

> 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	] ♣ 등

Q

Y Fork 2.8k

Sign in

Sign up

Star 9.7k

## T1560 - Archive Collected Data

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

Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.

Atomic Test #1 - Compress Data for Exfiltration With PowerShell

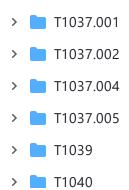
## Atomic Test #1 - Compress Data for Exfiltration With

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

auto\_generated\_guid: 41410c60-614d-4b9d-b66e-b0192dd9c597

Name	Description	Туре	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

 $\operatorname{ t dir}$  #{input\_file} -Recurse | Compress-Archive -DestinationPath #{output\_  $\Box$ 



Cleanup Commands:

Remove-Item -path #{output\_file} -ErrorAction Ignore