# Event Triggered Execution: Screensaver, Sub-technique T1546.002 - Enterprise

Archived: 2026-04-02 11:52:43 UTC

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.[1] 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\` ) 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.[2]

---

Source: https://attack.mitre.org/techniques/T1546/002