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.



Top 10 Industry Wise Attacks by LOCKBIT

Figure 1 – Industries Targeted by the LockBit Ransomware

In August 2021, <u>LockBit 2.0</u> 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).

Brief description of functionality: - admin panel on the Tor network; - admin panel on the Tor network; - communication with companies on the Tor network, chat with notifications and file transfer; - the ability to create private chats for secret communication with companies; - automatic decryption of test files; - automatic decrypter output, by pressing the button in the panel; - possibility of maximum protection of the decrypter, in this case the decrypter is stored on the flash drive; - StealBit stealer, searchable by file name and extension; - automatic data uploading to the blog, by you personally without our participation; - Possibility to specify any Internet port in StealBit for downloading, for example 22 or 3389, to bypass network security policies; - The ability to upload pictures to the blog; - Ability to post the history of correspondence with the attacked company to the blog; - ability to generate builds with different settings, but with one encryption key for one corporate network; - 2 different encryption lockers for Windows in one panel, written by different programmers, allowing to encrypt the network twice, if time allows, it will be useful for paranoiacs who doubt the reliability of recovery) of free space after encryption; - ability to edit the list to kill processes and services; - ability to edit the list of exceptions - computer name, names and file extensions that do not need to be encrypted;
 - shotting down the computer and missing work, to make it impossible to remove the dump from team, - printing claims on network printers in infinite numbers;

Figure 2 – LockBit 3.0 Ransomware Functionalities

While searching for the latest LockBit 3.0 sample, Cyble Research Labs came across a <u>Twitter</u> 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.

□ new_sample.exe (7500)	"C:\Users\vnew_sample.exe"-pass db66023ab2abcb9957fb01ed50cdfa6a
splwow64.exe (2332)	C:\Windows\splwow64.exe 12288
E8F0.tmp (7692)	"C:\ProgramData\E8F0.tmp"
Figure 3 LockBit 3 0 Panec	nmware Process Tree

Figure 3 – LockBit 3.0 Ransomware Process Tree

Technical Analysis

The sample hash (SHA256),

80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932cewas 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.

0041B492	ES E1DAFFFF	CALL new_sample_pkd.418F78	00418492	E8 E1DAFFFF	CALL new sample, 418F78
00418497	0F1F8400 00000000	NOP DWORD PTR DS: [EAX+EAX], EAX	0041B497	0F1F8400 00000000	NOP DWORD PTR DS: [EAX+EAX] .EAX
0041849F	6A 00	PUSH 0	0041849F	6A 00	PUSH 0
004184A1	FF15 C0754200	CALL DWORD PTR DS: [4275C0]	0041B4A1	FF15 C0754200	CALL DWORD PTR DS: [4275C0]
004184A7	0F1F80 00000000	NOP DWORD PTR DS: [EAX] EAX	0041B4A7	0F1F80 00000000	NOP DWORD PTR DS: [EAX], EAX
004184AE	E8 49F4FFFF	CALL new_sample_pkd.41A8FC	0041B4AE	E8 49F4FFFF	CALL <jmp.&getprocaddress></jmp.&getprocaddress>
00418483	E8 26F4FFFF	CALL new_sample_pkd.41A8DE	0041B4B3	E8 26F4FFFF	CALL <jmp.&getcommandlinea></jmp.&getcommandlinea>
00418488	E8 45F4FFFF	CALL new_sample_pkd.41A902	0041B4B8	E8 45F4FFFF	CALL < 3MP.&GetTickCount>
0041848D	E8 22F4FFFF	CALL new_sample_pkd.41A8E4	0041848D	E8 22F4FFFF	CALL < 3MP.&GetDateFormatW>
0041B4C2	E8 11F4FFFF	CALL new_sample_pkd.41A8D8	0041B4C2	E8 11F4FFFF	CALL <jmp.&formatmessagew></jmp.&formatmessagew>
004184C7	E8 36F4FFFF	CALL new_sample_pkd.41A902	0041B4C7	E8 36F4FFFF	CALL <jmp.&gettickcount></jmp.&gettickcount>
004184CC	E8 25F4FFFF	CALL new_sample_pkd.41A8F6	0041B4CC	E8 25F4FFFF	CALL < JMP.&GetModuleHandleW>
0041B4D1	E8 32F4FFFF	CALL new_sample_pkd.41A908	0041B4D1	E8 32F4FFFF	CALL <jmp.&loadlibraryexa></jmp.&loadlibraryexa>
004184D6	E8 15F4FFFF	CALL new_sample_pkd.41A8F0	0041B4D6	E8 15F4FFFF	CALL <jmp.&getlocaleinfow></jmp.&getlocaleinfow>
0041B4DB	E8 FEF3FFFF	CALL new_sample_pkd.41A8DE	0041B4DB	E8 FEF3FFFF	CALL <jmp.&getcommandlinea></jmp.&getcommandlinea>
004184E0	E8 05F4FFFF	CALL new_sample_pkd.41A8EA	0041B4E0	E8 05F4FFFF	CALL <jmp.&getlasterror></jmp.&getlasterror>
004184E5	E8 12F4FFFF	CALL new_sample_pkd.41A8FC	0041B4E5	E8 12F4FFFF	CALL <jmp.&getprocaddress></jmp.&getprocaddress>
004184EA	E8 FBF3FFFF	CALL new_sample_pkd.41A8EA	0041B4EA	E8 FBF3FFFF	CALL <jmp.&getlasterror></jmp.&getlasterror>
0041B4EF	E8 AEF3FFFF	CALL new_sample_pkd.41A8A2	0041B4EF	E8 AEF3FFFF	CALL <jmp.&createwindowexw></jmp.&createwindowexw>
004184F4	E8 C1F3FFFF	CALL new_sample_pkd.41A8BA	0041B4F4	E8 C1F3FFFF	CALL <jmp.&getdlgitem></jmp.&getdlgitem>
004184F9	E8 CEF3FFFF	CALL new_sample_pkd.41A8CC	0041B4F9	E8 CEF3FFFF	CALL <jmp.&getmessagew></jmp.&getmessagew>
004184FE	E8 ABF3FFFF	CALL new_sample_pkd.41A8AE	0041B4FE	E8 ABF3FFFF	CALL <jmp.&enddialog></jmp.&enddialog>
00418503	E8 CAF3FFFF	CALL new_sample_pkd.41A8D2	0041B503	E8 CAF3FFFF	CALL <jmp.&loadmenuw></jmp.&loadmenuw>
00418508	E8 B9F3FFFF	CALL new_sample_pkd.41A8C6	0041B508	E8 B9F3FFFF	CALL <jmp.&getkeynametextw></jmp.&getkeynametextw>
0041850D	E8 B4F3FFFF	CALL new_sample_pkd.41A8C6	0041850D	E8 B4F3FFFF	CALL <jmp.&getkeynametextw></jmp.&getkeynametextw>
00418512	E8 91F3FFFF	CALL new_sample_pkd.41A8A8	0041B512	E8 91F3FFFF	CALL <jmp.&dialogboxparamw></jmp.&dialogboxparamw>
00418517	E8 86F3FFFF	CALL new_sample_pkd.41A8A2	00418517	E8 86F3FFFF	CALL <jmp.&createwindowexw></jmp.&createwindowexw>
0041851C	E8 93F3FFFF	CALL new_sample_pkd.41A884	0041B51C	E8 93F3FFFF	CALL <jmp.&getclassnamew></jmp.&getclassnamew>
00418521	E8 A6F3FFFF	CALL new_sample_pkd.41A8CC	0041B521	E8 A6F3FFFF	CALL <jmp.&getmessagew></jmp.&getmessagew>
0041B526	E8 95F3FFFF	CALL new_sample_pkd.41A8C0	0041B526	E8 95F3FFFF	CALL <jmp.&getdlgitemtextw></jmp.&getdlgitemtextw>
00418528	E8 6CF3FFFF	CALL new_sample_pkd.41A89C	0041B52B	E8 GCF3FFFF	CALL <jmp.&createdialogparamw></jmp.&createdialogparamw>
e 0.0430530	EQ DODEEFEE		00440520	E8.000EEEEE	And a second

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.





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.

III ne	ew_sam	ple.exe:	196 Properties						
Imag	e Perf	formance	Performance Gra	aph Disk and Net	work	GPU Graph	Threads	TCP/IP	Se
Co	unt: 16	6							
	TID	CPU	Cycles Delta	Suspend Count	Star	t Address			
	7860			1	com	ase.dll!Ordina	al140+0x13	30	
	9016	< 0.01	2,75,532	1	new	_sample.exe+	0x10e24		
	3656			1	new	sample.exe+	0x1b46f		
	3384			1	new	sample.exe+	0x9328		Figure
	3460			1	new	sample.exe+	0x96ec		
	6376			1	new	sample.exe+	0x9cd8		
	2716			1	new	sample.exe+	0xc020		
	8692			1	new	sample.exe+	Oxfcac		
	3196			1	new	sample.exe+	Oxfcac		
	6720			1	new	sample.exe+	Oxfcac		
	2244			1	new	sample.exe+	Oxfcac		
	6304			1	new	sample.exe+	Oxfcac		
	888			1	ntdll.	dll!TpCallback	Independe	ent+0x140)
	5256			1	ntdll.	dll!TpCallback	Independe	ent+0x140)

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.

PUSH EAX	eax:L"SELECT * FROM Win32_ShadowCopy"
PUSH 1 PUSH 0	
LEA EAX, DWORD PTR SS: EBP-4C	
PUSH EAX	eax:L"SELECT * FROM Win32_ShadowCopy"
TEST EAX,EAX	eax:L"SELECT * FROM Win32_ShadowCopy"
JE new_sample.40998B	
PUSH D	
PUSH EAX	eax:L"Win32_ShadowCopy.ID='%s
CALL new_sample.401260	
LEA EAX, DWORD PTR SS: EBP-8	

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	1
Windows Bind Filter Driver	AsyncMac	
bindfit	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	Figuro
BasicDisplay	AppvVemgr	i iyure
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	applockerfitr	

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."*

→ This PC → Local Disk (C:) → programdata	>		
Name	Date modified	Туре	Size
🕼 HLJkNskOq.ico	04-07-2022 08:30	lcon	15 KB
Computer HKEY_CLASSES_ROOT\HLJkNskOq\Defa	ilticon		
HLJkNskOq Defaulticon	Name (Default)	Type REG SZ	Data C:\ProgramData\HLJkNskOg.ico

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."*

HLJkNskOq.README.txt - Notepad
File Edit View
<pre>~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~</pre>
>>>>> Your data is stolen and encrypted. If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our lea sooner your company will be safe.
Tor Browser Links: http://lockbitapt17711107711107711107711071100000000000
Links for normal browser: http://lockbitapt123b-1bour 27bulisur 20bour 27bulisur 20bour 27bulisur 20bour 27bulisur 20bour 27bulisur 20bour 20
>>>>> What guarantee is there that we won't cheat you? We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically data. After you pay the ransom, you will quickly make even more money. Treat this situation simply as a paid training for your system services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it. If we don't give yo Twitter https://twitter.com/hashtag/lockbit?f=live

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	Туре	Size
56RS4N6.HLJkNskOg	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
🗐 ajdl5Xn.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.

	у		
	DDATA TWITTER	HOW TO BUY BITCOIN AFFILIATE RULES	> 🕼 CONTACT US > 🚓 MIRRORS
A DESCRIPTION OF A DESC	Construction sees.	Contraction in contract	TRACTOR AND A DESCRIPTION OF
The state of the second	C P		
🕒 Updatesti D4 3.4. 2022. 44:05 UTC 564 👁	C Updavan 54 A.C. 2022. 54656 UTC 487 📀	S Updaver 14 AL 1922. SASA UTC S31 🔘	(C) Updavelt 04 34, 2022, 04054 UTC 65
Congressions Constants (mass	Land an extension	tipes afronts and	finite see
I and a second s		N E N	
S Opennet: 64 Art. 2022, 65:17 UTC 507 G	🕒 Sipelanen 54 Aug 2022, 45-17 UTC 4550 👁	G Updated: 14 Aug 2022. 15/18 UTC 1137 @	G Updatum 64 Aul. 2022. 05:17 UTC 1771
	PIC		
🕞 updatest: 54 a.e. 2022, 05:17 UTC 1702 🔿	C Updates \$4.34.2422, \$5.17.07C 1580 G		
	TWITTER > E HOW TO	BUY BITCOIN > CONTACT US	\$

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.

	HOW TO BUY BITCOIN				
L Ways To Buy Bitcoin — # — There are some options to buy Bitcoin. Choose what suits you the best.					
BANK ACCOUNT	CREDIT CARD	PAYPAL	CASH DEPOSIT		

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

Indicator Of Compromise (IOCs)

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