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 / T1560 / T1560.md

CircleCI Atomic Red Team doc... Generate docs from job=gener... 36d49de · 3 years ago History

Preview Code Blame 50 lines (26 loc) · 1.75 KB Raw

T1560 - Archive Collected Data

Description from ATT&CK

> An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender.
> Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.

Atomic Tests

- Atomic Test #1 - Compress Data for Exfiltration With PowerShell

Atomic Test #1 - Compress Data for Exfiltration With PowerShell

An adversary may compress data (e.g., sensitive documents) that is collected prior to exfiltration. When the test completes you should find the files from the $env:USERPROFILE directory compressed in a file called T1560-data-ps.zip in the $env:USERPROFILE directory

Supported Platforms: Windows

auto_generated_guid: 41410c60-614d-4b9d-b66e-b0192dd9c597

Inputs:

Name	Description	Type	Default Value
input_file	Path that should be compressed into our output file	Path	$env:USERPROFILE
output_file	Path where resulting compressed data should be placed	Path	$env:USERPROFILE\T1560-data-ps.zip

Attack Commands: Run with `powershell`!

```
dir #{input_file} -Recurse | Compress-Archive -DestinationPath #{output_
```

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

Cleanup Commands:

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