Net-security: i pericoli del Web 2.0 si combattono con siti civetta.
Per attirare gli hacker in trappole "honey", come le api sul miele.
Intanto crescono i furti di identità digitale

(Corriere Economia, settembre 2007)

Allarme rosso per il Web 2.0. Almeno per quanto riguarda la sicurezza informatica. Perché anche i siti dell'Internet "collaborativo" non sono esenti da attacchi hacker. A rivelarlo, nella giornata odierna, è Symantec Internet Security Threat Report, l'indagine dell'azienda californiana che fornisce aggiornamenti semestrali in tema di minacce Internet. Nel rapporto è data particolare enfasi alla vulnerabilità dei cosiddetti siti di social-networking. Quelli che gli utenti, per la loro valenza sociale, ritengono sicuri. Ma non è così. Spiega a Corriere Economia Marco Riboli, responsabile di Symantec Italia: «in fatto di attacchi alla rete, negli ultimi mesi abbiamo assistito a un cambio di tendenza. Adesso i cyber-criminali non cercano più le vittime in modo diretto, bensì attendono che siano gli stessi utenti inconsapevoli, a creare il contatto». La trappola viene tesa secondo due modalità. La prima, riguarda donwload di file e link verso siti che inseriscono agenti trojan nella memoria del computer preso di mira. Si tratta di software maligni in grado di mandare in esecuzione programmi per catturare informazioni e dati presenti nei dischi rigidi del Pc.

La seconda, più insidiosa, riguarda il furto dell'identità digitale. L'appostamento avviene nei siti pubblici dove l'utente lascia le proprie generalità, catturate poi dai criminali informatici per perpetrare frodi (economiche) a nome di terze persone. In passato, secondo il report Symantec, gli hacker creavano singoli accessi illegali, ma adesso le tecniche sono affinate. «In questo contesto parliamo di attacchi multi-fase – dice ancora Riboli - perchè viene creato un primo contatto che opera come porta di ingresso, per mettere a segno attacchi più violenti in un secondo tempo». Per contrastare il fenomeno Symantec ha dislocato nel mondo 40 mila siti "civetta" con i quali effettua un monitoraggio in tempo reale degli attacchi in arrivo. L'obiettivo? Mettere in quarantena i virus informatici, per creare in pochi minuti l'antidoto. E renderlo disponibile agli utenti attraverso l'aggiornamento degli antivirus.

Ma questa non è la sola risposta per difendersi. Sempre un'azienda californiana, Websense, per far fronte alle nuove minacce, ha progettato un originale sistema di difesa chiamato "HoneyJax". «Una serie di siti, localizzati in tutto il mondo – dice Maurizio Garavello, country manager per l'Italia - che emulano il comportamento degli utenti durante l'utilizzo dei servizi disponibili nel Web 2.0». E così, come le api sul miele, gli hacker sono attratti da queste home-page trappola. Entrano nella memoria del computer e depongono codici maligni e virus pensando di essere al sicuro. Invece, in questo modo, forniscono agli esperti gli strumenti per combatterli. L'ultimo codice intrappolato da Websense lo scorso mese, prima che producesse un'infezione su larga scala, era un filmato intitolato "After World Episode 6". In apparenza innocuo era ospitato nel noto sito YouTube. Però una volta aperto, avrebbe scatenato un virus trojan in grado di rubare informazioni personali dal Pc degli ignari cyber-naviganti.

# # #