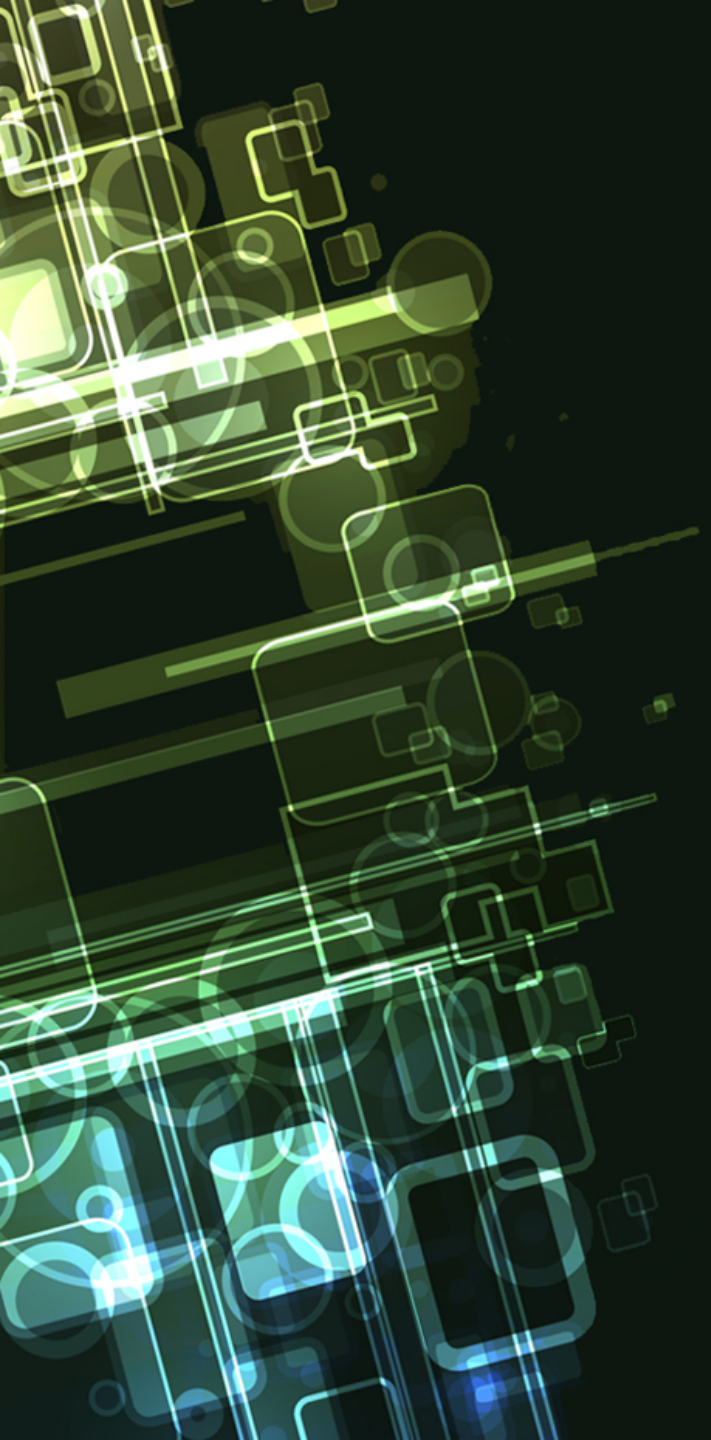


La sicurezza
Malware - Seconda parte

MALWARE

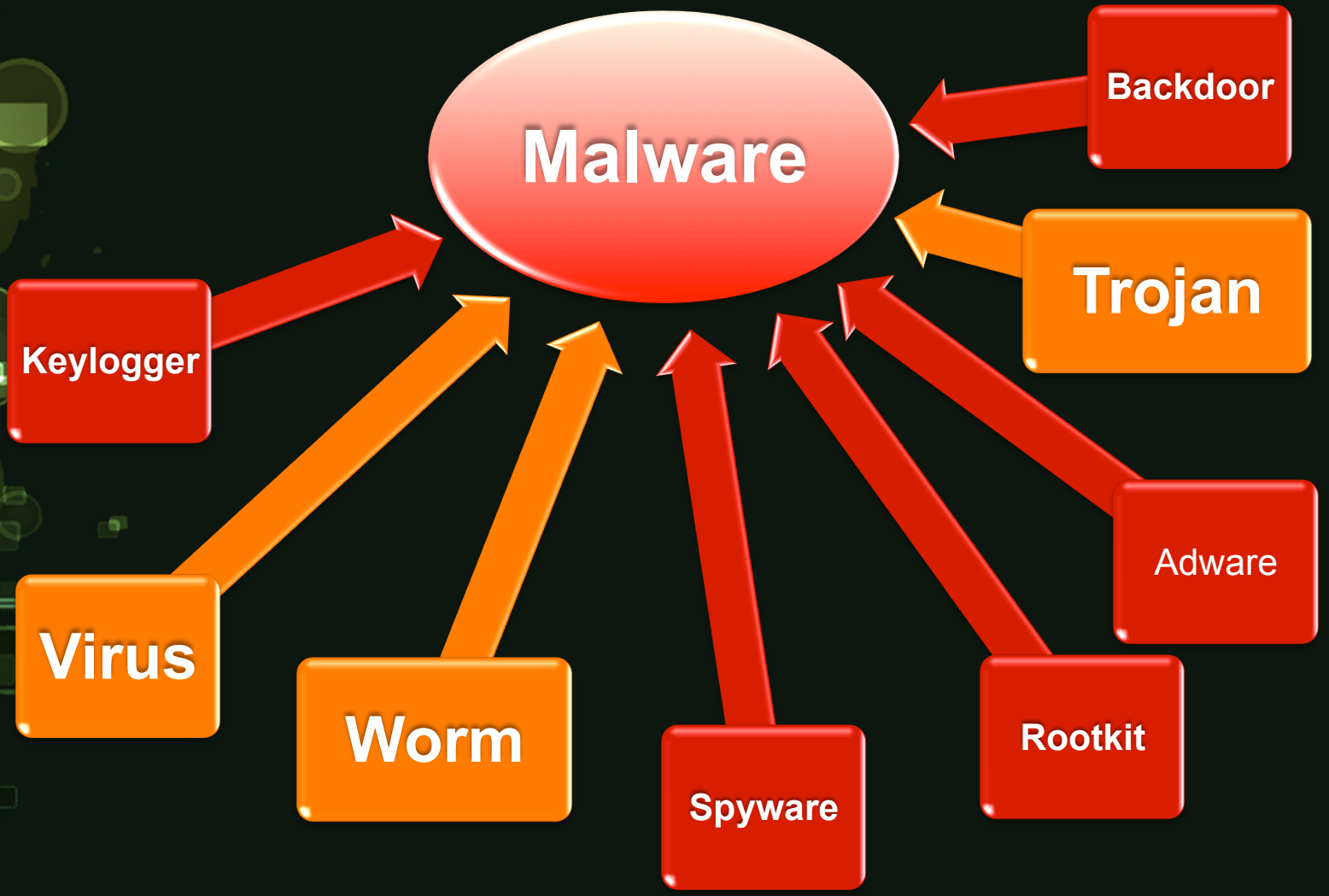
Malware è l'abbreviazione di **malicious software**

Ricordiamo....

Il malware è un programma

Il malware è un software scritto da un programmatore.

MALWARE tipologie



Abbiamo visto...

SPYWARE

Gli **spyware** spiano tutte le attività che avvengono su di un computer.

In genere raccolgono dati ed informazioni personali senza che l'utente se ne accorga.

KEYLOGGER

I keyloggers (keystroke loggers) registrano quello che si digita con la tastiera.

Con i keyloggers, i pirati informatici possono rubare username e passwords, numero della carta di credito, dati di accesso al tuo conto bancario e qualsiasi altra cosa si digiti, anche messaggi istantanei o mail.

I keyloggers sono spesso installati da un worm o da un trojan.

Hardware KEYLOGGER

I keylogger Hardware sono dei dispositivi con una memoria interna per monitorare le attività sulla tastiera. Possono essere:

1) Delle tastiere con un keylogger installato all'interno
2) Degli apparecchi esterni che sono installati su di una tastiera
3) Degli apparecchi esterni che si attaccano al cavo della tastiera.

ROOTKIT

Un rootkit è un malware progettato per infilarsi nel sistema nascondendosi in processi legittimi del computer ed è estremamente difficile individuarlo con dei normali antivirus.

ROOTKIT

Il rootkit serve ai pirati informatici per ottenere accesso remoto al computer con privilegi di amministratore.

Una volta ottenuto l'accesso, i pirati hanno il controllo totale del computer.

Possono eseguire programmi, rubare informazioni personali, modificare le impostazioni di sistema, installare altro malware, infatto sono spesso usati per installare backdoors e keyloggers.

BACKDOOR

Una backdoor permette di accedere ad un computer e a tutte le sue funzioni.

Spesso installate dopo l'esecuzione di un trojan, le backdoors maligne servono ai pirati informatici per far fare al computer infetto quello che vuole attraverso dei bots (programmi automatici).

BACKDOOR e BOTNET

Una volta infetto, il computer diventa parte di una botnet: una rete di computer infetti che il pirata informatico usa in remoto.

I bots sono usati per scopi illegali quali inviare in massa spam via email, nei commenti di siti o compiere attacchi informatici di tipo DoS (Denial of Service)

BOTNET

La figura (fonte wikipedia) mostra come funziona una BOTNET.

Un pirata informatico infetta una serie di computer, con vario malware (worm, trojan, rootkit) e si crea la sua "botnet"

Un compratore, acquista un servizio di "spamming" via email, o altri tipi di attacchi.

BOTNET

Per compiere queste azioni su grande scala i pirati informatici hanno bisogno di una botnet composta da migliaia di computer.

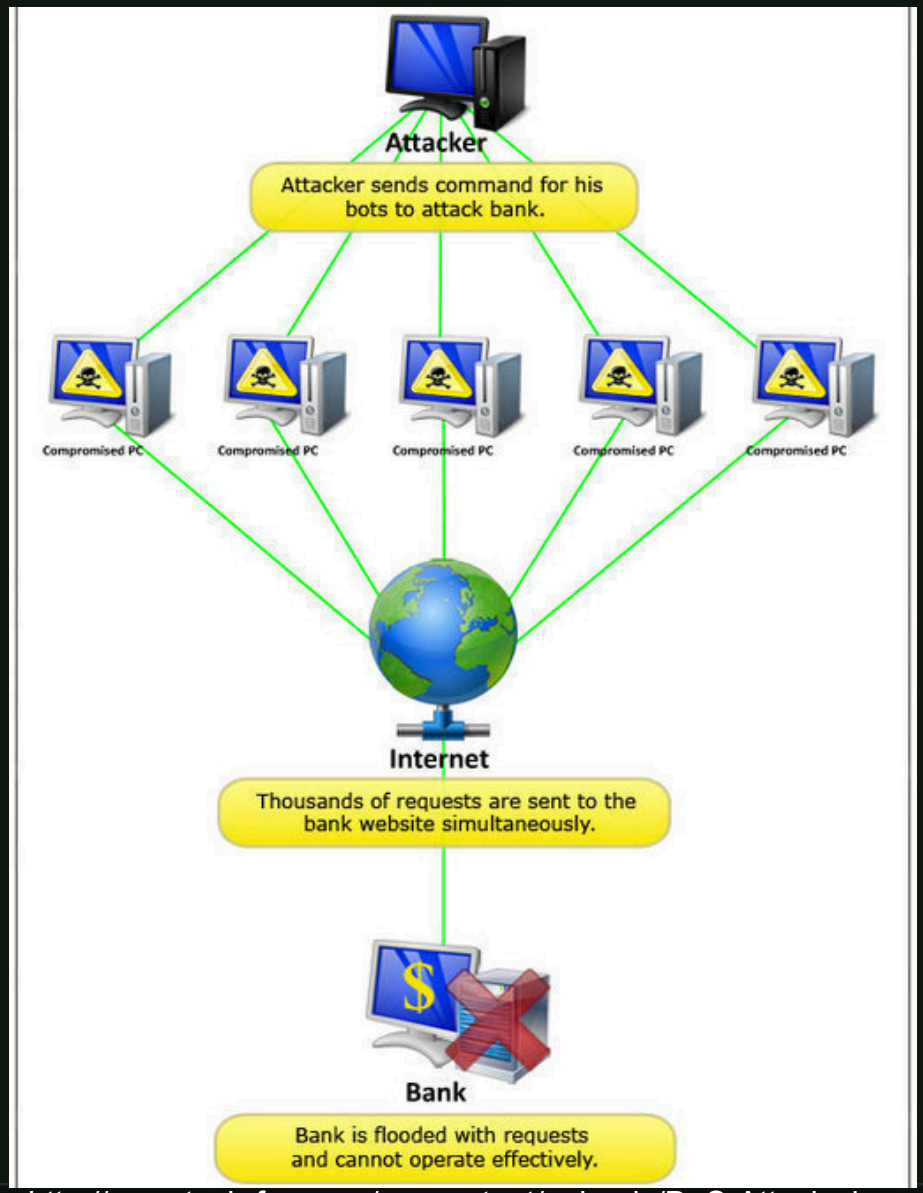
Un bot non danneggia attivamente il computer, ma lo rende complice di azioni illegali.

ATTACCO DENIAL of SERVICE

L'attacco DoS (Denial Of Service) indica un malfunzionamento dovuto ad un attacco informatico in cui si esauriscono deliberatamente le risorse di un sistema che fornisce un servizio come ad esempio un web server o un server di posta, fino a renderlo non più in grado di erogare il servizio ai client richiedenti.

(fonte wikipedia)

ATTACCO DENIAL of SERVICE



http://www.tech-faq.com/wp-content/uploads/DoS-Attacks.jpg

ADWARE

Gli ADWARE (advertisement e software) presentano inserzioni pubblicitarie esposte di proposito all'utente, allo scopo di indurlo ad effettuare ulteriori acquisti o eventuali upgrade del software utilizzato.

Gli annunci pubblicitari possono comparire nell'interfaccia utente del software, durante il processo d'installazione o in entrambi i casi.

ADWARE - SPYWARE?

- Talvolta i programmi adware presentano rischi: alcuni di essi aprono continuamente popup che rallentano notevolmente le prestazioni della macchina, altri modificano le pagine html per includere link e messaggi pubblicitari propri
- Molti adware inoltre comunicano le abitudini di navigazione dell'utente a server remoti.
- Non è facile, ed a volte quasi impossibile, essere a conoscenza di quali dati vengano inviati e ricevuti attraverso tale connessione, dati che possono essere potenzialmente dannosi se ricevuti o che violano la privacy se inviati (spyware)