Backdoor (Zadní vrátka)

Backdoor je v informatice skrytý vstupní bod do softwaru, hardwaru nebo počítačové sítě, který umožňuje získat přístup k systému bez nutnosti projít standardním ověřením identity (autentizací).

Zatímco legitimní zadní vrátka jsou někdy instalována výrobci pro účely servisu nebo obnovy hesel, útočníci je využívají k udržení trvalého a nenápadného přístupu do napadeného systému.

Klasifikace Backdoorů

V encyklopedii je důležité rozlišovat mezi různými typy zadních vrátek podle jejich původu a účelu:

1. Administrativní (Logistická) vrátka

Původně zamýšlená vývojáři jako „zadní cesta“ pro ladění kódu (debugging) nebo technickou podporu. Často se stávají bezpečnostním rizikem, pokud zůstanou v ostré verzi produktu zapomenuta.

- **Příklad:** Skrytý administrátorský účet s pevně daným heslem (hardcoded password) v routeru.

2. Malwarová vrátka

Instalovaná útočníkem po prvotním průniku do systému (např. pomocí phishingu nebo exploitu). Slouží k tomu, aby se útočník mohl do systému kdykoli vrátit, i když je původní zranitelnost opravena.

- **Příklad:** Rootkit, který modifikuje jádro operačního systému.

3. Kryptografická vrátka

Záměrné oslabení šifrovacího algoritmu nebo protokolu, které umožňuje třetí straně (např. vládní agentuře) dešifrovat komunikaci bez znalosti klíče.

4. Hardwarová vrátka

Modifikace na úrovni čipů nebo firmware přímo ve výrobě. Jsou extrémně těžko odhalitelná, protože se nacházejí pod úrovní operačního systému.

Jak Backdoor funguje?

Mechanismus fungování se liší podle úrovně, na které operuje:

- **Síťová úroveň:** Backdoor otevře na pozadí specifický port (TCP/UDP), na kterém naslouchá a čeká na instrukce od útočníka.
- **Aplikační úroveň:** Modifikace zdrojového kódu aplikace tak, aby po zadání speciálního řetězce (např. v poli pro jméno) uživatele okamžitě přihlásila jako administrátora.
- **Webové shelly:** Skript nahraný na webový server, který umožňuje útočníkovi spouštět systémové příkazy přes webový prohlížeč.

Rizika a dopady

Riziko	Popis
Ztráta kontroly	Majitel systému netuší, že v jeho zařízení operuje jiná osoba.
Exfiltrace dat	Možnost kdykoli a postupně stahovat citlivá data bez spuštění alarmů.
Botnet	Napadené zařízení může být zneužito k provádění DDoS útoků na jiné cíle.
Šíření nákazy	Backdoor může sloužit jako odrazový můstek pro útok na další zařízení v lokální síti.

Detekce a ochrana

Odhalení zadních vrátek je náročné, protože jsou navržena tak, aby byla neviditelná pro běžné monitorovací nástroje.

- **FIM (File Integrity Monitoring):** Sledování změn v systémových souborech. Pokud se změní binární soubor jádra, systém vyhlásí poplach.
- **Síťová analýza:** Sledování neobvyklého odchozího provozu na neznámé porty nebo IP adresy.
- **Code Auditing:** Důkladná kontrola zdrojového kódu (manuální i automatická) před nasazením softwaru.
- **Honeypoty:** Nastražení falešných systémů, které mají přilákat útočníka a odhalit jeho metody, včetně instalace zadních vrátek.

Známé historické případy

- **Dual_EC_DRBG (2013):** Algoritmus pro generování náhodných čísel, o kterém se zjistilo, že obsahuje matematická zadní vrátka vytvořená agenturou NSA.
- **Juniper Networks (2015):** V operačním systému ScreenOS byla nalezena neautorizovaná zadní vrátka, která umožňovala komukoli s „master heslem“ dešifrovat VPN provoz.
- **SolarWinds (2020):** Masivní útok na dodavatelský řetězec, kdy útočníci vložili backdoor

(Sunburst) přímo do aktualizace legitimního softwaru.

Související pojmy: Rootkit, Trojan, Exploit, Authentication, Encryption, Zero Trust.