

Sfatiamo il mito: Sicurezza nella poca diffusione

Forse il mito che più di altri ricorre riguardante la sicurezza di Windows rispetto a Linux è il fatto che Windows ha una maggiore incidenza di virus, worm, trojan ed altri problemi perchè gli hacker "cattivi" tendono a concentrare le loro forze per irrompere nel software con la maggiore diffusione. Questo modo di ragionare è usato per difendere Windows e le sue applicazioni. Nonostante questo fatto possa essere vero, almeno in parte, l'implicazione che ne segue non è necessariamente vera: ovvero che linux e le sue applicazioni non sono più sicure di Windows, ma Linux è semplicemente troppo insignificante come obiettivo per perpetrare un attacco.

Queste ragioni cadono quando si considera che Apache è in assoluto il server web più popolare su internet. Secondo le statistiche di Netcraft relative al settembre 2004 il 68% di siti web gira su Apache. Solo il 21% usa Microsoft IIS. Se i problemi di sicurezza si riducono al semplice fatto che gli hacker con cattive intenzioni puntano la base di installazione maggiore, ne segue che dovremmo vedere molti più worm, virus e oaltro malwer indirizzato ad Apache ed al sistema operativo sottostante, più che per Windows e IIS. Inoltre, dovremmo vedere una quantità maggiore di attacchi contro apache rispetto a IIS, dal momento che il punto di partenza del mito è che il problema è questione di numeri, non di vulnerabilità.

Tuttavia questo è l'esatto opposto di quanto storicamente possiamo trovare. IIS è stato per lungo tempo il bersaglio preferito per worm ed altri tipi di attacchi, e questi attacchi sono andati a segno. Il worm Code Red, che sfruttò un buffer overrun in un servizio di IIS per prendere il controllo del web server, infettò qualcosa come 300000 server, e il numero di infezioni si fermò perchè il worm era stato scritto con l'intenzione di interrompere la sua diffusione automaticamente. Code Red.A ebbe una velocità di infezione ancora maggiore, sebbene anche questo fosse stato programmato per auto-terminarsi dopo tre settimane. Un altro worm, IISWorm, ebbe un impatto limitato solo perchè il worm era scritto male, non perchè IIS riuscì a proteggersi correttamente.

Si, si è a conoscenza dell'esistenza di worm per Apache, come per esempio Slapper. (Slapper tuttavia sfrutta una conosciuta vulnerabilità di openssl, non di Apache). Ma i worm per Apache raramente vanno a segno perchè hanno un effetto limitato e sono facili da eliminare. E' inoltre molto semplice ripulire e ripristinare il sito infetto con pochi comandi, e senza neanche un riavvio, grazie alla natura modulare di Linux e Unix.

Forse è per questo che, secondo Netcraft, nella classifica dei 50 server web con il più lungo uptime, 47 usano Apache. Nessuno nella lista usa Windows o Microsoft IIS. Così se fosse vero che gli hacker "maligni" attaccano le piattaforme software con la maggiore diffusione, questo ci riporta alla domanda sul perchè gli hacker sono così abili a penetrare le applicazioni e i sistemi operativi più popolari, ma non riescono a fare gli stessi danni al server web più popolare ed al suo sistema operativo.

Qualche attento osservatore che avesse esaminato il sito di Netcraft, avrà notato che tutti i 50 server nella lista girano su una delle varianti di BSD, per lo più BSD/OS. Nessuno di loro gira con Windows, e nessuno di loro usa Linux. Il più lungo uptime nella top 50 è di 1768 giorni consecutivi, come dire 5 anni circa.

Questa evidenza renderebbe BSD superiore a tutti gli altri sistemi operativi in termini di raggiungibilità, ma le informazioni di Netcraft sono in maniera non intenzionale scorrette. Netcraft monitora l'uptime dei sistemi operativi in base a come gli stessi tengono traccia del proprio uptime. Linux, Solaris, HP-UX, ed alcune versioni di FreeBSD registrano solo fino a 497 giorni, persino se funzionano continuativamente per anni. Così le statistiche di Netcraft non potranno mai registrare un uptime più lungo di 497 giorni per nessuno di questi

sistemi operativi, persino se hanno continuato a funzionare per anni senza nemmeno un riavvio, che è dunque la ragione per la quale non appaiono mai nella top 50. Ma questo non spiega perchè Windows non si trova nella lista dei primi 50. Windows non resetta il contatore del proprio uptime. Se ne deduce in maniera ovvia che nessun sito web basato su Windows è stato in grado di girare abbastanza a lungo senza reset per raggiungere la top 50.

La conclusione è che la qualità, non la quantità, è il fattore determinante quando si valuta il numero di attacchi andati a segno contro un software