

stop-process -name "cmd" | out-null

remove-item "\$env:allusersprofile\cmd.exe" -force -erroraction silentlyc

Cleanup Commands:

T1003.008

T1003

T1006

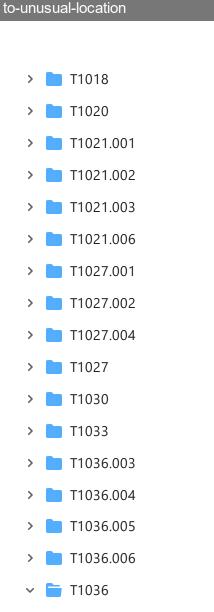
T1007

T1010

T1012

T1014

> T1016



bin

T1036.md

T1036.yaml

T1037.001

T1037.002

T1037.004

Atomic Test #2 - Malware Masquerading and Execution from Zip File

When the file is unzipped and the README.cmd file opened, it executes and changes the .pdf to .dll and executes the dll. This is a BazaLoader technique as reported here

Supported Platforms: Windows

auto_generated_guid: 4449c89b-ec82-43a4-89c1-91e2f1abeecc

Inputs:

Name	Description	Туре	Default Value
url	Location of zip file	Url	https://github.com/redcanaryco/atomic-red- team/raw/master/atomics/T1036/bin/T1036.zip

Attack Commands: Run with powershell!

Cleanup Commands:

```
taskkill /IM Calculator.exe /f >$null 2>$null
Remove-Item $env:userprofile\Downloads\T1036 -recurse -ErrorAction Ignor
```

Dependencies: Run with powershell!

Description: Zip file must be present.

Check Prereq Commands:

```
if (Test-Path $env:userprofile\Downloads\T1036.zip) {exit 0} else {exit □
```

Get Prereq Commands:

```
Invoke-WebRequest -OutFile "$env:userprofile\Downloads\T1036.zip" #{url}
```