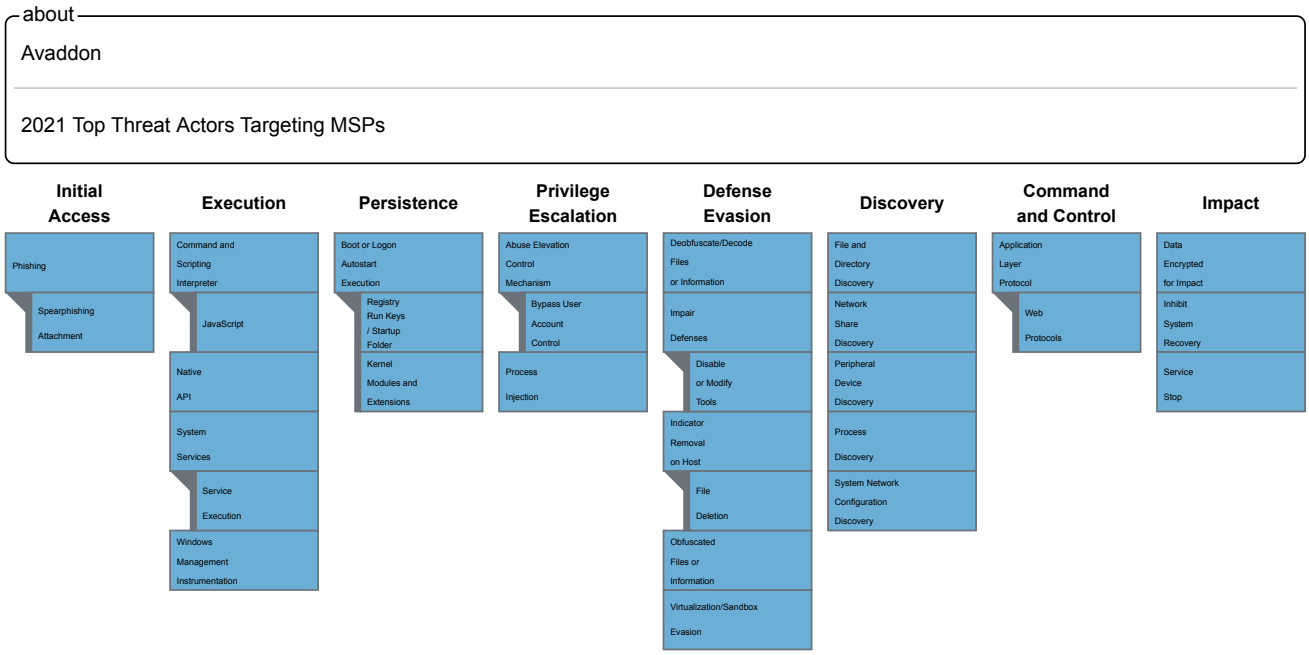
Threat Report

connectwise.com/resources/avaddon-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 that first appeared in June 2020
- Does not harm systems with operating system language or keyboard layouts set to the specific languages typically used in the Commonwealth of Independent States (formerly the Soviet Union)
- Uses a triple extortion method of encrypting files, threatening to leak stolen data, and using DDoS attacks to coerce victims into paying
- Responsible for 5% of all ransomware incidents we observed targeting MSPs and their customers in 2021
- Avaddon shut down operations and released its decryption keys on June 11, 2021



Initial Access	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	T1059.007 – Command and Scripting Interpreter: JavaScript: Adversaries may abuse various implementations of JavaScript for execution. JavaScript (JS) is a platform-independent scripting language (compiled just-in-time at runtime) commonly associated with scripts in webpages, though JS can be executed in runtime environments outside the browser.	M1040 - Behavior Prevention on Endpoint: On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent JavaScript scripts from executing potentially malicious downloaded content.
M1042 - Disable or Remove Feature or Program: Turn off or restrict access to unneeded scripting components.		

M1038 - Execution Prevention: Denylist scripting where appropriate.	
M1021 - Restrict Web-Based Content: Script blocking extensions can help prevent the execution of JavaScript 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.	
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.

T1569.002 – System Services: Service Execution:

Adversaries may abuse the Windows service control manager to execute malicious commands or payloads. The Windows service control manager (services.exe) is an interface to manage and manipulate services. The service control manager is accessible to users via GUI components as well as system utilities such as sc.exe and Net.

M1040 - Behavior Prevention on Endpoint:

On Windows 10, enable Attack Surface Reduction (ASR) rules to block processes created by PsExec from running.

M1026 - Privileged Account Management: Ensure that permissions disallow services that run at a higher permissions level from being created or interacted with by a user with a lower permission level.		
M1022 - Restrict File and Directory Permissions: Ensure that high permission level service binaries cannot be replaced or modified by users with a lower permission level.		
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.

T1547.006 – Boot or Logon Autostart Execution: Kernel Modules and Extensions: Adversaries may modify the kernel to automatically execute programs on system boot. Loadable Kernel Modules (LKMs) are pieces of code that can be loaded and unloaded into the kernel upon demand. They extend the functionality of the kernel without the need to reboot the system. For example, one type of module is the device driver, which allows the kernel to access hardware connected to the system.	M1049 - Antivirus/Antimalware: Common tools for detecting Linux rootkits include: rkhunter, chrootkit, although rootkits may be designed to evade certain detection tools.
M1038 - Execution Prevention: Application control and software restriction tools, such as SELinux, KSPP, grsecurity MODHARDEN, and Linux kernel tuning can aid in restricting kernel module loading. Since macOS High Sierra 10.13, Secure Kernel Extension Loading (SKEL) can also be used to restrict the loading of kernel modules.	
M1026 - Privileged Account Management: Limit access to the root account and prevent users from loading kernel modules and extensions through proper privilege separation and limiting Privilege Escalation opportunities.	

Privilege Escalation	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.		

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	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.	
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.
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.
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.	
T1497 – Virtualization/Sandbox Evasion: Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant.	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

Discovery	T1016 – System Network Configuration Discovery: Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include Arp, ipconfig/ifconfig, nbtstat, and route.	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
T1057 – Process Discovery: Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from Process 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.	

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.
T1135 – Network Share Discovery: Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.	M1028 - Operating System Configuration: Enable Windows Group Policy "Do Not Allow Anonymous Enumeration of SAM Accounts and Shares" security setting to limit users who can enumerate network shares.
T1120 – Peripheral Device Discovery: Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system. Peripheral devices could include auxiliary resources that support a variety of functionalities such as keyboards, printers, cameras, smart card readers, or removable storage. The information may be used to enhance their awareness of the system and network environment or may be used for further actions.	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.

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.