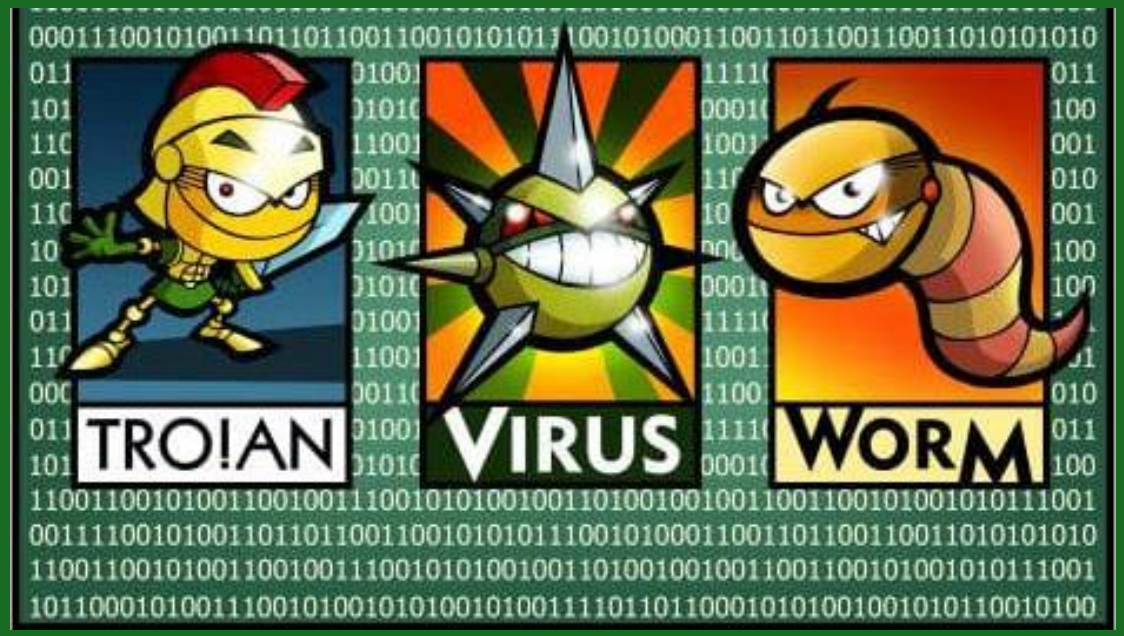
Powerpoint sui malware

Mihalache Mihai Alexandru 3D

Cosa sono i malware?

- I malware sono software malevoli progettati per danneggiare, compromettere o accedere illegalmente a sistemi informatici. Possono essere utilizzati per scopi dannosi come il furto di informazioni, il sabotaggio dei dati o il controllo non autorizzato di un computer.

Tipologie di Malware



Virus: Software che si attacca a file eseguibili e si diffonde quando questi file vengono eseguiti. Può danneggiare il sistema e comprometterne il funzionamento.

Trojan (Cavallo di Troia): Software che si maschera da programma legittimo per ottenere accesso non autorizzato al sistema. Viene usato per spiare o rubare informazioni.

Ransomware: Malware che cifra i dati e chiede un riscatto per decriptarli. Spesso colpisce aziende e utenti con dati sensibili.

Worm: Malware che si propaga autonomamente attraverso le reti senza bisogno di un file host. Consuma risorse di rete e può infettare dispositivi collegati.

Spyware: Software che raccoglie informazioni sensibili dall'utente senza il suo consenso, come attività online e credenziali.

Adware: Software che mostra pubblicità indesiderate e raccoglie informazioni per scopi pubblicitari.

Alcuni dei Malware più famosi

ILOVEYOU Virus (2000)

- **Tipo**: Virus
- **Descrizione**: Un virus che si diffondeva tramite email e si mascherava come un messaggio d'amore. Ha infettato milioni di computer in tutto il mondo, causando enormi danni e rallentamenti nei sistemi di posta elettronica.

WannaCry (2017)

- **Tipo**: Ransomware
- **Descrizione**: Un ransomware che ha criptato i file dei computer vulnerabili e ha richiesto un riscatto in Bitcoin per il recupero. Ha colpito in particolare ospedali e aziende in tutto il mondo, causando gravi danni e interruzioni.

Stuxnet (2010)

- **Tipo**: Worm
- **Descrizione**: Un worm progettato specificamente per sabotare i centrifughe nucleari in Iran. È uno degli attacchi informatici più sofisticati e mirati della storia, spesso considerato un attacco sponsorizzato da un governo.

Zeus (2007)

- **Tipo**: Trojan
- **Descrizione**: Un trojan bancario che rubava informazioni sensibili come credenziali di accesso e numeri di carte di credito. Ha infettato milioni di computer, ed è stato utilizzato per compiere frodi bancarie online.

CryptoLocker (2013)

- **Tipo**: Ransomware
- **Descrizione**: Un ransomware che cifrava i file delle vittime e chiedeva un riscatto in Bitcoin per decriptarli. Ha causato gravi danni a livello globale, mettendo in evidenza la crescente minaccia del ransomware.

Conseguenze di un Attacco Malware

Perdita di Dati Sensibili

- I malware possono rubare informazioni personali, come numeri di carta di credito, credenziali bancarie e dati aziendali. La perdita di queste informazioni può avere gravi ripercussioni per la privacy e la sicurezza degli utenti.

Interruzione dei Servizi

- Un attacco malware può causare il malfunzionamento di sistemi aziendali o dispositivi privati. Questo porta a periodi di downtime, impedendo l'accesso a file o applicazioni vitali e rallentando la produttività.

Danno Economico

- I costi per il recupero dei dati, le spese legali derivanti dalla violazione della privacy e i risarcimenti alle vittime possono essere molto alti. Le aziende potrebbero affrontare anche multe se non hanno implementato adeguate misure di sicurezza.

Danno alla Reputazione

- Un attacco malware può danneggiare irreparabilmente la fiducia che i clienti e i partner ripongono in un'azienda o in un individuo. La percezione di vulnerabilità può ridurre la clientela e influire negativamente sull'immagine del marchio.

Accesso Non Autorizzato

- Gli hacker possono ottenere accesso ai dispositivi infetti per controllarli da remoto, eseguire attacchi successivi o monitorare le attività, mettendo a rischio ulteriormente dati sensibili e la sicurezza.

Tipico programmatore di malware: