

Product

▼

Solutions

▼

Resources

▼

Open Source

▼

Enterprise

▼

Pricing

Search

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 / T1056.004 / T1056.004.md

CircleCI Atomic Red Team doc... Generate docs from job=genera... ecdd11f · 3 years ago History

PreviewCodeBlame62 lines (36 loc) · 2.77 KBRawCopyDownloadMenu

T1056.004 - Credential API Hooking

Description from ATT&CK

Adversaries may hook into Windows application programming interface (API) functions to collect user credentials. Malicious hooking mechanisms may capture API calls that include parameters that reveal user authentication credentials.(Citation: Microsoft TrojanSpy:Win32/Ursnif.gen!! Sept 2017) Unlike [Keylogging] (<https://attack.mitre.org/techniques/T1056/001>), this technique focuses specifically on API functions that include parameters that reveal user credentials. Hooking involves redirecting calls to these functions and can be implemented via:

- Hooks procedures**, which intercept and execute designated code in response to events such as messages, keystrokes, and mouse inputs.(Citation: Microsoft Hook Overview)(Citation: Elastic Process Injection July 2017)
- Import address table (IAT) hooking**, which use modifications to a process’s IAT, where pointers to imported API functions are stored.(Citation: Elastic Process Injection July 2017)(Citation: Adlice Software IAT Hooks Oct 2014)(Citation: MWRInfoSecurity Dynamic Hooking 2015)
- Inline hooking**, which overwrites the first bytes in an API function to redirect code flow.(Citation: Elastic Process Injection July 2017)(Citation: HighTech Bridge Inline Hooking Sept 2011)(Citation: MWRInfoSecurity Dynamic Hooking 2015)

Atomic Tests

- [Atomic Test #1 - Hook PowerShell TLS Encrypt/Decrypt Messages](#)

Atomic Test #1 - Hook PowerShell TLS Encrypt/Decrypt Messages

Hooks functions in PowerShell to read TLS Communications

Supported Platforms: Windows

auto_generated_guid: de1934ea-1fbf-425b-8795-65fb27dd7e33

Inputs:

Name	Description	Type	Default Value
file_name	Dll To Inject	Path	PathToAtomicsFolder\T1056.004\bin\T1056.004:
server_name	TLS Server To Test Get	Url	https://www.example.com

Page 1 of 2

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

	Request		
--	---------	--	--

Attack Commands: Run with powershell ! Elevation Required (e.g. root or admin)

```
mavinject $pid /INJECTRUNNING #{file_name}
Invoke-WebRequest #{server_name} -UseBasicParsing
```

Dependencies: Run with powershell !

Description: T1056.004x64.dll must exist on disk at specified location (#{file_name})

Check Prereq Commands:

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

Get Prereq Commands:

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