Reading Report: Vlajic12

Ricard Abril

April 14, 2019

1 Summary

En aquest text, es parla de l'impoprtancia dels valors TTL i del DNS, en la gestio d'un lloc web.
També es demostra l'importancia que te el seu control per evitar atacs i la sofisticació d'aquets temes en infrastructures critiques com la de la banca.

Els atacs DDos, son realment coneguts, ja que són senzills de realitzar i poden provocar la caiguda de tot un servei, de forma que cap usuari serà capas de accedir al lloc web. Aixo actualment ho pot fer qualsevol, ja que es pot contractar aquets serveis (de forma poc legal), a un preu no massa excesiu, per el qual obtindras una botnet, que durant un temps determinat, enviara peticions a un servei fins que aquet deixi de estar operatiu.

Però també existeixen maneres de evitar aquets atacs, com:

1. Ús adequat de tallafocs i sistemes de detecció d'intrusió
2. Subministrament excessiu d'ample de banda
3. Desplegament de múltiples rèpliques de servidors web separats físicament i lògicament

Aquestes tencinques pero, nomes es centren en la xarxa, però no en la part del usuari. Les empreses no sembla que siguin concients del paper que pot jugar el DNS en aquet aspecte.

El funcionament del DNS, de cara al usuari es podria resumir en un parell de senzills pasos:

1. Usuari proporciona URL al Navegador.
2. El navegador envia aquesta URL al DNS-Resolver local, aquet mira la seva cache, en cas de tenir-la, retorna al usuari la @IP, en cas de no tenir-la, envia una Query al servidor de DNS local.
3. El servidor DNS, consulta si ho te en cache, si no ho te, fa una consulta a in DNS de nivell superior, altrament retorna la @IP.
4. Quan el programa del usuari rep la @IP, aquet estableix una connexió HTTP amb la @IP, per descarregar el contingut.

Una de les coses molt importants en els registres DNS, és el TTL, que es el temps que l'autoritat DNS, permet als registres DNS conservar un record en la memoria cache abans de haverne de demanar una copia nova.
El TTL, es decideix en base a:

Freqüència de les actualitzacions del contingut del lloc web i / o de la ubicació del servidor amfitrió:

Si tenim un lloc web amb contingut estatic i amb una IP estatica, acostumarem a escollir una TTL llarg, ja que aixo repercutira en una millor velocitat de conexio per l'usuari, ja que la probabilitat de estar en la memoria cache, és més alta.
Per altra banda, aquells llocs web amb mapes de IP dinamics, que canvien de @IP amb frequencia, acostumen a escollir TTL's molt curts, per tal de evitar que un ususari intenti conectarse a una @IP incorrecte, per tant conve consultar més els DNS per tal de tenir una informació acurada.

Esforços per controlar el nombre de cerques de DNS:

l'augment de la c'arrega en els servidors de DNS, en particular els servidors de DNS autoritzats,és una conseqüència directa dels temps curts de TTL de DNS. Amb TTL curts, els registres DNS caduquen més aviat de les memòries cache dels DNS dels clients, per la qual cosa s'envien més sol·licituds de DNS als servidors de DNS de més alt nivell. Per aquest motiu, molts llocs web opten per utilitzar temps llargs de TTL com a mecanisme d'equilibri de càrrega de DNS
Escollir una tecnica, té certa complexitat. Esta be recordar que:

Els usuaris generalment es beneficiaran d'un TTL petit

El nombre d'actualitzacions amb un TTL petit, serà molt gran En empreses on el funcionament del seu lloc web es critic, no és extrany veure TTL's de 0.

Una estratègia més adequada per garantir una bona resistència a la possible fallada del servidor web i tractar amb èxit les situacions de Faulty DNS-Cache Lock és la utilització de múltiples repliques de servidors web que funcionen simultàniament, amb cada replica funcionant en una adreça IP única i en una ubicació física diferent. Aquesta solució suposa que diverses adreces IP estan associades amb el mateix nom simbolic i que totes les adreces IP utilitzades s'inclouen simultàniament al registre DNS del lloc. Si una de les adreces IP és víctima d'un atac Dos, els clients tindran altres adreces IP alternatives disponibles a la memoria cache del DNS local (SO). Aquesta solució és molt utilitzada per les CDN, i és al centre de la seva estratègia d'aconseguir l'equilibri de carrega i la tolerància a fallades dels llocs web allotjats.

S'ha fet una enquesta buscant els valors de TTL de DNS dels registres DNS a grans bancs de EEUU i la UE. S'han classificat en 3 grups: A) els 15 millors bancs de EEUU, B) els 15 bancs mes grans de EEUU i C) els 15 millors bancs i grups bancaris de la UE.

S'han fet servir 3 estratègies:

1. Mitjançant la realització de múltiples descarregues independents de les pagines web frontals dels 45 bancs en qüestió, amb Wireshark funcionant en segon pla i capturant el transit DNS que passa

2. Utilitzant la utilitat nslookup i adquirint els registres DNS dels 45 bancs en preguntes de tres servidors DNS públics diferents, ubicats en tres països/continents diferents

3. Amb l'adquisició dels registres DNS dels 45 bancs en qüestió mitjançant http://just-dnslookup.com/index.php. Aquesta eina en línia recupera els registres DNS de qualsevol domini web sol·licitat confiant en 63 servidors de control ubicats a diverses ciutats de tot el món. Un resum dels 63 registres obtinguts es presenta després a l'usuari.

Els resultats obtinguts han sigut:

1. Al grup A, hi ha valors de TTL de DNS de 60 minuts o més. S'observen els 15 bancs mitjançant un mapeig únic de nom simbòlic a adreça IP als registres DNS, el que suggereix que cap dels bancs no té cap disposició per a la redundància del servidor web i la migració automatitzada de servidors web. Aquests resultats són alarmants i són un indicador probable que el personal dels bancs desconeix els possibles perills associats a l'ús de valors del TTL excessivament llargs i dels riscos d'utilitzar un únic servidor web

2. Al grup B s'observen pocs valors de TTL de DNS de 60 min i més, mentre que la majoria utilitza TTL menors d'1 min. Alguns bancs s'observen mitjançant un mapeig múltiple de nom simbòlic a adreces IP als registres DNS, que suggereixen l'ús de diversos servidors web i provisions per a la migració de servidors. Un banc té el servei d'allotjament web d'Akamai CDN, una solució bastant costosa, però amb la millor capacitat de resistència davant possibles atacs DDoS

3. Al grup C, alguns bancs tenen TTL de més de 60 minuts, algun tenen TTLs inferiors a 1 min, mentre que altres tenen TTLs d'entre 5 i 30 minuts. S'observen pocs bancs amb mapeig múltiple de nom simbolic a adreces IP, i un banc confia en els serveis d'allotjament web d'Akamai CDN

Alguns dels problemes relacionats amb el Faulty DNS-Cache Lock que actualment s'està investigant pel nostre grup de recerca inclouen:

1. El terme memoria cache del DNS local s'utilitza generalment per referirse a la memoria cache del DNS del sistema operatiu del client. A la mateixa maquina del client, a més de la memòria cache del DNS del sistema operatiu, existeixen també les memòries cache dels DNS dels navegadors individuals. Hi ha hagut poques investigacions sobre la interacció mútua entre els diferents tipus de memòries cache dels DNS dels navegadors i l'impacte que podrien tenir cadascun d'ells en situacions de Faulty DNS-Cache Lock

2. La tasca de determinar el valor més òptim del TTL de DNS per a un lloc web particular no és gens trivial. El que constitueix el TTL òptim dependrà de diversos factors, incloent: A)el comportament real dels usuaris que visiten el lloc donat i la seva distribució física / geogràfica en relació amb la ubicació del servidor DNS autoritzat del lloc i B)si el lloc utilitza o no múltiples assignacions de "nom simbòlic a adreça IP"; C) probabilitat que el lloc es converteixi en l'objectiu d'un atac DDoS, etc

2 Assessment

Es un reading no gaire difícil d'entendre, i es fa molt lleuger, ja que tracta temes molt interesants dels quals no s'acostuma a parlar a les diferents carreres de la universitat