Event Triggered Execution: PowerShell Profile, Sub-technique T1546.013 - Enterprise

Archived: 2026-04-05 12:39:49 UTC

Adversaries may gain persistence and elevate privileges by executing malicious content triggered by PowerShell profiles. A PowerShell profile (`profile.ps1`) is a script that runs when PowerShell starts and can be used as a logon script to customize user environments.

PowerShell supports several profiles depending on the user or host program. For example, there can be different profiles for PowerShell host programs such as the PowerShell console, PowerShell ISE or Visual Studio Code. An administrator can also configure a profile that applies to all users and host programs on the local computer. [1]

Adversaries may modify these profiles to include arbitrary commands, functions, modules, and/or PowerShell drives to gain persistence. Every time a user opens a PowerShell session the modified script will be executed unless the `-NoProfile` flag is used when it is launched. [2]

An adversary may also be able to escalate privileges if a script in a PowerShell profile is loaded and executed by an account with higher privileges, such as a domain administrator. [3]
