BOTNET

«Sei sicuro che il tuo computer ubbidisce solo a te?»

Il termine BOTNET deriva dalla fusione parziale delle parole roBOT e NETwork e si riferisce ad una rete geografica di computer schiavi o zombi alle dipendenze di un computer di comando e controllo detto Server C & C [Command and Control]. Il controllore della botnet prende il nome di botmaster o di botherder. I computer schiavi vengono reclutati mediante infezioni con virus, worm, cavalli di Troia o altri tipi di software maligno e possono essere MAC, PC, tablet e perfino smartphone. Di solito un computer può infettarsi quando l'utente apre un allegato di posta elettronica o quando visita un sito o mediante l'inserimento di una pennetta USB.
Una botnet può essere composta da alcune centinaia fino a milioni di computer, sparsi per il mondo. Esse sono concepite per ottenere un guadagno economico sfruttando la loro intrinseca capacità distruttiva.
Alla loro accensione i computer della botnet si collegano al computer C&C in attesa di comandi. Questa comunicazione è cifrata per assicurarne la riservatezza e contemporaneamente la protezione contro le intercettazioni. Il botmaster alias il botherder, cioè il criminale che controlla l'attività della botnet, può ora dare istruzioni ai computer schiavizzati per utilizzarli come strumento per le sue attività criminose.
I sintomi più comuni di un'infezione da software maligno o malware che si rilevano a carico di un computer sono: la comparsa sul monitor di finestre pop-up pubblicitarie, il cambiamento delle impostazioni che l'utente non può reimpostare nella condizione voluta, l'installazione di software addizionale non richiesto, il rallentamento delle sue funzioni, la disattivazione inaspettata dell'antivirus ed infine i crash frequenti ed imprevedibili.
Il botmaster alcune volte affitta la sua botnet ad altri criminali informatici che la utilizzano per effettuare differenti tipi di cyber-attacchi a partenza dai suoi computer. Tutti questi attacchi possono essere dei tipi sottoelencati:

- Attacchi Distributed Denial of Service (DDoS): tentativi di rendere indisponibili ai loro utenti legittimi le macchine o le reti connesse ad Internet.
- Attacchi a forza bruta: ricerca sistematica ed esaustiva di chiavi o password fino a che non vengono calcolate correttamente.
- Espansione della botnet: installazione di un worm - un software maligno in grado di replicare se stesso ed infettare altri computer.
- Adware e Scareware: tentativi di convincere a comprare un prodotto specifico.
- Conio di monete virtuali: la potenza di calcolo viene utilizzata per creare o estrarre le monete virtuali come i Bitcoin.
- Ransomware: limita o impedisce l'accesso alla macchina che infetta e per rimuovere tali impedimenti chiede un riscatto in denaro.
- Frode in un clic: invio di materiale pubblicitario falso richiamabile con un clic.
- Spam: inoltro per tutto il pianeta di un'enorme quantità di e-mail non richieste e fraudolente.
- Cernita di dati: ricerca di dati personali quali quelli bancari o quelli relativi ai pagamenti, alle credenziali per il login, alle informazioni sensibili, ecc.
- Navigazione anonima: il computer viene utilizzato come network proxy per nascondere sia il vero indirizzo IP che la locazione del server C&C.

Contromisure: nel mese di aprile 2015 è stata smantellata la botnet Simda che aveva schiavizzato 770.000 computer in 190 nazioni e si incrementava, nell'ultimo anno, al ritmo di 128.000 nuovi zombi al mese. In tale operazione sono stati individuati, sequestrati e silenziati 14 server C&C situati in Olanda, negli Stati Uniti, nel Lussemburgo, in Polonia ed in Russia. Hanno collaborato in questa impresa l'Interpol Global Complex for Innovation di Singapore, gli ufficiali della Dutch National High Tech Crime Unit, dell'FBI, della Police Grand-Ducale Section Nouvelles

Technologies del Lussemburgo e del Dipartimento K contro il crimine cibernetico del Ministero degli Interni della Russia assieme a Microsoft, al Kaspersky Lab, a Trend Micro e al Japan's Cyber Defense Institute, per assistenza tecnica.

La botnet Kelihos spediva 3,8 miliardi di e-mail di spam ogni giorno prima di essere smantellata da Microsoft e dal Karspersky Lab. Dato preoccupante, un suo botmaster o collaboratore tecnico sarebbe stato, secondo Microsoft che lo ha citato in giudizio, Andrey N. Sabelnikov, cittadino russo di S. Pietroburgo. Questi in precedenza si era dedicato, come ingegnere informatico e project manager, alla produzione di firewall, di antivirus e di altro software per la sicurezza per conto della Agnitum, società informatica russa. Prima del suo silenziamento Kelihos controllava 41.000 computer ed alcune migliaia di essi ancora oggi incorporano i suoi software maligni.

La botnet Mariposa [farfalla, in spagnolo] è stata smantellata dal governo spagnolo con la collaborazione di Panda Security ed alcune società per la sicurezza IT e la Defense Intelligence. Mariposa tra il 23 dicembre 2009 e il 9 febbraio del 2010 compromise 11.000.000 di IP unici ed era presente in 190 nazioni. È la più grande botnet silenziata fino ad ora, aveva reclutato milioni di computer.

Queste ed altre botnet sono state smantellate, alcune sono pure state infiltrate e studiate dai ricercatori mentre erano attive. Ma diverse altre sono ancora operative e costituiscono una grave minaccia, perciò occorre essere cauti specialmente nella lettura delle e-mail e nella navigazione in Internet. Non sono da trascurare le pennette USB, apparentemente innocenti, che potrebbero essere infette ed una volta immesse nel computer potrebbero iniettargli un worm che lo arruola in una botnet.

Consiglio: essere sempre prudenti e cercare costantemente, per quanto possibile, di evitare le infezioni che potrebbero portare all'arruolamento del proprio computer in una botnet.

Silvio dr Coccaro
Medico – Chirurgo
Ex allievo 1972-73