# Persistence

Any access, action or configuration change on a system that gives an adversary a persistent presence on a system. Adversaries will often need to maintain access to systems through interruptions such as system rebooting or other failures that would require a remote access tool to restart in order for them to regain access.

Below is a list of all the Persistence techniques in ATT&CK:

| Technique | ID | Tactics | Technical Description |
|---|---|---|---|
| | | | Windows contains accessibility features that may be launched with a key combination before a user has logged in (for example when they are 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.<br>Two of these accessibility programs are "C:\Windows\System32\utilman.exe", launched when the Windows + U key combination is pressed and "C:\Windows\System32\sethc.exe", launched when the shift key is pressed five times. |

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com

Special pages
Printable version
Permanent link
Page information
Browse properties

| | | | |
|---|---|---|---|
| Accessibility features | 1015 | Persistence<br>Privilege Escalation | Depending on the version of Windows, the adversary will take advantage of this features in different ways:<br>On Windows XP and Windows Server 2003/R2, the program (e.g. "C:\Windows\System32\utilman.exe") may be replaced with cmd.exe (or another program that provides backdoor access). Then pressing the appropriate key combination at the login screen while sitting at the keyboard or when connected over RDP will cause the replaced file to be executed with SYSTEM privileges.<br>On Windows Vista and later and Windows Server 2008 and later: A registry key may be modified that configures cmd.exe, or another program that provides backdoor access, as a "debugger" for the accessibility program (e.g. utilman.exe). Then pressing the appropriate key combination at the login screen while sitting at the keyboard or when connected over RDP will cause the "debugger" program to be executed with SYSTEM privileges. |
| AddMonitor | 1013 | Privilege Escalation<br>Persistence | The AddMonitor application programming interface (API) can be called to register a DLL to be loaded at startup. This DLL is located in C:\Windows\System32 and will be loaded by spoolsv.exe on boot. Adversaries may use this API to load malicious code at startup. This same functionality is achieved by creating specifically formatted registry keys at |

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com

| | | | |
|---|---|---|---|
| | | | "HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors". |
| Basic Input/Output System | 1019 | Persistence | The BIOS (Basic Input/Output System), which underlies the functionality of an operating system, may be modified to perform malicious activity. |
| DLL search order hijacking | 1038 | Persistence<br>Privilege Escalation | Windows systems use a common method to look for required DLLs to load into a program. Adversaries may take advantage of the Windows DLL search order and programs that ambiguously specify DLLs to gain privilege escalation and persistence.<br>Adversaries may perform DLL preloading, also called binary planting attacks, by placing a malicious DLL with the same name as an ambiguously specified DLL in a location that Windows searches before the legitimate DLL. Often this location is the current working directory of the program. Remote DLL preloading attacks occur when a program sets its current directory to a remote location such as a web share, before loading a DLL. Adversaries may use this behavior to cause the program to load a malicious DLL.<br>Adversaries may also directly modify the way a program loads DLLs by replacing an existing DLL or modifying a .manifest or .local file to cause a different DLL to be loaded by the program to maintain persistence or privilege escalation. |

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com

| | | | |
|---|---|---|---|
| | | | Programs which fall victim path hijacking may appear to behave normally because malicious DLLs may be configured to also load the legitimate DLLs they were meant to replace. |
| Edit default file handlers | 1042 | Privilege Escalation<br>Persistence | When a file is opened, its file handler is checked to determine which program opens the file. File handlers are stored in the registry and can be edited by programs that have registry access. Applications can modify the file handler for a given file extension to call an arbitrary program when a file with the given extension is opened. |
| Hypervisor rootkit | 1062 | Persistence | A hypervisor is a software layer that sits between the operating system and the processor. It presents a virtual running environment to the operating system. An example of a common hypervisor is Xen. Because a hypervisor operates at a level below the operating system it can hide its existence from the operating system. |
| Legitimate Credentials | 1078 | Privilege Escalation<br>Defense Evasion<br>Persistence | Adversaries may steal the credentials of a specific user or service account using Credential Access techniques. Compromised credentials may be used to bypass access controls placed on various resources on hosts and within the network and may even be used for persistent access to remote systems. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. The adversary may choose not to use malware or tools in conjunction with |

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com

| | | | |
|---|---|---|---|
| | | Persistence | the legitimate access those credentials provide to make it harder to detect their presence. The overlap of credentials and permissions across a network is of concern because the adversary may be able to pivot across accounts and bypass any access controls. |
| Logon scripts | 1037 | Lateral Movement<br>Persistence | Windows allows logon scripts to be run whenever a specific user or users logon to a system. If adversaries can access these scripts, they may insert additional code into the logon script. This code can allow them to maintain persistence or move laterally within an enclave because it is executed every time the affected user or users logon to a computer. Modifying logon scripts can effectively bypass workstation and enclave firewalls. Depending on the access configuration of the logon scripts, either local credentials or a remote administrative account may be necessary. |
| Master boot record | 1067 | Persistence | The master boot record (MBR) is the section of disk that is first loaded after completing hardware initialization by the BIOS. It is the location of the boot loader. If an adversary has raw access to the boot drive, they may overwrite this area diverting execution during startup from the normal bootloader to adversary code. |
| | | | When Windows starts, it also starts programs called services. A service's configuration information, including the start executable, is stored in the registry. Adversaries |

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com

| | | | |
|---|---|---|---|
| Modify existing service | 1031 | Persistence | may modify an existing service to run adversary software by using tools that modify the registry (such as the command "sc") or by directly modifying the registry. Modifying existing services may break existing services or may enable services that are disabled/not commonly used. |
| New service | 1050 | Privilege Escalation<br>Persistence | When Windows starts, it also starts programs called services. A service's configuration information, including the service's executable, is stored in the registry. Adversaries may install a new service which will be executed at startup by directly modifying the registry or by using tools which do so. The service name may be disguised by using a name from a related operating system or benign software. Services may be created with ADMIN privileges but are run with SYSTEM privileges so a service may be used to escalate privileges from ADMIN to SYSTEM. |
| | | | Path interception occurs when an executable is placed in a specially crafted path so that it is executed instead of the intended target.<br>There are multiple distinct vulnerabilities or misconfigurations that adversaries take advantage of when performing path interception: unquoted paths, path environment variable misconfigurations, and search order hijacking. The first vulnerability deals with full program paths, while the second and third occur when program |

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com

|  |  |  |  |
|---|---|---|---|
| Path interception | 1034 | Persistence<br>Privilege Escalation | paths are not specified.<br>**Unquoted Paths**<br>Service paths (stored in Windows Registry keys) and shortcut paths are vulnerable to path interception if the path has one or more spaces and is not surrounded by quotation marks (e.g. C:\unsafe path with space\program.exe vs. "C:\safe path with space\program.exe"). An adversary can place an executable in a higher level directory of the path and Windows will resolve that executable instead of the intended executable. For example if the path in a shortcut is C:\program files\myapp.exe an adversary may create a program at C:\program.exe which will be run instead of the intended program.<br>**Path Environment Variable Misconfiguration**<br>The path environment variable contains a list of directories. Certain methods of executing a program (namely using cmd.exe or the command line) rely solely on the path environment variable to determine the locations that are searched for a program when the path for the program is not given. If any directories are listed in the path environment variable before the windows directory, "%SystemRoot%\system32" ("C:\Windows\system32"), a |

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com

program may be placed in the preceding directory that is named the same as a Windows program (such as cmd, powershell, or python) which will be executed when that command is executed from the command line.

For example, if the path "C:\example path" precedes "C:\Windows\system32" in the path environment variable, a program that is named net.exe and placed in "C:\example path" will be called instead of the Windows system "net" when "net" is executed from the commandline.

### Search order Hijacking

Search order hijacking occurs when an adversary abuses the order that windows searches for programs that are not given a path. Depending on the method that is used to execute the program, the search order differs. However it is common for Windows to search in the directory of the initiating program before searching through the Windows system directory. If an adversary finds a program vulnerable to search order hijacking (i.e. ap program that does not specify the path to an executable), they may take advantage of this vulnerability by creating a program named after improperly specified program and placing it within the initiating program's directory.

For example, if "example.exe" runs invokes "cmd.exe" with the commandline argument "net user". An adversary may

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com

| | | | |
|---|---|---|---|
| | | | place a program called "net.exe" within example.exe's directory that will be run instead of the Windows system utility net.<br>Search order hijacking is also a common practice for hijacking DLL loads. |
| Registry run keys / start folder | 1060 | Persistence | Adding a program to the "run keys" in the Registry will cause the program to be run when the computer starts. Adding programs to the start folder will cause them to run at startup. |
| Scheduled task | 1053 | Execution<br>Persistence<br>Privilege Escalation | Windows commands "at" and "schtasks", along with the Windows Task Scheduler schedule tasks to be run at a time in the future. Task scheduling may be used to execute programs on a scheduled basis to persist adversary code or gain SYSTEM privileges. Task scheduling requires administrator privileges, but tasks may be configured to run with SYSTEM privileges, representing an escalation of privilege. |
| Service file permissions weakness | 1044 | Privilege Escalation<br>Persistence | If the file system location of a service executable is modifiable by the user, it may be overwritten by another executable. An adversary may use this capability to gain SYSTEM privileges by putting their own executable in place of the service executable. Once the service is started, either directly by the user (requiring ADMIN privileges) or through some other means, the replaced executable will run instead of they original service executable. |

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com

| | | | |
|---|---|---|---|
| Service registry permissions weakness | 1058 | Privilege Escalation<br>Persistence | If the binPath/ImagePath registry value for a service is not properly secured a malicious user can change the path to point to a different executable under their control. Upon starting the service that will then run performing whatever action the user chose. |
| Shortcut modification | 1023 | Persistence<br>Privilege Escalation | Shortcuts store the location of the program that will be executed when the shortcut is clicked. The adversary may edit or replace a shortcut so when it is clicked a different program is run. |
| Windows Management Instrumentation event subscription | 1084 | Persistence | Windows Management Instrumentation (WMI) can be used to install event filters, consumers, and bindings which execute code when a defined event occurs. Adversaries may use the capabilities of WMI to subscribe to an event and execute arbitrary code when that event occurs. Examples of events that may be subscribed to are the wall clock time or the computer's uptime. |
| Winlogon helper DLL | 1004 | Persistence | Winlogon is a part of Windows that performs logon actions. In Windows systems prior to Windows Vista, a registry key can be modified that causes Winlogon to load a DLL on startup. Adversaries may take advantage of this feature to load adversarial code at startup. |

This page was last modified on 4 November 2014, at 15:11.

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com

Copyright © 2015, The MITRE Corporation. ATT&CK and ATT&CK Matrix are trademarks of The MITRE Corporation

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com