

Boot or Logon Initialization Scripts: Logon Script (Windows), Sub-technique T1037.001 - Enterprise

Archived: 2026-04-05 14:04:11 UTC

Adversaries may use Windows logon scripts automatically executed at logon initialization to establish persistence. Windows allows logon scripts to be run whenever a specific user or group of users log into a system.^[1] This is done via adding a path to a script to the `HKCU\Environment\UserInitMprLogonScript` Registry key.^[2]

Adversaries may use these scripts to maintain persistence on a single system. Depending on the access configuration of the logon scripts, either local credentials or an administrator account may be necessary.

Source: <https://attack.mitre.org/techniques/T1037/001>