# TTP Detail – T1546.013

## TTP Information

Name: PowerShell Profile

Description: Adversaries may gain persistence and elevate privileges by executing malicious content triggered by PowerShell profiles. A PowerShell profile (<code>profile.ps1</code>) is a script that runs when [PowerShell](https://attack.mitre.org/techniques/T1059/001) starts and can be used as a logon script to customize user environments.

[PowerShell](https://attack.mitre.org/techniques/T1059/001) supports several profiles depending on the user or host program. For example, there can be different profiles for [PowerShell](https://attack.mitre.org/techniques/T1059/001) 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. (Citation: Microsoft About Profiles)

Adversaries may modify these profiles to include arbitrary commands, functions, modules, and/or [PowerShell](https://attack.mitre.org/techniques/T1059/001) drives to gain persistence. Every time a user opens a [PowerShell](https://attack.mitre.org/techniques/T1059/001) session the modified script will be executed unless the <code>-NoProfile</code> flag is used when it is launched. (Citation: ESET Turla PowerShell May 2019)

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. (Citation: Wits End and Shady PowerShell Profiles)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: privilege-escalation

**•** mitre-attack: persistence

## APTs (Intrusion Sets)

* Turla