DDoS - Distributed Denial of Service

di Alessandro Demontis - Luglio 2021 (*)

La sigla **DDoS** sta per *Distributed Denial of Service*, ed indica un attacco di tipo **DoS** (*Denial of Service*) portato avanti su larga scala da molteplici sorgenti. Un Denial of Service é un attacco che ha lo scopo di saturare una o più porte in ascolto di un server, causando in genere la indisponibilità del servizio relativo da parte del server.

Ad ogni porta (o gruppo di porte) aperta in una connessione client/server corrisponde un servizio, ad esempio la porta 80 corrisponde al servizio web HTTP, la porta 21 al servizio FTP, la porta 53 al servizio DNE e così via; saturando di connessioni una porta, se il server non ha banda sufficiente per gestirle o non ha un piano di elisione delle connessioni multiple, é possibile mandare in overload quel dato servizio, ottenendo così un 'denial', cioè il servizio viene negato a chi lo va a richiedere lecitamente.

Cosa significa questo? Prendiamo il caso più facile, un attacco DDoS al servizio web HTTP, porta 80.

E' la porta alla quale si collegano tutti i computer quando visitano un sito web, cioè quando visitiamo un sito internet possiamo farlo grazie al fatto che quel sito é ospitato (hostato, in gergo tecnico) su un server il quale ha la porta 80 aperta per accettare richieste di connessione e, ricevutele, dispaccia tramite questo servizio le sue pagine web. Ora, se un attacco satura la porta 80, il server potrebbe non essere capace di fornire ad ulteriori visitatori che navigassero lecitamente le pagine web, ed il sito risulterebbe 'down' (offline).

C' é un altro fattore molto importante da tenere presente: anche se non si riesce a negare del tutto il servizio, attacchi lunghi, ripetuti ed articolati multi-porta (cioè rivolti a più porte del server) possono causare la saturazione della banda, specialmente in quei server che gestiscono tante attività dividendo tra loro la banda disponibile (load balancing).

Questo risulterà in:

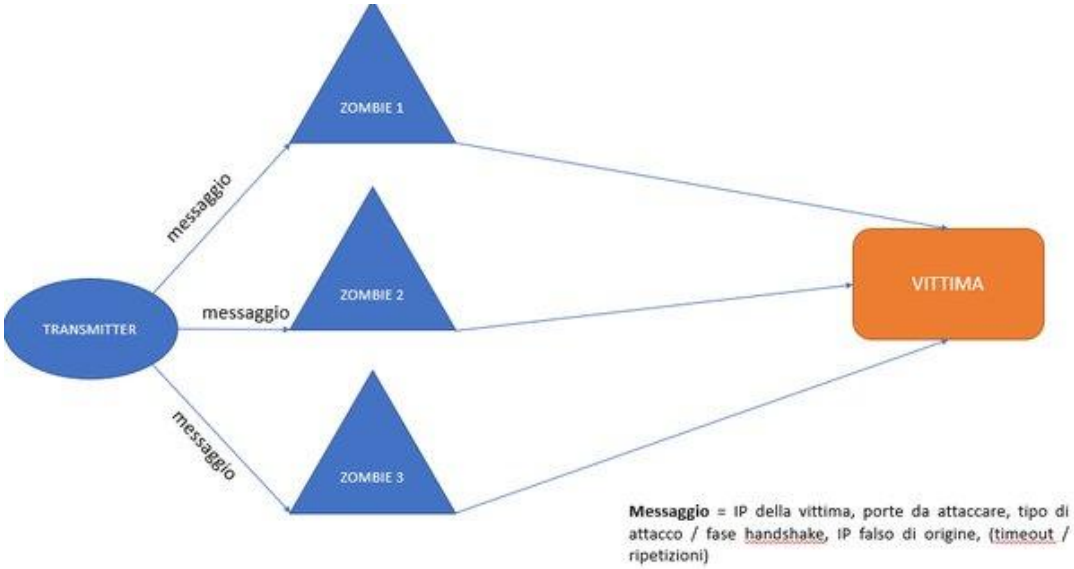
- navigazione lenta degli utenti;
- lentezza interna tra i servizi del server che comunicano tra di loro;
- eccessivo utilizzo di CPU e memoria per far fronte alla massiccia mole di attacchi e dei log conseguenti;

In molti casi, davanti ad attacchi del genere, l' unica soluzione é spegnere il server, cioè portarlo 'offline' isolandolo da Internet.

Ma come é costituito un attacco DDoS?

In genere si tratta di script *'trasmittori'* che sfruttano la presenza di '*Zombie*', cioè computer sparsi qui e li nella rete globale ed infettati con un '*ricettore - trasmettitore*'. Tali gruppi di zombie sono in genere

chiamati ‘*Botnet*’ ed ogni zombie della botnet é chimato ‘*Bot*’ (da ‘Robot’). Lo schema di massima di un DDoS é questo:

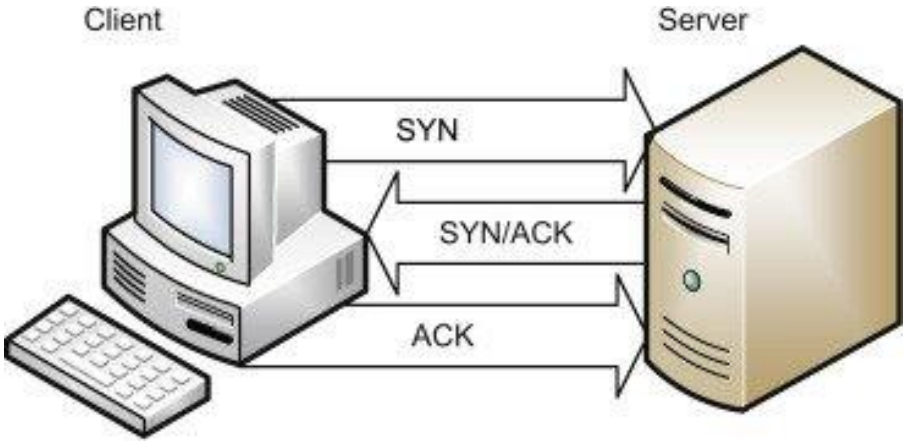


La sorgente, che poi é in genere il PC dal quale l' hacker attacca, si connette ad una lista nota di 'zombie' che può essere costituita da PC infettati appositamente o PC che hanno dei disservizi di configurazione i quali permettono ad utenti esterni di collegarsi e sfruttarli come ripetitori. Queste liste, che girano su Internet e vengono costantemente aggiornate dagli hacker, si chiamano '**cast list**' o '*liste di Broadcast*'.

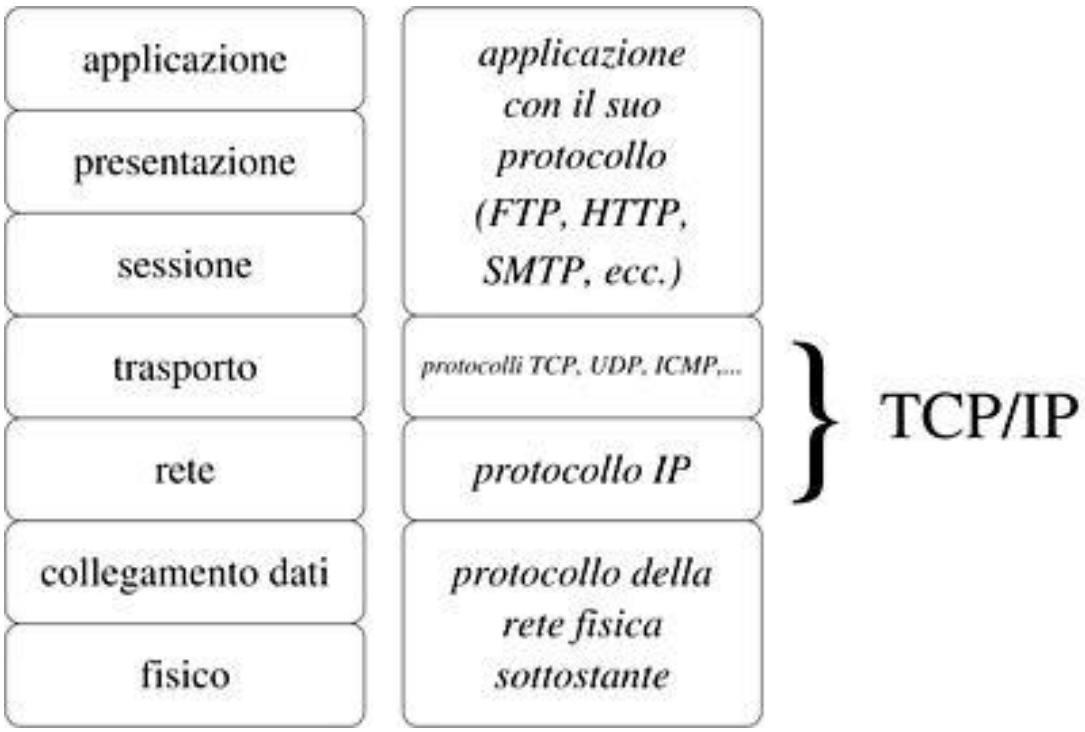
Una volta connessa agli zombie, la sorgente trasmette il messaggio di attacco, che contiene diversi parametri. Gli zombie ricevono il messaggio di attacco, e lo scompongono creando una serie di **pacchetti forgiati** artificialmente sfruttando le informazioni contenute nel messaggio. Iniziano così ad attaccare l' IP della vittima alle porte specificate nel messaggio, con il tipo di protocollo o sfruttando la **fase di handshake** specificata, facendo risultare però alla vittima che le connessioni non vengano da loro, ma da un **IP Spoofed**, anche esso forgiato.

Cosa é una *fase di handshake*? Il protocollo internet per le connessioni standard é il TCP, protocollo che prevede una 'handshake', ossia una ‘stretta di mano virtuale’ tra servers. Tale stretta di mano passa attraverso alcune fasi, una sorta di '*botta e risposta*' tra pacchetti di dati. Queste fasi sono tre:

- **SYN** sta per *synchronize*: il PC sorgente chiede al PC destinazione di sincronizzarsi con lui;
- **SYN-ACK** sta per *synchronize-acknowledge*: il PC destinazione si sincronizza (**syn**chronize) e richiede al PC sorgente di attestare (**ack**nowledge) la sua sincronizzazione preparandosi a scambiare i dati;
- **ACK** sta per *acknowledge*: il PC sorgente attesta (**ack**nowledge) la sincronizzazione e predisposizione del PC target a scambiare dati.

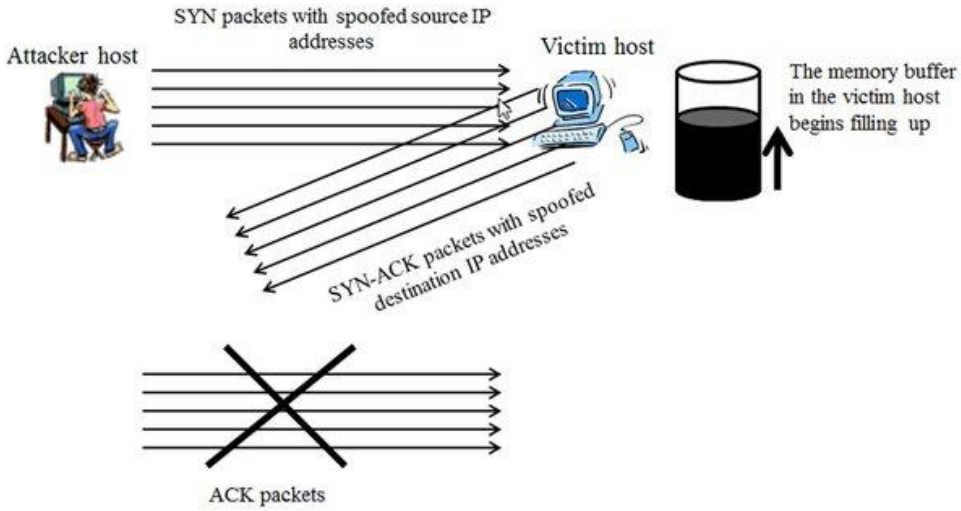


Benissimo, esistono diversi tipi di attacchi DDoS, i principali e più efficienti sono gli Handshake Flood (appartenenti al gruppo degli attacchi chiamati "*Attacchi sul Livello 4 o del Trasporto*") ed i Service Flood (appartenenti al gruppo di attacchi chiamati chiamati "*Attacchi sul Livello 7 o dell' Applicazione*"), e specificatamente i SYN FLOOD e gli HTTP FLOOD. Questi attacchi sfruttano diversi livelli del **Modello OSI** (Open System Interconnection), il modello di comunicazione tra PC in rete:



SYN FLOOD

Il SYN Flood agisce sul livello 4 del modello OSI, chiamato "*Livello del Trasporto*" perchè é il livello a cui avviene il trasporto dei dati tra client e server. E' un attacco che sfrutta l' Handshake del protocollo TCP.

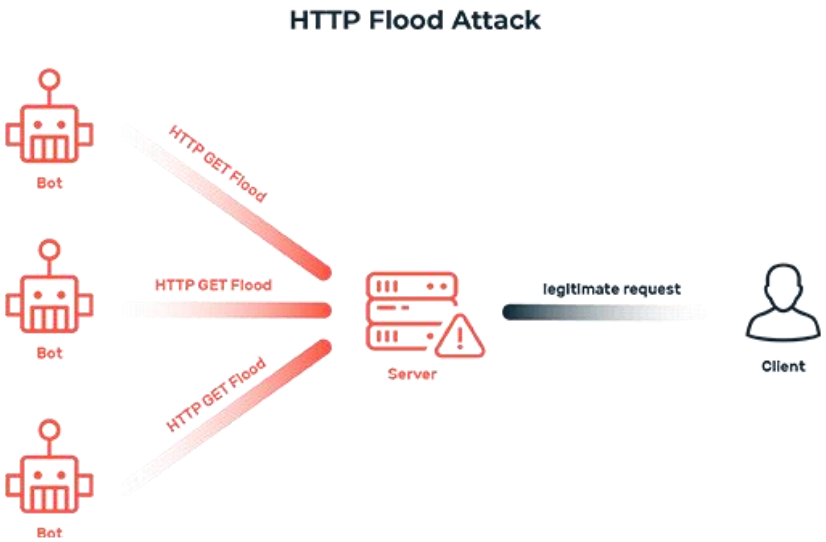


Come si può notare dall' immagine, la vittima riceve migliaia di richieste di SYN (sincronizzazione) provenienti da IP fasulli sempre diversi, in velocissima sequenza; a queste richieste risponde con altrettante richieste di SYN-ACK che non arriveranno mai a destinazione, perchè dirette a IP fasulli. Tutto ciò fa sì che la vittima aspetti le risposte ACK dei finti PC richiedenti, nel frattempo ricevendo sempre più richeste SYN e generando sempre più risposte SYN-ACK. Ciò alla lunga manda in saturazione la banda e l' utilizzo di CPU / memoria del server vittima.

HTTP FLOOD

E' un attacco più vecchio ma sempre attuale e dal quale é più difficile proteggersi, ed allo stesso tempo é molto più semplice del SYN Flood: migliaia di IP fasulli generano richieste per un servizio HTTP (visualizzazione pagine web e fetch dati via HTTP) in genere alternando richieste di tipo GET e di tipo POST.

Il server dovrà rispondere mandando dati a questi IP richiedenti forgiati e, a lungo andare, non riuscirà ad accogliere altre richieste lecite dai veri naviganti nel sito.



Come si presentano in genere questi 'script' DDoS? Si tratta generalmente di programmi complessi scritti in C o C++, ma é possibile scriverli anche in VB.NET e C#. In passato, gli attacchi più famosi di questo genere erano script in ambiente Linux (successivamente diffusi anche in ambiente Windows) chiamati **SMURF** e **TRIN0**.

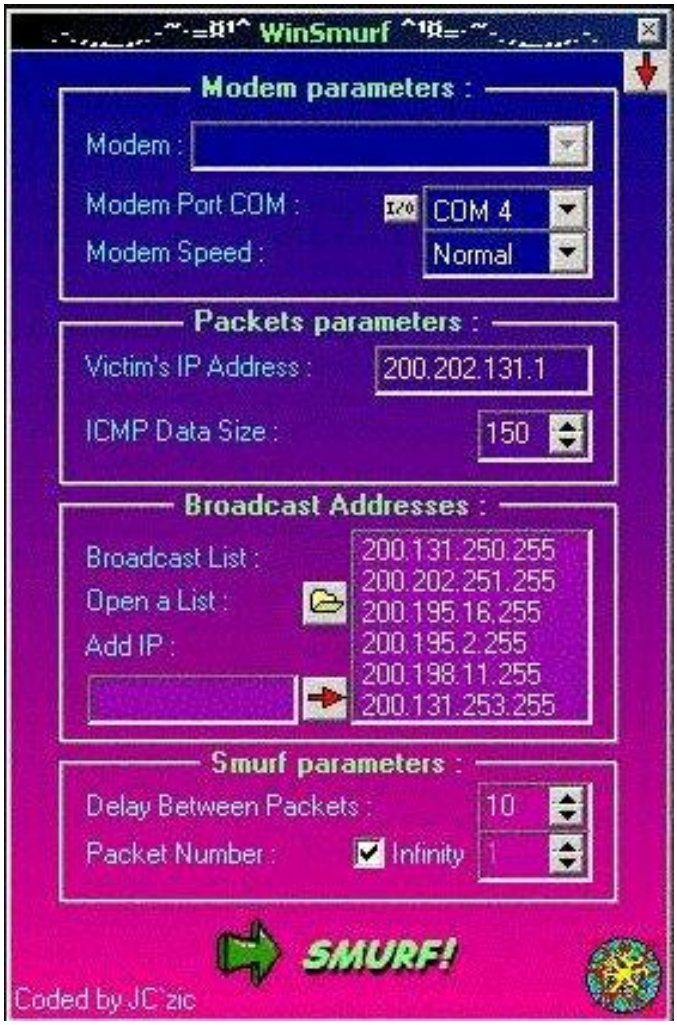
Qui di seguito viene proposta l' interfaccia del WinSmurf, il primo smurfer in ambiente Windows, codificato da un programmatore ed IRC warrior noto come JC. Il software, prodotto nel 2000, veniva utilizzato su connessioni dial-up classiche ed ISDN64 o 128 ma funzionava anche sulle CDN384, molto diffuse negli USA, in Canada, ed in alcune nazioni asiatiche; permetteva di aggiornare la cast list, di impostare il numero di pacchetti di attacco (con la possibilità di un attacco continuo o 'Infinite') e perfino di decidere il ritardo tra i pacchetti.

Di fatto, con le connessini dial-up dell' epoca, un ciclo Infinite con delay minore di 20-25ms risultava in una saturazione della banda locale, causando non la disconnessione del server vittima, ma quella del modem sorgente. Questo problema non si verificava con lo Smurf originale in ambiente Linux, grazie ad una migliore gestione dei pacchetti.

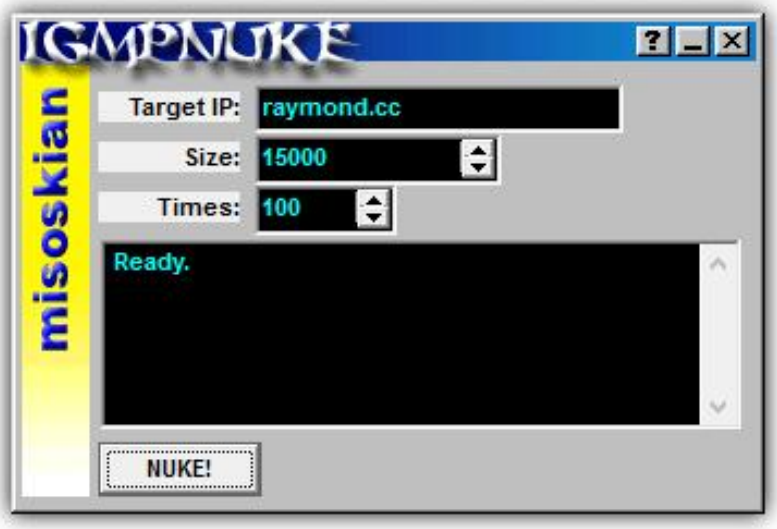
Lo scipt di Smurf veniva spesso caricato in 'shell onlne', cioè dei sistemi Linux messi a disposizione degli utenti per usi legittimi da provider di servizi di hosting, e lanciato da tali shell sfruttando la banda disponibile - in genere molto elevata - da tali servizi.

Il listato completo dello script Smurf.c é presente (a titolo di studio) sul sito di Computech:

https://www.computec.ch/archiv/software/denial_of_service/smurf.c



Oltre a questo genere di attacchi DDoS, ve ne furono tanti altri, spesso più malevoli, che hanno goduto di meno fama perchè più difficili da attuare e sensibili solo a determinati sistemi operativi. I PC Windows 9x ed ME, quindi tutti quelli SENZA il motore NT, erano violabili dal **Mass IGMP Flood**, un DoS che sfruttava pacchetti IGMP (Internet Group Management Protocol) e causava il riavvio automatico del PC vittima. Poteva essere eseguito da una sola sorgente o sfruttando connessioni zombi, quindi era allo stesso tempo sia un DoS che un DDoS. La versione più famosa di IGMP food per Windows era il **KOD / SuperKOD** (KOD sta per *Kiss of Death*), programmato e diffuso dal turco **Misoskian**, uno dei più abili programmatori di software di attacco degli anni 2000. La versione originale (SuperKOD) agiva dalla shell a riga di comando inviando alla vittima fino a 150.000 bytes di dati; successivamente venne trasposto con interfaccia grafica e diffuso (sepre da Misoskian) con il nome di **IGMP Nuke**.



Misoskian fu anche l' autore del primo **SYN FLOODER** in ambiente Windows.

(*) Il presente articolo é la rielaborazione della sezione relativa ai DDoS contenuta in un articolo più vasto scritto nel 2003 intitolato originariamente "*Principi di IRCwar - Floods, Nukes, DoS e DDoS*". Una versione riassuntiva di questo articolo é stata pubblicata dall' autore su Quora nel giugno 2022 come risposta alla domanda:

Che cos'è un attacco DDoS?