# TTP Detail – T1546.008

## TTP Information

Name: Accessibility Features

Description: Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by accessibility features. Windows contains accessibility features that may be launched with a key combination before a user has logged in (ex: when the user is on the Windows logon screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.

Two common accessibility programs are <code>C:\Windows\System32\sethc.exe</code>, launched when the shift key is pressed five times and <code>C:\Windows\System32\utilman.exe</code>, launched when the Windows + U key combination is pressed. The sethc.exe program is often referred to as "sticky keys", and has been used by adversaries for unauthenticated access through a remote desktop login screen. (Citation: FireEye Hikit Rootkit)

Depending on the version of Windows, an adversary may take advantage of these features in different ways. Common methods used by adversaries include replacing accessibility feature binaries or pointers/references to these binaries in the Registry. In newer versions of Windows, the replaced binary needs to be digitally signed for x64 systems, the binary must reside in <code>%systemdir%\</code>, and it must be protected by Windows File or Resource Protection (WFP/WRP). (Citation: DEFCON2016 Sticky Keys) The [Image File Execution Options Injection](https://attack.mitre.org/techniques/T1546/012) debugger method was likely discovered as a potential workaround because it does not require the corresponding accessibility feature binary to be replaced.

For simple binary replacement on Windows XP and later as well as and Windows Server 2003/R2 and later, for example, the program (e.g., <code>C:\Windows\System32\utilman.exe</code>) may be replaced with "cmd.exe" (or another program that provides backdoor access). Subsequently, pressing the appropriate key combination at the login screen while sitting at the keyboard or when connected over [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1021/001) will cause the replaced file to be executed with SYSTEM privileges. (Citation: Tilbury 2014)

Other accessibility features exist that may also be leveraged in a similar fashion: (Citation: DEFCON2016 Sticky Keys)(Citation: Narrator Accessibility Abuse)

\* On-Screen Keyboard: <code>C:\Windows\System32\osk.exe</code>
\* Magnifier: <code>C:\Windows\System32\Magnify.exe</code>
\* Narrator: <code>C:\Windows\System32\Narrator.exe</code>
\* Display Switcher: <code>C:\Windows\System32\DisplaySwitch.exe</code>
\* App Switcher: <code>C:\Windows\System32\AtBroker.exe</code>

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

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

**•** mitre-attack: persistence

## Tools

* Empire

## APTs (Intrusion Sets)

* APT29
* APT3
* APT41
* Axiom
* Deep Panda
* Fox Kitten