HS

Politiikantoimitus
hs.politiikka@hs.fi +358 9 122 2533
Kotimaantoimitus
hs.kotimaa@hs.fi +358 9 122 7575

Aurinko

Helsinki	Oulu	Utsjoki
↑ 3.55	2.22	17. toukokuuta
↓ 22.47	0.16	27. heinäkuuta

KOTIMAA

Verkkovakoilu yksinkertaistettuna

1 Käyttäjä klikkaa linkkiä

Käyttäjiin kohdistetaan isku, jossa käyttäjä saadaan lataamaan liitetiedosto tai klikkaamaan linkkiä. Vaihtoehtoisesti käyttäjä saadaan asettamaan koneelleen haluttu USB-tikku.

2 Yksi kone saastuu

Hyökkääjä pääsee käyttäjän koneelle ja siten myös järjestelmiin, joihin käyttäjällä on pääsy.

3 Saastunut kone saastuttaa muita

Haittaohjelma voi vaikkapa varastettujen salasanojen kautta uida koko kohdeorganisaation tietojärjestelmiin.

4 Tiedonkeruu käynnistyy

Haittaohjelma kerää informaatiota. Vaihe voi kestää kuukausista jopa yhdeksään vuoteen, kuten kuun alussa havaitun NetTraveler-ohjelman tapauksessa. Se oli laskettu liikkeelle 2004.

5 Varastettu tieto analysoidaan

Ohjelma välittää datan ulkopuoliselle palvelimelle tutkittavaksi ja analysoitavaksi. Vaihe kestää yleensä siihen asti, kunnes vakoilu paljastuu.

Koonnut: LAURA HALMINEN HS, grafiikka: JOONAS JANSSON HS

Verkkoja vakoillaan joka päivä

Hyökkäykset kohdistuvat Suomen valtionhallintoon, puolustusteollisuuteen ja teknologiayrityksiin

Valtiollisiin organisaatioihin kohdistuu enemmän verkkohyökkäyksiä kuin yritysmaailmaan. Kaikkia ei välttämättä edes huomata. Tavoitteena on yleensä laiton tiedonhankinta.

Laura Halminen HS

SUOMEN turvallisuuden kannalta tärkeitä toimijoita vastaan tehdään verkkohyökkäyksiä joka päivä.

Tyypillisesti hyökkäyksen tavoitteena on laiton tiedonhankinta eli suomeksi vakoilu. Tavallisia kohteita ovat valtionhallinto, puolustusteollisuus ja teknologiayritykset.

”Valitettavasti hyökkäykset ja vakoilu ovat nykyään arkipäivää”, toteaa turvallisuuskomitean pääsihteeri, eversti **Aapo Cederberg**.

”Se on tällä hetkellä Suomessa liian helppoa.”

Ensimmäiset havainnot verkkovakoilusta Suomessa on tehty jo vuonna 2004.

Helsingin Sanomien tietojen mukaan Suomessa on sattunut lukuisia vakoilutapauksia, joissa organisaatiosta on haittaohjelmien avulla varastettu gigatavuittain tietoa ennen kuin hyökkäystä on edes havaittu.

Kaikkia hyökkäyksiä ei välttämättä koskaan huomata.

TILASTOTIETOA verkkovakoilusta on hankalaa saada, sillä taitavat hyökkääjät välttävät kiinni jäämistä ja osaavat naamioida jälkensä jopa muistuttamaan toisten valtioiden käyttämiä keinoja.

Helsingin Sanomien saamien tietojen mukaan valtiollisiin organisaatioihin kohdistuu kuitenkin enemmän hyökkäyksiä kuin yritysmaailmaan. Osansa ovat saaneet myös Suomesta käsin toimivat sananvapausjärjestöt, kuten Tiibetin itsenäisyyteen keskittyvä liike.

Yhdysvaltojen ja Israelin yhteistyössä rakentama Stuxnet-haittaohjelma puolestaan saastutti Iranin ydinlaitoksen 2010. Suomessa Stuxnetista tehtiin tietoturvaviranomainen Cert-fille yhteensä seitsemän raporttia. Valtaosa ohjelman hyökkäyksistä onnistuttiin estämään.

Tammikuussa löydetystä, oletettavasti Venäjältä peräisin olevasta Red October -haittaohjelmasta on tehty muutamia havaintoja.

”Emme ole vakoilun suhteen maailmanpolitiikan polttopisteessä kuten vaikka Israel ja USA. Mutta varautumisen lähtökohta on se, että painopisteet voivat muuttua”, Cederberg selventää.

”Tiedon turvaamisessa pitää ottaa huomioon, mikä on kriittistä tietoa. Maailma ei kaadu siihen, että NSA:n palvelimilla on paljon tietoa, vaikka se kiusalliselta tuntuisikin.”

SUOMESSA ON Stuxnetin ja venäläislähtöisen Red Octoberin ohella havaittu myös Kiinan verkkovakoilua. Maassa toimivien Saksan, Ranskan, Yhdysvaltojen ja Britannian tiedustelujen verkkovakoilusta ei HS:n tietojen mukaan ole toistaiseksi havaittu näyttöjä. Sen sijaan kiinalaisten verkkovakoilutaktiikkaa kuvaillaan ”brutaaliksi”. He tulevat ja ottavat haluamansa välittämättä, jääkö siitä jälkiä.

Venäläisten taktiikat ovat hienostuneempia ja teknisesti hyvin monimutkaisia, mutta jopa romanialaiset harrastajat ovat onnistuneet kohdistetuissa vakoiluhyökkäyksissä suomalaisiin yrityksiin.

”Liikumme yhä liian vähän tiedon varassa”, toteaa Cert-fin johtaja **Erka Koivunen**.

”Hyökkäyksen tai sen uhan havaitsemisen jälkeen kuulemme kohteelta harvoin mitään.”

Tilanne on Koivusen mukaan huolestuttava, sillä Cert-fin mahdollisuudet tutkia ja auttaa ovat heikot, jos tietoa ei jaeta. Cert-fi on pitkälti ulkomaisten kollegojen lahjoittaman tiedon varassa.

”Hyökkäysten tekijät ovat kovia teknisiä osaajia, joilla on selkeä toimeksianto. Ei ole sattumaa, että tiettyjä organisaatioita jahdataan”, Koivunen sanoo.

TAUSTA

Tiedonjako auttaa torjunnassa

VERKKOVAKOILUUN varautuminen on vaikeaa, mutta kriittisten kohteiden suhteen auttaa Huoltovarmuuskeskuksen koordinoima Havaro-havaintojärjestelmä.

”Se seuraa verkkoliikennettä automatisoiduilla sensoreilla ja yhdistelee tietoa tästä kohinasta”, kuvailee Huoltovarmuuskeskuksen infrastruktuureista vastaava johtaja **Sauli Savisalo**. Sensoreita on muutaman kymmenen organisaation tiloissa.

”Kohinasta löydetään ja jaetaan varoituksia vajaalle kahdelle tuhannelle organisaatiolle. Näiltä organisaatiolta olen saanut palautetta, että verkkovakoiluakin on onnistuttu järjestelmän avulla ehkäisemään.”

Järjestelmää rahoittavat Huoltovarmuuskeskus sekä organisaatiot, joiden tiloissa sensoreita sijaitsee.