Threat Report

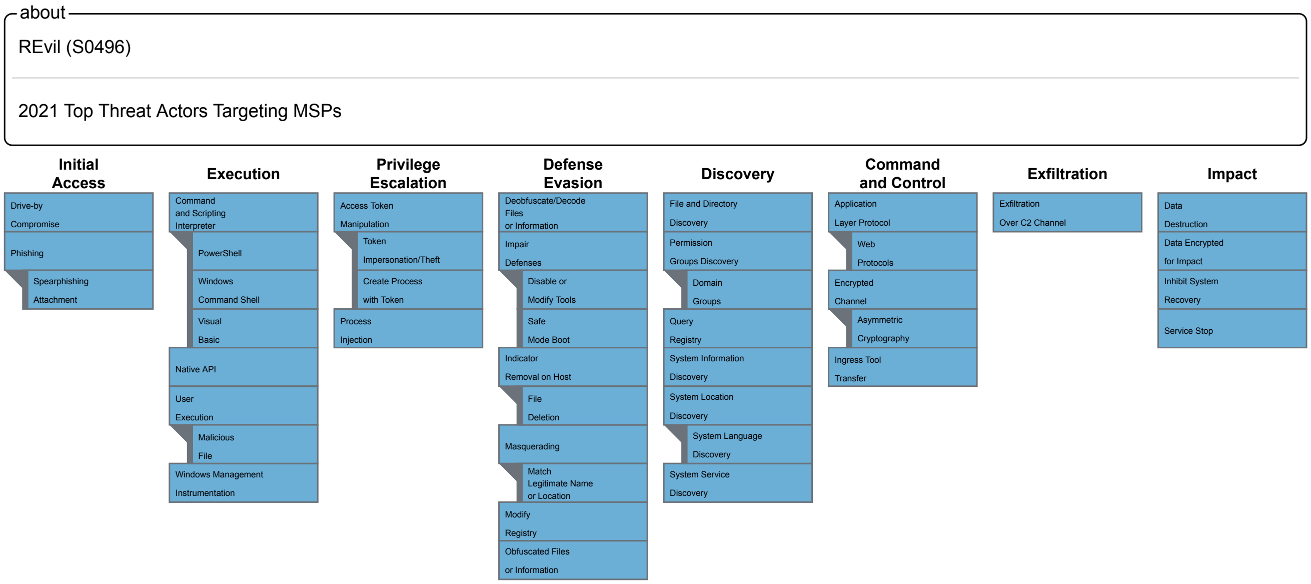
connectwise.com/resources/revil-profile

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.

REvil

- Ransomware-as-a-service that first appeared in April 2019
- Highly configurable, successor to GandCrab
- Uses the double extortion method of encrypting files and threatening to leak stolen data
- Responsible for large scale ransomware attacks targeting over 40 MSPs and at least 1500 of their customers using Kaseya VSA in July 2021
- REvil servers went offline in October 2021, then in January 2022, the Russian Federal Security Service said they had dismantled REvil and charged several of its members after being provided information by the US

MITRE ATT&CK® mapping



about

REvil (S0496)

2021 Top Threat Actors Targeting MSPs

Initial Access	Execution	Privilege Escalation	Defense Evasion	Discovery	Command and Control	Exfiltration	Impact
Drive-by Compromise	Command and Scripting Interpreter	Access Token Manipulation	Deobfuscate/Decode Files or Information	File and Directory Discovery	Application Layer Protocol	Exfiltration Over C2 Channel	Data Destruction
Phishing	PowerShell	Token Impersonation/Theft	Impair Defenses	Permission Groups Discovery	Web Protocols		Data Encrypted for Impact
Spearphishing Attachment	Windows Command Shell	Create Process with Token	Disable or Modify Tools	Domain Groups	Encrypted Channel		Inhibit System Recovery
	Visual Basic	Process Injection	Safe Mode Boot	Query Registry	Asymmetric Cryptography		Service Stop
	Native API		Indicator Removal on Host	System Information Discovery	Ingress Tool Transfer		
	User Execution		File Deletion	System Location Discovery			
	Malicious File		Masquerading	System Language Discovery			
	Windows Management Instrumentation		Match Legitimate Name or Location	System Service Discovery			
			Modify Registry				
			Obfuscated Files or Information				

REvil TTPs and Mitigations

ATT&CK Tactic	ATT&CK Technique	DEFEND Mitigations

Initial Access	T1189 – Drive-by Compromise: Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring Application Access Token.	M1048 - Application Isolation and Sandboxing: Browser sandboxes can be used to mitigate some of the impact of exploitation, but sandbox escapes may still exist.Other types of virtualization and application microsegmentation may also mitigate the impact of client-side exploitation. The risks of additional exploits and weaknesses in implementation may still exist for these types of systems.
M1050 - Exploit Protection: Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. Many of these protections depend on the architecture and target application binary for compatibility.		
M1021 - Restrict Web-Based Content: For malicious code served up through ads, adblockers can help prevent that code from executing in the first place. Script blocking extensions can help prevent the execution of JavaScript that may commonly be used during the exploitation process.		

M1051 – Update Software: Ensure all browsers and plugins kept updated can help prevent the exploit phase of this technique. Use modern browsers with security features turned on.	
T1566.001 – Phishing: Spearphishing Attachment: Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry.	M1049 - Antivirus/Antimalware: Anti-virus can also automatically quarantine suspicious files.
M1031 - Network Intrusion Prevention: Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity.	
M1021 - Restrict Web-Based Content: Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments.	

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.		
M1017 - User Training: Users can be trained to identify social engineering techniques and spearphishing emails.		
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.

T1059.005 – Command and Scripting Interpreter: Visual Basic: Adversaries may abuse Visual Basic (VB) for execution. VB is a programming language created by Microsoft with interoperability with many Windows technologies such as Component Object Model and the Native API through the Windows API. Although tagged as legacy with no planned future evolutions, VB is integrated and supported in the .NET Framework and cross-platform .NET Core.	M1049 - Antivirus/Antimalware: Anti-virus can be used to automatically quarantine suspicious files.
M1040 - Behavior Prevention on Endpoint: On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Visual Basic scripts from executing potentially malicious downloaded content.	
M1042 - Disable or Remove Feature or Program: Turn off or restrict access to unneeded VB components.	
M1038 - Execution Prevention: Use application control where appropriate.	
M1021 - Restrict Web-Based Content: Script blocking extensions can help prevent the execution of scripts and HTA files that may commonly be used during the exploitation process. For malicious code served up through ads, adblockers can help prevent that code from executing in the first place.	

T1106 – Native Application Programming Interface (API)	M1040 - Behavior Prevention on Endpoint: On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Office VBA macros from calling Win32 APIs.
M1038 - Execution Prevention: Identify and block potentially malicious software executed that may be executed through this technique by using application control tools, like Windows Defender Application Control, AppLocker, or Software Restriction Policies where appropriate.	
T1204.002 – User Execution: Malicious File: An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from Spearphishing Attachment. Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl.	M1040 - Behavior Prevention on Endpoint: On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria). Note: cloud-delivered protection must be enabled for certain rules.
M1038 - Execution Prevention: Application control may be able to prevent the running of executables masquerading as other files.	

M1017 - User Training: Use user training as a way to bring awareness to common phishing and spearphishing techniques and how to raise suspicion for potentially malicious events.	
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.		
Privilege Escalation	T1134.001 – Access Token Manipulation: Token Impersonation/Theft: Adversaries may duplicate then impersonate another user's token to escalate privileges and bypass access controls. An adversary can create a new access token that duplicates an existing token using DuplicateToken(Ex). The token can then be used with ImpersonateLoggedOnUser to allow the calling thread to impersonate a logged on user's security context, or with SetThreadToken to assign the impersonated token to a thread.	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 us	
T1134.002 – Access Token Manipulation: Create Process with Token: Adversaries may create a new process with a different token to escalate privileges and bypass access controls. Processes can be created with the token and resulting security context of another user using features such as CreateProcessWithTokenW and runas.	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	

T1055 – Process Injection: Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.	M1040 - Behavior Prevention on Endpoint: Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process. For example, on Windows 10, Attack Surface Reduction (ASR) rules may prevent Office applications from code injection.	
M1026 - Privileged Account Management: Utilize Yama (ex: /proc/sys/kernel/yama/ptrace_scope) to mitigate ptrace based process injection by restricting the use of ptrace to privileged users only. Other mitigation controls involve the deployment of security kernel modules that provide advanced		
Defense Evasion	T1140 - Deobfuscate/Decode Files or Information: Adversaries may use Obfuscated Files or Information to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system.	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

T1562.001 – Impair Defenses: Disable or Modify Tools: 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: Ensure proper process and file permissions are in place to prevent adversaries from disabling or interfering with security services.
M1024 - Restrict Registry Permissions: Ensure proper Registry permissions are in place to prevent adversaries from disabling or interfering with security services.	
M1018 - User Account Management: Ensure proper user permissions are in place to prevent adversaries from disabling or interfering with security services.	
T1562.009 – Impair Defenses: Safe Mode Boot: Adversaries may abuse Windows safe mode to disable endpoint defenses. Safe mode starts up the Windows operating system with a limited set of drivers and services. Third-party security software such as endpoint detection and response (EDR) tools may not start after booting Windows in safe mode. There are two versions of safe mode: Safe Mode and Safe Mode with Networking. It is possible to start additional services after a safe mode boot.	M1026 - Privileged Account Management: Restrict administrator accounts to as few individuals as possible, following least privilege principles, that may be abused to remotely boot a machine in safe mode.

M1054 - Software Configuration: Ensure that endpoint defenses run in safe mode.	
T1070.004 – Indicator Removal on Host: File Deletion: Adversaries may delete files left behind by the actions of their intrusion activity. Malware, tools, or other non-native files dropped or created on a system by an adversary may leave traces to indicate to what was done within a network and how. Removal of these files can occur during an intrusion, or as part of a post-intrusion process to minimize the adversary's footprint.	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
T1036.005 – Masquerading: Match Legitimate Name or Location: Adversaries may match or approximate the name or location of legitimate files or resources when naming/placing them. This is done for the sake of evading defenses and observation. This may be done by placing an executable in a commonly trusted directory (ex: under System32) or giving it the name of a legitimate, trusted program (ex: svchost.exe). In containerized environments, this may also be done by creating a resource in a namespace that matches the naming convention of a container pod or cluster.	M1045 - Code Signing: Require signed binaries and images.
M1038 - Execution Prevention: Use tools that restrict program execution via application control by attributes other than file name for common operating system utilities that are needed.	

M1022 - Restrict File and Directory Permissions: Use file system access controls to protect folders such as C:\Windows\System32.	
T1112 – Modify Registry: Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution.	M1024 - Restrict Registry Permissions: Ensure proper permissions are set for Registry hives to prevent users from modifying keys for system components that may lead to privilege escalation.
T1027 - Obfuscated Files or Information: Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses.	M1049 - Antivirus/Antimalware: Consider utilizing the Antimalware Scan Interface (AMSI) on Windows 10 to analyze commands after being processed/interpreted.
M1040 - Behavior Prevention on Endpoint: On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent execution of potentially obfuscated scripts.	

Discovery	T1083 – File and Directory Discovery: Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from File and Directory 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.
T1069.002 – Permission Groups Discovery: Domain Groups: Adversaries may attempt to find domain-level groups and permission settings. The knowledge of domain-level permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as domain administrators.	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.	
T1012 – Query Registry: Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.	

T1082 – System Information Discovery: An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from System Information 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.
T1614.001 – System Location Discovery: System Language Discovery: Adversaries may attempt to gather information about the system language of a victim in order to infer the geographical location of that host. This information may be used to shape follow-on behaviors, including whether the adversary infects the target and/or attempts specific actions. This decision may be employed by malware developers and operators to reduce their risk of attracting the attention of specific law enforcement agencies or prosecution/scrutiny from other entities.	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
T1007 – System Service Discovery	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

Command and Control	T1071.001 – Application Layer Protocol: Web Protocols: 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. 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: 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.

T1573.002 – Encrypted Channel: Asymmetric Cryptography: Adversaries may employ a known asymmetric encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Asymmetric cryptography, also known as public key cryptography, uses a keypair per party: one public that can be freely distributed, and one private. Due to how the keys are generated, the sender encrypts data with the receiver’s public key and the receiver decrypts the data with their private key. This ensures that only the intended recipient can read the encrypted data.	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.
M1020 - SSL/TLS Inspection: SSL/TLS inspection can be used to see the contents of encrypted sessions to look for network-based indicators of malware communication protocols.	

T1105 – Ingress Tool Transfer: Adversaries may transfer tools or other files from an external system into a compromised environment. Files may be copied from an external adversary controlled system through the command and control channel to bring tools into the victim network or through alternate protocols with another tool such as FTP. Files can also be copied over on Mac and Linux with native tools like scp, rsync, and sftp.	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. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.	
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.		
Impact	T1485 – Data Destruction: Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives	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.

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.	