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 / T1216 / T1216.md

Atomic Red Team doc generat... Generated docs from job=generate-d... 819934c · 2 years ago History

Preview Code Blame 83 lines (40 loc) · 2.28 KB Raw

T1216 - System Script Proxy Execution

Description from ATT&CK

> Adversaries may use trusted scripts, often signed with certificates, to proxy the execution of malicious files. Several Microsoft signed scripts that have been downloaded from Microsoft or are default on Windows installations can be used to proxy execution of other files.(Citation: LOLBAS Project) This behavior may be abused by adversaries to execute malicious files that could bypass application control and signature validation on systems.(Citation: GitHub Ultimate AppLocker Bypass List)

Atomic Tests

- Atomic Test #1 - SyncAppvPublishingServer Signed Script PowerShell Command Execution
- Atomic Test #2 - manage-bde.wsf Signed Script Command Execution

Atomic Test #1 - SyncAppvPublishingServer Signed Script PowerShell Command Execution

Executes the signed SyncAppvPublishingServer script with options to execute an arbitrary PowerShell command. Upon execution, calc.exe will be launched.

Supported Platforms: Windows

auto_generated_guid: 275d963d-3f36-476c-8bef-a2a3960ee6eb

Inputs:

Name	Description	Type	Default Value
command_to_execute	A PowerShell command to execute.	String	Start-Process calc

Attack Commands: Run with `command_prompt`!

```
C:\windows\system32\SyncAppvPublishingServer.vbs "\n;#{command_to_execut
```

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

Atomic Test #2 - manage-bde.wsf Signed Script Command Execution

Executes the signed manage-bde.wsf script with options to execute an arbitrary command.

Supported Platforms: Windows

auto_generated_guid: 2a8f2d3c-3dec-4262-99dd-150cb2a4d63a

Inputs:

Name	Description	Type	Default Value
command_to_execute	A command to execute.	Path	%windir%\System32\calc.exe

Attack Commands: Run with `command_prompt`!

```
set comspec=#{command_to_execute}
cscript %windir%\System32\manage-bde.wsf
```

Cleanup Commands:

```
set comspec=%windir%\System32\cmd.exe
```