STUDIA GENERALIA 2010
TIETO MUUTTUVASSA MAAILMASSA

4.11.2010 TIETOTURVA JA TIETOSOTA

TILANNEKATSAUS TIETOTURVATILANTEESEEN

Tutkimusjohtaja Mikko Hyppönen, F-Secure Oyj

Tietokonevirusten määrän kasvu jatkuu hälyttävällä tahdilla. Jättimäisiä epidemioita nähdään yhä harvemmin, mutta ongelmat eivät ole helpottaneet. Hyökkäysten takana toimivat nykyään harrastelijoiden sijaan ammattilaiset, jotka eivät halua aiheuttaa liian suuria epidemioita välttääkseen turhan huomion.

Uusien haittaohjelmien määrä ei ole koskaan ollut näin suuri. F-Securen tutkimuslaboratorio vastaanottaa yli sata tuhatta haittaohjelmanäytettä joka päivä.

Vaikka viruksia luodaan enemmän kuin koskaan aiemmin, monet ihmiset sanovat törmäävänsä niihin entistä harvemmin. Yksi selitys tälle illuusiolle on se, että haittaohjelmien tekijät muuttavat jatkuvasti keinoja, joilla virukset tunkeutuvat tietokoneisiin.

Ylivoimainen valtaosa nykyisistä haittaohjelmatapauksista voidaan luokitella taloudellista hyötyä tavoitteleviksi. Nämä virukset liittyvät joko roskapostin lähettämiseen, phishing-hyökkäyksiin, hajautettuihin palvelunestohyökkäyksiin tai tietovarkauksiin. Tyypillinen loppukäyttäjää koskettava ongelma ovat haittaohjelmat jotka sisältävät näppäimistönauhurin. Näppäimistönauhuri (keylogger) nauhoittaa saastuneella koneella kaiken, mitä käyttäjä koneellaan naputtelee ja lähettää sen haittaohjelman tekijälle. Näin käyttäjän salasanat ja vaikkapa sähköpostit päätyvät vääriin käsiin. Suurin ongelma on kuitenkin henkilötiedot ja luottokorttinumerot jotka käyttäjä syöttää tehdessään ostoksia verkkokaupassa. Suomessa nähdään jatkuvasti tapauksia joissa haittaohjelmilla viedyillä luottokorttinumeroilla on tehty petoksia.

Valtaosa kaikesta sähköpostista on nykyään roskapostia – ja suurin osa siitä tulee saastuneiden kotikoneiden kautta. Kun roskapostin lähettäjät ansaitsevat mukavasti rahaa roskapostilla, he voivat investoida toimintaansa – ja ongelma vain kasvaa.

Mobiiliuhat

Kiinnostus mobiililaitteiden haittaohjelmia kohtaan kasvaa jatkuvasti. Kännykkäviruksia oli vuoden 2010 lopulla tiedossa yli 500 kappaletta.

Suurin osa mobiililaitteiden haittaohjelmista on Symbian-päätelaitteille suunnattuja. Mielenkiinto Symbian-ympäristöä kohtaan on osoitus Symbian-laitteiden suosiosta, sillä haittaohjelmien kirjoittajia kiinnostaa juuri laaja käyttäjäkunta. Suomalainen Nokia on Symbian-käyttöjärjestelmän suurin käyttäjä ja myös omistaja.

Kaikki tunnetut Symbian-ympäristön troijalaiset ja madot näyttävät useita varoituksia jo niiden asennuksen aikana, joten haittaohjelmatartunnat olisi helppo panna käyttäjien osaamattomuuden ja välinpitämättömyyden piikkiin. Tavat, joilla Cabir-mato ja muut Bluetooth-madot leviävät, osoittaa kuitenkin, että syyt eivät ole näin yksiselitteiset. Suurimpana uhkana kännykkäpuolella pidetään kuitenkin tällä hetkellä mobiilivakoojasovelluksia, ei niinkään mobiiliviruksia.

Ensimmäiset haittaohjelmat uudemmille mobiilialustoille kuten iPhone ja Google Android on jo nähty.

Yhteenveto

Loppujen lopuksi kysymys on kuitenkin verkkorikollisuudesta. Modernin yhteiskunnan on pystyttävä suojaamaan toimintansa tämän tyyppistä rikollisuutta vastaan.

Verkkorikollisuus ei oikeastaan olekaan tekninen ongelma, vaan sosiaalinen ongelma. Pitkällä tähtäimellä ongelmaan voidaan vaikuttaa koulutuksella ja kansainvälisellä lainsäädännöllä. Ongelmana tässä onkin se, että internet on kansainvälinen. Virustenkirjoittajat, tietomurtajat ja verkkohyökkääjät kyllä osaavat kierrättää tekosensa maasta toiseen, tehden rikosten tutkinnasta vaikeaa tai mahdotonta. Tämän lisäksi valtioiden lainsäädännöissä on huomattavia eroja, tehden rikollisten syyttämisen vaikeaksi.

Tietoturvatilanne näyttää parantuvan, koska jättimäisiä globaaleja virusepidemioita on yhä harvemmin. Tämä on kuitenkin silmänlumetta. Todellisuudessa kyse on siitä, että taloudellista hyötyä tavoittelevat hyökkääjät suuntavat hyökkäyksensä paremmin ja tekevät enemmän pieniä hyökkäyksiä jättimäisten hyökkäysten sijaan. Näin heidän tekonsa pysyvät paremmin piilossa.

Tilanne siis näyttää paranevan vaikka se itse asiassa huononee koko ajan.

Lisätietoja:
www.f-secure.com/weblog
twitter.com/mikkohypponen

Studia Generalia -tilaisuudet videoidaan. Niitä voi seurata internetissä sekä suorina lähetyksinä että tallenteina: www.helsinki.fi/videot. Tilaisuuden jälkeen on mahdollista käydä blogi-keskustelua luentojen aiheista osoitteessa: http://blogs.helsinki.fi/studiageneralia/. Luentosarjan on suunnitellut Helsingin yliopiston Studia Generalia -toiminnan tieteellinen ohjausryhmä ja sen toteuttaa Helsingin yliopiston Avoin yliopisto.

Kevätlukukauden 2011 Studia Generalia -luentosarjan teema on IKÄ JA TERVEYS, ja sen ohjelma julkaistaan Studia Generalia -verkkosivuilla joulukuussa 2010. Luentosarja alkaa torstaina 3.2.2011.

Lisätietoja:
Tieteellisen ohjausryhmän puheenjohtaja,
vararehtori Kimmo Kontula
p. (09) 191 24150
kimmo.kontula@helsinki.fi

Koulutussuunnittelija
Sanna Saari-Salomeri
p. (09) 191 28047
studiageneralia@avoin.helsinki.fi