Que es un atac de DDOS?

Els atacs per denegació de servei distribuïts (DDoS) són una "arma" cada cop més utilitzada pels ciberdelinqüents que té principalment com a objectiu interrompre l'activitat del servei afectat o extorsionar les empreses víctimes de l'atac. Aquests atacs generalment obeeixen a motivacions de caràcter polític, religiós, competitiu ,econòmic o campanyes de *Hacktivisme* (cada cop més extenses, com es pot veure amb el context geopolític actual).

Un atac *denegació de servei distribuït* (DDoS) és una versió distribuïda d'un *atac per denegació de servei* (DoS), l'objectiu del qual és interrompre les activitats d'una empresa o xarxa, així com els seus serveis essencials. Aquest atac utilitza un gran volum de trànsit per provocant una sobrecàrrega sobre les operacions del servei, el servidor o la interconnexió de xarxa i, així, deixar-los inaccessibles. Els atacs DoS interrompen un servei, mentre que els atacs distribuïts (DDoS) s'executen a gran escala, arribant a inhabilitar infraestructures completes i serveis escalables com ara les solucions al *núvol*(cloud).

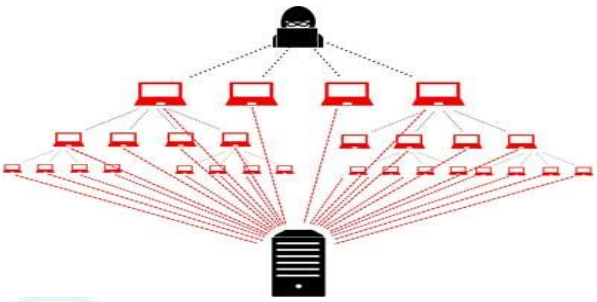

Figura 1. Tipologia atac DDOS

Lloc web inaccessible

Si el DDoS té com a objectiu el servidor web on s´allotja la pàgina d'inici de l´empresa, o institució, aquesta deixarà d'estar disponible per als clients considerats com a legítims. Com a conseqüència, la imatge de l´empresa es veruà danyada i els clients perdran la confiança, essent els danys reputacionals moltes vegades superiors als danys econòmics.

Reacció en cadena

Si diversos llocs web depenen directament d'un servei inhabilitat/vulnerat per l'atac, aquests també deixaran d'estar disponibles durant un període de temps arribant en ocasions a no "remuntar" el servei.

Tipus d´atacs de DDOS

Atacs DDoS per volum

Els atacs DDoS basats en volum, són els més coneguts. L'objectiu d'un atac DDoS és inhabilitar un servidor, servei o infraestructura mitjançant l'enviament d'un gran nombre de peticions(tràfic de paquets). D'aquesta manera, la connexió de xarxa o els recursos del servidor es saturaran provocant que les peticions legítimes no puguin arribar al servidor de forma habitual i fent que aquest no pugui gestionar la càrrega ni respondre les sol·licituds. Els ciberdelinqüents poden recórrer a un gran nombre d'ordinadors o dispositius infectats (dispositius *IoT(internet de les coses)* connectats com a càmeres,routers, endolls intel·ligents, termòstats, domòtica etc.), coneguts com a xarxa de *bots* o *botnets(xarxes fantasma)*, per fer que l'atac sigui més distribuït i, per tant, més efectiu. Una de les tècniques més utilitzades pels atacants és enviar grans quantitats de paquets de dades petites a una xarxa de bots amb una adreça IP(direcció de l´usuari a internet) falsificada o un rang de IP´s determinat; la *botnet* respon al seu torn enviant paquets encara més grans directament a la víctima (a la IP falsificada). Els dispositius/serveis víctima d'aquesta allau de peticions serán incapaços de respondre a tantes sol·licituds i les connexions a internet es sobrecarregaran arribant al límit de l'ample de banda de la xarxa. Aquesta tècnica es coneguda com atac de reflexió i amplificació.

Atacs sobre el protocol

Aquest tipus d'atac es dirigeix als protocols utilitzats per a la comunicació a les xarxes aprofitant els punts febles per deixar inaccessible el servidor/servei de la víctima. En alguns casos, es sobrecarreguen els dispositius intermitjos que connecten els serveis de la víctima amb la xarxa d´ internet. Un exemple serien els atacs DDoS Smurf.

Aquest tipus d'atac consisteix en un atac de denegació de servei distribuït(Ddos) a nivell de la xarxa on l'atacant envia un paquet a una adreça de xarxa de difusió, rebent una resposta automàtica per part de cada host(usuari o servidor). Combinant aquest mètode amb una IP d'origen falsificada (*spoofing*), els atacants activen un gran nombre de respostes i aconsegueixen saturar de trànsit de dades la víctima. Amb un nombre suficient de respostes és possible inhabilitar l'objectiu .

Atacs a la capa d'aplicació (L7)

Les aplicacions implementen una lògica més avançada i solen fer un ús més elevat dels recursos, per això són les més específiques i, probablement, les menys testejades o vigilades: aquesta condicionalitat les converteix en l'objectiu perfecte . La metodologia d'atac dirigida a aquesta capa requerirà una menor quantitat de recursos i, a la majoria dels casos, no són detectats pel *Firewall (tallafocs)* general ni pels sistemes de protecció antiDDoS.

Com identificar un atac de DDOS

Una excessiva latència(temps de càrrega) de la pàgina

Una de les maneres més comuns de saber que estem sent víctimes d'un atac Dos-DDoS és que observarem una excessiva latència de la pàgina. Això vol dir que els navegadors dels usuaris finals i els servidors responen de manera lenta, hi ha molt retard en la càrrega així com a l´hora de navegar pel lloc lentitud o interrupcions (ex: tallal estar visualitzant streaming).

Si això passa podríem estar davant d'un atac d'aquesta mena que estigui provocant un mal funcionament de la pàgina. Això ens obligarà a prendre mesures per aconseguir que tot torni a funcionar correctament .Per defensar-nos davant d'aquest tipus d'atacs, hem de conèixer molt bé la lògica de la capa d'aplicació i els usos específics.

Com protegir-nos

Mantenir els nostres equips segurs

Una part molt important en matèria de protecció per evitar que els nostres equips es vegin afectats per un atac DDoS és mantenir-los segurs. Cal tenir en compte tots els tipus de dispositiu que estiguem utilitzant i les seves característiques(ordinador, tablet, telèfon mòbil...), així com sistema operatiu. Un bon antivirus, com pot ser

Windows Defender, Avast, Bitdefender o Kaspersky, per nomenar-ne alguns, és una bona idea.

Amb això no podem oblidar el fet que es trobin perfectament actualitzats. Diàriament sorgeixen vulnerabilitats que són aprofitades pels ciberdelinqüents per desplegar i propagar les amenaces.

Estat actual i els últims incidents

En els darrers 2 mesos, els principals organismes oficials encarregats de la seguretat i la supervisió de les amenaces a la xarxa, han detectat un repunt d´aquests atacs per Ddos a escala global, hem vist afectacions a països veïns com Espanya,Alemanya,Irlanda on darrerament han sofert caigudes en sistemes tant claus pel país com el pagament de subsidis d´atur, o interrupcions als serveis sanitaris ,afectacions a serveis esencials. Les agències d'intel·ligència internacionals, avisen d´una reactivació de l´activitat de la botnet (xarxa fantasma) **Mirai**, és una botnet l'objectiu de la qual es infectar dispositius de l'anomenat Internet de les Coses (IoT).

Els principals objectius d'aquest codi maliciós han estat els routers, gravadors digitals de vídeo i càmeres IP de vigilància. Aquest codi maliciós(malware) ha estat usat principalment per realitzar atacs de denegació de servei (DoS) a tercers arribant a utilitzat en algunes ocasions més de 100.000 dispositius controlats remotament i sincronitzats per llençar atacs contra un objectiu determinat a una hora estipulada degradant la qualitat de servei d'un sistema o les xarxes privades o institucionals posades en el seu "punt de mira".

El principal mètode d'infecció de Mirai és mitjançant l'ús de credencials per defecte que el codi maliciós inclou ja que moltes de les quals són usades en dispositius IoT on la seguretat en molts casos en deficient.

Es per això una bona pràctica canviar les credencials per defecte que posa el fabricant dels dispositius, per credencials més robustes i així evitar que els nostres dispositius passin a formar part d´una botnet.