

Minacce web: non solo virus e spam

Tgcom intervista il manager di IronPort

Come si sono evolute le minacce che colpiscono i sistemi informatici? In principio c'erano solo *virus* e *spam*, ma ora gli hacker si sono evoluti e la gamma di attacchi in campo Web si è notevolmente ampliata: *image-based spam*, *phishing*, *spyware*, *rootkit*, *zombie*. Per capirci qualcosa di più, **Tgcom** si è rivolta a **Domenico Dominoni**, country manager di **IronPort Systems Italia**.

Come si sono evolute le minacce che colpiscono sistemi informatici?

Sono diventate più subdole e si sono moltiplicate, basta pensare che lo *spam* è aumentato di quattro volte negli ultimi sei mesi, diventando più cattivo e dannoso. Tutto questo crea un senso di insicurezza nell'utente.

Cosa intende per "minacce più subdole"?

Posso citare come esempio lo **spear-phishing**: è un attacco estremamente difficile da individuare, che consiste nell'invio di una e-mail ad un gruppo di destinatari precisi, come ad esempio i dipendenti di un'azienda. Il contenuto della lettera sarà credibile, dal momento che contiene informazioni riguardanti l'azienda stessa e magari viene inviata indicando l'esatto nome di un dirigente come mittente. E' quasi impossibile quindi per il destinatario non aprire il contenuto della e-mail, permettendo all'hacker di carpire informazioni preziose presenti sul computer di quella persona.

Se gli attacchi sono cambiati, significa che anche gli hacker si sono evoluti. Com'è cambiata la "figura" del pirata informatico?

Una volta si pensava all'hacker come al ragazzino che si divertiva a sfidare i grandi colossi informatici, ma ora è molto diverso. Nei mesi scorsi, ad esempio, è stato arrestato un informatico californiano: veniva pagato 100.000 dollari per effettuare attacchi mirati su commissione, controllando circa **400.000 personal computer** sparsi in tutto il mondo.

Qual è uno degli attacchi più pericolosi per un'azienda?

Sono parecchi, ma fra questi uno dei più comuni è il bouncing: dati alla mano, il 54% delle aziende italiane ha subito almeno un attacco di questo tipo nel corso del 2006. L'hacker invia migliaia di messaggi spazzatura a destinatari inventati, indicando come mittente l'azienda vittima dell'attacco. Il server dell'azienda riceverà quindi migliaia di messaggi di errore di ritorno (come avviene comunemente quando sbagliamo a digitare l'indirizzo del destinatario) e in meno di 8 ore crollerà.

Quali rischi corre invece un normale navigatore?

Una delle ultime tendenze è il **pharming**, cioè una mutazione dell'ormai noto phishing. Il pharming non prevede alcun invio di e-mail: l'utente si connette ad esempio al sito della propria banca e viene automaticamente rimandato in maniera trasparente ad un sito pirata e, dopo aver inserito codice password (recuperati dal pirata), viene riportato al sito corretto. E' molto diffuso anche l'**image-based spam**, cioè l'invio di immagini in allegato e con il testo non leggibile, eludendo così le tecniche anti-spam che prevedono la scansione del testo in chiaro o di un url su cui è possibile cliccare. Questo tipo di spam ha fatto quadruplicare il traffico di e-mail. Lo spam ha inoltre creato **il problema del falso positivo**: i sistemi di difesa "neutralizzano" e-mail che invece dovrebbero servire.

Quindi come ci si può difendere?

Prima di tutto è importante informarsi: si è parlato molto del **phishing** e quindi ora tutti sanno di cosa si tratta, rendendo inoffensivo più del 90% degli attacchi. Poi è fondamentale la prevenzione: muoversi alle prime avvisaglie è già troppo tardi e a quel punto si rischiano danni enormi e costi elevati.