Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

2021-006: ACSC Ransomware Profile - **Lockbit 2.0**

06 August 2021

Context: *LockBit (AKA LockBit 2.0, ABCD) is a ransomware variant first detected in September 2019, used by cybercriminals targeting multiple sectors and organisations around the world, including Australia.[1] LockBit 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 ransomware's background, recent initial access indicators, targeted sectors, 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

- The LockBit ransomware restricts access to corporate files and systems by encrypting them into a locked and unusable format. Victims receive instructions on how to engage with the offenders after encryption.
- LockBit affiliates have successfully deployed ransomware on corporate systems in a variety of countries and sectors, including Australia, where the ACSC is aware of numerous incidents since 2020.
- LockBit affiliates are known to implement the 'double extortion' technique by uploading stolen and sensitive victim information to their dark web site 'LockBit 2.0', and threatening to sell and/or release this information if their ransom demands are not met.

Background

Since January 2020, the 'LockBit' operators have appeared on Russian-language cybercrime forums. In June 2021, version two of the 'LockBit' RaaS was advertised as 'LockBit 2.0' and was allegedly bundled with a built in information stealing function known as 'StealBit'.

Dark web activity

LockBit affiliates are known to implement the 'double extortion' technique by uploading stolen and sensitive victim information to their dark web site 'LockBit 2.0', and threatening to sell and/or release this information if their ransom demands are not met. This is intended to coerce the victim into paying the ransom demand. The 'LockBit 2.0' site is hosted on The Onion Router (Tor) network, enabling greater anonymity to LockBit threat actors hosting illicitly obtained material.[2]

Initial access

The ACSC has recently observed LockBit threat actors actively exploiting existing vulnerabilities in the Fortinet FortiOS and FortiProxy products identified as CVE-2018-13379 in order to gain initial access to specific victim networks.

The LockBit RaaS operators have previously advertised partnership opportunities for threat actors that could provide credential based accesses to Remote Desktop Protocol (RDP) and Virtual Private Network (VPN) remote access

[1] Kaspersky: https://www.kaspersky.com/resource-center/threats/lockbit-ransomware
[2] Accenture: https://www.accenture.com/us-en/blogs/cyber-defense/extortion-entrepreneurs-how-cybercriminals-are-bullying-businesses

solutions.[3] Additional advertisements sought to recruit threat actors proficient in the use of threat emulation software Cobalt Strike and Metasploit. Threat emulation software is often used in penetration testing environments and by threat actors seeking to gain unauthorised access to or move laterally within target networks.

Threat activity

The ACSC is aware of numerous incidents involving LockBit and its successor 'LockBit 2.0' in Australia since 2020. The majority of victims known to the ACSC have been reported after July 2021, indicating a sharp and significant increase in domestic victims in comparison to other tracked ransomware variants.

The ACSC has observed LockBit affiliates successfully deploying ransomware on corporate systems in a variety of sectors including professional services, construction, manufacturing, retail and food. Additionally, threat actors involved in ransomware activity are opportunistic in nature and are capable of victimising organisations in any sector; as such, inclusion or exclusion from this list is not indicative of future LockBit behaviour.

Mitigations

Technique	Procedure	Mitigations
Initial Access [TA0001]		
Exploit Public-Facing Application [T1190]	Threat actors have exploited a vulnerability in an internet facing Fortinet device (CVE-2018-13379) to gain access to victim networks. Threat actors search for and opportunistically exploit vulnerabilities in internet facing devices to gain access to victim networks.	Check if your organisation operates Fortinet devices, and review this advisory to determine if they are vulnerable. If required, follow the instructions in the advisory to remediate the vulnerability. Establish processes to identify, assess and patch vulnerabilities affecting your organisation within appropriate timeframes.
Valid Accounts [T1078]	Actors have obtained credentials for valid accounts to gain access to victims' networks.	Require multifactor authentication (MFA) for all user accounts, particularly privileged accounts. Educate users to reduce password re-use.
Exfiltration [TA0010]		
Exfiltration Over Web Service [T1567]	Actors have exfiltrated sensitive data and threatened to publicly release it. Open source report suggests **LockBit 2.0** actors use publicly available web services to exfiltrate data.	Encrypt sensitive data at rest. Consider segmenting networks to separate sensitive data from corporate environments. Consider additional access controls such as MFA. Consider restricting access to web-based storage services from corporate networks.

[3] BleepingComputer: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-recruiting-insiders-to-breach-corporate-networks/

Lateral Movement [TA0008], Privilege Escalation [TA0004], Discovery [TA0007]		
Various	Actors have deployed common post-exploitation tools such as Cobalt Strike and Metasploit on victim networks. These are commonly used to move laterally through victim networks, harvest credentials, elevate privileges, exfiltrate data and deploy additional tools such as encryption binaries.	Segment networks and consider restricting or monitoring certain types of traffic such as SMB that are commonly used for lateral movement. Restrict administrative privileges to operating systems and applications based on user duties. Patch applications and operating systems and keep them up to date.
Impact [TA0040]		
Data Encrypted for Impact [T1486]	Actors have used the **LockBit 2.0** ransomware variant to encrypt valuable data, disrupt operations, and extort payment from victims.	Perform daily backups and test recovery and integrity procedures. Keep backups offline and encrypted. See [M1053 – Data Backup] and the ISM Chapter *Data backup and Restoration*.

Traffic light protocol

TLP Level	Restriction on access and use
RED	**Not for disclosure, restricted to participants only.** Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. 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.
AMBER	**Limited disclosure, restricted to participant's organisations.** Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organisations involved. Recipients may only share TLP:AMBER information with members of their own organisation, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
GREEN	**Limited disclosure, restricted to the community.** Sources may use TLP:GREEN when information is useful for the awareness of all participating organisations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organisations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not released outside of the community.
WHITE	**Disclosure is not limited.** Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.
Not classified	Any information received from the ACSC that is not classified in accordance with the Traffic light protocol must be treated as AMBER classified unless otherwise agreed in writing by the ACSC.