

I dodici paesi dove lo spamming è di casa

di Pino Fondati

Il richiamo è a un mitico film di guerra (dodici pregiudicati che si riscattano in un'azione temeraria contro i nazisti), ma ha ben poco di eroico invece la "sporca dozzina" di cui Sophos, società attiva nel settore della sicurezza informatica e nella tecnologia di controllo dell'accesso alla rete (la cosiddetta Nac), parla nel suo rapporto sulle ultime tendenze nel panorama dello spam. Si tratta infatti dei dodici paesi che hanno prodotto la maggior quantità di mail spazzatura nel secondo trimestre del 2008.

Premessa: le indagini della società rilevano un aumento allarmante del volume di spam in circolazione su Internet tra aprile e giugno 2008, e il vizio nuovo degli spammer a sfruttare i siti delle reti sociali come Facebook e i telefoni cellulari per diffondere messaggi non richiesti. Tutto questo fa un volume di spam che aumenta dal 92,3% dei primi tre mesi di quest'anno al 96,5% del secondo trimestre. In altre parole, 27 mail aziendali su 28 sono spam, un numero impressionante. E arriviamo alla dozzina di cui sopra. I dodici paesi che hanno prodotto la maggior quantità di spam a livello mondiale tra aprile e giugno 2008 sono Stati Uniti (14,9%) e Russia (7,5%), che confermano una "leadership" duratura, Turchia (col 6,8%, fa un bel balzo in avanti rispetto al secondo trimestre 2007, quando era nona), Cina (inclusa Hong Kong) col 5,6%, Brasile col 4,5%, Polonia al 3,6%, Italia anch'essa col 3,6% (era ottava..), Corea del Sud (3,5%), Gran Bretagna (3,4%), Spagna (3,2%), Germania (3,0%), Argentina (2,9%, un debutto assoluto a spese, si fa per dire, della Francia). Il restante 37,7% se lo divide il "resto del mondo". Se si guarda alla classifica per continente, l'Asia guida la poco lusinghiera classifica alla grande con il 35,4%, seguita da Europa (29,5%), Nord America al 18,2%, Sud America (14,8%), Africa con l'1,2 per cento.

I messaggi di spam vengono quasi sempre inviati da computer zombie, controllati dai cybercriminali per ricavare profitti illeciti all'insaputa dei proprietari. Si tratta in genere di computer privati sprovvisti di adeguata protezione antivirus, firewall o patch di sicurezza aggiornati. Gli spammer si servono sempre più dei siti di social network come Facebook e LinkedIn per diffondere messaggi contenenti collegamenti a negozi online, lotterie fittizie e operazioni finanziarie fraudolente. In queste attività, si trovano a fare i conti con i filtri antispam aziendali installati sul gateway di posta, che impediscono ai messaggi illeciti di giungere a destinazione. Per aggirare l'ostacolo, essi sfruttano i siti delle reti sociali come Facebook piazzando messaggi di spam nei profili degli iscritti. I messaggi vengono poi letti non soltanto dai titolari dei profili, ma da chiunque visiti la pagina in questione. Un altro canale di diffusione sempre più in voga è rappresentato dai messaggi Sms inviati ai telefoni cellulari. In aumento è il cosiddetto "spear phishing", consistente nell'invio di messaggi personalizzati a uno specifico dominio o azienda.

Queste mail sembrano provenire da una fonte attendibile (per esempio, un membro del team responsabile dei sistemi informativi all'interno della stessa azienda del destinatario), e includono richieste di informazioni personali (nome utente e password, ad esempio). Rispondendo a questi messaggi, i destinatari forniscono involontariamente informazioni utilizzabili dai truffatori a scopi malevoli, come il furto d'identità. I criminali informatici dediti allo spear phishing generano gli indirizzi delle vittime usando speciali software o elenchi di dipendenti scovati nei siti delle reti sociali. Il consiglio che Sophos rivolge alle aziende è di aggiornare la protezione antivirus in modo automatico e di adottare una soluzione integrata sul gateway web e di posta per proteggersi da virus e spam.