



La sicurezza Malware - Prima parte

MALWARE

Malware è l'abbreviazione di
malicious software



MALWARE

Il malware è un programma

Il malware è un software scritto da un programmatore.



MALWARE

Come per l'esecuzione di un qualsiasi programma, anche le istruzioni di un software malware vengono caricate nella memoria principale e il processore le esegue.

Se un programma comanda di cancellare tutti i file contenuti nell'Hard Disk, il processore esegue!

MALWARE caratteristiche

Come si classifica un software come malware?

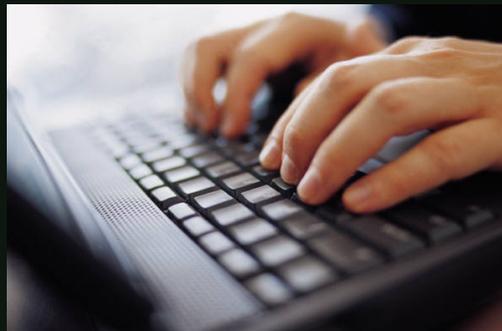
Il malware ha degli effetti dannosi sul sistema nel quale opera, anche se esiste del software burlone che si limita semplicemente a spaventare un utente



MALWARE caratteristiche

Come si classifica un software come malware?

Il malware si installa e si esegue in un sistema spesso all'insaputa dell'utente, che crede di svolgere tutte altre attività



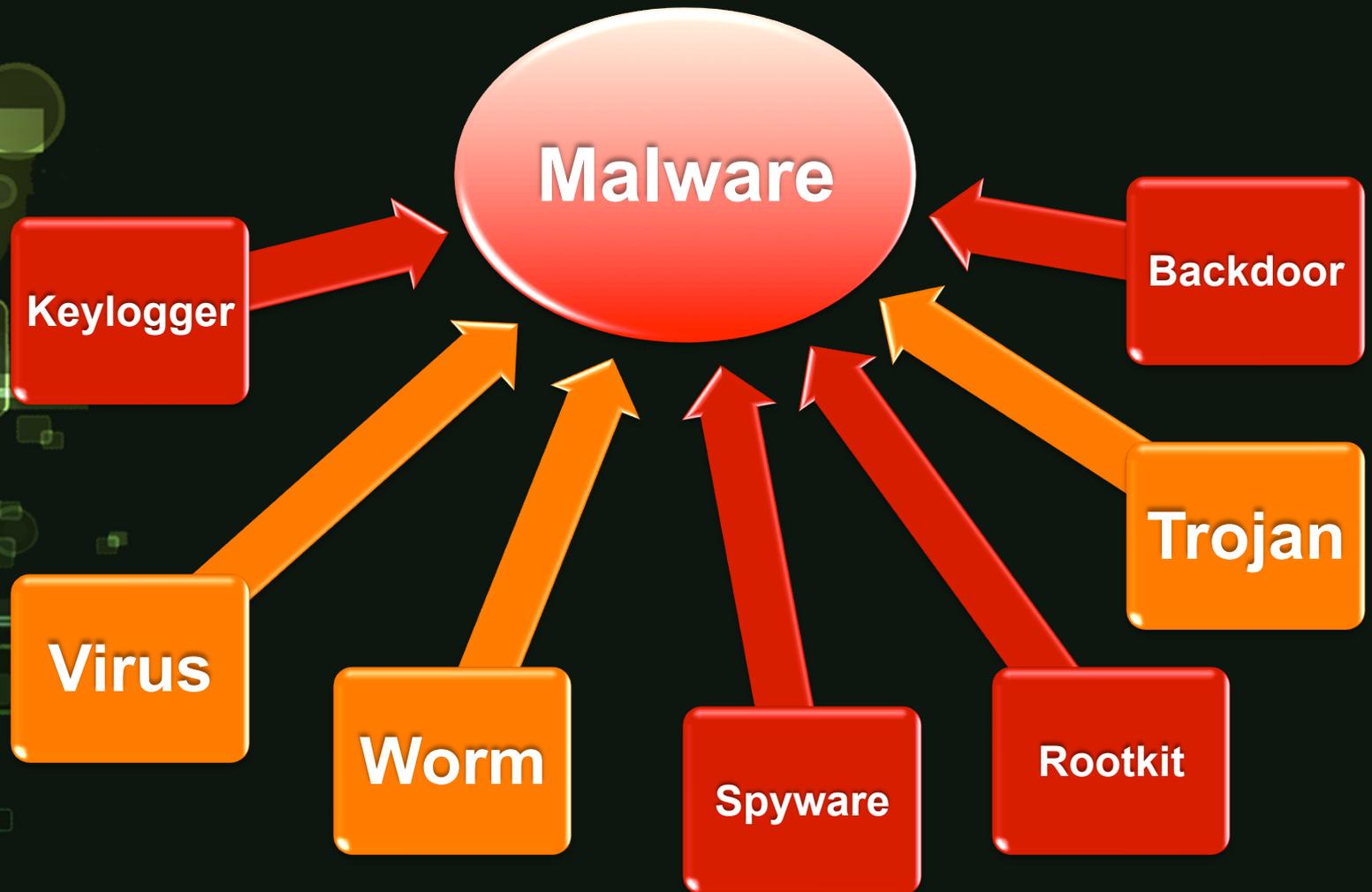
MALWARE caratteristiche

Come si classifica un software come malware?

Il malware si replica e cerca di avere una massima diffusione contagiando altri sistemi



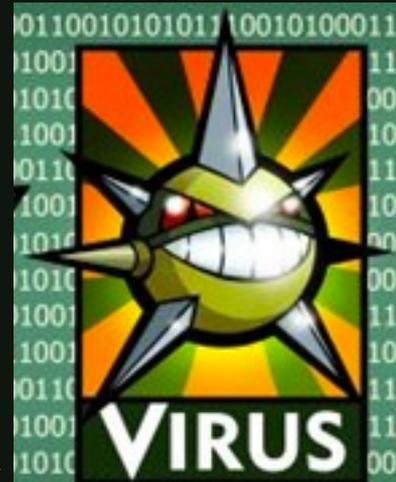
MALWARE tipologie



VIRUS

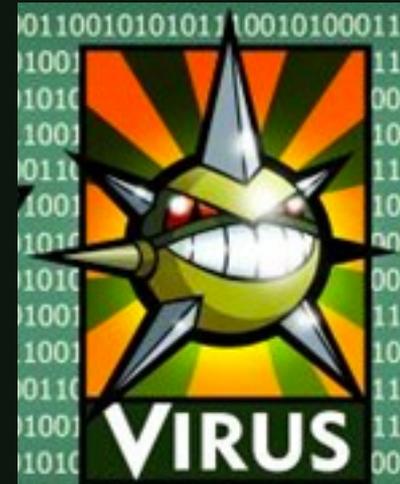
Un VIRUS è un malware che usa un altro programma come veicolo di diffusione e replicazione, esattamente come fanno i virus biologici.

Un virus ha quindi bisogno di un altro programma da infettare e viene eseguito quando l'utente avvia quel dato programma.



VIRUS trasmissione

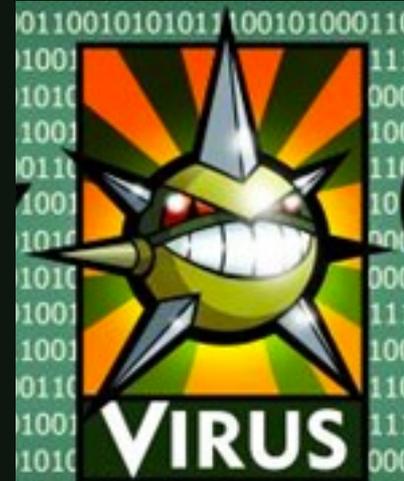
I VIRUS si diffondono attraverso file infetti trasmessi da computer a computer tramite chiavette USB, oppure scaricati da Internet, attraverso file-sharing, email o anche allegati in programmi di messaggistica istantanea.



VIRUS danni

I virus possono a vari livelli:

- Rallentare il sistema
- **Danneggiare dati e programmi**
- **Corrompere il sistema provocando gravi malfunzionamenti**
- **Bloccare completamente il computer**



TROJAN

Un TROJAN (cavallo di Troia) è un malware mascherato, da questo deriva il suo nome!

Fa credere all'utente di essere utile camuffandosi in un altro programma.

Un esempio classico sono i codec per la riproduzione di contenuti multimediali che molto spesso contengono dei TROJAN.



TROJAN trasmissione

A differenza dei VIRUS non si riproducono.

Si attivano su azione esplicita dell'utente: ad esempio aprendo allegati infetti alle email, oppure scaricando ed eseguendo file .exe da Internet.



TROJAN danni

Il trojan può provocare danni:

- lievi come aprire finestre di pop-ups o cambiare l'immagine dello schermo
- **Danni gravi come creare backdoors (vedremo più avanti) che permettono di accedere illegittimamente in remoto al tuo computer**



WORM

Un WORM (verme) è un programma malevolo che può riprodursi senza bisogno di farsi veicolare da un altro programma.



WORM trasmissione

A differenza dei virus i worms operano attraverso reti di computers.

Utilizzano infatti le reti per trasmettere repliche di se stessi a tutti i computers che sono connessi a quella rete.



WORM danni

La loro propagazione rallenta le prestazioni dei PC e delle reti, possono anche diffondere dati all'esterno.



<http://cdn.techpp.com/wp-content/uploads/2009/01/news-zotob-worm.jpg>