Anno XI n. 3163 di venerdì 13 febbraio 2009 - PI / News

WALEDAC, IL RITORNO DELLE BOTNET

La più celebre delle armate delle tenebre informatiche risorge. Storm è tornata, ed è più cattiva di prima. Questa volta, cavalca il giorno degli innamorati. E non è l'unica minaccia

Roma - Era stata data per spacciata, ma è tornata ed è più furba di prima. **Storm, la botnet più vasta fino ad oggi conosciuta** che nei suoi momenti di massimo splendore contava centinaia di migliaia di PC zombie ridotti a semplici schiavi dello spam, si è reincarnata in un temibile avversario per ogni esperto di sicurezza: ora si fa chiamare **Waledac**, e ha aggiunto ulteriori livelli di protezione alla propria infrastruttura e al suo codice. Per il momento è rimasta silente, ma potrebbe presto tornare a colpire.

La caduta di Storm, avvenuta più o meno a metà dell'anno scorso, secondo gli esperti è legata a una serie di fattori. Prima di tutto il tentativo riuscito di **intrufolarsi nel codice del malware**, decifrandone il funzionamento: in questo modo era divenuto possibile prevedere le prossime mosse del malware, capire quale sarebbe stato il successivo vettore d'attacco e identificare con certezza quale fosse il traffico generato in Rete. Da qui al secondo passo, la distanza è breve: una volta individuato il protocollo di comunicazione, **smantellare la rete P2P** che teneva in piedi la botnet era divenuta un'azione quasi banale.

In breve, individuare e rimuovere il malware che spargeva il seme di Storm era divenuto possibile: filtra oggi e filtra domani, i loschi figuri dietro alla botnet si erano praticamente ritirati. Ma di certo non arresi. La nuova variante di Storm, che come detto è stata denominata Waledac, agisce con gli stessi metodi e gli stessi scopi apparenti della sua progenitrice: tramite **consolidate tecniche di ingegneria sociale e phishing** induce ad installare un malware sulla propria macchina, che a quel punto diviene una pedina su una più ampia scacchiera che vede contrapporsi produttori di spam e chi si oppone alla posta spazzatura.

A differenza dello scorso anno, tuttavia, il codice installato sulle macchine vittima è molto cambiato: sfrutta in maniera massiccia il **polimorfismo**, vale a dire che è

protetto con diversi strati di codifiche per rendersi meno identificabile dagli antivirus, e ha sostituito alla rete P2P un più semplice ma efficace **protocollo di comunicazione sulla porta 80** (la stessa dell'HTTP). In questo modo, tracciare il traffico effettivamente veicolato dalla botnet diventa più complesso: senza il codice sorgente del virus, senza cioè le istruzioni per scovarlo, può essere facilmente confuso con quello diretto verso legittimi siti web.

Secondo le stime attuali, Waledac sarebbe composta da non meno di 20mila-30mila PC-zombie assoggettati, anche se per il momento non si sarebbe registrata alcuna particolare attività svolta dalla botnet in questione: i suoi padroni probabilmente attendono che **l'ondata di spam di San Valentino**, farcita di migliaia di messaggi esca che fanno riferimento ad una fantomatica cartolina d'amore che è in realtà il veicolo del malware, faccia il suo effetto. Quando i numeri si saranno avvicinati a quelli di un tempo, quando la massiccia operazione di scansione delle macchine infette alla ricerca di indirizzi email e password sarà a buon punto, allora torneranno a colpire.

Le armi dei malintenzionati, inoltre, in questo ultimo periodo si stanno affinando sempre di più. È di questi giorni la notizia di una nuova variante del già noto *Virut* (anche noto come *Virux*), un malware che in alcune versioni è in grado di **diffondersi anche attraverso script PHP o ASP** infetti: quando l'utente visita un sito compromesso, un *iframe* viene attivato per contagiare la macchina locale con lo stesso tipo di malware.

E se tutto questo non bastasse, c'è anche un'altra arma nell'arsenale dei cattivoni: **clonare i siti delle aziende di sicurezza**, produttori di antivirus in primis. Si crea una copia perfetta, a parte qualche piccola sgradita sorpresa nascosta del codice, si attacca il sito originale con un'aggressione DDoS per renderlo inoperativo e poi ci si mette comodi ad aspettare. Nella migliore (si fa per dire) delle ipotesi, i comuni utenti in cerca di protezione finiranno per infettarsi proprio dove dovrebbero sentirsi più al sicuro.

Luca Annunziata

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