

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 / T1037.001 / T1037.001.md

History

PreviewCodeBlame53 lines (29 loc) · 1.86 KB

Raw📄⬇️☰

T1037.001 - Logon Script (Windows)

Description from ATT&CK

Adversaries may use Windows logon scripts automatically executed at logon initialization to establish persistence. Windows allows logon scripts to be run whenever a specific user or group of users log into a system.(Citation: TechNet Logon Scripts) This is done via adding a path to a script to the `HKCU\Environment\UserInitMprLogonScript` Registry key.(Citation: Hexacorn Logon Scripts) Adversaries may use these scripts to maintain persistence on a single system. Depending on the access configuration of the logon scripts, either local credentials or an administrator account may be necessary.

Atomic Tests

- [Atomic Test #1 - Logon Scripts](#)

Atomic Test #1 - Logon Scripts

Adds a registry value to run batch script created in the %temp% directory. Upon execution, there will be a new environment variable in the HKCU\Environment key that can be viewed in the Registry Editor.

Supported Platforms: Windows

auto_generated_guid: d6042746-07d4-4c92-9ad8-e644c114a231







Inputs:

Name	Description	Type	Default Value
script_path	Path to .bat file	String	%temp%\art.bat
script_command	Command To Execute	String	echo Art "Logon Script" atomic test was successful. > > %USERPROFILE%\desktop\T1037.001-log.txt

Attack Commands: Run with `command_prompt` !

```
echo "#{script_command}" > #{script_path}
```

Page 1 of 2

- ▼  T1037.001
-  T1037.001.md
-  T1037.001.yaml
- >  T1037.002
- >  T1037.004
- >  T1037.005

```
REG.exe ADD HKCU\Environment /v UserInitMprLogonScript /t REG_SZ /d "#{s
```

Cleanup Commands:

```
REG.exe DELETE HKCU\Environment /v UserInitMprLogonScript /f >nul 2>&1
del #{script_path} >nul 2>&1
del "%USERPROFILE%\desktop\T1037.001-log.txt" >nul 2>&1
```

