Bootkit

Bootkit je typ škodlivého softwaru, který napadá zaváděcí mechanismy počítače (bootloader). Cílem bootkitu je usadit se v systému dříve, než se načte jádro operačního systému (kernel) a antivirový software.

Díky tomu, že bootkit ovládá startovací proces, může modifikovat jádro systému „za letu“ (patching) a zajistit si tak absolutní moc nad zařízením, přičemž zůstává pro běžné kontrolní nástroje zcela neviditelný.

Historie a evoluce

Vývoj bootkitů kopíruje vývoj hardwaru a způsobů, jakými počítače startují:

1. Éra MBR (Legacy BIOS)

Starší bootkity cílily na **Master Boot Record (MBR)** – první sektor pevného disku.

- Útočník přepsal původní zavaděč svým kódem.
- Po zapnutí PC se spustil nejdříve bootkit, ten načetl své ovladače do paměti a následně spustil originální operační systém.
- **Příklad:** Rootkit.Win32.TDSS (známý jako TDL-4).

2. Éra VBR (Volume Boot Record)

Bootkity cílící na zaváděcí sektor konkrétního diskového oddílu. Tato metoda se používala k obcházení některých kontrol integrity MBR.

3. Moderní éra: UEFI Bootkity

S nástupem moderního rozhraní UEFI se bootkity přesunuly přímo do firmwaru základní desky nebo do skrytých oddílů (ESP - EFI System Partition). Tyto verze jsou nejnebezpečnější, protože přežijí i výměnu pevného disku.

Jak Bootkit funguje?

Proces infekce a aktivace probíhá v několika krocích:

```
1. **Průnik:** Bootkit se do systému dostane nejčastěji skrze jiný malware (dropper) s administrátorskými právy, který přepíše zaváděcí sektory.
2. **Start:** Při zapnutí počítače předá BIOS/UEFI řízení kódu bootkitu.
3. **Příprava prostředí:** Bootkit zůstane rezidentní v paměti RAM a čeká na načítání souborů operačního systému.
4. **Patching:** Jakmile začne systém načítat jádro (ntoskrnl.exe ve Windows), bootkit jej v paměti upraví (vypne kontrolu digitálních podpisů ovladačů nebo vloží vlastní škodlivý kód).
5. **Neviditelnost:** Po startu systému bootkit filtruje veškeré požadavky na čtení infikovaných sektorů disku. Pokud se antivir pokusí přečíst MBR, bootkit mu "podstrčí" kopii čistého, neinfikovaného MBR.
```

Obrana a technologie Secure Boot

Hlavní zbraní proti bootkitům je technologie **Secure Boot**, která je součástí standardu UEFI.

- **Princip:** Každá součást zaváděcího procesu (bootloader, ovladače, jádro) musí být digitálně podepsána důvěryhodným výrobcem (např. Microsoftem). Pokud podpis chybí nebo je neplatný, počítač odmítne systém spustit.
- **Slabina:** Pokud útočník najde zranitelnost přímo ve firmwaru UEFI (jako u kauzy „BlackLotus“), může Secure Boot obejít.

Detekce a odstranění

Detekce běžícím antivirem je téměř nemožná, protože bootkit ovládá to, co antivir „vidí“.

Metody detekce:

- **VDI (Virtual Desktop Infrastructure):** Srovnání obrazu disku s jeho čistou šablonou na úrovni úložiště.
- **Analýza z vnějšku:** Připojení disku k jinému, čistému počítači a kontrola integrity zaváděcích sektorů.
- **TPM (Trusted Platform Module):** Hardwarový čip, který kontroluje, zda se nezměnil kontrolní součet (hash) bootloaderu.

Odstranění:

- U MBR bootkitů často stačí příkaz `fixmbr` z konzole pro zotavení.

- U UEFI bootkitů je situace kritická – často je nutné přehrát firmware základní desky (flash BIOSu) a kompletně odstranit a znovu vytvořit oddíly na disku.

Známé případy

- **BlackLotus (2023):** První reálně zachycený bootkit, který dokáže obejít Secure Boot na plně aktualizovaných systémech Windows 11.
- **FinSpy (FinFisher):** Špionážní software prodávaný vládám, který obsahoval modul UEFI bootkitu pro trvalé sledování cílů.
- **LoJax (2018):** První detekovaný bootkit v UEFI, připisovaný skupině APT28 (Sednit).

Související pojmy: UEFI, BIOS, MBR, Rootkit, Secure Boot, TPM, Kernel.

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

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

Last update: **2025/12/31 19:11**