Navigare în siguranță pe internet folosind DNS protection

Aducem către atenția dumneavoastră importanța crescândă a serviciului de DNS, serviciu pe care se sprijină într-o foarte mare parte internetul de astăzi. Acesta a servit și servește în tăcere, fără prea multe pretenții, miliarde de cereri pe zi de la orice utilizator care dorește să ajungă la o pagina web, fără să țină minte adresa IP a acesteia. Însă dată fiind importanța crescândă a acestui serviciu, a atras dupa sine și atenția atacatorilor, care-și ascund în spatele înregistrărilor DNS, infrastructuri de atac.

De ce acum? De ce prin DNS? Odată cu creșterea interesului în securitatea datelor și responsabilității utilizatorilor, a devenit populară funcția de URL filtering, de URL whitelisting sau de filtrare a site-urilor web bazată pe categorii și reputația acestora. Însă clasificarea site-urilor în categorii sau menținerea reputației necesită timp. La momentul înregistrării unui site nou în DNS, reputația acestuia este neutră, categoria acestuia e necunoscută, asta permițând de multe ori atacatorilor să dețină un interval de timp în care își desfasoară atacul, fără să fie filtrat de funcția de URL. Odata site-ul catalogat, devine blocat, dar asta nu face decât să îi motiveze pe atacatori să-și mute infrastructura în minute pe altă înregistrare DNS, revenind înapoi la ce faceau.

Tehnicile cel mai des folosite în acest tip de manipulare de DNS sunt:

- DNS fast flux, înregistrarea unui număr mare de IP-uri care sunt translatate către o singură înregistrare DNS concomitent cu schimbarea rapidă a acelui numar de IP-uri, forțând astfel imposibilitatea de IP block. DNS block însă funcționează, înregistrarea DNS fiind aceeași;

- DNS DGA, sau nume de domeniu DNS generate aleator, prin care atacatorii înregistrează multe înregistrări dns diferite, care pot duce la un singur IP sau pot duce la un fast flux pool de IP-uri descris mai sus. Acesta forțează imposibilitatea de a bloca IP blocks, dar nici înregistrările DNS nu sunt aceleași, ceea ce face filtrarea dificilă. Există algoritmi de detecție a numelor ce sunt suspecte să fie DGA, iar acestea să fie blocate.

Atacurile DDoS ca cel împotriva Dyn din oct16 ne-au arătat că infrastructura DNS în sine devine parte a unui atac, ori ca atac în sine, dar și ca paravan pentru alt atac sau succesiune de atacuri mascate. La momentul atacului de atunci, au fost companii care au trecut peste neafectate de nedisponibilitatea Dyn, prin simplul mecanism de caching oferit de un serviciu de DNS recursiv. Faptul ca serviciul de DNS recursiv nu putea face relay către DNS autoritative cum era Dyn nu a făcut decât să răspunda cu ultima adresă pe care o avea la cunoștință, ceea ce era suficient, din moment ce companiile oricum nu-și puteau anunța noile înregistrări de DNS către autoritative. Unul dintre serviciile de DNS recursiv care a facilitat aceasta este OpenDNS și funcția sa înglobată smartcache.

Deasemenea, dacă revenim la tehnicile exemplificate ca utilizate de atacatori, un DNS recursiv poate aplica algoritmi de detecție DGA, poate bloca cereri catre DGA, deasemenea poate aplica algoritmi de analytics către înregistrările de DNS noi prin care să evidențieze eventuale legături ascunse cu alte înregistrări DNS mai vechi și cunoscute ca fiind rău intenționate. Acești algortimi se pot baza pe apartenența la același AS number al providerului, are același e-mail înregistrator, conține aceleași servicii activate și hostează același conținut sau aceleași fișiere artifact și așa mai departe. Una dintre tehnicile cele mai puternice de prevenire a acestor tipuri de atac e pur și simplu blocarea accesului la site-uri ce au înregistrări de DNS foarte noi și nu sunt catalogate URL. Asta taie avântul atacurilor prin DNS bazate pe timpul necesar catalogarii site-urilor noi.

În acest moment serviciul DNS joacă o carte foarte puternică în amprentarea și detectarea nodurilor de ieșire ToR și a modului în care acestea interoghează DNS în favoarea celor care folosesc rețeaua pentru anonimizarea acțiunilor. Daca inițial ToR a pornit ca o idee bună de anonimitate completă pe internet și de a nu mai lasa altora șansa de a urmări ce fac pe internet, astăzi ToR este folosit din ce în ce mai mult pentru hostarea serverelor de atac, tocmai datorită anonimității date de acest serviciu. Cum ToR este organizat ca o rețea peer-to-peer, e foarte greu să poată fi blocată, e foarte greu să știm care dintre laptop-urile unei organizații este și ToR exit node, doar uitându-ne la traficul de rețea.

În concluzie, folosirea unui serviciu de DNS recursiv, fie el google.com, OpenDNS, Neustar ajută la filtrarea site-urilor web direct din cererea de DNS, este mult mai simplu de aplicat, nu e nevoie de un echipament local ce să filtreze URL, în plus putem aplica politici prin care să întârziem accesul către site-uri prea noi. ■