Anno XIII n. 3095 di lunedì 27 ottobre 2008 - PI / News

LO SPAM FA TANA SUI SERVER REMOTI

Altro che botnet, le schifezza-mail bypassano i PC dell'utente per attaccare direttamente i gateway di spedizione dei messaggi. Gli account fittizi la fanno da padrone

Roma - Guardandola dal punto di vista dei cyber-criminali e delle gang telematiche, nonostante i colpi mortali da parte dell'antispam, lo spam sta bene anzi benissimo. La posta-spazzatura fluisce costante e inesorabile dai gateway di tutto il mondo, anzi, persino più dai gateway che attraverso le botnet di PC zombie, avverte la società di sicurezza Cyberoam.

L'ultima frontiera di una piaga in evoluzione costante prevede **la compromissione di server, macchine remote e dispositivi per il routing delle missive**, schiavizzati al volere delle gang dello spam con tecniche sopraffine e senza che la maggioranza dei filtri anti-spazzatura riesca a porre un freno alla crescita del fenomeno.

Il meccanismo di attacco prevede inizialmente il furto delle credenziali di accesso dell'utente al server attraverso i malware di cui sopra, passando poi **all'hacking del processo di apertura di nuovi indirizzi**. Centinaia e migliaia di caselle e-mail fasulle e sparaspam vengono aperte grazie agli algoritmi di decifrazione delle sempre più inutili protezioni captcha, pensate proprio per combattere la registrazione in massa di account fittizi.

A quel punto il gioco è fatto e la corsa allo spam si sposta dalle botnet ai server, "zombificati" e trasformati in bot di una macchina spara-schifezze **ben più efficace** di quella che è possibile costruire infettando PC di utenti poco consapevoli.

Il malware fa la tana sui server, e non solo o non necessariamente in quelli per l'invio di e-mail: forte è la crescita di siti compromessi iniettando codice malevolo pensato per aprire una breccia nei browser fallati, trojan, virus e worm sono spesso incuneati in applicativi in tecnologia Flash, codice HTML o JavaScript o anche sui blog o i "journal" aperti su servizi gratuiti quali Blogspot/Blogger e

Flickr.

In quest'ultimo caso, avverte il VP di Cyberoam Abhilash Sonwane "Data la natura mista degli attacchi, una sicurezza composite che includa soluzioni antivirus, antimalware e di content filtering offre layer di protezione di secondo e terzo livello". Il primo livello, quello dei PC degli utenti da cui tutto può partire, **rimane un affare problematico da gestire** soprattutto dal punto di vista dell'utenza domestica.

Il layer numero uno del campo di battaglia della sicurezza in rete si difende "aumentando la consapevolezza del problema presso gli utenti e rafforzando comportamenti di navigazione responsabile nei network aziendali", sostiene Sonware, solo così è possibile "prevenire tali minacce in maniera significativa".

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