What is an accessibility backdoor?

An accessibility backdoor abuses Windows accessibility features that are reachable from the locked logon screen, such as Sticky Keys (`sethc.exe`) and the Utility Manager (`utilman.exe`), by replacing them (or hijacking their launch) so they open a SYSTEM command prompt instead. An attacker who triggers the feature at the login screen, for example pressing Shift five times, gets a SYSTEM shell without authenticating. It needs admin to set up and maps to MITRE T1546.008.

HOW IT WORKS

01 The technique and payload

With admin (typically post-exploitation), the attacker repoints the accessibility binary:

- Replace the binary: overwrite `C:\Windows\System32\sethc.exe` with `cmd.exe-`, then press Shift five times at the logon screen for a SYSTEM prompt.
- Or use Image File Execution Options to set a debugger: `reg add "HKLM\...\Image File Execution Options\sethc.exe" /v Debugger /d "cmd.exe"`, no file replacement needed.
- The same works with `utilman.exe`, `osk.exe`, and others.

Works even over RDP at the lock screen. Documented for defensive context.

> SYSTEM BEFORE LOGIN
>
> *The trick's power is getting a SYSTEM shell from the locked logon screen, no credentials required. It is also a re-entry backdoor: trigger the key combo anytime to get back in.*

HOW TO DEFEND

- Monitor the accessibility binaries (`sethc.exe`, `utilman.exe`, `osk.exe`) for replacement, and the Image File Execution Options keys for a `Debugger` value.
- Enable file integrity monitoring on System32 for these files.
- Restrict RDP and use Network Level Authentication so the lock screen is not exposed.
- Limit local admin, required to set the backdoor.
- Alert on cmd.exe or shells spawned by these binaries.

SOURCES

[1] MITRE ATT&CK: Event Triggered Execution (T1546)

[2] Microsoft: Windows logon and security

[3] MITRE ATT&CK: Persistence (TA0003)

Find the backdoors an attacker would leave behind.

`securelayer7.net/learn/persistence/what-is-an-accessibility-backdoor`

Open online