OsservatoriO
AttacchInformatici

Botnet: come nascono, come difendersi

Dallo spam al DDoS, molti attacchi originano da reti di computer infettati a livello mondiale.

M.R.A. Bozzetti, OAI Founder

Attacchi diversi come la saturazione di risorse, lo spamming, il phishing e il furto di dati riservati hanno spesso una comune base: una *botnet*. Con questo termine si fa riferimento a una rete di sistemi compromessi, ovvero che hanno codici maligni sotto il comando e il controllo del sistema dell'attaccante. I sistemi compromessi sono ignari di avere un codice maligno e di essere sotto il controllo di un sistema terzo. Il singolo sistema compromesso facente parte della rete è chiamato bot come semplificazione di robot: la metafora è chiara, il sistema infettato diviene un robot di attacco. Altri termini sinonimi di bot sono zombie e drone: il primo termine non ha bisogno di commenti, il secondo significa in italiano "fuco", il maschio dell'ape, in attesa dell'incontro con l'ape regina per fecondarla. Tutte metafore che indicano un oggetto silente, ben nascosto o non facilmente vedibile, pronto a svolgere il suo ruolo all'occorrenza: nel nostro caso il comando dal sistema dell'attaccante, pc o server che sia. La creazione di una botnet avviene tipicamente con l'infezione di un singolo sistema, che poi propaga l'infezione, in modalità tipicamente virale, ad altri sistemi che interagiscono con lui. Alcune botnet si basano su un solo malware, altre ne supportano diversi, anche contemporaneamente, e sono parti essenziali dei cosiddetti APT, Advanced Persistent Threats (si veda Office Automation, aprile 2011, pagg. 88-89 (1)). L'infezione avviene tramite codici maligni che si installano sul sistema via posta elettronica, oppure con interazioni su siti di social network o su siti malevoli ben mascherati da siti affidabili, come quelli di una banca, di una istituzione o di una azienda famosa. I canali di infezione sono i collegamenti via http, via peer-to-peer, via ICR, Internet Relay Chat, le prime forme di comunicazione

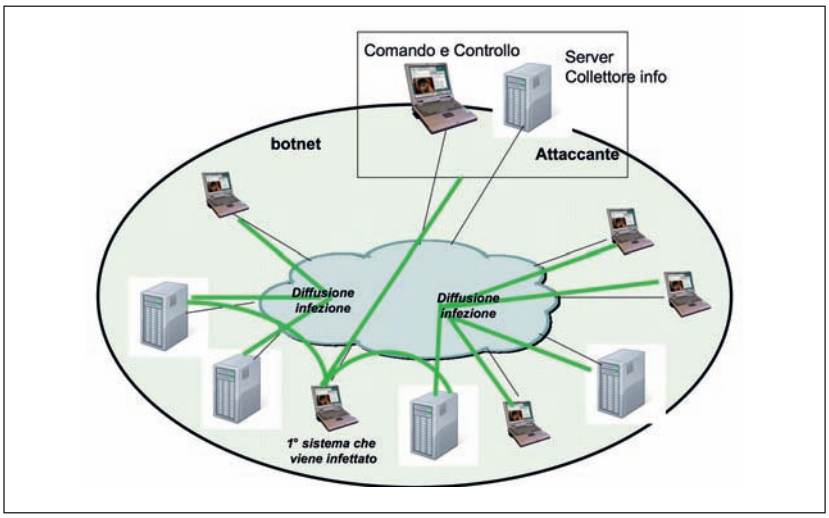
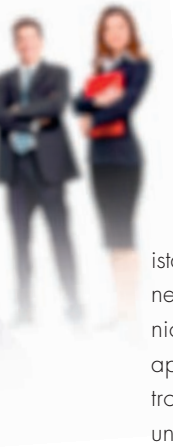


Fig. 1 Schema esplicativo di come viene creata una botnet

(1) Tutti gli articoli della Rubrica OAI su Office Automation sono gratuitamente disponibili sul sito dell'autore www.malaboadvisoring.it.



istantanea in Internet. Le modalità per la creazione di una botnet partono da vulnerabilità presenti sul software o da tecniche di social engineering: basta aprire un allegato della posta elettronica o cliccare su un indirizzo di una sito web proposto in un messaggio o in una social network e il codice maligno è installato. Da questo primo sistema compromesso, normalmente il PC di un utente, la botnet si diffonde sia per l'azione dell'attaccante, sia per una parallela azione di infezione da parte del primo sistema infettato. La replica continua appena si trovano sistemi vulnerabili. Si possono così creare botnet con migliaia o addirittura milioni di sistemi compromessi in tutto il mondo, pronti a svolgere tutti insieme un attacco combinato su uno specifico obiettivo, a seguito del comando dell'attaccante master.

> **La creazione di una botnet avviene tipicamente con l'infezione di un singolo sistema, che poi propaga l'infezione, in modalità tipicamente virale, ad altri sistemi che interagiscono con lui**

Botnet generaliste e mini

Esistono botnet generaliste, con un enorme numero di bot, il cui obiettivo è qualsiasi host vulnerabile in Internet, e tramite le quali sono normalmente effettuati attacchi su larga scala di spamming, phishing, saturazione di risorse (DDoS, si veda più avanti), oltre che di monitoraggio di attività per carpire identità digitali quali password, numeri di carte di credito, credenziali bancarie. Fra i nomi più noti, che derivano spesso dal codice maligno usato: AttackBot, SubSeven, EvilBot, Socket Clone Bots, Torpig, e i più recenti Bredolab (2), Storm (3) e Conficker (4). La nuova generazione di botnet, in linea con il macro-trend degli attacchi ICT, è chiamata mini-botnet e tende a focalizzarsi su obiettivi specifici (host) per effettuare crimini informatici. Il target di una mini-botnet è il sistema informativo di una grande azienda, banca o istituzione pubblica, per rubare specifiche informazioni necessarie per frodi e altri reati. Le modalità operative non cambiano rispetto a una botnet generalista, ma esistono codici maligni specializzati per il tipo di attacco da portare. Esempi diventati famosi includono Mariposa (5), Zeus, SpyEye (6), gli ultimi due simili e focalizzati al furto di credenziali bancarie. Con una mini-botnet l'attaccante sa cosa e come colpire, e personalizza la botnet per l'attacco, facilitato dalla disponibilità di strumenti di sviluppo e gestione delle botnet indicati con l'acronimo DIY.

> **Le modalità per la creazione di una botnet partono da vulnerabilità presenti sul software o da tecniche di social engineering: basta aprire un allegato della posta elettronica o cliccare su un indirizzo di una sito web proposto in un messaggio o in una social network e il codice maligno è installato**

Strumenti DIY

L'acronimo DIY (Do-It-Yourself) indica strumenti software (toolkit) per la creazione di codici maligni per botnet e per la loro gestione. In taluni casi sono sofisticati ambienti di sviluppo e di amministrazione che consentono di creare facilmente nuove versioni di una determinata famiglia di codici maligni e relative botnet. Le nuove versioni di uno o più codici maligni non possono essere subito identificate dagli strumenti anti-malware, pertanto hanno un lasso di tempo per operare indisturbate (zero-day). Questi strumenti permettono facilmente di crittare le comunicazioni tra il sistema di controllo e comando dell'attaccante e i sistemi bot, evitando così il filtraggio preventivo dei sistemi di sicurezza in uso, e di sviluppare codici maligni in grado automaticamente di raccogliere le

(2) Una delle più grandi botnet, di origine russa, con più di trenta milioni di zombie e quarantre command & control server, prevalentemente utilizzata per spamming. È stata smantellata.
(3) Botnet basata sul codice maligno Storm worm diffuso via posta elettronica in ambienti Windows.
(4) Botnet basata sull'omonimo worm per i sistemi operativi Windows. Un worm è simile a un virus, ma non ha bisogno di altri eseguibili per replicarsi.
(5) Botnet di origine spagnola, basata sul codice maligno Butterfly e costituita probabilmente da più di dieci milioni di sistemi compromessi. Smantellata con l'arresto dei cracker che l'avevano creata.
(6) Con questa botnet sono stati attaccati ambienti finanziari in Polonia, con il furto di innumerevoli credenziali bancarie.

credenziali dei clienti di una banca, oppure di rubare certificati digitali o cookies (http e/o Flash). Su Internet sono offerti differenti toolkit DIY per botnet a vari prezzi, anche per il medesimo strumento: un ormai classico DIY è Zeus Toolkit. Alcuni sono disponibili gratuitamente. È evidente che scaricare tali strumenti rappresenta un alto rischio per la sicurezza dei propri sistemi, soprattutto per improvvisati esperti o curiosi del mondo hacker-cracker. Non si può essere sicuri di cosa si acquista, e ci sono alte probabilità che o sia un inganno o, peggio, sia lo strumento di attacco per il supposto venditore.

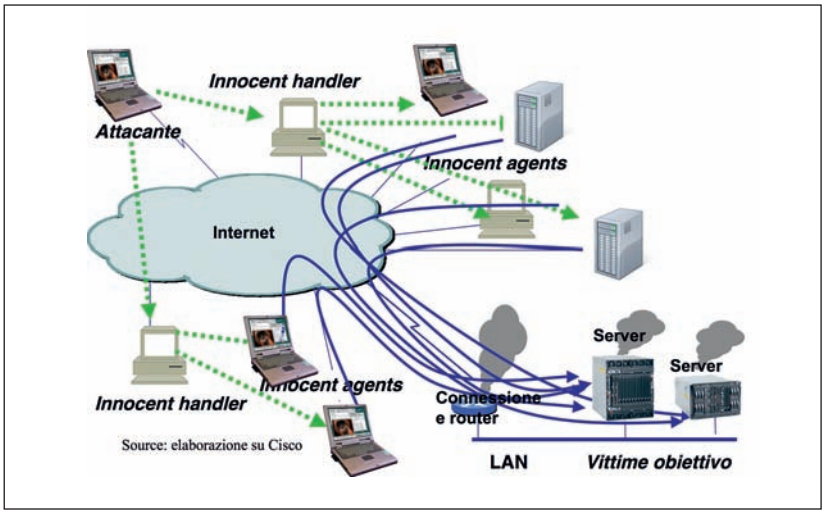


Fig. 2 Schema esplicativo di come avviene un attacco DDoS

DDoS

L'acronimo DDoS (Distributed Denial of Service) indica il tipico attacco per la saturazione di una risorsa ICT, partendo da un ambiente distribuito quale una botnet. L'attaccante prepara una botnet con codici maligni operanti come agenti in attesa di un suo comando o all'occorrenza di un evento prestabilito, ad esempio una data. A tale occorrenza, tutti gli zombie contemporaneamente iniziano una predeterminata azione sulla risorsa obiettivo. Se è un sito web la richiesta di una pagina, se è un banca dati una certa interrogazione, se è un file server la richiesta o l'invio di un file, e così via. In questo modo le azioni contemporanee mandano in saturazione la risorsa obiettivo e le sue connessioni con Internet.
Un attacco DDoS non modifica, copia o cancella dati o programmi, tanto meno l'hardware, ma rende satura e quindi non più utilizzabile per tutto il periodo dell'attacco la risorsa obiettivo. Non porta danni al patrimonio informativo, ma alla disponibilità dei servizi ICT forniti dalle risorse obiettivo: gli utenti di un sito, ad esempio di una banca, non possono quindi accedere ed effettuare transazioni tipiche dell'home o del corporate banking, quali l'analisi dei movimenti, pagamenti, bonifici, e così via. Con un DDoS può pertanto venir compromesso il business e le attività dell'azienda o dell'ente attaccato.

Come proteggersi

Proteggersi da un DDoS non è facile. Richiede il coinvolgimento del fornitore delle connessioni e, in Italia, della Polizia delle Comunicazioni per far bloccare il/i server di comando e controllo. Per prevenire l'inserimento di proprie risorse ICT in una botnet, ecco alcune le raccomandazioni:

- lato utente: è essenziale il sistematico aggiornamento del sistema operativo, dell'anti malware, delle patch dei programmi, oltre a un uso prudente di Internet: non aprire messaggi di e-mail da fonte sconosciuta, non scaricare file da host non affidabili, non cliccare su indirizzi di pubblicità, e così via;
- lato amministratore dei sistemi: è essenziale la corretta gestione e il puntuale aggiornamento del software e degli account utenti, incluse le password che dovrebbero essere crittate (così come le informazioni critiche). Tutti gli strumenti di prevenzione, dai sistemi IDS/IPS ai firewall, devono essere attivi, aggiornati e ben configurati. Per quanto riguarda specificatamente le botnet, è bene verificare e aggiornare le blacklist degli indirizzi dei server di comando e controllo scoperti: un significativo esempio è fornito da Zesus Tracker al sito https://zeustracker.abuse.ch/index.php.