Threat Report

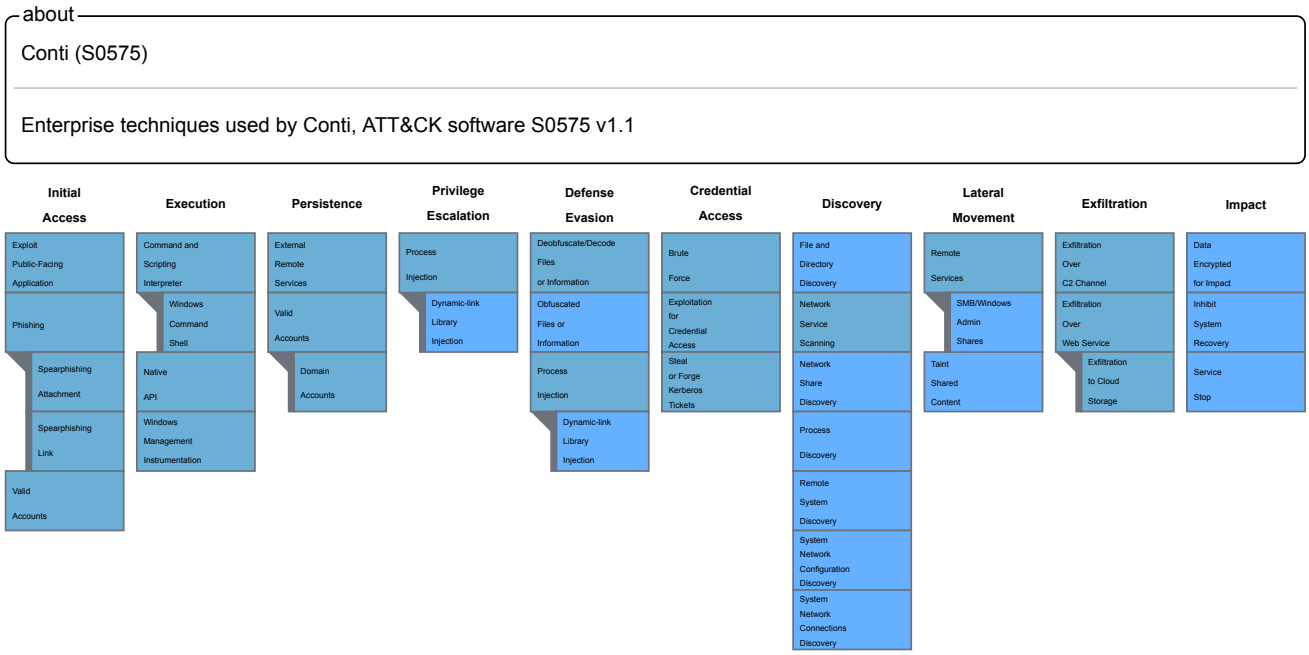
connectwise.com/resources/conti-profile

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

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 10% of all ransomware incidents we observed targeting MSPs and their customers in 2021

MITRE ATT&CK® mapping



Conti TTPs and Mitigations

ATT&CK Tactic	ATT&CK Technique	Mitigations

Initial Access	T1078 – Valid Accounts: Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.	M1013 - Application Developer Guidance: Ensure that applications do not store sensitive data or credentials insecurely. (e.g. plaintext credentials in code, published credentials in repositories, or credentials in public cloud storage).
M1027 - Password Policies: Applications and appliances that utilize default username and password should be changed immediately after the installation, and before deployment to a production environment. When possible, applications that use SSH keys should be updated periodically and properly secured.		
M1026 - Privileged Account Management: Audit domain and local accounts as well as their permission levels routinely to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account. These audits should also include if default accounts have been enabled, or if new local accounts are created that have not be authorized. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers.		

M1017 - User Training:

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

T1190 – Exploit Public-Facing Application:
Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability.

M1048 - Application Isolation and Sandboxing:
Application isolation will limit what other processes and system features the exploited target can access.

M1050 - Exploit Protection:

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

M1030 - Network Segmentation:

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

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

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

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

T1566.001 – Phishing: Spearphishing Attachment:
Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry.

M1049 - Antivirus/Antimalware:

Anti-virus can also automatically quarantine suspicious files.

M1031 - Network Intrusion Prevention:

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

M1021 - Restrict Web-Based Content:

Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments.

M1054 - Software Configuration: Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross domain) to perform similar message filtering and validation.	
M1017 - User Training: Users can be trained to identify social engineering techniques and spearphishing emails.	
T1566.002 – Phishing: Spearphishing Link	M1021 - Restrict Web-Based Content: Determine if certain websites that can be used for spearphishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.
M1054 - Software Configuration: Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross domain) to perform similar message filtering and validation.	

M1017 - User Training: Users can be trained to identify social engineering techniques and spearphishing emails with malicious links.		
Execution	T1059.003 – Windows Command Shell: Adversaries may abuse the Windows command shell for execution. The Windows command shell (cmd) is the primary command prompt on Windows systems.	M1038 - Execution Prevention: Use application control where appropriate.
T1106 – Native Application Programming Interface (API)	M1040 - Behavior Prevention on Endpoint: On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Office VBA macros from calling Win32 APIs.	
M1038 - Execution Prevention: Identify and block potentially malicious software executed that may be executed through this technique by using application control tools, like Windows Defender Application Control, AppLocker, or Software Restriction Policies where appropriate.		

T1047 – Windows Management Instrumentation: Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is an administration feature that provides a uniform environment to access Windows system components.	M1040 - Behavior Prevention on Endpoint: On Windows 10, enable Attack Surface Reduction (ASR) rules to block processes created by WMI commands from running. Note: many legitimate tools and applications utilize WMI for command execution.
M1038 - Execution Prevention: Use application control configured to block execution of wmic.exe if it is not required for a given system or network to prevent potential misuse by adversaries. For example, in Windows 10 and Windows Server 2016 and above, Windows Defender Application Control (WDAC) policy rules may be applied to block the wmic.exe application and to prevent abuse.	
M1026 - Privileged Account Management: Prevent credential overlap across systems of administrator and privileged accounts.	
M1018 - User Account Management: By default, only administrators are allowed to connect remotely using WMI. Restrict other users who are allowed to connect, or disallow all users to connect remotely to WMI.	

Persistence	T1078.002 – Valid Accounts: Domain Accounts: Adversaries may obtain and abuse credentials of a domain account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Domain accounts are those managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of that domain. Domain accounts can cover users, administrators, and services.	M1032 - Multi-factor Authentication: Integrating multi-factor authentication (MFA) as part of organizational policy can greatly reduce the risk of an adversary gaining control of valid credentials that may be used for additional tactics such as initial access, lateral movement, and collecting information. MFA can also be used to restrict access to cloud resources and APIs.
M1026 - Privileged Account Management: Audit domain account permission levels routinely to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account. Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled and use of accounts 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. Limit credential overlap across systems to prevent access if account credentials are obtained.		

M1017 - User Training:

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

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

M1042 - Disable or Remove Feature or Program:

Disable or block remotely available services that may be unnecessary.

M1035 - Limit Access to Resource Over Network:

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

M1032 - Multi-factor Authentication:

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

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

Privilege Escalation	T1055.001 – Process Injection: Dynamic-link Library Injection: Adversaries may inject dynamic-link libraries (DLLs) into processes in order to evade process-based defenses as well as possibly elevate privileges. DLL injection is a method of executing arbitrary code in the address space of a separate live process.	M1040 - Behavior Prevention on Endpoint: Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process.
Defense Evasion	T1027 - Obfuscated Files or Information: Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses.	M1049 - Antivirus/Antimalware: Consider utilizing the Antimalware Scan Interface (AMSI) on Windows 10 to analyze commands after being processed/interpreted.
M1040 - Behavior Prevention on Endpoint: On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent execution of potentially obfuscated scripts.		

T1055.001 – Process Injection: Dynamic-link Library Injection: Adversaries may inject dynamic-link libraries (DLLs) into processes in order to evade process-based defenses as well as possibly elevate privileges. DLL injection is a method of executing arbitrary code in the address space of a separate live process.	M1040 - Behavior Prevention on Endpoint: Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process.	
T1140 - Deobfuscate/Decode Files or Information: Adversaries may use Obfuscated Files or Information to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system.	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.	
Credential Access	T1110 – Brute Force: Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism.	M1036 - Account Use Policies: Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial of service condition and render environments un-usable, with all accounts used in the brute force being locked-out.

M1032 - Multi-factor Authentication:

Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services.

M1027 - Password Policies:

Refer to NIST guidelines when creating password policies.

M1018 - User Account Management:

Proactively reset accounts that are known to be part of breached credentials either immediately, or after detecting bruteforce attempts.

T1212 – Exploitation for Credential Access:

Adversaries may exploit software vulnerabilities in an attempt to collect credentials. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Credentialing and authentication mechanisms may be targeted for exploitation by adversaries as a means to gain access to useful credentials or circumvent the process to gain access to systems.

M1048 - Application Isolation and Sandboxing:

Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of exploitation. Risks of additional exploits and weaknesses in these systems may still exist.

M1050 - Exploit Protection:

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. Many of these protections depend on the architecture and target application binary for compatibility and may not work for software targeted for defense evasion.

M1019 - Threat Intelligence Program:

Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization.

M1051 - Update Software:

Update software regularly by employing patch management for internal enterprise endpoints and servers.

T1558.003 – Steal or Forge Kerberos Tickets: Kerberoasting:

Adversaries may abuse a valid Kerberos ticket-granting ticket (TGT) or sniff network traffic to obtain a ticket-granting service (TGS) ticket that may be vulnerable to Brute Force.

Service principal names (SPNs) are used to uniquely identify each instance of a Windows service. To enable authentication, Kerberos requires that SPNs be associated with at least one service logon account (an account specifically tasked with running a service).

M1041 - Encrypt Sensitive Information:

Enable AES Kerberos encryption (or another stronger encryption algorithm), rather than RC4, where possible.

M1027 - Password Policies: Ensure strong password length (ideally 25+ characters) and complexity for service accounts and that these passwords periodically expire. Also consider using Group Managed Service Accounts or another third party product such as password vaulting.		
M1026 - Privileged Account Management: Limit service accounts to minimal required privileges, including membership in privileged groups such as Domain Administrators.		
Discovery	T1016 – System Network Configuration Discovery: Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include Arp, ipconfig/ifconfig, nbtstat, and route.	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

T1018 – Remote System Discovery: Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used such as Ping or net view using Net. Adversaries may also use local host files (ex: C:\Windows\System32\Drivers\etc\hosts or /etc/hosts) in order to discover the hostname to IP address mappings of remote systems.	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
T1046 – Network Service Scanning: Adversaries may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation. Methods to acquire this information include port scans and vulnerability scans using tools that are brought onto a system.	M1042 - Disable or Remove Feature or Program: Ensure that unnecessary ports and services are closed to prevent risk of discovery and potential exploitation.
M1031 - Network Intrusion Prevention: Use network intrusion detection/prevention systems to detect and prevent remote service scans.	
M1030 - Network Segmentation: Ensure proper network segmentation is followed to protect critical servers and devices.	

T1049 – System Network Connections Discovery: Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
T1057 – Process Discovery: Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from Process Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
T1083 – File and Directory Discovery: Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from File and Directory Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

T1135 – Network Share Discovery: Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.	M1028 - Operating System Configuration: Enable Windows Group Policy "Do Not Allow Anonymous Enumeration of SAM Accounts and Shares" security setting to limit users who can enumerate network shares.	
Lateral Movement	T1021.002 – Remote Services: SMB/Windows Admin Shares: Adversaries may use Valid Accounts to interact with a remote network share using Server Message Block (SMB). The adversary may then perform actions as the logged-on user. SMB is a file, printer, and serial port sharing protocol for Windows machines on the same network or domain. Adversaries may use SMB to interact with file shares, allowing them to move laterally throughout a network. Linux and macOS implementations of SMB typically use Samba.	M1037 - Filter Network Traffic: Consider using the host firewall to restrict file sharing communications such as SMB.
M1035 - Limit Access to Resource Over Network: Consider disabling Windows administrative shares.		

M1027 - Password Policies:

Do not reuse local administrator account passwords across systems. Ensure password complexity and uniqueness such that the passwords cannot be cracked or guessed.

M1026 - Privileged Account Management:

Deny remote use of local admin credentials to log into systems. Do not allow domain user accounts to be in the local Administrators group multiple systems.

T1080 – Taint Shared Content:

Adversaries may deliver payloads to remote systems by adding content to shared storage locations, such as network drives or internal code repositories. Content stored on network drives or in other shared locations may be tainted by adding malicious programs, scripts, or exploit code to otherwise valid files. Once a user opens the shared tainted content, the malicious portion can be executed to run the adversary's code on a remote system. Adversaries may use tainted shared content to move laterally.

M1038 - Execution Prevention:

Identify potentially malicious software that may be used to taint content or may result from it and audit and/or block the unknown programs by using application control [14] tools, like AppLocker, or Software Restriction Policies where appropriate.

M1050 - Exploit Protection:

Use utilities that detect or mitigate common features used in exploitation, such as the Microsoft Enhanced Mitigation Experience Toolkit (EMET).

M1022 - Restrict File and Directory Permissions:

Protect shared folders by minimizing users who have write access.

Exfiltration	T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage: Adversaries may exfiltrate data to a cloud storage service rather than over their primary command and control channel. Cloud storage services allow for the storage, edit, and retrieval of data from a remote cloud storage server over the Internet.	M1021 - Restrict Web-Based Content: Web proxies can be used to enforce an external network communication policy that prevents use of unauthorized external services.
Impact	T1486 - Data Encrypted for Impact: Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key.	M1040 - Behavior Prevention on Endpoint: On Windows 10, enable cloud-delivered protection and Attack Surface Reduction (ASR) rules to block the execution of files that resemble ransomware.

M1053 - Data Backup: Consider implementing IT disaster recovery plans that contain procedures for regularly taking and testing data backups that can be used to restore organizational data. Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery. Consider enabling versioning in cloud environments to maintain backup copies of storage objects.

T1490 - Inhabit System Recovery:

Adversaries may delete or remove built-in operating system data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery. Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of Data Destruction and Data Encrypted for Impact.

M1053 - Data Backup: Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data. Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery.

M1028 - Operating System Configuration: Consider technical controls to prevent the disabling of services or deletion of files involved in system recovery.

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