

■ ■ ■ Osservatorio In crescita gli investimenti: 3,5 miliardi entro il 2011 in Emea

# Sicurezza, dopo le mail la minaccia è il phishing

di Lorenzo Facchinotti

**S**ono destinati a crescere gli investimenti in sicurezza in Europa, Medio Oriente e Africa. Secondo le previsioni di Gartner, il mercato del software passerà da 2,2 a 3,5 miliardi di euro tra il 2006 e il 2011. Intanto cambia il volto delle minacce informatiche. La diffusione di malware attraverso le e-mail continua a essere una pratica consistente. Tuttavia, la messa a punto di contromisure efficaci ha spinto truffatori e criminali a privilegiare altre tattiche. Il pericolo, infatti, passa ora attraverso i siti web.

**Alcuni dati.** Secondo i dati forniti da Gartner, alla fine del 2006 il segmento più redditizio è stato quello degli antivirus per i consumatori (26,9% del mercato), che ha superato quello dei software antivirus per le aziende (26,5%).

Le crescite più sostenute sono attese nel security information and event management (+20,3% anno su anno), nell'Url filtering (+18,7%) e, appunto, nel consumer antivirus (+13,5%). La crescita del segmento business antivirus sarà estremamente contenuta (+1,4%).

L'Europa occidentale vale oggi il 92,7% del mercato. Nonostante la crescita dell'Europa orientale, di Africa e Medio Oriente procederà a ritmi più elevati (13,6 e 14,7% anno su anno, rispetto al 9,2% della prima), nel 2011 il peso delle tre aree sarà solo lievemente differente. La Gran Bretagna è il mercato nazionale più grande, seguito da Germania, Francia e Italia.

**Dall'e-mail a Internet.** Nel passato recente, gli autori di virus sfruttavano l'ingenuità degli utenti, inducendoli a scaricare e ad aprire file allegati ai messaggi di posta elettronica. Secondo i dati forniti da Sophos, nel 2005 era infetta

una e-mail su 44. Grazie ai progressi dei sistemi di protezione nel primo semestre del 2007, tale rapporto è migliorato, passando a una e-mail infetta su 322. I criminali informatici hanno quindi cambiato strategia. Sempre secondo Sophos, infatti, il world wide web rimane un canale insicuro, che si presta a essere sfruttato per accedere a desktop e laptop. Spyware e altri tipi di malware sono quindi posizionati direttamente sui siti web (non importa la tipologia, solo un quinto di quelli infetti è stato concepito per fini illeciti). Iframe, che agisce inserendo codici «maligni» sulle pagine internet, ne è un esempio. Questo virus è all'origine del 49% degli attacchi sulle circa 260 mila pagine web trovate infette a giugno di quest'anno. Per dare consistenza alla loro azione, i criminali informatici sviluppano campagne spam che spingono gli utenti internet a visitare i siti infetti. Gli attacchi sono condotti in maniera rapida. Spesso il codice «maligno» viene rimosso dal sito dalle stesse persone che lo hanno messo per impedire che sia rilevato. Le principali precauzioni adottabili sono quindi il blocco dei siti per contenuto o tipologia (in questo senso un avvertimento viene lanciato nei confronti dei siti di social networking) e l'aggiornamento dei server web e dei browser (spesso infatti gli hacker sfruttano vulnerabilità già corrette dal rilascio di opportune patch dalle software house). Il 51% degli attacchi colpisce i server Apache, seguiti dai server IIS 6 (34%). Il 35% dei siti web infetti si trova in Cina,

il 27,2% negli Stati Uniti e il 4,5% in Russia. L'Italia non figura nelle prime dieci posizioni.

**Spam e phishing.** Lo spam e il phishing si confermano una minaccia in costante crescita. Secondo Rsa si registra un aumento della disponibilità di «Phishing Kit Man-in-the-Middle». Con questo termine si intendono pacchetti software accessibili presso repository on-line che comprendono programmi necessari per sferrare attacchi di questo genere. Tali kit sono molto semplici da usare, anche da chi è alle prime armi. La ragione per cui essi sono disponibili gratuitamente dipende dal fatto che contengono una backdoor, ovvero un pezzo di codice che invia i risultati dell'attacco (con, per esempio, le informazioni rubate) non solo a chi li utilizza ma anche a chi li ha creati.

Secondo Sophos anche la modalità di invio dei messaggi è evoluta. A quelli che includevano solo testo (facilmente filtrabili) e a quelli contenenti immagini si sono aggiunti messaggi con allegati in pdf. Spesso questi allegati sembrano contenere suggerimenti per investimenti finanziari redditizi. Rsa e Sophos sottolineano, infatti, che uno dei principali bersagli degli attacchi di phishing sono le istituzioni finanziarie. Secondo Rsa gli attacchi condotti contro queste ultime a livello mondiale oscillano tra i 150 e i 250 attacchi al mese (dati luglio



2006-luglio 2007). Sophos afferma anche che gli attacchi non sono finalizzati solamente a ottenere informazioni dai loro clienti. In alcuni casi, gli attacchi hanno lo scopo di alterare l'andamento dei mercati azionari, suggerendo per esempio l'acquisto delle azioni di una determinata società di cui, all'aumentare del valore, i truffatori vendono

le quote in loro possesso.

Tali attacchi sono chiamati «pump-and-dump». Inizialmente questa strategia ruotava soprattutto

intorno ai titoli nordamericani. In seguito all'intervento della Securities and Exchange Commission statunitense, che ha sospeso le contrattazioni di 35 titoli, l'attenzione si è spostata verso l'Europa.

I primi due paesi da cui provengono gli attacchi di spam sono Stati Uniti e Cina/Hong Kong (seppure con percentuali differenti). L'Italia è il quinto paese per attacchi ricevuti dopo Stati Uniti, Gran Bretagna, Canada e Spagna.

**Dispositivi mobili e memorie removibili.** Secondo Sophos un'ulteriore minaccia alla sicurezza viene dai dispositivi mobili (cellulari e palmari) e dalle memorie removibili (per esempio le «chiavette» Usb). Un primo ordine di problemi è legato alla diffusione di malware. Benché siano sempre più utilizzati per connettersi alla rete, solo un numero esiguo di palmari e di telefoni cellulari ha installato un sistema di protezione.

Le memorie removibili, da parte loro, facilitano la circolazione di virus e rappresentano una minaccia per la sicurezza dei dati. Ospiti e lavoratori temporanei che accedono alle risorse informatiche delle aziende possono inavvertitamente o di proposito copiare e fare uscire dati preziosi. In un sondaggio di quest'anno, il 63% dei responsabili dei sistemi informativi intervistati ha dichiarato che i lavoratori temporanei rappresentano una minaccia per la sicurezza più seria rispetto ai dipendenti.