A Deep-dive Analysis of LOCKBIT 2.0

blog.cyble.com/2021/08/16/a-deep-dive-analysis-of-lockbit-2-0/

August 16, 2021

The LOCKBIT 2.0 ransomware group has been highly active in the past few months. The Threat Actors (TAs) linked to this ransomware use a Ransomware-as-a-Service (RaaS) business model. LOCKBIT 2.0 developers customize ransomware variants as per their affiliates' needs. They also offer various panels and attack statistics to provide victim management capabilities to their affiliates.

The malware uses the double extortion technique to compel victims into paying ransoms. Through this technique, attackers exfiltrate the victim's data, after which they proceed to encrypt the data on the victim's system. Data encryption is followed by the TAs demand ransom in exchange for a decryptor. If the victim refuses or cannot pay the ransom, the TA threatens to leak the data. This ransomware was previously known as ABCD ransomware as the file extension used for encrypting files was .abcd. Now the extension used by this ransomware is *.lockbit*.

Figure 1 shows the LOCKBIT 2.0 ransomware gang hosting a blog in the TOR network. This blog, in particular, is used by the TA to share the list of victims and screenshots of the sample data exfiltrated by the attackers from affected systems.

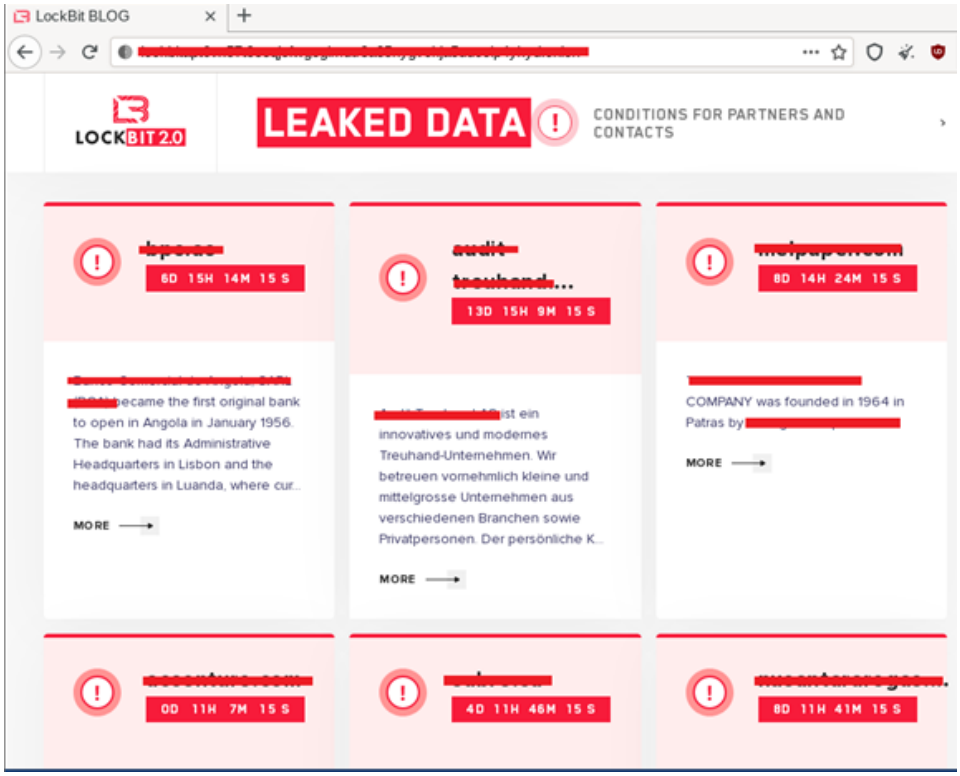


Figure 1: LOCKBIT 2.0 Blog displaying Victim companies

Like other recently emerging RaaS gangs, LOCKBIT 2.0 also has an affiliate program to attract potential affiliates. Figure 2 shows the affiliate program page.

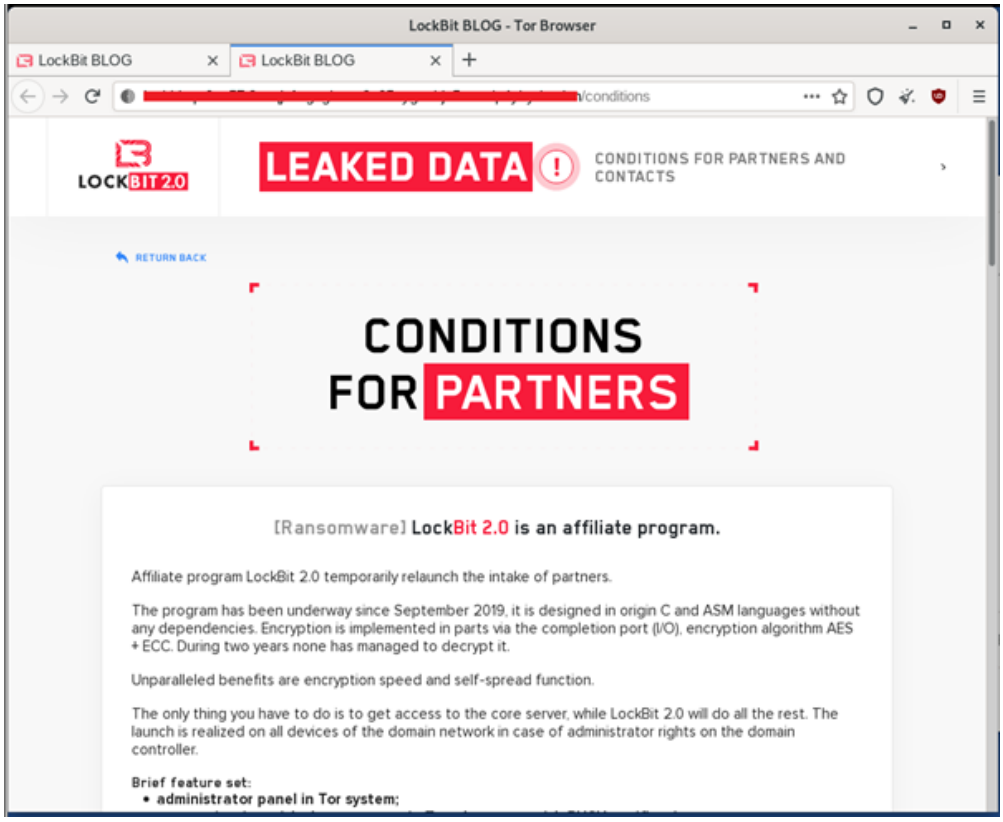


Figure 2: Affiliate Program of LOCKBIT 2.0

LockBit is trying to position itself as the fastest encryptor compared to its competitor, RaaS gangs. They have listed the time spent on encryption for datasets of 100GB, 10TB, etc. Figure 3 shows the comparison of LOCKBIT 2.0 with other ransomware gangs.

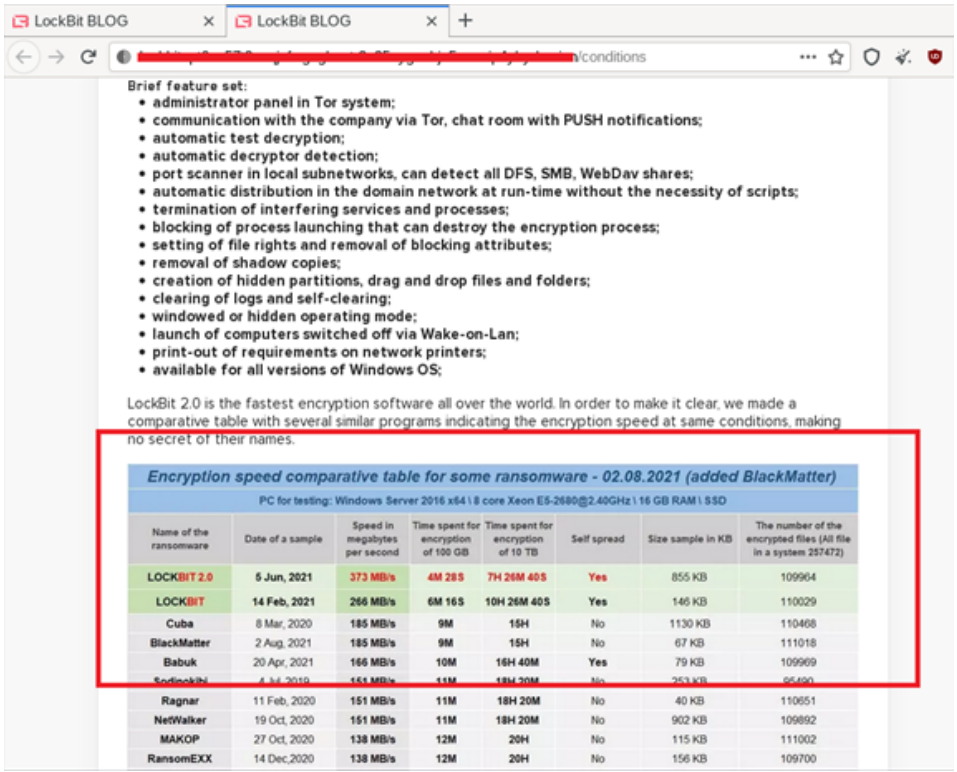
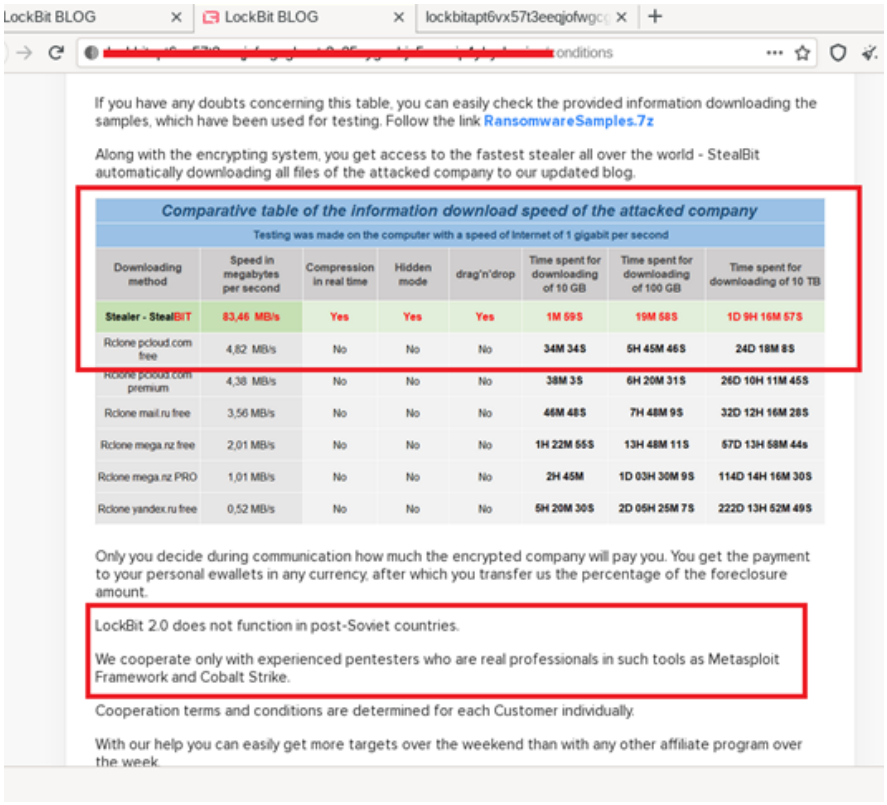


Figure 3: LOCKBIT 2.0 Comparing itself with other Ransomware Gangs

Additionally, this ransomware gang does not function in countries formerly a part of the Soviet Union. This gang also uses tools such as StealBIT, Metasploit Framework, and Cobalt Strike.

StealBIT is an information stealer used by the gang for data exfiltration. Metasploit Framework and Cobalt Strike are penetration testing tools used to emulate targeted attacks on sophisticated networks.

Figure 4 shows the post in detail.



If you have any doubts concerning this table, you can easily check the provided information downloading the samples, which have been used for testing. Follow the link RansomwareSamples.7z

Along with the encrypting system, you get access to the fastest stealer all over the world - StealBit automatically downloading all files of the attacked company to our updated blog.

Comparative table of the information download speed of the attacked company

Testing was made on the computer with a speed of Internet of 1 gigabit per second

Downloading method	Speed in megabytes per second	Compression in real time	Hidden mode	drag'n'drop	Time spent for downloading of 10 GB	Time spent for downloading of 100 GB	Time spent for downloading of 10 TB
Stealer - StealBIT	83,46 MB/s	Yes	Yes	Yes	1M 59S	19M 58S	1D 9H 16M 57S
Rclone pcloud.com free	4,82 MB/s	No	No	No	34M 34S	5H 45M 46S	24D 18M 8S
Rclone pcloud.com premium	4,38 MB/s	No	No	No	38M 3S	6H 20M 31S	26D 10H 11M 45S
Rclone mail.ru free	3,56 MB/s	No	No	No	46M 48S	7H 48M 9S	32D 12H 16M 28S
Rclone mega.nz free	2,01 MB/s	No	No	No	1H 22M 55S	13H 48M 11S	57D 13H 58M 44s
Rclone mega.nz PRO	1,01 MB/s	No	No	No	2H 45M	1D 03H 30M 9S	114D 14H 16M 30S
Rclone yandex.ru free	0,52 MB/s	No	No	No	5H 20M 30S	2D 05H 25M 7S	222D 13H 52M 49S

Only you decide during communication how much the encrypted company will pay you. You get the payment to your personal ewallets in any currency, after which you transfer us the percentage of the foreclosure amount.

LockBit 2.0 does not function in post-Soviet countries.

We cooperate only with experienced pentesters who are real professionals in such tools as Metasploit Framework and Cobalt Strike.

Cooperation terms and conditions are determined for each Customer individually.

With our help you can easily get more targets over the weekend than with any other affiliate program over the week.

Figure 4: Additional affiliate details shared by the LOCKBIT 2.0

Technical Analysis

Our static analysis of the ransomware shows that the malware file is a Windows x86 architecture Graphical User Interface (GUI) executable compiled on *2021-07-26 13:04:01*, as shown in Figure 5.

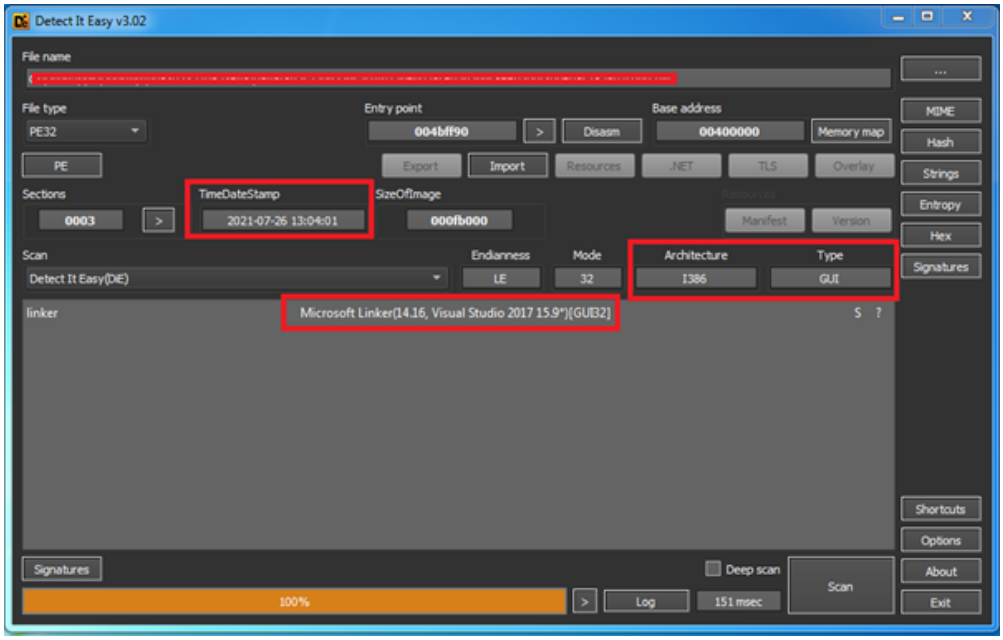


Figure 5: Static information About LOCKBIT 2.0 Ransomware

Cyble Research Labs has also found that the malware uses only a few libraries, shown in Figure 6.

library (5)	blacklist (1)	type (1)	imports (11)	description
shlwapi.dll	-	implicit	1	Shell Light-weight Utility Library
activeds.dll	x	implicit	2	ADs Router Layer DLL
kernel32.dll	-	implicit	4	Windows NT BASE API Client DLL
advapi32.dll	-	implicit	2	Advanced Windows 32 Base API
ole32.dll	-	implicit	2	Microsoft OLE for Windows

Figure 6: Libraries Used by Ransomware

Furthermore, only a few Application Programming Interfaces (APIs) were present in the ransomware import table, as shown in Figure 7.

name (11)	blacklist (5)	group (5)	ordinal (2)	library (5)
CheckTokenMembership	x	security	-	advapi32.dll
CreateWellKnownSid	x	security	-	advapi32.dll
CoSetProxyBlanket	-	security	-	ole32.dll
GetSystemTime	-	reckoning	-	kernel32.dll
9 (ADsOpenObject)	x	network	x	activeds.dll
15 (FreeADsMem)	x	network	x	activeds.dll
LocalFree	-	memory	-	kernel32.dll
CreateProcessW	x	execution	-	kernel32.dll
PathAppendW	-	-	-	shlwapi.dll
lstrlenW	-	-	-	kernel32.dll
CoCreateInstance	-	-	-	ole32.dll

Figure 7: Import Table APIs List

Figure 8 shows that the ransomware has encrypted user document files and appended them with a *.lockbit* extension while also changing the icon of all encrypted files. Additionally, the ransomware also drops a ransom note in several folders.

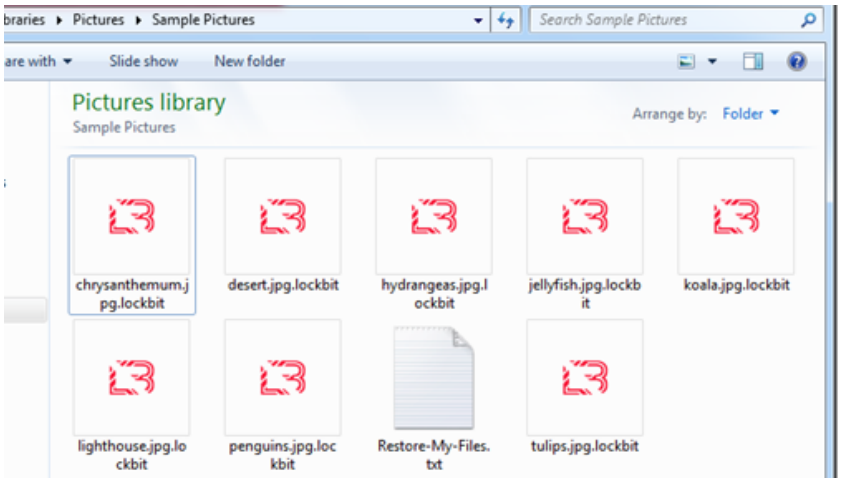


Figure 8: Encrypted Files and Ransom Note dropped by ransomware

Figure 9 shows the content of the ransom note, which instructs the victims on how they can contact the ransomware gang.

Figure 9: Content of ransom note

The ransomware also changes the desktop background, showing additional ransomware gang information, as shown below.

Figure 10: LOCKBIT 2.0 Changing Desktop Background

To get further insights into the ransomware, we checked which string symbols were present in the malware.

Figure 11 shows the details of the initial strings which are present in the malware. These strings indicate that the malware can query connected systems in the Active Directory
Domain using the Lightweight Directory Access Protocol (LDAP). In query strings, CN stands for Common Name, OU stands for Organization Unit, and DC stands for Domain Component. This information could be used for discovering other linked networks and systems.

Figure 11: Setting LDAP parameters for Microsoft Active Directory

As seen in Figure 12, the ransomware could use PowerShell commands to query the DC to get the list of computers. Once the list is received, malware could invoke the GPUpdate command remotely on the listed systems.

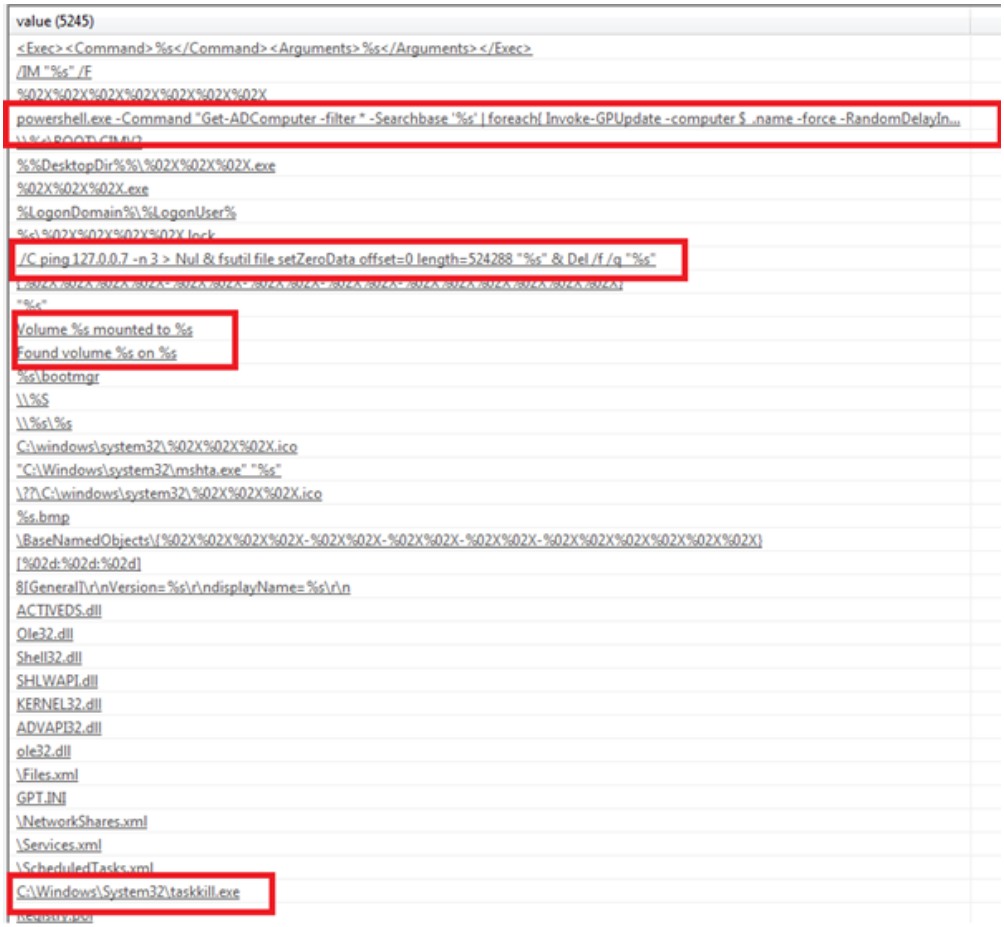


Figure 12: PowerShell command for searching computers in the network

Additionally, the ransomware checks for additional mounted hard drives, network shared drives, shared folders of VMs, and deletes the running process using *taskkill.exe shown in Figure 12.*

Figure 13 depicts the policy updates that ransomware can push in the active directory environment to other connected systems. To evade detection, the ransomware can disable Windows Defender on running systems and remote systems as well.

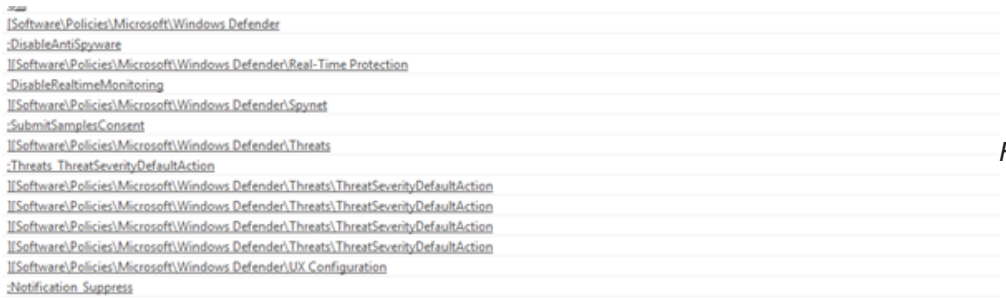


Figure 13: Windows Defender Policies are changed by the ransomware

While running the ransomware, we observed that it injects itself in *dllhost.exe,* as shown in Figure 14.

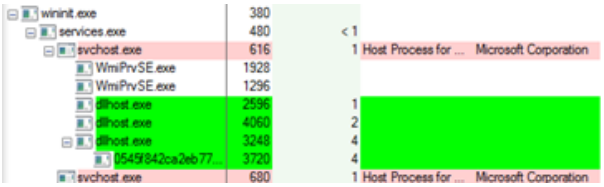


Figure 14: Ransomware infecting dllhost.exe

The ransomware adds its execution folder to the Path of the System variables, as shown in Figure 15.

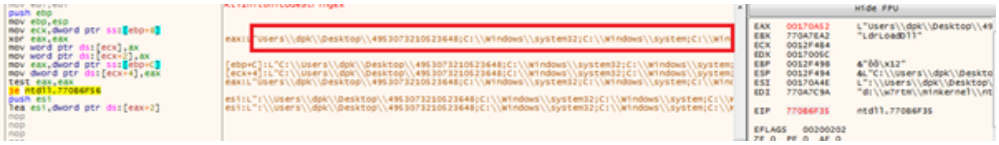


Figure 15: Malware Added its Present Working Directory in System Path

Figure 16 shows the ransomware looking for various running services like backup services, database-related applications, and other applications shown in Figure 15. If any service is found running in the system, the ransomware kills it. The ransomware uses *OpenSCManager* and *OpenServiceA,* as shown in Figure 16.

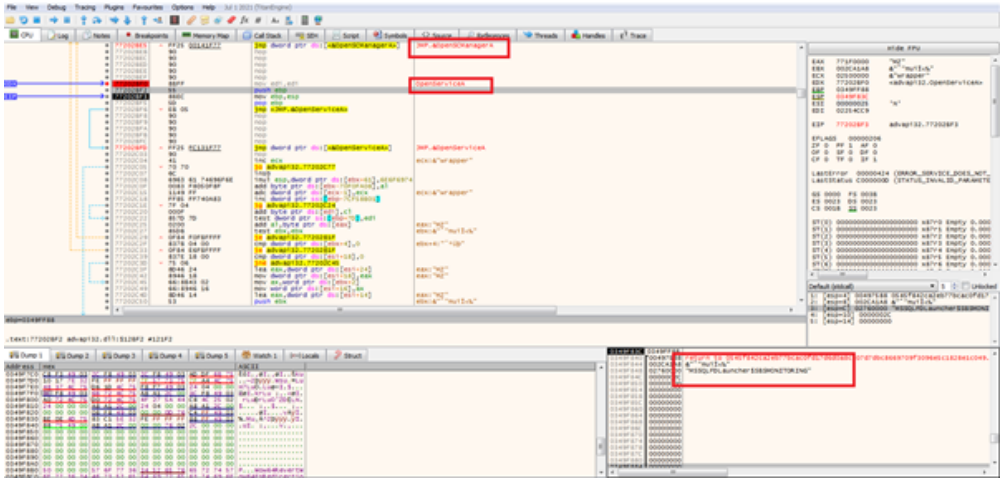


Figure 16: Ransomware searching for Services

An additional list of services searched by the ransomware is shown in the table below.

DefWatch	RTVscan	tomcat6
ccEvtMgr	sqlbrowser	zhudongfangyu
SavRoam	SQLADHLP	vmware-usbarbitator64
Sqlservr	QBIDPService	vmware-converter
sqlagent	Intuit.QuickBooks.FCS	dbsrv12
sqladhlp	QBCFMonitorService	dbeng8
Culserver	msmdsrv	MSSQL$MICROSOFT##WID
MSSQL$KAV_CS_ADMIN_KIT	MSSQLServerADHelper100	msftesql-Exchange
SQLAgent$KAV_CS_ADMIN_KIT	MSSQL$SBSMONITORING	MSSQL$SHAREPOINT
MSSQLFDLauncher$SHAREPOINT	SQLAgent$SBSMONITORING	SQLAgent$SHAREPOINT
MSSQL$VEEAMSQL2012	QBFCService	QBVSS
SQLAgent$VEEAMSQL2012	YooBackup	YooIT
SQLBrowser	vss	SQL
SQLWriter	svc$	PDVFSService
FishbowlMySQL	MSSQL	memtas
MSSQL$MICROSOFT##WID	MSSQL$	mepocs
MySQL57	sophos	veeam

MSSQL$MICROSOFT##SSEE	backup	MSSQLFDLauncher$SBSMONITORING

The ransomware creates a shared folder for VMWare to spread to other systems, as shown in Figure 17.

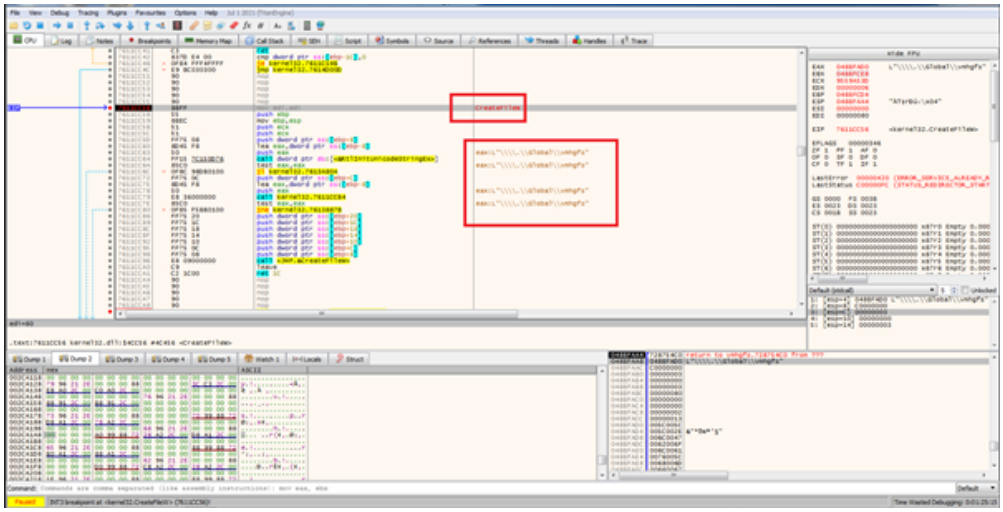


Figure 17: Ransomware creating VMWare shared folder and Dropping Sample

The encryption operation of the LOCKBIT 2.0 is similar to what we have observed in other ransomware groups. The flow of operation is shown below.

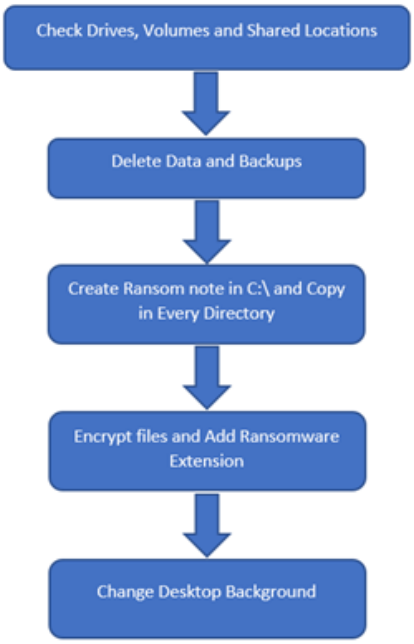


Figure 18: Common Encryption Operation

Conclusion

LOCKBIT 2.0 is a highly sophisticated form of ransomware that uses various state-of-the-art techniques to perform ransomware operations. Current and potential LOCKBIT 2.0 victims' range across multiple domains, from IT, services to banks. Our research indicates that affiliates of the group drop this ransomware inside an already

compromised network.

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 suggestions given below:

- Use strong passwords and enforce multi-factor authentication wherever possible.
- 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.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.
- Conduct regular backup practices and keep those backups offline or in a separate network.

Indicators of Compromise (IoCs):

Indicators	Indicator type	Description
0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049	Hash	SHA-256

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, and India, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com.