Boot or Logon Autostart Execution: Winlogon Helper DLL, Sub-technique T1547.004 - Enterprise

Archived: 2026-04-02 10:38:08 UTC

Adversaries may abuse features of Winlogon to execute DLLs and/or executables when a user logs in. Winlogon.exe is a Windows component responsible for actions at logon/logoff as well as the secure attention sequence (SAS) triggered by Ctrl-Alt-Delete. Registry entries in `HKLM\Software[\Wow6432Node\]\Microsoft\Windows NT\CurrentVersion\Winlogon\` and `HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\` are used to manage additional helper programs and functionalities that support Winlogon.[1]

Malicious modifications to these Registry keys may cause Winlogon to load and execute malicious DLLs and/or executables. Specifically, the following subkeys have been known to be possibly vulnerable to abuse: [1]

- Winlogon\Notify - points to notification package DLLs that handle Winlogon events
- Winlogon\Userinit - points to userinit.exe, the user initialization program executed when a user logs on
- Winlogon\Shell - points to explorer.exe, the system shell executed when a user logs on

Adversaries may take advantage of these features to repeatedly execute malicious code and establish persistence.

Source: https://attack.mitre.org/techniques/T1547/004