

Relazione Progetto NSD

Cristiano Cuffaro

matricola: 0299838

cristiano.cuffaro@outlook.com

12 maggio 2022

Indice

1	Descrizione preliminare del problema e dell'attacco	2
1.1	Boot del sistema	2
1.2	Utilizzo di initrd	2
1.3	Horse Pill	3
2	Implementazione	3

1 Descrizione preliminare del problema e dell'attacco

La maggior parte dei sistemi operativi convenzionali *Unix-like*, come Linux, durante la fase di boot fa uso di un *initial ram disk*, chiamato *initrd*. Il problema è che ad oggi quest'ultimo non è sicuro e può essere compromesso per ottenere il controllo del sistema.

1.1 Boot del sistema

Tipicamente, quando si fa uso di *initrd*, l'avvio del sistema avviene nel seguente modo:

1. il bootloader carica il kernel e *initrd*;
2. il kernel converte *initrd* in un RAM disk "normale" e libera la memoria usata da *initrd*;
3. *initrd* viene montato come root;
4. viene eseguito `/linuxrc` (chiamato anche `/init`), che può essere qualsiasi eseguibile valido (inclusi gli shell script) e viene eseguito con UID 0;
5. `linuxrc` monta il file system root "reale";
6. `linuxrc` assegna il file system root alla directory root utilizzando la system call `pivot_root`;
7. `linuxrc` esegue la `exec` di `/sbin/init` sul nuovo file system root, consentendo la sequenza di avvio ordinaria;
8. viene rimosso il file system *initrd*.

1.2 Utilizzo di *initrd*

È possibile avviare un sistema Linux senza utilizzare un *initrd*, ma questo normalmente richiede la compilazione di un kernel specifico per l'installazione.

Infatti, se non si usa un *initrd* non si possono caricare moduli del kernel prima di aver montato la partizione radice, e quindi quest'ultima deve poter essere montata utilizzando solo moduli che sono compilati nel kernel. Quindi un kernel generico dovrebbe contenere il supporto necessario a montare qualsiasi tipo di partizione radice, e finirebbe così per contenere molti moduli non necessari.

L'utilizzo di un *initrd* permette invece alle distribuzioni Linux di fornire un kernel precompilato con tutte le funzionalità realizzate come moduli, e di costruire per ciascuna installazione un *initrd* contenente i moduli necessari per montare il filesystem radice su quella particolare installazione.

1.3 Horse Pill

L'idea dell'attacco è che il rootkit Horse Pill sostituisce il file `run-init`¹ in `initrd` e quindi ottiene il controllo sul sistema al momento dell'avvio. Poiché `initrd` è generato dinamicamente e non ci sono controlli di integrità su di esso, è improbabile che un tale cambiamento venga notato attraverso un'osservazione casuale.

Quando il rootkit viene eseguito, a valle dell'infezione, inserisce l'intero sistema in un container creato sfruttando il meccanismo dei *namespace* presente in Linux. Avvia anche un processo backdoor, al di fuori di quel container. Tutto il resto, incluso il processo `systemd` e tutti i servizi e le applicazioni di sistema regolarmente previsti, sono in esecuzione all'interno del sistema containerizzato. Il processo `run-init` compromesso crea anche dei processi e li rinomina in modo che sembrino gli autentici thread del kernel. Gli utenti e gli amministratori che sono "vittime" del rootkit non possono vedere i processi e la backdoor in esecuzione al di fuori del sistema containerizzato. Il sistema appare praticamente normale dall'interno.

La backdoor installata dal rootkit Horse Pill crea una sorta di connessione effimera sfruttando un tunnel DNS, che consente di connettersi al server attaccante per ricevere comandi e scambiare dati.

2 Implementazione

Ciò che viene fatto dall'initial ramdisk infetto sono i seguenti task:

- caricamento dei moduli necessari per l'architettura specifica
- rispondere agli eventi di hotplug
- cryptsetup (opzionale)
- ricerca e montaggio del file system rootfs
- enumerazione dei thread del kernel
- `clone(CLONE_NEWPID, CLONE_NEWNS)`
 - remount di `/proc`
 - creazione dei kernel thread fittizi
 - **clean up e smontaggio di `initrd`**
 - **esecuzione di `init`**
- remount di root
- montaggio di uno spazio di lavoro *scratch*
- `fork()`

¹All'avvio, una volta montato il disco `initrd` il kernel esegue `/linuxrc` che, tra le altre cose, lancia il binario `/usr/bin/run-init` per avviare il processo user-mode iniziale del sistema.

- aggancio agli aggiornamenti di initrd
- esecuzione della shell backdoor
- `waitpid()`
- catch dello shutdown o del reboot

dove in grassetto sono evidenziate le attività eseguite anche da un ramdisk regolare.