# Threat Report

connectwise.com/resources/hive-profile

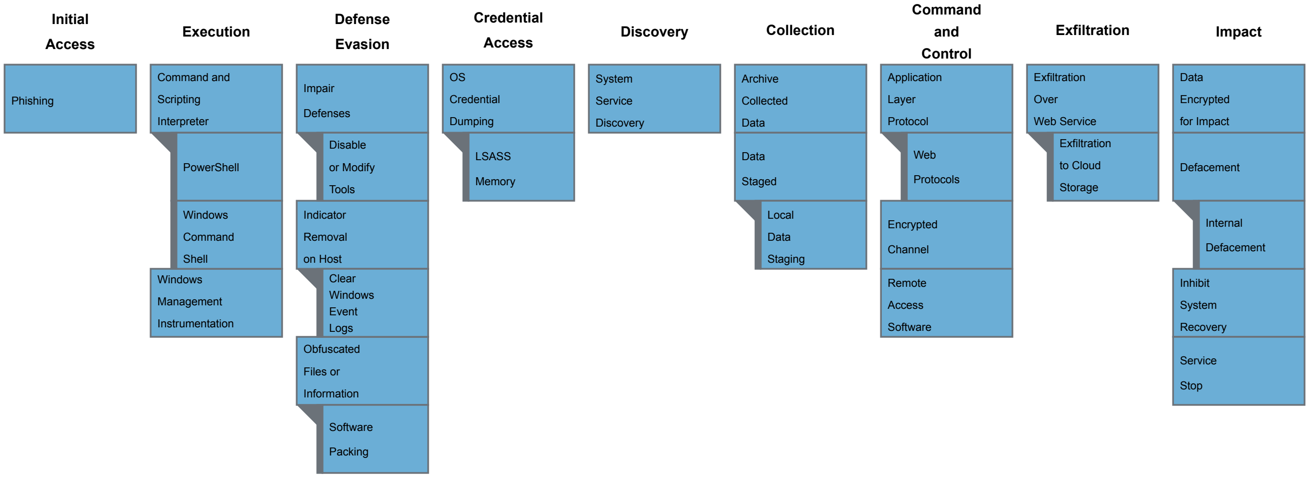
In the 2022 MSP Threat Report, the CRU identified the top 5 ransomware threats targeting MSPs in 2021 and provided a brief description of each. This page includes supplemental material with a more detailed breakdown of the TTPs and suggested mitigation techniques.

- Ransomware-as-a-service that first appeared in June 2021
- Targets Windows, Linux, and ESXi
- Written in Golang
- Uses the double extortion method of encrypting files and threatening to leak stolen data
- Responsible for 5% of all ransomware incidents we observed targeting MSPs and their customers in 2021

about

Hive

2021 Top Threat Actors Targeting MSPs



**Initial Access**
- Phishing

**Execution**
- Command and Scripting Interpreter
  - PowerShell
  - Windows Command Shell
- Windows Management Instrumentation

**Defense Evasion**
- Impair Defenses
  - Disable or Modify Tools
- Indicator Removal on Host
  - Clear Windows Event Logs
- Obfuscated Files or Information
  - Software Packing

**Credential Access**
- OS Credential Dumping
  - LSASS Memory

**Discovery**
- System Service Discovery

**Collection**
- Archive Collected Data
- Data Staged
  - Local Data Staging

**Command and Control**
- Application Layer Protocol
  - Web Protocols
- Encrypted Channel
- Remote Access Software

**Exfiltration**
- Exfiltration Over Web Service
  - Exfiltration to Cloud Storage

**Impact**
- Data Encrypted for Impact
- Defacement
  - Internal Defacement
- Inhibit System Recovery
- Service Stop

| ATT&CK Tactic | ATT&CK Technique | Mitigations |
|---|---|---|
| Initial Access | T1566 – Phishing:<br><br>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.

| | | |
|---|---|---|
| Execution | T1059.001 – Command and Scripting Interpreter – PowerShell:<br>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:<br>Anti-virus can be used to automatically quarantine suspicious files. |
| M1045 - Code Signing:<br>Set PowerShell execution policy to execute only signed scripts. | | |
| M1042 - Disable or Remove Feature or Program:<br>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.<br>Disable/restrict the WinRM Service to help prevent uses of PowerShell for remote execution. | | |
| M1038 - Execution Prevention:<br>Use application control where appropriate. | | |
| M1026 - Privileged Account Management:<br>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:<br>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:<br>Use application control where appropriate. |
| T1047 – Windows Management Instrumentation:<br>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:<br>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:<br>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:<br>Prevent credential overlap across systems of administrator and privileged accounts. | |

| | | |
|---|---|---|
| M1018 - User Account Management:<br>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. | | |
| Defense Evasion | T1070.001 – Indicator Removal on Host: Clear Windows Event Logs:<br>Adversaries may clear Windows Event Logs to hide the activity of an intrusion. Windows Event Logs are a record of a computer's alerts and notifications. There are three system-defined sources of events: System, Application, and Security, with five event types: Error, Warning, Information, Success Audit, and Failure Audit. | M1041 - Encrypt Sensitive Information:<br>Obfuscate/encrypt event files locally and in transit to avoid giving feedback to an adversary. |
| M1029 - Remote Data Storage:<br>Automatically forward events to a log server or data repository to prevent conditions in which the adversary can locate and manipulate data on the local system. When possible, minimize time delay on event reporting to avoid prolonged storage on the local system. | | |

| | |
|---|---|
| M1022 - Restrict File and Directory Permissions:<br>Protect generated event files that are stored locally with proper permissions and authentication and limit opportunities for adversaries to increase privileges by preventing Privilege Escalation opportunities. | |
| T1027.002 – Obfuscated Files or Information: Software Packing:<br>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:<br>Employ heuristic-based malware detection. Ensure updated virus definitions and create custom signatures for observed malware. |
| T1562.001 – Impair Defenses: Disable or Modify Tools:<br>Adversaries may modify and/or disable security tools to avoid possible detection of their malware/tools and activities. This may take the many forms, such as killing security software processes or services, modifying / deleting Registry keys or configuration files so that tools do not operate properly, or other methods to interfere with security tools scanning or reporting information. | M1022 - Restrict File and Directory Permissions:<br>Ensure proper process and file permissions are in place to prevent adversaries from disabling or interfering with security services. |

| | | |
|---|---|---|
| M1024 - Restrict Registry Permissions:<br>Ensure proper Registry permissions are in place to prevent adversaries from disabling or interfering with security services. | | |
| M1018 - User Account Management:<br>Ensure proper user permissions are in place to prevent adversaries from disabling or interfering with security services. | | |
| Credential Access | T1003.001 – OS Credential Dumping: LSASS Memory:<br>Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct Lateral Movement using Use Alternate Authentication Material. | M1040 - Behavior Prevention on Endpoint:<br>On Windows 10, enable Attack Surface Reduction (ASR) rules to secure LSASS and prevent credential stealing. |

M1043 - Credential Access Protection:

With Windows 10, Microsoft implemented new protections called Credential Guard to protect the LSA secrets that can be used to obtain credentials through forms of credential dumping. It is not configured by default and has hardware and firmware system requirements. It also does not protect against all forms of credential dumping.

M1028 - Operating System Configuration:

Consider disabling or restricting NTLM. Consider disabling WDigest authentication.

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.

| | | |
|---|---|---|
| M1025 - Privileged Process Integrity:<br>On Windows 8.1 and Windows Server 2012 R2, enable Protected Process Light for LSA. | | |
| M1017 - User Training:<br>Limit credential overlap across accounts and systems by training users and administrators not to use the same password for multiple accounts. | | |
| Discovery | T1007 – System Service Discovery:<br>Adversaries may try to get information about registered services. Commands that may obtain information about services using operating system utilities are "sc," "tasklist /svc" using Tasklist, and "net start" using Net, but adversaries may also use other tools as well. Adversaries may use the information from System Service Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. |

| | | |
|---|---|---|
| Collection | T1074.001 – Data Staged: Local Data Staging:<br>Adversaries may stage collected data in a central location or directory on the local system prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as Archive Collected Data. Interactive command shells may be used, and common functionality within cmd and bash may be used to copy data into a staging location. | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. |
| T1560 – Archive Collected Data:<br>An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender. | M1047 - Audit:<br>System scans can be performed to identify unauthorized archival utilities. | |

| | | |
|---|---|---|
| Command and Control | T1071.001 – Application Layer Protocol: Web Protocols:<br>Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.<br>Protocols such as HTTP and HTTPS that carry web traffic may be very common in environments. HTTP/S packets have many fields and headers in which data can be concealed. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic. | M1031 - Network Intrusion Prevention:<br>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. |
| T1573 – Encrypted Channel:<br>Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files. | M1031 - Network Intrusion Prevention:<br>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. | |

| | |
|---|---|
| M1020 - SSL/TLS Inspection:<br>SSL/TLS inspection can be used to see the contents of encrypted sessions to look for network-based indicators of malware communication protocols. | |
| T1219 – Remote Access Software:<br>An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, LogMein, AmmyyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. | M1038 - Execution Prevention:<br>Use application control to mitigate installation and use of unapproved software that can be used for remote access. |
| M1037 - Filter Network Traffic:<br>Properly configure firewalls, application firewalls, and proxies to limit outgoing traffic to sites and services used by remote access tools. | |
| M1031 - Network Intrusion Prevention:<br>Network intrusion detection and prevention systems that use network signatures may be able to prevent traffic to remote access services. | |

| | | |
|---|---|---|
| Exfiltration | T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage:<br>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:<br>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:<br>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:<br>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:<br>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. | |
| T1491.001 – Internal Defacement:<br>An adversary may deface systems internal to an organization in an attempt to intimidate or mislead users. This may take the form of modifications to internal websites, or directly to user systems with the replacement of the desktop wallpaper. Disturbing or offensive images may be used as a part of Internal Defacement in order to cause user discomfort, or to pressure compliance with accompanying messages. Since internally defacing systems exposes an adversary's presence, it often takes place after other intrusion goals have been accomplished. | M1053 - Data Backup:<br>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. |