Boot or Logon Autostart Execution: Active Setup, Sub-technique T1547.014 - Enterprise

Archived: 2026-04-05 13:27:56 UTC

Adversaries may achieve persistence by adding a Registry key to the Active Setup of the local machine. Active Setup is a Windows mechanism that is used to execute programs when a user logs in. The value stored in the Registry key will be executed after a user logs into the computer.[1] These programs will be executed under the context of the user and will have the account's associated permissions level.

Adversaries may abuse Active Setup by creating a key under `HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\` and setting a malicious value for `StubPath`. This value will serve as the program that will be executed when a user logs into the computer.[2][3][4][5][6]

Adversaries can abuse these components to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use Masquerading to make the Registry entries look as if they are associated with legitimate programs.

Source: https://attack.mitre.org/techniques/T1547/014