Boot or Logon Autostart Execution

Sub-techniques (14)

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.[1][2][3][4][5] These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel.

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

ID: T1547

Sub-techniques: T1547.001, T1547.002, T1547.003, T1547.004, T1547.005, T1547.006, T1547.007, T1547.008, T1547.009, T1547.010, T1547.012, T1547.013, T1547.014, T1547.015

ⓘ

Tactics: Persistence, Privilege Escalation

ⓘ

Platforms: Linux, Network, Windows, macOS

ⓘ

Permissions Required: Administrator, User, root

Version: 1.2

Created: 23 January 2020

Last Modified: 12 September 2024

Version Permalink

Procedure Examples

ID	Name	Description
S0651	BoxCaon	BoxCaon established persistence by setting the `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\load` registry key to point to its executable.[6]
S0567	Dtrack	Dtrack's RAT makes a persistent target file with auto execution on the host start.[7]
S0084	Mis-Type	Mis-Type has created registry keys for persistence, including `HKCU\Software\bkfouerioyou`, `HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{6afa8072-b2b1-31a8-b5c1-{Unique Identifier}`, and `HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{3BF41072-B2B1-31A8-B5C1-{Unique Identifier}`.[8]
S0083	Misdat	Misdat has created registry keys for persistence, including `HKCU\Software\dnimtsoleht\StubPath`, `HKCU\Software\snimtsOleht\StubPath`, `HKCU\Software\Backtsaleht\StubPath`, `HKLM\SOFTWARE\Microsoft\Active Setup\Installed. Components\{3bf41072-b2b1-21c8-b5c1-bd56d32fbda7}`, and `HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{3ef41072-a2f1-21c8-c5c1-70c2c3bc7905}`.[8]
S0653	xCaon	xCaon has added persistence via the Registry key `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\load` which causes the malware to run each time any user logs in.[6]

Mitigations

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

Detection

ID	Data Source	Data Component	Detects
DS0017	Command	Command Execution	Monitor executed commands and arguments that 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.
DS0027	Driver	Driver Load	Monitor for unusual kernel driver installation activity that 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.
DS0022	File	File Creation	Monitor for newly constructed files that 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.
		File Modification	Monitor for changes made to files that 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.
DS0008	Kernel	Kernel Module Load	Monitor for unusual kernel driver installation activity that 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.
DS0011	Module	Module Load	Monitor DLL loads by processes, specifically looking for DLLs that are not recognized or not normally loaded into a process. Look for abnormal process behavior that may be due to a process loading a malicious DLL.
DS0009	Process	OS API Execution	Monitor for API calls that 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.
		Process Creation	Suspicious program execution as autostart programs may show up as outlier processes that have not been seen before when compared against historical data to increase confidence of malicious activity, data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as network connections made for Command and Control, learning details about the environment through Discovery, and Lateral Movement.
DS0024	Windows Registry	Windows Registry Key Creation	Monitor for additions of mechanisms that could be used to trigger autostart execution, such as relevant additions to the Registry.
		Windows Registry Key Modification	Monitor for modifications of mechanisms that could be used to trigger autostart execution, such as relevant additions to the Registry.

References

1. Microsoft. (n.d.). Run and RunOnce Registry Keys. Retrieved September 12, 2024.
2. Microsoft. (n.d.). Authentication Packages. Retrieved March 1, 2017.
3. Microsoft. (n.d.). Time Provider. Retrieved March 26, 2018.
4. Langendorf, S. (2013, September 24). Windows Registry Persistence, Part 2: The Run Keys and Search-Order. Retrieved April 11, 2018.
5. Pomerantz, O., Salzman, P.. (2003, April 4). The Linux Kernel Module Programming Guide. Retrieved April 6, 2018.
6. CheckPoint Research. (2021, July 1). IndigoZebra APT continues to attack Central Asia with evolving tools. Retrieved September 24, 2021.
7. Konstantin Zykov. (2019, September 23). Hello! My name is Dtrack. Retrieved January 20, 2021.
8. Gross, J. (2016, February 23). Operation Dust Storm. Retrieved December 22, 2021.