What is a backdoor?

A backdoor is a hidden method of accessing a system that bypasses normal authentication, planted by an attacker (or shipped in malicious software) so they can return at will. Backdoors range from a web shell on a server, an extra SSH key, or a rogue account, to deep rootkits and firmware implants. They are the mechanism behind most persistence: a quiet, reliable door back in that survives reboots and avoids the front-door login.

HOW IT WORKS

01 The forms backdoors take

Backdoors exist at every layer:

- Application: a web shell dropped into a website's files.
- Account: a rogue account or an extra SSH key.
- Service/scheduler: a malicious service-, scheduled task, or cron job.
- Kernel/system: a rootkit that hides itself.
- Domain: a forged Golden Ticket that grants access without a password.

02 Why backdoors are dangerous

A backdoor combines stealth and durability. It avoids the authentication and logging the front door has, and it is designed to persist. Attackers also plant several, so removing the obvious one still leaves a way in.

That is why eradicating an intrusion means hunting every backdoor and autostart location, not just closing the hole the attacker first used.

> BYPASSES THE FRONT DOOR
>
> *The defining trait of a backdoor is bypassing normal authentication. It does not need the password or MFA, which is exactly why it is both effective for attackers and dangerous to miss.*

SOURCES

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

[2] MITRE ATT&CK: Server Software Component (T1505)

[3] NIST SP 800-83 Malware Incident Prevention and Handling

Find the backdoors an attacker would leave behind.

securelayer7.net/learn/persistence/what-is-a-backdoor

Open online