Panda Software: come nei Labs di Bilbao i ghostbuster della rete combattono i virus informatici
Corriere Economia (maggio 2004)

Da qualche minuto Enrique guarda preoccupato il messaggio apparso a video. Perchè la banda verde, segno della situazione di normalità, è diventata improvvisamente arancione. Il segnale di pre-allerta significa che il nuovo virus informatico deve essere scaricato e immediatamente mandato in esecuzione, per verificarne il grado di pericolosità. E come Enrique temeva dopo pochi secondi ha la risposta. Si tratta di un attacco maligno, così fa scattare l'allarme rosso. Ci troviamo a Bilbao, nei laboratori di Panda Software. Nell'immenso palazzo di sette piani lavorano i 300 esperti e ricercatori software che ogni giorno si trasformano in cyberpoliziotti della rete. Perchè dal momento in cui parte il "red alarm" si scatena la guerra del tempo contro gli hacker. Ogni istante è prezioso per trovare l'antivirus da mettere online a disposizione degli utenti. Noi abbiamo avuto la possibilità di seguire in diretta gli eventi di questi minuti.

A spiegarci quali sono le procedure messe in atto per combattere i virus informatici è Mikel Urizarbarrena. Il 42enne fondatore di Panda software, da 14 anni Ceo e presidente dell'azienda spagnola. A fine anni '80 assieme alla moglie, sviluppa programmi per la gestione delle scuole guida. Poi un giorno, da un dischetto infetto prese il virus del "ping pong", quello che faceva scorrere sullo schermo il cursore, come una pallina impazzita. «Allora ho capito che questo sarebbe diventato uno dei problemi, ma anche dei mercati futuri dell'informatica. Così ho deciso di dedicarmi alla lotta e prevenzione dei virus». Oggi Panda Software è il primo produttore europeo di antivirus e occupa 800 dipendenti in 47 paesi del mondo.

Può spiegarci come rivelate la presenza di un virus che sta attaccando Internet?
«In diversi modi. Per prima cosa siamo collegati con i maggiori produttori di security e antivirus del mondo. In qualunque istante, come si passa dal primo al secondo livello di allerta, partono i messaggi di attenzione. Poi abbiamo un monitoraggio in tempo reale dei siti sospetti, delle news group e delle chat. Infine, per stabilire quanto partirà un attacco, ci appoggiamo a siti civetta e informatori web»

Di che cosa si tratta?
«I primi sono computer, sparsi in diversi paesi del mondo, che abbiamo programmato con una spiccata predisposizione a infettarsi e quindi ad essere attaccati da virus. I secondi sono invece esperti delle comunicazioni, che in modo analogo a quanto fanno gli informatori della polizia, spiano le rete e lanciano esche per attirare gli hacker».
E una volta individuato il virus come vi comportate?
«I laboratori di Bilbao sono strutturati con una rete protetta che prende in carico i virus. Una volta catturato e scaricato il codice, lo mandiamo in esecuzione su più computer mantenuti isolati dal resto della rete. Così valutiamo il grado di aggressività e quali sono gli effetti nocivi sul Pc, verificando la vulnerabilità dei sistemi operativi sotto test. Come Windows, Mac, Linux, Unix. La stessa procedura la effettuiamo nei confronti di programmi di lavoro come Office».
A questo punto quanto tempo passa per realizzare l'antivirus?
«In base alla pericolosità rilevata mettiamo subito al lavoro più team di ricercatori. In media entro due ore abbiamo trovato l'antivirus che trasmettiamo su Internet a disposizione gratuita di tutti gli utenti. Ma abbiamo registrato casi, come per Netsky.A in cui la soluzione è arrivata dopo solo 20 minuti».
Come sono cambiati gli attacchi hacker negli ultimi tempi?
«Sono più frequenti, fino a 100 al giorno, ma soprattutto portati con tecniche di strategie congiunte, lanciate da più punti del mondo e in stretta sequenza temporale».
Ci sono implicazioni tra virus informatici e terrorismo?
«Esistono similitudini di comportamento tra le celle del terrorismo internazionale e quelle dei pirati informatici. Entrambe rimangono spente e isolate per lunghi periodi, poi d'improvviso fanno convergere attacchi verso obiettivi comuni. Quindi non escludo, vista la possibilità economica dei primi, di assoldare gruppi di hacker per sferrare attacchi alle istituzioni dei paesi occidentali».

In rete: www.pandasoftware.com

###