Lehdistötiedote

F-Secure Oyj
PL 24
FIN-00181 HELSINKI
Tel. +358 9 2520 0700
Fax. +358 9 2520 5001
http://www.F-Secure.com

JULKAISTAVISSA 18.12.2001

F-Securen vuoden 2001 tietoturvayhteenveto

Vuosi 2001 on ollut tähänastisesti vilkkain tietoturvatapahtumiltaan

Perinteisistä viruksista monimutkaisiin verkkomatoihin

Virusmaailma on selkeästi muuttumassa. Monet uudet vuonna 2001 käytetyt tekniikat hyödynsivät perinteisiä hakkerointimenetelmiä, kuten ohjelmien tunnettuja turvaukkoja. Code Redin kaltaiset madot ovat hankalia pysäyttää perinteisillä virustentorjuntaohjelmilla, koska ne eivät saastuta tiedostoja. "Ratkaisu näyttäisi olevan perinteisen virustentorjuntaohjelman ja palomuurin toimintojen yhdistäminen, mikä silloin tuottaisi turvan sekä viruksia, hakkerointia, että näiden yhdistelmiä vastaan", sanoo Mikko Hyppönen, F-Securen tutkimuspäällikkö.

Sekä kokeneet että aloittelevat internetin käyttäjät kohtasivat todelliset tietoturvauhat vuonna 2000, mikä lisääntyi vuoden 2001 aikana. Vuoden 2001 aikana viruksia löydettiin keskimäärin viisi päivässä, ja Hyppösen mukaan vuoden loppuun mennessä niiden yhteismäärä oli 59 000. Tämä luku kattaa vain ne, jotka löydettiin ja raportoitiin.

Nimda-mato

Luultavasti tuhoiltaan pahamaineisin virus vuoden aikana oli sähköpostimato Nimda; ensimmäinen Internetvirus, joka otti hallintaansa web-sivustoja levitäkseen. Leviten neljällä eri tavalla Nimda saastutti 2,5 miljoonaa tietokonetta, tukkien suuriakin lähiverkkoja aiheuttamansa suuren verkkokuorman takia. "Meillä ei ole mitään tietoa mistä Nimda on lähtöisin. On löydetty viittauksia Kiinan suuntaan, mutta ne voivat olla tekaistuja", Hyppönen kommentoi. "Mistä tahansa se alunperin onkin, se on luultavasti useamman ihmisen kirjoittama". Tällaisen madon kehittämiseen ja testaamiseen tarvitaan testauslaboratorio, lähiverkko,palvelimia ja reitittimiä. Viruksen kehittämisen ajallinen ja rahallinen panostus herättää kysymyksen viruksen kirjoittajien motiiveista.

Suuri osa Nimdan ja myöhemmin löydetyn madon, BadTransin aiheuttamista tuhoista olisi ollut ennalta ehkäistävissä. Saatavilla olevien kaupallisten virustentorjunta-tuotteiden lisäksi myös Microsoft varoitti useista heikkouksista sovelluksissaan ja tarjosi ilmaisia korjauksia niihin. Moni käyttäjä kuitenkin tuudittautui väärään turvallisuuden tunteeseen.

Virustentorjujat eivät silti jääneet ilman voittojakaan. Anna Kournikova -viruksen hollantilainen kirjoittaja ja ryhmä israelilaisia teinejä, jotka tekivät Goner-viruksen,

jäivät kiinni ja heidät luovutettiin virkavallan haltuun. "Ainoa tapa, jolla voimme voittaa, on ottamalla tekijät kiinni ja osoittamalla maailmalle, että virusten kirjoittaminen on rikos, josta jää kiinni", Hyppönen sanoo.

Toisesta petostapauksesta selvisi, että viruksia oli jaettu sähköpostipalvelimien kautta. Suurin osa tällaisten palvelimien käyttäjistä, kuten musiikkikerhojen ja muiden yhdistysten, avaavat sähköpostinsa palvelimilla, koska luottavat niiden sisältöön. Jo ensimmäisen kuukauden aikana, jona F-Securen suojausohjelmaa testattiin, L-Soft raportoi ohjelman pysäyttäneen yli 100 000 virusta n. 630 isännöimällään sähköpostilistalla.

Suurin osa vuoden tietoturvaongelmista kohdistui Microsoftin käyttöjärjestelmään, mutta myös muita käyttöjärjestelmiä kohtaan hyökättiin. Tammikuussa kirjoitettiin ensimmäinen laajasti levinnyt Ramen-niminen Linux-mato ja toukokuussa Sadmin-mato saastutti Solaris-pohjaisia Unix-käyttöjärjestelmiä. Kesäkuussa Mac.Simpsons-mato levisi Macintosh-käyttöjärjestelmässä.

Tulevaisuuden näkymät

Samaan aikaan vastaanotettiin innolla Microsoftin uusin kämmentietokone, Pocket PC 2002. Langattomien laitteiden lisääntyvän kasvun myötä yritysten sähköpostiliikenne ja luottamukselliset tiedot ovat yhä alttiimpia varkauksille ja väärinkäytölle. Pocket PC 2002:n myötä on ennustettavissa täysin uusi langattomien laitteiden sukupolvi. Monet näistä ovat kämmentietokoneita ja uusina laitteina tuovat mukanaan myös täysin uudenlaiset tietoturvauhat.

"Tammikuussa 2002 niiden aiheuttamat tietoturvariskit moninkertaistuvat, kun joululahjaksi saadut kämmentietokoneet otetaan käyttöön ja niihin siirretään tietoa varsinaisilta työkoneilta. Tietoa voidaan salakuunnella ja varastaa. Virustentorujunnan ja tiedostonsalauksen tulee kattaa yritysten kaikki IT-laitteet", toteaa Anthony Gyursanszky, Johtaja, Wireless Security Solution Unit, F-Secure Oyj.

"Valitettavasti tulevaisuus ei näytä yhtään valoisammalta", Hyppönen sanoo."Nettihäiriköt jatkavat tuhotöitään kiihtyvällä tahdilla". Ennakoituaan jatkuvan aktiviteetin tällä rintamalla, F-Secure nosti virustentorjuntaohjelmansa päivitykset kahteen kertaan päivässä, joka on oletettavasti alan yleisin päivitystahti.

On oletettavissa, että tietoturvahyökkäykset tulevat lisääntymään ja ne tulevat yhä ammattimaisemmiksi. On yhdentekevää edustavatko niiden tekijät terroristiryhmiä, järjestäytyneitä rikollisia tai muita järjestäytyneitä tahoja. Pääasia on, että tietokoneistuneen yhteiskunnan on pystyttävä toimimaan haavoittumatta hyvin vahingollisisista tietoturvahyökkäyksistä huolimatta.

Suurimmat virustapaukset vuonna 2001

Tammikuu: Hybris
Tammikuu: Matrix (MTX)
Helmikuu: Anna Kournikova
Maaliskuu: Magistr
Toukokuu: Homepage
Heinäkuu: Sircam
Heinäkuu: Code Red

Syyskuu: Nimda
Marraskuu: BadTrans
Joulukuu: Goner

Tarkempia tietoja yllämainituista viruksista löytyy osoitteesta
http://www.f-secure.com/v-descs/

F-Secure Oyj

F-Secure Oyj on suomalainen yritys, joka toimittaa keskitetysti hallittavia tietoturvaratkaisuja. F-Securen tuotevalikoima sisältää palkittuja, keskitetysti hallittuja virustentorjunta-, tiedosto- ja verkkosalaus- sekä hajautettuja palomuurituotteita yritysten kaikille keskeisille laitealustoille työasemista, verkkolaitteisiin ja palvelimista langattomiin taskutietokoneisiin.

F-Securen tuotteet sopivat tietoturvan toimittamiseen myös automaattisena palveluna. Palvelu tarjoaa luotettavan, aina toimivan ja ajanmukaisen tietoturvan hajautetulle käyttäjäkunnalle. F-Securen tuotteet ja ratkaisut voidaan toimittaa asiakkaiden omien IT-osastojen tai palveluntarjoajien kautta. Ratkaisujen avulla turvakäytäntöpohjainen tietoturva ja tarvittavat hälytykset saadaan kaikkiin laitteisiin, joilla tietoa luodaan ja tallennetaan tai joilta tietoa haetaan. Vuonna 1988 perustettu F-Secure Oyj on noteerattu Helsingin pörssissä. Yhtiön pääkonttori on Helsingissä ja Pohjois-Amerikan yhteystoimisto San Josessa. Yhtiöllä on lisäksi toimistoja eri puolilla maailmaa.

Lisätietoja:

Mikko Hyppönen, Virustentorjuntayksikön päällikkö
F-Secure Oyj
PL 24
00181 Helsinki
Puh. 09 2520 5513
Fax +358 9 2520 5001
Gsm +358 400 648 180
Sähköposti: Mikko.Hypponen@F-Secure.com

http://www.F-Secure.com