LockBit: Ransomware Puts Servers in the Crosshairs

By About the Author

Archived: 2026-04-05 17:08:06 UTC

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 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.

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

```
C:\Windows\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}
```

B. Bypass method in hfiref0x's UACME

```
C:\Windows\SysWOW64\DllHost.exe /Processid:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}
```

C. Exploiting the ICMLuaUtil elevated COM Interface-Object

```
C:\Windows\SysWOW64\DllHost.exe /Processid:{D2E7041B-2927-42FB-8E9F-7CE93B6DC937}
```

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

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

 Figure 6. Group Policy used to map network drives.
Figure 6. Group Policy used to map network drives.

 Figure 7. Group Policy used to disable SQL services at startup.
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.
Figure 8 Group Policy used to copy LockBit from the SYSVOL shared location to the desktop.

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

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

```
powershell.exe. exe -Command "Get-ADComputer -filter * -Searchbase 'DC=symcdemos,DC=local' | foreach{
Invoke-GPUpdate -computer $_.name -force -RandomDelayInMinutes 0}"
```

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.

```
gpupdate.exe /target:computer /force gpupdate.exe /target:user /force
```

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:

```
C:\Windows\system32\DllHost.exe /Processid:{E2B3C97F-6AE1-41AC-817A-F6F92166D7DD}
```

11. Impact

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

```
"C:\Windows\System32\cmd.exe" /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete &
bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no
```

- Deletes Windows event logs using:

```
wevtutil cl security wevtutil cl system wevtutil cl application
```

12. Encrypts files and appends the .lockbit file extension.

13. MSHTA.exe

- Creates the file lockbit.hta and executes it to display a ransom note.


Figure 11. LockBit ransom note.

Figure 11. LockBit ransom note.

LockBit has been one of, if not the most active of RaaS gangs in 2022. The drop in Conti activity in May helped LockBit reach the top spot, with some reports stating that the threat was behind as much as 40% of ransomware attacks.

LockBit's success is also due to its developers and affiliates continued evolution of features and tactics, which include the malware's fast encryption speed, ability to target both Windows and Linux machines, its brash recruitment drives, and high-profile targets. In addition, as previously mentioned, the launch of a rewards program for vulnerabilities in LockBit's code and for suggestions on improving the RaaS operation will no-doubt help the ransomware remain a serious threat to organizations.

Indicators of Compromise (IOCs)

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

- 5181d2e71e8e73a82712a483a80aaea94e1efa785f2b8b8ee9641544c0b652f0 - lockbit_6341d6e5844c8289.exe

- llll.exe – copy of LockBit ransomware
- hxxps://temp[.]sh/AErDa/LockBit_6341D6E5844C8289[.]exe - Payload URL

MITRE Techniques


Figure 12. MITRE techniques used by the LockBit ransomware.
Figure 12. MITRE techniques used by the LockBit ransomware.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Symantec Endpoint Protection (SEP) protects against ransomware attacks using multiple static and dynamic technologies.

AV Protection

- Ransom.LockBit
- Ransom.LockBit!g2
- Scr.Malscript!gen1

Behavior Protection

- SONAR.RansomLckbit!g3
- SONAR.RansomNokibi!g1
- SONAR.RansomLckbit!g1

Intrusion Prevention System (IPS) Protection

- [SID: 33705] Attack: Lockbit Ransomware Binary Copy GPO Config
- [SID: 33706] Attack: Lockbit Ransomware Services Disable GPO Config
- [SID: 33707] Attack: Lockbit Ransomware Enable Share GPO Config
- [SID: 33708] Attack: Lockbit Ransomware Security Services Taskkill GPO

Symantec Data Center Security (DCS) hardening policies for Windows Servers and Domain Controllers prevent LockBit ransomware installation. The default DCS lockdown prevents lateral movement of LockBit ransomware on the network and protects servers from LockBit execution attempts to tamper with Group Policies and critical system resources.


LockBit: Ransomware Puts Servers in the Crosshairs


Vishal Kamble

Vishal Kamble

Principal Threat Analysis Engineer


Lahu Khatal

Lahu Khatal

Senior Threat Analysis Engineer
