Cyber Guerrieri: *Alla Scoperta degli Strumenti DDoS*

Storia del DDoS

Cos'è un attacco DDoS?

Un attacco DDoS (Distributed Denial-of-Service) è una tipologia di attacco informatico che si caratterizza per il sovraccarico intenzionale di un sito web, server o risorsa di rete con traffico malevolo. Questo provoca un blocco o un malfunzionamento del sistema bersagliato, impedendo agli utenti legittimi di accedere al servizio e bloccando il traffico normale. A un livello generale, un attacco DDoS o DoS può essere paragonato a un ingorgo stradale creato da centinaia di richieste false ai servizi di "car sharing". Queste richieste appaiono legittime ai servizi di "car sharing", che inviano i loro autisti per prelevare i clienti, bloccando le strade e impedendo al traffico autentico di raggiungere la destinazione.

Il primo attacco

Alcune testimonianze indicano che la prima dimostrazione di un attacco DoS fu eseguita da Khan C. Smith nel 1997 durante un evento DEF CON, interrompendo l'accesso a Internet sulla Las Vegas Strip per oltre un'ora. Tuttavia, sembra che il primo vero attacco si sia verificato qualche anno dopo, il 22 luglio 1999. In quel giorno, un computer dell'Università del Minnesota fu sommerso da pacchetti di dati inutili inviati da 114 computer compromessi, restando offline per due giorni. Secondo la MIT Technology Review, si trattò del primo attacco DDoS documentato. Nelle settimane e nei mesi successivi, quando vennero interrotte le connessioni di importanti aziende come CNN o Amazon, i cybercriminali si resero conto della semplicità di sferrare questi tipi di attacchi, che richiedevano solo poche righe di codice. All'inizio del 2000, più precisamente il 7 febbraio, lo studente liceale canadese Michael Calce, alias MafiaBoy, all'età di soli 14 anni, riuscì a mettere in ginocchio Yahoo! con il più grande attacco DDoS della storia, bloccando completamente uno dei principali siti web dell'epoca. Nella settimana successiva, il giovane canadese prese di mira e riuscì a bloccare altri siti come Amazon, CNN ed eBay. La tecnica usata da Mafiaboy consisteva nell'inviare un enorme quantitativo di pacchetti all'host bersaglio,

fino a rallentare notevolmente o addirittura bloccare il caricamento delle pagine web. La novità e il punto di forza degli attacchi di Mafiaboy era l'uso di molti computer detti zombie, precedentemente hackerati e sui quali il quattordicenne aveva il totale controllo. Questi zombie, sparsi su tutto il territorio americano, venivano usati per sferrare l'attacco contemporaneamente. Gli zombie preferiti di Mafiaboy erano computer universitari, aventi una banda internet molto più elevata della media, rendendo l'attacco più potente.

Evoluzione degli attacchi

Nonostante oggi richiedano un volume di traffico superiore rispetto a qualche anno fa, gli attacchi DDoS rimangono una minaccia concreta. Secondo i report di Kaspersky Labs, il numero complessivo di questo tipo di attacco è aumentato del 32% ogni anno. Un altro trend allarmante è rappresentato dalla disponibilità di piattaforme di lancio per attacchi DDoS come 0x-booter. In gergo tecnico, si parla di "DDos-as-a-service", ovvero attacchi DDoS su richiesta (o chiavi in mano), in grado di attivare circa 16.000 dispositivi IoT infettati dal malware Bushido. Questo evidenzia come la servitizzazione del cyber crimine sia ormai un fenomeno affermato. Come accennato in precedenza, è sempre più comune che gli attacchi vengano lanciati da botnet di terze parti, pagate per questo preciso scopo, e il trend sembra destinato a crescere.

UFONet

Ufonet è un toolkit gratuito P2P e criptografico che permette di eseguire attacchi DoS e DDoS, sfrutta dei vettori di Open Redirect, ovvero la possibilità di ridirigere una chiamata verso un altro URL. Un attaccante può sfruttare delle vulnerabilità di una macchina per installarvi software RAT permettendogli di controllarla da remoto. A queto punto si parla di macchina "zombie", ovvero una macchina pronta ad attaccare. Un insieme di questi "zombie costituisce una botnet capace di effettuare vari tipi di attacchi come il DDoS.

Pro:

- Ufonet ha una buona capacità di nascondere le proprie tracce
- Offre vari tool per trovare vittime da infettare
- È un P2P/darkent che gli permette di connettersi con altre macchine per eseguire complessi schemi d'attacco potendo, ad esempio, condividere i propri "zombie";
- È gratuito e opensource

Contro:

L'unico "svantaggio" è che la sua efficacia dipende dalla quantità e qualità delle macchine infettate.

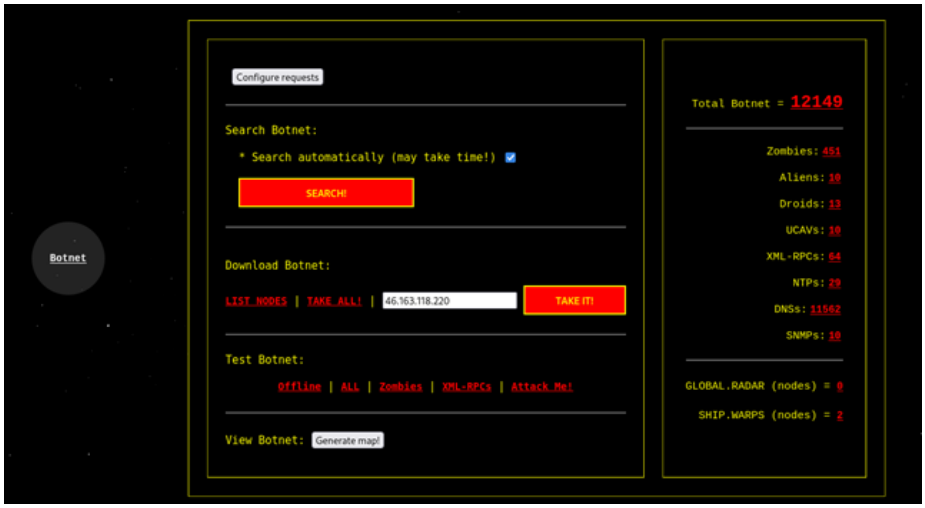

Figure 1: Esempio di attacco DDoS da LOIC

LOIC

LOIC, acronimo di "Low Orbit Ion Cannon", è uno strumento di attacco di tipo denial-of-service (DoS) o distributed denial-of-service (DDoS). È un software open source originariamente creato per testare la sicurezza delle reti, ma è diventato noto per il suo utilizzo da parte di gruppi di hacktivisti come Anonymous per condurre attacchi contro vari siti web e servizi online. Quando utilizzato da numerose persone contemporaneamente, effettua un attacco di tipo distributed denial-of-service (DDoS) contro un IP vittima inondando il server con pacchetti TCP, UDP o richieste HTTP, nell'intento di interrompere il servizio di un particolare host. Il funzionamento di LOIC, quindi, si basa sul contributo di volontari che, coordinandosi tra loro con altri sistemi (ad esempio: chat, forum, ecc), possono emulare una botnet. LOIC è noto per la sua interfaccia semplice, che consente anche agli utenti meno esperti di eseguire attacchi DDoS. Gli utenti possono inserire un URL o un indirizzo IP e avviare un attacco con pochi clic. Sebbene non offra meccanismi di anonimato intrinsechi, viene spesso utilizzato insieme a strumenti di anonimato come VPN o Tor per nascondere l'identità dell'attaccante.

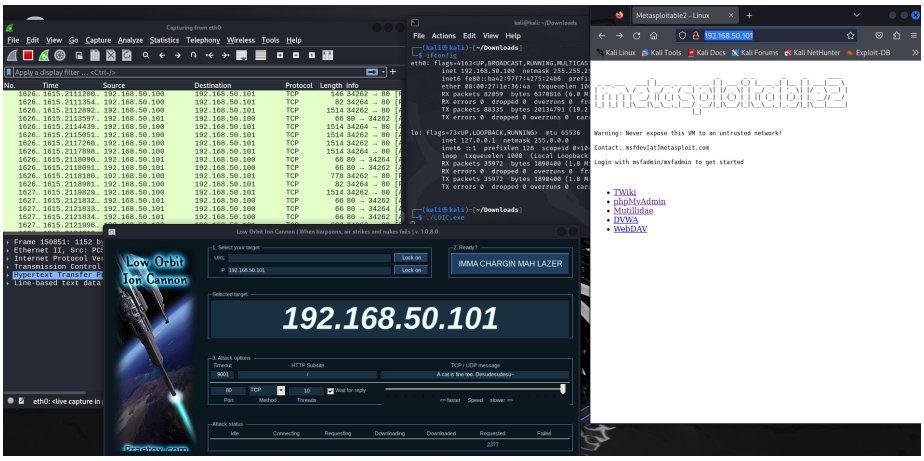

Figure 2: Esempio di attacco DDoS da LOIC

Pro:

- Facilità d'Uso
- Open Source
- Ampia Disponibilità
- Versatilità
- Uso per Test di Stress

Contro:

- Tracciabilità
- Efficacia Limitata contro Protezioni Moderne
- Legalità e Rischi
- Consumo di Risorse
- Mancanza di Anonimato Integrato

HOIC

HOIC è una piattaforma open-source progettata per valutare la resistenza delle reti e per eseguire attacchi di tipo DoS, capaci di colpire simultaneamente fino a 256 URL. È stato creato per sostituire il Low Orbit Ion Cannon (LOIC). HOIC è utilizzato per lanciare attacchi di tipo DoS e DDoS, coordinati da diversi individui. L'attacco consiste nell'inondare un URL con traffico eccessivo

al fine di renderlo inaccessibile. La sua interfaccia grafica semplice facilita il controllo e l'avvio degli attacchi mediante l'uso di "booster file", che consentono la personalizzazione degli attributi delle richieste. I "booster file" sono moduli configurabili che randomizzano gli header HTTP dei computer che partecipano all'attacco.

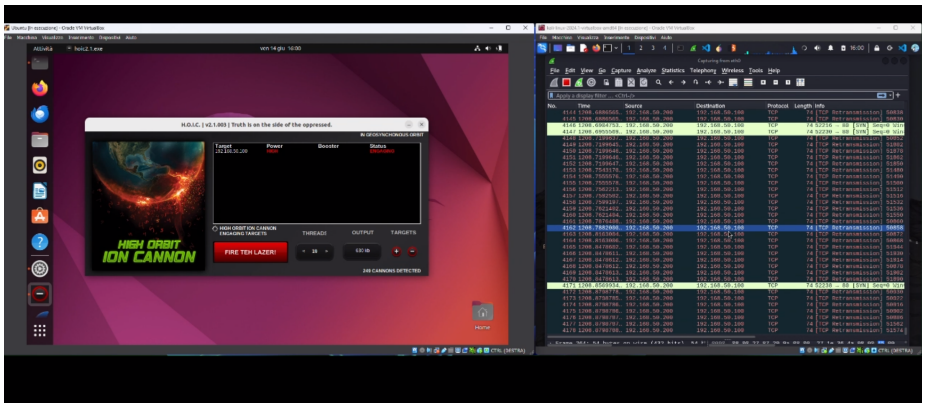

Figure 3: Esempio di attacco DDoS da LOIC

Contro:

Le principali limitazioni di HOIC sono che richiede un gruppo di utenti coordinati per essere efficace, con almeno 50 utenti necessari per lanciare un attacco e un numero maggiore per mantenerlo nel tempo se il sito target è protetto. Inoltre, manca di capacità sufficienti di anonimizzazione e randomizzazione per proteggere gli attaccanti.

L'evoluzione dei sistemi informatici ha portato a comportamenti illeciti online, spingendo il legislatore a introdurre norme specifiche nel diritto penale informatico. Tra questi comportamenti, gli attacchi Denial of Service (DoS e DDoS) sono particolarmente rilevanti e sono regolati da specifici articoli del Codice Penale italiano.

Articoli relativi agli attacchi DoS e DDoS

Art. 635-quater

In Italia l'articolo 635-quater del Codice Penale punisce chiunque danneggi o distrugga dati con il fine di rendere inservibili i sistemi informatici o telematici, o di ostacolarne il normale funzionamento. Le pene previste variano da 1 a 5 anni di reclusione. Questo articolo è particolarmente applicabile in caso di attacchi Denial of Service (DoS e DDoS), che mirano a interrompere o bloccare il funzionamento dei servizi online.

In America invece secondo il Federal Computer Fraud and Abuse Act, un attacco DDoS non autorizzato può portare fino a 10 anni di reclusione e una multa di 500.000$. Anche solamente cospirare a per fare ciò può portare a 5 anni di prigione e una multa di 250.000$.

Esempi di tali attacchi includono:

- Sovraccarico di un server con traffico eccessivo.
- Utilizzo di botnet per eseguire attacchi distribuiti (DDoS).
- Exploit di vulnerabilità nei sistemi per causare interruzioni.

Giurisdizione

Se un attacco DDoS viene eseguito dall'Italia verso un obiettivo situato negli Stati Uniti, le questioni legali e la giurisdizione dipenderanno da diversi fattori:

1. **Leggi Nazionali**: In primo luogo, le leggi italiane regoleranno l'azione compiuta dall'attaccante situato in Italia. In Italia, gli attacchi informatici, inclusi i DDoS, sono regolati dal Codice Penale italiano e da altre normative locali.
2. **Leggi degli Stati Uniti**: Gli Stati Uniti hanno normative specifiche che regolano gli attacchi informatici, inclusi i DDoS. Il Federal Computer Fraud and Abuse Act (CFAA) è una delle leggi principali che disciplina questi crimini negli Stati Uniti.
3. **Esigenze di Estradizione**: Se l'attaccante in Italia viene identificato e processato, potrebbe essere oggetto di richiesta di estradizione da parte degli Stati Uniti, soprattutto se ci sono accordi bilaterali tra i due paesi in materia di criminalità informatica.
4. **Giurisdizione Internazionale**: In casi di crimini informatici transnazionali come un attacco DDoS dall'Italia agli Stati Uniti, potrebbe essere coinvolta la cooperazione internazionale tra le forze dell'ordine e i tribunali di entrambi i paesi per determinare la giurisdizione primaria e coordinare le indagini e le azioni legali.

In generale, la giurisdizione principale dipenderà da dove avviene l'azione criminosa (l'attacco informatico) e le leggi del paese in cui si trova l'attaccante. Tuttavia, nel caso di crimini informatici transnazionali, possono emergere complessità aggiuntive dovute alla natura globale e interconnessa della rete Internet.

DDoS Etico?

L'unica ragione etica per un attacco DoS sarebbe quella che permette di aumentare la sicurezza della propria rete. Questo può essere fatto assumendo qualcuno per penetrare nel proprio sistema o per attaccarlo con un DoS.