CONNECTWISE

WHITEPAPER SERIES

2023 MSP THREAT REPORT

Contents

Introduction

Whether you are just starting in managed services with a few hundred endpoints or a former hardware and peripherals company transforming your business into a world-class digital software and services firm serving tens of thousands of users, 100% of today's MSP clients need a digital presence. Plain and simple. If your business doesn't have a digital presence, chances are your customer base won't be able to find you. Nowadays, having a digital presence means leveraging the internet, cloud computing, the Internet of Things (IoT), and more.

All this time spent in cyberspace leaves businesses vulnerable to an onslaught of hacking and system infiltration attempts. Unfortunately, most businesses consider cybersecurity an expense, not an investment. These organizations would rather put money to use elsewhere than protect their most important asset—their data.

One of the unfortunate challenges we continue to see MSPs facing as they try to deploy more advanced cybersecurity software is hesitancy from their clients. Many small- and medium-businesses (SMBs) say they don't need advanced security because they "feel they won't be targeted."

We now understand that this isn't the case. It doesn't matter what size your business is, everyone is a target. And attackers often go after the low-hanging fruit—those without advanced protection or dedicated cybersecurity staff, which is more characteristic status quo for SMBs. So, what can we do about this?

As IT solution providers and cybersecurity practitioners, we need to prioritize cybersecurity. We need to get better at making everyone understand that nobody is off-limits when it comes to cyberattacks.

Attackers will target anyone they can, and the easier the target, the higher the likelihood that they will be the victim of a cyberthreat. Nothing in cybersecurity is 100%. That's why protection works best in layers.

One of the most important steps organizations can take to improve their posture is to leverage threat intelligence. Your organization should compose your CTI team of individuals with different skills and expertise, such as data scientists, security analysts, and engineers. Each team member should have the knowledge and experience to properly analyze incoming data and develop strategies for responding to threats.

Building a team can be challenging and costly, as a limited talent pool with the necessary expertise is available. Organizations should look beyond their walls and consider partnering with specialized vendors or other organizations that can provide additional resources and support.

An effective CTI team will work together to identify potential threats, develop strategies for responding to them, and securely share information. While there is no one-size-fits-all approach to building a CTI team, following these steps can help organizations have the resources and expertise they need to avoid cyberthreats.

The ConnectWise Cyber Research Unit (CRU) is comprised of seasoned cybersecurity professionals with deep engineering, IT administration, security operations, and incident analysis and response expertise. Leveraging years of real-world, hard knocks experience, the CRU team is dedicated to expanding the industry's collective understanding of today's threat landscape. Armed with this intelligence, we seek to help defenders improve their defense-in-depth and keep critical assets safe.

Our findings are based on an analysis of over half a million discrete incidents that the CRU put together for the fourth edition of the ConnectWise MSP Threat Report.

Get an eye-opening look at what MSPs faced in 2022 and predictions for 2023 and beyond.

Chapter 1: 2022 Security Incidents in Review

The CRU reviewed data from over 440,000 cybersecurity incidents that impacted our MSP partners and their clients in 2022. Below is a breakdown of the number of incidents reviewed per business sector.

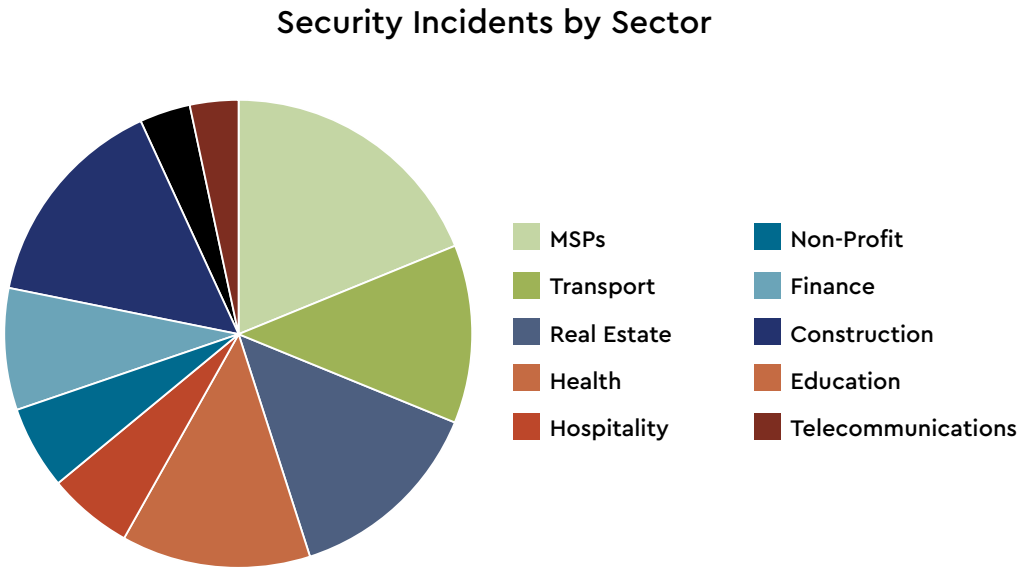


Figure 1.0: Top 10 Business Sectors affected by the 440,000 security incidents reviewed by the CRU in 2022

Top 10 MITRE ATT&CK® Techniques in Security Incidents

We identified 214 unique MITRE ATT&CK techniques and sub-techniques used by threat actors in these cybersecurity incidents. Below is a summary of the incidents we captured and a breakdown of the top 10 MITRE ATT&CK techniques we observed in 2022. This includes sub-techniques, mitigation and detection guidance, and detection signatures currently in ConnectWise SIEM™, which designed to detect these techniques in action.

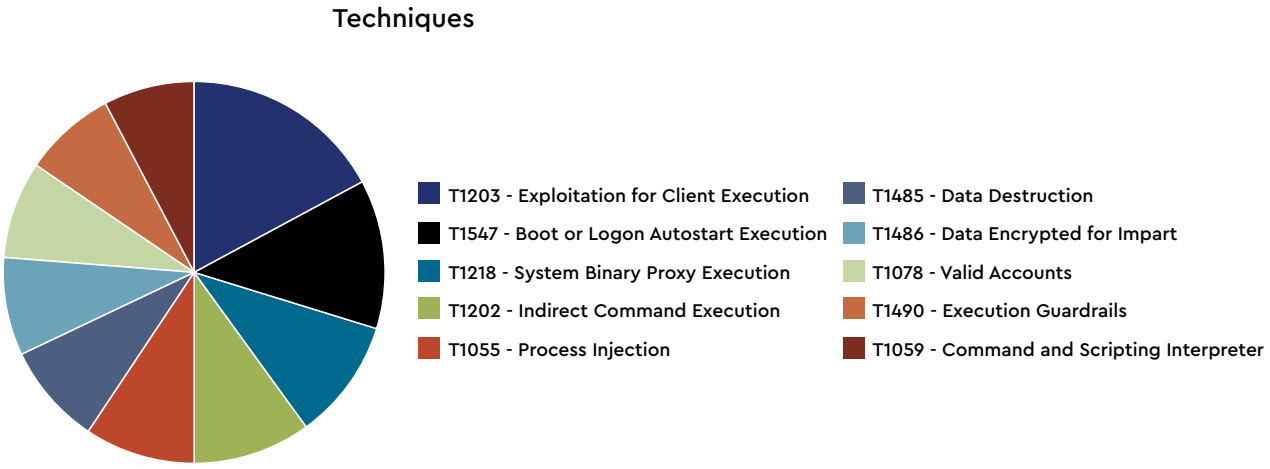


Figure 1.1: Top 10 MITRE ATT&CK(C) Techniques observed in the 440,000 security incidents reviewed by the CRU in 2022

1. MITRE ATT&CK Technique T1203: Exploitation for Client Execution

Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that can lead to unpredictable behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Frequently, the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly use to do work, so they are a useful target for exploit research and development because of their high utility.

Several types exist:

a. Browser-Based Exploitation

Web browsers are a common target through drive-by compromise and spearphishing. Endpoint systems may be compromised through normal web browsing or from targeting certain users with links in spearphishing emails to adversary-controlled sites used to exploit the web browser. These often do not require action by the user for the exploit to be executed.

b. Office Applications

Common office and productivity applications, such as Microsoft® Office, are also targeted through phishing. Malicious files will be transmitted directly as attachments or through links to download them. These require the user to open the document or file for the exploit to run.

c. Common Third-party Applications

Other applications that are commonly seen or are part of the software deployed in a target network may also be used for exploitation. Applications such as Adobe Reader and Flash, which are common in enterprise environments, have been routinely targeted by adversaries attempting to gain access to systems. Depending on the software and nature of the vulnerability, some may be exploited in the browser or require the user to open a file. For instance, some Flash exploits have been delivered as objects within Microsoft Office documents.

General Detection Guidance

Detecting software exploitation may be difficult depending on the tools available. Look for behavior on the endpoint system that may indicate successful compromise, such as abnormal behavior of the browser or Office processes. This could include suspicious files written to disk, evidence of process injection for attempts to hide execution, evidence of discovery, or other unusual network traffic that may indicate additional tools transferred to the system.

Mitigation Guidance

- Exploit protection (M1050): Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring
- Application isolation and sandboxing (M1048): Restrict the execution of code to a virtual environment on or in transit to an endpoint system

Exploitation for Client Execution Mitigation

- Browser sandboxes can be used to mitigate some of the impact of exploitation, but sandbox escapes may still exist.
- Other virtualization and application micro-segmentation types may also mitigate the impact of client-side exploitation. The risks of additional exploits and weaknesses in implementation may still exist.
- 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.

2. MITRE ATT&CK Technique T1547: Boot or Logon Autostart Execution

Adversaries may configure system settings to automatically execute a program during system boot or login to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account login. These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel.

Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

General Detection Guidance

Monitor for additions or modifications of mechanisms that could trigger autostart execution, such as relevant additions to the Registry. Look for changes that are not correlated with known updates, patches, or other planned administrative activity. Tools such as Sysinternals Autoruns may also be used to detect system autostart configuration changes that could be attempts at persistence, per TechNet Autoruns. Changes to some autostart configuration settings may happen under normal conditions when legitimate software is installed.

Suspicious program execution as autostart programs may show up as outlier processes that have not been seen before when compared against historical data. To increase confidence of malicious activity, data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities, such as network connections made for Command and Control, learning details about the environment through discovery, and lateral movement.

Monitor DLL loads by processes, specifically looking for DLLs that are not recognized or not normally loaded into a process. Look for abnormal process behavior that may be due to a process loading a malicious DLL.

Monitor for abnormal usage of utilities and command-line parameters involved in kernel modification or driver installation.

Mitigation Guidance

- User Account Management (M1018): Manage the creation, modification, use, and permissions associated to user accounts.
- Restrict Library Loading (M1044): Prevent abuse of library loading mechanisms in the operating system and software to load untrusted code by configuring appropriate library loading mechanisms and investigating potential vulnerable software.
- Privileged Process Integrity (M1025): Protect processes with high privileges that can be used to interact with critical system components through use of protected process light, anti-process injection defenses, or other process integrity enforcement measures.
- Credential Access Protection (M1043): Use capabilities to prevent successful credential access by adversaries, including blocking forms of credential dumping.
- Execution Prevention (M1038): Block execution of code on a system through application control, and/or script blocking.
- Antivirus/Antimalware (M1049): Use signatures or heuristics to detect malicious software. Within industrial control environments, antivirus/antimalware installations should be limited to assets that are not involved in critical or real-time operations. To minimize the impact to system

availability, all products should first be validated within a representative test environment before deployment to production systems.

- Disable or Remove Feature or Program (M1042): Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.
- User Training (M1017): Train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spearphishing, social engineering, and other techniques that involve user interaction.
- Restrict Registry Permissions (M1024): Restrict the ability to modify certain hives or keys in the Windows Registry.
- Restrict File and Directory Permissions (M1022): Restrict access by setting directory and file permissions that are not specific to users or privileged accounts.
- Limit Software Installation (M1033): Block users or groups from installing unapproved software.

Related Detection Signatures in ConnectWise SIEM

- [CRU][Windows] Autoruns Winlogon Shell Value Set
- CRU][Windows] Creation/Modification of Assistive Technology (AT) Applications
- [CRU][Windows] Winlogon Registry Edit via Powershell
- [CRU][Windows] Executable Created In Startup Folder
- [CRU][Windows] Executable Created In Startup Folder
- [CRU][Windows] Autoruns Run Key Value Set By Suspicious Process
- [CRU][Windows] Suspicious Process Write to Startup
- [CRU][Windows] Modification of Default Startup Folder via 'Common Startup' Registry Key (Security Auditing)
- [CRU][Windows] Autoruns RDP Logon Key Set
- [CRU][Windows] Autoruns Active Setup Registry Values Set
- [CRU][Windows] Registry Edit with Modification of Userinit, Shell or Notify
- [CRU][Windows] MUDDYWATER Small Sieve (Gramdoor) Activity 2022-02 P1
- [CRU][Windows] Autoruns General Winlogon Key Value Set
- [CRU][Windows] Raspberry Robin Campaign
- [CRU][Windows] Registry Modification of Userinit, Shell, or Notify Through Command Line Field
- [CRU][Windows] Powershell Persistence in Registry
- [CRU][Windows] LOLBin Atbroker.exe Running Unusual Executable
- [CRU][Windows] Spoolsv.exe Create or Delete Driver Files
- [CRU][Windows] Twisted Panda Spinner Backdoor Registry Entry
- [CRU][Windows] Registry Run Key Value Set by wscript.exe
- [CRU][Windows] Command Launched from WinLogon
- [CRU][Windows] Autoruns Explorer Startup Registry Value
- [CRU][Windows] Modification of Default Startup Folder via 'Common Startup' Registry Key (Sysmon)
- [CRU][Windows] MUDDYWATER Small Sieve (Gramdoor) Activity 2022-02 P2
- [CRU][Windows] Autoruns Userinit Value Set
- [CRU][Windows] Registry Modification of Userinit, Shell, or Notify Through Winlog.Event_Data.ObjectName Field (Security Auditing)
- CRU][Windows] MUDDYWATER StarWhale (Canopy) persistence 2022-02
- [CRU][Windows] Modification of Default Startup Folder via 'Common Startup' Registry Key (Command Line)

3. MITRE ATT&CK T1218: System Binary Proxy Execution

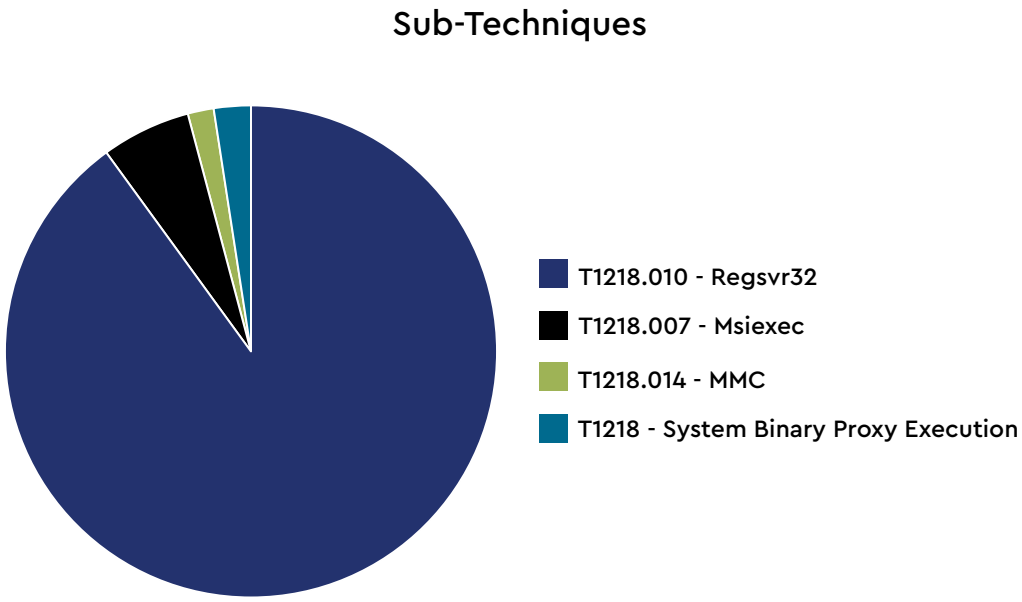


Figure 1.2: MITRE ATT&CK(C) Sub-techniques under the Technique T1218: System Binary Proxy Execution observed in the 440,000 security incidents reviewed by the CRU in 2022

Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed or otherwise trusted binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native to the operating system. Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft-signed binaries that are default on Windows installations can be used to proxy execution of other files or commands.

Similarly, on Linux systems, adversaries may abuse trusted binaries such as "split" to proxy execution of malicious commands.

General Detection Guidance

Be sure to monitor processes and command-line parameters for signed binaries that may be used to proxy execution of malicious files. Also, compare recent invocations of signed binaries that may be used to proxy execution with prior history of known good arguments and loaded files to determine anomalous and potentially adversarial activity. Legitimate programs used in suspicious ways, like msiexec.exe downloading an MSI file from the internet, may indicate an intrusion. Correlate activity with other suspicious behavior to reduce false positives that may be due to normal, benign use by users and administrators.

Monitor for file activity (creations, downloads, modifications, etc.), especially for file types that are not typical within an environment and may indicate adversary activity.

Mitigation Guidance

- Privileged Account Management (M1026): Manage the creation, modification, use, and permissions associated with privileged accounts, including SYSTEM and root.
- Disable or Remove Feature or Program (M1042): Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.
- Exploit Protection (M1050): Use capabilities to detect and block conditions that may lead to or indicate a software exploit occurring.
- Execution Prevention (M1038): Block execution of code on a system through application control and/or script blocking.
- Restrict File and Directory Permissions (M1022): Restrict access by setting directory and file permissions that are not specific to users or privileged accounts.
- Filter Network Traffic (M1037): Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic. Perform inline allow/denylisting of network messages based on the application layer (OSI Layer 7) protocol, especially for automation protocols. Application allowlists are beneficial when well-defined communication sequences, types, rates, or patterns are needed during expected system operations. Application denylists may be needed if all acceptable communication sequences cannot be defined, but instead a set of known malicious uses can be denied (e.g., excessive communication attempts, shutdown messages, invalid commands). Devices performing these functions are often referred to as deep-packet inspection (DPI) firewalls, context-aware firewalls, or firewalls blocking specific automation/SCADA protocol-aware firewalls.
- Restrict Web-Based Content (M1021): Restrict use of certain websites, block downloads/attachments, block JavaScript, restrict browser extensions, etc.

Related Detection Signatures in ConnectWise SIEM

- [CRU][Windows] LOLBin extexport.exe Possible Malicious DLL Execution
- [CRU][Windows] LOLBin odbcconf.exe DLL Loading
- [CRU][Windows] regsvr32 Registering DLL From Suspicious Directory
- [CRU][Windows] BitsAdmin File Download or Persistence
- [CRU][Windows] LOLBin MpCmdRun.exe Arbitrary File Download
- [CRU][Windows] regsvr32 Used To Run Script From Remote Source
- [CRU][Windows] LOLBin Ieexec.exe Arbitrary File Download
- [CRU][Windows] Fsutil Suspicious Invocation
- [CRU][Windows] Likely Qakbot Command Line Execution
- [CRU][Windows] control.exe Creating Suspicious .cpl or .inf Files in AppData
- [CRU][Windows] msdt.exe Creating Files in Non-Standard Paths
- [CRU][Windows] Powershell Execution via Powershdll
- [CRU][Windows] Creation/Modification of Assistive Technology (AT) Applications
- [CRU][Windows] LOLBin HTML Help Proxy Execution
- [CRU][Windows] regsvr32 Launched By mshta
- [CRU][Windows] LOLBin mavinject.exe Injecting DLL into Arbitrary Process
- [CRU][Windows] Microsoft Office Application Running regsvr32.exe

- [CRU][Windows] regsvr32 Launching wscript
- [CRU][Windows] LOLBin cmstp.exe Silent Install of Local .INF
- [CRU][Windows] LOLBin Control_RunDLL DLL Call
- [CRU][Windows] regsvr32.exe Usage From a Mounted Directory Path
- [CRU][Windows] LOLBin Diskshadow.exe Proxy Execution
- [CRU][Windows] Microsoft Office Applications Launching rundll32, msiexec, verclsid or control.exe
- [CRU][Windows] Raspberry Robin Campaign
- [CRU][Windows] Use of Wuauclt.exe to Proxy Execute Code
- [CRU][Windows] Possible Injection rundll32 Launching explorer.exe
- [CRU][Windows] UAC Bypass via CMSTP.exe
- [CRU][Windows] Finger.exe Suspicious Invocation
- [CRU][Windows] LOLBin Application Launched via pcwutl.dll
- [CRU][Windows] Potential Evasion via Filter Manager
- [CRU][Windows] Network Connection via Compiled HTML File
- [CRU][Windows] Non-Typical Rundll32 Execution With Numbered Entry Point
- [CRU][Windows] Potential UAC Bypass
- [CRU][Windows] LOLBin InstallUtil.exe AWL bypass
- [CRU][Windows] Emotet (Operation Reacharound) Rundll.exe Activity
- [CRU][Windows] Suspicious mshta Proxy Execution
- [CRU][Windows] LOLBin Atbroker.exe Running Unusual Executable
- [CRU][Windows] Equation Group DLL_U Load
- [CRU][Windows] RemcosRat Process Injection
- [CRU][Windows] LOLBin Suspicious Esentutl.exe File Copies
- [CRU][Windows] LOLBin ShellExec_RunDLL launching an Exectuable
- [CRU][Windows] LOLBin SyncAppvPublishingServer.exe Proxy Execution
- [CRU][Windows] cmdl32.exe usage observed. (Suspicious)
- [CRU][Windows] Abusing Findstr for Defense Evasion
- [CRU][Windows] Microsoft Office Application Launching an HTML Application via mshta
- [CRU][Windows] Cobalt Strike Password Dump File Written to Disk
- [CRU][Windows] ShimCache Flushed
- [CRU][Windows] LPE InstallerFileTakeOver PoC CVE-2021–41379
- [CRU][Windows] LOLBin ScriptRunner.exe Proxy Execution
- [CRU][Windows] – Windows MSI installer via Powershell or Cmd – Possible AlwaysInstallElevated privesc
- [CRU][Windows] MS Diagnostic Tool Launched from Microsoft Office Application – Potential RCE
- [CRU][Windows] Use of WorkFolders.exe to execute control.exe
- [CRU][Windows] LOLBin runexehelper.exe
- [CRU][Windows] PowerShell Process Launched by mshta.exe
- [CRU][Windows] Bitsadmin transfer from remote server
- [CRU][Windows] MsiExec Install From Remote Source
- [CRU][Windows] Suspicious Powershell and mshta Activity

4. MITRE ATT&CK Technique T1202: Indirect Command Execution

Adversaries may abuse utilities that allow for command execution to bypass security restrictions that limit the use of command-line interpreters. Various Windows utilities may be used to execute commands, possibly without invoking [cmd]. For example, [Forfiles], the Program Compatibility Assistant (pcalua.exe), components of the Windows Subsystem for Linux (WSL), as well as other utilities may invoke the execution of programs and commands from a [Command and Scripting Interpreter], Run window, or via scripts.

Adversaries may abuse these features for [Defense Evasion], specifically to perform arbitrary execution while subverting detections and/or mitigation controls (such as Group Policy) that limit/prevent the usage of [cmd] or file extensions more commonly associated with malicious payloads.

General Detection Guidance

Monitor and analyze logs from host-based detection mechanisms, such as Sysmon, for events such as process creations that include or are resulting from parameters associated with invoking programs/commands/files and/or spawning child processes/network connections.

Mitigation Guidance

- **Indirect Command Execution Mitigation**: Identify or block potentially malicious software that may contain abusive functionality by using safelist tools such as AppLocker or Software Restriction Policies where appropriate. These mechanisms can also be used to disable and/or limit user access to Windows utilities and file types/locations used to invoke malicious execution.

Related Detection Signatures in ConnectWise SIEM

- [CRU][Windows] LOLBin ScriptRunner.exe Proxy Execution
- [CRU][Windows] LOLBin ftp.exe Running A Script File
- [CRU][Windows] LOLBin Diskshadow.exe Execution
- [CRU][Windows] Microsoft Office Application Executing Script Via wscript
- [CRU][Windows] Possible SyncAppvPublishing Exploitation
- [CRU][Windows] Use of Forfiles to run an executable file
- CRU][Windows] Microsoft Office Application Executing Command via bash.exe or sh.exe

5. MITRE ATT&CK Technique T1055: Process Injection

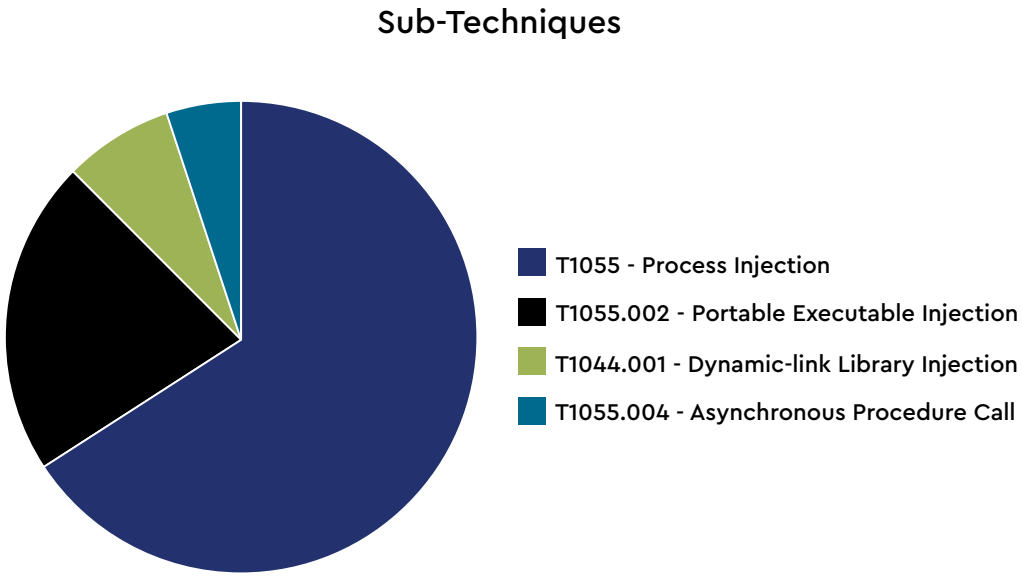


Figure 1.3: MITRE ATT&CK(C) Sub-techniques under the Technique T1055: Process Injection observed in the 440,000 security incidents reviewed by the CRU in 2022

Adversaries may inject code into processes 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.

There are many different ways to inject code into a process, and several abuse legitimate functionalities. These implementations exist for every major OS but are typically platform-specific.

More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

General Detection Guidance

Monitoring Windows API calls indicative of the various types of code injection may generate a significant amount of data. This may not be directly useful for defense unless collected under specific circumstances for known bad sequences of calls because benign use of API functions may be common and difficult to distinguish from malicious behavior, including Windows API calls such as:

Windows API calls such as:

- CreateRemoteThread
- ResumeThread
- SuspendThread
- QueueUserAPC
- SetThreadContext
- NtQueueApcThread

and those that can be used to modify memory within another process, such as:

- VirtualAllocEx
- WriteProcessMemory

Monitor DLL/PE file events, specifically the creation of these binary files, as well as the loading of DLLs into processes. Look for DLLs that are not recognized or not normally loaded into a process.

Monitoring for Linux-specific calls, such as the uptrace system call, should not generate large amounts of data due to their specialized nature and can be a very effective method to detect some of the common process injection methods.

Monitor for named pipe creation and connection events (Event IDs 17 and 18) for possible indicators of infected processes with external modules.

Analyze process behavior to determine if a process is performing actions it usually does not, such as opening network connections, reading files, or other suspicious actions that could relate to post-compromise behavior.

Mitigation Guidance

- Privileged Account Management (M1026): Manage the creation, modification, use, and permissions associated to privileged accounts, including SYSTEM and root.
- Behavior Prevention on Endpoint (M1040): Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious processes, files, API calls, behaviors, etc.
- Restrict File and Directory Permissions (M1022): Restrict access by setting directory and file permissions that are not specific to users or privileged accounts.

Related Detection Signatures in ConnectWise SIEM

- [CRU][Windows] Common PowerShell Functionality Used by Cobalt Strike
- [CRU][Windows] RemcosRat Process Injection
- [CRU][Windows] Common Cobalt Strike rundll32 Entry Point
- [CRU][Windows] Powershell Reflective DLL Injection
- [CRU][Windows] Confluence Atlassian (CVE-2022-26134) RCE
- [CRU][Windows] Excessive Notepad.exe spawning from executable.
- [CRU][Windows] Possible Injection rundll32 Launching explorer.exe
- [CRU][Windows] API Imports Common For Process Hollowing in PowerShell Script
- [CRU][Windows] DLL Injection via LoadLibraryA and LoadLibraryW

6. MITRE ATT&CK Technique 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 will likely render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives. Common operating system file deletion commands such as del and rm often only remove pointers to files without wiping the contents of the files themselves, making the files recoverable by proper forensic methodology. This behavior is distinct from disk content wipe and disk structure wipe because individual files are destroyed rather than sections of a storage disk or the disk's logical structure.

Adversaries may attempt to overwrite files and directories with randomly generated data to make it irrecoverable. In some cases, politically oriented image files have been used to overwrite data.

To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware designed for destroying data may have worm-like features to propagate across a network by leveraging additional techniques like Valid Accounts, OS Credential Dumping, and SMB/Windows Admin Shares.

In cloud environments, adversaries may leverage access to delete cloud storage, cloud storage accounts, machine images, and other infrastructure crucial to operations to damage an organization or their customers.

General Detection Guidance

Use process monitoring to monitor the execution and command-line parameters of binaries that could be involved in data destruction activity, such as SDelete. Monitor for the creation of suspicious files and high unusual file modification activity. In particular, look for large quantities of file modifications in user directories and under C:\Windows\System32.

In cloud environments, the occurrence of anomalous high-volume deletion events, such as the DeleteDBCluster and DeleteGlobalCluster events in AWS, or a high quantity of data deletion events, such as DeleteBucket, within a short time may indicate suspicious activity.

Mitigation Guidance

- Data Backup (M1053): Take and store data backups from end user systems and critical servers. Ensure backup and storage systems are hardened and kept separate from the corporate network to prevent compromise. Maintain and exercise incident response plans, including the management of "gold-copy" back up images and configurations for key systems to enable quick recovery and response from adversarial activities that impact control, view, or availability.
- Privileged Account Management (M1026): Manage the creation, modification, use, and permissions associated with privileged accounts, including SYSTEM and root.
- Restrict File and Directory Permissions (M1022): Restrict access by setting directory and file permissions that are not specific to users or privileged accounts.

- Data Destruction Mitigation: 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 are protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery.
- Identify potentially malicious software and audit and/or block it by using allowlisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Related Detection Signatures in ConnectWise SIEM

- [CRU][Windows] LOLBin diskshadow.exe Shadow Copy Deletion
- [CRU][Windows] WMI shadowcopy delete
- [CRU][Windows] vssadmin.exe Shadow Volume Deletion
- [CRU][Windows] Stealth Delete Shadow Volumes via VssAdmin COM API
- [CRU][Windows] Backup Deletion via wbadmin.exe
- [CRU][Windows] Suspicious WMI spawning Powershell to Remove Files

7. MITRE ATT&CK Technique T1486: Data Encrypted for Impact

Adversaries may encrypt data on target systems or 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. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.

In the case of ransomware, it is typical that common user files such as Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification] or [System Shutdown/Reboot], in order to unlock and/or gain access to manipulate these files. In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.

To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts], [OS Credential Dumping], and [SMB/Windows Admin Shares]. Encryption malware may also leverage [Internal Defacement], such as changing victim wallpapers or otherwise intimidating victims by sending ransom notes or other messages to connected printers (known as "print bombing").

In cloud environments, storage objects within compromised accounts may also be encrypted.

General Detection Guidance

Use process monitoring to monitor the execution and command line parameters of binaries involved in data destruction activity, such as vssadmin, wbadmin, and bcdedit. Monitor for the creation of suspicious files and unusual file modification activity. In particular, look for large quantities of file modifications in user directories.

In some cases, monitoring for unusual kernel driver installation activity can aid in detection.

In cloud environments, monitor for events that indicate storage objects have been anomalously replaced by copies.

Mitigation Guidance

- Consider implementing IT disaster recovery plans that contain procedures for regularly taking and testing data backups that can be used to restore organizational data.
    + In some cases, the means to decrypt files affected by a ransomware campaign is released to the public. Research trusted sources for public releases of decryptor tools/keys to reverse the effects of ransomware.
    + Identify potentially malicious software and audit and/or block it by using safelist tools, such as AppLocker or Software Restriction Policies where appropriate.
- Data Backup (M1053): Take and store data backups from end user systems and critical servers. Ensure backup and storage systems are hardened and kept separate from the corporate network to prevent compromise. Maintain and exercise incident response plans, including the management of "gold-copy" back up images and configurations for key systems to enable quick recovery and response from adversarial activities that impact control, view, or availability.
- Behavior Prevention on Endpoint (M1040): Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious

Related Detection Signatures in ConnectWise SIEM

- [CRU][Windows] Suspicious Bitlocker Key Activity
- [CRU][Windows] Quantum Locker Extension
- [CRU][Windows] Conti Ransomware Execution
- [CRU][Windows] LockerGoga Ransomware

8. MITRE ATT&CK Technique T1078: Valid Accounts

Adversaries may obtain and abuse credentials of existing accounts to gain initial access, persistence, privilege escalation, or defense evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity on the account.

The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.

General Detection Guidance

Configure robust, consistent account activity audit policies across the enterprise and with externally accessible services. Look for suspicious account behavior across systems that share accounts, either user, admin, or service accounts. Examples: one account logged into multiple systems simultaneously; multiple accounts logged into the same machine simultaneously; accounts logged in at odd times or outside of business hours. Activity may be from interactive login sessions or process ownership from accounts being used to execute binaries on a remote system as a particular account. Correlate other security systems with login information (e.g., a user has an active login session but has not entered the building or does not have VPN access).

Perform regular audits of domain and local system accounts to detect accounts that may have been created by an adversary for persistence. Checks on these accounts could also include whether default accounts such as Guest have been activated. These audits should also include checks on any appliances and applications for default credentials or SSH keys, and if any are discovered, they should be updated immediately.

Mitigation Guidance

- Take measures to detect or prevent techniques such as [OS Credential Dumping] or installation of keyloggers to acquire credentials through [Input Capture]. Limit credential overlap across systems to prevent access if account credentials are obtained. Ensure that local administrator accounts have complex, unique passwords across all systems on the network. Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled and account use is segmented, 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. 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 been authorized.
- Applications and appliances that use 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.
- Password Policies (M1027): Set and enforce secure password policies for accounts.
- Application Developer Guidance (M1013): This mitigation describes any guidance or training given to developers of applications to avoid introducing security weaknesses that an adversary may be able to take advantage of.
- User Training (M1017): Train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spearphishing, social engineering, and other techniques that involve user interaction.
- User Account Management (M1018): Manage the creation, modification, use, and permissions associated to user accounts.

- Privileged Account Management (M1026): Manage the creation, modification, use, and permissions associated to privileged accounts, including SYSTEM and root.
- Multi-factor Authentication (M1032): Use two or more pieces of evidence to authenticate to a system, such as username and password in addition to a token from a physical smart card or token generator. Within industrial control environments assets such as low-level controllers, workstations, and HMIs have real-time operational control and safety requirements which may restrict the use of multi-factor.

Related Detection Signatures in ConnectWise SIEM

- [O365] Risk Detection: New Country (Azure P2 Required)
- Windows: Excessive logon failures for user
- [AWS] Root Account Used for Non-Service Event
- [AWS] AWS Root Login Without MFA
- [Okta] User Session Impersonation
- [O365] Impossible Travel Alert
- Windows: Excessive NTLM logon failures for user
- [AWS] AWS IAM Password Recovery Requested
- O365 Alert: Disabled account login attempt
- [Okta] Suspicious Activity Reported by Okta User
- O365 Alert: Excessive Login Failures for User
- Windows: Successful Remote or Local Interactive Administrator Logon
- [AWS] AWS SAML Activity
- [AWS] AWS Management Console Root Login
- [CRU][Windows] Adding Default User account to groups
- Windows: Excessive Remote Interactive logon failures for user
- [AWS] AWS IAM Assume Role Policy Update
- [Okta] High Number of Okta User Password Reset or Unlock Attempts
- O365 Alert: User Failed MFA

9. MITRE ATT&CK Technique T1480: Execution Guardrails

Adversaries may use execution guardrails to constrain execution or actions based on adversary-supplied and environment-specific conditions that are expected to be present on the target. Guardrails ensure that a payload only executes against an intended target and reduces collateral damage from an adversary's campaign. Values an adversary can provide about a target system or environment to use as guardrails may include specific network share names, attached physical devices, files, joined $ (AD) domains, and local/external IP addresses.

Guardrails can be used to prevent exposure of capabilities in environments that are not intended to be compromised or operated within. This use of guardrails is distinct from typical [Virtualization/Sandbox Evasion]. While use of [Virtualization/Sandbox Evasion] may involve checking for known sandbox values and continuing with execution only if there is no match, the use of guardrails will involve checking for an expected target-specific value and only continuing with execution if there is such a match.

General Detection Guidance

Detecting the use of guardrails may be difficult depending on the implementation. Monitoring for suspicious processes being spawned that gather a variety of system information or perform other forms of [Discovery], especially in a short period of time, may aid in detection.

Mitigation Guidance

Execution Guardrails Mitigation: This technique likely should not be mitigated with preventative controls because it may protect unintended targets from being compromised. If targeted, efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior if compromised.

10. MITRE ATT&CK Technique T1059: Command and Scripting Interpreter

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities; for example, macOS and Linux distributions include some flavor of Unix Shell, while Windows installations include the Windows Command Shell and PowerShell.

There are also cross-platform interpreters such as Python, as well as those commonly associated with client applications such as JavaScript and Visual Basic. Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in Initial Access payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various remote services in order to achieve remote execution.

General Detection Guidance

Command-line and scripting activities can be captured through proper logging of process execution with command-line arguments. This information can be useful in gaining additional insight into adversaries' actions through how they use native processes or custom tools. Also monitor for loading of modules associated with specific languages.

If scripting is restricted for normal users, then any attempt to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent.

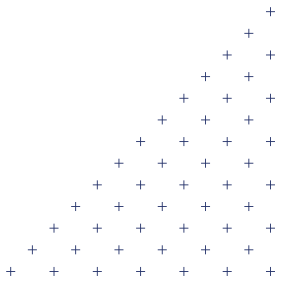
Scripts are likely to perform actions with various effects on a system that may generate events, depending on the types of monitoring used. Monitor processes and command-line arguments for script execution and subsequent behavior. Actions may be related to network and system information discovery, collection, or other scriptable post-compromise behaviors and could be used as indicators of detection leading back to the source script.

Mitigation Guidance

- Execution Prevention (M1038): Block execution of code on a system through application control and/or script blocking.
- Disable or Remove Feature or Program (M1042): Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.
- Behavior Prevention on Endpoint (M1040): Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious processes, files, API calls, behaviors, etc.
- Privileged Account Management (M1026): Manage the creation, modification, use, and permissions associated with privileged accounts, including SYSTEM and root.
- Antivirus/Antimalware (M1049): Use signatures or heuristics to detect malicious software. Within industrial control environments, antivirus/antimalware installations should be limited to assets that are not involved in critical or real-time operations. To minimize the impact on system availability, all products should first be validated within a representative test environment before deployment to production systems.
- Restrict Web-Based Content (M1021): Restrict use of certain websites, block downloads/attachments, block JavaScript, restrict browser extensions, etc.
- Code Signing (M1045): Enforce binary and application integrity with digital signature verification to prevent untrusted code from executing.

Related Detection Signatures in ConnectWise SIEM

- [CRU][Windows] Powershell Execution via Powershell
- [CRU][Windows] mshta.exe Executing Script Commands
- [CRU][Windows] Command Launched from WinLogon
- [CRU][Windows] Cmd or Powershell Process Created From 7zip
- [CRU][Windows] Powershell Executed with Truncated Parameters
- [CRU][Windows] Powershell Persistence in Registry
- [CRU][Windows] Suspicious mshta Proxy Execution
- [CRU][Windows] Script Run from Archive File (.zip, .7z, .iso) via wscript.exe
- [CRU][Windows] Suspicious WMI spawning Powershell to Remove Files
- [CRU][Windows] Evasive Jscript Code Execution via cscript.exe
- [CRU][Windows] Atera RMM Agent Running Cmd or PowerShell
- [CRU][Windows] Suspicious w3wp.exe running as parent to Powershell or cmd that is running child command processes



Chapter 2: Cyberwarfare in the Russia-Ukraine War

Russia used cyberwarfare techniques against Ukraine before the physical conflict began in February 2022. Since then, cyberwarfare has continued to escalate. Considering this, what threats do MSPs and their clients realistically face? Below we summarize actions already taken by Russian state-sponsored threat actors and provide some information on what can be expected going forward.

Early Cyber Attack Targeting Ukraine

Beginning January 13, 2022, Microsoft Threat Intelligence Center (MSTIC) began observing samples of new destructive malware operations (dubbed WhisperGate) targeting multiple Ukrainian organizations. This malware operates in two stages:

- **Stage 1** overwrites the master boot record (MBR) of a hard drive with a ransom note that includes a Bitcoin address and a Tox ID (Tox is an encrypted messaging protocol). When the system reboots, the ransom note is displayed.
- **Stage 2** locates common file types likely to contain user data and overwrites them. Since the WhisperGate malware overwrites rather than encrypts data, the data is not recoverable even if the ransom is paid.

On January 14, 2022, threat actors attempted to deface nearly 70 Ukrainian government websites, including sites for the Ukrainian Ministry of Foreign Affairs, Ministry of Defense, the State Emergency Service, and others. They only managed to deface 10 and left vague messages to "wait for the worst."

This activity has been attributed to UNC1151, a threat actor group believed to be linked to Belarusian intelligence, and it's also believed to be associated with the Russian special services. Messages left on the government sites appear to be attempts at creating dissent between native Ukrainian and the Polish minority.

On February 15, 2022, a large-scale DDoS attack targeted Ukraine's armed forces, defense ministry, public radio, and the two largest banks for about several hours. The attack brought several vital services offline and left many Ukrainians unable to access their bank accounts, use mobile apps, or issue online payments. During the DDoS attack, users of Privatbank, one of those targeted by the attack, reported receiving alerts from the bank that their ATMs were not working. According to Privatbank, they did not send these messages, and Ukrainian cyber police stated that "it was an information attack."

Ongoing Cyberattacks

The cyberattacks continued after the physical attacks began. Microsoft released a report in April 2022 that discussed details regarding nearly 40 cyberattacks believed to be launched by Russian intelligence organizations against the Ukrainian government and other targets. According to the report, more than 40% were destructive attacks targeting critical infrastructure. Most of the cyber activity related to the war has involved data-destroying attacks that look like ransomware or DDoS attacks.

In September 2022, the Google Threat Analysis Group (TAG) released a report detailing five financially motivated campaigns conducted between April and August 2022 by UAC-0098. Based on their research, they believe UAC-0098 is backed by the Russian government, and several members of UAC-0098 are former members of Conti.

Hacktivism

Cyberwarfare between Russia and Ukraine has expanded beyond the efforts of intelligence services. Multiple APTs and hacktivist groups are taking sides and working to undermine governments and businesses on both sides. A researcher going by the name of CyberKnow has been actively tracking groups that have involved themselves in this conflict, and they are currently tracking 200 groups.

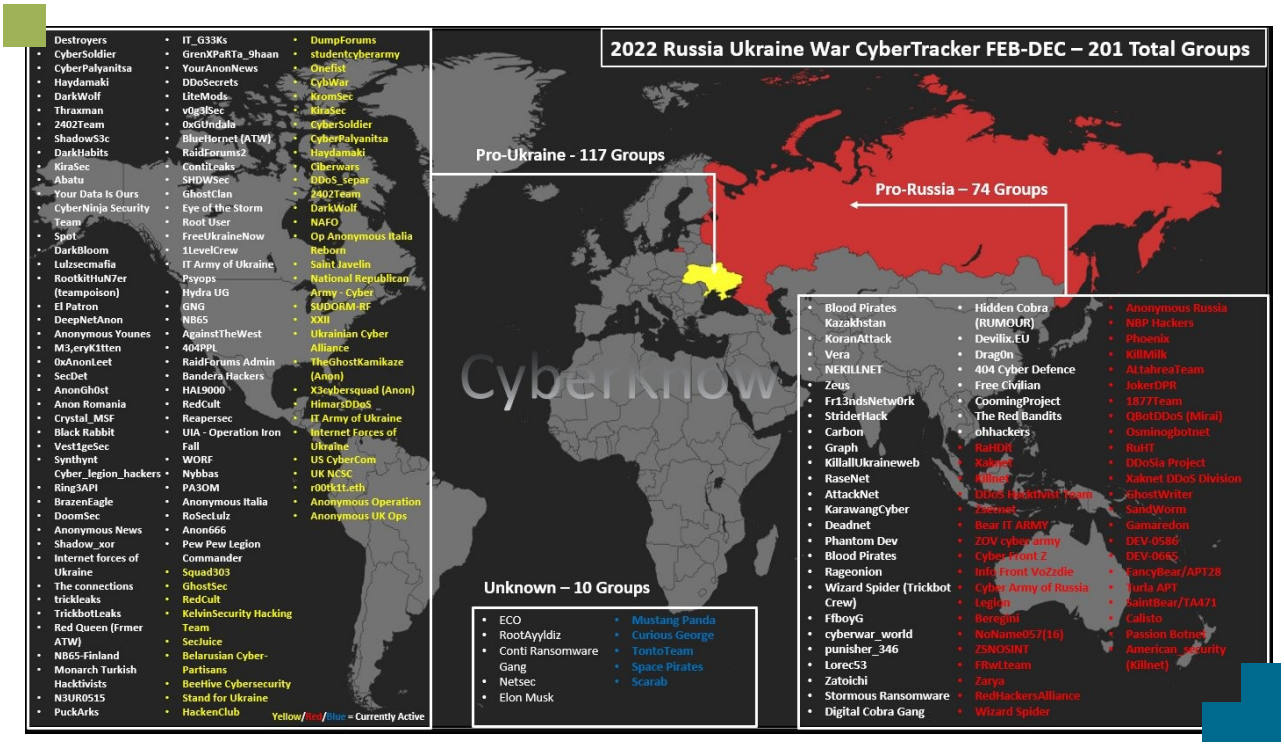


Image source: https://twitter.com/Cyberknow20/status/1604805201885417472/photo/1

Much of the activity has involved web defacement, DDoS attacks, and classified data theft and leaks.

Conti leaks

Conti emerged during the war as a large ransomware-as-a-service (RaaS) organization believed to be supported by Russian intelligence. The group publicly came out in support of Russia once the conflict began. Below are screenshots taken from their data leaks site on the dark web:

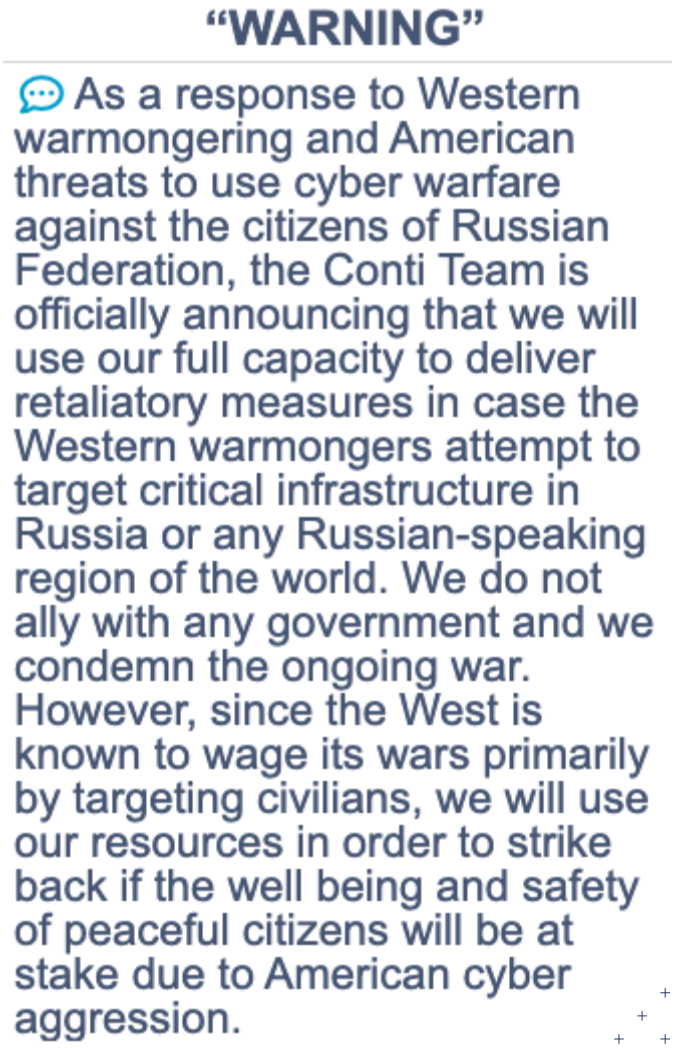


Figure 2.0: Message posted on Conti's darknet data leaks site

In response to this proclamation, on February 27, 2022, a new Twitter account, Contileaks, posted links to archived chat messages taken from Conti's private communications going back to January 2021. The owner of the ContiLeaks Twitter account is believed to be a Ukrainian security researcher. The leaks show a surprisingly professional organization with employees holding specific positions such as administrators, reverse engineers, and penetration testers/hackers, with more than 60 people on staff. KrebsonSecurity's has a breakdown with full details.

These events led to a decline in Conti's success, and they soon began slowly dismantling their organization. While ransomware groups come and go on a regular basis, Conti's shutdown was slow and organized as the group began splitting itself up by joining other groups and redistributing their assets. AdvIntel provides an in-depth analysis of the discontinuation of Conti.

Vulnerabilities Commonly Exploited by Russian State-Sponsored APTs

Below is a list of vulnerabilities commonly exploited by Russian state-sponsored APTs, according to a report by the Cybersecurity and Infrastructure Security Agency (CISA). Detection signatures for all these vulnerabilities are available for all ConnectWise SIEM IDS customers in the "Emerging Threats" and "ConnectWise SIEM Users" communities. Both communities are enabled by default for all ConnectWise SIEM IDS customers. We recommend an audit of your systems and your clients' systems for the vulnerabilities below, especially for organizations related to critical infrastructure, government, defense contractors, and financial institutions. This is not meant to be a comprehensive list of all methods these threat actors might use; it's intended to be a guide to help focus attention on where to start.

- CVE-2018-13379 FortiGate VPNs
- CVE-2019-1653 Cisco router
- CVE-2019-2725 Oracle WebLogic Server
- CVE-2019-7609 Kibana
- CVE-2019-9670 Zimbra software
- CVE-2019-10149 Exim Simple Mail Transfer Protocol
- CVE-2019-11510 Pulse Secure
- CVE-2019-19781 Citrix
- CVE-2020-0688 Microsoft Exchange
- CVE-2020-4006 VMWare (note: this was a zero-day at time.)
- CVE-2020-5902 F5 Big-IP
- CVE-2020-14882 Oracle WebLogic
- CVE-2021-26855 Microsoft Exchange
  (Note: this vulnerability is frequently observed used in conjunction with CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065).

Malware Used in the Russia-Ukraine War

January 4, 2021

Industroyer – [Industroyer] is a sophisticated malware framework designed to cause an impact to the working processes of Industrial Control Systems (ICS), specifically components used in electrical substations. [Industroyer] was used in the attacks on the Ukrainian power grid in December 2016. This is the first publicly known malware specifically designed to target and impact operations in the electric grid.

Febuary 23, 2022

PartyTicket – PartyTicket is a Go-written ransomware, which was described as a poorly designed one by Zscaler. According to Brett Stone-Gross this malware is likely intended to be a diversion from the Hermetic wiper (aka. KillDisk.NCV, DriveSlayer) attack.

Febuary 24, 2022

GraphSteel – This malware was seen during the cyberattacks on Ukrainian state organizations. It is one of two used backdoors written in Go and attributed to UAC-0056 (SaintBear, UNC2589, TA471).

March 3, 2022

CyclopsBlink – According to CISA, Cyclops Blink appears to be a replacement framework for the VPNFilter malware exposed in 2018, and which exploited network devices, primarily small office/home office (SOHO) routers and network attached storage (NAS) devices. Cyclops Blink has been deployed since at least June 2019, fourteen months after VPNFilter was disrupted. In common with VPNFilter, Cyclops Blink deployment also appears indiscriminate and widespread. The actor has so far primarily deployed Cyclops Blink to WatchGuard and ASUS devices, but it is likely that Sandworm would be capable of compiling the malware for other architectures and firmware.

September 6, 2021

Mars Stealer – 3xp0rt describes Mars Stealer as an improved successor of Oski Stealer, supporting stealing from current browsers and targeting crypto currencies and 2FA plugins.

September 6, 2021

MicroBackdoor – Open-source lightweight backdoor for C2 communication.

Febuary 24, 2022

GrimPlant – This malware was seen during the cyberattacks on Ukrainian state organizations. It is one of two used backdoors written in Go and attributed to UAC-0056 (SaintBear, UNC2589, TA471).

Febuary 24, 2022

Issac Wiper – Issac Wiper malware observed during the Russia-Ukraine war.

Febuary 24, 2022

SunSeed – According to Proofpoint, this is a Lua-based malware likely used by a nation-state sponsored attacker used to target European government personnel involved in managing the logistics of refugees fleeing Ukraine.

March 1, 2022

RURansom – RURansom shows characteristics of typical ransomware, but despite its name, TrendMicro's assumptions after analysis showed that this malware is more a wiper than ransomware, because the irreversible destruction of encrypted files.

March 10, 2022

WhisperGate – [WhisperGate] is a multi-stage wiper designed to look like ransomware that has been used in attacks against Ukraine since at least January 2022.

March 17, 2022

DoubleZero – A wiper identified by CERT-UA, written in C#.

March 18, 2022

LoadEdge – LoadEdge is a malicious backdoor program developed using the C++ programming language.

March 23, 2022

CaddyWiper – [CaddyWiper] is a destructive data wiper that has been used in attacks against organizations in Ukraine since at least March 2022.

March 25, 2022

DesertBlade – According to Microsoft, this was used in a limited destructive malware attack in early March 2022 impacting a single Ukrainian entity. DesertBlade is responsible for iteratively overwriting and then deleting overwritten files on all accessible drives (sparing the system if it is a domain controller).

March 25, 2022

HermeticWiper – [HermeticWiper] is a data wiper that has been used since at least early 2022, primarily against Ukraine with additional activity observed in Latvia and Lithuania. Some sectors targeted include government, financial, defense, aviation, and IT services.

May 6, 2022

Jester Stealer – Jester Stealer is a backdoor that enables the theft of authentication and other data from Internet browsers, MAIL/FTP/VPN clients, cryptocurrency wallets, password managers, messengers, game programs, etc. Jester Stealer may be related to Eternity Stealer and DynamicStealer.

August 25, 2022

AcidRain – A MIPS ELF binary with wiper functionality used against Viasat KA-SAT modems.

September 6, 2022

CredoMap – CredoMap is a password-stealing banking trojan.

Impact to MSPs

Based on the activity so far, Russian state sponsored APTs have been focused on defense contractors, critical infrastructure (such as internet infrastructure or the power grid), government, and banking targets. MSPs with these client types should review the information below regarding the common vulnerabilities, tactics, and techniques used by Russian state sponsored APTs. We have also seen in recent years that MSPs are **increasingly directly targeted** by threat actors as these groups realize that MSPs are critical infrastructure and are a rich target for affecting multiple victims at once.

Chapter 3: 2022 Ransomware Incidents in Review

The CRU reviewed data from about 2,300 ransomware incidents in 2022, including data collected from our MSP partners and their clients and incidents reported by ransomware groups on their data leak sites. Below is a summary of that data:

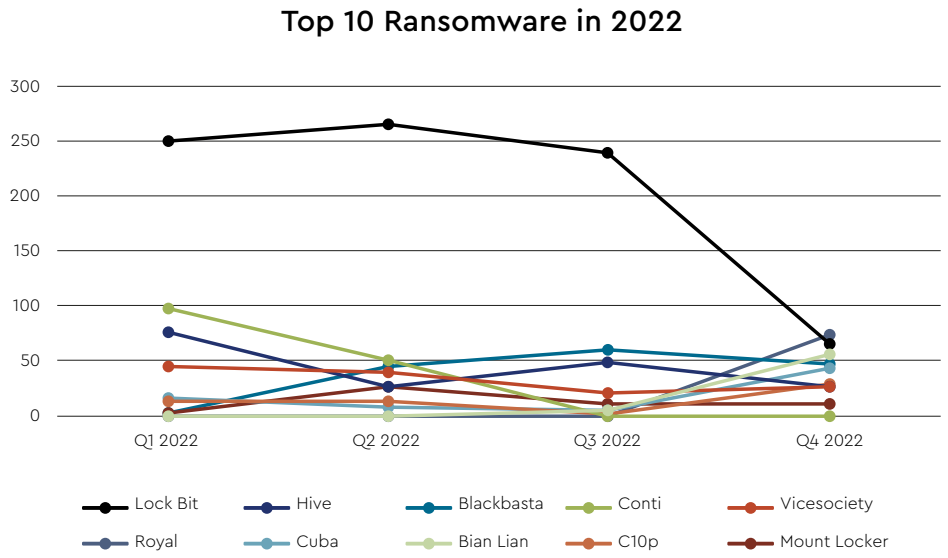


Figure 3.0: Number of ransomware incidents by ransomware per quarter in 2022

LockBit has by far been the most prevalent ransomware in use; however, there was a decline in LockBit ransomware incidents in the last quarter of the year. This could indicate a change in behavior for some of LockBit's affiliates. According to a publication from CISA, there was an increase in ransomware activity targeting healthcare in the latter part of 2022. LockBit has strict rules for its affiliates, banning them from targeting healthcare organizations.

In December 2022, a Toronto-based children's hospital was the victim of a ransomware attack from one of LockBit's affiliates using LockBit. The LockBit organization issued a public apology and offered a free decryptor to help restore systems impacted by their ransomware.

LockBit is still very active. In January 2023, they released a new version of their software dubbed "LockBit Green," which can target cloud-based services.

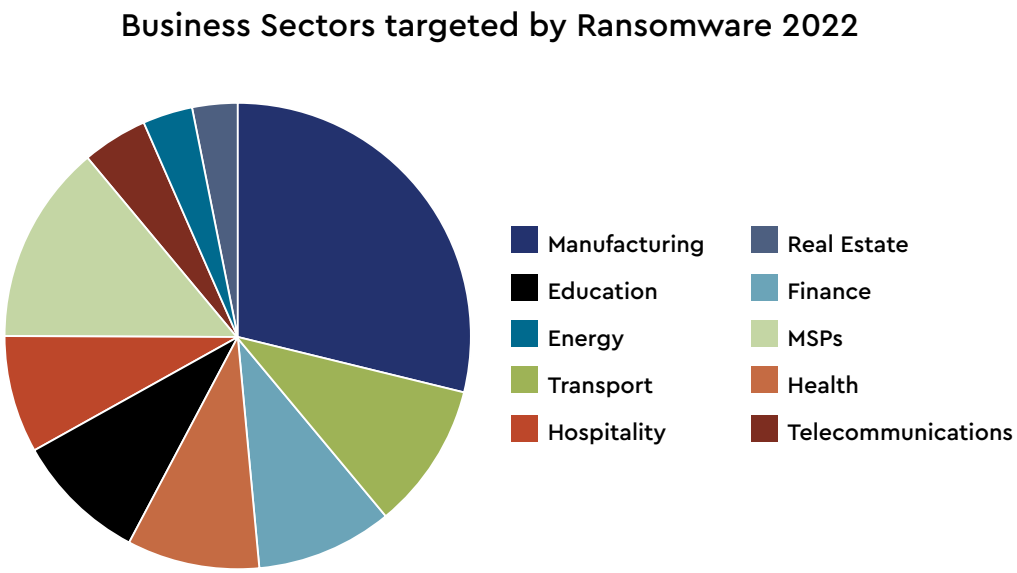


Figure 3.1: Business Sectors targeted by Ransomware 2022

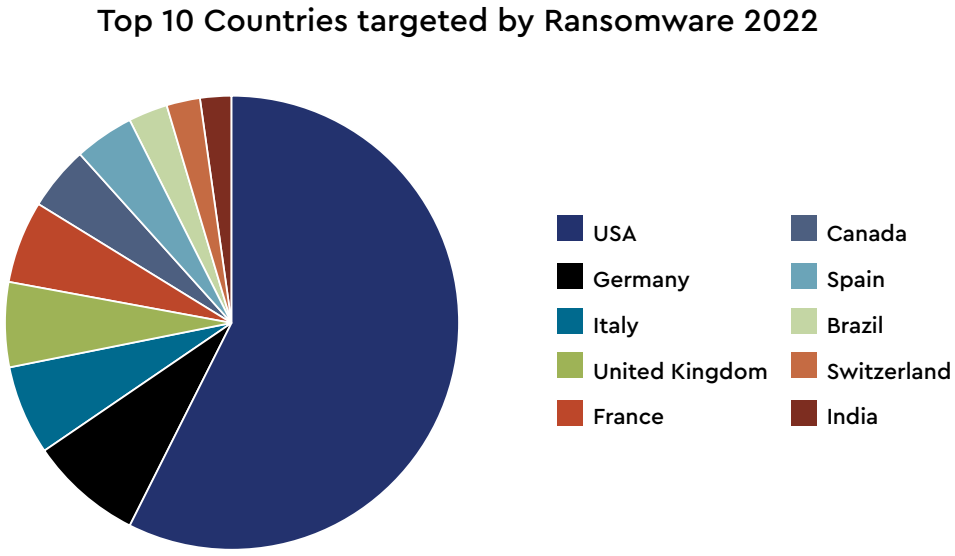


Figure 3.2: Top 10 Countries targeted by ransomware 2022

Ransomware Targeting MSPs in 2022

The CRU filtered all the ransomware incidents from above and took a closer look at ransomware specifically used to target MSPs directly. As we've mentioned in past MSP Threat Reports, MSPs can be a high-value target for threat actors as compromising one MSP can lead to subsequent compromises of their clients in an attack known as a Buffalo Jump. We examined the tactics, techniques, and procedures used in these ransomware attacks to help MSPs prioritize their defenses and keep their clients safe. The following is a breakdown of the top ransomware used in attacks targeting MSPs directly.

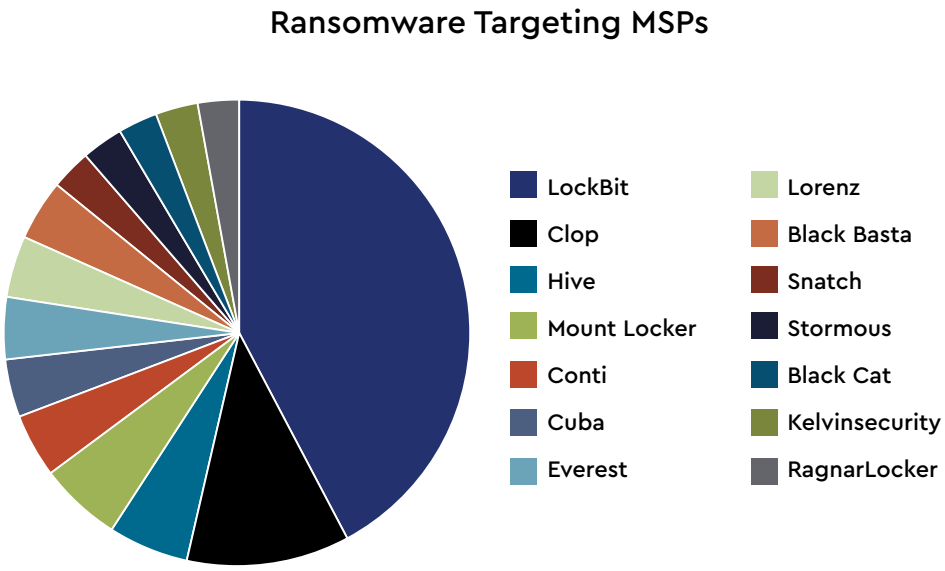


Figure 3.3: Breakdown of ransomware incidents of ransomware incidents specifically targeting MSPs in 2022 by ransomware

Breakdown of Top 5 Ransomware targeting MSPs

The following is a breakdown of the top five ransomware used in attacks directly targeting MSPs in 2022, including a brief description of each ransomware, countries targeted, and other sectors also targeted by the same ransomware.

LockBit/LuckyDay/LockBit 2.0/ ABCD

- 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
- Responsible for 42% of all ransomware incidents directly targeting MSPs in 2022

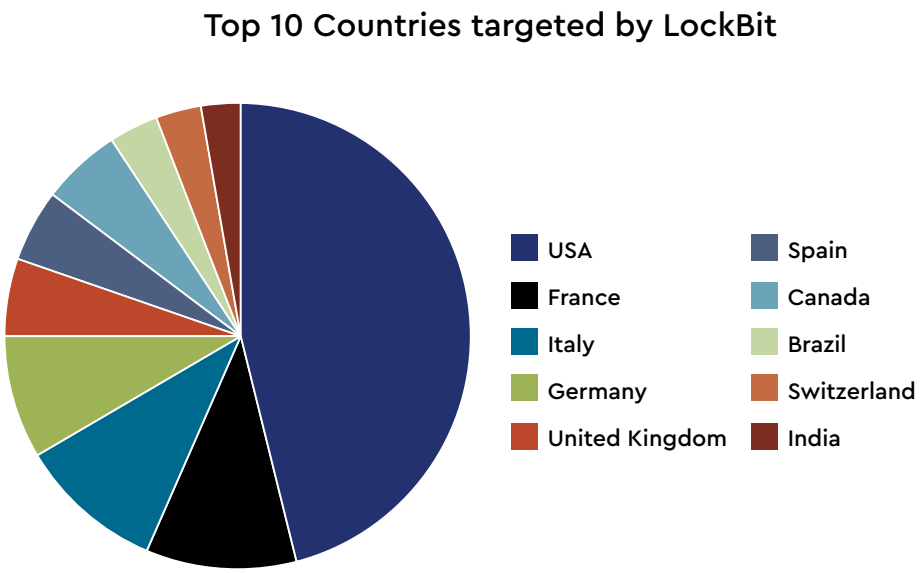


Figure 3.4: Top 10 Countries targeted by LockBit in 2022

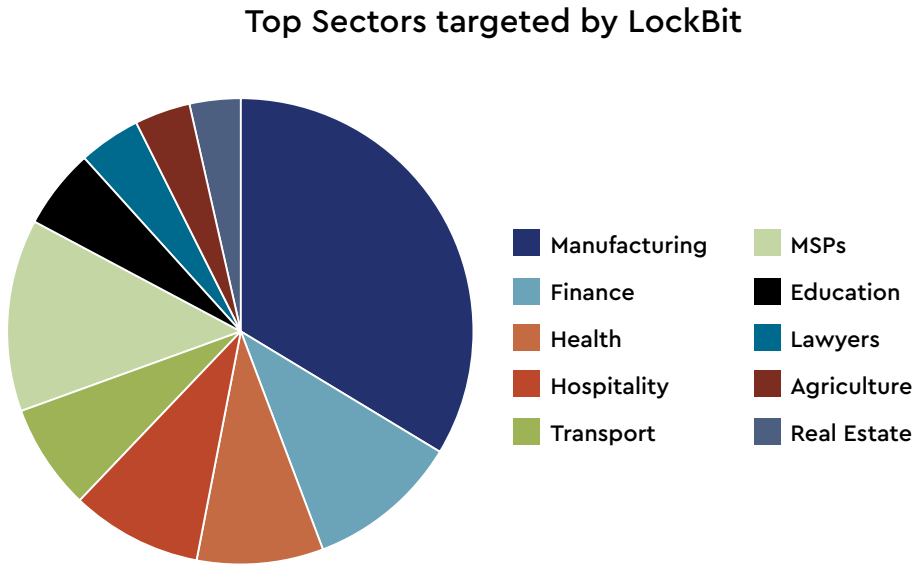


Figure 3.5: Top 10 business sectors targeted by LockBit in 2022

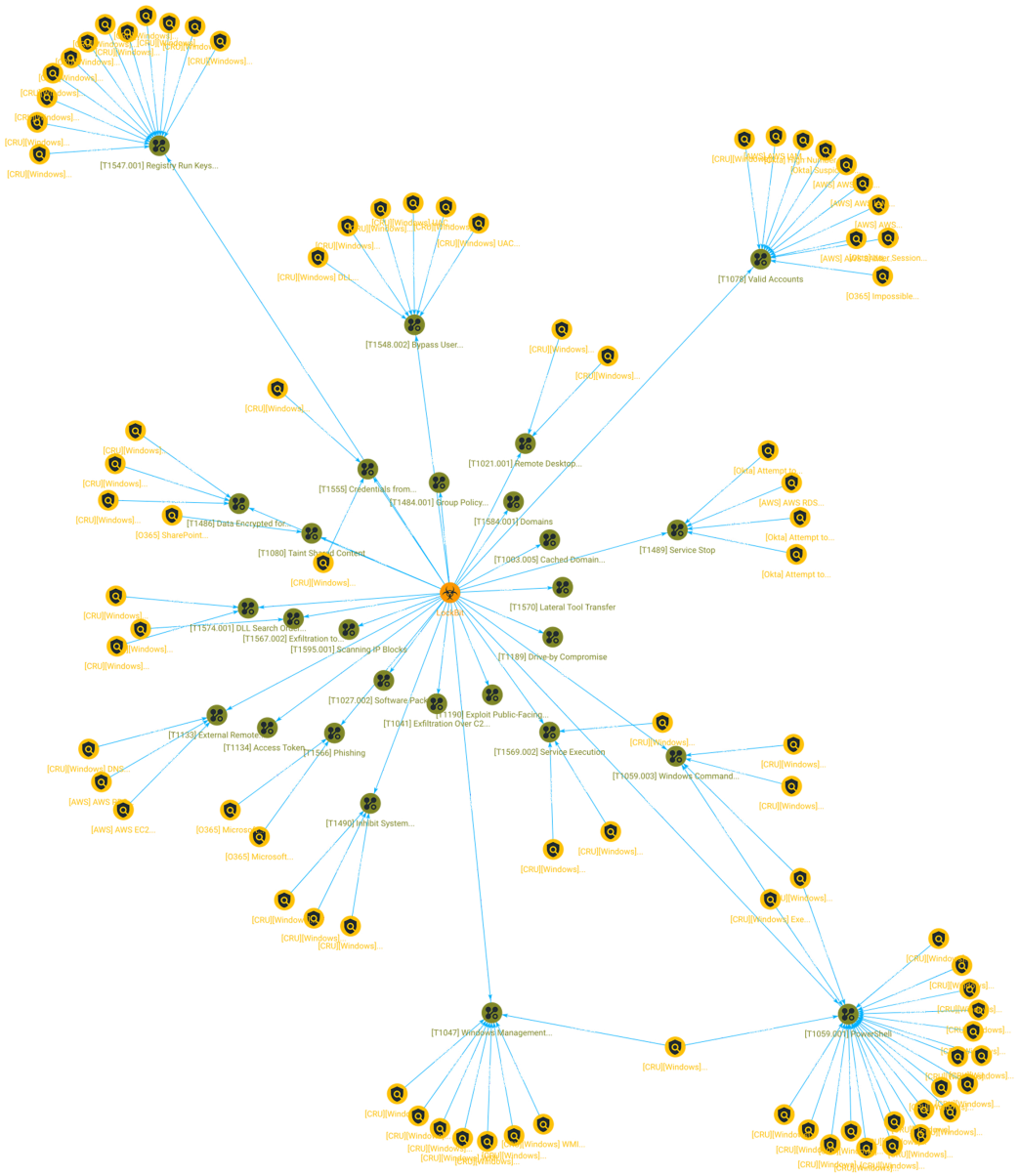


Figure 3.6: Illustration of LockBit techniques tied to ConnectWise SIEM detection signatures

Cl0p

- Variant of CryptoMix first observed in February 2019
- Uses signed executables
- Attempts to disable Windows Defender and remove the Microsoft Security Essentials to avoid user space detection
- Responsible for 11% of all ransomware incidents directly targeting MSPs in 2022

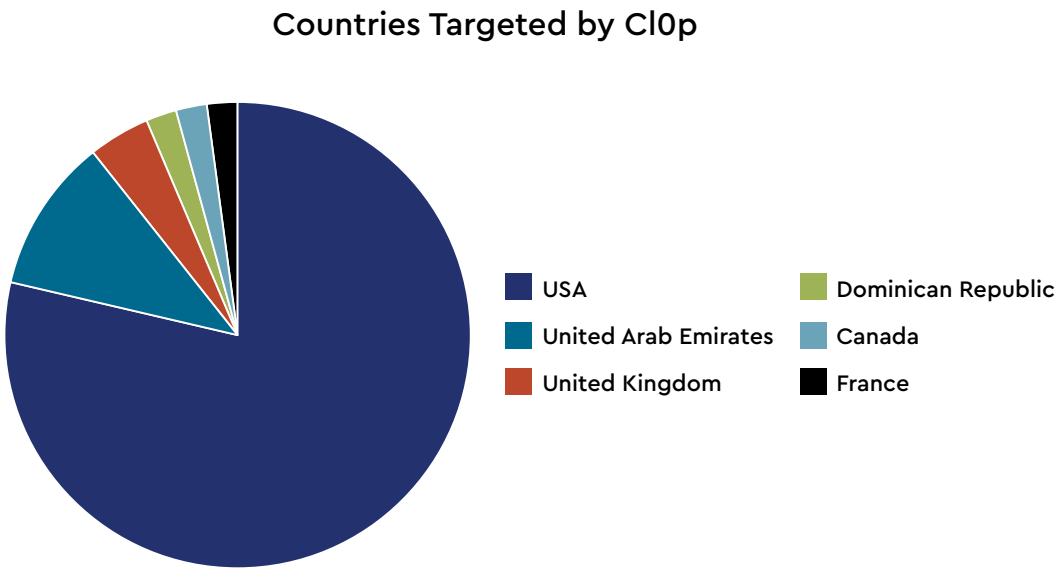


Figure 3.7: Countries targeted by Cl0p in 2022

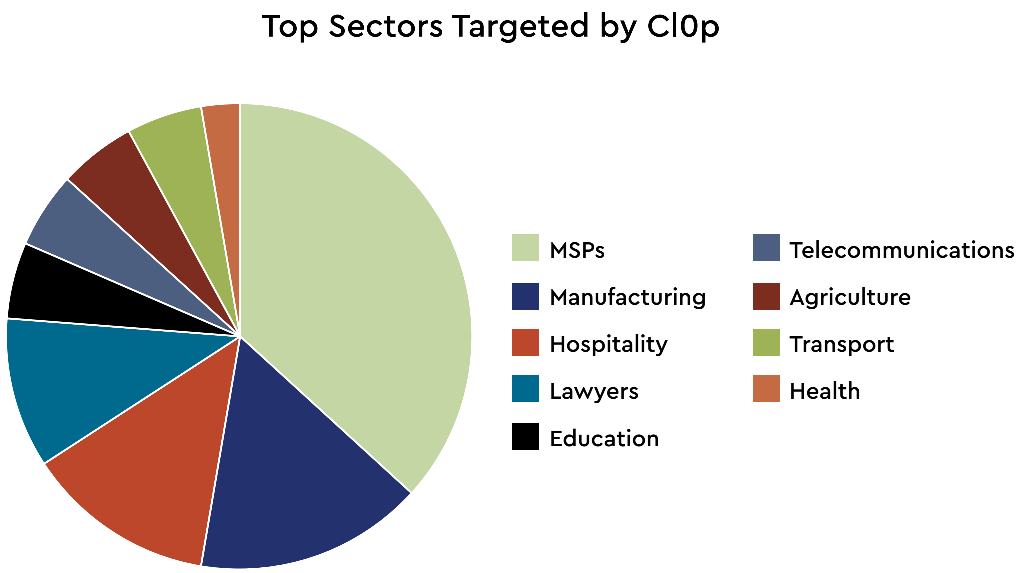


Figure 3.8: Business sectors targeted by Cl0p in 2022

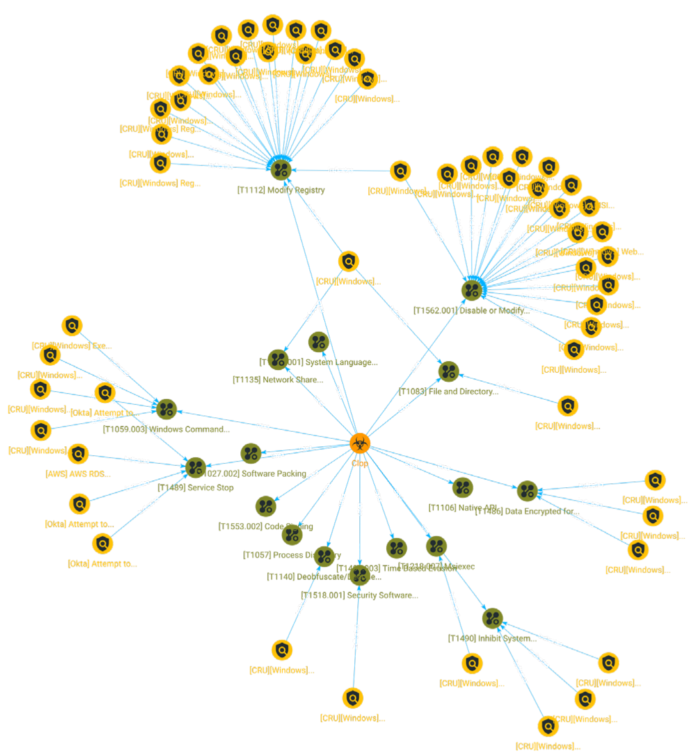


Figure 3.9: Illustration of Cl0p techniques tied to ConnectWise SIEM detection signatures

Hive

- 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 6% of all ransomware incidents directly targeting MSPs in 2022

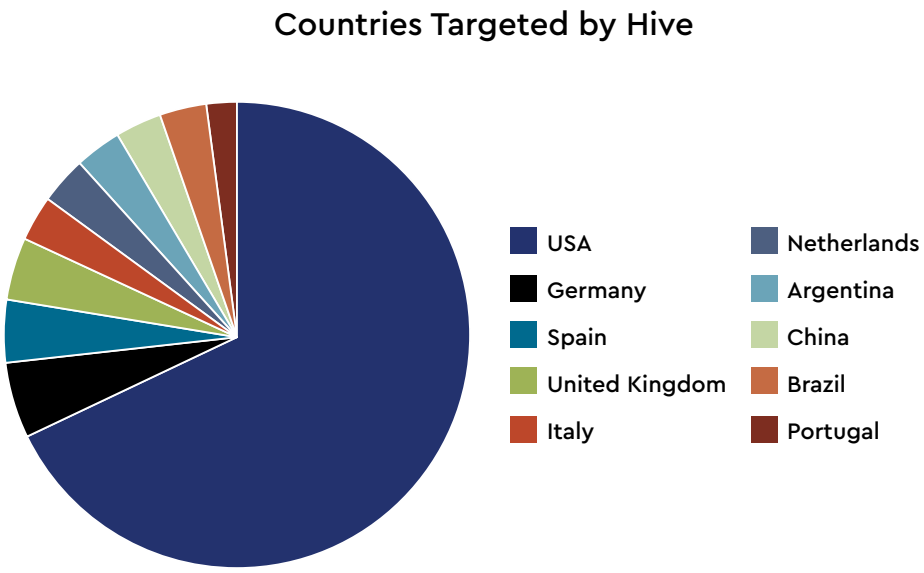


Figure 3.10: Countries targeted by Hive in 2022

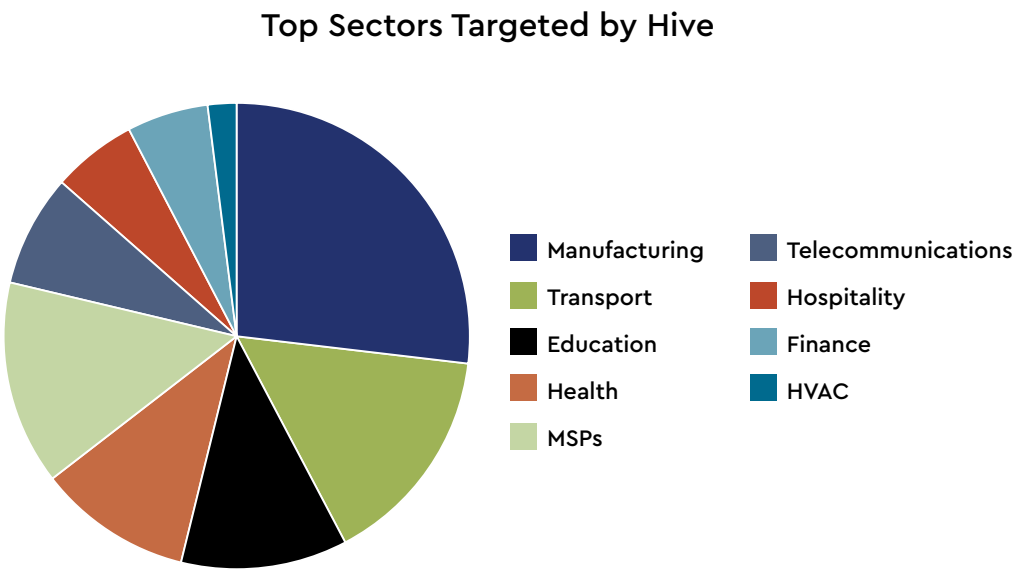


Figure 3.11: Business Sectors targeted by Hive in 2022

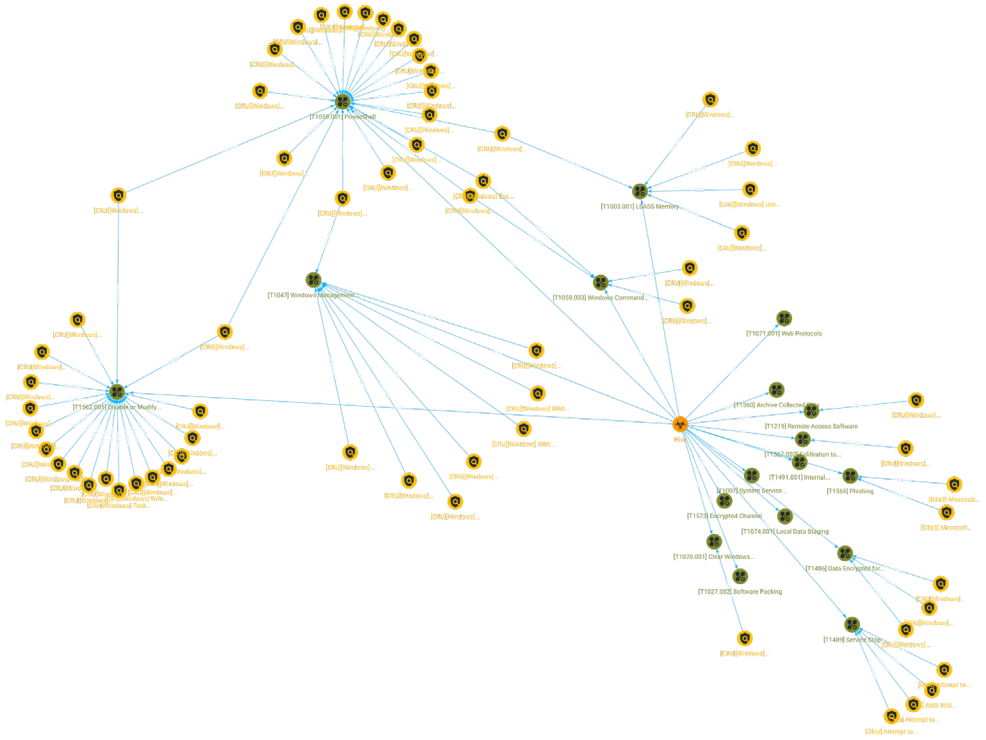


Figure 3.12: Illustration of Hive techniques tied to ConnectWise SIEM detection signatures

Mount Locker/DagonLocker/QuantumLocker

- Ransomware first appeared in July 2020
- Uses the double extortion method of encrypting files and threatening to leak stolen data
- Responsible for 6% of all ransomware incidents directly targeting MSPs in 2022

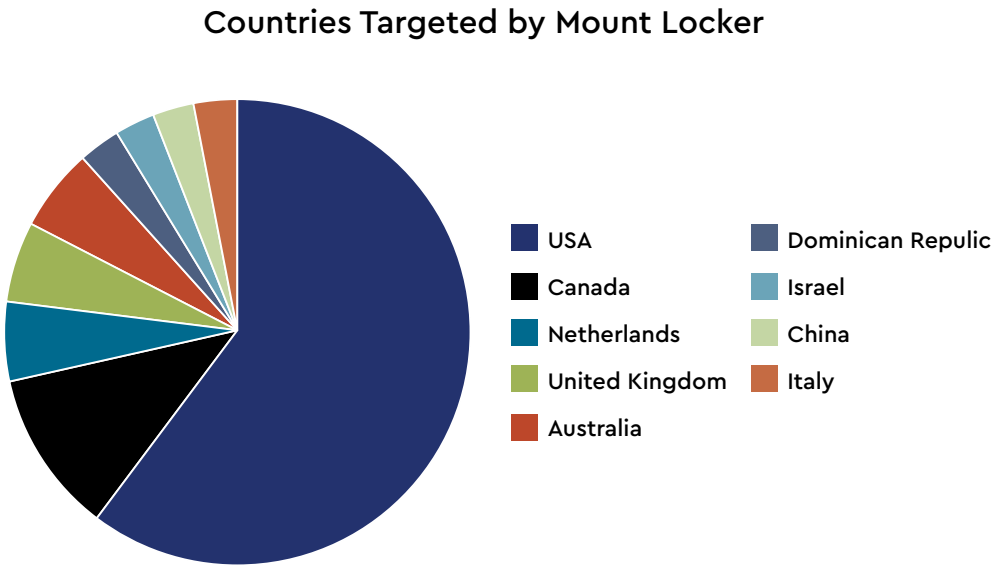


Figure 3.13: Countries targeted by Mount Locker in 2022

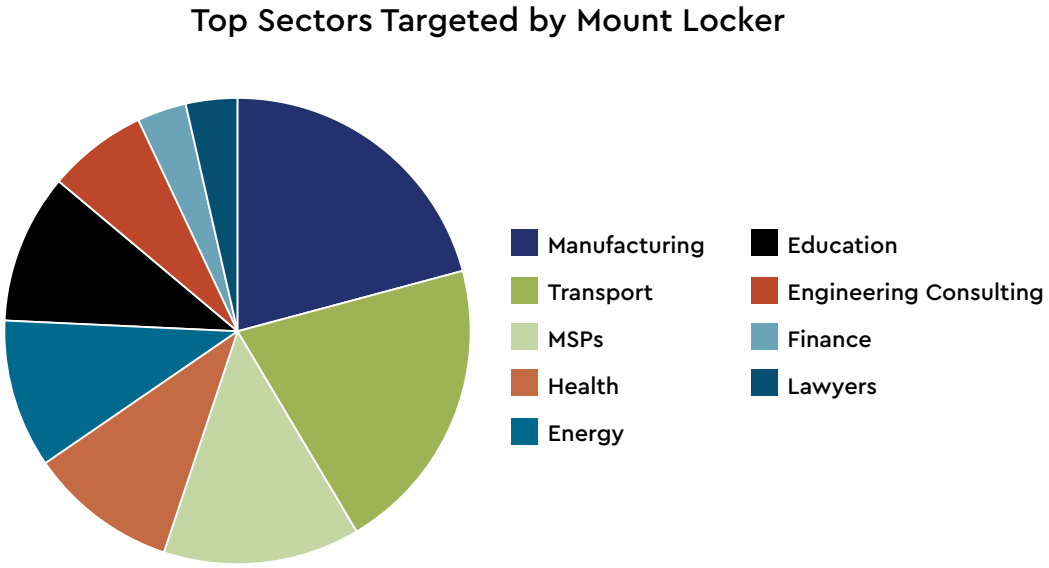


Figure 3.14: Business sectors targeted by Mount Locker in 2022

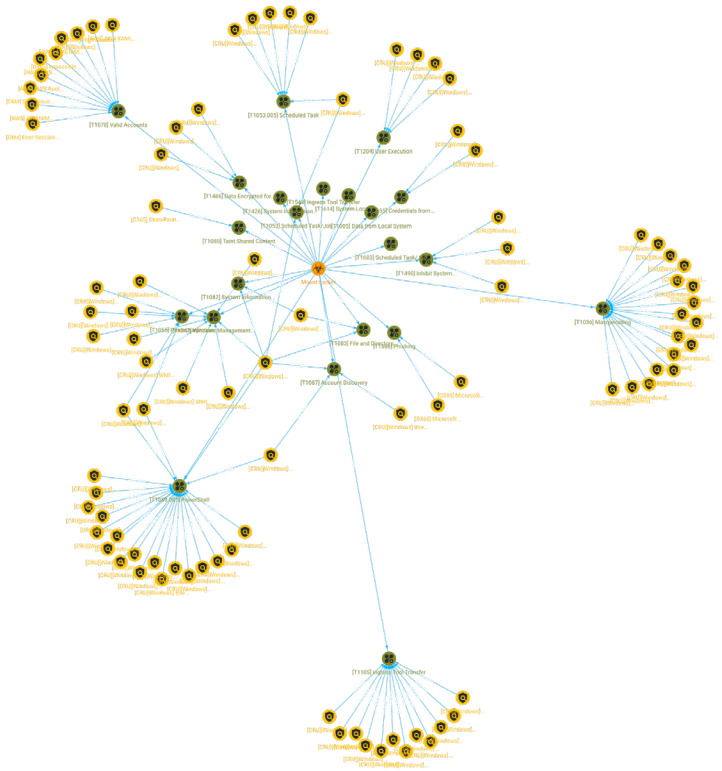


Figure 3.15: Illustration of Mount Locker techniques tied to ConnectWise SIEM detection signatures

Conti

- Ransomware-as-a-Service provider that first appeared in December 2019
- Typically distributed via TrickBot
- Uses the double extortion method of encrypting files and threatening to leak stolen data
- Responsible for 4% of all ransomware incidents directly targeting MSPs in 2022
- No longer in operation

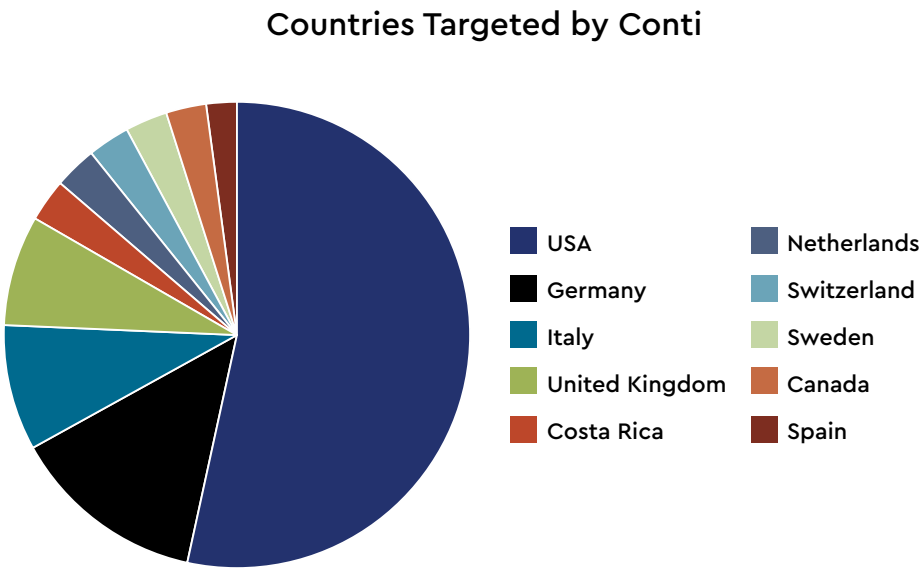


Figure 3.16: Countries targeted by Conti in 2022

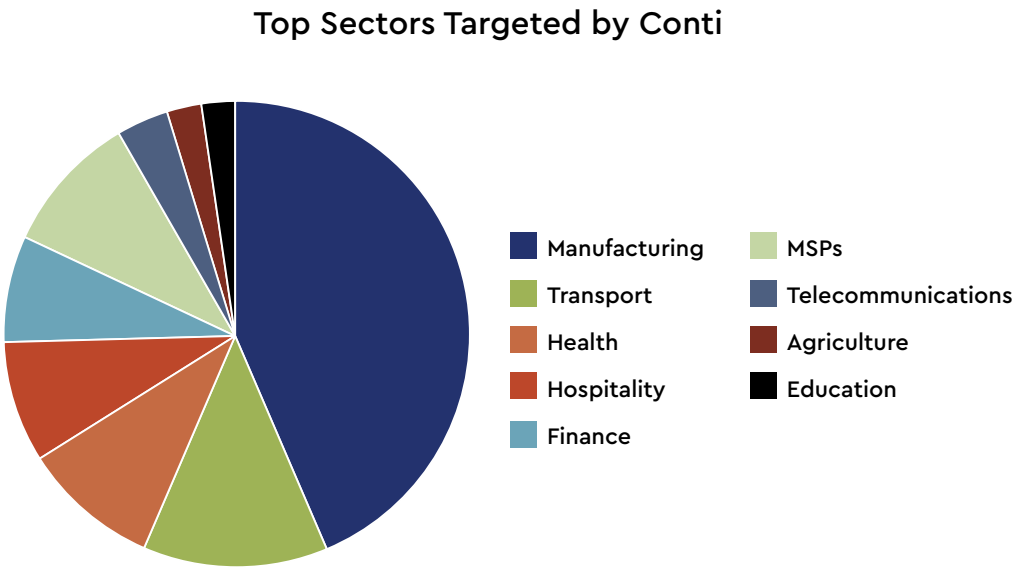


Figure 3.17: Business sectors targeted by Conti in 2022

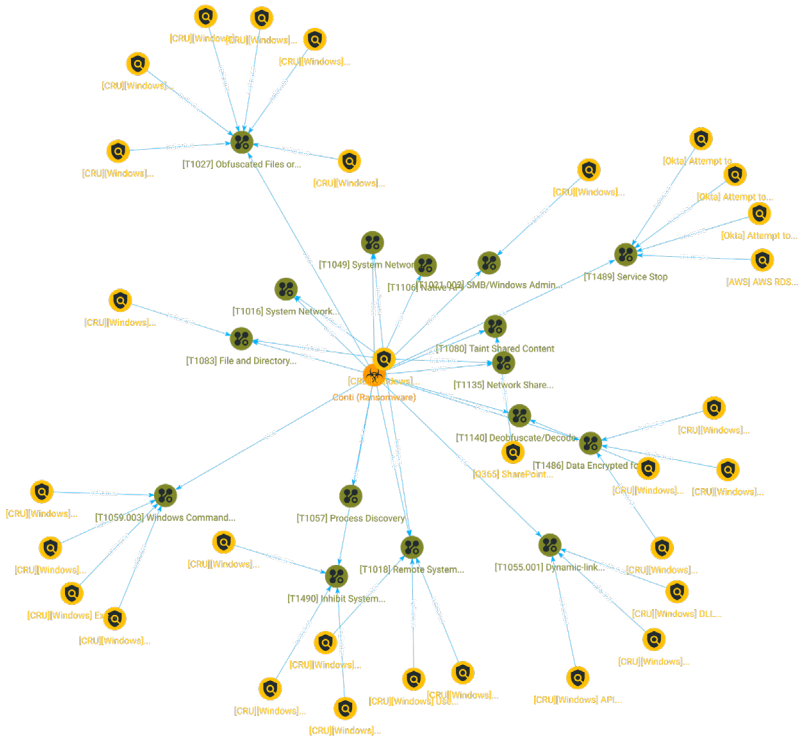


Figure 3.18: Illustration of Conti techniques tied to ConnectWise SIEM detection signatures

Top 5 Ransomware Heat Map

Immediately below is a heat map of the MITRE ATT&CK techniques used by ransomware affiliates specifically targeting MSPs in 2022. MSPs can compare common techniques used by multiple groups to be more confident that time and money dedicated to cybersecurity are focused on areas that will have the most impact. This best practice answers the question: "What techniques do we realistically need to be prepared to defend against?"

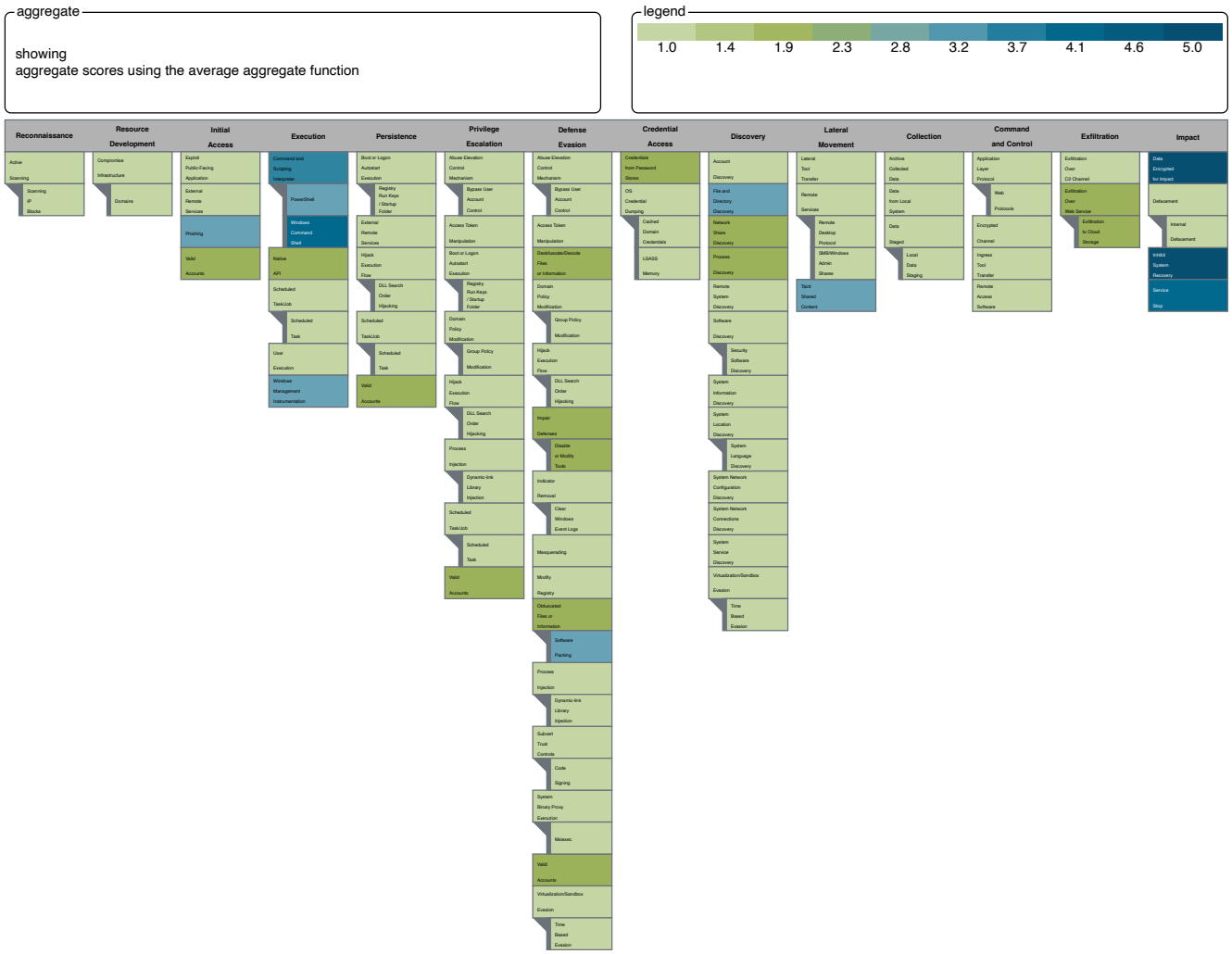


Fig 3.19: Heat map of the MITRE ATT&CK(c) techniques used by ransomware affiliates specifically targeting MSPs in 2022

We can see that phishing (T1566) and valid accounts (T1078) are still common methods used for initial access (TA0001). MSPs can significantly reduce their attack surface by implementing common mitigations such as email filters, user training, password hygiene, and MFA.

Execution (TA0002) is often performed using tools and applications built into the operating system with Windows Command shell (T1059.003) scripting being the most common technique and PowerShell (T1059.001) and Windows Management Instrumentation (T1047) tying for second.

Impact to MSPs

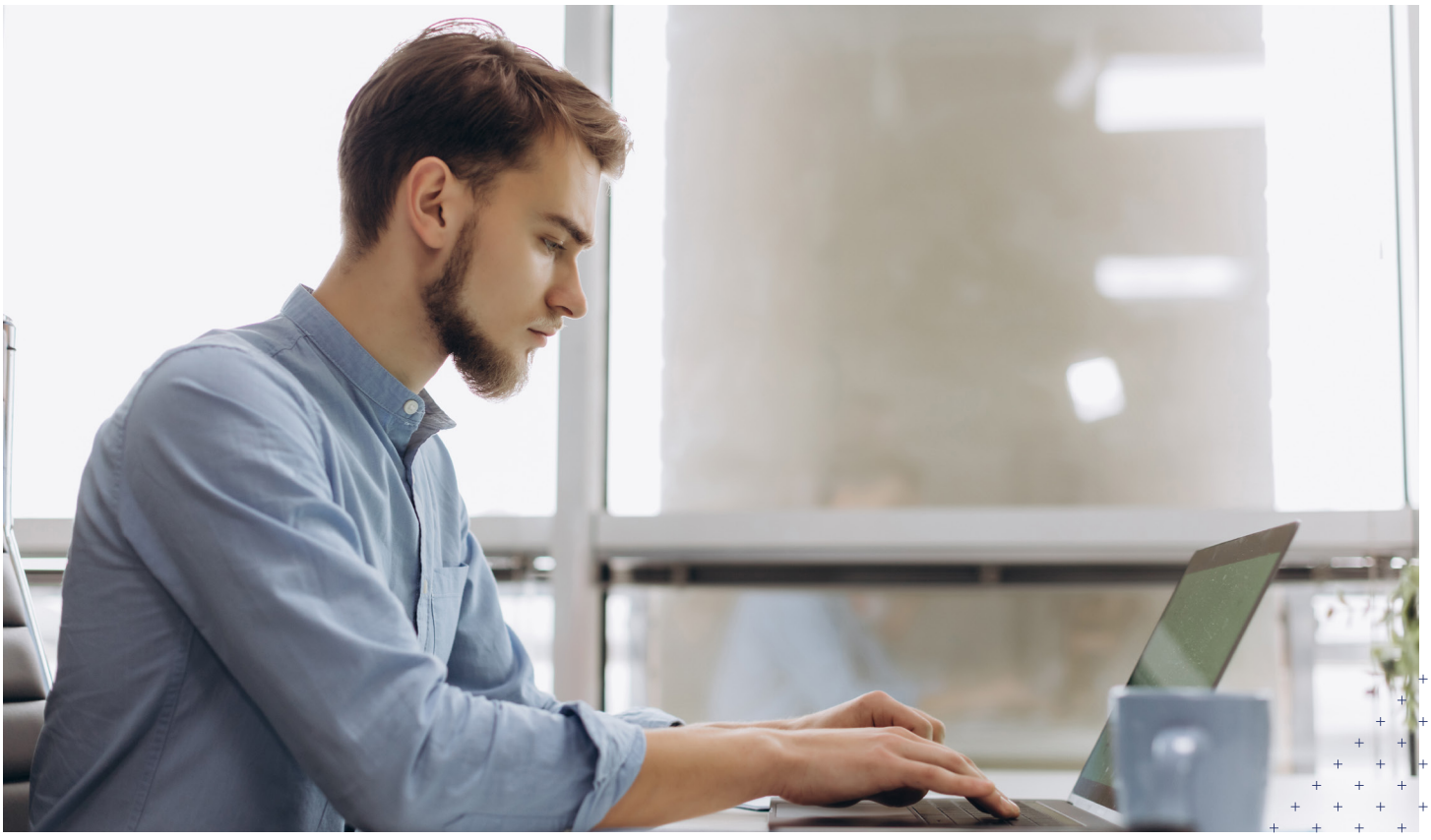
A SIEM can be a powerful tool for detecting these techniques, especially if you enable PowerShell script block logging. Execution prevention (M1038), privileged account management (M1026), and code signing (M1045) are all reasonable mitigations for dealing with these techniques. A good EDR solution can also help prevent malicious code from executing.

Taint shared content (T1080) is the most common technique used for lateral movement (TA0008). With this technique, threat actors deliver payloads to other systems attached to a compromised host using shared storage locations such as network drives or code repositories. Besides the mitigations mentioned above, you can restrict file and directory permissions (M1022) to help mitigate this technique.

Chapter 4: 2022 Vulnerabilities in Review

In 2022, there were over 25,000 vulnerabilities disclosed that were assigned a common vulnerabilities and exposures (CVE) number and included in the National Vulnerability Database (NVD) via the National Institute of Standards and Technology. (Click here for the full list.)

The CRU tracks and builds detections for exploitation attempts of known vulnerabilities when possible. The full listing of new vulnerabilities is too broad a subject for a single report, so we compiled a timeline of new vulnerabilities disclosed in 2022 and highlights of actively exploited vulnerabilities. We based this list on what vulnerabilities MSPs are discussing and following in various MSP security-focused chat rooms, forums, and social media.



2022 Vulnerabilities in Review

January 11, 2022

CVE-2022-21969[1] – Microsoft Exchange Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21846, CVE-2022-21855.

January 11, 2022

CVE-2022-21907 – HTTP Protocol Stack Remote Code Execution Vulnerability.

April 13, 2022

CVE-2022-22957 – VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two remote code execution vulnerabilities (CVE-2022-22957 & CVE-2022-22958). A malicious actor with administrative access can trigger deserialization of untrusted data through malicious JDBC URI which may result in remote code execution.

April 13, 2022

CVE-2022-22956 – VMware Workspace ONE Access has two authentication bypass vulnerabilities (CVE-2022-22955 & CVE-2022-22956) in the OAuth2 ACS framework. A malicious actor may bypass the authentication mechanism and execute any operation due to exposed endpoints in the authentication framework.

April 13, 2022

CVE-2022-22959 – VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a cross site request forgery vulnerability. A malicious actor can trick a user through a cross site request forgery to unintentionally validate a malicious JDBC URI.

January 11, 2022

CVE-2022-21855[1] – Microsoft Exchange Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21846, CVE-2022-21969.

January 11, 2022

CVE-2022-21846[1] – Microsoft Exchange Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21855, CVE-2022-21969.

April 13, 2022

CVE-2022-22961 – VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an information disclosure vulnerability due to returning excess information. A malicious actor with remote access may leak the hostname of the target system. Successful exploitation of this issue can lead to targeting victims.

April 13, 2022

CVE-2022-22958 – VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two remote code execution vulnerabilities (CVE-2022-22957 & CVE-2022-22958). A malicious actor with administrative access can trigger deserialization of untrusted data through malicious JDBC URI which may result in remote code execution.

Microsoft Exchange Specific

April 13, 2022

CVE-2022-22955 – VMware Workspace ONE Access has two authentication bypass vulnerabilities (CVE-2022-22955 & CVE-2022-22956) in the OAuth2 ACS framework. A malicious actor may bypass the authentication mechanism and execute any operation due to exposed endpoints in the authentication framework.

May 10, 2022

CVE-2022-26925 – Windows LSA Spoofing Vulnerability.

June 21, 2022

CVE-2022-22954 – VMware Workspace ONE Access and Identity Manager allow for remote code execution due to server-side template injection.

June 21, 2022

CVE-2022-26134 – Atlassian Confluence Server and Data Center contain a remote code execution vulnerability that allows for an unauthenticated attacker to perform remote code execution.

July 29, 2022

CVE-2022-22280[3] – Improper Neutralization of Special Elements used in an SQL Command leading to Unauthenticated SQL Injection vulnerability, impacting SonicWall GMS 9.3.1-SP2-Hotfix1, Analytics On-Prem 2.5.0.3-2520 and earlier versions.

April 15, 2022

CVE-2022-26809 – Remote Procedure Call Runtime Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24492, CVE-2022-24528.

May 18, 2022

CVE-2022-30138 – Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-29104, CVE-2022-29132.

June 21, 2022

CVE-2022-22960 – VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability due to improper permissions in support scripts.

June 21, 2022

CVE-2022-30190 – A remote code execution vulnerability exists when MSDT is called using the URL protocol from a calling application such as Word. An attacker who successfully exploits this vulnerability can run code with the privileges of the calling application.

IoT Specific

August 29, 2022

CVE-2022-32548[3] – An issue was discovered on certain DrayTek Vigor routers before July 2022 such as the Vigor3910 before 4.3.1.1. /cgi-bin/wlogin.cgi has a buffer overflow via the username or password to the aa or ab field.

October 3, 2022

CVE-2022-41040[1] – Microsoft Exchange Server Elevation of Privilege Vulnerability.

November 9, 2022

CVE-2022-41080[1] – Microsoft Exchange Server Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41123.

September 23, 2022

CVE-2022-3236[3] – A code injection vulnerability in the User Portal and Webadmin allows a remote attacker to execute code in Sophos Firewall version v19.0 MR1 and older.

October 3, 2022

CVE-2022-41082[1] – Microsoft Exchange Server Remote Code Execution Vulnerability.

November 9, 2022

CVE-2022-41091[2] – Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41049.

Microsoft Exchange Specific	In 2022, there were 18 CVEs published related toMicrosoft Exchange. We highlighted six of these in the timeline above in lime green boxes.
Mark of the Web Bypass	Bypassed Mark of the Web, which Microsoft attempted to fix in November's Patch Tuesday, highlighted in midnightblue in the timeline above.
IoT Specific	We've highlighted above in light cerulean blue a few IoT vulnerabilities disclosed in 2022 for devices often used by MSPs.

Microsoft Exchange

In March 2021, Microsoft published details regarding critical vulnerabilities, commonly called ProxyLogon, in Microsoft Exchange that were actively being exploited by an APT known as HAFNIUM. Since that day, several new vulnerabilities have been discovered in the Microsoft Exchange Server that have become a focus of study for security researchers and threat actors alike. In 2022, there were 18 CVEs published related to Microsoft Exchange. We highlighted six of these in the timeline above in lime green boxes[1].

Impact to MSPs

All the recently disclosed Exchange vulnerabilities only affect servers running on-premises. Most MSPs use Microsoft 365 for their clients, reducing the impact; however, if your MSP still supports on-premises Exchange paying close attention to these vulnerabilities is critical.

Due to the nature of Exchange, the data it hosts, and where it typically exists on the network, a compromised Exchange server can be catastrophic to an organization, including complete domain takeover and critical data theft. Best practices for MSPs with on-premises Exchange include timely deployment of the latest Exchange patches, prohibiting domain admin access for email users, and putting Outlook Web Access behind a VPN to prevent unauthorized access if possible.

New Phishing Technique

In July, Microsoft changed their default behavior for handling visual basic application (VBA) macros in Office documents downloaded online. Previously, Office applications presented a notification with the option to enable the macros; now, macros are disabled by default and require a change to group policy. Malicious actors quickly acted to sidestep this new security hurdle by adopting a variety of other techniques for tricking users into triggering payloads. The most prominent method observed in 2022 was the use of LNK files. They are simple to craft, appear innocuous, allow nearly arbitrary execution, and do not incur many of the Mark of the Web defenses in Office documents.

Throughout the year, we most frequently observed malicious LNK files being packaged within zip archives disk images, such as ISO, VHD files, and in a chain of both file types. These methods of delivery offered several extra benefits to attackers in combination with LNK files. Instead of being downloaded, payloads were delivered along with this initial execution vector, simplifying the chain of compromise. Archives were commonly password protected and sent in phishing emails with the password to prevent security solutions from detecting their malicious contents. In some situations, either method of delivery bypassed Mark of the Web, which Microsoft attempted to fix in November's Patch Tuesday, highlighted in midnight blue[2] in the timeline above.

The biggest malicious LNK file usage perpetrators were campaigns dropping Qakbot, IcedID, and Emotet, eventually leading to ransomware deployment. A common feature of these campaigns was to use the LNK files to proxy execution of packaged payloads through LOLBins, such as rundll32 or regsvr32, to bypass any potential application safelists. Other campaigns dropped vulnerable versions of legitimate system applications with known DLL sideloading vulnerabilities, such as older versions of Windows Calculator. Otherwise, campaigns typically used LNK files to run encoded or obfuscated PowerShell payloads or launch scripts packaged with the LNKs via Wscript.

Mitigation Guidance

While there is no direct mitigation for protecting against malicious LNK files, MSPs can take steps to protect against some delivery vectors and limit options for execution. When viable, email restrictions can be implemented against the delivery of LNK, zip, 7-zip, RAR, ISO, VHD, or HTML files. Disk image files can be blocked from automatically mounting via group policy by adding the device ID "SCSI\CdRomMsft____ Virtual_DVD-ROM_" to the "Prevent Installation of Devices" setting of the "Device Installation Restriction" GPO. To limit malicious LNK file execution possibilities, enact applications controls through WDAC or AppLocker to prevent users from running anything unnecessary to their business roles. Otherwise, EDR solutions can be leveraged to protect against the types of executions expected out of most campaigns.

Impact to MSPs

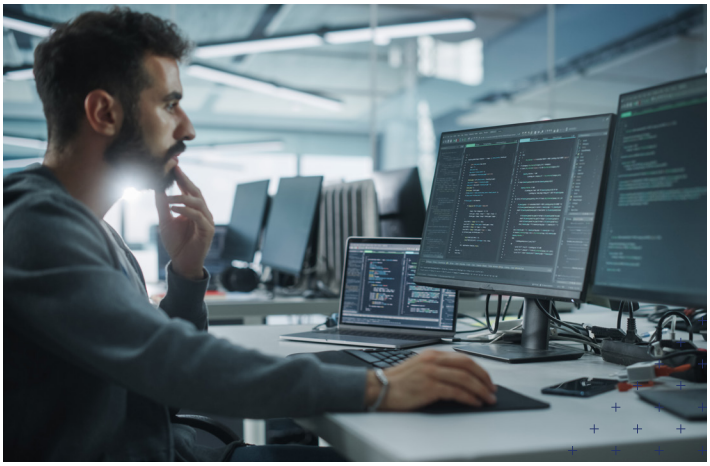
Phishing is still one of the most common methods used by threat actors for initial access. Even though new technologies are available and changes are being made to default behaviors of software (such as Office) to help combat this problem, threat actors continue to find new techniques to bypass these safeguards. This makes user education a crucial component of your MSP's security policy. These safeguards still help reduce your overall attack surface and should be deployed where possible, including designing your networks using the principle of least privileges and zero trust to minimize the impact when a user gets compromised.

IoT Vulnerabilities

The Internet of Things (IoT) is rapidly increasing the number of connected devices globally, which poses new security challenges. Many IoT devices have limited computing power and memory. Additionally, they often run outdated software because they are frequently overlooked by patch management policies focusing only on servers and workstations.
We've highlighted above in light cerulean blue[3] a few IoT vulnerabilities disclosed in 2022 for devices often used by MSPs.

Impact to MSPs

Some organizations with a patch management policy overlook IoT devices and focus only on workstations and servers. However, IoT devices are often connected directly to the public internet, and we frequently see unpatched devices being compromised. CISA has some tips for securing the Internet of Things as well as guidance on acquiring devices.



Chapter 5: Predictions from the CRU

Based on information from this and past ConnectWise MSP Threat Reports, the CRU has identified trends for 2023 (and beyond) that will affect MSP cybersecurity best practices and service offerings.

1. MSPs remain targets of supply chain and critical infrastructure attacks

Governments worldwide have issued warnings and statements about escalating cyberattacks against supply chains and critical government infrastructures. Escalating geopolitical tensions are driving the attacks as parties seek ways to compromise digital infrastructure.

"In 2020, a number of Federal agencies and large corporations were compromised by malicious code that was added into SolarWinds software. This small change created a backdoor into the digital infrastructure of Federal agencies and private sector companies," a White House communication stated in September 2022. "This incident was one of a string of cyber intrusions and significant software vulnerabilities over the last two years that have threatened the delivery of government services to the public, as well as the integrity of vast amounts of personal information and business data that is managed by the private sector."

One month later, the United Kingdom's National Cyber Security Centre (NCSC) updated its recommendations for securing supply chains. This update was based on the DCMS Cyber Security Breaches Survey 2022, which stated that "just over one in ten businesses review the risks posed by their immediate suppliers (13%), and the proportion for the wider supply chain is half that figure (7%)."

Similarly, the Federal Government of Australia researched vulnerabilities in import supply chains. ZDNet reported that the findings prompted the Australian Cyber Security Center (ACSC) to update its guidance for identifying and managing supply chain risks.

Many MSPs will look to an outside partner with the right expertise to start strengthening their cybersecurity posture. Expert help with 24/7 threat detection monitoring, incident detection and response, and risk assessments offers a notable peace of mind when navigating the complexities of cybersecurity best practices.

2. Zero trust network architecture is critical for MSPs

The most vulnerable MSPs are those without zero-trust network architecture (ZTNA), which is why governments worldwide will continue to expand their programs to require ZTNA from their vendors.

The pandemic pushed a rapid expansion of digital transformation for many businesses, which rapidly increased the attack surface for everyone. According to Ruggero Contu, a senior director analyst with Gartner, the result is that "demand for technologies and services such as cloud security, application security, ZTNA, and threat intelligence has been rising to tackle new vulnerabilities and risks arising from this exposure."

As you work to come to grips with the swiftly changing landscape yourself, you will likely have the added responsibility of educating your clients about new risks and why they should even care. A good place to solidify ZTNA basics is here.

3. Leveraging threat intelligence research and inter-organizational collaboration is essential for MSPs

In 2021, several high-profile ransomware incidents prompted ransomware operators to change tactics to stay out of the public eye. In other words, they shifted their focus to smaller organizations.

While it's true that fewer ransomware incidents were reported in the first half of 2022, many experts don't believe attacks decreased, according to the Washington Post. We simply saw fewer reports because smaller companies are less likely to report incidents, and they don't receive the same media coverage as attacks on larger businesses.

Threat actors (most notably LAPSUS) also switched focus to pure data extraction and extortion without encryption in 2022. Additionally, primarily via cyberwarfare used in the Russia-Ukraine War, some threat actors used data wipers for the sole purpose of destroying data to cause harm.

With these developments, It's clear that MSPs and their clients are at risk. Understanding current threats can help you prioritize your time and efforts on what will have the most significant impact on you and your clients. The CRU is founded on the principle that sharing threat intelligence makes the whole industry stronger. We share intel whenever possible, and we share sightings, TTPs, and IOCs with Microsoft Advanced Protection Program and MITRE Sightings.

You can stay up to date with our findings here.

4. MSPs will continue to solve the IT talent gap with tech stack consolidation and leveraging outside services

About 73% of IT industry leaders predict difficulties when recruiting data scientists or filling other tech positions in the coming years. While some MSPs aren't feeling that pressure right now, it will inevitably come down the pipeline as they start building the solutions to cover the increased attack surface caused by widespread digital transformation.

One way forward for MSPs is partnering with third-party experts, including NOC and SOC services. These kinds of partnerships have many benefits when it comes to growing an MSP and adding or boosting cybersecurity services. The right partner can serve as an extension of your team so you can do the following and more:

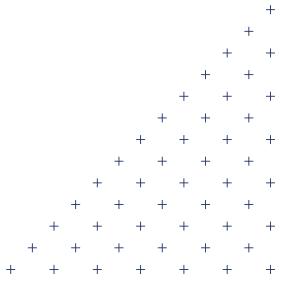
- Offload most of the technical work needed in a growing practice, allowing your technical staff to focus on high-value projects (MSPs don't profit from "need to be done" tasks)
- Scale services up and down as needed so you don't pay for unused or unproductive labor
- Leverage expert cybersecurity knowledge to create incident response plans and have immediate support when an incident occurs

5. Specialized cybersecurity training will increase across the industry, but ramp-up will take time

There's only so much time in a day for an MSP to run day-to-day operations, grow a business, and add or build cybersecurity services. Diversified skillsets have worked so far for MSPs, but it can't replace the need for cybersecurity specialization in an ever-changing threat landscape.

Forbes reported in November 2022 that "cybersecurity specialists can anticipate strong employment growth over the coming decade. For example, the U.S. **Bureau of Labor Statistics** reports a 35% projected employment growth rate for information security analysts from 2021 to 2031." However, the growth will not be fast enough to meet the demands of companies that need cybersecurity specialists, and ramping up your current staff is also a progressive process.

Once again, third-party partnerships can offer the extra support and expertise needed as the hiring pool and your staff catch up to demand. Leveraging SOC services can give you the flexibility to meet client cybersecurity needs, and it's a proven way to maintain long-term growth without burdening your bottom line.



About the MSP Threat Report

This report was created by the ConnectWise Cyber Research Unit (CRU)—a dedicated team of ConnectWise threat hunters who identify and research new vulnerabilities and publicly share what they find across the community. The CRU monitors ransom leak sites and malicious botnets for new threats, uses OSINT resources, and utilizes data from ConnectWise SIEM to help create content and complete research.

See all of the CRU's threat reports >

ConnectWise CRU Feeds

For continuing insights beyond this report, please sign up for the ConnectWise Cyber Research Unit feeds. This repository contains lists of threat intelligence indicators discovered by the CRU using ConnectWise SIEM or found during threat hunting. This data is threat intelligence the CRU has been collecting for years and using internally at ConnectWise for threat hunting and threat analysis assistance. We use this intelligence daily, searching for these indicators in our partners' network data to find new threats and filter out false positives. This feed is updated daily.

Sign up now >

See the latest MITRE ATT&CK mappings with mitigations >

ConnectWise Cybersecurity Management

The ConnectWise Cybersecurity Management solution includes software and support services that enable TSPs to protect their client's critical assets. With tools for 24/7 threat detection monitoring, incident response, and security risk assessment, ConnectWise removes the complexity of building an MSP-powered cybersecurity stack while lowering support staff costs.

Learn more >

ConnectWise

ConnectWise is the world's leading software company dedicated to the success of IT solution providers (TSPs) through unmatched software, services, community, and marketplace of integrations. ConnectWise offers an innovative, integrated, and security-centric platform—Asio™—which provides unmatched flexibility that fuels profitable, long-term growth for partners. ConnectWise enables TSPs to drive business efficiency with automation, IT documentation, and data management capabilities and increase revenue with remote monitoring, cybersecurity, and backup and disaster recovery technologies.

Learn more >