T1553.005 - Mark-of-the-Web Bypass

Description from ATT&CK

> Adversaries may abuse specific file formats to subvert Mark-of-the-Web (MOTW) controls. In Windows, when files are downloaded from the Internet, they are tagged with a hidden NTFS Alternate Data Stream (ADS) named `Zone.Identifier` with a specific value known as the MOTW.(Citation: Microsoft Zone.Identifier 2020) Files that are tagged with MOTW are protected and cannot perform certain actions. For example, starting in MS Office 10, if a MS Office file has the MOTW, it will open in Protected View. Executables tagged with the MOTW will be processed by Windows Defender SmartScreen that compares files with an allowlist of well-known executables. If the file in not known/trusted, SmartScreen will prevent the execution and warn the user not to run it.(Citation: Beek Use of VHD Dec 2020)(Citation: Outflank MotW 2020)(Citation: Intezer Russian APT Dec 2020)
> Adversaries may abuse container files such as compressed/archive (.arj, .gzip) and/or disk image (.iso, .vhd) file formats to deliver malicious payloads that may not be tagged with MOTW. Container files downloaded from the Internet will be marked with MOTW but the files within may not inherit the MOTW after the container files are extracted and/or mounted. MOTW is a NTFS feature and many container files do not support NTFS alternative data streams. After a container file is extracted and/or mounted, the files contained within them may be treated as local files on disk and run without protections.(Citation: Beek Use of VHD Dec 2020)(Citation: Outflank MotW 2020)

Atomic Tests

- Atomic Test #1 - Mount ISO image
- Atomic Test #2 - Mount an ISO image and run executable from the ISO
- Atomic Test #3 - Remove the Zone.Identifier alternate data stream

Atomic Test #1 - Mount ISO image

Mounts ISO image downloaded from internet to evade Mark-of-the-Web. Upon successful execution, powershell will download the .iso from the Atomic Red Team repo, and mount the image. The provided sample ISO simply has a Reports shortcut file in it. Reference: https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

Supported Platforms: Windows

auto_generated_guid: 002cca30-4778-4891-878a-aaffcfa502fa

Inputs:

Name	Description	Type	Default Value
path_of_iso	Path to ISO file	Path	PathToAtomicsFolder\T1553.005\bin\T1553.005.is

Attack Commands: Run with `powershell`!

```
Mount-DiskImage -ImagePath "#{path_of_iso}"
```

Cleanup Commands:

```
Dismount-DiskImage -ImagePath "#{path_of_iso}" | Out-Null
```

Dependencies: Run with `powershell`!

Description: T1553.005.iso must exist on disk at specified location (#{path_of_iso})

Check Prereq Commands:

Get Prereq Commands:

```
New-Item -Type Directory (split-path #{path_of_iso}) -ErrorAction ignore
Invoke-WebRequest https://raw.githubusercontent.com/redcanaryco/atomic-r
```

Atomic Test #2 - Mount an ISO image and run executable from the ISO

Mounts an ISO image downloaded from internet to evade Mark-of-the-Web and run hello.exe executable from the ISO. Upon successful execution, powershell will download the .iso from the Atomic Red Team repo, mount the image, and run the executable from the ISO image that will open command prompt echoing "Hello, World!". ISO provided by:https://twitter.com/mattifestation/status/1398323532988399620

Reference:https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/,

Supported Platforms: Windows

auto_generated_guid: 42f22b00-0242-4afc-a61b-0da05041f9cc

Inputs:

Name	Description	Type	Default Value
path_of_iso	Path to ISO file	Path	PathToAtomicsFolder\T1553.005\bin\FeelTheBurn

Attack Commands: Run with `powershell`!

```
$keep = Mount-DiskImage -ImagePath "#{path_of_iso}" -StorageType ISO -Ac
$driveLetter = ($keep | Get-Volume).DriveLetter
invoke-item "$($driveLetter):\hello.exe"
```

Cleanup Commands:

T1027.004
T1027
T1030
T1033
T1036.003
T1036.004
T1036.005
T1036.006
T1036
T1037.001
T1037.002
T1037.004
T1037.005
T1039
T1040

```
Dismount-DiskImage -ImagePath "#{path_of_iso}" | Out-Null
Stop-process -name "hello" -Force -ErrorAction ignore
```

Dependencies: Run with `powershell`!

Description: FeelTheBurn.iso must exist on disk at specified location (#{path_of_iso})

Check Prereq Commands:

```
if (Test-Path #{path_of_iso}) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
New-Item -Type Directory (split-path #{path_of_iso}) -ErrorAction ignore
Invoke-WebRequest https://raw.githubusercontent.com/redcanaryco/atomic-r
```

Atomic Test #3 - Remove the Zone.Identifier alternate data stream

Remove the Zone.Identifier alternate data stream which identifies the file as downloaded from the internet. Removing this allows more freedom in executing scripts in PowerShell and avoids opening files in protected view.

Supported Platforms: Windows

auto_generated_guid: 64b12afc-18b8-4d3f-9eab-7f6cae7c73f9

Inputs:

Name	Description	Type	Default Value
file_to_download	File that will be downloaded to test against.	Url	https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/README.md
file_path	File to have the Zone.Identifier removed.	String	$env:tmp\ReadMe.md

Attack Commands: Run with `powershell`!

```
Unblock-File -Path #{file_path}
```

Cleanup Commands:

```
Set-Content -Path #{file_path} -Stream Zone.Identifier -Value '[ZoneTran
```

Dependencies: Run with `powershell`!

Description: A test file with the Zone.Identifier attribute must be present.

Check Prereq Commands:

```
if (Test-Path #{file_path}) { EXIT 0 } else { EXIT 1 }
```

Get Prereq Commands:

```
Invoke-WebRequest #{file_to_download} -OutFile #{file_path}
Set-Content -Path #{file_path} -Stream Zone.Identifier -Value '[ZoneTran
```