ASEVARUSTELUA VERKOSSA

RISTO K. JÄRVINEN

Skepsiksen rivijäsen, F-Securen tutkimusjohtaja Mikko Hyppönen kertoi Skepsiksen luennolla Tieteiden talolla syyskuussa, että suojautuminen verkossa on nykyään yhä vaikeampaa, mutta ei mahdotonta.

MIKKO HYPPÖNEN kertoi, että ”lerppujen” ja ”korppujen” kautta leviävät virukset olivat oikea ongelma 1980-luvun lopussa ja 1990-luvun alussa ennen kuin internet ja sähköposti yleistyivät. Viruksia ei silloin otettu vakavasti. Niiden olemassaoloa ja ajatusta, että ne leviävät tietokoneesta toiseen, pidettiin urbaanina legendana.

Lerppujen ja korppujen aikakauden jälkeen virukset alkoivat levitä netin kautta: tutuiksi tulivat ensin sähköpostimadot ja sitten verkkomadot, webbimadot, exploit kitet, pankki- ja lunnastroijalaiset sekä bitcoin mining -hyökkäykset. Tekninen muutos ja murros on ollut todella iso.

Vielä suurempi muutos on ollut se, ketä vastaan tiedon turvaajat taistelevat.

- Silloin, kun aloitin alalla, hyökkääjät oli helppo määritellä. He olivat kaikki teinipoikia, jotka kirjoittelivat viruksia huvikseen, Hyppönen sanoi.

Tällaisia täysin pyyteettömiä harrastelijahyökkääjiä ei nykypäivänä enää ole. Tänään kaikilla hyökkääjillä on motiivi, eli he hyötyvät teoistaan jollain lailla. Tärkein ryhmä on rikolliset, jotka tekevät verkkomadoilla, troijalaisilla tai muilla haittaohjelmilla rahaa. Toki pyyteettömiäkin hyökkääjiä on, esimerkiksi erilaiset aktivistiryhmät, joiden motiivina on yleensä protesti.

Verkossa esiintyy myös hyökkäyksiä, joiden takana on valtiovalta. Tämän vuoden alusta Suomen poliisilla on ollut oikeus kirjoittaa ja käyttää viruksia rikoksia tutkiessaan. Samoin tekevät myös eri maiden tiedusteluorganisaatiot ja armeijat.

Kaikkein uusin, vielä syntymässä oleva ääriryhmä, ovat terroristit. Minkäänlaista todellista kyber-terrorismia emme ole Hyppösen mukaan kuitenkaan vielä nähneet, mutta yhä lähemmäs sitä koko ajan menemme. Ääriryhmistä löytyy koko ajan enemmän ihmisiä, joiden osaaminen riittää verkkohyökkäysten tekemiseen. Heidän päämotiivinsa on aiheuttaa tuhoa ja kaaosta, ei saada rahallista tai vakoiluhyötyä.

- Suurin yllätys minulle on ollut, että valtiot ovat tulleet kuvioon mukaan. Nykyään normaalit, kehittyneet länsimaiset valtiot kirjoittavat viruksia, takaportteja sekä troijalaisia haittaohjelmia ja käyttävät niitä aktiivisesti muita demokraattisia länsimaita vastaan.

Verkkorikosten tekeminen on helppoa ja halpaa. Valtaosa verkkorikollisista ei jää koskaan kiinni ja vaikka he jäisivätkin kiinni, niin todennäköisyys saada tuomio ja joutua vankilaan on Hyppösen mukaan edelleen liian pieni.

- Meidän pitäisi paremmin pystyä osoitamaan, että verkkorikos ei kannata.

Suomessa on helppo saada töitä, jos osaa koodata ja ymmärtää verkkoprotokollia, mutta jos asut Siperian perämetsissä tai Brasilian slummeissa, työnsaanti ei ole niin helppoa. Tästä seuraa, että verkkorikosten tekijöitä löytyy yhä enemmän kehittyviltä alueilta.

Tällä hetkellä koko Afrikan alueen verkkokaista on suunnilleen yhtä suuri kuin Suomen verkkokaista. Tämä on muuttumassa kovaa vauhtia. Pian Afrikka on linjoilla ihan yhtä laajasti kuin koko muukin maailma. Koska kyseessä on alue, jossa on paljon nuoria osaajia, mutta ei yhtä paljon tilaisuuksia, saattaa Afrikasta tulla seuraava iso verkkorikosaaalto.

EMME TOTTELE POLIISIA

Viruksiin liittyy paljon salaliittoteorioita ja epäilyjä. Yksi asia, mihin Hyppönen joutui yli kymmenen vuotta sitten usein vastaamaan, oli väite jonka mukaan virustorjuntafirmat itse kirjoittavat virukset ja sitten myyvät niihin torjuntaohjelmat.

- Enää en kuule väitettä oikeastaan koskaan.

90-luvulla ihmiset tiesivät, että haittaohjelmia ja viruksia on, mutta he eivät tienneet, mistä ne tulevat, miksi niitä tulee ja kuka niistä hyötyy. Tällöin oli helppo päätellä väärin, että viruksista hyötyvät virustorjuntafirmat. Tänä päivänä kaikki tietävät, että netissä on rikollisjengejä, jotka ansaitsevat vääryydellä miljoonia. Enää ei tarvitse keksiä verkkohyökkäyksille tekijöitä ja motiiveja.

Eräs epäily on, kuinka luotettavia ovat eri maista käsin toimivat virustentorjuntafirmat niiden haittaohjelmien kohdalla, joita heidän oma hallituksensa kirjoittaa. F-Secureen tuli vuosi sitten kirje hollantilaiselta sananvapausorganisaatiolta ”Bits of Freedom”, jossa kysyttiin onko heihin koskaan ollut yhteydessä meidän oma valtiovaltamme tai jonkun muun maan valtiovalta ja pyytänyt jättämään tunnistamatta jotain määrättyjä haittaohjelmia. Toinen kysymys kuului, että jos näin on käynyt/kävisi, mitä F-Secure vastaisi.

- Vastauksemme oli helppo: kukaan ei ole ottanut meihin yhteyttä ja jos olisi ottanut, vastauksemme olisi ollut ei.

Jos esimerkiksi Keskusrikospoliisi ottaisi F-Secureen yhteyttä ja pyytäisi jättämään tunnistamatta heidän kirjoittamansa haittaohjelman, yritys ei tottelisi. Sen tehtävä on yksinkertainen: pysäyttää haittaohjelmat. Firman asiakkaat ostavat tuotteita pysäyttääkseen haittaohjelmia riippumatta siitä, mistä haittaohjelmat tulevat. Jos Suomen poliisille sanottaisiin kyllä, niin seuraavaksi saattaisi tulla puhelu Ruotsista ja sitten Saksasta, Ranskasta, Italiasta, Israelista, Syyriasta...

Bits of Freedom lähetti kyselyn monelle muullekin alan firmaille – yli puolet niistä eivät ole vastanneet kyselyyn.

- Suojautumistaistelu käy koko ajan vaikeammaksi, mutta meillä ei ole mitään tarkoitusta luovuttaa.

Kaikkein suurin toivo suojausjärjestelmien suhteen Hyppösellä on liittyen järjestelmiin, jotka eivät yritä suojata mitään tiettyä uhkaa vastaan, vaan kokonaisia hyökkäysluokkia vastaan. Hän mainitsee ”digitaalisen judon”, jossa käytetään hyökkääjän voimaa hyökkääjää itseään vastaan. Mitä enemmän hyökkääjät pyrkivät salaamaan omaa haittaohjelmaansa, sitä helpommin tunnistettavaksi se tulee, koska se on silloin välttämättä yksilöllinen.

- Me pystymme taistelemaan myös tällaisia vastaan.

Katso ja kuuntele luento kokonaisuudessaan: youtube.com/user/SkepsisFinland