DoH webean pribatutasuna bermatzeko azken pausoa

Webeko jardueretan erabiltzaileon pribatutasuna eta segurtasuna bermatzeko helburuarekin, hainbat aldaketa egin dituzte azken urteetan sareko agente garrantzitsuenek. Bide horretan ematen ari den azken pausoa da konfidentzialtasuna ezartzea DNS sistemak egiten dituen eskaeretan ere; eskaerak HTTPS protokolo seguruaren bidez egin daitezen bultzatzen da, DoH deitu duten teknologiaren bidez.

Duela ia bost urte (zehazki, 2015eko urtarrilean) atal honetan idatzitako artikulu batean kontatzen genuen nola neurriak hartzen ari ziren webeko eragile nagusiak erabiltzaileon jarduera inork ezin zelatatu ahal izateko. Han genionez, aurkeztu berri zen HTTP protokoloaren bertsio berri bat, HTTP/2 izenekoa, non ahal den guztietan nabigazioa HTTPSren gainean egiten den (HTTPS protokoloan komunikazio guztia zifratua doa). Web-nabigatzaile guztiek 2015aren amaierarako jada inplementatua zuten HTTP/2 protokoloa.

Artikulu hartan, laster sortzekoa zen Let's Encrypt ziurtagiri-jaulkitzailearen berri ere ematen genuen, web-zerbitzarietan HTTPSren erabilera sustatuko zuena. Ekimen horrek aukera emango zien lehenbizikoz web-zerbitzariei ziurtagiri digitalak dohainik eta erraz eskuratu eta berriztatzeko. 2016ko apirilean jarri zen martxan zerbitzua, eta asko zabaldu dela esango nuke.

Alabaina, webgune batekiko komunikazioak osoki HTTPS bidez egiten ditugunean ere, bada web-nabigazioaren beste osagarri oso garrantzitsu eta beharrezko bat, oraingoz ez duena segurtasun- eta pribatutasun-neurririk, eta espioitzaren eta amarruen aurrean babesgabe uzten gaituena: DNS sistema.

Zer da DNS sistema?

DNS siglek *Domain Name System* esan nahi dute, hau da, domeinu-izenen sistema. Domeinu-izenak webeko zerbitzuak eta webguneak identifikatzeko gizakiok erabiltzen ditugun izenak dira: www.google.com, www.berria.eus... Baina web-zerbitzariak IP helbide baten bidez identifikatu eta aurkitzen dira Interneten, 172.217.17.4 edo 145.239.192.54 modukoak direnak. Beraz, web-nabigatzaile batek web-orri bat atzitu ahal izateko, aurrez jakin behar du eskatutako domeinu-izena zer IP helbideri dagokion. Eta horretarako da DNS sistema.

Interneteko zerbitzuetako bat da DNS. Eta zerbitzu banatua da: zerbitzari batzuek domeinu batzuen informazioa dute, eta beste batzuek, beste batzuena. Gure ordenagailuak lehen eskaera DNS-ebazle bati egiten dio, eta hark bideratzen ditu eskaerak beste zerbitzarietara, domeinu-izenari dagokion IP helbidea lortu arte.

Igor Leturia Azkarate
Informatikaria eta ikertzailea

ARG.: Gerd Altmann / Pixabay

DNS protokoloaren arazoak

DNS protokoloa weba baino lehenagokoa da, 1983koa, eta geroztik apenas izan du aldaketa edo segurtasun-eguneraketa garrantzitsurik. DNS-eskaerak eta erantzunak ez doaz zifratuta, eta horrek segurtasun-arriskuak eta pribatutasun eza dakartza.

Alde batetik, Interneteko gure zerbitzu-hornitzaileak, konektatu garen WiFiaren jabeak zein DNS-eskaera eta erantzunen bidean zeharkatzen diren tarteko zerbitzari eta router guztiek ikusten dute zer DNS-eskaera egiten ari garen, eta, beraz, zer webgune bisitatu nahi dugun. Hori balia daiteke, adibidez, gure lehentasunen profil bat egiteko eta publizitate-enpresei saltzeko.

Bestetik, bidean dagoen edozeinek alda dezake erantzunaren IP helbidea, eta behar ez den orri batera bidali. Hala, gure bankuaren edo posta-hornitzailearen webgunera joatea eskatzen dugunean, itxura bereko webgune maltzur batera bidera gaitzakete, eta gure datuak lapurtu. Edo saltoki handi batean gaudela telefonoa baliatu nahi badugu ikusteko ea produktu bat konpetentziak merkeago duen, saltokiko WiFiaren bidez konektatu bagara, esan diezagukete konpetentziaren webgunea ez dabilela. Kasu horiek apur bat muturrekoak eta ez hain ohikoak badira ere, DNS-erantzunaren aldaketa hori bera baliatzen da zentsurarako; berriki, Tsunami Democràtic-en webguneak ixteko, adibidez. Internet-hornitzaileei agintzen zaie domeinu horietarako eskaerak beste IP helbide batera bideratzeko, non webgune hori itxi dela adierazten duen web-orri bat erakusten den.

Konponbidea, DoH

Horren irtenbidea DoH (DNS over HTTPS) izan daiteke, DNS-eskaerak eta -erantzunak HTTPS protokolo zifratuaren bidez egiten dituen teknologia, alegia. Hala, mezuak zifratuta daudenez, tartean daudenek ezin dute ikusi zer domeinu bisitatu nahi dugun eta ezin dute erantzuneko IP helbidea aldatu.

> *"DoH zabalkundea izaten ari bada ere, kritikak ere jasotzen ari da, eta polemika bat baino gehiago piztu ditu."*

Web-nabigatzaile nagusiek jada inplementatu dute. Firefoxek duela urtebete baino gehiago ematen du aukeran, baina ez lehenespen gisa; eskuz aktibatu behar dugu. Googleren Chrome nabigatzaileak ere aurtengo irailetik ematen du erabiltzeko aukera, eta Androidek, 9 bertsiotik aurrera.

DNS-ebazle batzuek ere inplementatu dute jada; Cloudflare enpresa ezagunak, adibidez (hau erabiltzen du Firefoxek lehenespen gisa). Chromek, bestalde, Googlek berak eskaintzen duen DoH-ebazle bat darabil.

Benetan da konponbidea?

DoH zabalkundea izaten ari bada ere, mundu guztiak ez du begi onez ikusten. Kritikak ere jasotzen ari da, eta polemika bat baino gehiago piztu ditu.

Batetik, esaten dute DoH-arekin ere ezerk ez duela bermatzen DNS-ebazleak ez duenik gure nabigazioaren profila egingo eta publizitate-enpresei salduko, eta arrazoia dute; kasu horretan, DNS ebasle deitu beharko genioke (barkatu, txiste txarra ;-). Baina inoiz ekidin ezin izango den kontu bat da hori, beti fidatu beharko dugu DNS-ebazleaz.

Bestetik, orain artean, ordenagailuko sistema eragile mailan guztientzat definituta dagoen DNS-ebazlea erabili izan dute Internet-zerbitzu guztiek. Etxeko sareetan, Interneteko gure zerbitzu-hornitzaileak routerrean definitutako ebazlea izan ohi da, eta enpresetakoetan, sistema-administrariek definitutakoa. Haiek iragazkiak jar ditzakete DNS-ebazleetan edo routerrean bertan, hainbat tokitara sar ez gaitezen. Gure seme-alabek zer webgunetan nabiga dezaketen mugatzeko erabiltzen den softwareak ere DNS sistema baliatzen du, eta baita webgune maltzurrak saihesten dituzten antibirusek eta suhesiek ere. Web-nabigatzaileak sistemako DNSa erabili beharrean DoH-ebazle bat erabiltzen badu, ezin dute hori egin.

Azkenik, gorago aipatutako zentsura ekiditen du DoH sistemak. Erraz egiazta dezakezu hori: DoH aktibatu Firefoxen ezarpenetan eta Tsunami Democràticen webgunea arazorik gabe ikusi ahal izango duzu. Eta, jakina, gobernuek ez dute hori atsegin...

Enpresen, Interneteko konexio-hornitzaileen, software-ekoizleen eta gobernuen kritikak ikusita, Mozillak esan du Firefoxek begiratuko duela ea sarean edo sisteman enpresa- edo guraso-iragazkirik instalatuta dagoen, eta hala bada, ez duela DoH erabiliko. Horrez gain, esan du herrialde batzuetan ez duela DoH lehenetsita jarriko, zilegi diren gobernu-blokeoak nola onartu adostu arte. Baina nola erabakiko du zer herrialdetako gobernu-blokeoak diren zilegi, eta zein diren zentsura? Txina, Turkia eta halakoetan soilik jarriko du DoH, zentsura ekiditeko? Eta Espainian zein Frantzian? Azkenean, besteak beste, zentsura ekiditeko sortutako sistemari kasu batzuetan zentsura onartzeko bidea irekitzen dio Mozillak horrela.

Horiek guztiak ikusita, argi dago izenburuan esan dugunean DNS over HTTPS dela webean pribatutasuna bermatzeko azken pausoa, *azken* horrek berriena adierazi nahi duela eta ez besterik ez dela behar izango... Soka luzea ekarriko du oraindik webeko segurtasun eta pribatutasunaren gai honek.