PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 9 - numero 1773 di martedì 04 settembre 2007

Aumentano le minacce via internet

Pagine web infette sono tra le modalità di attacco più diffuse. La sicurezza nel primo semestre 2007.

Pubblicità

google_ad_client

Infettare server web è il metodo di attacco prediletto dai cybercriminali nel primo semestre del 2007; in tale periodo si è registrato infatti un forte incremento delle minacce provenienti da internet.

Lo rivela la Sophos, società operante nel settore della sicurezza informatica, nel suo ultimo "Rapporto sulla sicurezza". Nel mese di giugno le rilevazioni hanno isolato in media 29.700 nuove pagine infette al giorno, una cifra decisamente superiore alla media dei primi mesi del 2007, pari a circa 5.000 pagine infette al giorno.

Sul web. In una analisi svolta su un campione di un milione di pagine web tra quelle bloccate da Sophos, gli esperti hanno riscontrato che il 28,8% dei siti ospitava malware.

Un ulteriore 28,0% presentava contenuti destinati agli adulti; nella maggior parte dei casi, infatti, si trattava di siti pornografici o per il gioco d'azzardo.

Il 19,4% della pagine web bloccate era costituito da pagine create dagli spammer, mentre nel 4,3% dei casi i siti presi in esame sono stati classificati come illegali perché legati alla vendita di software pirata o a truffe on line (phishing).

I siti web non protetti divengono, loro malgrado, veicoli di infezione. Di tutti i siti web contenenti malware analizzati, solo il 20% era stato progettato specificamente per scopi illeciti; il restante 80% era costituito, infatti, da siti legittimi controllati dagli hacker.

"Per infettare facilmente e rapidamente un elevato numero di siti web ? affermano gli esperti di Sophos - , è sufficiente in molti casi che gli hacker manomettano un singolo file su un server web. Se il file fa parte di diversi siti web non correlati tra loro, ma ospitati su uno stesso server controllato dagli hacker, questi sono in grado di attaccare contemporaneamente un'enorme quantità di siti web."

La tipologia di server maggiormente colpiti dalle minacce via web a livello globale nel primo semestre 2007 è risultata Apache. "Vista l'enorme percentuale di pagine web infette, ben l'80%, ospitate su siti legittimi, sorge spontanea la domanda sul perché i gestori di spazio web non stiano adottando le dovute contromisure per rendere sicuri i propri server", ha commentato Walter Narisoni, Security Consultant di Sophos Italia. "[...] I gestori di spazio web sono chiamati ad agire in maniera responsabile, rafforzando la sicurezza dei propri server. Il semplice utilizzo di Apache non rende i server web completamente immuni agli attacchi degli hacker che tentano di piazzare malware sui siti web. Il fatto che tali attacchi non rappresentino un problema per le sole piattaforme Windows servirà ad aprire gli occhi a tanti utenti".

Pubblicità

In vetta alla classifica dei malware ospitati sui siti web nei primi sei mesi del 2007 troviamo Mal/Iframe, che agisce inserendo codici dannosi su siti vulnerabili.

"Le soluzioni per la sicurezza web non devono limitarsi a bloccare i siti web in base alla categoria: un sito per il gioco d'azzardo può sembrare pericoloso, ma talvolta i pericoli maggiori si annidano nei siti apparentemente più innocui", ha aggiunto Narisoni.

Posta elettronica.
Sebbene i criminali della Rete prediligano ormai il web alla posta elettronica come vettore di diffusione, le mail contenenti malware continuano a minacciare la sicurezza delle aziende e degli utenti privati. Nel corso dell'ultimo anno la percentuale di malware contenuto nei messaggi e-mail si è mantenuta costante. Durante il primo semestre 2007, una e-mail su 322 era infetta.

In tale periodo è stato registrato un significativo incremento dei messaggi di spam contenenti allegati. Gli spammer inseriscono sempre più spesso i propri messaggi pubblicitari in formato grafico non più all'interno delle e-mail, bensì negli allegati, adoperando file in formato PDF.
Gli hacker hanno sfruttato anche la funzione di avvio automatico sui PC con sistema operativo Windows. Se questa è abilitata, i codici dannosi vengono eseguiti automaticamente, non appena un'unità USB infetta viene connessa al computer.
Pubblicità
google_ad_client

Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

www.puntosicuro.it