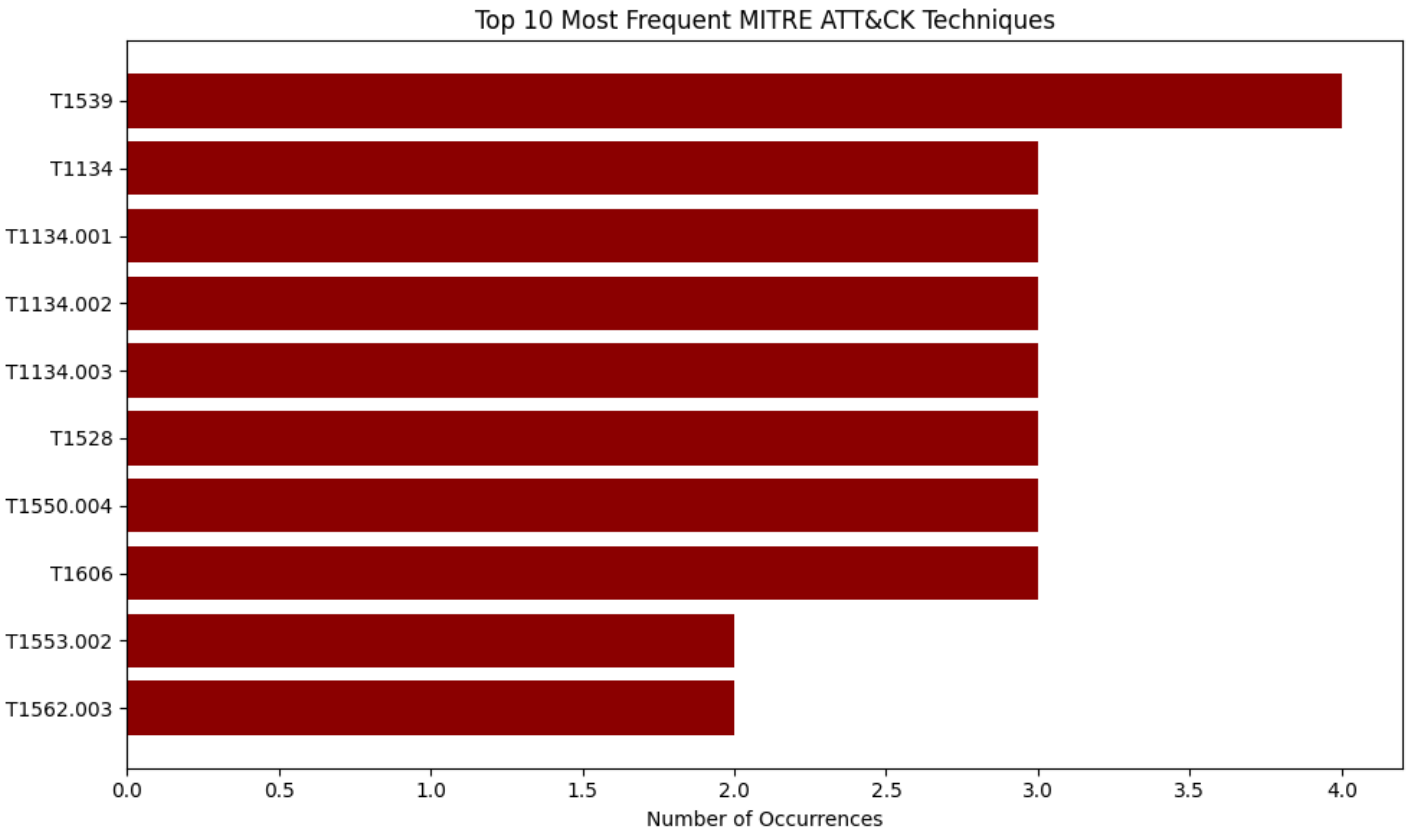
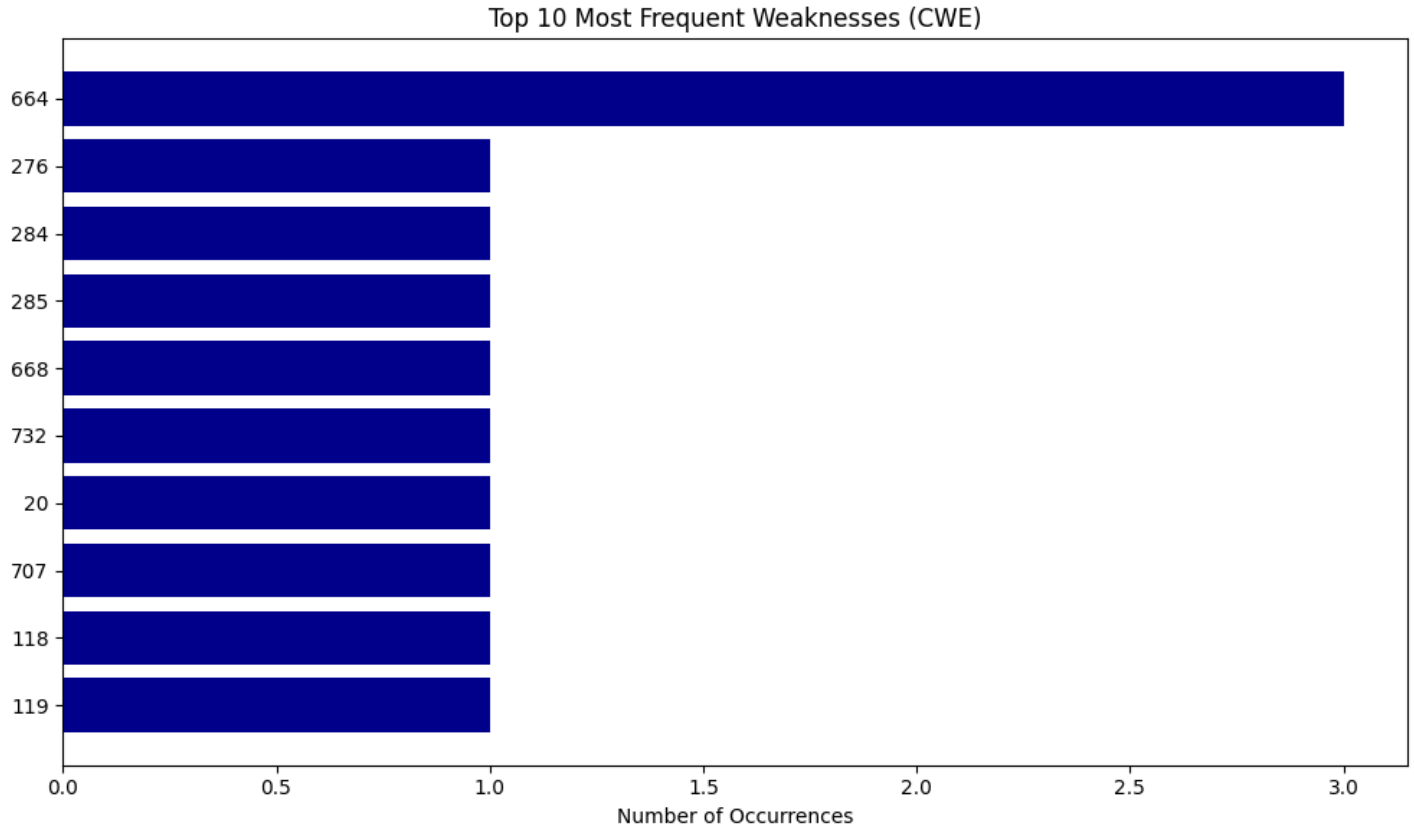
Vulnerability Intelligence Report

Vulnerabilities Analyzed: 8

Report Date: 2025-09-01 00:00:33

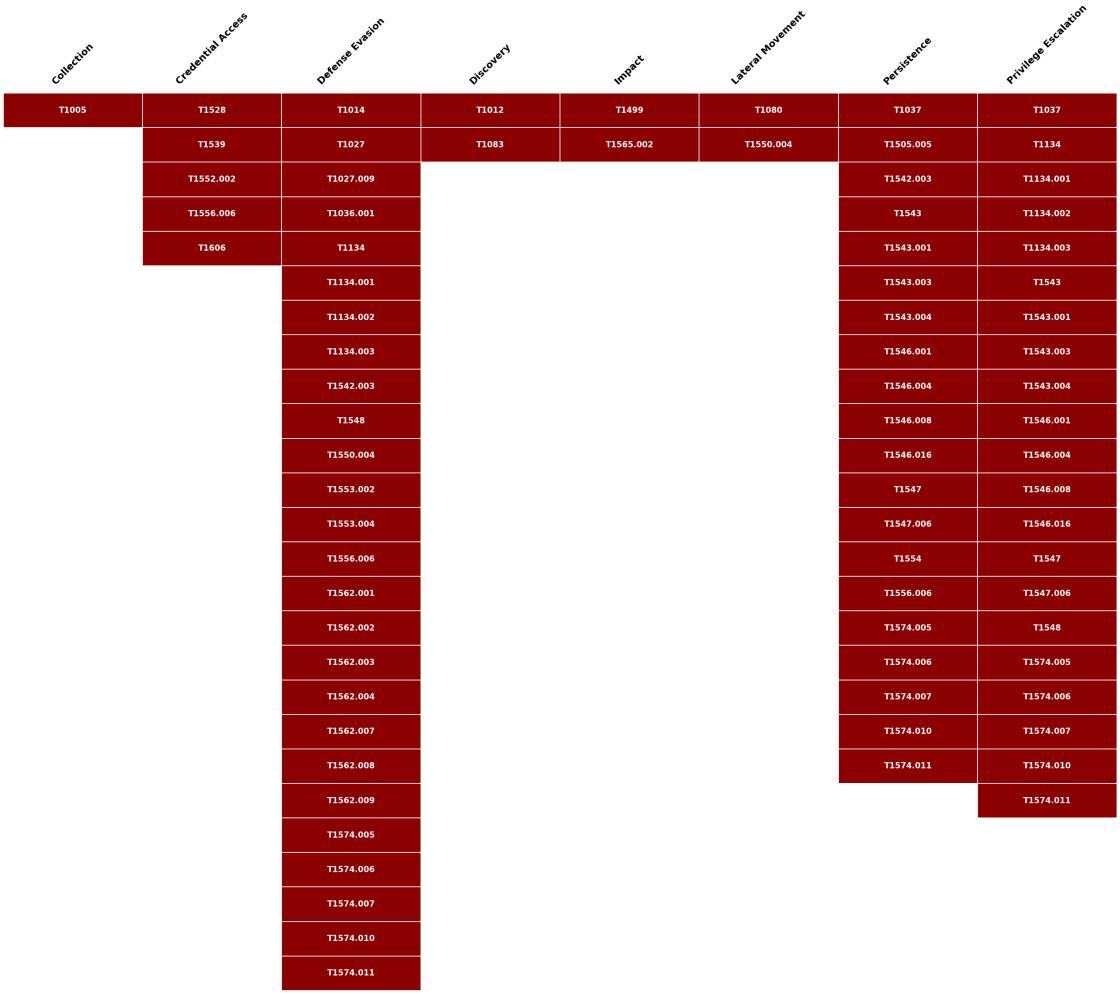
Executive Summary & Trends




Top 10 Most Frequent Weaknesses (CWE)
664
276
284
285
668
732
20
707
118
119
0.0
0.5
1.0
1.5
2.0
2.5
3.0
Number of Occurrences

Consolidated MITRE ATT&CK; Matrix

This matrix shows all techniques identified across all analyzed vulnerabilities.



Vulnerability Analysis for CVE-2020-1518

Vulnerability Summary

CVSS Score (v3.1): 7.8 (HIGH)

No associated MITRE ATT&CK; techniques were found in the database.

Vulnerability Analysis for CVE-2020-1566

Vulnerability Summary

CVSS Score (v3.1): 4.2 (MEDIUM)

No associated MITRE ATT&CK; techniques were found in the database.

Vulnerability Analysis for CVE-2020-1571

Vulnerability Summary

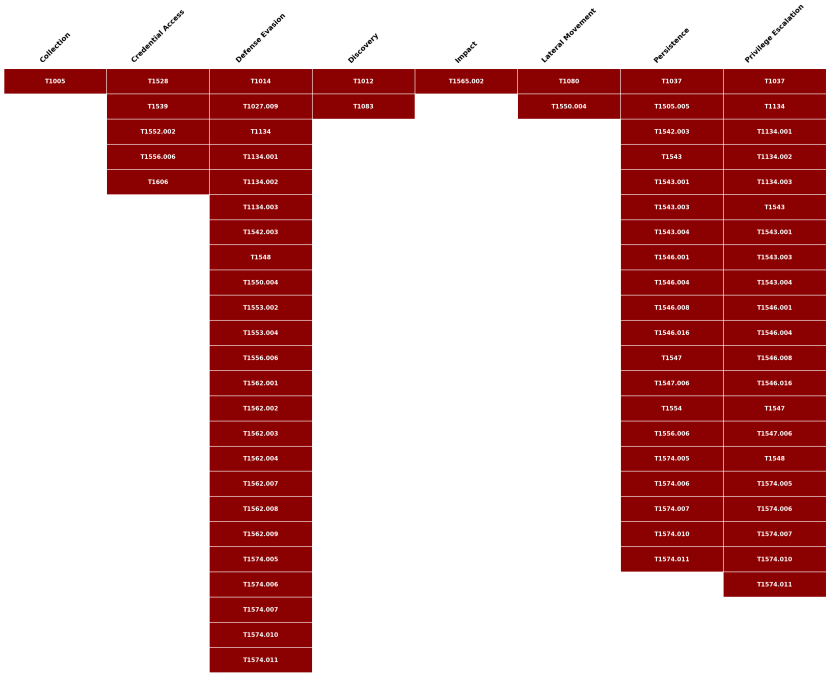
CVSS Score (v3.1): 7.3 (HIGH)

Weaknesses (CWE): 276, 284, 285, 664, 668, 732

Attack Patterns (CAPEC): 87, 1, 196, 503, 59, 478, 441, 60, 402, 562, 556, 122, 546, 536, 39, 558, 552, 563, 104, 19, 550, 21, 578, 668, 17, 61, 551, 206, 5, 180, 642, 76, 502, 564, 81, 127, 62, 13, 647, 77, 51, 479, 45, 234

Tactical Summary (MITRE ATT&CK;)

Observed Tactics: Collection, Credential Access, Defense Evasion, Discovery, Impact, Lateral Movement, Persistence, Privilege Escalation



ATT&CK; Technique Details

T1005: Data from Local System

Summary: *Adversaries may search local system sources, such as file systems, configuration files, local databases, or virtual machine files, to find files of interest and sensitive data prior to Exfiltration.*

Source: https://attack.mitre.org/techniques/T1005

T1012: Query Registry

Summary: *Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.*

Source: https://attack.mitre.org/techniques/T1012

T1014: Rootkit

Summary: *Adversaries may use rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components. Rootkits are programs that hide the existence of malware by intercepting/hooking and modifying operating system API calls that supply system information. (Citation: Symantec Windows Rootkits)*

Source: https://attack.mitre.org/techniques/T1014

T1027.009: Embedded Payloads

Summary: *Adversaries may embed payloads within other files to conceal malicious content from defenses. Otherwise seemingly benign files (such as scripts and executables) may be abused to carry and obfuscate malicious payloads and content. In some cases, embedded payloads may also enable adversaries to [Subvert Trust Controls](https://attack.mitre.org/techniques/T1553) by not impacting execution controls such as digital signatures and notarization tickets.(Citation: Sentinel Labs)*

Source: https://attack.mitre.org/techniques/T1027/009

T1037: Boot or Logon Initialization Scripts

Summary: *Adversaries may use scripts automatically executed at boot or logon initialization to establish persistence.(Citation: Mandiant APT29 Eye Spy Email Nov 22)(Citation: Anomali Rocke March 2019) Initialization scripts can be used to perform administrative functions, which may often execute other programs or send information to an internal logging server. These scripts can vary based on operating system and whether applied locally or remotely.*

Source: https://attack.mitre.org/techniques/T1037

T1080: Taint Shared Content

Summary:
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.

Source: https://attack.mitre.org/techniques/T1080

T1083: File and Directory Discovery

Summary: *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](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target*

and/or attempts specific actions.

Source: https://attack.mitre.org/techniques/T1083

T1134: Access Token Manipulation

Summary: *Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token.*

Source: https://attack.mitre.org/techniques/T1134

T1134.001: Token Impersonation/Theft

Summary: *Adversaries may duplicate then impersonate another user's existing token to escalate privileges and bypass access controls. For example, an adversary can duplicate an existing token using `DuplicateToken` or `DuplicateTokenEx`.(Citation: DuplicateToken function) The token can then be used with `ImpersonateLoggedOnUser` to allow the calling thread to impersonate a logged on user's security context, or with `SetThreadToken` to assign the impersonated token to a thread.*

Source: https://attack.mitre.org/techniques/T1134/001

T1134.002: Create Process with Token

Summary: *Adversaries may create a new process with an existing token to escalate privileges and bypass access controls. Processes can be created with the token and resulting security context of another user using features such as CreateProcessWithTokenW and runas.(Citation: Microsoft RunAs)*

Source: https://attack.mitre.org/techniques/T1134/002

T1134.003: Make and Impersonate Token

Summary: *Adversaries may make new tokens and impersonate users to escalate privileges and bypass access controls. For example, if an adversary has a username and password but the user is not logged onto the system the adversary can then create a logon session for the user using the `LogonUser` function.(Citation: LogonUserW function) The function will return a copy of the new session's access token and the adversary can use `SetThreadToken` to assign the token to a thread.*

Source: https://attack.mitre.org/techniques/T1134/003

T1505.005: Terminal Services DLL

Summary: *Adversaries may abuse components of Terminal Services to enable persistent access to systems. Microsoft Terminal Services, renamed to Remote Desktop Services in some Windows Server OSs as of 2022, enable remote terminal connections to hosts. Terminal Services allows servers to transmit a full, interactive, graphical user interface to clients via RDP.(Citation: Microsoft Remote Desktop Services)*

Source: https://attack.mitre.org/techniques/T1505/005

T1528: Steal Application Access Token

Summary: *Adversaries can steal application access tokens as a means of acquiring credentials to access remote systems and resources.*

Source: https://attack.mitre.org/techniques/T1528

T1539: Steal Web Session Cookie

Summary: *An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing credentials. Web applications and services often use session cookies as an authentication token after a user has authenticated to a website.*

Source: https://attack.mitre.org/techniques/T1539

T1542.003: Bootkit

Summary: *Adversaries may use bootkits to persist on systems. A bootkit is a malware variant that modifies the boot sectors of a hard drive, allowing malicious code to execute before a computer's operating system has loaded. Bootkits reside at a layer below the operating system and may make it difficult to perform full remediation unless an organization suspects one was used and can act accordingly.*

Source: https://attack.mitre.org/techniques/T1542/003

T1543: Create or Modify System Process

Summary: *Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence. When operating systems boot up, they can start processes that perform background system functions. On Windows and Linux, these system processes are referred to as services.(Citation: TechNet Services) On macOS, launchd processes known as [Launch Daemon](https://attack.mitre.org/techniques/T1543/004) and [Launch Agent](https://attack.mitre.org/techniques/T1543/001) are run to finish system initialization and load user specific parameters.(Citation: AppleDocs Launch Agent Daemons)*

Source: https://attack.mitre.org/techniques/T1543

T1543.001: Launch Agent

Summary: *Adversaries may create or modify launch agents to repeatedly execute malicious payloads as part of persistence. When a user logs in, a per-user launchd process is started which loads the parameters for each launch-on-demand user agent from the property list (.plist) file found in /System/Library/LaunchAgents, /Library/LaunchAgents, and ~/Library/LaunchAgents.(Citation: AppleDocs Launch Agent Daemons)(Citation: OSX Keydnap malware) (Citation: Antiquated Mac Malware) Property list files use the Label, ProgramArguments , and RunAtLoad keys to identify the Launch Agent's name, executable location, and execution time.(Citation: OSX.Dok Malware) Launch Agents are often installed to perform updates to programs, launch user specified programs at login, or to conduct other developer tasks.*

Source: https://attack.mitre.org/techniques/T1543/001

T1543.003: Windows Service

Summary: *Adversaries may create or modify Windows services to repeatedly execute malicious payloads as part of persistence. When Windows boots up, it starts programs or applications called services that perform background system functions.(Citation: TechNet Services) Windows service configuration information, including the file path to the service's executable or recovery programs/commands, is stored in the Windows Registry.*

Source: https://attack.mitre.org/techniques/T1543/003

T1543.004: Launch Daemon

Summary: *Adversaries may create or modify Launch Daemons to execute malicious payloads as part of persistence. Launch Daemons are plist files used to interact with Launchd, the service management framework used by macOS. Launch Daemons require elevated privileges to install, are executed for every user on a system prior to login, and run in the background without the need for user interaction. During the macOS initialization startup, the launchd process loads the parameters for launch-on-demand system-level daemons from plist files found in /System/Library/LaunchDaemons/ and /Library/LaunchDaemons/. Required Launch Daemons parameters include a Label to identify the task, Program to provide a path to the executable, and RunAtLoad to specify when the task is run. Launch Daemons are often used to provide access to shared resources, updates to software, or conduct automation tasks.(Citation: AppleDocs Launch Agent Daemons)(Citation: Methods of Mac Malware Persistence)(Citation: launchd Keywords for plists)*

Source: https://attack.mitre.org/techniques/T1543/004

T1546.001: Change Default File Association

Summary: *Adversaries may establish persistence by executing malicious content triggered by a file type association. When a file is opened, the default program used to open the file (also called the file association or handler) is checked. File association selections are stored in the Windows Registry and can be edited by users, administrators, or programs that have Registry access or by administrators using the built-in assoc utility.(Citation: Microsoft Change Default Programs)(Citation: Microsoft File Handlers)(Citation: Microsoft Assoc Oct 2017) Applications can modify the file association for a given file extension to call an arbitrary program when a file with the given extension is opened.*

Source: https://attack.mitre.org/techniques/T1546/001

T1546.004: Unix Shell Configuration Modification

Summary: *Adversaries may establish persistence through executing malicious commands triggered by a user's shell. User [Unix Shell](https://attack.mitre.org/techniques/T1059/004)s execute several configuration scripts at different points throughout the session based on events. For example, when a user opens a command-line interface or remotely logs in (such as via SSH) a login shell is initiated. The login shell executes scripts from the system (/etc) and the user's home directory (~/) to configure the environment. All login shells on a system use /etc/profile when initiated. These configuration scripts run at the permission level of their directory and are often used to set environment variables, create aliases, and customize the user's environment. When the shell exits or terminates, additional shell scripts are executed to ensure the shell exits appropriately.*

Source: https://attack.mitre.org/techniques/T1546/004

T1546.008: Accessibility Features

Summary: *Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by accessibility features. Windows contains accessibility features that may be launched with a key combination before a user has logged in (ex: when the user is on the Windows logon screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.*

Source: https://attack.mitre.org/techniques/T1546/008

T1546.016: Installer Packages

Summary: *Adversaries may establish persistence and elevate privileges by using an installer to trigger the execution of malicious content. Installer packages are OS specific and contain the resources an operating system needs to install applications on a system. Installer packages can include scripts that run prior to installation as well as after installation is complete. Installer scripts may inherit elevated permissions when executed. Developers often use these scripts to prepare the environment for installation, check requirements, download dependencies, and remove files after installation.(Citation: Installer Package Scripting Rich Trouton)*

Source: https://attack.mitre.org/techniques/T1546/016

T1547: Boot or Logon Autostart Execution

Summary: *Adversaries may configure system settings to automatically execute a program during system boot or logon 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 logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) 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.*

Source: https://attack.mitre.org/techniques/T1547

T1547.006: Kernel Modules and Extensions

Summary: *Adversaries may modify the kernel to automatically execute programs on system boot. Loadable Kernel Modules (LKMs) are pieces of code that can be loaded and unloaded into the kernel upon demand. They extend the functionality of the kernel without the need to reboot the system. For example, one type of module is the device driver, which allows the kernel to access hardware connected to the system.(Citation: Linux Kernel Programming)*

Source: https://attack.mitre.org/techniques/T1547/006

T1548: Abuse Elevation Control Mechanism

Summary: *Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk.(Citation: TechNet How UAC Works)(Citation: sudo man page 2018) An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.(Citation: OSX Keydnap malware)(Citation: Fortinet Fareit)*

Source: https://attack.mitre.org/techniques/T1548

T1550.004: Web Session Cookie

Summary: *Adversaries can use stolen session cookies to authenticate to web applications and services. This technique bypasses some multi-factor authentication protocols since the session is already authenticated.(Citation: Pass The Cookie)*

Source: https://attack.mitre.org/techniques/T1550/004

T1552.002: Credentials in Registry

Summary: *Adversaries may search the Registry on compromised systems for insecurely stored credentials. The Windows Registry stores configuration information that can be used by the system or other programs. Adversaries may query the Registry looking for credentials and passwords that have been stored for use by other programs or services. Sometimes these credentials are used for automatic logons.*

Source: https://attack.mitre.org/techniques/T1552/002

T1553.002: Code Signing

Summary: *Adversaries may create, acquire, or steal code signing materials to sign their malware or tools. Code signing provides a level of authenticity on a binary from the developer and a guarantee that the binary has not been tampered with. (Citation: Wikipedia Code Signing) The certificates used during an operation may be created, acquired, or stolen by the adversary. (Citation: Securelist Digital Certificates) (Citation: Symantec Digital Certificates) Unlike [Invalid Code Signature](https://attack.mitre.org/techniques/T1036/001), this activity will result in a valid signature.*

Source: https://attack.mitre.org/techniques/T1553/002

T1553.004: Install Root Certificate

Summary: *Adversaries may install a root certificate on a compromised system to avoid warnings when connecting to adversary controlled web servers. Root certificates are used in public key cryptography to identify a root certificate authority (CA). When a root certificate is installed, the system or application will trust certificates in the root's chain of trust that have been signed by the root certificate.(Citation: Wikipedia Root Certificate) Certificates are commonly used for establishing secure TLS/SSL communications within a web browser. When a user attempts to browse a website that presents a certificate that is not trusted an error message will be displayed to warn the user of the security risk. Depending on the security settings, the browser may not allow the user to establish a connection to the website.*

Source: https://attack.mitre.org/techniques/T1553/004

T1554: Compromise Host Software Binary

Summary: *Adversaries may modify host software binaries to establish persistent access to systems. Software binaries/executables provide a wide range of system commands or services, programs, and libraries. Common software binaries are SSH clients, FTP clients, email clients, web browsers, and many other user or server applications.*

Source: https://attack.mitre.org/techniques/T1554

T1556.006: Multi-Factor Authentication

Summary: *Adversaries may disable or modify multi-factor authentication (MFA) mechanisms to enable persistent access to compromised accounts.*

Source: https://attack.mitre.org/techniques/T1556/006

T1562.001: Disable or Modify Tools

Summary: *Adversaries may modify and/or disable security tools to avoid possible detection of their malware/tools and activities. This may take many forms, such as killing security software processes or services, modifying / deleting Registry keys or configuration files so that tools do not operate properly, or other methods to interfere with security tools scanning or reporting information. Adversaries may also disable updates to prevent the latest security patches from reaching tools on victim systems.(Citation: SCADAfence_ransomware)*

Source: https://attack.mitre.org/techniques/T1562/001

T1562.002: Disable Windows Event Logging

Summary: *Adversaries may disable Windows event logging to limit data that can be leveraged for detections and audits. Windows event logs record user and system activity such as login attempts, process creation, and much more.(Citation: Windows Log Events) This data is used by security tools and analysts to generate detections.*

Source: https://attack.mitre.org/techniques/T1562/002

T1562.003: Impair Command History Logging

Summary: *Adversaries may impair command history logging to hide commands they run on a compromised system. Various command interpreters keep track of the commands users type in their terminal so that users can retrace what they've done.*

Source: https://attack.mitre.org/techniques/T1562/003

T1562.004: Disable or Modify System Firewall

Summary: *Adversaries may disable or modify system firewalls in order to bypass controls limiting network usage. Changes could be disabling the entire mechanism as well as adding, deleting, or modifying particular rules. This can be done numerous ways depending on the operating system, including via command-line, editing Windows Registry keys, and Windows Control Panel.*

Source: https://attack.mitre.org/techniques/T1562/004

T1562.007: Disable or Modify Cloud Firewall

Summary: *Adversaries may disable or modify a firewall within a cloud environment to bypass controls that limit access to cloud resources. Cloud firewalls are separate from system firewalls that are described in [Disable or Modify System Firewall](https://attack.mitre.org/techniques/T1562/004).*

Source: https://attack.mitre.org/techniques/T1562/007

T1562.008: Disable or Modify Cloud Logs

Summary: *An adversary may disable or modify cloud logging capabilities and integrations to limit what data is collected on their activities and avoid detection. Cloud environments allow for collection and analysis of audit and application logs that provide insight into what activities a user does within the environment. If an adversary has sufficient permissions, they can disable or modify logging to avoid detection of their activities.*

Source: https://attack.mitre.org/techniques/T1562/008

T1562.009: Safe Mode Boot

Summary: *Adversaries may abuse Windows safe mode to disable endpoint defenses. Safe mode starts up the Windows operating system with a limited set of drivers and services. Third-party security software such as endpoint detection and response (EDR) tools may not start after booting Windows in safe mode. There are two versions of safe mode: Safe Mode and Safe Mode with Networking. It is possible to start additional services after a safe mode boot.(Citation: Microsoft Safe Mode)(Citation: Sophos Snatch Ransomware 2019)*

Source: https://attack.mitre.org/techniques/T1562/009

T1565.002: Transmitted Data Manipulation

Summary: *Adversaries may alter data en route to storage or other systems in order to manipulate external outcomes or hide activity, thus threatening the integrity of the data.(Citation: FireEye APT38 Oct 2018)(Citation: DOJ Lazarus Sony 2018) By manipulating transmitted data, adversaries may attempt to affect a business process, organizational understanding, and decision making.*

Source: https://attack.mitre.org/techniques/T1565/002

T1574.005: Executable Installer File Permissions Weakness

Summary: *Adversaries may execute their own malicious payloads by hijacking the binaries used by an installer. These processes may automatically execute specific binaries as part of their functionality or to perform other actions. If the permissions on the file system directory containing a target binary, or permissions on the binary itself, are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.*

Source: https://attack.mitre.org/techniques/T1574/005

T1574.006: Dynamic Linker Hijacking

Summary: *Adversaries may execute their own malicious payloads by hijacking environment variables the dynamic linker uses to load shared libraries. During the execution preparation phase of a program, the dynamic linker loads specified absolute paths of shared libraries from various environment variables and files, such as LD_PRELOAD on Linux or DYLD_INSERT_LIBRARIES on macOS.(Citation: TheEvilBit DYLD_INSERT_LIBRARIES)(Citation: Timac DYLD_INSERT_LIBRARIES)(Citation: Gabilondo DYLD_INSERT_LIBRARIES Catalina Bypass) Libraries specified in environment variables are loaded first, taking precedence over system libraries with the same function name.(Citation: Man LD.SO)(Citation: TLDP Shared Libraries)(Citation: Apple Doco Archive Dynamic Libraries) Each platform's linker uses an extensive list of environment variables at different points in execution. These variables are often used by developers to debug binaries without needing to recompile, deconflict mapped symbols, and implement custom functions in the original*

library.(Citation: Baeldung LD_PRELOAD)

Source: https://attack.mitre.org/techniques/T1574/006

T1574.007: Path Interception by PATH Environment Variable

Summary: *Adversaries may execute their own malicious payloads by hijacking environment variables used to load libraries. The PATH environment variable contains a list of directories (User and System) that the OS searches sequentially through in search of the binary that was called from a script or the command line.*

Source: https://attack.mitre.org/techniques/T1574/007

T1574.010: Services File Permissions Weakness

Summary: *Adversaries may execute their own malicious payloads by hijacking the binaries used by services. Adversaries may use flaws in the permissions of Windows services to replace the binary that is executed upon service start. These service processes may automatically execute specific binaries as part of their functionality or to perform other actions. If the permissions on the file system directory containing a target binary, or permissions on the binary itself are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.*

Source: https://attack.mitre.org/techniques/T1574/010

T1574.011: Services Registry Permissions Weakness

Summary: *Adversaries may execute their own malicious payloads by hijacking the Registry entries used by services. Adversaries may use flaws in the permissions for Registry keys related to services to redirect from the originally specified executable to one that they control, in order to launch their own code when a service starts. Windows stores local service configuration information in the Registry under HKLM\SYSTEM\CurrentControlSet\Services. The information stored under a service's Registry keys can be manipulated to modify a service's execution parameters through tools such as the service controller, sc.exe, [PowerShell](https://attack.mitre.org/techniques/T1059/001), or [Reg](https://attack.mitre.org/software/S0075). Access to Registry keys is controlled through access control lists and user permissions. (Citation: Registry Key Security)(Citation: malware_hides_service)*

Source: https://attack.mitre.org/techniques/T1574/011

T1606: Forge Web Credentials

Summary: *Adversaries may forge credential materials that can be used to gain access to web applications or Internet services. Web applications and services (hosted in cloud SaaS environments or on-premise servers) often use session cookies, tokens, or other materials to authenticate and authorize user access.*

Source: https://attack.mitre.org/techniques/T1606

Potential Threat Actors

2015 Ukraine Electric Power Attack uses: T1562.001

2016 Ukraine Electric Power Attack uses: T1543.003, T1554, T1562.002

APT1 uses: T1005

APT18 uses: T1083

APT19 uses: T1543.003

APT28 uses: T1005, T1014, T1083, T1134.001, T1528, T1542.003

APT28 Nearest Neighbor Campaign uses: T1562.004

APT29 uses: T1005, T1037, T1528, T1546.008, T1562.008

APT3 uses: T1005, T1083, T1543.003, T1546.008

APT32 uses: T1012, T1083, T1543.003, T1552.002

APT37 uses: T1005

APT38 uses: T1005, T1083, T1543.003, T1562.001, T1562.003, T1562.004, T1565.002

APT39 uses: T1005, T1012, T1083

APT41 uses: T1005, T1012, T1014, T1037, T1083, T1542.003, T1543.003, T1546.008, T1553.002, T1574.006

APT41 DUST uses: T1543.003, T1553.002

APT42 uses: T1539, T1547

APT5 uses: T1083, T1554

Agrius uses: T1005, T1543.003, T1562.001

Akira uses: T1562.001

Andariel uses: T1005

Aoqin Dragon uses: T1083

Aquatic Panda uses: T1005, T1543.003, T1562.001, T1574.006

ArcaneDoor uses: T1014, T1037, T1562.001, T1562.003

Axiom uses: T1005, T1546.008

BRONZE BUTLER uses: T1005, T1080, T1083, T1562.001

BlackByte uses: T1012, T1134.003, T1543.003, T1562.001, T1562.004

Blue Mockingbird uses: T1134, T1543.003

C0015 uses: T1005, T1083, T1553.002

C0017 uses: T1005, T1134

C0021 uses: T1027.009

C0026 uses: T1005

CURIUM uses: T1005

Carbanak uses: T1543.003, T1562.004

Chimera uses: T1012, T1083

Cinnamon Tempest uses: T1080, T1543.003

Cobalt Group uses: T1543.003

Confucius uses: T1083

CopyKittens uses: T1553.002

CostaRicto uses: T1005

Cutting Edge uses: T1005, T1554, T1562.001

Daggerfly uses: T1012, T1553.002

Dark Caracal uses: T1005, T1083

DarkVishnya uses: T1543.003

Darkhotel uses: T1080, T1083, T1553.002

Deep Panda uses: T1546.008

Dragonfly uses: T1005, T1012, T1083, T1562.004

Earth Lusca uses: T1543.003

Ember Bear uses: T1005, T1562.001

Evilnum uses: T1539

FIN13 uses: T1005, T1083, T1134.003

FIN6 uses: T1005, T1134, T1553.002, T1562.001

FIN7 uses: T1005, T1543.003, T1553.002

FIN8 uses: T1134.001

Fox Kitten uses: T1005, T1012, T1083, T1546.008

Frankenstein uses: T1005

GALLIUM uses: T1005, T1553.002

Gamaredon Group uses: T1005, T1080, T1083, T1562.001

Gorgon Group uses: T1562.001

HAFNIUM uses: T1005, T1083

HomeLand Justice uses: T1134.001, T1562.001, T1562.002

INC Ransom uses: T1562.001

Inception uses: T1005, T1083

Indrik Spider uses: T1012, T1562.001

KV Botnet Activity uses: T1083, T1562.001

Ke3chang uses: T1005, T1083, T1543.003

Kimsuky uses: T1005, T1012, T1083, T1539, T1543.003, T1546.001, T1553.002, T1562.001, T1562.004

LAPSUS$ uses: T1005

Lazarus Group uses: T1005, T1012, T1027.009, T1083, T1134.002, T1542.003, T1543.003, T1553.002, T1562.001, T1562.004

Leafminer uses: T1083

Leviathan uses: T1553.002

Leviathan Australian Intrusions uses: T1528, T1562.004

Lotus Blossom uses: T1012, T1083, T1134, T1539, T1543.003

LuminousMoth uses: T1005, T1083, T1539, T1553.002

Magic Hound uses: T1005, T1083, T1562.001, T1562.002, T1562.004

Molerats uses: T1553.002

Moonstone Sleet uses: T1027.009

Moses Staff uses: T1553.002, T1562.004

MuddyWater uses: T1083, T1562.001

Mustang Panda uses: T1083

Night Dragon uses: T1005, T1083, T1562.001

OilRig uses: T1005, T1012, T1543.003, T1553.002, T1562.004

Operation CuckooBees uses: T1005, T1083, T1543.003, T1547.006

Operation Dream Job uses: T1005, T1083, T1553.002

Operation Honeybee uses: T1005, T1083, T1543.003, T1553.002, T1574.011

Operation MidnightEclipse uses: T1005

Operation Wocao uses: T1005, T1012, T1083, T1562.004

PROMETHIUM uses: T1543.003, T1553.002

Patchwork uses: T1005, T1083, T1553.002

Play uses: T1083, T1562.001

Putter Panda uses: T1562.001

RedCurl uses: T1005, T1080, T1083, T1552.002

RedDelta Modified PlugX Infection Chain Operations uses: T1553.002

Rocke uses: T1014, T1037, T1562.001, T1562.004, T1574.006

Saint Bear uses: T1553.002, T1562.001

Salt Typhoon uses: T1562.004

Sandworm Team uses: T1005, T1083, T1539

Scattered Spider uses: T1083, T1539, T1553.002, T1556.006

Sea Turtle uses: T1562.003

ShadowRay uses: T1546.004

Sidewinder uses: T1083

Silence uses: T1553.002

SolarWinds Compromise uses: T1005, T1083, T1539, T1550.004, T1553.002, T1562.001, T1562.002, T1562.004

Sowbug uses: T1083

Star Blizzard uses: T1539, T1550.004

Stealth Falcon uses: T1005, T1012

Suckfly uses: T1553.002

TA2541 uses: T1562.001

TA505 uses: T1553.002, T1562.001

TA577 uses: T1027.009

TeamTNT uses: T1014, T1083, T1543.003, T1562.001, T1562.004

Threat Group-3390 uses: T1005, T1012, T1543.003, T1562.002

ToddyCat uses: T1005, T1083, T1562.004

Tropic Trooper uses: T1083, T1543.003

Turla uses: T1005, T1012, T1083, T1134.002, T1562.001

Velvet Ant uses: T1083, T1562.001, T1562.004

Volt Typhoon uses: T1005, T1012, T1083

Windigo uses: T1005, T1083

Winnti Group uses: T1014, T1083, T1553.002

Winter Vivern uses: T1083

Wizard Spider uses: T1005, T1543.003, T1553.002, T1562.001

ZIRCONIUM uses: T1012

admin@338 uses: T1083

menuPass uses: T1005, T1083, T1553.002

Vulnerability Analysis for CVE-2020-1574

Vulnerability Summary

CVSS Score (v3.1): 5.5 (MEDIUM)

No associated MITRE ATT&CK; techniques were found in the database.

Vulnerability Analysis for CVE-2020-1577

Vulnerability Summary

CVSS Score (v3.1): 7.8 (HIGH)

No associated MITRE ATT&CK; techniques were found in the database.

Vulnerability Analysis for CVE-2023-42981

Vulnerability Summary

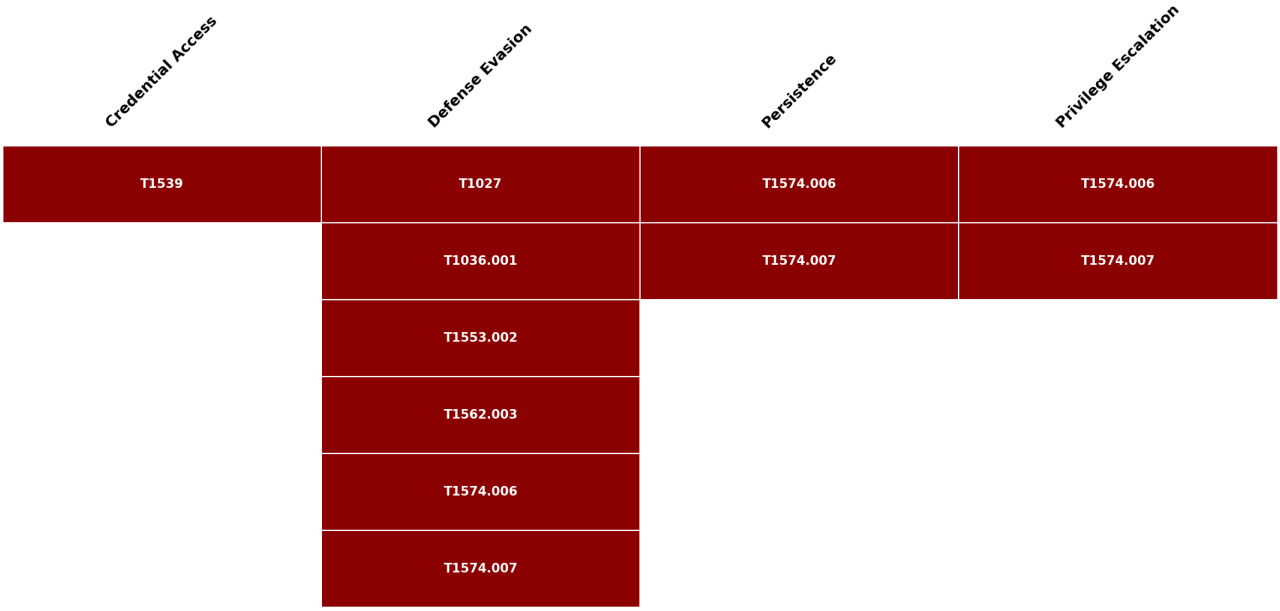
CVSS Score (v3.1): 5.4 (MEDIUM)

Weaknesses (CWE): 20, 707

Attack Patterns (CAPEC): 120, 42, 23, 231, 153, 277, 261, 136, 473, 104, 47, 22, 67, 468, 72, 28, 8, 24, 45, 88, 85, 664, 80, 81, 109, 108, 63, 278, 46, 73, 79, 10, 31, 83, 230, 279, 84, 14, 588, 52, 250, 3, 71, 13, 276, 182, 64, 78, 9, 135, 267, 7, 53, 43, 110, 101, 209

Tactical Summary (MITRE ATT&CK;)

Observed Tactics: Credential Access, Defense Evasion, Persistence, Privilege Escalation



ATT&CK; Technique Details

T1027: Obfuscated Files or Information

Summary: *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.*

Source: https://attack.mitre.org/techniques/T1027

T1036.001: Invalid Code Signature

Summary: *Adversaries may attempt to mimic features of valid code signatures to increase the chance of deceiving a user, analyst, or tool. Code signing provides a level of authenticity on a binary from the developer and a guarantee that the binary has not been tampered with. Adversaries can copy the metadata and signature information from a signed program, then use it as a template for an unsigned program. Files with invalid code signatures will fail digital signature validation checks, but they may appear more legitimate to users and security tools may improperly handle these files.(Citation: Threatexpress MetaTwin 2017)*

Source: https://attack.mitre.org/techniques/T1036/001

T1539: Steal Web Session Cookie

Summary: *An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing credentials. Web applications and services often use session cookies as an authentication token after a user has authenticated to a website.*

Source: https://attack.mitre.org/techniques/T1539

T1553.002: Code Signing

Summary: *Adversaries may create, acquire, or steal code signing materials to sign their malware or tools. Code signing provides a level of authenticity on a binary from the developer and a guarantee that the binary has not been tampered with. (Citation: Wikipedia Code Signing) The certificates used during an operation may be created, acquired, or stolen by the adversary. (Citation: Securelist Digital Certificates) (Citation: Symantec Digital Certificates) Unlike [Invalid Code Signature](https://attack.mitre.org/techniques/T1036/001), this activity will result in a valid signature.*

Source: https://attack.mitre.org/techniques/T1553/002

T1562.003: Impair Command History Logging

Summary: *Adversaries may impair command history logging to hide commands they run on a compromised system. Various command interpreters keep track of the commands users type in their terminal so that users can retrace what they've done.*

Source: https://attack.mitre.org/techniques/T1562/003

T1574.006: Dynamic Linker Hijacking

Summary: *Adversaries may execute their own malicious payloads by hijacking environment variables the dynamic linker uses to load shared libraries. During the execution preparation phase of a program, the dynamic linker loads specified absolute paths of shared libraries from various environment variables and files, such as LD_PRELOAD on Linux or DYLD_INSERT_LIBRARIES on macOS.(Citation: TheEvilBit DYLD_INSERT_LIBRARIES)(Citation: Timac DYLD_INSERT_LIBRARIES)(Citation: Gabilondo DYLD_INSERT_LIBRARIES Catalina Bypass) Libraries specified in environment variables are loaded first, taking precedence over system libraries with the same function name.(Citation: Man LD.SO)(Citation: TLDP Shared Libraries)(Citation: Apple Doco Archive Dynamic Libraries) Each platform's linker uses an extensive list of environment variables at different points in execution. These variables are often used by developers to debug binaries without needing to recompile, deconflict mapped symbols, and implement custom functions in the original library.(Citation: Baeldung LD_PRELOAD)*

Source: https://attack.mitre.org/techniques/T1574/006

T1574.007: Path Interception by PATH Environment Variable

Summary: *Adversaries may execute their own malicious payloads by hijacking environment variables used to load libraries. The PATH environment variable contains a list of directories (User and System) that the OS searches sequentially through in search of the binary that was called from a script or the command line.*

Source: https://attack.mitre.org/techniques/T1574/007

Potential Threat Actors

2016 Ukraine Electric Power Attack uses: T1027

APT-C-36 uses: T1027

APT3 uses: T1027

APT37 uses: T1027, T1036.001

APT38 uses: T1562.003

APT41 uses: T1027, T1553.002, T1574.006

APT41 DUST uses: T1553.002

APT42 uses: T1539

Aquatic Panda uses: T1574.006

ArcaneDoor uses: T1562.003

BackdoorDiplomacy uses: T1027

BlackOasis uses: T1027

C0015 uses: T1027, T1553.002

C0017 uses: T1027

CopyKittens uses: T1553.002

Daggerfly uses: T1553.002

Darkhotel uses: T1553.002

Earth Lusca uses: T1027

Evilnum uses: T1539

FIN6 uses: T1553.002

FIN7 uses: T1553.002

GALLIUM uses: T1027, T1553.002

Gallmaker uses: T1027

Gamaredon Group uses: T1027

Ke3chang uses: T1027

Kimsuky uses: T1027, T1539, T1553.002

Lazarus Group uses: T1553.002

Leviathan uses: T1553.002

Lotus Blossom uses: T1539

LuminousMoth uses: T1539, T1553.002

Molerats uses: T1553.002

Moonstone Sleet uses: T1027

Moses Staff uses: T1553.002

Mustang Panda uses: T1027

OilRig uses: T1553.002

Operation Dream Job uses: T1553.002

Operation Honeybee uses: T1553.002

PROMETHIUM uses: T1553.002

Patchwork uses: T1553.002

RedCurl uses: T1027

RedDelta Modified PlugX Infection Chain Operations uses: T1553.002

Rocke uses: T1027, T1574.006

Saint Bear uses: T1553.002

Sandworm Team uses: T1027, T1539

Scattered Spider uses: T1539, T1553.002

Sea Turtle uses: T1562.003

Silence uses: T1553.002

SolarWinds Compromise uses: T1539, T1553.002

Star Blizzard uses: T1539

Suckfly uses: T1553.002

TA505 uses: T1553.002

Windshift uses: T1027, T1036.001

Winnti Group uses: T1553.002

Wizard Spider uses: T1553.002

menuPass uses: T1553.002

Vulnerability Analysis for CVE-2023-42982

Vulnerability Summary

CVSS Score (v3.1): 6.4 (MEDIUM)

Weaknesses (CWE): 118, 119, 125, 664

Attack Patterns (CAPEC): 42, 60, 8, 123, 24, 61, 540, 62, 100, 45, 14, 196, 47, 44, 46, 21, 10, 9

Tactical Summary (MITRE ATT&CK;)

Observed Tactics: Credential Access, Defense Evasion, Lateral Movement, Privilege Escalation

ATT&CK; Technique Details

T1134: Access Token Manipulation

Summary: *Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token.*

Source: https://attack.mitre.org/techniques/T1134

T1134.001: Token Impersonation/Theft

Summary: *Adversaries may duplicate then impersonate another user's existing token to escalate privileges and bypass access controls. For example, an adversary can duplicate an existing token using `DuplicateToken` or `DuplicateTokenEx`.(Citation: DuplicateToken function) The token can then be used with `ImpersonateLoggedOnUser` to allow the calling thread to impersonate a logged on user's security context, or with `SetThreadToken` to assign the impersonated token to a thread.*

Source: https://attack.mitre.org/techniques/T1134/001

T1134.002: Create Process with Token

Summary: *Adversaries may create a new process with an existing token to escalate privileges and bypass access controls. Processes can be created with the token and resulting security context of another user using features such as CreateProcessWithTokenW and runas.(Citation: Microsoft RunAs)*

Source: https://attack.mitre.org/techniques/T1134/002

T1134.003: Make and Impersonate Token

Summary: *Adversaries may make new tokens and impersonate users to escalate privileges and bypass access controls. For example, if an adversary has a username and password but the user is not logged onto the system the adversary can then create a logon session for the user using the `LogonUser` function.(Citation: LogonUserW function) The function will return a copy of the new session's access token and the adversary can use `SetThreadToken` to assign the token to a thread.*

Source: https://attack.mitre.org/techniques/T1134/003

T1528: Steal Application Access Token

Summary: *Adversaries can steal application access tokens as a means of acquiring credentials to access remote systems and resources.*

Source: https://attack.mitre.org/techniques/T1528

T1539: Steal Web Session Cookie

Summary: *An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing credentials. Web applications and services often use session cookies as an authentication token after a user has authenticated to a website.*

Source: https://attack.mitre.org/techniques/T1539

T1550.004: Web Session Cookie

Summary: *Adversaries can use stolen session cookies to authenticate to web applications and services. This technique bypasses some multi-factor authentication protocols since the session is already authenticated.(Citation: Pass The Cookie)*

Source: https://attack.mitre.org/techniques/T1550/004

T1606: Forge Web Credentials

Summary: *Adversaries may forge credential materials that can be used to gain access to web applications or Internet services. Web applications and services (hosted in cloud SaaS environments or on-premise servers) often use session cookies, tokens, or other materials to authenticate and authorize user access.*

Source: https://attack.mitre.org/techniques/T1606

Potential Threat Actors

APT28 uses: T1134.001, T1528

APT29 uses: T1528

APT42 uses: T1539

BlackByte uses: T1134.003

Blue Mockingbird uses: T1134

C0017 uses: T1134

Evilnum uses: T1539

FIN13 uses: T1134.003

FIN6 uses: T1134

FIN8 uses: T1134.001

HomeLand Justice uses: T1134.001

Kimsuky uses: T1539

Lazarus Group uses: T1134.002

Leviathan Australian Intrusions uses: T1528

Lotus Blossom uses: T1134, T1539

LuminousMoth uses: T1539

Sandworm Team uses: T1539

Scattered Spider uses: T1539

SolarWinds Compromise uses: T1539, T1550.004

Star Blizzard uses: T1539, T1550.004

Turla uses: T1134.002

Vulnerability Analysis for CVE-2023-42983

Vulnerability Summary

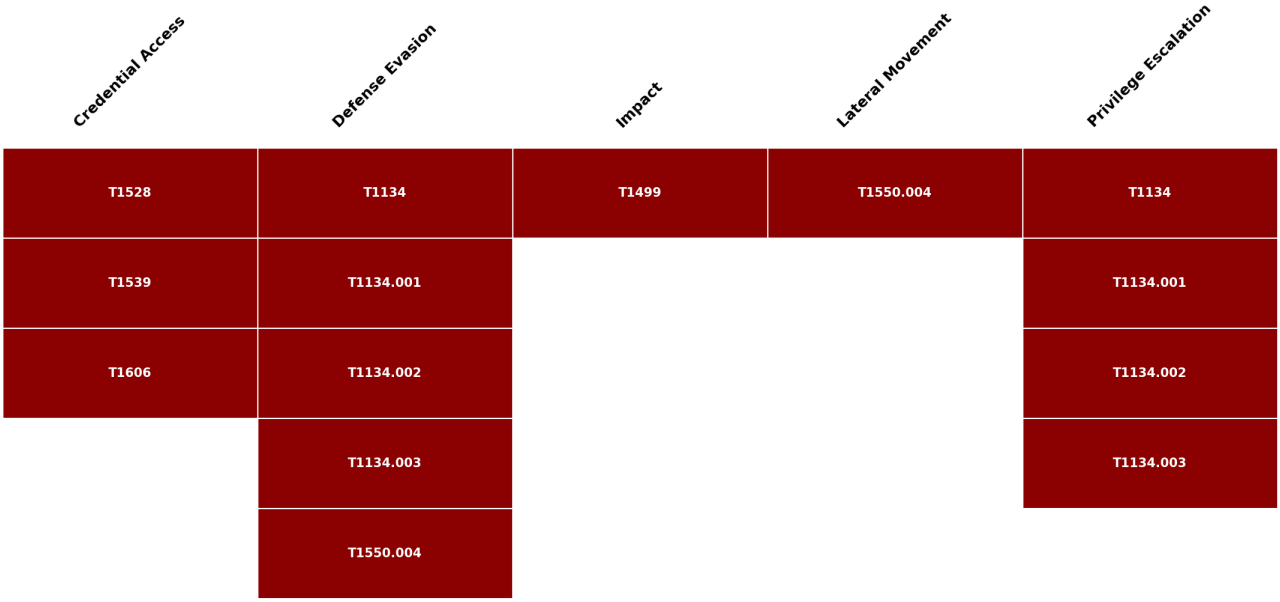
CVSS Score (v3.1): 6.4 (MEDIUM)

Weaknesses (CWE): 400, 664

Attack Patterns (CAPEC): 21, 196, 227, 60, 62, 147, 61, 492

Tactical Summary (MITRE ATT&CK;)

Observed Tactics: Credential Access, Defense Evasion, Impact, Lateral Movement, Privilege Escalation



ATT&CK; Technique Details

T1134: Access Token Manipulation

Summary: *Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token.*

Source: https://attack.mitre.org/techniques/T1134

T1134.001: Token Impersonation/Theft

Summary: *Adversaries may duplicate then impersonate another user's existing token to escalate privileges and bypass access controls. For example, an adversary can duplicate an existing token using `DuplicateToken` or `DuplicateTokenEx`.(Citation: DuplicateToken function) The token can then be used with `ImpersonateLoggedOnUser` to allow the calling thread to impersonate a logged on user's security context, or with `SetThreadToken` to assign the impersonated token to a thread.*

Source: https://attack.mitre.org/techniques/T1134/001

T1134.002: Create Process with Token

Summary: *Adversaries may create a new process with an existing token to escalate privileges and bypass access controls. Processes can be created with the token and resulting security context of another user using features such as CreateProcessWithTokenW and runas.(Citation: Microsoft RunAs)*

Source: https://attack.mitre.org/techniques/T1134/002

T1134.003: Make and Impersonate Token

Summary: *Adversaries may make new tokens and impersonate users to escalate privileges and bypass access controls. For example, if an adversary has a username and password but the user is not logged onto the system the adversary can then create a logon session for the user using the `LogonUser` function.(Citation: LogonUserW function) The function will return a copy of the new session's access token and the adversary can use `SetThreadToken` to assign the token to a thread.*

Source: https://attack.mitre.org/techniques/T1134/003

T1499: Endpoint Denial of Service

Summary: *Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users. Endpoint DoS can be performed by exhausting the system resources those services are hosted on or exploiting the system to cause a persistent crash condition. Example services include websites, email services, DNS, and web-based applications. Adversaries have been observed conducting DoS attacks for political purposes(Citation: FireEye OpPoisonedHandover February 2016) and to support other malicious activities, including distraction(Citation: FSISAC FraudNetDoS September 2012), hacktivism, and extortion.(Citation: Symantec DDoS October 2014)*

Source: https://attack.mitre.org/techniques/T1499

T1528: Steal Application Access Token

Summary: *Adversaries can steal application access tokens as a means of acquiring credentials to access remote systems and resources.*

Source: https://attack.mitre.org/techniques/T1528

T1539: Steal Web Session Cookie

Summary: *An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing credentials. Web applications and services often use session cookies as an authentication token after a user has*

authenticated to a website.

Source: https://attack.mitre.org/techniques/T1539

T1550.004: Web Session Cookie

Summary: *Adversaries can use stolen session cookies to authenticate to web applications and services. This technique bypasses some multi-factor authentication protocols since the session is already authenticated.(Citation: Pass The Cookie)*

Source: https://attack.mitre.org/techniques/T1550/004

T1606: Forge Web Credentials

Summary: *Adversaries may forge credential materials that can be used to gain access to web applications or Internet services. Web applications and services (hosted in cloud SaaS environments or on-premise servers) often use session cookies, tokens, or other materials to authenticate and authorize user access.*

Source: https://attack.mitre.org/techniques/T1606

Potential Threat Actors

APT28 uses: T1134.001, T1528

APT29 uses: T1528

APT42 uses: T1539

BlackByte uses: T1134.003

Blue Mockingbird uses: T1134

C0017 uses: T1134

Evilnum uses: T1539

FIN13 uses: T1134.003

FIN6 uses: T1134

FIN8 uses: T1134.001

HomeLand Justice uses: T1134.001

Kimsuky uses: T1539

Lazarus Group uses: T1134.002

Leviathan Australian Intrusions uses: T1528

Lotus Blossom uses: T1134, T1539

LuminousMoth uses: T1539

Sandworm Team uses: T1499, T1539

Scattered Spider uses: T1539

SolarWinds Compromise uses: T1539, T1550.004

Star Blizzard uses: T1539, T1550.004

Turla uses: T1134.002