LockBit: Ransomware Puts Servers in the Crosshairs

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lockbit-targets-servers





Vishal KamblePrincipal Threat Analysis Engineer



Lahu KhatalSenior Threat Analysis Engineer

LockBit affiliates using servers to spread ransomware throughout networks.

Symantec, a division of <u>Broadcom Software</u>, has observed threat actors targeting server machines in order to spread the LockBit ransomware threat throughout compromised networks.

In one attack observed by Symantec, LockBit was seen identifying domain-related information, creating a Group Policy for lateral movement, and executing a "gpupdate /force" command on all systems within the same domain, which forcefully updates group policy.

LockBit

LockBit is a ransomware-as-a-service (RaaS) operated by malicious actors Symantec tracks as Syrphid.

Shortly after it first appeared in September 2019, the Syrphid gang expanded its operations, using a network of affiliates to deploy the LockBit ransomware on victim networks. The ransomware, which has currently reached <u>version 3.0</u>, has evolved over the past few years, as has its operators who have recently <u>launched a bug bounty program</u> in order to weed out weaknesses in the malware's code and the RaaS operation as a whole.

Attack chain

In one observed instance, before dropping and executing the LockBit ransomware, an attacker had RDP access to the enterprise network for a couple of weeks at least. This access may have been obtained through remote desktop applications such as AnyDesk or Windows RDP, or by exploiting a known vulnerability, etc.

LockBit behaves differently on server machines with domain controllers than on Windows 10 machines. When executed on a server, it has the capability to spread through the network using Group Policy. On Windows 10 machines it performs routine ransomware activity and encrypts files.

When LockBit is executed on a server machine it carries out the following actions:

1. Debugger check

LockBit first checks if the malware process is being debugged. If this is the case, it goes into an infinite loop.

	000000000040FF90 var_20 00000000040FF90 var_20 00000000040FF90	8C= dword ptr -20Ch 88= byte ptr -20Ch	Entry point
	000000000040FF91 mov 00000000040FF93 and 00000000040FF95 mov 00000000040FF95 sub 0000000040FF92 test	eBp, esp esp, BFFFFFFFBh Logical MD eak, lange fs:30h esp, 480h Integer Sustraction byte ptr [eak+68h], 70h Logical Compo-	
	000000000048FFA7 push 000000000048FFA8 jz	edi short loc_40FF02 ; Jump lf Zero (ZF=1)	
00000000000000000000000000000000000000			000000000000000000000000000000000000
interpreterent for the second of FDB interpreterent	Infinite Loop		<pre>Dependence(CD)10 econoconcect(CD)10 econoconcect(CD)10 econoconcect(CD)10 econoconcect(CD)10 econoconcect(CD)10 econoconcect(CD)1 eco</pre>

Figure 1. If malware process is being debugged, LockBit goes into an infinite loop 2. Language Check

- It calls GetSystemDefaultUILanguage and GetUserDefaultUILanguage to check the language.
- If the language matches with the one on the malware's list then it terminates immediately.
- LockBit does not target Russia or a selection of nearby countries.

NO LENGT	-			
0049B2F9	>	A3 108C4F00	MOU DWORD PTR DS:[4F8C10],EAX	
0049B2FE	>	FFDØ	CALL EAX	A
0049B300		B9 2C040000	MOU ECX,42C	Azeri (Cyrillic) Azerbaijan
0049B305		ØFB7C0	MOUZX EAX,AX	Kazakh Kazakhatan
0049B308		C745 F0 2C08	MOV DWORD PTR SS:[EBP-10],82C	Kazakristan
0049B30F		8D51 FF	LEA EDX,[ECX-1]	Kurguz Kurguzetan
00498312		8D59 F7	LEA EBX,[ECX-9]	Kyrgyz i Kyrgyzstan
0849B315		8D71 ØB	LEA ESI,[ECX+0B]	Russian Russia
0049B318	,	8D79 F6	LEA EDI,[ECX-0A]	
0049B31B		66:3B45 F0	CMP AX, WORD PTR SS:[EBP-10]	Tajik (Cyrillic) , Tajikistan
0049B31F	·	74 6D	JE SHORT 0049B38E	TI TI II
0049B321		66:3BC1	CMP AX,CX	Turkmen , Turkmenistan
0049B324	14	74 68	JE SHORT 0049B38E	Uzhak (Cuvillia) Uzhakiatan
0049B326		66:3BC2	CMP AX, DX	UZDEK (Cyriffic) , UZDEKIStan
0049B329	•	74 63	JE SHORT 0049B38E	Ilzbek (Latin) Ilzbekistan
0049B32B		66:3BC3	CMP AX, BX	OZDER (Latin) i Ozberistan
0049B32E	* v	74 5E	JE SHORT 0049B38E	
0049B330		66:3BC6	CMP AX,SI	
0049B333	*.~	74 59	JE SHORT 0049B38E	
0049B335		B9 3F040000	MOU ECX, 43F	
0049B33A		66:3BC1	CMP AX,CX	
0049B33D	• •	74 4F	JE SHORT 0049B38E	
0049B33F		B9 40040000	MOU ECX,448	
0049B344		66:3BC1	CMP AX,CX	
0049B347	• .	74 45	JE SHORT 0049B38E	
0049B349		B9 19080000	MOU ECX,819	
0049B34E		66:3BC1	CMP AX,CX	
0049B351	*~	74 38	JE SHORT 0049B38E	
0049B353		B9 19848888	MOU ECX, 419	
0049B358		66:3BC1	CMP AX,CX	
0049B35B	•~	74 31	JE SHORT 0049B38E	
0049B35D		B9 28040000	MOU ECX,428	
0049B362		66:3BC1	CMP AX,CX	
0049B365	• •	74 27	JE SHORT 0049B38E	
0049B367		B9 42040000	MOU ECX,442	
0049B36C		66:3BC1	CMP AX,CX	

EAX=00000419 (decimal 1049.) (current registers) [004F8C10]=74F52C52 (kernel32.GetSystemDefaultUILanguage) Jump from 49B7EB

Figure 2. LockBit calls GetSystemDefaultUILanguage and GetUserDefaultUILanguage to check the language.

3. End running processes and disable services

- LockBit ends a list of running processes related to malware analysis and other processes like Process Explorer, Process Monitor, Wireshark, Dumpcap, Process Hacker, cmd.exe, TeamViewer, Notepad, Notepad++, WordPad etc.
- Disables a list of services related to SQL, backup, and MSExchange etc.
- 4. Privilege escalation
 - Duplicates the token by calling **DuplicateTokenEx** and creates a new process using **CreateProcessAsUserW.**
 - After it achieves privilege escalation, LockBit relaunches itself under DLLHost.exe. Once the new process is spawned, the LockBit process ends itself.
- 5. Bypass UAC

LockBit injects code into dllhost.exe with CLSIDs of COM objects, which runs the following command to bypass UAC:

A. Exploiting USERENV.dll to bypass UAC

- B. Bypass method in hfiref0x's UACME
- C. Exploiting the ICMLuaUtil elevated COM Interface-Object

6. LockBit creates a copy of itself under the SYSVOL directory "c:\windows\sysvol\domain\scripts\< Lockbit executable>"

7. Creating a Group Policy:

- Once the malware identifies it is running as an admin user and a domain controller is installed on the system, it creates a Group Policy to stop services, end processes, and copy LockBit etc.
- Under the "C:\Windows\SYSVOL\domain\Policies\<policy GUID>" folder, LockBit creates XML files that are required for the Group Policy.

Computer configurations:

- It first creates a policy to turn off Windows Defender, suppress all notifications, disable file submissions, turn off real-time protection etc.
- It then maps the network drive through Group Policy.
- Disables services related to SQL server at startup.

User Configurations:

- The malware copied the ransomware from SYSVOL to the Desktop directory.
- It then creates a scheduled task to end the list of processes previously mentioned.

	ows + SYSVOL + domain + Policies + (CFA31D2E-A12F-4005-BF66-B784F447171B) + User + Preferences + Files	
SystemApps	Name Outermodified Type Size	
SVSVOL	- PHELATR - 4/27/2022 T1/2/488 AMAL DOCUMENC 11 KB	
🦲 domain		
/ DfsiPrivate		
Policies	C\Windows\SYSVOL\domain\Paticies\[CFA3ID2E-A12F-4005-8F66-8784F447171B]\User\Preferences\Files\Files\aml-Natepad++	
6AC1786C-016F-11D2-945F-00C04/8984F9;	File Edit Search View Encoding Language Settings Tools Macro Run TestFX Plugins Window ?	
(31B2F340-016D-11D2-945F-00C04FB984F9)		
CFA31D2E-A12F-4005-8F66-8784F4471718	Flearer [2]	
Machine	3 «7zml version="1.0" encoding="wif-6"7>	_
Preferences	2 E <files clsid="(215B2E53-57CE-4750-80FE-9EEC14635851)"> <file clsid="(30BE44C8-567A-4ed1-B1D0-9234FE1F38AF)" name-<="" p=""></file></files>	
Natural Shares	"41854C8986F76E01" status="41854C3986F78E01" image="2" bypassError="1" changed="2022-04-27 11:05:55" did=	
THEOWY DIRECTION OF THE PLAN AND A DECEMBER OF THE PLAN AND AND AND A DECEMBER OF THE PLAN AND A DECEM	<pre>(introduces local system) synchrones. local local systems interested to the state "interested to the system interest interested to the system interest interest interested to the system interest inter</pre>	all the second
Services		Contract The International Contract of the International Contract
Services	*1" hidden="0" suppress="0"/>	Ullave
Services	*1* hidden*"0" suppress*"0"/> -	CHATE-
Veries Veries Veries Veries Veries	*1* hidden*"0" suppress*"0"/>	CII2 VE
Services User Proferences Files ScheduleaTasks	*1* hidden*"0" suppress*"0"/>	
Free of the second	"1" hidden="0" suppress="0"/>	CHIL YE

Figure 3.Group Policy XML file used to copy LockBit from the shared SYSVOL location to client's desktop location.



Figure 4. Group Policy created by LockBit can be seen in the Group Policy Management console.

puter Configuration (Enabled)			
licies			
Administrative Templates			
Policy definitions (ADMX files) retrieved from the central store.			
Windows Components/Windows Defender Antivirus			
Policy	Setting		Comment
Turn off Windows Defender AntiVirus	Enabled		
Windows Components/Windows Defender Antivirus/Client Interface			
Policy	Setting		Comment
Suppress all notifications	Enabled		
Windows Components/Windows Defender Antivirus/MAPS			
Policy	Setting		Comment
Send file samples when further analysis is required	Enabled		
Send file samples when further analysis is required		Never send	
Windows Components/Windows Defender Antivirus/Real-time Protection			
Policy	Setting		Comment
Turn off real-time protection	Enabled		
Windows Components/Windows Defender Antivirus/Threats			
Policy	Setting		Comment
Specify threat alert levels at which default action should not be taken when detected	Enabled		
Specify threat alert levels at which default action should not be taken when detected			
1		6	
2		6	
+		6	
5		6	

Figure 5. Group Policy details to disable Defender and several additional options.

ferences	
Vindows Settings	
Network Shares	
Network Share (Name: %ComputerName%_D)	
%ComputerName%_D (Order: 1)	
Sharing	
Action	Update
Share name	%ComputerName%_D
Folder path	D:
User limit	No change
Access-based Enumeration	No change
Common	
Options	
Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No
Network Share (Name: %ComputerName%_E)	
Network Share (Name: %ComputerName%_F)	
Network Share (Name: %ComputerName%_G)	
Network Share (Name: %ComputerName%_H)	
Network Share (Name: %ComputerName%_I)	
Network Share (Name: %ComputerName%_J)	
Network Share (Name: %ComputerName%_K)	

Figure 6. Group Policy used to map network drives.

1

onfiguration (Enabled)	
erences	and the set of the set of the set of the
indows Settings	
Files	
File (Target Path: %DesktopDir%)6341D6.exe)	
41E54C89B6FF8E01 (Order: 1)	
General	
Áction	Update
Properties	
Source file(s)	symcdemos local sysvol symcdemos local scripts 6341D6 e
Destination file	%DesktopDir%i6341D6.exe
Suppress errors on individual file actions	Disabled
Attributes	
Read-only	Disabled
Hidden	Disabled
Archive	Enabled
Common	
Options	
Stop processing items on this extension if an error occurs on this item	No
Run in logged-on user's security context (user policy option)	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

Figure 7. Group Policy used to disable SQL services at startup.

ences	
dows Settings	
les .	
File (Target Path: %DesktopDir%6341D6.exe)	
41E54C89B6FF8E01 (Order: 1)	
General	
Action	Update
Properties	
Source file(s)	symcdemos local sysvol symcdemos local scripts 6341D6
Destination file	%DesktopDir%6341D6.exe
Suppress errors on individual file actions	Disabled
Attributes	
Read-only	Disabled
Hidden	Disabled
Archive	Enabled
Common	
Options	
Stop processing items on this extension if an error occurs on this item	No
Run in logged-on user's security context (user policy option)	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

Figure 8 Group Policy used to copy LockBit from the SYSVOL shared location to the desktop.

(11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			
(B64C4157B2B9 (Order: 2)			
General			
Action.		Update	,
Task			
	Name	84B64C4157B2B9	
	Author	SYMCDEMOS testuser	
	Description		
	Run only when user is logged on	InteractiveToken	
	UserId	SYMCDEMOS testuser	
	Run with highest privileges	HighestAvailable	
	Hidden	Ne	
	Configure for	12	
	Enabled	Yes	
Triggers			
1. At task creation modification			
	Enabled	Yes	
Actions			
1. Start a program			
	Program/script	%DesktopDir%6341D6.exe	
	Arguments		
Settings			
	Stop if the computer ceases to be idle	No	
	Restart if the idle state resumes	No	
	Start the task only if the computer is on AC power	No	
	Stop if the computer switches to battery power	No	
	Allow task to be run on demand	Yes	
	Stop task if it runs longer than	3 days	
	If the running task does not end when requested, force it to stop	Yes	
	If the task is already running, then the following rule applies	IgnoreNew	
onimon			
Options			
Stop processing items on this extension if an error occurs on this item		Ne	
Run in logged-on user's security context (user policy option)		No	
Remove this item when it is no longer applied		No	
A make some and do not so some		No	

Figure 9. Group Policy used to end processes using the taskkill command.

B04C4157B2B9 (Order: 2)			
ieneral			
Action			Update
Task			
	Name	84B64C4157B2B9	
	Author	SYMCDEMOS testuser	
	Description		
	Run only when user is logged on	InteractiveToken	
	UserId	SYMCDEMOS testuser	
	Run with highest privileges	HighestAvailable	
	Hidden	No	
	Configure for	1.2	
	Enabled	Yes	
Triggers			
1. At task creation/modification			
	Enabled	Yes	
Actions			
1. Start a program			
	Program/script	%DesktopDir%6341D6.exe	
	Arguments		
Settings			
1	Stop if the computer ceases to be idle	No	
	Restart if the idle state resumes	No	
	Start the task only if the computer is on AC power	No	
	Stop if the computer switches to battery power	No	
	Allow task to be run on demand	Yes	
	Stop task if it runs longer than	3 days	
	If the running task does not end when requested, force it to stop	Yes	
	If the task is already running, then the following rule applies	IgnoreNew	
ominon			
Options			
Stop processing items on this extension if an error occurs on this item			Ne
Run in logged-on user's security context (user policy option)			No
Remove this item when it is no longer applied			No
hash were and do and some he			

Figure 10. Group Policy used to execute the LockBit ransomware.

8. Lateral movement:

LockBit launches powershell.exe to run the command shown below in order to search through all the computers on the Active Directory. For each host it uses the GPUpdate force command (gpupdate) to apply the newly created Group Policy.

9. Executes gpupdate command on the domain controller where LockBit is running. Also runs gpupdate to run policies from the computer configurations and user configurations.

10. Firewall

LockBit reads firewall rules using the Windows Defender Firewall with Advanced Security API's "**FwPolicy2**" object. The following CLSID COM object is called:

11. Impact

LockBit attempts to delete shadow copies using VSSADMIN and WMIC. It also tries to disable recovery using the BCDEdit command.

Want to comment on this post?