Rootkit

Rootkit je kolekce škodlivého softwaru (malwaru) navržená tak, aby útočníkovi poskytla trvalý a privilegovaný přístup k počítači, zatímco svou přítomnost aktivně skrývá před uživatelem i bezpečnostními mechanismy operačního systému.

Zatímco běžný virus se snaží množit a backdoor otevřít přístup, rootkit se zaměřuje na **neviditelnost**. Dokáže zmanipulovat hlášení operačního systému tak, aby nebyly vidět jeho procesy, soubory ani síťová spojení.

Úrovně působení (Typy Rootkitů)

Rootkity se dělí podle toho, v jaké vrstvě systému operují. Čím hlouběji jsou uloženy, tím obtížnější je jejich detekce.

1. Uživatelská úroveň (User Mode)

Nahrazují nebo modifikují standardní systémové soubory (např. .dll ve Windows nebo knihovny v Linuxu).

- **Jak funguje:** Pokud uživatel spustí příkaz pro výpis souborů, rootkit tento výpis „přefiltruje“ a smaže z něj své vlastní záznamy.

2. Úroveň jádra (Kernel Mode)

Cílí přímo na jádro operačního systému (kernel). Jsou extrémně nebezpečné, protože mají stejná práva jako samotný systém.

- **Jak funguje:** Mění vnitřní datové struktury jádra nebo zachytává systémová volání. Může tak zcela převzít kontrolu nad hardwarem.

3. Hypervisor (Virtualizační)

Vytvoří si vlastní neviditelnou vrstvu (hypervisor) a původní operační systém do ní „uzavře“ jako virtuální stroj. Operační systém pak nemá žádnou šanci zjistit, že pod ním běží ještě něco jiného.

4. Firmware / Bootkit

Infikují nízkoúrovňový kód jako BIOS, UEFI nebo MBR (Master Boot Record).

- **Dopad:** Přežijí i úplné zformátování pevného disku a přeinstalaci operačního systému, protože jsou uloženy v čipu na základní desce nebo v zaváděcí sekci disku.

Techniky maskování

Rootkit využívá k utajení několik pokročilých metod:

- **Hooking (Háčkování):** Zachytávání zpráv nebo funkcí putujících mezi aplikací a operačním systémem.
- **Direct Kernel Object Manipulation (DKOM):** Přímá úprava seznamů běžících procesů v paměti RAM. Rootkit se ze seznamu prostě „vymaže“, ale dál běží.
- **Filtrace systémových volání:** Pokud se antivir zeptá „Jaké soubory jsou v této složce?“, rootkit odpověď zachytí a pošle antiviru upravený seznam bez škodlivých souborů.

Detekce a odstranění

Protože rootkit lže operačnímu systému, nelze se spolehnout na běžné nástroje (Správce úloh, Antivir spuštěný v napadeném systému).

Metody detekce:

- **Skenování z vnějšku (Offline scanning):** Nabootování z čistého USB disku (např. Linux Live CD). Rootkit na pevném disku není spuštěn, a tudíž se nemůže bránit ani skrývat.
- **Behaviorální analýza:** Sledování neobvyklého chování hardwaru (např. CPU běží na 100 %, ale Správce úloh ukazuje 0 %).
- **Kontrola integrity (Signature checking):** Porovnávání digitálních podpisů systémových souborů s originály od výrobce (např. Microsoftu).

Odstranění:

U nízkoúrovňových rootkitů (Kernel, Firmware) je odstranění velmi riskantní a často selhává. Nejbezpečnějším řešením je obvykle:

```
1. Úplné zformátování všech disků.
2. Flashování BIOSu/UEFI (pokud je podezření na infekci firmwaru).
3. Čistá instalace operačního systému.
```

Známé případy

- **Sony BMG Rootkit (2005):** Sony instalovala na hudební CD ochranu proti kopírování, která se do počítače nainstalovala jako rootkit. Způsobilo to obrovský skandál, protože to otevřelo bezpečnostní díry do milionů počítačů.
- **Stuxnet (2010):** Komplexní kybernetická zbraň cílící na íránské jaderné zařízení, která využívala kernel-mode rootkit k maskování sabotáže průmyslových kontrolérů.
- **LoJax (2018):** První detekovaný UEFI rootkit použitý při skutečném útoku, který přežil i výměnu pevného disku.

Související pojmy: Malware, Backdoor, Bootkit, Kernel, UEFI, Virtualizace, Antivirus.

From:
https://serviceit.cz/ - **IT ENCYKLOPEDIE**

Permanent link:
https://serviceit.cz/doku.php?id=rootkit

Last update: **2025/12/31 19:10**