THE BRIDGE

CYBER SECURITY

Post-Explotación: Persistencia Windows

Persistencia. Windows

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/local/ps_wmi_exec	2012-08-19	excellent	No	Authenticated WMI Exec via Powershell
1	exploit/windows/local/vss_persistence	2011-10-21	excellent	No	Persistent Payload in Windows Volume Shadow Copy
2	post/windows/manage/sshkey_persistence		good	No	SSH Key Persistence
3	post/windows/manage/sticky_keys		normal	No	Sticky Keys Persistence Module
4	exploit/windows/local/wmi_persistence	2017-06-06	normal	No	WMI Event Subscription Persistence
5	post/windows/gather/enum_ad_managedby_groups		normal	No	Windows Gather Active Directory Managed Groups
6	post/windows/manage/persistence_exe		normal	No	Windows Manage Persistent EXE Payload Installer
7	exploit/windows/local/s4u_persistence	2013-01-02	excellent	No	Windows Manage User Level Persistent Payload Installer
8	exploit/windows/local/persistence	2011-10-19	excellent	No	Windows Persistent Registry Startup Payload Installer
9	exploit/windows/local/persistence_service	2018-10-20	excellent	No	Windows Persistent Service Installer
10	exploit/windows/local/registry_persistence	2015-07-01	excellent	Yes	Windows Registry Only Persistence
11	exploit/windows/local/persistence_image_exec_options	2008-06-28	excellent	No	Windows Silent Process Exit Persistence

.001	Registry Run Keys / Startup Folder	Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. These programs will be executed under the context of the user and will have the account's associated permissions level.
.003	Windows Service	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. Windows service configuration information, including the file path to the service's executable or recovery programs/commands, is stored in the Windows Registry.

Persistencia. Windows

Un vistazo a Mitre: https://attack.mitre.org/techniques/T1547/001/

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Other sub-techniques of Boot or Logon Autostart Execution (14)

Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in.[1] These programs will be executed under the context of the user and will have the account's associated permissions level.

The following run keys are created by default on Windows systems:

- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce`

Run keys may exist under multiple hives.[2][3] The `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx` is also available but is not created by default on Windows Vista and newer. Registry run key entries can reference programs directly or list them as a dependency.[1] For example, it is possible to load a DLL

ID: T1547.001

Sub-technique of: T1547

ⓘ Tactics: Persistence, Privilege Escalation

ⓘ Platforms: Windows

ⓘ Permissions Required: Administrator, User

Contributors: Dray Agha, @Purp1eW0lf, Huntress Labs; Harun Küßner; Oddvar Moe, @oddvarmoe

Version: 2.0

Created: 23 January 2020

Last Modified: 16 October 2023

Version Permalink

Home > Techniques > Enterprise > Create or Modify System Process

Create or Modify System Process

Sub-techniques (5)

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.[1] On macOS, launchd processes known as Launch Daemon and Launch Agent are run to finish system initialization and load user specific parameters.[2]

Adversaries may install new services, daemons, or agents that can be configured to execute at startup or a repeatable interval in order to establish persistence. Similarly, adversaries may modify existing services, daemons, or agents to achieve the same effect.

Services, daemons, or agents may be created with administrator privileges but executed under root/SYSTEM privileges. Adversaries may leverage this functionality to create or modify system processes in order to escalate privileges.[3]

ID: T1543

Sub-techniques: T1543.001, T1543.002, T1543.003, T1543.004, T1543.005

ⓘ Tactics: Persistence, Privilege Escalation

ⓘ Platforms: Containers, Linux, Windows, macOS

Version: 1.2

Created: 10 January 2020

Last Modified: 15 February 2024

Version Permalink


THE
BRIDGE