Anno XIII n. 3105 di lunedì 10 novembre 2008 - PI / News

BOTNET, INFILTRATI MISURANO L'ECONOMIA DELLO STORM WORM

Si sono finti parte attiva della rete di PC zombie e hanno dirottato ignari utenti verso server virtuali per misurare la vera portata del business del malware

Roma - Arrivano ancora conferme "sperimentali" per quello che è già noto da tempo, vale a dire che il business delle botnet è enormemente profittevole, relativamente semplice da mettere su e senza particolari controindicazioni se si ha cura di camuffare adeguatamente le proprie tracce. Un business che, nel caso del notorio Storm Worm, **frutta quasi 4 milioni di dollari di ricavi netti all'anno**, sostengono i ricercatori dell'Università della California di San Diego e della UC Berkeley.

Per ottenere le informazioni necessarie a quantificare il valore effettivo della botnet riconducibile allo Storm Worm, i team delle due università statunitensi hanno adoperato una classica strategia da infiltrato, **prendendo il posto di un componente chiave per la ricezione e lo smistamento degli ordini impartiti ai bot** dal centro di *comando&controllo* del network malevolo.

Fatto questo i ricercatori hanno avuto la possibilità di fare il *redirect* di una parte dello spam del worm verso server da essi controllati, in tutto e per tutto uguali a quelli dello verme "reale" camuffati da dispensatori di pillole blu, arancioni e a pois per truffe finanziarie e per la raccolta fraudolenta di informazioni su account bancari.

Il "subset" dirottato dai ricercatori dovrebbe equivalere all'1,5% della dimensione totale della botnet, e nonostante questo i numeri registrati sono notevoli: su un periodo di 26 giorni il worm ha mandato in circolazione qualcosa come **350 milioni di mail-spam** contenenti i link ai siti fasulli controllati dagli esperti californiani. Di queste, la maggior parte delle e-mail è andata perduta nei filtri automatici anti-spazzatura, trasformandosi in potenziali "vendite" in 28 casi e portando a un ordine effettivo di "pillole della virilità".

Il valore di ogni singola vendita, e quindi la quantità di denaro sottratto agli utenti creduloni, è stato calcolato in 2.731 dollari complessivi, il che ha portato i ricercatori a stimare - considerando quell'1,5% di rete analizzata - **un guadagno annuo complessivo per il business di Storm Worm di 3,5 milioni di dollari**.

Tra gli altri interessanti dati evidenziati dall'indagine, tutti disponibili nello studio in formato PDF, vi sono la capacità di propagazione del malware, con un numero di nuovi bot giornalieri stimato tra i 3.500 e gli 8.500, e l'allarmante percentuale di utenti che, nonostante gli avvisi, le raccomandazioni e le campagne di "sensibilizzazione" alle problematiche concernenti la sicurezza informatica soprattutto in rete, **continua a fare click sui link presenti nelle mail-spazzatura**.

"Una persona su 10 che fa click per ricevere il malware è un dato serio" ha commentato il professore associato della USCD Stefan Savage, un dato che suggerisce "che per gli autori del worm il catturare un numero sempre maggiore di vittime sia poco più che una semplice questione di marketing".

Alfonso Maruccia

Punto Informatico è testata giornalistica quotidiana - Tribunale di Roma n. 51 del 7.2.1996
Fondato da Andrea De Andreis nel 1995
De Andreis Editore Srl - P.IVA: 06696301008 - ROC: 7983