Product ∨   Solutions ∨   Resources ∨   Open Source ∨   Enterprise ∨   Pricing   Sign in   Sign up

☐ redcanaryco / atomic-red-team   Public   🔔 Notifications   ⑂ Fork 2.8k   ☆ Star 9.7k

<> Code   ⊙ Issues 6   ⑂ Pull requests 5   ▶ Actions   📖 Wiki   ⊘ Security   ⩘ Insights

Files

⑂ f339e7d ▾

🔍 Go to file

> 📁 .github
> 📁 atomic_red_team
∨ 📁 atomics
  > 📁 Indexes
  > 📁 T1003.001
  > 📁 T1003.002
  > 📁 T1003.003
  > 📁 T1003.004
  > 📁 T1003.005
  > 📁 T1003.006
  > 📁 T1003.007
  > 📁 T1003.008
  > 📁 T1003
  > 📁 T1006
  > 📁 T1007
  > 📁 T1010
  > 📁 T1012
  > 📁 T1014
  > 📁 T1016
  > 📁 T1018
  > 📁 T1020
  > 📁 T1021.001
  > 📁 T1021.002
  > 📁 T1021.003
  > 📁 T1021.006
  > 📁 T1027.001
  > 📁 T1027.002
  > 📁 T1027.004
  > 📁 T1027
  > 📁 T1030
  > 📁 T1033
  > 📁 T1036.003
  > 📁 T1036.004
  > 📁 T1036.005
  > 📁 T1036.006
  > 📁 T1036

atomic-red-team / atomics / T1547.010 / **T1547.010.md** 📋   ⋯

🐙 Atomic Red Team doc generat...   Generated docs from job=generate-d...   819934c · 2 years ago   🕘 History

Preview   Code   Blame   55 lines (29 loc) · 2.16 KB   Raw 📋 ⬇   ☰

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	Path	C:\Path\AtomicRedTeam.dll

	permissions allow writing a fully-qualified pathname for that DLL.		

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

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

Cleanup Commands:

```
reg delete "hklm\system\currentcontrolset\control\print\monitors\ART" /f
```