

Cosa sono e come funzionano le Botnet

Tra le varie minacce informatiche che costellano la rete, le botnet rappresentano di sicuro uno dei principali rischi alla sicurezza. Gruppi di criminali hacker organizzati riescono con queste reti, costituite da computer e dispositivi infettati da appositi malware, ad infiltrarsi in sistemi e infrastrutture telematiche sfruttando ogni vulnerabilità possibile per eludere gli strumenti di rilevamento.

L'obiettivo di una botnet è infatti quello di infettare quanti più dispositivi possibili allo scopo di utilizzare le relative risorse e potenze di calcolo attraverso processi automatizzati e nascosti agli occhi degli ignari utenti che si ritrovano così a usare degli apparati compromessi e facenti parte integrante di una rete di zombie/bot telecomandati.



In questo modo il dispositivo manipolato, contattando un server remoto o altri bot simili, riceve opportune istruzioni da chi presidia (botmaster) l'intera rete per veicolare il download di altri tipi di malware, per reclutare altri bot operanti avviare ulteriori attività congiunte. Così facendo secondo un meccanismo diffuso, persistente e distribuito si arriva a costituire una botnet con milioni di dispositivi adepti.

Botnet: modalità di comando e controllo

Senza dubbio per i criminal hacker, le modalità di comando e controllo rappresentano un'opzione di scelta cruciale per la buona resa della governance della botnet, in considerazione del fatto che alcune di queste modalità risultano più facili da sventare e altre meno. Vediamo le principali.

Il modo più semplice per controllare una botnet è quello di connettere ogni bot a un server remoto. In tal caso una singola sorgente di controllo potrebbe inviare comandi e aggiornamenti con metodi di comunicazione sincroni oppure asincroni:

- **Il metodo asincrono** basato su HTTP prevede una connessione verso un server Web per caricare/eseguire istruzioni a intervalli predefiniti;
- **Il metodo sincrono** basato su IRC (Internet Relay Chat) consiste nell'instaurare un canale persistente (chat) tra i bot e il server IRC per ricevere i comandi in real time.

La centralità di queste configurazioni li rende, però, particolarmente vulnerabili. Infatti per annientare la funzionalità dell'intera botnet basterebbe semplicemente individuare e oscurare il server C2 (HTTP/IRC).

Esistono allora per i criminal hacker diverse alternative:

- **la possibilità di implementare una modalità di comunicazione distribuita peer-to-peer (P2P)**. In questo scenario, in cui un dispositivo zombie può fungere sia da bot e che da server C2, non esiste alcun punto di riferimento da cui i bot ottengono le proprie istruzioni. Quest'ultima configurazione, anche se meno diffusa a causa della complessità realizzativa, risulterebbe meno vulnerabile ad un

eventuale contrattacco. Sarebbe più problematico oscurare tutti i bot per annientare la funzionalità dell'intera botnet;

- **la possibilità di implementare una modalità di comunicazione mista.** Una buona soluzione potrebbe essere quella di adottare una configurazione cercando di cogliere tutti i vantaggi delle modalità di controllo centralizzato/P2P. Ad esempio, creando una botnet P2P per comunicare con i server C2 tramite protocollo HTTP;
- **la possibilità di implementare una modalità di comunicazione utilizzando la rete TOR.** Questa rete, come noto, essendo crittografata e progettata per essere anonima consentirebbe di nascondere le azioni botnet. Fine modulo

Scopo di utilizzo delle Botnet

Le botnet poiché possono consentire l'azione simultanea di centinaia di migliaia di dispositivi potrebbero essere utilizzate dai botmaster:

- **per eseguire attacchi DDoS** (Distributed Denial of Service) su server Web, bersagliando con traffico anomalo un sito Web, allo scopo di sovraccaricare i servizi bloccandone il funzionamento;
- **per lo spamming.** Le botnet risultano essere i principali mezzi impiegati allo scopo;
- **per frodi web.** La simulazione di clic su link pubblicitari o il caricamento in background di siti Web (magari estranei a queste attività), potrebbero essere fonte di profitti fraudolenti, qualora questi siti pagassero in base al numero di click o di visualizzazioni;
- **per minare Bitcoin,** sfruttando la potenza di calcolo dei computer zombie;
- **per distribuire altro malware.** Come visto le infezioni botnet si diffondono attraverso malware/Trojan che,

- individuando le vulnerabilità di sistemi firewall o antivirus obsoleti (o non aggiornati), scaricano altri software malevoli (adware, spyware, ransomware etc.) per una vasta gamma di impieghi illeciti e data breach;
- per noleggiare MaaS e/o ulteriori servizi malevoli a pagamento.

Come difendersi

La migliore strategia di difesa contro questa minaccia in continua evoluzione è quella di proteggere la rete e i potenziali punti di accesso, ovvero gli utenti (che andrebbero adeguatamente indottrinati).

Anche in questo caso gioca un ruolo fondamentale il fattore umano e tutti quegli aspetti legati alle disattenzioni degli utenti nel rispettare delle buone regole di sicurezza.

Entrando nell'ordine delle idee che basta una mail (infetta), il download di un programma (non controllato) o un exploit (che sfrutta falle di sicurezza) per far diventare un apparato (PC, dispositivo mobile, sistema IoT) uno zombie, ecco alcuni consigli di sicurezza minima per gli utenti:

- aggiornare il proprio dispositivo con le ultime versioni di sistema operativo e/o firmware;
- proteggere il proprio dispositivo con applicazioni antivirus e firewall aggiornati;
- scaricare software/app attendibile e verificato ed aggiornarlo periodicamente;
- prestare attenzione ad allegati e link presenti nei messaggi di posta elettronica.

Consigli per le aziende

Di seguito anche alcuni accorgimenti che le aziende potrebbero attuare per ridurre l'esposizione al rischio botnet:

- Utilizzare strumenti per interrompere il flusso di e-mail indesiderate e ad alto rischio di contenere allegati malevoli;
- prevedere strumenti per filtrare i contenuti in uscita dalla rete aziendale, gli accessi e limitare l'esposizione alle minacce, in modo da scongiurare eventuali interazioni tra un malware bot insediatosi e il suo server C2;
- contrastare l'eventuale diffusione laterale dell'infezione, all'interno della rete, tramite l'attuazione di restrizioni sulle relazioni trust dei domini e sugli account locali amministrativi;
- intensificare il rilevamento di attività insolite attraverso un perfezionamento del monitoring della rete e delle connessioni;
- offrire formazioni e aggiornamenti frequenti ai dipendenti sulle regole di supporto alla sicurezza di rete sulle minacce informatiche e le eventuali truffe perpetrate tramite phishing o altre tecniche.

Cosa sono e come funzionano le Botnet