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 / T1059.003 / T1059.003.md

CircleCI Atomic Red Team doc… Generate docs from job=genera… 7091fa8 · 2 years ago History

T1059.003 - Windows Command Shell

Description from ATT&CK

> Adversaries may abuse the Windows command shell for execution. The Windows command shell ([cmd](https://attack.mitre.org/software/S0106)) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. The command prompt can be invoked remotely via [Remote Services](https://attack.mitre.org/techniques/T1021) such as [SSH](https://attack.mitre.org/techniques/T1021/004).(Citation: SSH in Windows)
> Batch files (ex: .bat or .cmd) also provide the shell with a list of sequential commands to run, as well as normal scripting operations such as conditionals and loops. Common uses of batch files include long or repetitive tasks, or the need to run the same set of commands on multiple systems.
>
> Adversaries may leverage cmd to execute various commands and payloads. Common uses include cmd to execute a single command, or abusing cmd interactively with input and output forwarded over a command and control channel.

Atomic Tests

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

atomic-red-team / atomics / T1059.003 / T1059.003.md Top

Preview Code Blame 194 lines (105 loc) · 5.81 KB Raw

- Atomic Test #4 - Simulate BlackByte Ransomware Print Bombing

Atomic Test #1 - Create and Execute Batch Script

Creates and executes a simple batch script. Upon execution, CMD will briefly launch to run the batch script then close again.

Supported Platforms: Windows

auto_generated_guid: 9e8894c0-50bd-4525-a96c-d4ac78ece388

Inputs:

Name	Description	Type	Default Value
command_to_execute	Command to execute within	String	dir

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

	script.		
script_path	Script path.	Path	$env:TEMP\T1059.003_script.bat

Attack Commands: Run with `powershell`!

```
Start-Process #{script_path}
```

Cleanup Commands:

```
Remove-Item #{script_path} -Force -ErrorAction Ignore
```

Dependencies: Run with `powershell`!

Description: Batch file must exist on disk at specified location (#{script_path})

Check Prereq Commands:

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

Get Prereq Commands:

```
New-Item #{script_path} -Force | Out-Null
Set-Content -Path #{script_path} -Value "#{command_to_execute}"
```

Atomic Test #2 - Writes text to a file and displays it.

Writes text to a file and display the results. This test is intended to emulate the dropping of a malicious file to disk.

Supported Platforms: Windows

auto_generated_guid: 127b4afe-2346-4192-815c-69042bec570e

Inputs:

Name	Description	Type	Default Value
file_contents_path	Path to the file that the command prompt will drop.	Path	%TEMP%\test.bin
message	Message that will be written to disk and then displayed.	String	Hello from the Windows Command Prompt!

Attack Commands: Run with `command_prompt`!

```
echo "#{message}" > "#{file_contents_path}" & type "#{file_contents_path
```

Cleanup Commands:

```
del "#{file_contents_path}" >nul 2>&1
```

Atomic Test #3 - Suspicious Execution via Windows Command Shell

Command line executed via suspicious invocation. Example is from the 2021 Threat Detection Report by Red Canary.

Supported Platforms: Windows

auto_generated_guid: d0eb3597-a1b3-4d65-b33b-2cda8d397f20

Inputs:

Name	Description	Type	Default Value
output_file	File to output to	String	hello.txt
input_message	Message to write to file	String	Hello, from CMD!

Attack Commands: Run with `command_prompt`!

```
%LOCALAPPDATA:~-3,1%md /c echo #{input_message} > #{output_file} & type
```

Atomic Test #4 - Simulate BlackByte Ransomware Print Bombing

This test attempts to open a file a specified number of times in Wordpad, then prints the contents. It is designed to mimic BlackByte ransomware's print bombing technique, where tree.dll, which contains the ransom note, is opened in Wordpad 75 times and then printed. See https://redcanary.com/blog/blackbyte-ransomware/.

Supported Platforms: Windows

auto_generated_guid: 6b2903ac-8f36-450d-9ad5-b220e8a2dcb9

Inputs:

Name	Description	Type	Default Value
file_to_print	File to be opened/printed by Wordpad.	String	$env:temp\T1059_003note.txt
max_to_print	The maximum number of Wordpad windows the test will open/print.	String	75

Attack Commands: Run with `powershell`!

```
cmd /c "for /l %x in (1,1,#{max_to_print}) do start wordpad.exe /p #{fil
```

Cleanup Commands:

```
stop-process -name wordpad -force -erroraction silentlycontinue
```

Dependencies: Run with `powershell`!

Description: File to print must exist on disk at specified location (#{file_to_print})

Check Prereq Commands:

```
if (test-path "#{file_to_print}"){exit 0} else {exit 1}
```

Get Prereq Commands:

```
new-item #{file_to_print} -value "This file has been created by T1059.00
```