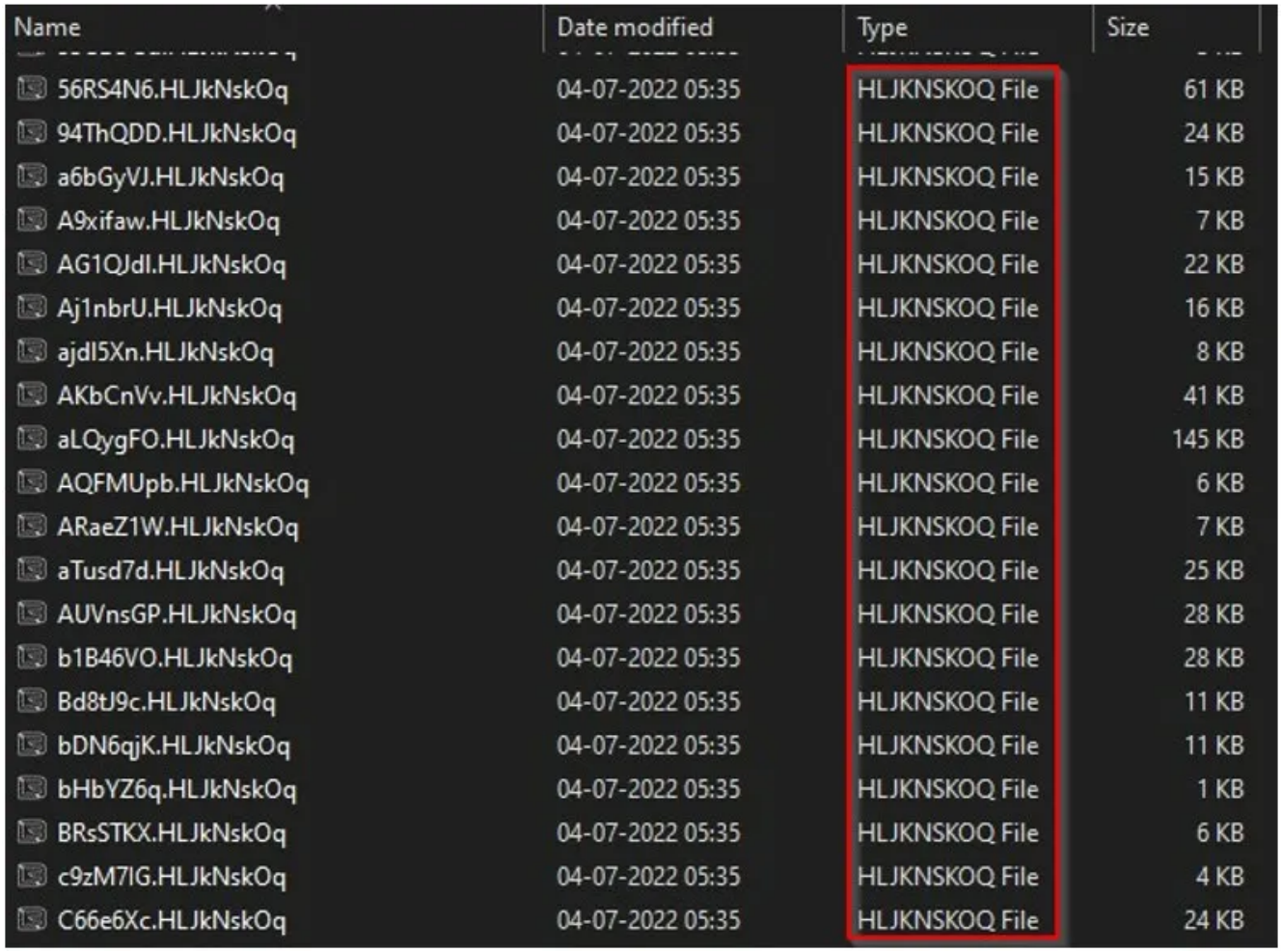


Figure 10 – LockBit 3.0 Ransomware Note

The ransomware then encrypts the victim's files, appends the extension "*.HLJkNskOq,"* and changes the file's icon as shown below.



Name	Date modified	Type	Size
56RS4N6.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	61 KB
94ThQDD.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	24 KB
a6bGyVJ.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	15 KB
A9xifaw.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	7 KB
AG1QJdI.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	22 KB
Aj1nbrU.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	16 KB
ajdI5Xn.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	8 KB
AKbCnVv.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	41 KB
aLQygFO.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	145 KB
AQFMUpb.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	6 KB
ARaeZ1W.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	7 KB
aTusd7d.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	25 KB
AUVnsGP.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	28 KB
b1B46VO.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	28 KB
Bd8tJ9c.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	11 KB
bDN6qjK.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	11 KB
bHbYZ6q.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	1 KB
BRsSTKX.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	6 KB
c9zM7lG.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	4 KB
C66e6Xc.HLJkNskOq	04-07-2022 05:35	HLJKNSKOQ File	24 KB

Figure 11 – Encrypted Files

Finally, the ransomware changes the victim's wallpaper leveraging the file *"HLJkNskOq.bmp"* using the *systemparametersinfoW()* API function.

Figure 12 – LockBit 3.0 Changing Desktop Background

In the dropped ransom note, victims are instructed on how to pay the ransom to decrypt their encrypted files. Additionally, the TAs threaten the victims stating that their personal data will be posted on their leak site if the ransom is not paid within the specified window.

After visiting the TOR link mentioned in the ransom note, it opens the TA's leak site page, which is updated with new features containing a Twitter icon to search for posts related to this ransomware on Twitter.

Additionally, TAs created a link on their leak site, redirecting users to a page where they have announced the Bug Bounty program. This program invites all

security researchers/ethical and unethical hackers to find flaws in their ransomware project to make it bug-free and more stable.

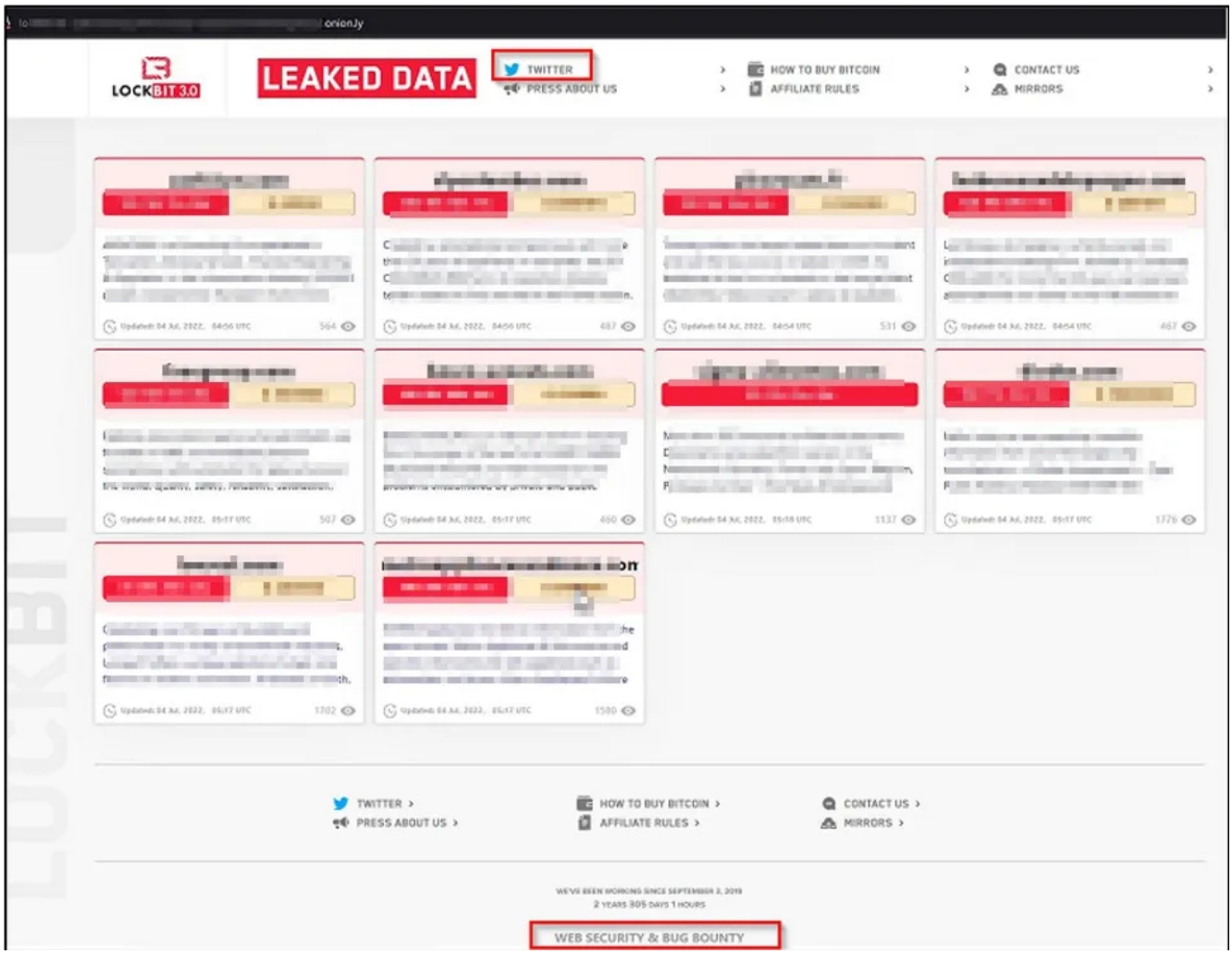


Figure 13 – LockBit 3.0 Ransomware Home Page

The affiliate rules page of the leak site includes ransomware functionalities and affiliate program details, which support languages such as English, Chinese, Spanish, etc.

The TAs behind LockBit 3.0 suggest that their victims buy Bitcoin using the payment options shown in the figure below.

Figure 14 – Ways to Buy Bitcoin to decrypt files

The figure below shows the chat option on the leak site for communication with the TAs. Also, the “Trial Decrypt” option is available to victims to test an encrypted file’s decryption.

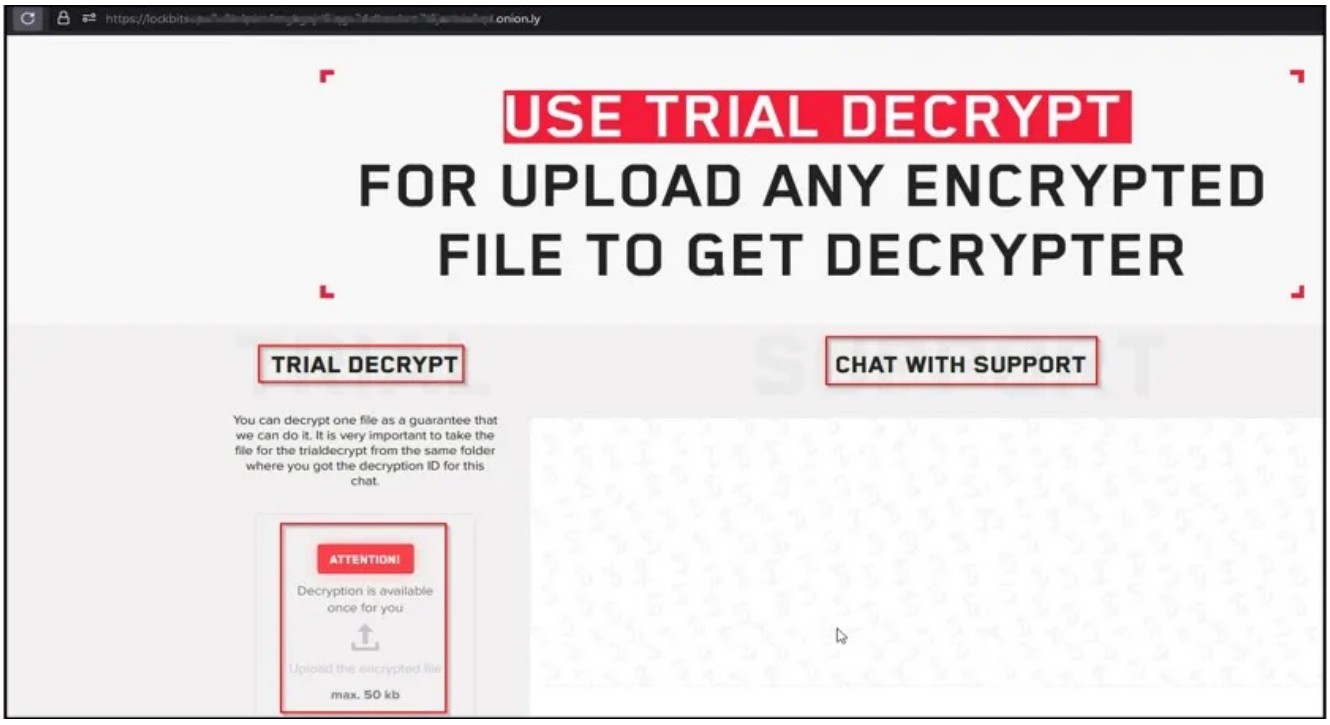


Figure 15 – Trial Decryption & Chat Options

Conclusion

Ransomware is becoming an increasingly common and effective attack method to target organizations and adversely impact their productivity.

LockBit 3.0 is a highly sophisticated form of ransomware that uses various techniques to conduct its operations. Cyble will closely monitor the campaign and continue to update our readers with the latest information on ransomware.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

Safety Measures Needed to Prevent Ransomware Attacks

- Conduct regular backup practices and keep those backups offline or in a separate network.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Use a reputed anti-virus and Internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.

Users Should Take the Following Steps After the Ransomware Attack

- Detach infected devices on the same network.
- Disconnect external storage devices if connected.
- Inspect system logs for suspicious events.

Impacts And Cruciality of LockBit 3.0 Ransomware

- Loss of Valuable data.
- Loss of the organization’s reputation and integrity.
- Loss of the organization’s sensitive business information.
- Disruption in organization operation.
- Financial loss.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Execution	T1204	User Execution
Defence Evasion	T1112 T1497	Modify Registry Virtualization/Sandbox Evasion
Discovery	T1082 T1083	System Information Discovery File and Directory Discovery
Impact	T1486	Data Encrypted for Impact
CNC	T1071	Application Layer Protocol

Defense Evasion	T1070	Indicator Removal on Host

Indicator Of Compromise (IOCs)

Indicators	Indicator Type	Description
38745539b71cf201bb502437f891d799 f2a72bee623659d3ba16b365024020868246d901 80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce	MD5 SHA1 Sha256	LockBit 3.0 EXE file