

Virus: le malattie del computer...



Giacomo Ghirardini

giacomo@mt-lab.org

ICQ: 232757096

MSN: gh1r4z@hotmail.com



Creative Commons
Attribution-ShareAlike License



Cos'è un virus?

- Insieme di istruzioni.
- NON è un programma.
- NON è un file eseguibile ma bensì è “ospite”.
- Solamente l'apertura del file causa l'esecuzione del virus.
- Solitamente esegue copie di se stesso.
- Può cancellare o rovinare file, formattare l'hard disk, aprire backdoor, far apparire messaggi, disegni e modificare l'aspetto del pc.



Cos'è un worm?

- Insieme di istruzioni, che modificano lo stato del computer per auto eseguirsi.
- E' un programma (eseguibile).
- Si auto riproduce.
- Si auto invia come allegato camuffato a tutti i contatti della rubrica.
- Sfrutta bug dei programmi per eseguirsi automaticamente all'apertura dell'email, senza che l'utente se ne renda conto.
- Può sprecare risorse, installare backdoor, keylogger, rendere inutilizzabile il sistema.

Precisiamo che...

- Virus e worm attualmente sono sviluppati e infettano per la quasi totalità sistemi Windows, in quanto sono i più diffusi per un utilizzo desktop.
- Non c'è ancora “interesse” nello sviluppare questo tipo di applicazioni per ambienti Linux. Ciò non toglie che non siano presenti anche per altri sistemi operativi.
- La differenza sostanziale invece risiede nella filosofia open source.

Linux però offre “qualche” garanzia in più!
Il motivo principale risiede nella filosofia
Open Source.

Scopriamo perché..



Punto 1

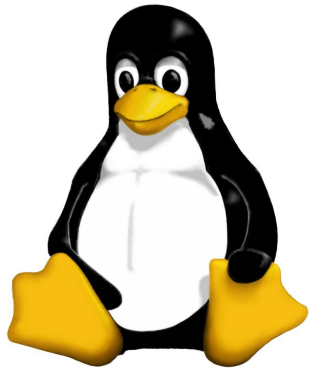
- Il codice è ispezionabile dal singolo e dalla comunità
- Chi scrive codice “aperto” è tenuto a mantenere dei canoni “qualitativi” che gli garantiscano professionalità.



Punto 2

- La comunità collabora: tutti possono partecipare.
- Se viene scoperta una vulnerabilità, può essere segnalata o addirittura corretta... da chiunque!
- Sarà compito di chi rilascia il software, dopo opportune revisioni, integrarla nelle successive versioni o rilasciare delle patch.
- Grazie a questo i tempi si accorciano.

Ma nella pratica?



In linux...

- Un utente normale non è in grado di eseguire comandi che possano compromettere file di altri utenti o al peggio il sistema.
- Un file per essere eseguito necessita di determinate caratteristiche e permessi.
- Non sono ancora diffusi worm e virus paragonabili a quelli per windows.

uhm... sono al sicuro allora!

La risposta è NO!

- In linux il problema risiede negli applicativi di rete.
- Problemi più grossi si presentano a livello server.
- I bug dei programmi, vengono sfruttati con l'utilizzo di appositi "exploit" che consentono ad un cracker, a seconda dell'entità del bug, di modificare lo stato del computer sotto attacco.