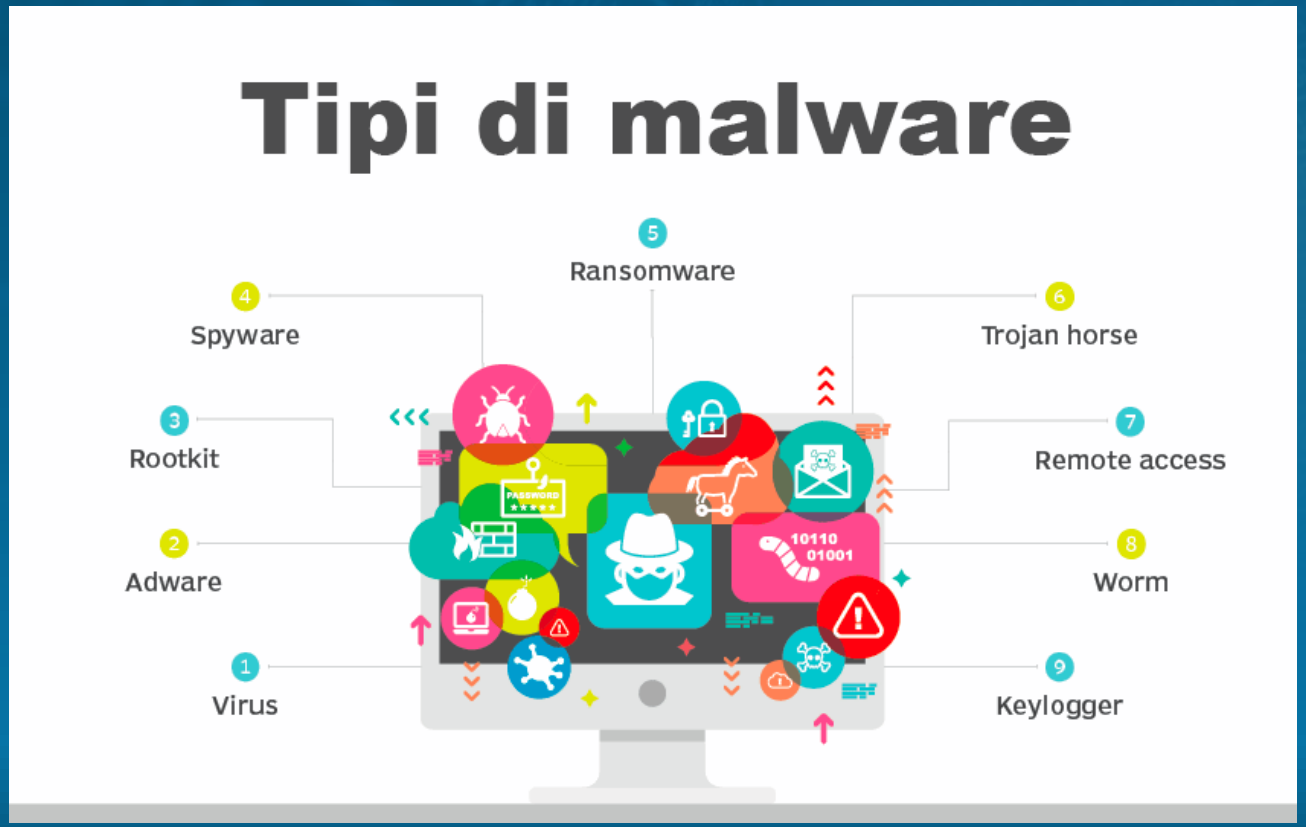
CYBER SECURITY

Malware

Il Malware

- Definizione e funzione
- Tipologie di minacce
- Protezione dai malware

I Malware



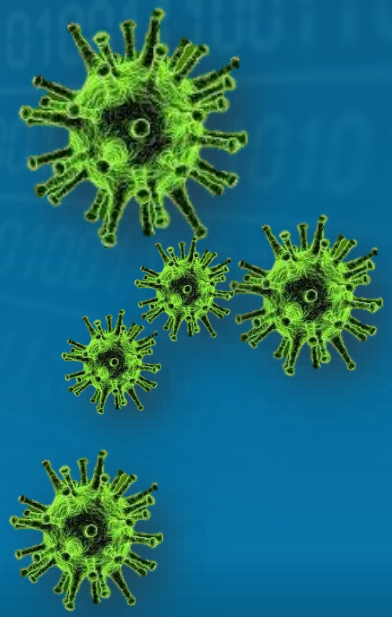
- Malware (abbreviazione dell'inglese **mal**icious software, lett. "soft**ware** malevolo"), nella sicurezza informatica, indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un utente di un computer.

- Approfondimenti…

Il Malware: Definizione e funzione

Programma, documento o messaggio di posta elettronica in grado di:

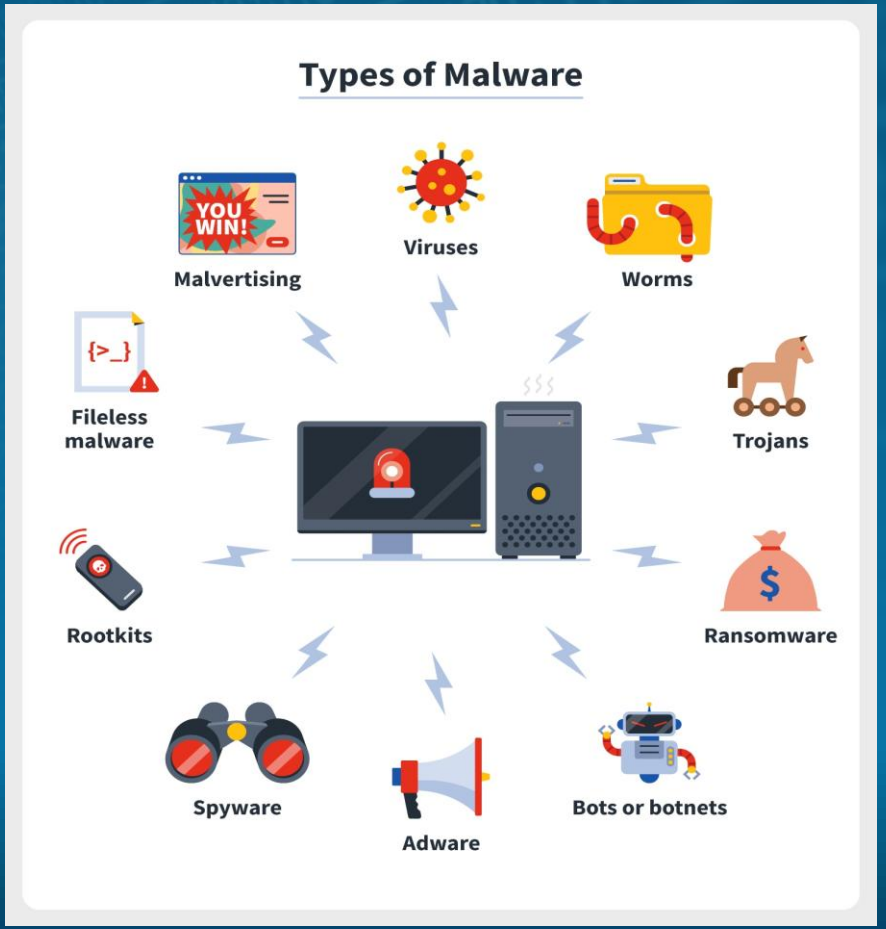
- apportare danni a un sistema informatico
- disturbare le operazioni svolte da un computer
- rubare informazioni sensibili
- accedere a sistemi informatici privati
- mostrare pubblicità indesiderata



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

Il Malware : Tipologie di minacce

- Virus
- Worm
- Trojan horse
- Backdoor
- Spyware
- Dialer
- Hijacker
- Rootkit
- Scareware
- Rabbit
- Adware
- Malvertising
- Keylogger
- Ransomware
- Bomba logica
- Zip Bomb



Il Malware : RootKit

- Seria minaccia ai sistemi informatici
- Meno conosciuti a torto meno temuti dei virus.
- Strumenti o insiemi di strumenti, come sequenze di macro o veri e propri software, atti ad ottenere sul computer bersaglio i permessi di root
- Il proprietario del sistema oggetto dell'attacco non se ne accorge
- Nella terminologia dei sistemi Unix/Linux, root è l'utente con pieni poteri sul sistema : è l'equivalente dell'account Administrator sui sistemi Windows.

Il Malware: Virus

Un virus, in informatica, è un software appartenente alla categoria dei malware che, una volta eseguito, infetta dei file in modo da fare copie di se stesso, generalmente senza farsi rilevare dall'utente

I Virus:Tipi

- 1) Boot Sector Virus
- 2) Trojan
- 3) Virus diretto e Worm
- 4) File infector Virus
- 5) Macro Virus
- 6) Virus multipartito
- 7) Virus polimorfi
- 8) Il Resident Virus
- 9) Web Virus Script

Worm e Trojan possono portare i Keylogger

I Virus

- Coloro che creano virus sono detti *virus writer*, che sfruttando le vulnerabilità (exploit) di un sistema operativo arrecando danni al sistema, rallentando o rendendo inutilizzabile il dispositivo infetto.
- I virus comportano comunque un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso. Come regola generale si assume che un virus possa danneggiare direttamente solo il software della macchina che lo ospita, anche se esso può indirettamente provocare danni anche all'hardware, ad esempio causando il surriscaldamento della CPU mediante overclocking, oppure fermando la ventola di raffreddamento.

VIRUS : I SINTOMI

- *Rallentamento del computer*
- *Impossibilità di eseguire un determinato programma o aprire uno specifico file;*
- *Scomparsa di file e cartelle*
- *Impossibilità di accesso al contenuto di file*
- *Messaggi di errore inattesi o insoliti*
- *Riduzione di spazio nella memoria e nell'hard disk*
- *Modifiche delle proprietà del file*
- *Errori del sistema operativo*
- *Ridenominazione di file*
- *Problemi di avvio del computer*
- *Interruzione del programma in esecuzione*
- *Tastiera e/o mouse non funzionanti correttamente*
- *Scomparsa di sezioni di finestre*
- *Antivirus disattivato automaticamente*
- *Lentezza della connessione Internet*
- *Limitazioni nella visualizzazione di alcuni siti Internet*

I VIRUS: EFFETTI

- Danneggiamento / Cancellazione / Cifratura Archivi
- Danneggiamento / Cancellazione / Cifratura Programmi /OS
- Effetti grafici
- Rallentamenti
- Segnalazioni di errori / guasti inesistenti

I Virus

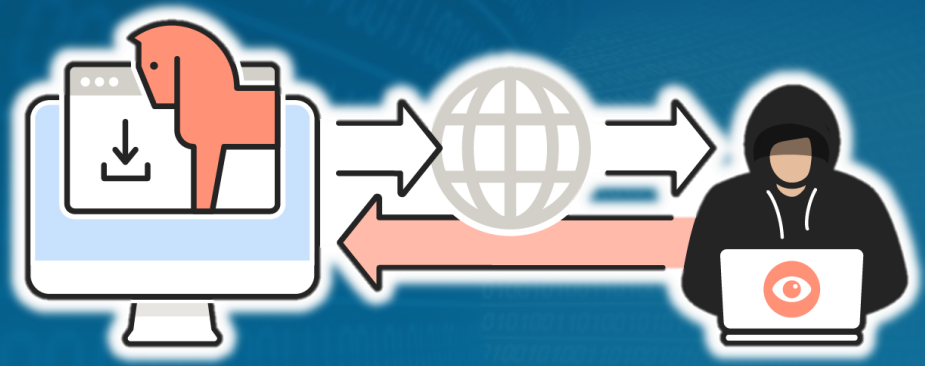
- **TRASMISSIONE**
  - Memorie di massa
  - Via rete
  - EMail
- **ATTIVAZIONE**
  - Immediata
  - Ritardata
  - A Comando
- **RIPRODUZIONE** automatica

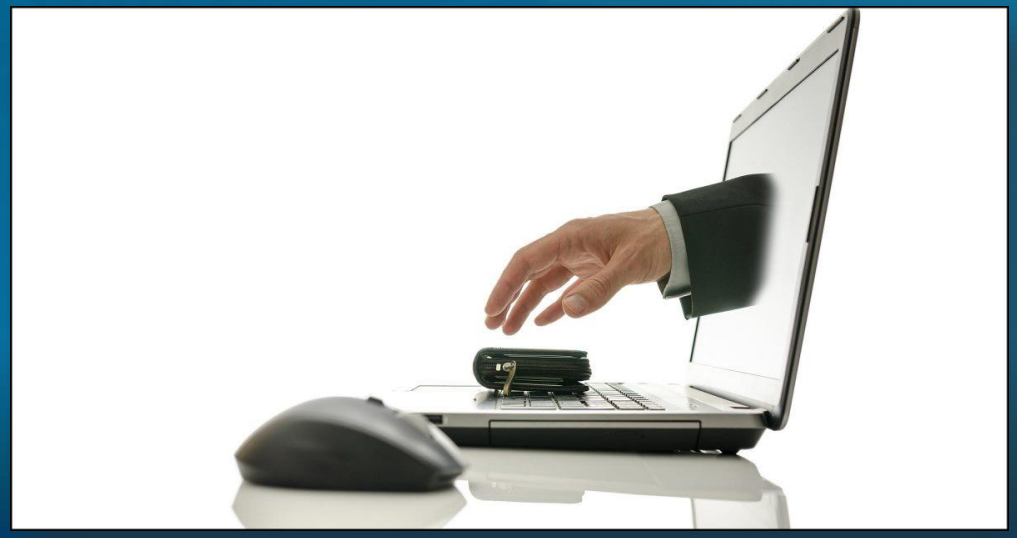
ALCUNE TIPOLOGIE DI ATTACCO

Trojan - RAT

Un **trojan** o **trojan** horse (in italiano Cavallo di Troia), nell'ambito della sicurezza informatica, indica un tipo di malware. Il **trojan** nasconde il suo funzionamento all'interno di un altro programma apparentemente utile e innocuo.

COSA SONO I REMOTE ACCESS TROJANS (RAT)?





- Un RAT è un tipo di malware che consente a un attaccante di accedere e controllare un dispositivo da remoto senza il consenso dell'utente.
- I RAT possono essere utilizzati per effettuare attacchi di phishing, rubare informazioni personali e finanziarie o per installare altri tipi di malware sulla macchina bersaglio.
- I RAT possono essere distribuiti attraverso e-mail di phishing, siti web compromessi o download di software indesiderati.

GLI ANTIVIRUS

- Programma in grado di riconoscere e neutralizzare un virus
- Operazioni:
  - Prevenzione
  - Aggiornamento
  - Cura
- CONTROLLI PERIODICI
  - Dischi, RAM e Supporti
- CONTROLLI APERIODICI / CONTINUATIVI
  - Posta elettronica, navigazione e scaricamento WEB
- NO Programmi Sconosciuti NO Macro