Reti aziendali nella morsa delle Botnet

di Francesco Armando

Il tono è asciutto: «Una nuova botnet ha infettato più di quattro milioni di PC ed è praticamente indistruttibile». La fonte autorevole: Sergey Golovanov, researcher dei Kaspersky Labs. Nel documento pubblicato poco prima dell'estate viene descritta in modo particolareggiato una botnet di almeno 4,5 milioni di PC virati, tenuti sotto scacco da "Tdl-4", la versione più aggiornata del malware Tdss, conosciuto almeno dal 2008.

Tdl-4 è un malware sofisticato. Incorpora funzionalità di difesa contro il codice di botnet concorrenti, un componente rootkit a 64-bit per cifrare le comunicazioni con i server di comando e controllo remoti e si serve della rete P2P Kademlia per inviare e ricevere i comandi qualora si rendessero inutilizzabili i suddetti server. Quella che a detta di molti è la botnet più pericolosa oggi in attività è poi soprattutto una formidabile macchina da soldi capace - scrive l'esperto Kaspersky - di remunerare gli affiliati al programma Tdl con almeno 200 dollari per ogni 1.000 installazioni di malware andate a segno. Grazie a queste credenziali il fenomeno botnet ha travalicato l'ambito ristretto della sicurezza informatica. Esso incarna meglio di qualsiasi altro malware l'evoluzione più rilevante sia dal punto di vista qualitativo che quantitativo dei pericoli della rete, la minaccia combinata definitiva che scaturisce dalla concentrazione in unico punto di gran parte del malware in circolazione: motori di spamming, downloader, rootkit, spyware.

Il nostro Paese non è immune al contagio. Secondo l'ultimo Internet Security Threat Report redatto da Symantec occupiamo la seconda posizione in ambito EMEA e la quarta su scala globale per numero di botnet rilevate. Di fronte alla portata di questa minacce non si esagera - come peraltro spesso accade nel campo della sicurezza - quando si dice che questo fenomeno richiede una risposta efficace e immediata da parte di forze dell'ordine, vendor, e aziende.

DOMANDE

1. Come ci si difende dalle botnet? (patching, blocco JavaScript, sorveglianza porte, education, ecc).

Le botnet sono costituite da device il cui controllo è operato e coordinato da un command & control center. E' possibile quindi intervenire cercando di impedire l'installazione del malware o rilevandone l'attività. Stonesoft offre un ampio ventaglio di soluzioni applicabili allo scopo produce tecnologia pensata per aggiornamenti rapidi e dinamici, come rapida e dinamica è l'evoluzione della minaccia che dobbiamo fronteggiare quotidianamente.

2. Su quale modello di difesa si basano le soluzioni tecnologiche/servizi di cui disponete (detection by cooperative behaviour – detection by signatures – detection by attack behaviour)?

Non esiste un modello di difesa specifico e puntuale per qualsiasi botnet. Stonesoft ritiene che la miglior strategia in proposito consista nell'avere a disposizione strumenti che consentano un presidio puntuale della propria architettura di rete. In particolare le funzionalità di identificare gli indirizzi IP ed i nomi a dominio utilizzati per intermediare la distribuzione di malware o le funzionalità di controllo remoto delle botnet sono integrate nelle capacità di URL filtering che Stonesoft offre sia nei propri engine firewall che nei sistemi di Intrusion Prevention/Detection.

3. Alcuni esperti notano che uno dei problemi con le botnet è la difficoltà di misurare la portata dei danni che potrebbero provocare. Come ci rapportiamo in qualità di Network Security vendor?

La portata dei danni è difficile da calcolare a priori, richiede considerazioni calate sul singolo caso e non è parte del nostro mestiere di vendor. Il nostro mestiere è mettere a disposizione i migliori strumenti per contrastare qualsiasi tipo di minaccia sulla rete.

Forse non tutti sanno che...

....è facile rimanere sempre aggiornati sulle ultime novità tecniche e commerciali di Stonesoft entrando a far parte del nostro Club 2.0:

http://www.facebook.com/StonePartnerIT (prima di cliccare sull'icona, entrate in facebook con il vostro profilo)

http://twitter.com/#!/StonePartner_IT

http://www.linkedin.com/pub/stonepartner-it/2a/42b/37a