

Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing

Q

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 / T1137 / T1137.md

CircleCI Atomic Red Team doc... Generate docs from job=genera...

8985aaf · 3 years ago

History

Preview

Code

Blame

50 lines (27 loc) · 2.02 KB

Raw

T1137 - Office Application Startup

Description from ATT&CK

Adversaries may leverage Microsoft Office-based applications for persistence between startups. Microsoft Office is a fairly common application suite on Windows-based operating systems within an enterprise network. There are multiple mechanisms that can be used with Office for persistence when an Office-based application is started; this can include the use of Office Template Macros and add-ins.

A variety of features have been discovered in Outlook that can be abused to obtain persistence, such as Outlook rules, forms, and Home Page.(Citation: SensePost Ruler GitHub) These persistence mechanisms can work within Outlook or be used through Office 365.(Citation: TechNet O365 Outlook Rules)

Atomic Tests

- [Atomic Test #1 - Office Application Startup - Outlook as a C2](#)

Atomic Test #1 - Office Application Startup - Outlook as a C2

As outlined in MDSEC's Blog post <https://www.mdsec.co.uk/2020/11/a-fresh-outlook-on-mail-based-persistence/> it is possible to use Outlook Macro as a way to achieve persistence and execute arbitrary commands. This transform Outlook into a C2. Too achieve this two things must happened on the syste

- The macro security registry value must be set to '4'
- A file called VbaProject.OTM must be created in the Outlook Folder.

Supported Platforms: Windows







auto_generated_guid: bfe6ac15-c50b-4c4f-a186-0fc6b8ba936c

Attack Commands: Run with **command_prompt !**

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Securi
mkdir %APPDATA%\Microsoft\Outlook\ >nul 2>&1
echo "Atomic Red Team TEST" > %APPDATA%\Microsoft\Outlook\VbaProject.OTM
```

Cleanup Commands:

Page 1 of 2

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

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Sec
del %APPDATA%\Microsoft\Outlook\VbaProject.OTM >nul 2>&1
```