Reading Report: Vlajic12

Eric Casanovas

April 14, 2019

Upload your report in PDF format.
Use this LaTeX template to format the report, keeping the proposed headers.
The length of the report must not exceed **5 pages**.

1 Summary

Aquest document es un paper presentat a una conferencia, especificament a The 3rd International Conference on Ambient Systems, Networks and Technologies (ANT).

En aquest paper s'examinarà l'impacte del DNS TTL values en l'experiencia de l'usuari i que un ús inapropiat d'aquest pugui tenir conseqüencies com per exemple caure victìma d'un atac DDoS.

1. **Introducció**
   Els atacs DDoS són una de les amenaces més importants a internet a dia d'avui degut a la seva simplicitat i baix cost d'executar. Aquest atac consisteix en l'enviament massiu de dades a una màquina fent-la inservible degut a la impossibilitat de respondre totes les requests. Normalment es fan servir xarxes de botnets que són conjunts d'ordinadors infectats per un ordinador "mare". Tenint en compte aquests factors, les solucions anti-DDoS són una prioritat alta pels negocis web. Per evitar DDoS podem fer servir:

   - Firewalls i sistemes de detecció d'intrusos.
   - Aprovisionament excessiu d'ample de banda.
   - Desplegament de repliques de servidors web separades físicament.

   Tot i així aquestes tècniques no arreglen el problema ja que també té un paper molt important el sistema de DNS.

2. **Impacte del valor de DNS TTL** Com funciona un DNS:

   (a) L'usuari proporciona la URL de la pàgina web.

   (b) El navegador envia la URL al DNS-resolver, el resolver busca a la seva cache per si té una coincidencia, en cas afirmatiu reotrna la IP, en cas contrari envia una consulta al DNS local.

   (c) El DNS local busca a la memoria cau si té una coincidencia, sinó s'envia la consulta a un DNS superior.

(d) Una vegada que el programa d'usuari obtingui la IP, el programa estableix un connexió HTTP.

Un important component es el camp TTL que es el temps que es quedara a la cache. El temps escollit normalment es dicta pel següent:

- Freqüencia de les actualitzacions del web-site i la seva localització: Llocs web amb contingut estàtic solen triar valors TTL llargs per aconseguir una baixada de pàgina web més ràpida. Degut a que llargues TTL és probable que les peticions DNS estiguin ja cachejades. D'altra banda, llocs web amb freqüència canviar el contingut tendeixen a escollir valors curts de TTL per forçar freqüentment refrescant els seus registres DNS i aconseguint així un lliurament puntual i precís d'informació.
- Esforços per controlar el nombre de DNS-lookup: Augment de la càrrega en els servidors de DNS. És a dir, amb curt TTLs, els DNS Records caducen més aviat des de les memòries cau DNS dels clients, per la qual cosa hi ha un nombre més gran de sol·licituds de DNS acaben sent reenviats als servidors de DNS de més alt nivell. Per aquest motiu, molts llocs web opten per utilitzar-lo durant molt de temps TTL vegades com a mecanisme d'equilibri de càrrega DNS.

Per a la majoria de llocs web, els valors TTL de 15 a 30 minuts són considerats òptims. No obstant això, hi ha situacions en què els TTL d'aquesta durada poden tenir molt conseqüències perjudicials i costoses per a una organització. Assumim que un client accedeix a un lloc web d'interès poc abans de l'inici d'un atac DDoS. La intensitat del DDoS és tal que paralitza el servidor, per la qual cosa després d'alguns segons el servidor migra a una altra ubicació. Malauradament les memòries cau de resolució de DNS del client són vàlides segons el TTL. En conseqüència, tots les sol·licituds del client generades en els propers segons TTL es reenvien a l'antiga que esta bloquejada. Ens referirem a aquesta situació com a *Faulty DNS-Cache Lock*. L'única manera d'arreglar un *Faulty DNS-Cache Lock* es fent un flush de la cache (ipconfig /flushdns terminal de windows).

Un estudi recent ha demostrat que entre el 37% i el 49% dels usuaris que experimenten els problemes de rendiment en realitzar una transacció abandonaran el lloc i/o, es passaran a un competidor. De la mateixa manera, un estudi conjunt dels investigadors de Google i de Bing ha demostrat que el 57% dels consumidors abandonen un lloc web després d'esperar 3 segons perquè es carregui una pàgina. 8 de cada 10 persones no tornen a lloc després d'una experiència decebedora. Un estudi de 2010 de Forrester Consulting s'ha centrat en els usuaris de bancs a la xarxa i les seves expectatives de rendiment del lloc web. Els resultats d'aquest estudi mostren que el 75% dels consumidors en línia de serveis financers esperen un 99% o més de disponibilitat de llocs web, i classifiquen el rendiment del lloc en segon lloc en una llista de les expectatives dels usuaris, just després de la seguretat. Les conclusions que podem treure podrien ser:

- TTL de llarga durada són estadísticament més propensos a posar un nombre més gran de màquines client en *Faulty DNS-Cache Lock*. Per un website sota un atac DDoS, molts d'intents de recàrrega per

part d'usuaris legítims només agreujarà la congestió de l'amplada de banda i/o la càrrega de processament al servidor, ajudant així l'atacant a aconseguir el objectiu.

- Els *Faulty DNS-Cache Lock* llargs TTL, tal com hem comentat abans, és probable que tinguin conseqüencies negatives a llarg termini al website, ja que l'usuari experimenta un lloc web deficient.

3. **Escollir valor DNS Record/TTL Strategy**
   Els usuaris que accedeixin a un lloc web generalment es beneficiaran d'un petit valor TTL al registre DNS del lloc, ja que implicaria actualitzacions freqüents de les memòries caché DNS dels clients i una bona resistència en cas d'un error del lloc (possiblement causat per un DDoS). Però, amb un TTL petit, el nombre de sol·licituds i, en conseqüència, la càrrega total dels servidors DNS locals i autoritzats podrien ser significatius. A més, els estudis han demostrat que una TTL petita augmenta els riscos d'un atac per intoxicació de DNS.
   Per a les empreses que depenen críticament del rendiment dels seus llocs web, no és estrany veure els valors de DNS TTL establerts a 0 [sec].

4. **Survey of DNS Record / TTL Strategies in Major US and EU Banks**
   Grup A: 15 bancs nord-americans amb millor rendiment segons Forbes.com; grup B: 15 grans bancs nord-americans, pel que fa al seu actiu total, de nou segons Forbes.com; grup C: 15 principals bancs de la UE i grups bancaris, segons BanksDaily.com.
   Al grup A, s'observen 8 dels 15 bancs que utilitzen valors DNS TTL de 60 minuts o més. A més, s'observen els 15 bancs utilitzant un sol mapatge "nom simbòlic a adreça IP" en els seus registres DNS, el que suggereix que cap dels dos els bancs d'aquest grup tenen disposicions per a la redundància del servidor web i / o la migració automatitzada de servidors web.
   D'altra banda, al grup B només s'observen 2 de cada 15 bancs utilitzant valors DNS TTL de 60 min i més, mentre que 10 de cada 15 s'observen utilitzant DNS TTLs menors d'1 min. 6 d'aquests bancs també s'observen mitjançant l'ús de múltiples assignacions de "noms simbòlics a adreces IP" en els seus registres DNS, que suggereixen l'ús de diversos servidors web i / o provisions per a la migració de servidors.
   Al grup C, 5 dels 15 bancs s'observen mitjançant DNS TTL de més de 60 minuts, 4 s'observen utilitzant TTLs inferiors a 1 min, mentre que els restants 6 bancs tenien TTLs d'entre 5 i 30 minuts. S'observen que tres bancs d'aquest grup utilitzen assignacions de "nom simbòlic a adreça IP" múltiples, mentre que un banc confia en els serveis d'allotjament web d'Akamai CDN.

5. **Ongoing Work**
   El terme DNS localCache (client) generalment s'utilitza per referir-se a la memòria cache DNS del sistema operatiu del client. No s'ha d'oblidar, tanmateix, que a la mateixa màquina del client, a més de la memòria cache DNS del sistema operatiu, existeixen també les memòries cache DNS dels

navegadors individuals. Fins a la data, hi ha hagut poques investigacions sobre la interacció mútua entre els diferents tipus de memòries cau de DNS del navegador i l'impacte que cadascun d'ells podria tenir en situacions de bloqueig de cache DNS defectuós. per a un lloc web particular no és gens trivial. És a dir, 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 respecte a la ubicació del servidor DNS autoritzat del lloc; 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. Segons el nostre coneixement, no hi ha hagut cap treball previ en la interacció de tots aquests factors i proporcionant un model analític per al càlcul de valors DNS TTL òptims.

2 Assessment

En la meva opinió el text ha sigut de fàcil lectura i fàcil de comprendre, a mes a mes es un text molt interessant i s'hauria de seguir ficant els següents cursos.