T1560.001 - Archive via Utility

An adversary may compress or encrypt data that is collected prior to exfiltration using 3rd party utilities. Many utilities exist that can archive data, including 7-Zip(Citation: 7zip Homepage), WinRAR(Citation: WinRAR Homepage), and WinZip(Citation: WinZip Homepage). Most utilities include functionality to encrypt and/or compress data.

**Make sure that 7zip/winrar installed in the machine.**

## Compress Data for Exfiltration With Rar/7zip

"#{rar\_exe/7zip.exe path}" a -r #{output\_file} #{input\_path}\\*#{file\_extension}

When the test completes you should find the specified extension files from the input path compressed in a output file.

## Compress Data and lock with password for Exfiltration with 7zip

mkdir $PathToAtomicsFolder\T1560.001\victim-files

cd $PathToAtomicsFolder\T1560.001\victim-files

echo "This file will be encrypted" > .\encrypted\_file.txt

"#{7zip\_exe path}" u archive.7z \*txt -pblue

dir

cmd/k