Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

2023-06: ACSC Ransomware Profile – Lockbit 3.0

15 June 2023

Context: *Lockbit 3.0 is the newest version of Lockbit ransomware first discovered in March 2022. It is used by cybercriminals to conduct ransomware attacks against multiple sectors and organisations worldwide, including Australia. Once gaining access to a victim's environment, cybercriminals use this ransomware for similar purposes as other variants such as encrypting their data, and extorting a ransom to return access to the sensitive files. LockBit 3.0 is offered as a Ransomware-as-a-Service (RaaS), enabling affiliates to utilise it as desired, provided a percentage of the illicitly gained profits are shared with the LockBit operators as commission. This profile provides information covering the LockBit 3.0 ransomware's background, threat activity, and mitigations advice.*

The Australian Cyber Security Centre (ACSC) is providing this information to enable organisations to undertake their own risk assessments and take appropriate actions to secure their systems and networks. The ACSC will only revise and update this document in the event of further significant information coming to light.

Key Points

- Lockbit 3.0 ransomware encrypts files on compromised computer systems and make them inoperable. Victims receive instructions to initiate ransom negotiation with the threat actors.
- Lockbit 3.0 ransomware performs a check to avoid executing on computer systems with installed languages common to Commonwealth of Independent States (CIS) countries.
- Lockbit 3.0 threat actors operate as a Ransomware-as-a-Service (RaaS). LockBit affiliates have compromised organisations worldwide, including Australia, where the ACSC is aware of numerous incidents since 2022.
- LockBit 3.0 threat actors conduct multifaceted extortions as they steal victim data, encrypt files, and threaten to publish the stolen data as a strategy for pressuring victims into paying the ransom.
- Lockbit 3.0 threat actors rely on stolen or compromised credentials to establish the initial access into the victim's network.

Background

LockBit threat actors first appeared on Russian-language based cybercrime forums in January 2020. Version 2.0 of the LockBit RaaS was released in June 2021 as "LockBit 2.0", known as Lockbit RED, and was allegedly shared with a built-in information-stealing tool called StealBit. In March 2022, LockBit was rebranded as "LockBit 3.0" also known as LockBit BLACK. The variant appears to reuse the source code from another ransomware BlackMatter. Recently, in January 2023, Lockbit ransomware threat actors have advertised another variant of Lockbit 3.0 as LockBit GREEN. According to public reporting, the LockBit GREEN variant source code has significant similarities with the Conti ransomware that was leaked on March 2022.

Threat activity

The ACSC is aware of an increase in domestic and global activities of LockBit 3.0 ransomware group in 2022 and they continued targeting organisations in 2023. Since 2022, the threat actors claimed to have compromised more than five hundred organisations worldwide across various sectors including healthcare, education and critical infrastructures. The Lockbit 3.0 BLACK variant is the most observed ransomware variant worldwide.

Tactics, Techniques and Procedures

Lockbit 3.0 ransomware threat actors use a range of techniques to gain initial access into the victim's network, such as:

- Brute-force attacks against user credentials to compromise internet-facing Remote Desktop Protocol (RDP) and Virtual Private Network (VPN) access
- Use of purchased or stolen credentials from initial access brokers
- Phishing attacks to obtain user credentials
- Exploitation of known vulnerabilities in software and security misconfigurations

After gaining access into a system, Lockbit 3.0 threat actors use Living-off-the-Land (LoL) techniques and additional tools for post-exploitation activities and lateral movement within the victim's network. For example, during the post-exploitation phase, threat actors use built-in PowerShell commands that are already available in the victim computer to execute malicious actions. In addition, the Lockbit 3.0 BLACK variant implements defence evasion techniques and anti-forensics features.

LockBit 3.0 ransomware is often delivered to the victim machines using *PsExec*, Windows Management Instrumentation (WMI), and RDP protocol. Additionally, Lockbit 3.0 threat actors leverage remote administration software such as AnyDesk, Splashtop, and Atera RMM to establish persistent access in the victim's network. These tools are often paired with proxy solutions such as SystemBC and ngrok. The Lockbit 3.0 ransomware performs checks to avoid executing on systems with installed language-pack for Commonwealth of Independent States (CIS) countries. This includes countries such as Azerbaijan, Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan and Ukraine.

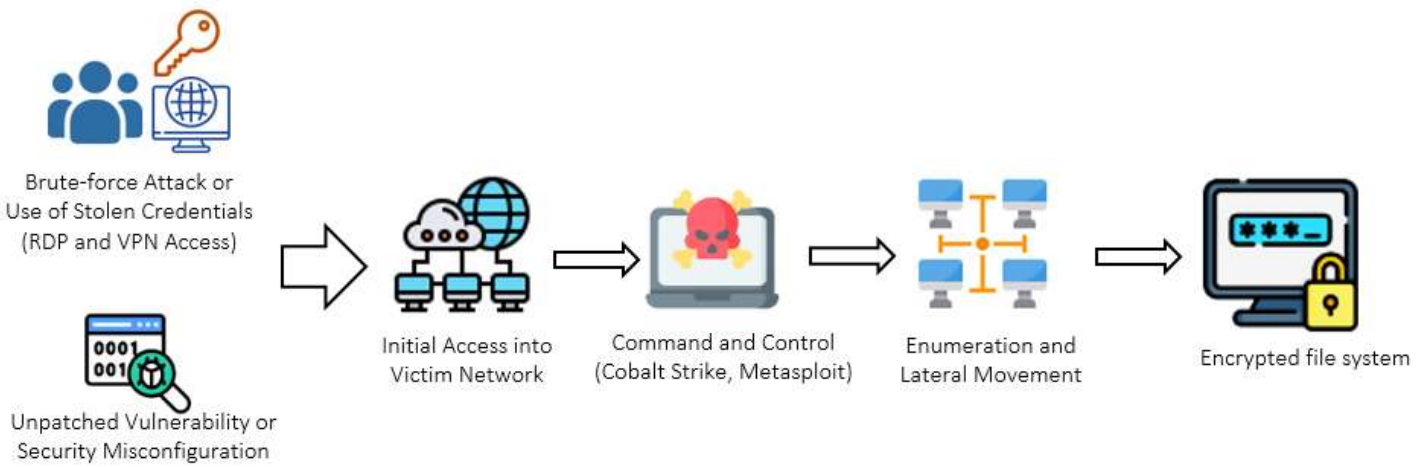

Figure-1: Lockbit 3.0 Ransomware Infection Chain

The LockBit 3.0 BLACK variant uses its own custom-built "*Ransomware Runner*" feature to distribute the ransomware payload across the victim network and also abuses the Group Policy Object (GPO) configurations. In some instances, threat actors use an additional "*screenlocker*" malware to hinder recovery operations by preventing interaction with the compromised system. The Lockbit 3.0 ransomware payload encrypts both local and shared files on the network. The files are encrypted using AES encryption algorithm and the AES Key is generated using BCryptGenRandom algorithm. Lastly, the encrypted files are appended with a random string that the Lockbit 3.0 ransomware builder generates for each payload.

Other Tactics, Techniques and Procedures (TTPs) associated with Lockbit 3.0 ransomware activity include but are not limited to:

- Using Mimikatz to harvest credentials after gaining access inside the victim network
- Using software tools such as GMER, PCHunter, and Process Hacker to disable end-device security software
- Abusing group policy to disable Windows Defender on the victim computer
- Using ICMLuaUtil COM interface under dllhost.exe to bypass user account control (UAC) for privilege escalation
- Using Netscan, Advanced Port Scanner to enumerate internal network
- Using the AdFind tool to locate the Domain Controller or Active Directory server
- Data exfiltration through RClone to publicly available cloud file-sharing services like MEGASync, and FileZilla
- Deleting all volume shadow copies to prevent data recovery using WMI through COM objects as opposed to LockBit 2.0's use of vssadmin.exe.

Post-Exploitation

During the post exploitation phase, Lockbit 3.0 threat actors usually steal sensitive data from victim systems. Once Lockbit 3.0 threat actors complete data exfiltration, they execute the ransomware payload to encrypt the file system and deliver a ransom note to their victims. The desktop background of the victim machine is changed to display a LockBit banner and instructions to follow for the decryption key.

The ransom note may be sent to printers on the victim network or a file named README.txt may also be created in the file system of the victim computer where the encrypted files are stored. The ransom note for LockBit 3.0 GREEN variant is identical to the one used by the LockBit BLACK variant; however, filename may appear as "!!!-Restore-My-Files-!!!.txt". Lockbit 3.0 threat actors conduct the ransom negotiation communication with their victims through web portals hosted on The Onion Router (TOR) network. The ransom note contains instructions to install the TOR browser, links for a chat, and the personal ID unique to the victim to communicate with the threat actors. For failed negotiations, the stolen data is posted to the LockBit 3.0 Dedicated Leak Site (DLS) on the dark web.

Assistance

The ACSC monitors a range of activity involving the Lockbit 3.0 ransomware variant. The ACSC is able to provide assistance and advice if required. Organisations that have been impacted or require assistance in regards to a Lockbit 3.0 ransomware incident can contact the ACSC via 1300 CYBER1 (1300 292 371), or by submitting a report to cyber.gov.au.

Mitigations

The ACSC recommends organisations implement the following mitigations:

- Enable and enforce multifactor authentication to prevent actors from accessing valid accounts with stolen credentials.
- Keep all operating systems, software, and firmware up to date. Patch vulnerable software and hardware systems within 24 to 48 hours from when the vulnerability is disclosed.
- Closely monitor user access to systems and strong password policies are essential.
- 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.
- Network traffic filtering using the stateful firewall rule will prevent unauthorised traffic from traversing network boundaries.
- Terminate VPN connections in a controlled network segment, only allowing authorised connections.
- Block access to Uniform Resource Identifier's (URI's) outside of the top 1 million websites or domains registered in the past month.
- Review domain controllers, servers, workstations, and active directories for new and/or unrecognized accounts.
- Configure the Windows Registry to require User Access Control (UAC) approval for any PsExec operations requiring administrator privileges to reduce the risk of lateral movement by PsExec.
- Implement hypervisor log monitoring and ensure that logs are processed on a separate system preferably with SIEM.
- Implement Application Control (at a minimum in monitor mode to capture unusual activity).
- Threat actors use file-less malware techniques which means governments, businesses and individuals should monitor for execution of any software that was not scheduled or run by a trusted program or a trusted user.
- Perform daily backups and keep them offline and encrypted. ACSC recommends businesses to follow the 3-2-1 backup strategy. It means organisations should have 3 copies of data (1 copy of production data and 2 backup copies) on two different media such as disk and tape with one copy off-site for disaster recovery.
- A robust backup and disaster recovery plan that is well exercised will give governments, businesses and individuals greater power when making a decision about recover of their files should they fall victim.
- Securely storing sensitive data and actively reducing what is available on a shared networks will reduce the impact of any extortion from ransomware groups should the files be stolen.

The below table maps the mitigations to the techniques leveraged by the actor and to the resources to implement these mitigations to protect your infrastructure.

Technique	Procedure	Mitigations
Initial Access [TA0001]		
Exploit Public-Facing Application [T1190]	Threat actors search for and opportunistically exploit vulnerabilities in internet facing applications and devices to gain access to victim networks.	Update Software [M1051] Establish processes to identify, assess and patch vulnerabilities affecting internet facing applications and devices within appropriate timeframes. This allows organisations to address security vulnerabilities before they are discovered and exploited by actors.

		See also: • Assessing Security Vulnerabilities and Applying Patches Exploit Protection [M1050] Security applications that look for behaviour can be used to mitigate some exploitation behaviour. Many of these protections depend on the architecture and target application binary for compatibility.
Valid Accounts [T1078]	Threat actors have obtained credentials for valid accounts and gain access victim networks.	Multi-factor authentication [M1032] Require multifactor authentication for all user accounts, particularly privileged accounts. This prevents actors from accessing valid accounts with stolen credentials. See also: • Multi-factor Authentication - Technique D3-MFA • Implementing Multi-Factor Authentication • Strategies to Mitigate Cyber Security Incidents – Mitigation Details User training [M1017] Educate users to avoid password reuse. This prevents actors from obtaining credentials through public breaches or by compromising non-corporate systems. See also: • Creating Strong Passphrases
External Remote Services [T1133]	Threat actors leverage external-facing remote services such as RDP/VPN to initially access and/or persist within a network	Disable or Remove Feature or Program [M1042] Remove or deny access to unnecessary and potentially vulnerable software. Disable the RDP service if it is unnecessary. Filter Network Traffic [M1037] Prevent network traffic from unknown or untrusted origins from accessing remote services

		on internal systems. This prevents actors from directly connecting to remote access services they have established for persistence. See also: • Inbound Traffic Filtering - Technique D3-ITF Network Segmentation [M1030] Segment networks and restrict traffic for remote access services where possible. This limits the ability of threat actors moving laterally within compromised networks. Utilising network segmentation as a form of defence in depth also prevents actors from connecting to external remote access services that they have established for persistence via compromised systems within victim networks. See also: • Broadcast Domain Isolation - Technique D3-BDI • Implementing Network Segmentation and Segregation
Execution [TA0002]		
System Services: Service Execution [T1569.002]	Threat actors have used the legitimate Windows Sysinternals tool PsExec [S0029] to execute malicious content.	Enable Attack Surface Reduction (ASR) on Microsoft Windows 10, and configure ASR to block process creations originating from PsExec commands. Note: PsExec is commonly used for legitimate system administration tasks. Organisations should consider how this mitigation could impact business practices before implementing. See also: • Hardening Microsoft Windows 10 version 21H1 Workstations
Command and Scripting Interpreter [T1059]	Threat actors abuse command and script interpreters such as windows command shell or PowerShell to execute commands, scripts, or binaries.	Privileged Account Management [M1026] When PowerShell is necessary, restrict PowerShell execution policy to administrators. Be aware that there are methods of bypassing the PowerShell

		execution policy, depending on environment configuration.
Windows Management Instrumentation [T1047]	Threat actors use Windows Management Instrumentation (WMI) to execute malicious commands and payloads.	Execution Prevention [M1038] Use application control configured to block execution of wmic.exe if it is not required for a given system or network to prevent potential misuse by adversaries. For example, in Windows 10 and Windows Server 2016 and above, Windows Defender Application Control (WDAC) policy rules may be applied to block the wmic.exe application and to prevent abuse. Privileged Account Management [M1026] Restrict administrative privileges to operating systems and applications based on user duties. This reduces actors' ability to elevate privilege, move laterally in networks, bypass security controls and access sensitive data. See also: • Restricting Administrative Privileges
Persistence [TA0003]		
Create Account [T1136]	Threat actors configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems.	Multi-factor authentication [M1032] Require multifactor authentication for all user accounts, particularly privileged accounts. This prevents actors from accessing valid accounts with stolen credentials. Operating System Configuration [M1028] Protect domain controllers by ensuring proper security configuration for critical servers.
Exfiltration [TA0010]		
Exfiltration Over Web Service [T1567]	Threat actors have exfiltrated sensitive data and threatened to publicly release it. Threat actors have exfiltrated data to legitimate and publicly	Encrypt Sensitive Information [M1041] Encrypt sensitive data at rest. This prevents actors from accessing sensitive data even if they can access the systems storing the data.

	available web services, and in some cases have used legitimate tools such as RClone.	Network Segmentation [M1030] Segment networks to separate sensitive data, and services that provide access to sensitive data, from corporate environments. This prevents adversaries from compromising vulnerable systems, such as desktop environments, and immediately accessing and exfiltrating sensitive data. See also: • Broadcast Domain Isolation - Technique D3-BDI • Implementing Network Segmentation and Segregation Restrict Web-Based Content [M1021] Restrict access to web-based storage services from corporate networks, except where required for legitimate business activity. This prevents actors from directly uploading sensitive data to blocked web-based storage services.
Lateral Movement [TA0008], Privilege Escalation [TA0004], Discovery [TA0007]		
Various	Threat actors have deployed post-exploitation tools such as PCHunter, PowerTool, GMER, NetScan and Process Hacker on victim networks. These techniques are commonly used to move laterally through victim networks, harvest credentials, elevate privileges, exfiltrate data and deploy additional tools.	Network Segmentation [M1030] Segment networks and restrict or monitor certain types of traffic that are commonly used for lateral movement or reconnaissance. This prevents actors from moving laterally in networks and accessing sensitive systems or data. See also: • Broadcast Domain Isolation - Technique D3-BDI • Implementing Network Segmentation and Segregation Update Software [M1051] Patch applications and operating systems and keep them up to date. This prevents actors from exploiting known vulnerabilities in applications and

		operating systems to elevate privilege, bypass security controls and move laterally in networks. Limit Software Installation [M1033] Restrict access to installing or executing unapproved software. This prevents actors from using unapproved software on corporate devices to perform some of their objectives. See also: • System Patching
Impact [TA0040]		
Data Encrypted for Impact [T1486]	Threat actors have used Lockbit 3.0 ransomware to encrypt valuable data, disrupt operations, and extort payment from victims.	Backup Data [M1053] Perform daily backups and keep them offline and encrypted. Test recovery and integrity procedures to make sure data and operations can be quickly and reliably restored. This will allow business operations to be recovered if data is exfiltrated and released. See also: • Data backup and restoration

Document Change Log

Version	Date	Change summary
2	15 June 2023	Updated information on the emergence of Lockbit RED and Lockbit BLACK variants
1	20 March 2023	First Published

Traffic Light Protocol

TLP Level	Restriction on access and use
TLP:RED	**Not for disclosure, restricted to participants only.** Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER+STRICT	**Limited disclosure, restricted to participants' organization.** Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization. Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.
TLP:AMBER	**Limited disclosure, restricted to participants' organization and its clients** Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only. Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.
TLP:GREEN	**Limited disclosure, restricted to the community.** Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.
TLP:CLEAR	**Disclosure is not limited.** Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Recipients may share this information without restriction. Information is subject to standard copyright rules.