VIRUS INFORMATICI

MALWARE

- **MAL**icious soft**WARE** = software malvagio
- Vengono diffusi dai malintenzionati per danneggiare il nostro computer oppure per modificare i nostri dati.
- Si trasmettono tramite scambio di file, download di file, allegati email.

MALWARE

- TROJAN (''cavalli di Troia'')
- BACKDOOR (''porta sul retro'')
- ROOTKIT
- VIRUS
- WORM
- RANSOMWARE

TROJAN

- Software dannosi mascherati da ‘’buoni’’.
- Si insidiano all’interno di programmi che l’utente installa.
- Contengono istruzioni dannose che vengono eseguite durante l’installazione.

BACKDOOR

Sono paragonabili a porte di servizio che consentono di superare totalmente o in parte le procedure di sicurezza attivate in un sistema informatico.

Possono essere porte appositamente create dai gestori del sistema informatico per permettere una più agevole opera di manutenzione dell'infrastruttura informatica (**BACKDOOR LEGITTIME**) oppure dai cracker intenzionati a manomettere il Sistema (**BACKDOOR MALEVOLE**).

Le backdoor possono presentarsi in varie form: Software (codice nascosto in un programma che accetta comandi segreti per bypassare i controlli di sicurezza); Hardware (modifiche fisiche ai dispositivi che permettono accessi non documentati, ad esempio, in microchip o router); Protocollo (configurazioni vulnerabili o servizi di rete mal configurati che consentono accessi non autorizzati).

Tecniche di difesa: aggiornare regolarmente i sistemi per correggere eventuali vulnerabilità sfruttabili come backdoor, usare antivirus e firewall per rilevare attività sospette, controllare il codice sorgente specialmente nei software open source; auditing di sicurezza verificare periodicamente l'integrità del sistema; segmentazione della rete per limitare l'impatto di una backdoor.

PORTE

- Permettono ad un computer di effettuare più connessioni contemporaneamente verso altri computer, permettendo ai dati contenuti nei pacchetti che viaggiano nella rete di essere indirizzati verso il processo che li sta aspettando

PORTE

- Possono essere:
  - **Porte Conosciute** → sono assegnate dall'autorità IANA (Internet Assigned Numbers Authority) e sono inferiori a 1024
    - **FTP 21**
    - **SSH 22**
    - **TELNET 23**
    - **SMTP 25**
    - **HTTP 80**
    - **HTTPs 443**

PORTE

- **Porte Registrate** → sono richieste dalle aziende per le proprie applicazioni e vanno da 1024 a 49151
- **Porte Dinamiche** → sono liberamente utilizzabili da tutte le applicazioni utente e vanno da 49152 a 65535

- Per evitare che siano colpite è necessario un software di scansione delle porte oppure aggiornare continuamente i firmware

RANSOMWARE

- Impedisce all'utente di accedere alle aree del proprio computer.
- Una volta entrati, i criminali si impossessano dei dati chegli utenti, quando accedono, non riescono a vedere. Al loro posto, visualizzano un messaggio che li costringe a pagare un riscatto.

MALWARE INFETTIVI

- ***VIRUS***: software che rallentano il sistema operativo ed infettano i file, facendo delle copie di se stessi.
- ***WORM***: Simili ai virus ma non hanno bisogno di agganciarsi ad altri file; si propagano via Internet (allegati di email).

MALWARE FURTO DATI

- ***SPYWARE***: software che raccolgono le informazioni riservate e sensibili presenti nel computer (siti visitati, password, indirizzi email) e le diffondono all'esterno.
- ***ADWARE***: Sono le pubblicità che compaiono (ad esempio quando si gioca).

MALWARE FURTO DATI

- ***KEYLOGGER***: software che registrano tutto ciò che l'utente digita sulla tastiera.
- ***DIALER***: software che crea connessione ad Internet con associate elevate tariffazioni.

ANTIVIRUS

- Software utilizzato per prevenire, rilevare ed eliminare i malware.
- Confronta i file da analizzare con un archivio di tutti i malware conosciuti, con le specifiche ‘’firme’’.

ANTIVIRUS

- Sono efficaci se sono aggiornati di frequente.
- Quando è rilevata la presenza di un malware, solitamente si può decidere cosa fare: **eliminare sempre i file infetti**!
- A volte i file sono messi '' in quarantena'' perché sono stati riconosciuti come pericolosi ma non sono stati associati ad uno specifico malware.

ANTIVIRUS

- I file in quarantena sono trasferiti in una zona della memoria per essere analizzati nuovamente quando l'antivirus è aggiornato con i malware più recenti.
- I file in quarantena si possono recuperare ed utilizzare.