**Lez7 25/11/2024**

**Antivirus**

virus the creeper nel 1971

antivirus the reaper nel 1972

**Come funziona un antivirus?**

tecniche

**Sandbox detection:** rilevo file sospetto, crea ambiente virtuale e analizza comportamento. se non sospetto viene eseguito (altrimenti segnalato, cancellato o in quarantena). Efficace ma richiede tempo e non performante

**Data-mining:** sfrutto algoritmi machine learning, ci si basa su ciò che si conosce ma continua ricerca

**Firme:** hash di un virus, salvato in DB, farà da riferimento per possibili match o riconosce la firma (etico pubblicare la firma). complicazioni se algoritmo cifrato e manomesso

**Rootkit detection:** continua scansione sistema dei malware che cercano di ottenere poteri di amministrazione(rischio disabilitare antivirus)

**Protezione real time:** attività background

tendenziale efficacia tra 91-99%

**Problemi**

**rogueware:** malware spacciato per antivirus, non sempre rilevabile che fa casini nel sistema

**falsi positivi:** segnare file come pericolosi anche se sono normali(rischio quarantena dei file di sistema)

**nuovi virus ofc**

**Soluzioni**

**firewall:** perimetro, difesatra macchina a mondo virtuale (inizialmente passivo, non sempre attivo come antivirus) (sia entrata sia uscita)

*default-allow*

*default-deny*

come funziona firewall?

ha 3 azioni: Allow, Drop(user non sa del rifiuto), Deny (sa avviso del rifiuto, ma ripetitivo se sempre usato)

tipi

*hardware, software*

*stateless, stateful*

di solito le minacce non sono sempre esterne(es computer infetto lavora dentro azienda)

**Cloud antivirus** Alleggerisce macchina

**Online antivirus**

**Tools Specializzati**