# TTP Detail – T1546.002

## TTP Information

Name: Screensaver

Description: 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 <code>C:\Windows\System32\</code>, and <code>C:\Windows\sysWOW64\</code> on 64-bit Windows systems, along with screensavers included with base Windows installations.

The following screensaver settings are stored in the Registry (<code>HKCU\Control Panel\Desktop\</code>) and could be manipulated to achieve persistence:

\* <code>SCRNSAVE.exe</code> - set to malicious PE path
\* <code>ScreenSaveActive</code> - set to '1' to enable the screensaver
\* <code>ScreenSaverIsSecure</code> - set to '0' to not require a password to unlock
\* <code>ScreenSaveTimeout</code> - 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)

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: privilege-escalation

**•** mitre-attack: persistence

## Malware

* Gazer