55 lines (29 loc) · 2.16 KB

T1547.010 - Port Monitors

Description from ATT&CK

> Adversaries may use port monitors to run an adversary supplied DLL during system boot for persistence or privilege escalation. A port monitor can be set through the `AddMonitor` API call to set a DLL to be loaded at startup.(Citation: AddMonitor) This DLL can be located in `C:\Windows\System32` and will be loaded by the print spooler service, spoolsv.exe, on boot. The spoolsv.exe process also runs under SYSTEM level permissions.(Citation: Bloxham) Alternatively, an arbitrary DLL can be loaded if permissions allow writing a fully-qualified pathname for that DLL to `HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors`.
> The Registry key contains entries for the following:
>
> - Local Port
> - Standard TCP/IP Port
> - USB Monitor
> - WSD Port

> Adversaries can use this technique to load malicious code at startup that will persist on system reboot and execute as SYSTEM.

Atomic Tests

- Atomic Test #1 - Add Port Monitor persistence in Registry

Atomic Test #1 - Add Port Monitor persistence in Registry

Add key-value pair to a Windows Port Monitor registry. On the subsequent reboot dll will be execute under spoolsv with NT AUTHORITY/SYSTEM privilege.

Supported Platforms: Windows

auto_generated_guid: d34ef297-f178-4462-871e-9ce618d44e50

Inputs:

Name	Description	Type	Default Value
monitor_dll	Addition to port monitor registry key. Normally refers to a DLL name in C:\Windows\System32. arbitrary DLL can be loaded if permissions allow writing a fully-qualified pathname for that DLL.	Path	C:\Path\AtomicRedTeam.dll

Attack Commands: Run with `command_prompt`! Elevation Required (e.g. root or admin)

```
reg add "hklm\system\currentcontrolset\control\print\monitors\ART" /v "Atomic Red
```

Cleanup Commands:

```
reg delete "hklm\system\currentcontrolset\control\print\monitors\ART" /f >nul 2>&1
```