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 / T1571 / **T1571.md**

80 lines (37 loc) · 2 KB

Preview Code Blame Raw

T1571 - Non-Standard Port

Description from ATT&CK

> Adversaries may communicate using a protocol and port paring that are typically not associated. For example, HTTPS over port 8088(Citation: Symantec Elfin Mar 2019) or port 587(Citation: Fortinet Agent Tesla April 2018) as opposed to the traditional port 443. Adversaries may make changes to the standard port used by a protocol to bypass filtering or muddle analysis/parsing of network data.

Atomic Tests

- Atomic Test #1 - Testing usage of uncommonly used port with PowerShell
- Atomic Test #2 - Testing usage of uncommonly used port

Atomic Test #1 - Testing usage of uncommonly used port with PowerShell

Testing uncommonly used port utilizing PowerShell. APT33 has been known to attempt telnet over port 8081. Upon execution, details about the successful port check will be displayed.

Supported Platforms: Windows

auto_generated_guid: 21fe622f-8e53-4b31-ba83-6d333c2583f4

Inputs:

Name	Description	Type	Default Value
port	Specify uncommon port number	String	8081
domain	Specify target hostname	String	google.com

Attack Commands: Run with `powershell`!

```
Test-NetConnection -ComputerName #{domain} -port #{port}
```

Atomic Test #2 - Testing usage of uncommonly used port

Testing uncommonly used port utilizing telnet.

Supported Platforms: Linux, macOS

auto_generated_guid: 5db21e1d-dd9c-4a50-b885-b1e748912767

Inputs:

Name	Description	Type	Default Value
port	Specify uncommon port number	String	8081
domain	Specify target hostname	String	google.com

Attack Commands: Run with `sh`!

```
telnet #{domain} #{port}
```