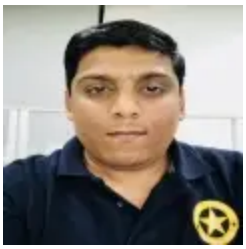
LockBit: Ransomware Puts Servers in the Crosshairs

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 Broadcom Software, 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 version 3.0, has evolved over the past few years, as has its operators who have recently launched a bug bounty program 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.

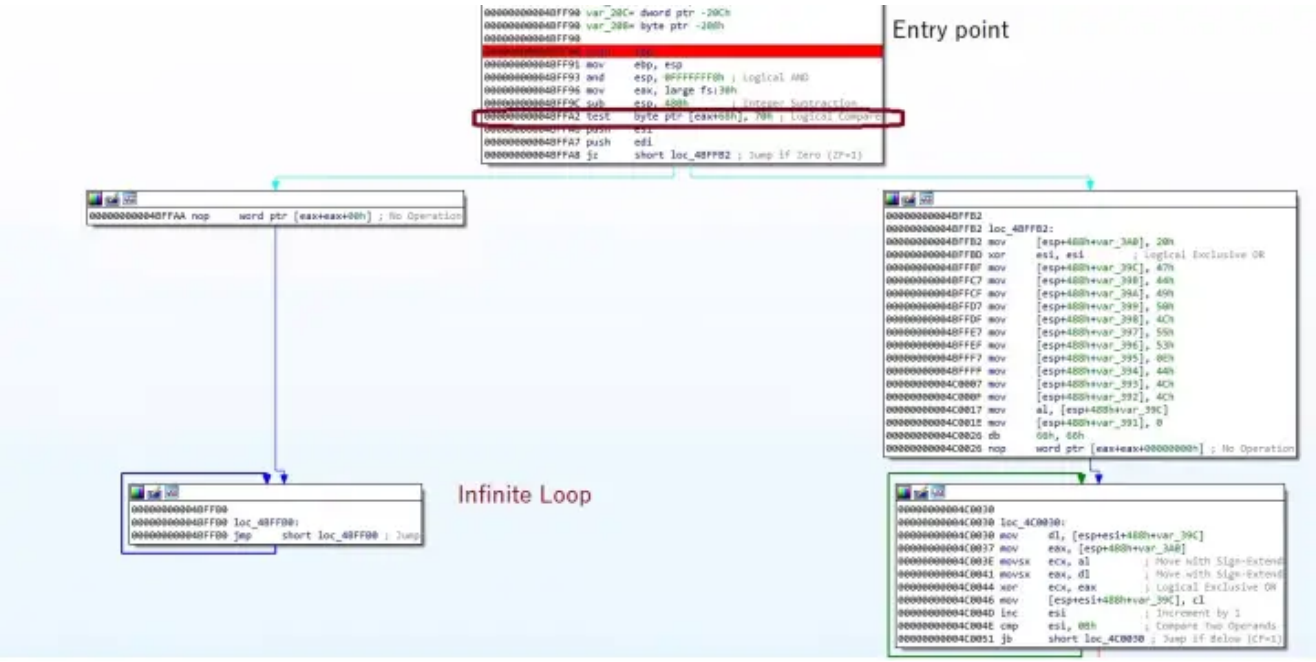


Figure 1. If malware process is being debugged, LockBit goes into an infinite loop

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.

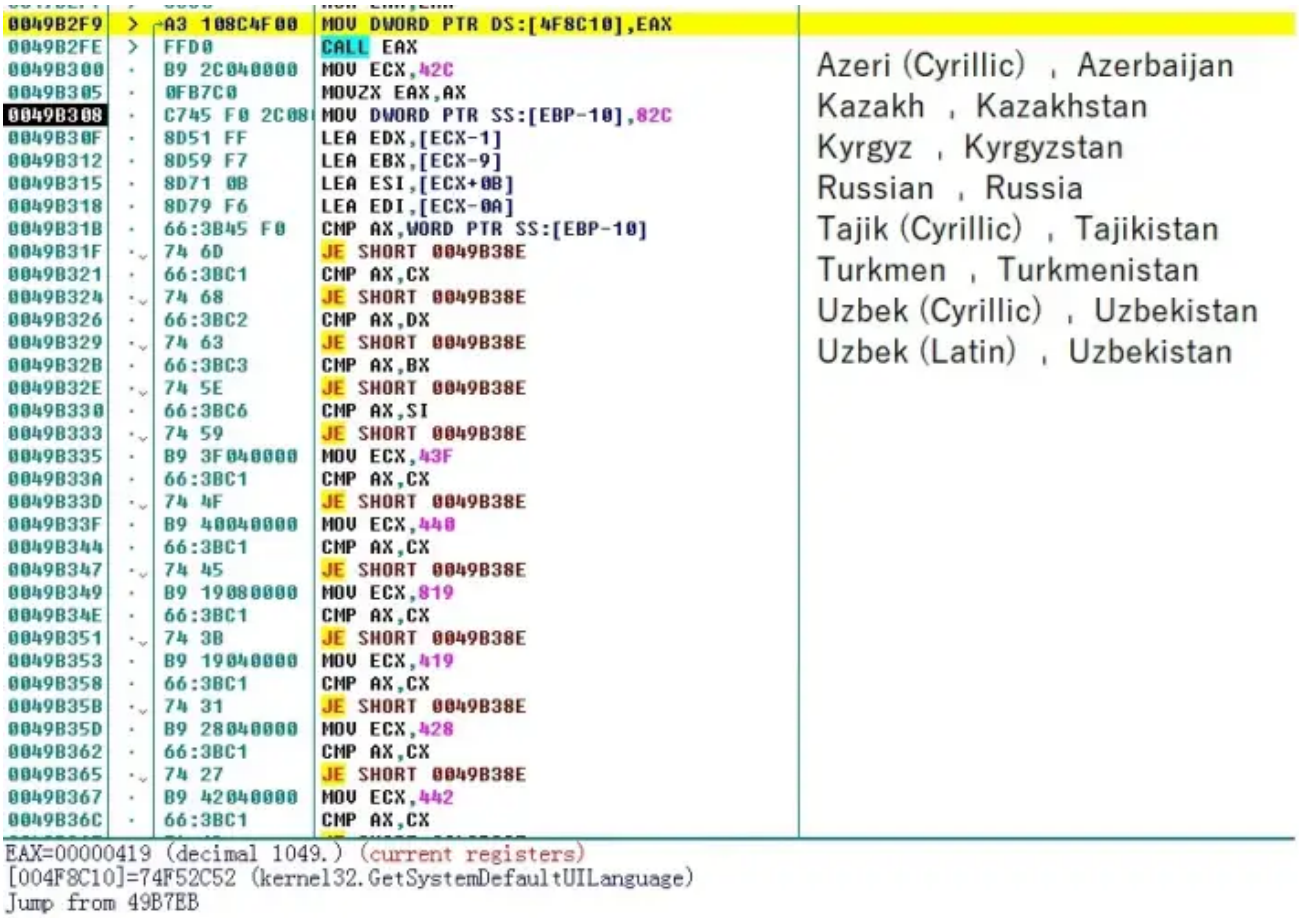


Figure 2. LockBit calls GetSystemDefaultUILanguage and GetUserDefaultUILanguage to check the language.

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.

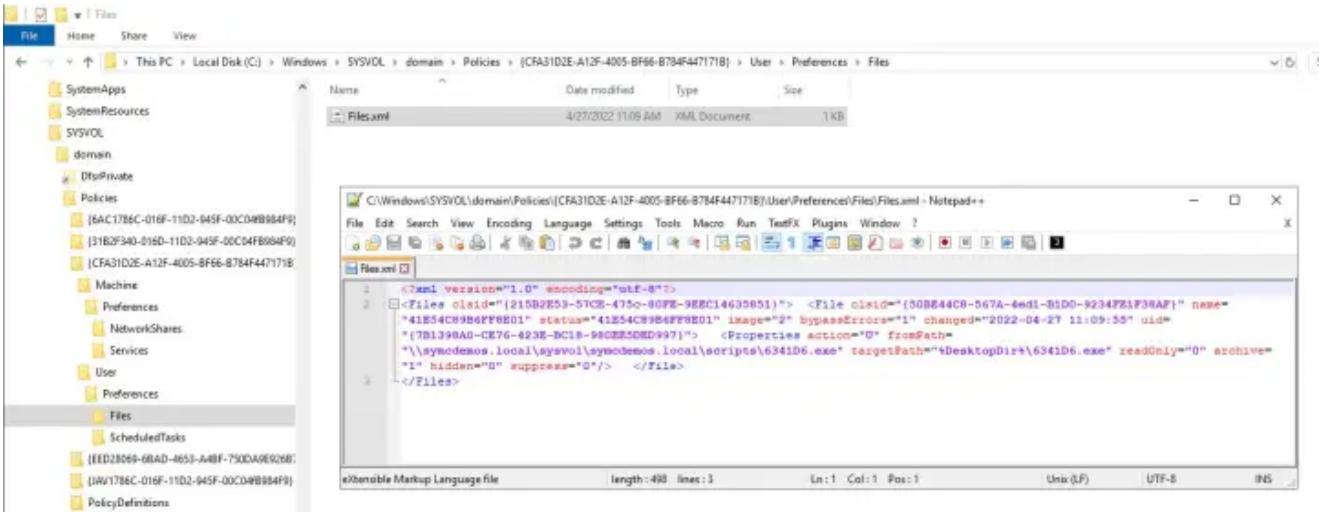


Figure 3.Group Policy XML file used to copy LockBit from the shared SYSVOL location to client's desktop location.

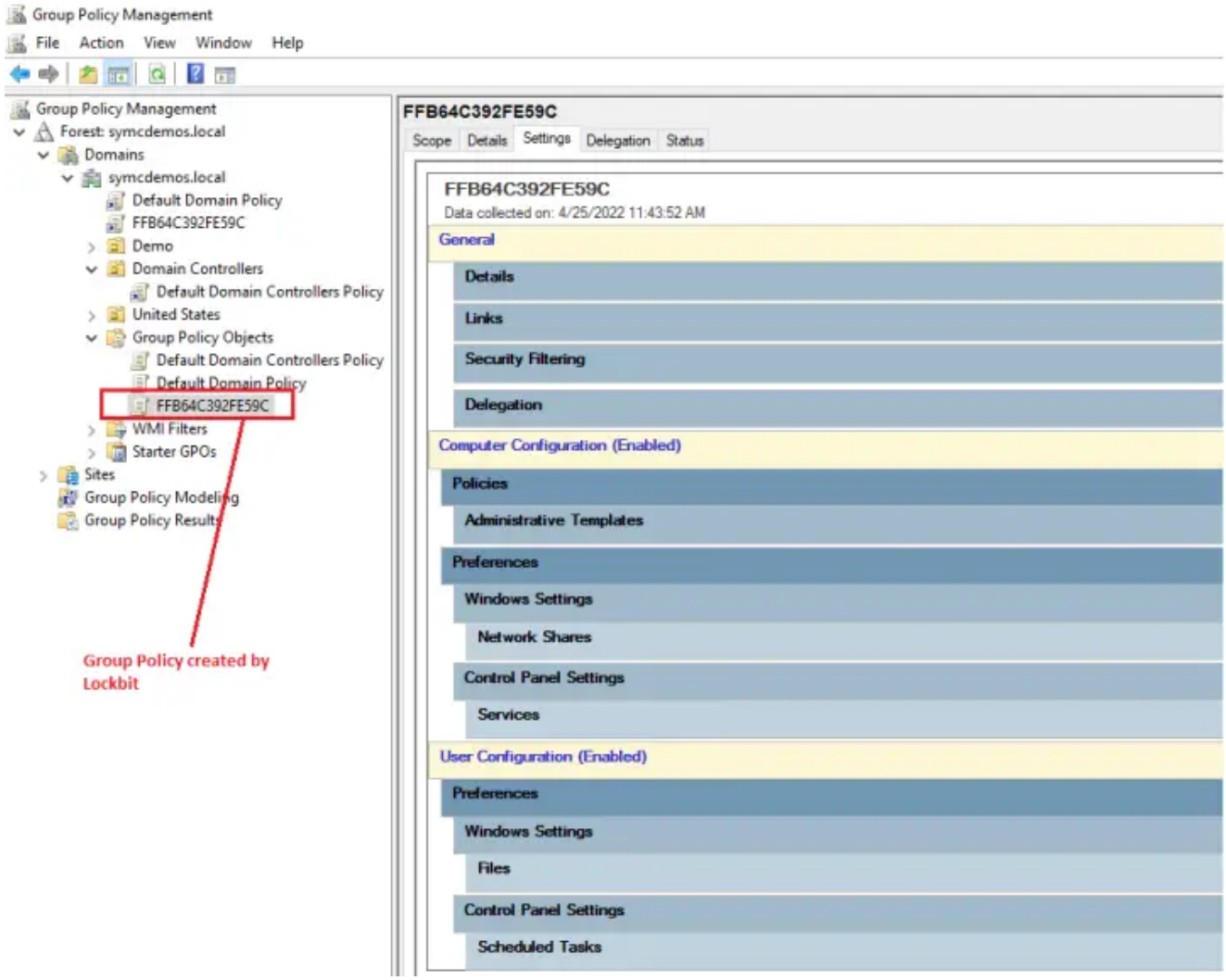
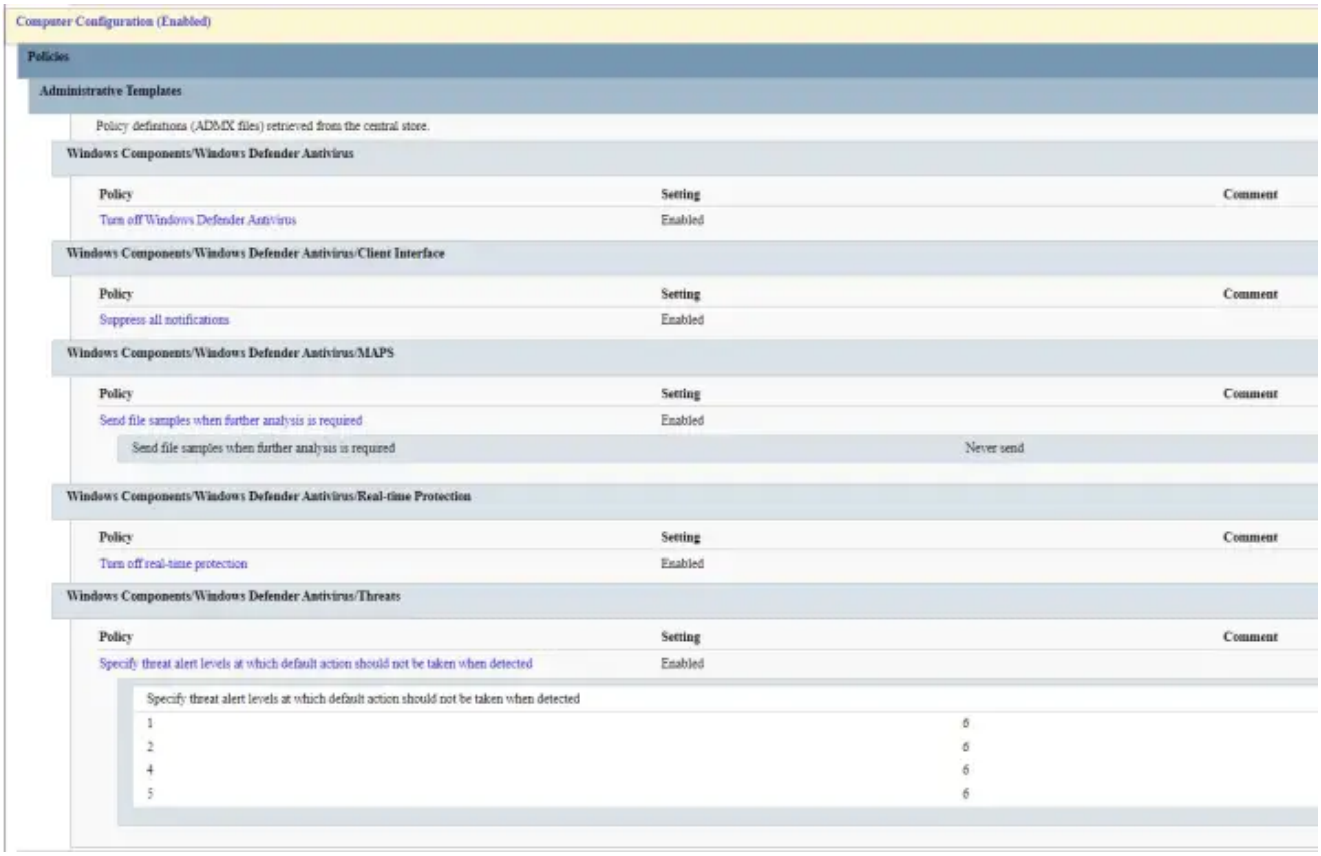


Figure 4. Group Policy created by LockBit can be seen in the Group Policy Management console.



Computer Configuration (Enabled)

Policies

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	
Send file samples when further analysis is required	Never send

Windows Components/Windows Defender Antivirus/Real-time Protection

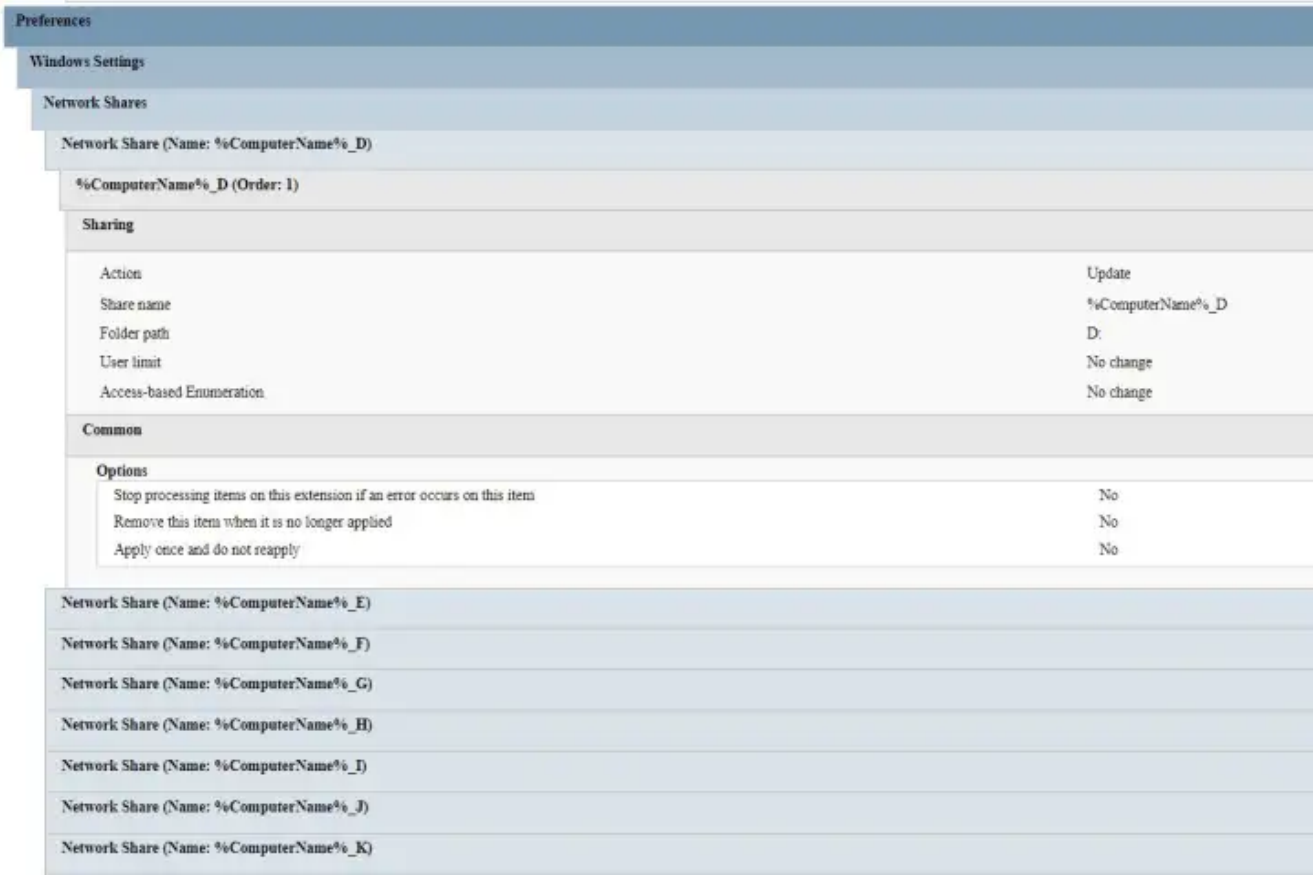
Policy	Setting	Comment
Turn off real-time protection	Enabled	

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
4	6
5	6

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



Preferences

Windows 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.

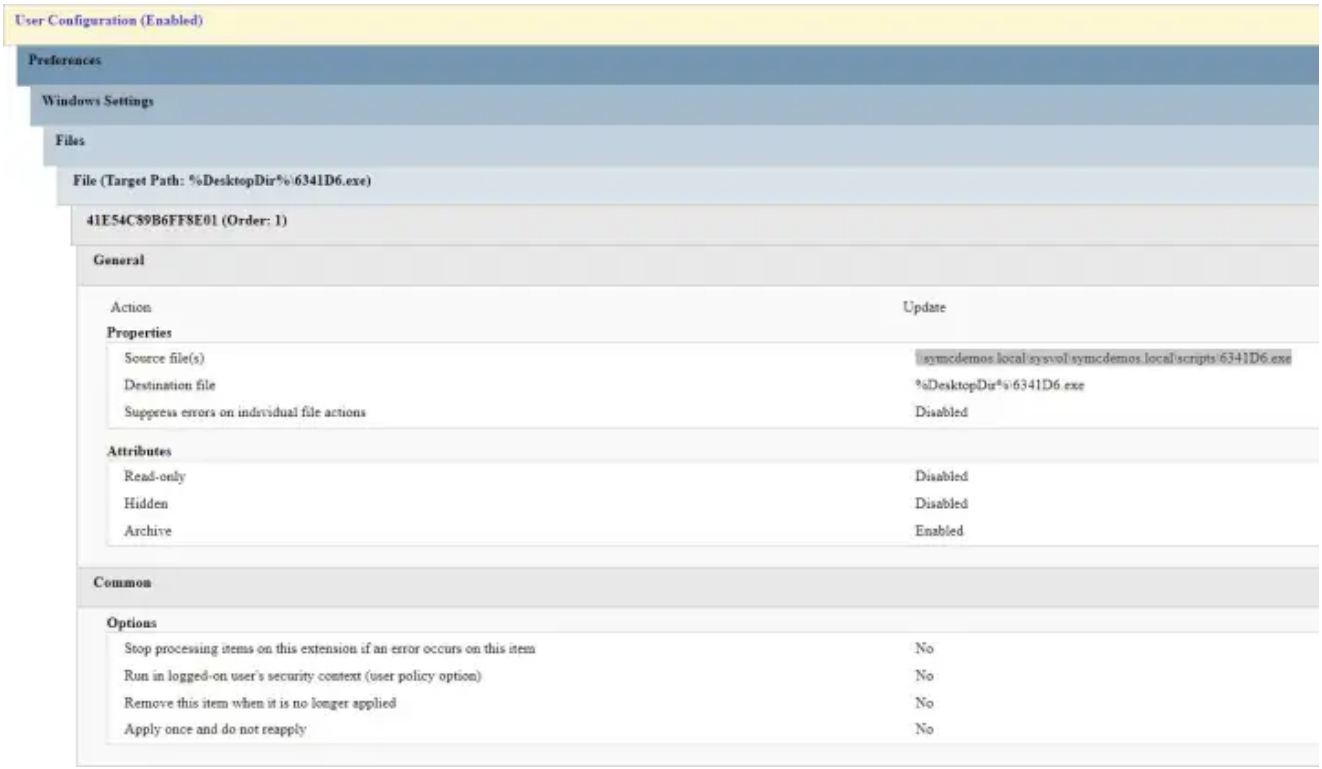


Figure 7. Group Policy used to disable SQL services at startup.

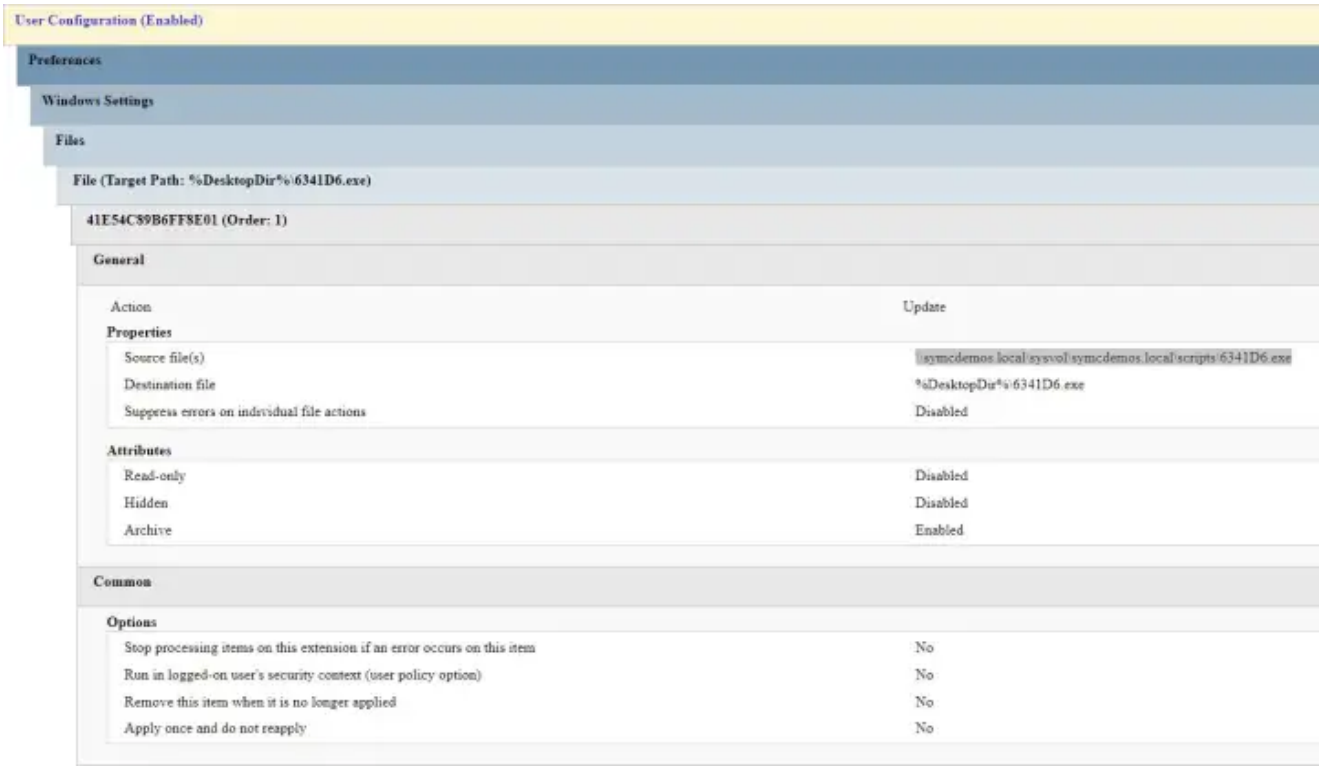
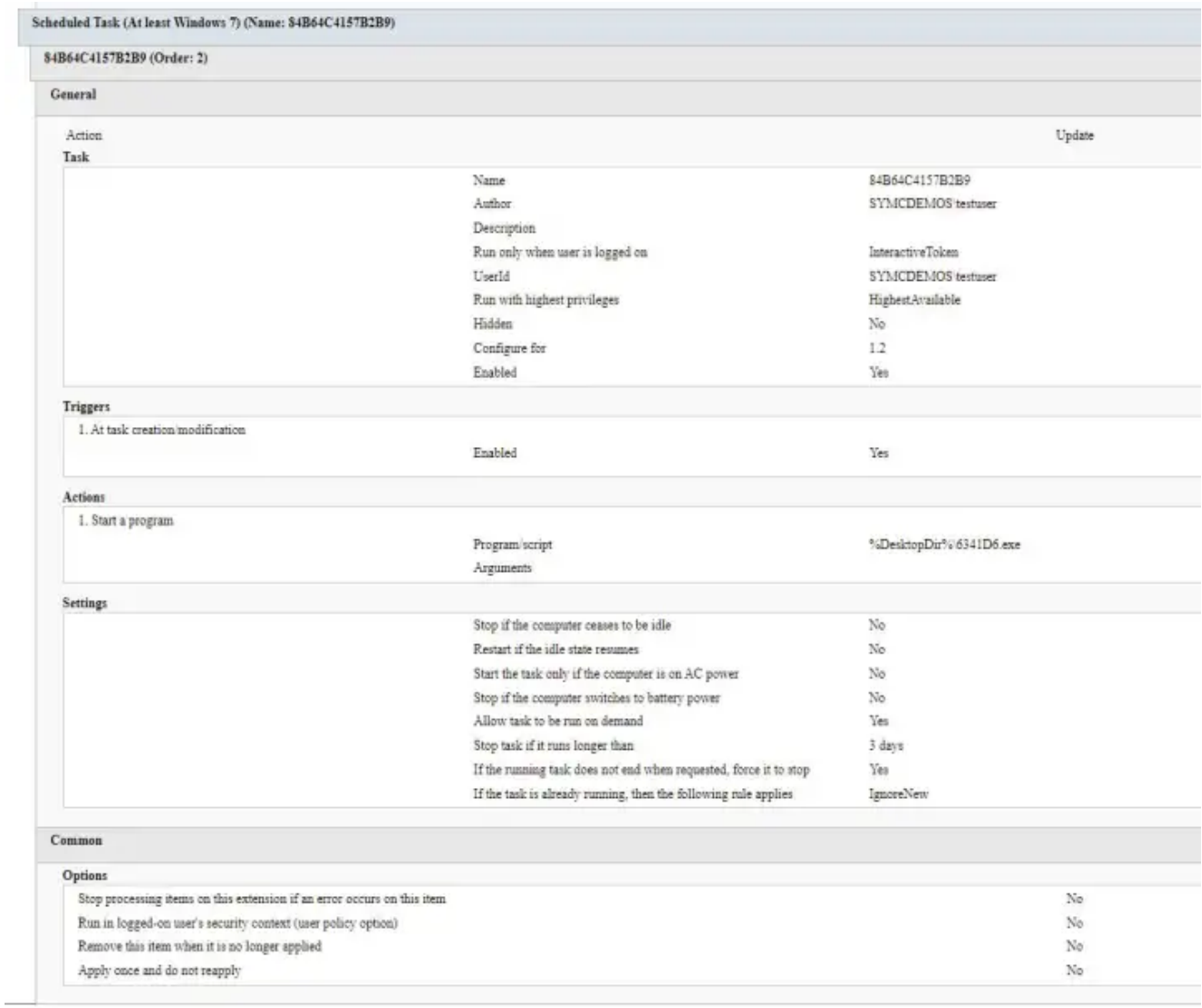


Figure 8 Group Policy used to copy LockBit from the SYSVOL shared location to the desktop.



Scheduled Task (At least Windows 7) (Name: 84B64C4157B2B9)

84B64C4157B2B9 (Order: 2)

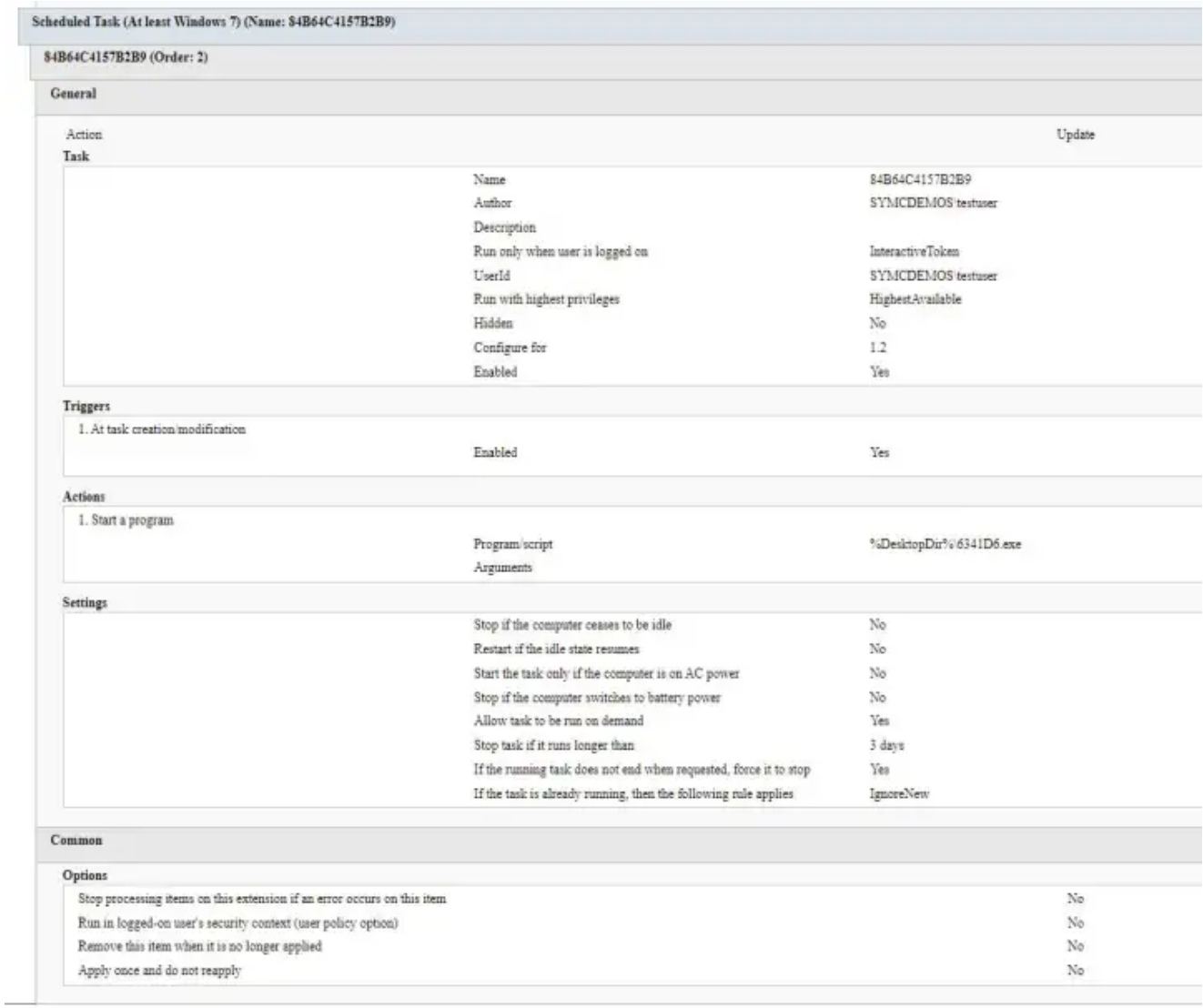
General

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	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		
	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

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



Scheduled Task (At least Windows 7) (Name: 84B64C4157B2B9)

84B64C4157B2B9 (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	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		
	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

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 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?