Sign in

redcanaryco / **atomic-red-team** Public

Notifications | Fork 2.8k | Star 9.7k

Code | Issues 6 | Pull requests 5 | Actions | Wiki | Security | Insights

atomic-red-team / atomics / T1546.007 / **T1546.007.md**

44 lines (20 loc) · 1.66 KB

Preview | Code | Blame | Raw

T1546.007 - Netsh Helper DLL

Description from ATT&CK

> Adversaries may establish persistence by executing malicious content triggered by Netsh Helper DLLs. Netsh.exe (also referred to as Netshell) is a command-line scripting utility used to interact with the network configuration of a system. It contains functionality to add helper DLLs for extending functionality of the utility.(Citation: TechNet Netsh) The paths to registered netsh.exe helper DLLs are entered into the Windows Registry at `HKLM\SOFTWARE\Microsoft\Netsh`.
> Adversaries can use netsh.exe helper DLLs to trigger execution of arbitrary code in a persistent manner. This execution would take place anytime netsh.exe is executed, which could happen automatically, with another persistence technique, or if other software (ex: VPN) is present on the system that executes netsh.exe as part of its normal functionality.(Citation: Github Netsh Helper CS Beacon)(Citation: Demaske Netsh Persistence)

Atomic Tests

- Atomic Test #1 - Netsh Helper DLL Registration

Atomic Test #1 - Netsh Helper DLL Registration

Netsh interacts with other operating system components using dynamic-link library (DLL) files

Supported Platforms: Windows

auto_generated_guid: 3244697d-5a3a-4dfc-941c-550f69f91a4d

Inputs:

Name	Description	Type	Default Value
helper_file	Path to DLL	Path	C:\Path\file.dll

Attack Commands: Run with `command_prompt`!

```
netsh.exe add helper #{helper_file}
```