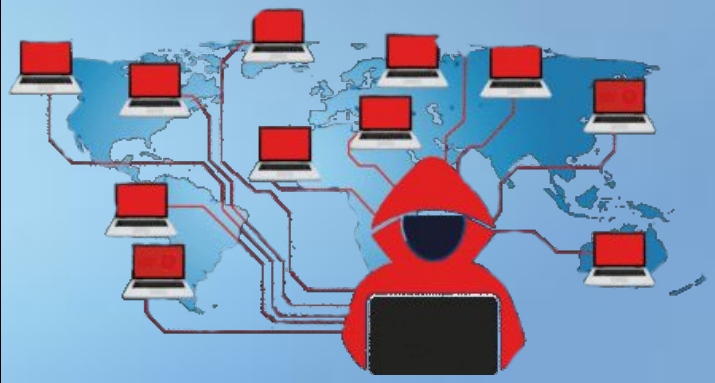
ATTACCHI DOS DISTRIBUITI

Negli attacchi DoS distribuiti il bersaglio viene attaccato contemporaneamente da più parti, rendendo l'identificazione della fonte originaria dell'attacco molto più complessa.

1. Nella prima fase, l'attaccante, spesso tramite l'uso di malware, infetta un numero elevato di computer, detti **zombies**.

2. I computer infettati formano una **botnet**. L'attaccante, che ne ha completa disposizione, al momento opportuno lascia partire l'attacco.



SINTOMI DI UN ATTACCO DOS

Alcuni sintomi di un attacco DoS possono essere:

- Improvviso peggioramento delle prestazioni di rete
- indisponibilità di un determinato sito web
- Impossibilità di accedere al Web o servizi Internet
- Mail bomb: aumento del numero di e-mail di spam ricevute

COME DIFENDERSI

- **Prevenzione**

Filtrare i dati in arrivo può essere di grande aiuto. Si possono utilizzare **firewall** o sistemi di **intrusion detection** and **prevention**.

Utilizzare captcha o semplici puzzle logici per evitare attacchi da bots verso servizi web

- **Durante e dopo un attacco**

Tracciare e filtrare i pacchetti contenenti informazioni sulla provenienza dei dati alterata (Compito dell' Internet Service Provider)

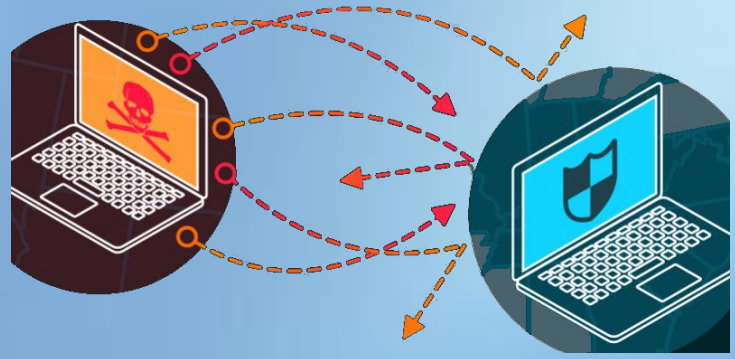
Avere sempre un piano di emergenza: essere pronti a spostarsi su server alternativi.

Gli attacchi DoS, purtroppo, non sono completamente evitabili!

RIFERIMENTI

➢ https://www.c3t.it/projects/awareness/articoli&brochure/dos/

POR FESR 2014-2020 obiettivo Crescita e Occupazione (CreO)



GLI ATTACCHI DENIAL OF SERVICE

Scopri cosa sono gli attacchi denial of service e come difenderti

Gli attacchi denial of service (letteralmente in italiano **negazione del servizio** abbreviato in **DoS**) sono azioni che impediscono il regolare accesso al servizio da parte di utenti autorizzati. L'attaccante prova ad ottenere questo obiettivo **esaurendo le risorse del sistema** (ampiezza di banda, CPU, memoria, spazio sul disco). Se l'attacco ha successo, il sistema non sarà più in grado di funzionare normalmente e sarà costretto a scartare anche richieste legittime.
Di solito gli attacchi DoS possono essere sfruttati per richiedere un riscatto, come preludio di un altro attacco (magari bloccando un servizio di difesa o addirittura il servizio stesso per sostituirlo con uno falso), come atti vandalici o come una forma di protesta (Hacktivism).

Gli attacchi DoS possono essere divisi in diverse categorie in base al tipo di risorse attaccate

1. Attacco alle risorse di rete, di solito l'ampiezza di banda : si prova ad esaurire la connessione all' ISP (Internet Service Provider)

2. Attacco alle risorse del sistema: l'attacco è diretto al software che gestisce l'interazione con la rete. Invece di esaurire la banda con un enorme quantità di traffico dati, si inviano specifici pacchetti per esaurire una risorsa specifica (SYN flooding attack)

Due esempi di attacchi DoS molto conosciuti sono l'attacco SYN-Flooding e l'attacco Http flood

Attacco SYN-Flooding

L'attacco Syn Flooding ("inondazione di pacchetti di tipo Syn") si basa sul protocollo TCP che regola l'inizio di una connessione.

Il protocollo impone che il sistema memorizzi in una tabella tutte le comunicazioni pendenti. L'attaccante inizierà un numero elevato di comunicazioni senza mai mandare il segnale finale di acknowledgment necessario per concludere la comunicazione. Quando la tabella sarà piena, il server sarà costretto a rigettare le successive richieste

Attacco Http flood

L'attacco HTTP Flood si basa su una vera e propria inondazione del web server target con richieste lecite: lo scopo dei criminal hacker è, ovviamente, quello di mantenerlo in una situazione di saturazione/crash per aver superato i limiti massimi di richieste consentiti. Questo tipo di attacco è particolarmente insidioso perché è molto difficile distinguere un attacco da richieste legittime.