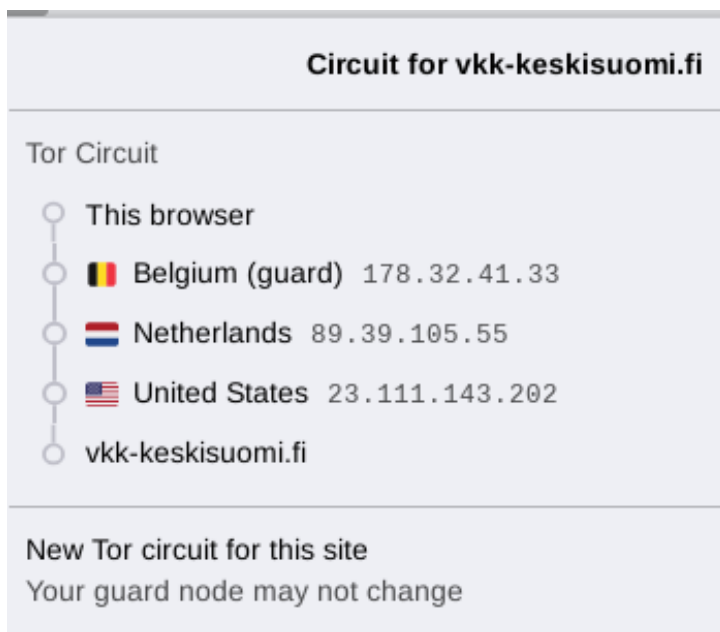


Tor-verkko, kenen palveluksessa olet?

Testasin näitä vkk-keskisuomi.fi sivuja tor-selaimella jolla kytkeytyminen vkk-keskisuomi.fi web-serverille tapahtuu kolmen satunnaisesti valitun välipalvelimen kautta.

Esimerkiksi:



Kuva 1: Esimerkki tor-verkon serveriketjusta.

Alkuun sivut toimivat normaalisti, mutta sitten sivut yhtäkkiä hajosivat oudosti. Tutkin web-palvelimen logia ja sen mukaan viimeinen serveri, johon vkk-keskisuomi.fi web-serveri oli yhteydessä, oli IP-osoitteessa 192.42.116.182, jonka omistaa Mitre niminen yritys. Tämän saa helposti selville <https://dnslytics.com/> sivuilla.

Mutta tämä IP ei ollut sen serverin osoite, joka käytetyn tor-selaimen mukaan olisi pitänyt olla. Selaimen mukaan serveri sijaitsi Saksassa, jonka IP oli jotain aivan muuta.

Mikä mahtaisi olla selitys? Se, että sen Saksassa sijaitsevan serverin oli asettanut Mitren organisaatio osaksi tor-verkoa. Tämän pystyy tekemään kuka tahansa ilmoittamalla serverinsä tor-verkon välityspalvelimeksi. Myös poliisi tekee tätä samaa, metsästäessään vaikkapa huumekauppiaita. Koska tor-serverit valitaan arpomalla satunnaisesti kaikkien saatavilla olevien servereiden joukosta, on huonoa säkää jos oma tietoliikenne sattuu kulkemaan tällaisen ansa-severin kautta. Tämä ansa-serveri sitten kytkeytyy johonkin viranomaisserveriin tai yrityksen serveriin joka sitten kytkee oman serverinsä siihen serveriin, johon olit ottamassa yhteyttä. Ketjussa on nyt neljä serveriä, josta tuo neljäs, viranomais/yritys serveri voi seurata tosiaikaisena sinun tietoliikennettäsi ja mitä siellä tapahtuu. Jos yhteys ei ole salattu (http), niin myös kaikki data on avoimena luettavissa. Pystyvätkö he purkamaan kryptauksen? En tiedä, mutta jos niillä on kvanttietokoneet käytössä, pystyvät.

Avainkysymys kuuluukin: pystyvätkö viranomaiset/yritykset valituttamaan oman serverinsä haluamallaan tavalla osaksi tuota kolmen serverin ketjua. Jos pystyvät, tor-verkko pitää kiertää kaukaa. Toivon hyvin, hyvin, HYVIN hartaasti, että tämä ei ole mahdollista!

Tapaus vkk-keskisuomi.fi kertauksena: Tor-serveri, joka ei siis kytkeytynyt suoraan vkk-keskisuomi.fi web-serverille, vaan Mitren omalle serverille, jonka IP on yllä. Mitreltä sitten on kytkeydytty vkk-keskisuomi.fi serverille, mutta mainituin huonoin tuloksin. Siis vkk-keskisuomi.fi sivut tekivät ylimääräisen kiekän Mitren toimitiloissa, jossa sivuille on tehty jotain ja jotka sitten on lähetetty käyttämälleni tor-selaimelle mutta paljastavasti ”särkyneenä”. Kun vaihdoin tor-selaimen käyttämiä servereitä, sivut korjautuivat kuin taikauskusta normaaleiksi.

Mikä sitten on Mitre? Se on hämärän oloinen iso monialayritys, joka toimii USA:n viranomaisten kanssa yhteistyössä fokuksena (katso kuva) esimerkiksi kotimaan turvallisuus, tietoturvallisuus ja tekoäly. Kyseessä on siten puhtaasti viranomaisvakoilusta. Nyt ne jäivät kiinni housut kintuissa. Tosin poliisin menetöt olivat jo tiedossa ja kuka tahansa valistunut ihminen olisi voinut valistaa, että jotain tällaista on tapahtunut ja tulee tapahtumaan. Vieläpä koko ajan ja kaikkialla.

Koska kaikkien valtioiden salaiset- ja turvallisuuspalvelut toimivat kiinteässä yhteistyössä keskenään ilman rajoja, myös Suomen viranomaiset saavat tiedon, jos USA:n päässä päätellään, että tässä on jotain epäilyttävää meneillään.

Lisää Mitrestä sen sivustolta mitre.org.