

Koneen käyttäjiä kiusataan hienostuneemmin

21.3.2005 16:41 — Tuomas Karvonen

Tietoturvayhtiö Symantecin tänään julkaistu Internet Security Threat -raportti osoittaa tietoturvahyökkääjien kehittyneen entistä taitavammiksi pääsemään käsiksi yritysten ja yksityisten koneen käyttäjien luottamuksellisiin tietoihin.

Seitsemännen kerran julkaistu puolivuositainen raportti analysoi tietoturvahyökkäysten trendejä, haavoittuvuuksia, haittakoodia ja muita tietoturvauhkia viime vuoden jälkipuoliskon ajalta.

- Tietoturvahyökkäykset ovat muuttuneet entistä hienostuneemmiksi pyrkiessään häiritsemään yritysten ja yksityisten koneen käyttäjien tietojen koskemattomuutta. Esittelemällä tämän hetkisen uhkakentän lisäksi kriittisen kuvauksen tulevaisuuden trendeistä, Symantecin Internet Security Threat -raportti on arvokas työkalu yrityksille ja yksityisille turvata luottamuksellisen tiedon koskemattomuus kaikissa tilanteissa, mainostaa **Arthur Wong**, joka vastaa Symantecin tietoturva-analysoinnista ja informaatiosta.

Tietojen kalastelu "hyvin vakava uhka"

Raportin keskeisimpien tulosten valossa luottamuksellista tietoa uhkaavat riskit ovat kasvaneet tasaisesti viimeisen kolmen raportointiperiodin aikana. Symantecin saamista 50 yleisimmästä haittakoodista 54 prosenttia on kehitetty luottamuksellisen tiedon keräämiseen. Pääasiassa kasvu on johtunut yleistyvistä troijalaisista hevosista.

Tietojen kalastelu (phishing) jatkaa kasvuaan. Phising on tapa varastaa luottamuksellisia tietoa, kuten salasanoja tai luottokorttien numeroita. Joulukuun 2004 loppuun mennessä Symantecin Brightmail AntiSpam -suodattimiin oli jäänyt viikoittain noin 33 miljoonaa phising-yritystä verrattuna heinäkuun yhdeksään miljoonaan viikoittaiseen yritykseen. Symantecin asiantuntijat olettavat phishing-toiminnan jatkuvan hyvin vakavana uhkana myös tulevina vuosina.

Web-hyökkäysten kasvu: Web-työkalut ovat suosittu hyökkäyskohde, koska ne ovat hyvin yleisesti käytössä ja

mahdollistavat hyökkääjille perinteisten turvajärjestelyjen, kuten palomuurien, ohittamisen. Web-työkaluihin kohdistuvat hyökkäykset ovat vakava uhka, koska niiden kautta hyökkääjät pääsevät käsiksi luottamuksellisiin tietoihin tarvitsematta tunkeutua yksittäisiin palvelimiin. Aikavälillä 1.7.2004 - 31.12.2004 lähes 48 prosenttia kaikista haavoittuvuuksista löytyi web-työkaluista. Kasvu on huomattava edellisen raportointiperiodin 39 prosenttiin.

Windows-virukset räjähtivät

Raportin aikavälillä Symantec dokumentoi yli 7360 uutta Windows 32 -virus- ja matovarianttia. Kasvu edelliseen raportointiperiodiin oli 64 prosenttia. Jos tilannetta vertaa vuoden 2003 toiseen puoliskoon, saadaan kasvuprosentiksi 332 prosenttia.

Windows 32 -vihulaisten yhteismäärä joulukuun 2004 jälkeen on lähes 17 500. Näiden uhkien epäonnistunut havainnointi, torjunta tai poisto voi johtaa vakaviin taloudellisiin menetyksiin tai luottamuksellisen tiedon vuotoihin, minkä vuoksi yritysten on tärkeää päivittää virustorjuntaratkaisujansa useammin kuin koskaan aikaisemmin. Symantecin mukaan tämä lisää painetta nykyisille tietoturvaresursseille.

Symantec havaitsi viime vuoden jälkipuoliskolla yli 1403 uutta haavoittuvuutta, mikä tarkoittaa yli 54 haavoittuvuutta viikossa tai lähes kahdeksaa päivässä. Näistä 97 prosenttia luokiteltiin erittäin vakaviksi, mikä tarkoittaa sitä, että haavoittuvuuden onnistunut hyväksikäyttö voi johtaa kohdejärjestelmän osittaiseen tai täydelliseen käyttöhäiriöön.

Lisäksi 70 prosenttia haavoittuvuuksista luokiteltiin helposti hyödynnettäviksi ja lähes 80 prosenttia kauko-ohjautuvasti hyödynnettäviksi, mikä lisää mahdollisten hyökkääjien määrää, raportti huomioi.

13,6 hyökkäystä päivässä

Yleisin tietoturvahyökkäys oli Microsoft SQL -palvelimen Resolution Service -puskurinylivuotohyökkäys (aikaisemmin tunnettu nimellä Slammer-hyökkäys). Sitä käytti noin 22 prosenttia kaikista hyökkääjistä. Toiseksi yleisin hyökkäys oli TCP SYN Flood -palvelunestohyökkäys, jota käytti noin 12 prosenttia hyökkääjistä.

Yrityksiin kohdistui 13,6 hyökkäystä päivässä verrattuna edellisen raportointiperiodin 10,6 hyökkäykseen päivässä.

Yhdysvallat on edelleen yleisin hyökkäyskohdema. Sitä seuraavat Kiina ja Saksa. Suurin määrä hyökkäyksistä kohdistui rahalaitoksiin määrän ollessa 16 vakavaa hyökkäystä 10 000:tta tietoturvatapahtumaa kohden.

Raportin mukaan aika haavoittuvuuden havainnoinnista hyväksikäyttökoodin leviämiseen oli erittäin lyhyt, keskimäärin 6,4 päivää. Web-työkalujen haavoittuvuudet lisääntyivät edelliseen raportointiperiodiin verrattuna, ja suuri osa web-työkalujen haavoittuvuuksista luokitellaan helposti hyväksikäytettäviksi.

Haavoittuvuudet löytyivät usein uusista, vaihtoehtoisista selaimista, esimerkiksi 21 haavoittuvuutta löytyi Mozilla-selaimesta verrattuna Internet Explorer -selaimen 13 haavoittuvuuteen.

Massasähköpostimadot johtivat haittakoodilukuja vuoden 2004 jälkimmäisen vuosipuoliskon aikana. Kymmenen yleisimmän Symantecille raportoidun näytteen joukosta kahdeksan olivat massapostimatoja, kuten Netsky, Sober, Beagle, and MyDoom, jotka olivat mukana myös aikaisemmissa raporteissa.

Kymmenen yleisimmän haittakoodin joukossa oli kaksi botkoodia: Gabot oli kolmanneksi yleisimpänä listalla ja sen perässä Spybot. Spybot-varianttien määrä kasvoi jopa 180 prosenttia edelliseen puolivuotiskauteen verrattuna. Bot-haittakoodit mahdollistavat koneen luvattoman etäkäytön.

Trojialainen löytyi Symbian-pelistä

Vuoden lopussa oli olemassa 21 tunnettua näytettä kännyköihin kohdistetuista haittaohjelmista, kun niitä heinäkuussa tunnettiin yksi, Cabir. Uusien uhkien joukossa oli Duts-virus, ensimmäinen uhka Windows CE:tä kohtaan, ja Mos Trojan, joka löytyi Symbian-pelistä.

Viisi prosenttia 50 yleisimmästä Symantecilla raportoidusta hyökkäyksestä oli adware-ohjelmia, verrattuna edellisen raportointiperiodin neljään prosenttiin. Idefits oli yleisimmin raportoitu adware-ohjelma, ja Webhancer yleisin spyware-ohjelma.

Roskasähköpostin määrä kasvoi 77 prosenttia yhtiöissä, joissa on käytössä roskapostin valvontajärjestelmä. Roskaviestien määrä oli 60 prosenttia kaikista Symantecin tarkkailemista sähköpostiviesteistä.

Rahaa luvattomalla etäkäytöllä

Symantec uskoo, että koneen luvattoman etäkäytön mahdollistavia bot-haittaohjelmia ja bot-verkkoja tullaan todennäköisesti käyttämään yhä enenevässä määrin taloudellisen hyödyn saavuttamiseksi.

Kännyköihin ja muihin bluetooth-laitteisiin suunnitellut haittakoodit tulevat todennäköisesti yleistymään ja kehittymään

vahingollisimmiksi.

Symantec olettaa kuluttajapuolelle suuntautuvien matoja tai viruksia hyödyntävien hyökkäysten lisääntyvän. Audio- tai videokuvien taakse kätkeytyvien hyökkäysten oletetaan myös lisääntyvän. Tämä on huolestuttavaa, koska kuvatiedostot ovat yleisiä, maailmanlaajuisesti luotettuja ja keskeinen osa nykypäivän tietotekniikkaa, Symantec sanoo.

Adware- ja spyware-ohjelmien määrän oletetaan kasvavan. Erillinen lainsäädäntö näiden ohjelmien ehkäisemiseksi ei ole yksistään riittävän tehokas pelote, yhtiö korostaa.

<http://www.digitoday.fi/tietoturva/2005/03/21/koneen-kayttajia-kiusataan-hienostuneemmin/20059489/66>