T1036 - Masquerading

Description from ATT&CK

> Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names.
> Renaming abusable system utilities to evade security monitoring is also a form of Masquerading. (Citation: LOLBAS Main Site)

Atomic Tests

- Atomic Test #1 - System File Copied to Unusual Location
- Atomic Test #2 - Malware Masquerading and Execution from Zip File

Atomic Test #1 - System File Copied to Unusual Location

It may be suspicious seeing a file copy of an EXE in System32 or SysWOW64 to a non-system directory or executing from a non-system directory.

Supported Platforms: Windows

auto_generated_guid: 51005ac7-52e2-45e0-bdab-d17c6d4916cd

Attack Commands: Run with `powershell`!

```
copy-item "$env:windir\System32\cmd.exe" -destination "$env:allusersprofile\cmd.exe
start-process "$env:allusersprofile\cmd.exe"
sleep -s 5
stop-process -name "cmd" | out-null
```

Cleanup Commands:

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

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	Type	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`!

```
Expand-Archive -Path $env:userprofile\Downloads\T1036.zip -DestinationPath $env:us
cd $env:userprofile\Downloads\T1036
cmd /c $env:userprofile\Downloads\T1036\README.cmd >$null 2>$null
```

Cleanup Commands:

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

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 1}
```

Get Prereq Commands:

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