



SPAM IV, IL GRANDE RITORNO

Era troppo bello per essere vero, e infatti è durato pochissimo: dopo la chiusura del più grande network spara-spazzatura, lo spam sta tornando a riempire le reti di tutti

Roma - Lo avevano detto, i ricercatori di sicurezza che avevano contribuito a buttare giù il [mega-network dello spam McColo](#), che la drastica riduzione del livello di mail-spazzatura in circolazione (si parla di un 65% in meno) non poteva durare a lungo. E infatti sono passati appena pochi giorni che già le più grandi botnet note agli esperti **danno segni di una decisa ripresa delle attività**.

D'altronde la stagione natalizia incombe, quindi i cyber-criminali e i truffatori **si sono dati un gran da fare nell'individuare nuovi provider** di banda in *upstream* magari meno sensibili alle sirene delle società di sicurezza di quelli del fu-network di McColo.

Secondo l'opinione di Matt Sergeant, senior anti-spam technologist di MessageLabs, le maggiori botnet attualmente conosciute **hanno ricominciato a spammare il mondo con rinnovato vigore**: "Le botnet dietro Asprox e Rustock sono tornate a colpire con violenza dopo aver individuato un nuovo centro di comando&controllo", [dice](#) Sergeant, così come sono più attive che mai Meda-D e la botnet controllata da Warezov, una delle *worm-pestilenze* con un *rate* di proliferazione delle varianti più alto di tutti i tempi.

Il network di *Cutwail* "non se ne è mai andato via", continua il ricercatore, e ha colto l'occasione del rilassamento nell'attività dei concorrenti per aumentare ulteriormente i propri spam-tentacoli. Il quadro è completo con il ritorno anche di *Srizbi*, la super-botnet che secondo Sergeant è responsabile del 50% di tutte le mail-spazzatura in circolazione e che aveva evidentemente **subito la maggior parte dei danni** causati dallo *shuttdown* di McColo.

"Nelle ultime 24 ore - sostiene il ricercatore - *Srizbi* è riuscita a riprendere il controllo di alcuni dei PC zombi che erano rimasti inattivi dopo la disconnessione di McColo". Per ora la botnet non è al pieno della sua operatività ma, avverte

Sergeant, visti questi ultimi sviluppi nel "settore" "ci aspettiamo di veder tornare i volumi di spam ai livelli *normali* in una settimana circa". E [buon natale a tutti voi](#).

Alfonso Maruccia

Punto Informativo 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.MA: 06696301008 - ROC: 7983
