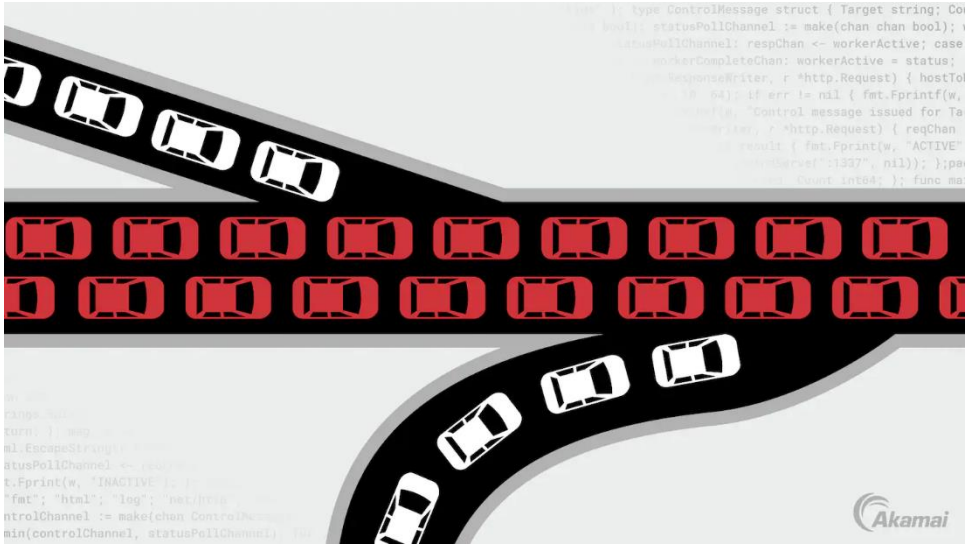
ATTACCO DDOS

Un DDoS, o Distributed Denial-of-Service, è un tipo di attacco informatico che tenta di rendere non disponibile un sito web o una risorsa di rete sovraccaricandoli con traffico dannoso e rendendoli, così, inutilizzabili.

In un attacco DDoS (Distributed Denial-of-Service), un criminale sovraccarica la sua vittima con traffico Internet indesiderato, impedendo al traffico normale di giungere alla destinazione prevista.

Ad un livello elevato, un attacco DDoS o DoS è come un ingorgo del traffico causato da centinaia di richieste fittizie ai servizi di "car sharing". Le richieste sembrano legittime ai servizi di "car-sharing", che mandano i loro conducenti per prelevare i clienti, bloccando inevitabilmente le strade cittadine e impedendo, in tal modo, al traffico legittimo di arrivare a destinazione.

Un attacco DDoS o DoS è come un ingorgo del traffico



Durante un attacco DDoS, i malintenzionati sfruttano una grande quantità di macchine e dispositivi connessi su Internet, come dispositivi IoT (Internet of Things), smartphone, personal computer e server di rete, per inviare un afflusso di traffico verso le varie destinazioni.

Un attacco DDoS al sito web di un'azienda, a un'applicazione web, alle API, a una rete o all'infrastruttura di un data center può causare downtime e impedire agli utenti legittimi di acquistare prodotti, fruire di un servizio, ottenere informazioni o qualsiasi altra cosa.

Gli attacchi DdoS sfruttano reti di dispositivi connessi a internet per negare agli utenti l'accesso a un server o a una risorsa di rete ad esempio un sito web o un'applicazione che adoperano spesso.

1. Per sferrare un attacco DDoS, i malintenzionati utilizzano dei malware o sfruttano le vulnerabilità della sicurezza per infettare in maniera dannosa macchine e dispositivi e assumerne il controllo. Ogni computer o dispositivo infettato, detto "bot" o "zombie", diventa così in grado di diffondere ulteriormente il malware, oltre che di prendere parte ad attacchi DDoS. Questi bot si accumulano formando eserciti interi, detti "botnet", che, facendo leva sulla potenza della propria numerosità, amplificano la portata degli attacchi. E, poiché non si accorgono che i dispositivi IoT sono infetti, proprio come capita quando si scarica il filmetto di turno sugli zombie senza sapere che è infetto, i proprietari dei dispositivi legittimi diventano vittime secondarie o partecipanti inconsapevoli degli attacchi, mentre le organizzazioni colpite hanno difficoltà a identificare i malintenzionati.

2. Dopo aver creato una botnet, un malintenzionato può inviare istruzioni a ogni bot da remoto, indirizzando un attacco DDoS verso il sistema preso di mira. Quando una botnet attacca una rete o un server, il malintenzionato ordina ai singoli bot di inviare richieste all'indirizzo IP della vittima. Proprio come noi umani abbiamo impronte digitali univoche, così i nostri dispositivi hanno un indirizzo univoco che li identifica su Internet o su una rete locale. Il sovraccarico di traffico è il rifiuto di un servizio, che impedisce, così, al traffico normale di accedere a siti o applicazioni web, API o reti.

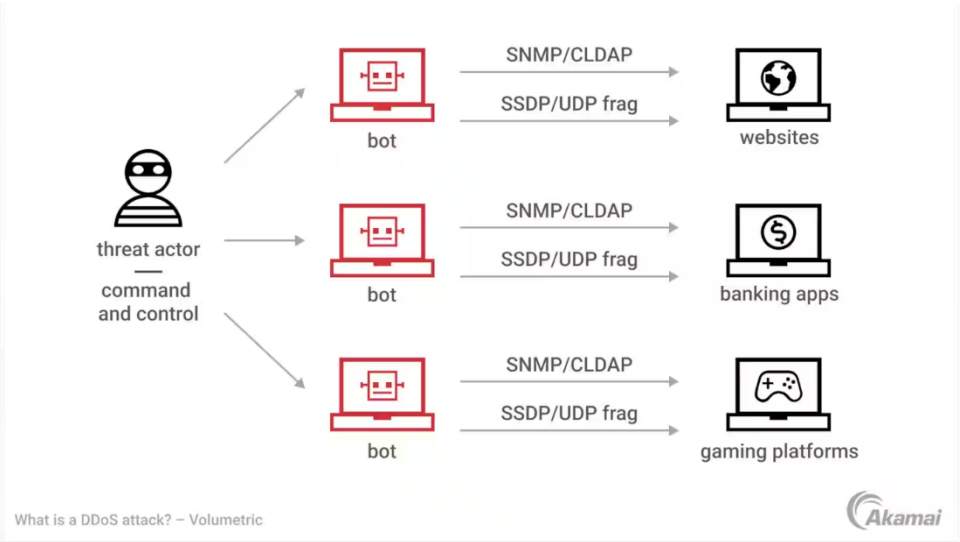
A volte le botnet, con le loro reti di dispositivi compromessi, vengono affittate per sferrare altri potenziali attacchi tramite servizi di hacking "su commissione". Ciò consente alle persone malintenzionate, ma prive di formazione o esperienza in merito, di sferrare facilmente attacchi DDoS anche da soli

Tipi di attacchi DDoS

Esistono molti tipi diversi di attacchi DDoS e i malintenzionati spesso ne utilizzano vari quando creano scompiglio negli ambienti colpiti. I tre tipi principali sono attacchi volumetrici, attacchi di protocolli e attacchi a livello di applicazione. Lo scopo di tutti gli attacchi è rallentare gravemente o impedire del tutto al traffico legittimo di raggiungere la sua destinazione. Degli esempi potrebbero essere il fatto di negare a un utente di accedere a un sito web, acquistare un prodotto o servizio, guardare un video o interagire sui social media. Inoltre, non rendendo più disponibili le risorse o riducendone le performance, un attacco DDoS può causare l'arresto completo di un'azienda. Ne conseguirebbe l'impossibilità dei dipendenti di accedere alle e-mail o ad applicazioni web o, semplicemente, di lavorare come al solito.

Per meglio comprendere il funzionamento di un attacco DDoS, analizziamo le varie strade che possono intraprendere i malintenzionati. Il modello di interconnessione a sistema aperto (OSI) è un modello multilivello per vari standard di rete e contiene sette livelli diversi. Ogni livello del modello OSI ha uno scopo univoco, come i piani di un edificio in cui ogni ufficio svolge la propria funzione

individuale. I malintenzionati prendono di mira i vari livelli, a seconda del tipo di risorsa web o su Internet che desiderano intralciare.



Che cos'è un attacco DDoS volumetrico?

L'intento di un attacco DDoS volumetrico è quello di sopraffare una rete con enormi quantità di traffico, congestionando la larghezza di banda della risorsa della vittima prescelta. Le grandi quantità di traffico di attacco impediscono agli utenti legittimi di accedere a un'applicazione o servizio, arrestando, al contempo, il flusso in entrata o in uscita del traffico. A seconda di quale sia la vittima di un attacco, l'arresto del traffico legittimo può significare ad esempio che il cliente di una banca non ha modo di pagare una bolletta per tempo, i clienti di un e-commerce non possono completare le transazioni online, la cartella clinica del paziente di un ospedale può essere esclusa o un cittadino può non riuscire più a visualizzare le tasse pagate a un ente governativo. A prescindere dall'organizzazione vittima, impedire alle persone di utilizzare un servizio online che si aspettano funzioni ha un impatto negativo.

Gli attacchi volumetrici utilizzano botnet create a partire da eserciti di singoli sistemi e dispositivi infettati da malware. Controllati da un malintenzionato, i bot vengono utilizzati per congestionare una vittima precisa e Internet in generale con del traffico dannoso che occupa tutta la larghezza di banda disponibile.

Una quantità imprevista di traffico di bot può ridurre notevolmente o impedire l'accesso a una risorsa web o servizio su Internet. Poiché i bot assumono il controllo di dispositivi legittimi per amplificare gli attacchi DDoS che fanno un uso intensivo della larghezza di banda, spesso a insaputa degli utenti, il traffico dannoso è difficile da individuare da parte dell'organizzazione vittima.

Esistono vari tipi di vettori di attacchi DDoS volumetrici utilizzati dai criminali. Molti sfruttano tecniche di attacchi di riflessione e amplificazione per sopraffare una rete o un servizio preso di mira.