JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA23-165A

June 14, 2023

MS-ISAC® Multi-State Information Sharing & Analysis Center®

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Federal Office for Information Security

certnz

National Cyber Security Centre
PART OF THE GCSB

UNDERSTANDING RANSOMWARE THREAT ACTORS:

LockBit

Publication: June 14, 2023

Cybersecurity and Infrastructure Security Agency

FBI | MS-ISAC | ACSC | NCSC-UK | CCCS | ANSSI | BSI | CERT NZ | NCSC-NZ

SUMMARY

In 2022, LockBit was the most deployed ransomware variant across the world and continues to be prolific in 2023. Since January 2020, affiliates using LockBit have attacked organizations of varying sizes across an array of critical infrastructure sectors, including financial services, food and agriculture, education, energy, government and emergency services, healthcare, manufacturing, and transportation. LockBit ransomware operation functions as a Ransomware-as-a-Service (RaaS) model where affiliates are recruited to conduct ransomware attacks using LockBit ransomware tools and infrastructure. Due to the large number of unconnected affiliates in the operation, LockBit ransomware attacks vary significantly in observed tactics, techniques, and procedures (TTPs). This variance in observed ransomware TTPs presents a notable challenge for organizations working to maintain network security and protect against a ransomware threat.

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the following international partners, hereafter referred to as "authoring organizations," are releasing this Cybersecurity Advisory (CSA) detailing observed activity in LockBit ransomware incidents and providing recommended mitigations to enable network defenders to proactively improve their organization's defenses against this ransomware operation.

- Australian Cyber Security Centre (ACSC)
- Canadian Centre for Cyber Security (CCCS)
- United Kingdom's National Cyber Security Centre (NCSC-UK)
- National Cybersecurity Agency of France (ANSSI)
- Germany's Federal Office for Information Security (BSI)
- New Zealand's Computer Emergency Response Team (CERT NZ) and National Cyber Security Centre (NCSC NZ)

The authoring organizations encourage the implementation of the recommendations found in this CSA to reduce the likelihood and impact of future ransomware incidents.

Table of Contents

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK for Enterprise framework, version 13.1. See the MITRE ATT&CK Tactics and Techniques section for tables of LockBit's activity mapped to MITRE ATT&CK® tactics and techniques.

Introduction

The LockBit RaaS and its affiliates have negatively impacted organizations, both large and small, across the world. In 2022, LockBit was the most active global ransomware group and RaaS provider in terms of the number of victims claimed on their data leak site. [1] A RaaS cybercrime group maintains the functionality of a particular ransomware variant, sells access to that ransomware variant to individuals or groups of operators (often referred to as "affiliates"), and supports affiliates' deployment of their ransomware in exchange for upfront payment, subscription fees, a cut of profits, or a combination of upfront payment, subscription fees, and a cut of profits. Some of the methods LockBit has used to successfully attract affiliates include, but are not limited to:

- Assuring payment by allowing affiliates to receive ransom payments before sending a cut to the core group; this practice stands in stark contrast to other RaaS groups who pay themselves first and then disburse the affiliates' cut.
- Disparaging other RaaS groups in online forums.
- Engaging in publicity-generating activities stunts, such as paying people to get LockBit tattoos and putting a $1 million bounty on information related to the real-world identity of LockBit's lead who goes by the persona "LockBitSupp."
- Developing and maintaining a simplified, point-and-click interface for its ransomware, making it accessible to those with a lower degree of technical skill. [2, 3]

LockBit has been successful through innovation and ongoing development of the group's administrative panel and the RaaS supporting functions. In parallel, affiliates that work with LockBit and other notable variants are constantly revising the TTPs used for deploying and executing ransomware.

Table 1 shows LockBit RaaS's innovation and development.

Table 1: Evolution of LockBit RaaS

Date	Event
September 2019	First observed activity of **ABCD ransomware**, the predecessor to LockBit. [4]
January 2020	**LockBit-named ransomware** first seen on Russian-language based cybercrime forums.

Date	Event
June 2021	Appearance of **LockBit version 2 (LockBit 2.0)**, also known as LockBit Red including StealBit, a built-in information-stealing tool.
October 2021	Introduction of **LockBit Linux-ESXi Locker version 1.0** expanding capabilities to target systems to Linux and VMware ESXi. [5]
March 2022	Emergence of **LockBit 3.0**, also known as LockBit Black, that shares similarities with BlackMatter and Alphv (also known as BlackCat) ransomware.
September 2022	Non-LockBit affiliates able to use **LockBit 3.0** after its builder was leaked. [2, 6]
January 2023	Arrival of **LockBit Green** incorporating source code from Conti ransomware. [7]
April 2023	LockBit ransomware encryptors targeting **macOS** seen on VirusTotal [8, 9]

LockBit 2.0, LockBit 3.0, LockBit Green, and LockBit Linux-ESXi Locker are still available for affiliates' use on LockBit's panel.

LockBit Statistics

Percentage of ransomware incidents attributed to LockBit:

- Australia: From April 1, 2022, to March 31, 2023, LockBit made up 18% of total reported Australian ransomware incidents. This figure includes all variants of LockBit ransomware, not solely LockBit 3.0.
- Canada: In 2022, LockBit was responsible for 22% of attributed ransomware incidents in Canada.[10]
- New Zealand: In 2022, CERT NZ received 15 reports of LockBit ransomware, representing 23% of 2022 ransomware reports.
- United States: In 2022, 16% of the State, Local, Tribal, and Tribunal (SLTT) government ransomware incidents reported to the MS-ISAC were identified as LockBit attacks. This included ransomware incidents impacting municipal governments, county governments, public higher education and K-12 schools, and emergency services (e.g., law enforcement).

Number of LockBit ransomware attacks in the U.S. since 2020:

- About 1,700 attacks according to the FBI.

Total of U.S. ransoms paid to LockBit:

- Approximately $91M since LockBit activity was first observed in the U.S. on January 5, 2020.

Earliest observed LockBit activity:

- Australia: The earliest documented occurrence of LockBit 3.0 was in early August 2022.
- Canada: The first recorded instance of LockBit activity in Canada was in March 2020.
- New Zealand: The first recorded incident involving LockBit ransomware was in March 2021.
- United States: LockBit activity was first observed on January 5, 2020.

Most recently observed LockBit activity:

- Australia: April 21, 2023.
- New Zealand: February 2023.
- United States: As recently as May 25, 2023.

Operational activity related to LockBit in France

Since the first case in July 2020 to present, ANSSI has handled 80 alerts linked to the LockBit ransomware, which accounts for 11% of all ransomware cases handled by ANSSI in that period. In about 13% of those cases, ANSSI was not able to confirm nor deny the breach of its constituents' networks – as the alerts were related to the threat actor's online claims. So far, 69 confirmed incidents have been handled by ANSSI. Table 2 shows the LockBit activity observed by ANSSI versus overall ransomware activity tracked by the Computer Emergency Response Team-France (CERT-FR).

Table 2: ANSSI-Observed LockBit vs. Overall Ransomware Activity

Year	Number of Incidents	Percentage of CERT-FR's Ransomware-Related Activity
2020 (from July)	4	2%
2021	20	10%
2022	30	27%
2023	15	27%
Total (2020-2023)	**69**	**11%**

Table 3 shows the number of instances different LockBit strains were observed by ANSSI from July 2020 to present.

Table 3: ANSSI-Observed LockBit Strain and Number of Instances

Name of the Strain*	Number of Instances
LockBit 2.0 (LockBit Red)	26
LockBit 3.0 (LockBit Black)	23
LockBit	21
LockBit Green	1
LockBit (pre-encryption)	1
Total	**72****

** Name either obtained from ANSSI's or the victim's investigations*

*** Includes incidents with multiple strains*

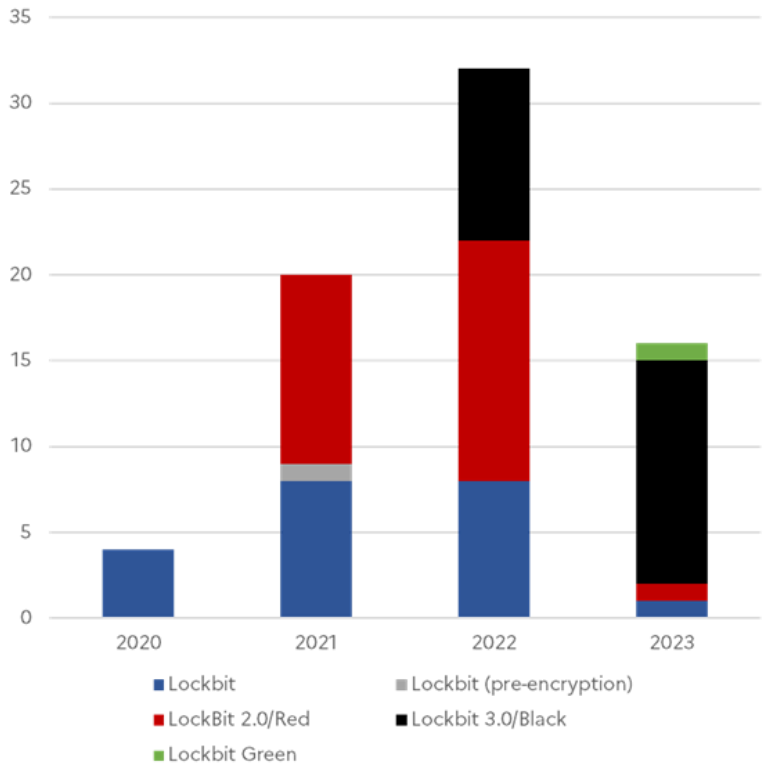


Figure 1: ANSSI-Observed LockBit Strains by Year

From the incidents handled, ANSSI can infer that LockBit 3.0 widely took over from LockBit 2.0 and the original LockBit strain from 2022. In two cases, victims were infected with as many as three different strains of LockBit (LockBit 2.0/Red, LockBit 3.0/Black, and LockBit Green).

Leak Sites

The authoring agencies observe data leak sites, where attackers publish the names and captured data of victims if they do not pay ransom or hush money. Additionally, these sites can be used to record alleged victims who have been threatened with a data leak. The term 'victims' may include those who have been attacked, or those who have been threatened or blackmailed (with the attack having taken place).

The leak sites only show the portion of LockBit affiliates' victims subjected to secondary extortion. Since 2021, LockBit affiliates have employed double extortion by first encrypting victim data and then exfiltrating that data while threatening to post that stolen data on leak sites. Because LockBit only reveals the names and leaked data of victims who refuse to pay the primary ransom to decrypt their data, some LockBit victims may never be named or have their exfiltrated data posted on leak sites. As a result, the leak sites reveal a portion of LockBit affiliates' total victims. For these reasons, the leak sites are not a reliable indicator of when LockBit ransomware attacks occurred. The date of data publication on the leak sites may be months after LockBit affiliates actually executed ransomware attacks.

Up to the Q1 2023, a total of 1,653 alleged victims were observed on LockBit leak sites. With the introduction of LockBit 2.0 and LockBit 3.0, the leak sites have changed, with some sources choosing to differentiate leak sites by LockBit versions and others ignoring any differentiation. Over time, and through different evolutions of LockBit, the address and layout of LockBit leak sites have changed and are aggregated under the common denominator of the LockBit name. The introduction of LockBit 2.0 at the end of the Q2 2021 had an immediate impact on the cybercriminal market due to multiple RaaS operations shutting down in May and June 2021 (e.g., DarkSide and Avaddon). LockBit competed with other RaaS operations, like Hive RaaS, to fill the gap in the cybercriminal market leading to an influx of LockBit affiliates. Figure 2 shows the alleged number of victims worldwide on LockBit leak sites starting in Q3 2020.

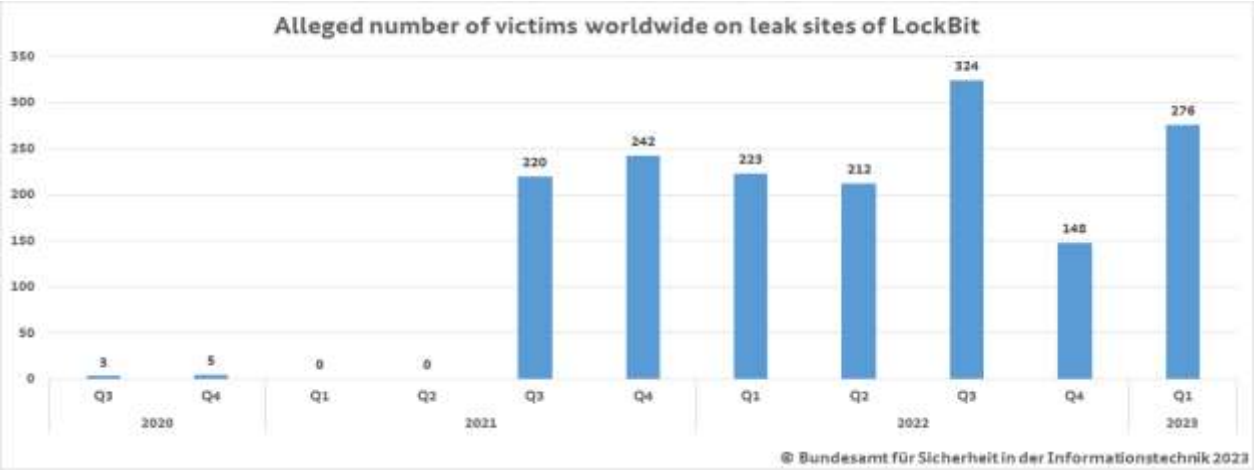


Figure 2: Alleged Number of Victims Worldwide on LockBit Leak Sites

Tools

During their intrusions, LockBit affiliates have been observed using various freeware and open-source tools that are intended for legal use. When repurposed by LockBit, these tools are then used for a range of malicious cyber activity, 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.

Table 4 shows a list of legitimate freeware and open-source tools LockBit affiliates have repurposed for ransomware operations. The legitimate freeware and open-source tools mentioned in this product are all publicly available and legal. The use of these tools by a threat actor should not be attributed to the freeware and open-source tools, absent specific articulable facts tending to show they are used at the direction or under the control of a threat actor.

Table 4: Freeware and Open-Source Tools Used by LockBit Affiliates

Tool	Intended Use	Repurposed Use by LockBit Affiliates	MITRE ATT&CK ID
7-zip	Compresses files into an archive.	Compresses data to avoid detection before exfiltration.	T1562 Impair Defenses
AdFind	Searches Active Directory (AD) and gathers information.	Gathers AD information used to exploit a victim's network, escalate privileges, and facilitate lateral movement.	S0552 AdFind
Advanced Internet Protocol (IP) Scanner	Performs network scans and shows network devices.	Maps a victim's network to identify potential access vectors.	T1046 Network Service Discovery
Advanced Port Scanner	Performs network scans.	Finds open Transmission Control Protocol (TCP) and User Data Protocol (UDP) ports for exploitation.	T1046 Network Service Discovery
AdvancedRun	Allows software to be run with different settings.	Enables escalation of privileges by changing settings before running software.	TA0004 Privilege Escalation

Tool	Intended Use	Repurposed Use by LockBit Affiliates	MITRE ATT&CK ID
AnyDesk	Enables remote connections to network devices.	Enables remote control of victim's network devices.	T1219 Remote Access Software
Atera Remote Monitoring & Management (RMM)	Enables remote connections to network devices.	Enables remote control of victim's network devices.	T1219 Remote Access Software
Backstab	Terminates antimalware-protected processes.	Terminates endpoint detection and response (EDR)-protected processes.	T1562.001 Impair Defenses: Disable or Modify Tools
Bat Armor	Generates `.bat` files using PowerShell scripts.	Bypasses PowerShell execution policy.	T1562.001 Impair Defenses: Disable or Modify Tools
Bloodhound	Performs reconnaissance of AD for attack path management.	Enables identification of AD relationships that can be exploited to gain access onto a victim's network.	T1482 Domain Trust Discovery
Chocolatey	Handles command-line package management on Microsoft Windows.	Facilitates installation of LockBit affiliate actors' tools.	T1072 Software Deployment Tools
Defender Control	Disables Microsoft Defender.	Enables LockBit affiliate actors to bypass Microsoft Defender.	T1562.001 Impair Defenses: Disable or Modify Tools
ExtPassword	Recovers passwords from Windows systems.	Obtains credentials for network access and exploitation.	T1003 Operating System (OS) Credential Dumping
FileZilla	Performs cross-platform File Transfer Protocol (FTP) to a site, server, or host.	Enables data exfiltration over FTP to the LockBit affiliate actors' site, server, or host.	T1071.002 Application Layer Protocol: File Transfer Protocols
FreeFileSync	Facilitates cloud-based file synchronization.	Facilitates cloud-based file synchronization for data exfiltration.	T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage

Tool	Intended Use	Repurposed Use by LockBit Affiliates	MITRE ATT&CK ID
GMER	Removes rootkits.	Terminates and removes EDR software.	T1562.001 Impair Defenses: Disable or Modify Tools
Impacket	Collection of Python classes for working with network protocols.	Enables lateral movement on a victim's network.	S0357 Impacket
LaZagne	Recovers system passwords across multiple platforms.	Collect credentials for accessing a victim's systems and network.	S0349 LaZagne
Ligolo	Establishes SOCKS5 or TCP tunnels from a reverse connection for pen testing.	Enables connections to systems within the victim's network via reverse tunneling.	T1095 Non-Application Layer Protocol
LostMyPassword	Recovers passwords from Windows systems.	Obtains credentials for network access and exploitation.	T1003 OS Credential Dumping
MEGA Ltd MegaSync	Facilitates cloud-based file synchronization.	Facilitates cloud-based file synchronization for data exfiltration.	T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage
Microsoft Sysinternals ProcDump	Monitors applications for central processing unit (CPU) spikes and generates crash dumps during a spike.	Obtains credentials by dumping the contents of Local Security Authority Subsystem Service (LSASS).	T1003.001 OS Credential Dumping: LSASS Memory
Microsoft Sysinternals PsExec	Executes a command-line process on a remote machine.	Enables LockBit affiliate actors to control victim's systems.	S0029 PsExec
Mimikatz	Extracts credentials from a system.	Extracts credentials from a system for gaining network access and exploiting systems.	S0002 Mimikatz

Tool	Intended Use	Repurposed Use by LockBit Affiliates	MITRE ATT&CK ID
Ngrok	Enables remote access to a local web server by tunnelling over the internet.	Enables victim network protections to be bypassed by tunnelling to a system over the internet.	S0508 Ngrok
PasswordFox	Recovers passwords from Firefox Browser.	Obtains credentials for network access and exploitation.	T1555.003 Credentials from Web Browsers
PCHunter	Enables advanced task management including system processes and kernels.	Terminates and circumvents EDR processes and services.	T1562.001 Impair Defenses: Disable or Modify Tools
PowerTool	Removes rootkits, as well as detecting, analyzing, and fixing kernel structure modifications.	Terminates and removes EDR software.	T1562.001 Impair Defenses: Disable or Modify Tools
Process Hacker	Removes rootkits.	Terminates and removes EDR software.	T1562.001 Impair Defenses: Disable or Modify Tools
PuTTY Link (Plink)	Automates Secure Shell (SSH) actions on Windows.	Enables LockBit affiliate actors to avoid detection.	T1572 Protocol Tunneling
Rclone	Manages cloud storage files using a command-line program.	Facilitates data exfiltration over cloud storage.	S1040 Rclone
Seatbelt	Performs numerous security-oriented checks.	Performs numerous security-oriented checks to enumerate system information.	T1082 System Information Discovery
ScreenConnect (also known as ConnectWise)	Enables remote connections to network devices for management.	Enables LockBit affiliate actors to remotely connect to a victim's systems.	T1219 Remote Access Software

Tool	Intended Use	Repurposed Use by LockBit Affiliates	MITRE ATT&CK ID
SoftPerfect Network Scanner	Performs network scans for systems management.	Enables LockBit affiliate actors to obtain information about a victim's systems and network.	T1046 Network Service Discovery
Splashtop	Enables remote connections to network devices for management.	Enables LockBit affiliate actors to remotely connect to systems over Remote Desktop Protocol (RDP).	T1021.001 Remote Services: Remote Desktop Protocol
TDSSKiller	Removes rootkits.	Terminates and removes EDR software.	T1562.001 Impair Defenses: Disable or Modify Tools
TeamViewer	Enables remote connections to network devices for management.	Enables LockBit affiliate actors to remotely connect to a victim's systems.	T1219 Remote Access Software
ThunderShell	Facilitates remote access via Hypertext Transfer Protocol (HTTP) requests.	Enables LockBit affiliate actors to remotely access systems while encrypting network traffic.	T1071.001 Application Layer Protocol: Web Protocols
WinSCP	Facilitates file transfer using SSH File Transfer Protocol for Microsoft Windows.	Enables data exfiltration via the SSH File Transfer Protocol.	T1048 Exfiltration Over Alternative Protocol

Common Vulnerabilities and Exposures (CVEs) Exploited

Based on secondary sources, it was noted that affiliates exploit older vulnerabilities like CVE-2021-22986, F5 iControl REST unauthenticated Remote Code Execution Vulnerability, as well as newer vulnerabilities such as:

- CVE-2023-0669: Fortra GoAnyhwere Managed File Transfer (MFT) Remote Code Execution Vulnerability
- CVE-2023-27350: PaperCut MF/NG Improper Access Control Vulnerability

LockBit affiliates have been documented exploiting numerous CVEs, including:

- CVE-2021-44228: Apache Log4j2 Remote Code Execution Vulnerability,
- CVE-2021-22986: F5 BIG-IP and BIG-IQ Centralized Management iControl REST Remote Code Execution Vulnerability,
- CVE-2020-1472: NetLogon Privilege Escalation Vulnerability,
- CVE-2019-0708: Microsoft Remote Desktop Services Remote Code Execution Vulnerability, and
- CVE-2018-13379: Fortinet FortiOS Secure Sockets Layer (SSL) Virtual Private Network (VPN) Path Traversal Vulnerability.

For further information on these CVEs , see CISA's Known Exploited Vulnerabilities (KEV) Catalog.

Post Detonation TTPs

When LockBit affiliates target an organization responsible for managing other organizations' networks, CERT NZ has observed LockBit affiliates attempt secondary ransomware extortion after detonation of the LockBit variant on the primary target. Once the primary target is hit, LockBit affiliates then attempt to extort the companies that are customers of the primary target. This extortion is in the form of secondary ransomware that locks down services those customers consume. Additionally, the primary target's customers may be extorted by LockBit affiliates threatening to release those customers' sensitive information.

MITRE ATT&CK TACTICS AND TECHNIQUES

Tables 5-16 show the LockBit affiliate tactics and techniques referenced in this advisory.

Table 5: LockBit Affiliates' ATT&CK Techniques for Enterprise – Initial Access

Technique Title	ID	Use
Drive-by Compromise	T1189	LockBit affiliates gain access to a system through a user visiting a website over the normal course of browsing.
Exploit Public-Facing Application	T1190	LockBit affiliates may exploit vulnerabilities (e.g., Log4Shell) in internet-facing systems to gain access to victims' systems.
External Remote Services	T1133	LockBit affiliates exploit RDP to gain access to victims' networks.
Phishing	T1566	LockBit affiliates use phishing and spearphishing to gain access to victims' networks.

Technique Title	ID	Use
Valid Accounts	T1078	LockBit affiliates obtain and abuse credentials of existing accounts as a means of gaining initial access.

Table 6: LockBit Affiliates' ATT&CK Techniques for Enterprise – Execution

Technique Title	ID	Use
Execution	TA0002	LockBit 3.0 launches commands during its execution.
Command and Scripting Interpreter: Windows Command Shell	T1059.003	LockBit affiliates use batch scripts to execute malicious commands.
Software Deployment Tools	T1072	LockBit affiliates may use Chocolatey, a command-line package manager for Windows.
System Services: Service Execution	T1569.002	LockBit 3.0 uses PsExec to execute commands or payloads.

Table 7: LockBit Affiliates' ATT&CK Techniques for Enterprise – Persistence

Technique Title	ID	Use
Boot or Logon Autostart Execution	T1547	LockBit affiliates enables automatic logon for persistence.
Valid Accounts	T1078	LockBit affiliates may use a compromised user account to maintain persistence on the target network.

Table 8: LockBit Affiliates' ATT&CK Techniques for Enterprise – Privilege Escalation

Technique Title	ID	Use
Privilege Escalation	TA0004	LockBit affiliates will attempt to escalate to the required privileges if current account privileges are insufficient.

Technique Title	ID	Use
Abuse Elevation Control Mechanism	T1548	LockBit affiliates may use ucmDccwCOM Method in UACMe, a GitHub collection of User Account Control (UAC) bypass techniques.
Boot or Logon Autostart Execution	T1547	LockBit affiliates enable automatic logon for privilege escalation.
Domain Policy Modification: Group Policy Modification	T1484.001	LockBit affiliates may create Group Policy for lateral movement and can force group policy updates.
Valid Accounts	T1078	LockBit affiliates may use a compromised user account to escalate privileges on a victim's network.

Table 9 LockBit Affiliates' ATT&CK Techniques for Enterprise – Defense Evasion

Technique Title	ID	Use
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.
Impair Defenses: Disable or Modify Tools	T1562.001	LockBit 3.0 affiliates use Backstab, Defender Control, GMER, PCHunter, PowerTool, Process Hacker or TDSSKiller to disable EDR processes and services. LockBit 3.0 affiliates use Bat Armor to bypass the PowerShell execution Policy. LockBit affiliates may deploy a batch script, `123.bat`, to disable and uninstall antivirus software. Lockbit 3.0 may modify and/or disable security tools including EDR and antivirus to avoid possible detection of malware, tools, and activities.
Indicator Removal: Clear Windows Event Logs	T1070.001	LockBit executable clears the Windows Event Logs files.

Technique Title	ID	Use
Indicator Removal: File Deletion	T1070.004	LockBit 3.0 will delete itself from the disk.
Obfuscated Files or Information	T1027	LockBit 3.0 will send encrypted host and bot information to its command and control (C2) servers.
Obfuscated Files or Information: Software Packing	T1027.002	LockBit affiliates may perform software packing or virtual machine software protection to conceal their code. Blister Loader has been used for such purpose.

Table 10: LockBit Affiliates' ATT&CK Techniques for Enterprise – Credential Access

Technique Title	ID	Use
Brute Force	T1110	LockBit affiliates may leverage VPN or RDP brute force credentials as an initial access.
Credentials from Password Stores: Credentials from Web Browsers	T1555.003	LockBit 3.0 actors use PasswordFox to recover passwords from Firefox Browser.
OS Credential Dumping	T1003	LockBit 3.0 actors use ExtPassword or LostMyPassword to recover passwords from Windows systems.
OS Credential Dumping: LSASS Memory	T1003.001	LockBit affiliates may use Microsoft Sysinternals ProDump to dump the contents of `lsass.exe`. LockBit affiliates have used Mimikatz to dump credentials.

Table 11: LockBit Affiliates' ATT&CK Techniques for Enterprise – Discovery

Technique Title	ID	Use
Network Service Discovery	T1046	LockBit affiliates use SoftPerfect Network Scanner, Advanced IP Scanner, or Advanced Port Scanner to scan target networks. LockBit affiliates may use SoftPerfect Network Scanner, Advanced Port Scanner, and AdFind to enumerate connected machines in the network.
System Information Discovery	T1082	LockBit affiliates 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.

Table 12: LockBit Affiliates' ATT&CK Techniques for Enterprise – Lateral Movement

Technique Title	ID	Use
Lateral Movement	TA0008	LockBit affiliates will laterally move across networks and access domain controllers.
Remote Services: Remote Desktop Protocol	T1021.001	LockBit affiliates use Splashtop remote-desktop software to facilitate lateral movement.
Remote Services: Server Message Block (SMB)/Admin Windows Shares	T1021.002	LockBit affiliates may use Cobalt Strike and target SMB shares for lateral movement.

Table 13: LockBit Affiliates' ATT&CK Techniques for Enterprise – Collection

Technique Title	ID	Use
Archive Collected Data: Archive via Utility	T1560.001	LockBit affiliates may use 7-zip to compress and/or encrypt collected data prior to exfiltration.

Table 14: LockBit Affiliates' ATT&CK Techniques for Enterprise – Command and Control

Technique Title	ID	Use
Application Layer Protocol: File Transfer Protocols	T1071.002	LockBit affiliates may use FileZilla for C2.
Application Layer Protocol: Web Protocols	T1071.001	LockBit affiliates use ThunderShell as a remote access tool that communicates via HTTP requests.
Non-Application Layer Protocol	T1095	LockBit affiliates use Ligolo to establish SOCKS5 or TCP tunnels from a reverse connection.
Protocol Tunneling	T1572	LockBit affiliates use Plink to automate SSH actions on Windows.
Remote Access Software	T1219	LockBit 3.0 actors use AnyDesk, Atera RMM, ScreenConnect or TeamViewer for C2.

Table 15: LockBit Affiliates' ATT&CK Techniques for Enterprise – Exfiltration

Technique Title	ID	Use
Exfiltration	TA0010	LockBit affiliates use StealBit, a custom exfiltration tool first used with LockBit 2.0, to steal data from a target network.
Exfiltration Over Web Service	T1567	LockBit affiliates use publicly available file sharing services to exfiltrate a target's data.

Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002	LockBit affiliates use (1) Rclone, an open-source command line cloud storage manager or FreeFileSync to exfiltrate and(2) MEGA, a publicly available file sharing service for data exfiltration.

Table 16: LockBit Affiliates' ATT&CK Techniques for Enterprise – 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. LockBit affiliates can encrypt Windows and Linux devices, as well as VMware instances.
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.
Inhibit System Recovery	T1490	LockBit 3.0 deletes volume shadow copies residing on disk.
Service Stop	T1489	LockBit 3.0 terminates processes and services.

MITIGATIONS

The authoring organizations recommend implementing the mitigations listed below to improve their cybersecurity posture to better defend against LockBit'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 threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

The listed mitigations are ordered by MITRE ATT&CK tactic. Mitigations that apply to multiple MITRE ATT&CK tactics are listed under the tactic that occurs earliest in an incident's lifecycle. For example,

account use polices are mitigations for initial access, persistence, privilege escalation, and credential access but would be listed under initial access mitigations.

Initial Access

- **Consider implementing sandboxed browsers** to protect systems from malware originating from web browsing. Sandboxed browsers isolate the host machine from malicious code.
- **Require all accounts** with password logins (e.g., service account, admin accounts, and domain admin accounts) to comply with NIST standards for developing and managing password policies [CPG 2.L].
    - Enforce use of longer passwords consisting of at least 15 characters in length [CPG 2.B, 2.C].
    - Store passwords in a salted and hashed format using industry-recognized password hashing algorithms.
    - Prevent use of commonly used or known-compromised passwords [CPG 2.C].
    - Implement multiple failed login attempt account lockouts [CPG 2.G].
    - 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 [CPG 2.Q].
- **Implement filters at the email gateway** to filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious IP addresses at the firewall [CPG 2.M].
- **Install a web application firewall** and configure with appropriate rules to protect enterprise assets.
- **Segment networks** 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. Isolate web-facing applications to further minimize the spread of ransomware across a network [CPG 2.F].
- **Follow the least-privilege best practice** by requiring administrators to use administrative accounts for managing systems and use simple user accounts for non-administrative tasks [CPG 2.E].
- **Enforce the management of and audit user accounts with administrative privileges**. Configure access controls according to the principle of least privilege [CPG 2.E].
- **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.

- **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. Public-facing applications must be patched in a timely manner as vulnerabilities can often be exploited directly by the threat actor. By closely monitoring the threat landscape, threat actors often take advantage of vulnerabilities before systems are patched. Organizations should patch vulnerable software and hardware systems within 24 to 48 hours from when a vulnerability is disclosed. Prioritize patching known exploited vulnerabilities in internet-facing systems [CPG 1.E].
- **Restrict service accounts from remotely accessing other systems.** Configure group policy to `Deny log on locally`, `Deny log on through Terminal Services`, and `Deny access to this computer from the network for all service accounts` to limit the ability for compromised service accounts to be used for lateral movement.
- **Block direct internet access for administration interfaces** (e.g., application protocol interface (API)) and for remote access.
- **Require phishing-resistant multifactor authentication** (MFA) for all services to the extent possible, particularly for webmail, virtual private networks, and privileged accounts that access critical systems [CPG 2.H].
- **Consolidate, monitor, and defend internet gateways.**
- **Install, regularly update, and enable real-time detection for antivirus software** on all hosts.
- **Raise awareness for phishing threats in your organization.** Phishing is one of the primary infection vectors in ransomware campaigns, and all employees should receive practical training on the risks associated with the regular use of email. With the rise of sophisticated phishing methods, such as using stolen email communication or artificial intelligence (AI) systems such as ChatGPT, the distinction between legitimate and malicious emails becomes more complex. This particularly applies to employees from corporate divisions that have to deal with a high volume of external email communication (e.g., staff recruitment) [CPG 2.I, 2.J].
- **Consider adding an external email warning banner** for emails sent to or received from outside of your organization [CPG 2.M].
- **Review internet-facing services and disable any services that are no longer a business requirement** to be exposed or restrict access to only those users with an explicit requirement to access services, such as SSL, VPN, or RDP. If internet-facing services must be used, control access by only allowing access from an admin IP range [CPG 2.X].
- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts.
- **Regularly verify the security level of the Active Directory domain** by checking for misconfigurations.

Execution

- **Develop and regularly update comprehensive network diagram(s)** that describes systems and data flows within your organization's network(s) [CPG 2.P].
- **Control and restrict network connections** accordingly with a network flow matrix.
- **Enable enhanced PowerShell logging** [CPG 2.T, 2.U].
    - PowerShell logs contain valuable data, including historical OS, registry interaction, and possibility of a threat actor's PowerShell use.
    - Ensure PowerShell instances are configured to use the latest version, and have module, script block, and transcription logging enabled (enhanced logging).
    - The two logs that record PowerShell activity are the `PowerShell` Windows Event Log and the `PowerShell Operational` Log. It is recommended to turn on these two Windows Event Logs with a retention period of at least 180 days. These logs should be checked on a regular basis to confirm whether the log data has been deleted or logging has been turned off. Set the storage size permitted for both logs to as large as reasonably practical.
- **Configure the Windows Registry to require UAC approval for any PsExec operations** requiring administrator privileges to reduce the risk of lateral movement by PsExec.

Privilege Escalation

- **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 [CPG 2.N].
- **Enable Credential Guard** to protect your Windows system credentials. This is enabled by default on Windows 11 Enterprise 22H2 and Windows 11 Education 22H2. Credential Guard prevents credential dumping techniques of the Local Security Authority (LSA) secrets. Be aware that enabling this security control has some downsides. In particular, you can no longer use New Technology Local Area Network (LAN) Manager (NTLM) classic authentication single sign-on, Kerberos unconstrained delegation, as well as Data Encryption Standard (DES) encryption.
- **Implement Local Administrator Password Solution (LAPS)** where possible if your OS is older than Windows Server 2019 and Windows 10 as these versions do not have LAPS built in. **NOTE:** The authoring organizations recommend organizations upgrade to Windows Server 2019 and Windows 10 or greater.

Defense Evasion

- **Apply local security policies to control application execution** (e.g., Software Restriction Policies (SRP), AppLocker, Windows Defender Application Control (WDAC)) with a strict allowlist.
- **Establish an application allowlist** of approved software applications and binaries that are allowed to be executed on a system. This measure prevents unwanted software to be run.

Usually, application allowlist software can also be used to define blocklists so that the execution of certain programs can be blocked, for example `cmd.exe` or `PowerShell.exe` [CPG 2.Q].

Credential Access

- **Restrict NTLM uses** with security policies and firewalling.

Discovery

- **Disable unused ports**. Disable ports that are not being used for business purposes (e.g., RDP-TCP Port 3389). Close unused RDP ports.

Lateral Movement

- **Identify Active Directory control paths** and eliminate the most critical among them according to the business needs and assets.
- **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 1.E]. EDR tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.

Command and Control

- **Implement a tiering model** by creating trust zones dedicated to an organization's most sensitive assets.
- **VPN access should not be considered as a trusted network zone.** Organizations should instead consider moving to zero trust architectures.

Exfiltration

- **Block connections to known malicious systems** by using a Transport Layer Security (TLS) Proxy. Malware often uses TLS to communicate with the infrastructure of the threat actor. By using feeds for known malicious systems, the establishment of a connection to a C2 server can be prevented.
- **Use web filtering or a Cloud Access Security Broker (CASB)** to restrict or monitor access to public-file sharing services that may be used to exfiltrate data from a network.

Impact

- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (e.g., hard drive, storage device, the cloud) [CPG 2.R].

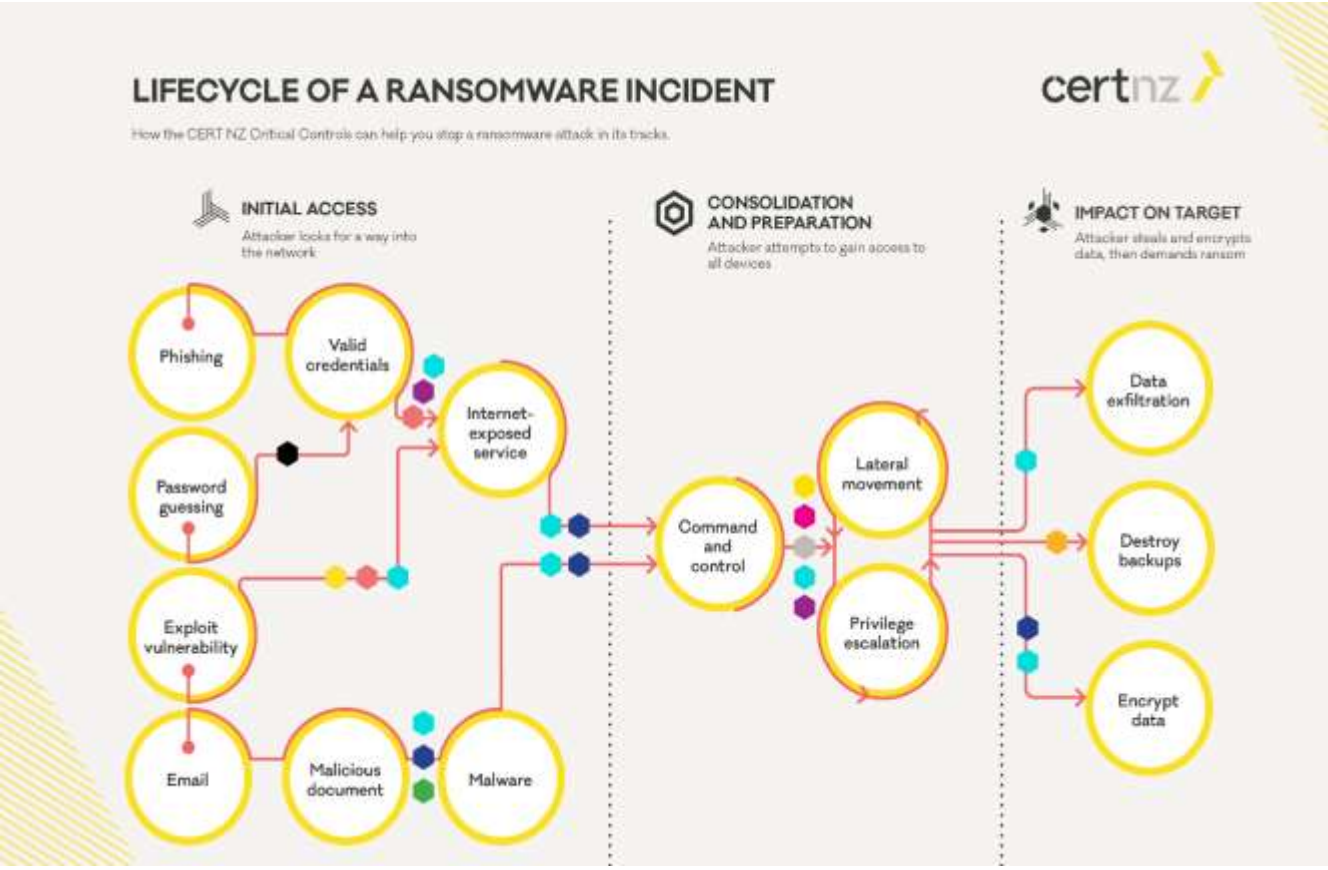
- **Maintain offline backups of data**, and regularly maintain backup and restoration (daily or weekly at the minimum). By instituting this practice, the organization ensures they will not be severely interrupted, and/or only have irretrievable data [CPG 2.R]. ACSC recommends organizations follow the 3-2-1 backup strategy in which organizations have three copies of data (one copy of production data and two backup copies) on two different media, such as disk and tape, with one copy kept off-site for disaster recovery.
- **Ensure all backup data is encrypted, immutable** (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure [CPG 2.K, 2.R].

Implement Mitigations for Defense-in-Depth

Implementing multiple mitigations within a defense-in-depth approach can help protect against ransomware, such as LockBit. CERT NZ explains How ransomware happens and how to stop it by applying mitigations, or critical controls, to provide a stronger defense to detect, prevent, and respond to ransomware before an organization's data is encrypted. By understanding the most common attack vectors, organizations can identify gaps in network defenses and implement the mitigations noted in this advisory to harden organizations against ransomware attacks. In Figure 3, a ransomware attack is broken into three phases:

- **Initial Access** where the cyber actor is looking for a way into a network.
- **Consolidation and Preparation** when the actor is attempting to gain access to all devices.
- **Impact on Target** where the actor is able to steal and encrypt data and then demand ransom.

Figure 3 shows the mitigations/critical controls, as various colored hexagons, working together to stop a ransomware attacker from accessing a network to steal and encrypt data. In the Initial Access phase, mitigations working together to deny an attacker network access include securing internet-exposed services, patching devices, implementing MFA, disabling macros, employing application allowlisting, and using logging and alerting. In the Consolidation and Preparation phase, mitigations working together to keep an attacker from accessing network devices are patching devices, using network segmentation, enforcing the principle of least privilege, implementing MFA, and using logging and alerting. Finally, in the Impact on Target phase, mitigations working together to deny or degrade an attacker's ability to steal and/or encrypt data includes using logging and alerting, using and maintaining backups, and employing application allowlisting.



Critical Controls Key

Internet-exposed services	Backups
Patching	Application allowlisting
MFA	Logging and alerting
Network segmentation	Disable macros
Principle of least privilege	Password manager

Figure 3: Stopping Ransomware Using Layered Mitigations

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, the authoring organizations 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 authoring organizations 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 Tables 5-16).

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 authoring organizations recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

RESOURCES

- ACSC:
  - See 2023-03: ACSC Ransomware Profile – LockBit 3.0 for additional information.
- CISA:
  - Stopransomware.gov is a whole-of-government approach that gives one central location for ransomware resources and alerts.
  - Information on no-cost cyber hygiene services is available at Cyber Hygiene Services and Ransomware Readiness Assessment.
- CISA, NSA, FBI, and MS-ISAC:
  - See the #StopRansomware Guide developed through the Joint Ransomware Task Force (JRTF) to provide a one-stop resource to help organizations reduce the risk of ransomware incidents through best practices to detect, prevent, respond, and recover, including step-by-step approaches to address potential attacks.
- FBI and CISA:
  - See Alert AA23-075A - #StopRansomware: LockBit 3.0 for information on IOCs and TTPs identified through FBI investigations as recently as March 2023.
- MS-ISAC:
  - See the Center for Internet Security (CIS) Critical Security Controls (CIS Controls) https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0for information on strengthening an organization's cybersecurity posture through implementing a prescriptive, prioritized, and simplified set of best.
  - See the CIS Community Defense Model 2.0 (CDM 2.0) for the effectiveness of the CIS Controls against the most prevalent types of attacks and how CDM 2.0 can be used to design, prioritize, implement, and improve an organization's cybersecurity program.
  - See Blueprint for Ransomware Defense for a clear, actionable framework for ransomware mitigation, response, and recovery built around the CIS Controls.
- NCSC-UK
  - See guidance on Mitigating malware and ransomware attacks for information on defending organizations against malware or ransomware attacks.

- BSI:
  - See BSI's Ransomware – Facts and Defense Strategies for a comprehensive collection of resources on ransomware prevention, detection, and reaction. Note: These resources are in German.
- CCCS:
  - See CCCS's Ransomware playbook (ITSM.00.099) for information on ransomware prevention and response.
  - See CCCS's Top 10 IT security actions based on analysis of cyber threat trends to help minimize intrusions or the impacts of a successful cyber intrusion.
- CERT NZ:
  - See CERT NZ's Security awareness building and Creating an effective security awareness program to assist organization's in providing adequate security awareness and training to personnel while creating a positive security culture.
  - Businesses can find information on developing an incident response plan, creating a contact list, and communicating ransomware incidents at CERT NZ's Creating an incident response plan.
- NCSC NZ:
  - For guidance on ransomware for public service agencies, see NCSC NZ's Ransomware: Your organization should be both protected and prepared.

REPORTING

The authoring organizations 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 authoring organizations urge you to promptly report ransomware incidents to your country's respective authorities.

- Australia: Australian organizations that have been impacted or require assistance in regard to a ransomware incident can contact ACSC via 1300 CYBER1 (1300 292 371), or by submitting a report to cyber.gov.au.
- Canada: Canadian victims of ransomware are encouraged to consider reporting cyber incidents to law enforcement (e.g., local police or the Canadian Anti-Fraud Centre) as well as to the Canadian Centre for Cyber Security online via My Cyber Portal.
- France:
  - Individuals and small organizations can seek assistance with Cybermalveillance – https://www.cybermalveillance.gouv.fr/.
  - Larger organizations, as well as public and regulated entities, can request assistance from CERT-FR via cert-fr@ssi.gouv.fr.

- Germany: German victims of ransomware are encouraged to consider reporting cyber incidents to law enforcement (e.g., local police or the Central Contact Point for Cybercrime as well as to the Federal Office for Information Security (BSI) via the Reporting and Information Portal.
- New Zealand: New Zealand organizations and businesses can report security incidents to the NCSC at incidents@ncsc.govt.nz or call 04 498 7654, or to CERT NZ through https://www.cert.govt/nz/it-specialists/report-an-incident/ or to ir@ops.cert.govt.nz.
- United States:
    - Report ransomware incidents to a local FBI Field Office or CISA's 24/7 Operations Center at Report@cisa.dhs.gov, cisa.gov/report, or (888) 282-0870. When available, please include the 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.
    - For SLTTs, email soc@msisac.org or call (866) 787-4722.
- United Kingdom: UK organizations should report any suspected compromises to NCSC.

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. The authoring organizations 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 authoring organizations.

REFERENCES

[1] LockBit, BlackCat, and Royal Dominate the Ransomware Scene

[2] Ransomware Diaries: Volume 1

[3] What is LockBit ransomware and how does it operate?

[4] Ransomware Spotlight: LockBit

[5] Analysis and Impact of LockBit Ransomware's First Linux and VMware ESXi Variant

[6] A first look at the builder for LockBit 3.0 Black

[7] LockBit ransomware gang releases LockBit Green version

[8] LockBit Ransomware Now Targeting Apple macOS Devices

[9] Apple's Macs Have Long Escaped Ransomware. That May be Changing

[10] Intelligence agency says ransomware group with Russian ties poses 'an enduring threat' to Canada