Veniamo attaccati semplicemente perché siamo online. Fingere di non esserci può essere molto di più di una semplice scusa.

Si è parlato e si parla molto degli ultimi virus (worm, per l'esattezza) che non hanno bisogno di veicolarsi tramite e-mail ma possono colpire un qualsiasi computer semplicemente se collegato a Internet.

Negli anni, siamo stati abituati a installare coscienziosamente le ultimissime versioni dei più noti prodotti antivirus e gli aggiornamenti del sistema operativo, così da assicurarci una certa tranquillità dal punto di vista della sicurezza.

Oggi non è più possibile ritenere che questo sia sufficiente, poiché un antivirus non rileva attacchi dall'esterno, ne configura le nostre connessioni in modo che vengano trasmessi e ricevuti solo i dati desiderati. La diffusione di un mail-less virus inizia con un "censimento" dei computer vulnerabili presenti in Rete.

La fase preliminare di un attacco avviene tramite una scansione più o meno casuale di Internet allo scopo di ottenere informazioni utili sulla presenza, sistema operativo e vulnerabilità dei computer interrogati; se i dati ottenuti da un indirizzo Ip soddisfano i requisiti necessari al worm per entrare in azione, il computer verrà attaccato.

Molto è stato detto sulle vulnerabilità che vengono sfruttate da worm di vario genere, e sul come risolverle, ma è ragionevole pensare che gli attacchi possono essere evitati a monte, non permettendo al nostro sistema operativo di fornire le informazioni richieste dagli attaccanti?

Per esempio, uno dei più semplici strumenti di scansione è il ping, che utilizza il protocollo di controllo ICMP (Internet Control Message Protocol) per rilevare la presenza di un computer o di un intera sottorete (Broadcast ICMP). Il ping non fa altro che inviare delle particolari richieste di ECHO, se il destinatario è attivo risponderà con un ICMP ECHO REPLY.

Può sembrare banale ma, se il nostro computer risponde a richieste di questo tipo, le probabilità di un attacco e di un infezione aumentano in modo esponenziale; sicuramente, per motivi funzionali, non verranno fatti tentativi estremi di rilevare computer che sembrano essere spenti o non connessi alla rete.

Per assicurarci davvero una certa sicurezza, è allora necessario dedicare pazienza e tempo all'installazione di un firewall, che ci consente di filtrare i pacchetti in entrata e in uscita e di risultare molto meno visibili alle scansioni da parte di worm e anche di hacker maligni (o *cracker* , come qualcuno preferisce definirli). Esistono molti prodotti freeware e altrettanto validi liberamente scaricabili.

Un ultimo aspetto. Nel caso il nostro computer fosse usato come punto di attacco da parte di un virus, i log del firewall potrebbero esserci utili per dimostrare di non essere noi stessi gli autori

dell'attacco.

Cristian Zavettieri