IGOR LETURIA AZKARATE
Informatikaria eta ikertzailea

INTERNETEKO KOMUNIKAZIOEN SEGURTASUNA III

Anonimotasuna

Interneteko komunikazioen segurtasunari buruzko artikulu-sorta honen barruan, aztertu dugu nola bermatu daitezkeen konfidentzialtasuna (mezu pribatu bat hirugarrenek ez atzematea) eta autentifikazioa (gure solaskidea berak dioena dela egiaztatzea). Oraingoan, Interneten anonimotasuna ziurtatzeko bideak landuko ditugu, eta, ikusiko dugunez, aurreko bietan bezala, gako publiko bidezko kriptografia dago honen oinarrian ere.

Interneten anonimotasunez aritzeko metodoez entzutean, jende askoren lehen erreakzioa mesfidantza da. Modu anonimoan aritu nahi denean zer edo zer okerra egiteko izango dela pentsatu ohi dugu: legez kanpoko zerbaitetan jardun, edo komunikabideren bateko komentarioetan *troleatu*, eta horrelakoak.

Baina badaude anonimotasuna bermatu beharra dagoen kasuak guztiz zilegi direnak. Herritarron pribatutasun-eskubidea dago, adibidez: bizitzako beste edozein arlotan bezala sarean ere nahi duguna egin ahal izatea inongo gobernuk, zerbitzu-hornitzailek edo bilatzailek zertan ari garen jakin gabe. Baita sareko zentsura aplikatzen duten herrialdeetan nabigatzeko eskubidea bermatzea ere. Edo kazetarien informatzaileen anonimotasun eta segurtasuna ahalbidetzea, Wikileaksen kasuan bezala. Eta beste horrelako asko.

Ziberkafe batera jotzea izan liteke bururatuko litzaigukeen lehenengo gauza, baina horren desabantailak ugariak eta nabariak dira: lekukoek identifikatu ahal izatea, hurbiltasun geografikoaren beharra, maiz aldatu beharra...

Beste modu bat proxy edo bideratzaile anonimoak erabiltzea da. Zerbitzu batzuk dira, ikusi nahi dugun web-orriaren helbidea bertan sartuz gero eskaera berek egin eta orria guri bueltatzen digutenak. Horiek ere ez dira oso egokiak: zerbitzu horien hornitzaileek badakite nor aritu den; sarritan ordainpekoak edo publizitate gogaikarria dutenak izaten dira; nabigatzeko soilik balio dute, eta ez, esaterako, posta bidaltzeko...

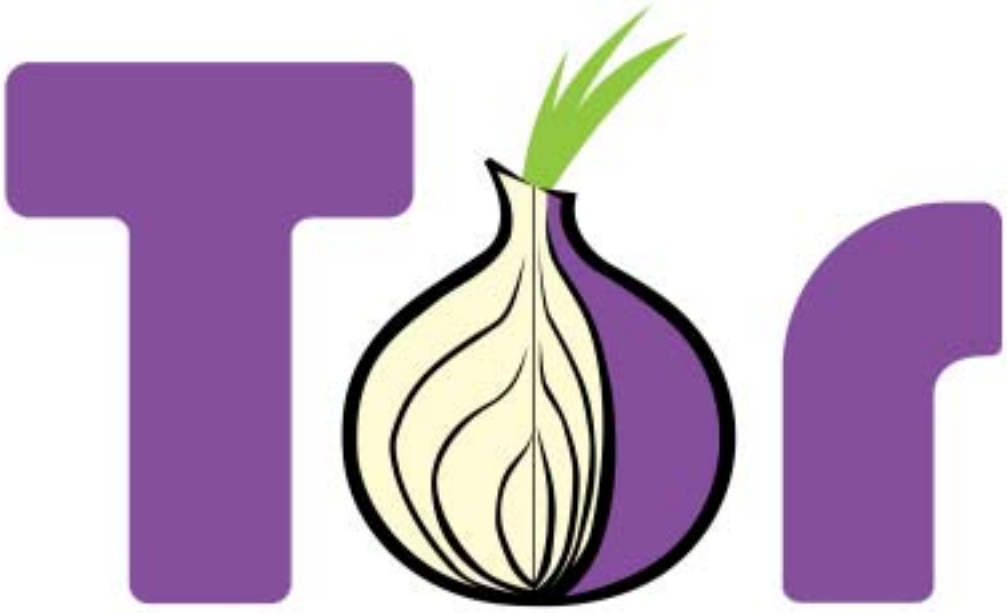
Baliabide edo informatika-ezagutza handiak dituztenek (inteligentzia-zerbitzuek edo gaizkileek) erabil dezaketen bide bat da *malware*ren baten bidez jende arruntaren ordenagailuen kontrola hartzea eta, jabeak ohartu gabe, eskaerak edo mezuak haien bidez bideratzea, arrastorik utzi gabe. Baina modu hau ez dago edonoren esku, eta ez da legezkoa, jakina.

TOR SOFTWARE ETA SARE LIBREAK

Gaur egun, Interneten anonimotasunez aritzeko modurik seguruena eta edonoren eskura dagoena Tor erabiltzea da. Tor siglek *The Onion Router* esan nahi dute, hau da, tipula bideratzailea. Izen bitxia, baina bere izateko arrazoia duena, geroago ikusiko dugun bezala.

Tor software libre bat eta sare ireki bat da, aukera ematen diguna gure sareko komunikazioak boluntarioen sare bateko hainbat ordenagailutan jauzi eginez bideratzeko. Mezuak hainbat ordenagailutatik pasatzeak zaildu egiten du atzerakako aztarnatzea, baina Tor-ek, gainera, lortzen du bideko ordenagailu edo nodo horietako batek ere ez ezagutzea mezua bera eta mezuaren jatorria eta helburua; nodo bakoitzak aurreko nodoa eta ondokoa zein diren soilik ezagutzen du, ez daki bera bide horretako zenbatgarren nodoa den, eta ezin du mezua irakurri. Nola lortzen da hori? Berriz ere, gako publiko bidezko kriptografiaz.

Sortako aurreko artikuluetan esan bezala, gako publiko bidezko kriptografian mezu bat kodetu edo zifratzen da jasotzaileak edonoren esku jarri duen bere gako publikoaren bidez, baina ezin da mezua bueltan deszifratu gako horren bidez, jasotzaileak soilik dakien gako pribatu baten bidez baizik; hala, jasotzaileak soilik irakurri ahal izango du mezua.



TIPULA-ZIFRAKETA

Tor erabiltzen dugunean mezu bat bidaltzeko, software horrek egiten duen lehen gauza da Tor sarea osatzen duten ordenagailuetatik hainbat ausaz hartuta bide bat aukeratu. Ondoren, bide horretako azken nodoaren gako publikoa erabilita zifratzen ditu mezua eta mezuaren azken helburua. Gero, jada zifratuta dagoen mezu hori guztia eta bideko azken nodoaren helbidea zifratzen ditu, bideko azken aurreko nodoaren gako publikoa erabilita. Eta horrela egiten du atzeraka bideko nodo bakoitzarekin: nodoaren gako publikoaren bidez zifratzen dira aurrez zifratuta dagoen mezu guztia eta hurrengo nodoaren helbidea.

Dena prest duenean, bideko lehenengo nodoari bidaltzen dio mezua; han dagoen Tor softwareak bere gako pribatuaren bidez deszifratzen du mezua, hurrengo nodoaren helbidea lortzen du hala, eta geratzen den mezua hari bidaltzen dio; hurrengoak gauza bera egiten du, deszifratu, hurrengo helbidea lortu eta hari pasatu; eta horrela amaieraraino. Ikusten denez, bideko nodoek ez dakite aurrekoa eta ondokoa zein diren baino, beste ezer ezin dute jakin, guztia berek ez dituzten gakoen bidez zifratuta baitoa. Eta hartzaileak edo mezua bidean atzeman duen edozeinek jakin nahiko balu zein den jatorria, gako publiko bidezko kriptografiaren hainbat geruza deszifratu beharko lituzke; eta, esan genuen bezala ezinezkoa bada gaur egungo bitartekoekin kriptografia mota hori haustea, pentsa horrelako hainbat geruza.

Beraz, hortik datorkio *tipula bideratzaile* izena metodo honi: mezuak, tipulak bezala, bata bestearen gaineko hainbat zifraketa-geruza dauzka eta bidean geruza horiek deszifratuz edo kenduz doaz.

Mezu baten edukia, helburua edo jatorria zein den jakiteko modu bakarra infiltratzea izan daiteke (ordenagailu *satorrak* sartzea Tor sarean) edo nodoen kontrola lortzea. Baina Tor sarean ordenagailu asko daude, eta bide luze samarrak egiten dira; beraz, bideko nodo guztiak satorrak edo kontrolatuak izatea ezinezkoa da praktikan.

Bestalde, Tor konfiguratu dezakegu bideko azken nodoa herrialde jakin batekoa izan dadin; horrela gaindi daiteke webgune batzuek herrialde batzuekiko duten zentsura (maiz herrialdeko gobernuak bere herrikideei inposatua), edo onlineko eduki kultural edo audiobisual batzuei ezartzen zaizkien ustiaketa-leiho geografikoak.

Egun, Tor da anonimotasun-bermerik handiena lortzen duen tresna, eta edonoren esku dago. Eta egia da legez kanpoko kontuetan aritzeko ere erabil daitekeela. Horregatik (edo, agian, horren aitzakian), herrialde batzuek Tor-en erabilera debekatu egin nahi dute (Japoniak, adibidez). Lortuko balute, beste erabilera zilegi eta beharrezko asko ezinezko bihurtuko lirateke. Eta ez dira debekatzen autoak edo armak, bankuak lapurtzeko erabiltzen direlako…●

“Gaur egun, Interneten anonimotasunez aritzeko modurik seguruena eta edonoren eskura dagoena Tor erabiltzea da”