Threat Report

connectwise.com/resources/lockbit-profile

In the 2022 MSP Threat Report, the CRU identified the top 5 ransomware threats targeting MSPs in 2021 and provided a brief description of each. This page includes supplemental material with a more detailed breakdown of the TTPs and suggested mitigation techniques.

LockBit

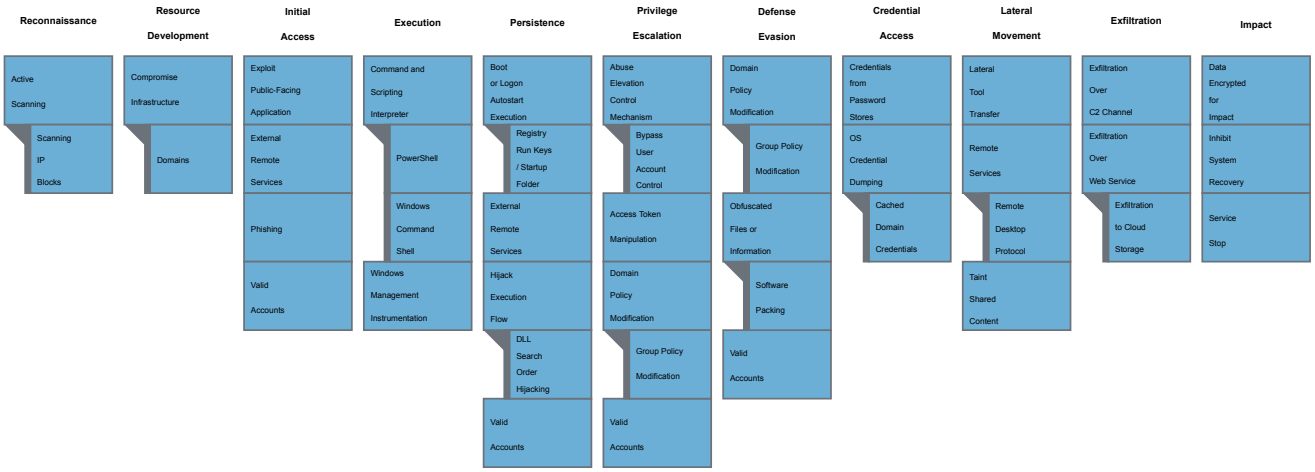
- Ransomware-as-a-service provider that first appeared in September 2019, originally dubbed "ABCD"
- Known for their fast encryption, they claim to have the fastest encryption of any ransomware
- Uses the double extortion method of encrypting files and threatening to leak stolen data

MITRE ATT&CK® mapping

about

LockBit/LuckyDay/LockBit 2.0/ABCD

2021 Top Threat Actors Targeting MSPs



LockBit TTPs and Mitigations

ATT&CK Tactic	ATT&CK Technique	Mitigations

Reconnaissance	T1595.001 – Active Scanning – Scanning IP Blocks: Adversaries may scan victim IP blocks to gather information that can be used during targeting. Public IP addresses may be allocated to organizations by block, or a range of sequential addresses.	M1056 – Pre-compromise: This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.
Resource Development	T1584.001 – Compromise Infrastructure – Domains: Adversaries may hijack domains and/or subdomains that can be used during targeting. Domain registration hijacking is the act of changing the registration of a domain name without the permission of the original registrant.	M1056 – Pre-compromise: This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.
Initial Access	T1190 – Exploit Public-Facing Application: Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability.	M1048 - Application Isolation and Sandboxing: Application isolation will limit what other processes and system features the exploited target can access.

M1050 - Exploit Protection:

Web Application Firewalls may be used to limit exposure of applications to prevent exploit traffic from reaching the application.

M1030 - Network Segmentation:

Segment externally facing servers and services from the rest of the network with a DMZ or on separate hosting infrastructure.

M1026 - Privileged Account Management:
Use least privilege for service accounts will limit what permissions the exploited process gets on the rest of the system.

M1051 – Update Software:
Update software regularly by employing patch management for externally exposed applications.

M1016 – Vulnerability Scanning:
Regularly scan externally facing systems for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure.

T1133 – External Remote Services:
Adversaries may leverage external-facing remote services to initially access and/or persist within a network.

M1042 - Disable or Remove Feature or Program:

Disable or block remotely available services that may be unnecessary.

M1035 - Limit Access to Resource Over Network:

Limit access to remote services through centrally managed concentrators such as VPNs and other managed remote access systems.

M1032 - Multi-factor Authentication:

Use strong two-factor or multi-factor authentication for remote service accounts to mitigate an adversary's ability to leverage stolen credentials, but be aware of Two-Factor Authentication Interception techniques for some two-factor authentication implementations.

M1030 - Network Segmentation:
Deny direct remote access to internal systems through the use of network proxies, gateways, and firewalls.

T1566 – Phishing:

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering.

M1049 - Antivirus/Antimalware:
Anti-virus can automatically quarantine suspicious files.

M1031 - Network Intrusion Prevention:

Network intrusion prevention systems and systems designed to scan and remove malicious email attachments or links can be used to block activity.

M1021 - Restrict Web-Based Content:

Determine if certain websites or attachment types (ex: .scr, .exe, .pif, .cpl, etc.) that can be used for phishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.

M1054 - Software Configuration:

Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross domain) to perform similar message filtering and validation.[3][4]

M1017 - User Training:

Users can be trained to identify social engineering techniques and phishing emails.

T1078 – Valid Accounts:

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.

M1013 - Application Developer Guidance:

Ensure that applications do not store sensitive data or credentials insecurely. (e.g. plaintext credentials in code, published credentials in repositories, or credentials in public cloud storage).

M1027 - Password Policies:

Applications and appliances that utilize default username and password should be changed immediately after the installation, and before deployment to a production environment. When possible, applications that use SSH keys should be updated periodically and properly secured.

M1026 - Privileged Account Management:

Audit domain and local accounts as well as their permission levels routinely to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account. These audits should also include if default accounts have been enabled, or if new local accounts are created that have not be authorized. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers.

M1017 - User Training:

Applications may send push notifications to verify a login as a form of multi-factor authentication (MFA). Train users to only accept valid push notifications and to report suspicious push notifications.

Execution	T1059.001 – Command and Scripting Interpreter – PowerShell: Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.	M1049 - Antivirus/Antimalware: Anti-virus can be used to automatically quarantine suspicious files.
M1045 - Code Signing: Set PowerShell execution policy to execute only signed scripts.		
M1042 - Disable or Remove Feature or Program: It may be possible to remove PowerShell from systems when not needed, but a review should be performed to assess the impact to an environment, since it could be in use for many legitimate purposes and administrative functions. Disable/restrict the WinRM Service to help prevent uses of PowerShell for remote execution.		
M1038 - Execution Prevention: Use application control where appropriate.		
M1026 - Privileged Account Management: 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.		
T1059.003 – Windows Command Shell: Adversaries may abuse the Windows command shell for execution. The Windows command shell (cmd) is the primary command prompt on Windows systems.	M1038 - Execution Prevention: Use application control where appropriate.	

T1047 – Windows Management Instrumentation: Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is an administration feature that provides a uniform environment to access Windows system components.	M1040 - Behavior Prevention on Endpoint: On Windows 10, enable Attack Surface Reduction (ASR) rules to block processes created by WMI commands from running. Note: many legitimate tools and applications utilize WMI for command execution.
M1038 - Execution Prevention: 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.	
M1026 - Privileged Account Management: Prevent credential overlap across systems of administrator and privileged accounts.	
M1018 - User Account Management: By default, only administrators are allowed to connect remotely using WMI. Restrict other users who are allowed to connect, or disallow all users to connect remotely to WMI.	

Persistence	T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder: Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in.	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
T1574.001 – Hijack Execution Flow: DLL Search Order Hijacking: Adversaries may execute their own malicious payloads by hijacking the search order used to load DLLs. Windows systems use a common method to look for required DLLs to load into a program. Hijacking DLL loads may be for the purpose of establishing persistence as well as elevating privileges and/or evading restrictions on file execution.	M1047 – Audit: Use auditing tools capable of detecting DLL search order hijacking opportunities on systems within an enterprise and correct them. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for DLL hijacking weaknesses. Use the program sxstrace.exe that is included with Windows along with manual inspection to check manifest files for side-by-side problems in software.	
M1038 - Execution Prevention: Adversaries may use new DLLs to execute this technique. Identify and block potentially malicious software executed through search order hijacking by using application control solutions capable of blocking DLLs loaded by legitimate software.		

M1044 - Restrict Library Loading:

Disallow loading of remote DLLs. This is included by default in Windows Server 2012+ and is available by patch for XP+ and Server 2003+.

Enable Safe DLL Search Mode to force search for system DLLs in directories with greater restrictions (e.g. %SYSTEMROOT%)to be used before local directory DLLs (e.g. a user's home directory)

The Safe DLL Search Mode can be enabled via Group Policy at Computer Configuration > [Policies] > Administrative Templates > MSS (Legacy): MSS: (SafeDllSearchMode) Enable Safe DLL search mode. The associated Windows Registry key for this is located at HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDLLSearchMode

Privilege Escalation	T1134 – Access Token Manipulation: Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token.	M1026 - Privileged Account Management: Limit permissions so that users and user groups cannot create tokens. This setting should be defined for the local system account only. GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Create a token object. Also define who can create a process level token to only the local and network service through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Replace a process level token. Administrators should log in as a standard user but run their tools with administrator privileges using the built-in access token manipulation command runas.
M1018 - User Account Management: An adversary must already have administrator level access on the local system to make full use of this technique; be sure to restrict users and accounts to the least privileges they require.		

T1484.001 – Domain Policy Modification: Group Policy Modification: Adversaries may modify Group Policy Objects (GPOs) to subvert the intended discretionary access controls for a domain, usually with the intention of escalating privileges on the domain. Group policy allows for centralized management of user and computer settings in Active Directory (AD).	M1047 – Audit: Identify and correct GPO permissions abuse opportunities (ex: GPO modification privileges) using auditing tools such as BloodHound (version 1.5.1 and later).
M1018 – User Account Management: Consider implementing WMI and security filtering to further tailor which users and computers a GPO will apply to.	
T1548.002 - Abuse Elevation Control Mechanism: Bypass User Account Control: Adversaries may bypass UAC mechanisms to elevate process privileges on system. Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by prompting the user for confirmation.	M1047 – Audit: Check for common UAC bypass weaknesses on Windows systems to be aware of the risk posture and address issues where appropriate.
M1026 - Privileged Account Management: Remove users from the local administrator group on systems.	
M1051 – Update Software: Consider updating Windows to the latest version and patch level to utilize the latest protective measures against UAC bypass.	
M1052 - User Account Control: Although UAC bypass techniques exist, it is still prudent to use the highest enforcement level for UAC when possible and mitigate bypass opportunities that exist with techniques such as DLL Search Order Hijacking.	

Defense Evasion	T1484.001 – Domain Policy Modification: Group Policy Modification: Adversaries may modify Group Policy Objects (GPOs) to subvert the intended discretionary access controls for a domain, usually with the intention of escalating privileges on the domain. Group policy allows for centralized management of user and computer settings in Active Directory (AD).	M1047 – Audit: Identify and correct GPO permissions abuse opportunities (ex: GPO modification privileges) using auditing tools such as BloodHound (version 1.5.1 and later).
M1018 – User Account Management: Consider implementing WMI and security filtering to further tailor which users and computers a GPO will apply to.		
T1027.002 – Obfuscated Files or Information: Software Packing: Adversaries may perform software packing or virtual machine software protection to conceal their code. Software packing is a method of compressing or encrypting an executable. Packing an executable changes the file signature in an attempt to avoid signature-based detection. Most decompression techniques decompress the executable code in memory.	M1049 - Antivirus/Antimalware: Employ heuristic-based malware detection. Ensure updated virus definitions and create custom signatures for observed malware.	

T1550 – Use Alternate Authentication Material: Adversaries may use alternate authentication material, such as password hashes, Kerberos tickets, and application access tokens, in order to move laterally within an environment and bypass normal system access controls.	M1026 - Privileged Account Management: Limit credential overlap across systems to prevent the damage of credential compromise and reduce the adversary's ability to perform Lateral Movement between systems.	
M1018 - User Account Management: Enforce the principle of least-privilege. Do not allow a domain user to be in the local administrator group on multiple systems.		
Credential Access	T1555 – Credentials from Password Stores: Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications that store passwords to make it easier for users manage and maintain. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.	M1027 - Password Policies: The password for the user's login keychain can be changed from the user's login password. This increases the complexity for an adversary because they need to know an additional password. Organizations may consider weighing the risk of storing credentials in password stores and web browsers. If system, software, or web browser credential disclosure is a significant concern, technical controls, policy, and user training may be used to prevent storage of credentials in improper locations.

T1003.005 – OS Credential Dumping: Cached Domain Credentials: Adversaries may attempt to access cached domain credentials used to allow authentication to occur in the event a domain controller is unavailable.	M1015 - Active Directory Configuration: Consider adding users to the "Protected Users" Active Directory security group. This can help limit the caching of users' plaintext credentials.
M1028 - Operating System Configuration: Consider limiting the number of cached credentials (HKLM\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon\cachedlogonscountvalue)	
M1027 - Password Policies: Ensure that local administrator accounts have complex, unique passwords across all systems on the network.	
M1026 - Privileged Account Management: Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers.	
M1017 - User Training: Limit credential overlap across accounts and systems by training users and administrators not to use the same password for multiple accounts.	

Lateral Movement	T1021.001 – Remote Services – Remote Desktop Protocol: Adversaries may use Valid Accounts to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user.	M1047 - Audit: Audit the Remote Desktop Users group membership regularly. Remove unnecessary accounts and groups from Remote Desktop Users groups.
M1042 - Disable or Remove Feature or Program: Disable the RDP service if it is unnecessary.		
M1035 - Limit Access to Resource Over Network: Use remote desktop gateways.		
M1032 - Multi-factor Authentication: Use multi-factor authentication for remote logins.		
M1030 - Network Segmentation: Do not leave RDP accessible from the internet. Enable firewall rules to block RDP traffic between network security zones within a network.		
M1028 - Operating System Configuration: Change GPOs to define shorter timeouts sessions and maximum amount of time any single session can be active. Change GPOs to specify the maximum amount of time that a disconnected session stays active on the RD session host server.		
M1026 - Privileged Account Management: Consider removing the local Administrators group from the list of groups allowed to log in through RDP.		
M1018 - User Account Management: Limit remote user permissions if remote access is necessary.		

T1570 – Lateral Tool Transfer: Adversaries may transfer tools or other files between systems in a compromised environment. Files may be copied from one system to another to stage adversary tools or other files over the course of an operation.	M1037 - Filter Network Traffic: Consider using the host firewall to restrict file sharing communications such as SMB.
M1031 - Network Intrusion Prevention: Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware or unusual data transfer over known tools and protocols like FTP can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions.	
T1080 – Taint Shared Content: Adversaries may deliver payloads to remote systems by adding content to shared storage locations, such as network drives or internal code repositories. Content stored on network drives or in other shared locations may be tainted by adding malicious programs, scripts, or exploit code to otherwise valid files.	M1038 - Execution Prevention: Identify potentially malicious software that may be used to taint content or may result from it and audit and/or block the unknown programs by using application control tools, like AppLocker, or Software Restriction Policies where appropriate.
M1050 - Exploit Protection: Use utilities that detect or mitigate common features used in exploitation, such as the Microsoft Enhanced Mitigation Experience Toolkit (EMET).	
M1022 - Restrict File and Directory Permissions: Protect shared folders by minimizing users who have write access.	

Exfiltration	T1041 – Exfiltration Over C2 Channel: Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.	M1057 - Data Loss Prevention: Data loss prevention can detect and block sensitive data being sent over unencrypted protocols.
M1031 - Network Intrusion Prevention: Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools.		
T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage: Adversaries may exfiltrate data to a cloud storage service rather than over their primary command and control channel. Cloud storage services allow for the storage, edit, and retrieval of data from a remote cloud storage server over the Internet.	M1021 - Restrict Web-Based Content: Web proxies can be used to enforce an external network communication policy that prevents use of unauthorized external services.	

Impact	T1486 - Data Encrypted for Impact: Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key.	M1040 - Behavior Prevention on Endpoint: On Windows 10, enable cloud-delivered protection and Attack Surface Reduction (ASR) rules to block the execution of files that resemble ransomware.
M1053 - Data Backup: Consider implementing IT disaster recovery plans that contain procedures for regularly taking and testing data backups that can be used to restore organizational data. Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery. Consider enabling versioning in cloud environments to maintain backup copies of storage objects.		
T1490 - Inhabit System Recovery: Adversaries may delete or remove built-in operating system data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery. Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of Data Destruction and Data Encrypted for Impact.	M1053 - Data Backup: Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data. Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery.	

M1028 - Operating System Configuration: Consider technical controls to prevent the disabling of services or deletion of files involved in system recovery.	
T1489 - Service Stop: Adversaries may stop or disable services on a system to render those services unavailable to legitimate users. Stopping critical services or processes can inhibit or stop response to an incident or aid in the adversary's overall objectives to cause damage to the environment.	M1030 - Network Segmentation: Operate intrusion detection, analysis, and response systems on a separate network from the production environment to lessen the chances that an adversary can see and interfere with critical response functions.
M1022 - Restrict File and Directory Permissions: Ensure proper process and file permissions are in place to inhibit adversaries from disabling or interfering with critical services.	
M1024 - Restrict Registry Permissions: Ensure proper registry permissions are in place to inhibit adversaries from disabling or interfering with critical services.	
M1018 - User Account Management: Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service configurations.	