ROOTKIT

LISA VIVIANI 5DSA

A.S. 2016/2017

INTRODUZIONE

- Un rootkit è una collezione di programmi che permettono di ottenere accesso ad un computer
- Il termine «rootkit» è composto dal termine *root* (amministratore del sistema) e *kit* (insieme di software che implementa lo strumento)

COME FUNZIONA?

- Il rootkit prende possesso della macchina su cui viene installato sfruttando delle vulnerabilità del sistema o scoprendo password che gli permettono di acquisire diritti di amministratore (*Privilege Escalation*)
- Una volta ottenuto il controllo del computer, il rootkit può inibire diversi programmi, tra cui antivirus o altri software atti a rilevare malware

INSTALLAZIONE

La prima fase riguarda l'installazione, che può avvenire in diversi modi:

- *accesso fisico*
- *accesso tramite rete*
- *accesso tramite altro software*

RILEVAMENTO

- Scansione anti-malware (rimovibile)
- Analisi del comportamento (rilevabile ma non rimovibile)
- Controllo di integrità (rilevabile ma non rimovibile)

USI E ABUSI

- I rootkit possono essere installati volontariamente dall'utente allo scopo di bypassare controlli di sicurezza, ad esempio sistemi di protezione dalla copia presenti nei cd.
- Al contrario, gli hacker abusano di questi strumenti allo scopo di prendere il controllo di macchine o rubare dati importanti

CURIOSITÀ

Nel 2011, con l'aggiornamento firmware 3.56, la Sony ha introdotto nel sistema operativo della console PS3 un rootkit che le consentiva di riconoscere le console modificate e non permettere loro l'accesso online

Informazioni tratte da

https://it.wikipedia.org/wiki/Rootkit

https://en.wikipedia.org/wiki/Rootkit