hyväksymispäivä arvosana

arvostelija

Tietokonevirusten ja muiden haitallisten ohjelmien historia

Kare Piekkola

Helsinki 27.01.2005

Seminaarityö: Tietojenkäsittelytieteen historia

HELSINGIN YLIOPISTO

Tietojenkäsittelytieteen laitos

Sisältö

1 Johdanto

Yksi tämän päivän suurimmista vitsauksista tietokoneiden maailmassa ovat erilaiset haitalliset ohjelmat, joita yleisesti hieman virheellisesti nimitetään yhteisellä tietokonevirus-termillä. Haitallisia ohjelmia on nimittäin olemassa hyvin monenlaisia niin toiminnallisuudeltaan kuin käyttötarkoitukseltaankin. Tietokonevirukset kattavat tästä joukosta vain yhden osa-alueen. Yksi asia on kuitenkin kaikille haitallisille ohjelmille yhteinen – ne tuottavat harmia pahaa-aavistamattomalle tietokoneen käyttäjälle [Jär90]. Koska nykyään tietokoneille tallennetaan korvaamattoman tärkeää tietoa [Hel94], asettavat haitalliset ohjelmat todellisen uhkan ympäri maailman sekä yksityisille henkilöille että kokonaisille yrityksille. Haitallisia ohjelmia vastaan suojautuminen onkin kasvanut ensiarvoisen tärkeäksi osaksi jokapäiväistä tietokoneiden käyttöämme.

Kirjoituksen loppuosa rakentuu seuraavasti. Kappaleessa 2 jaotellaan tarkemmin haitallisia ohjelmia omiin alaluokkiinsa, kappaleessa 3 kuvataan melko tarkasti kronologisessa järjestyksessä virustentorjunnan ja erityisesti haitallisten ohjelmien historian kulku ja lopuksi, kappaleessa 4, luodaan yhteenveto käsitellyistä asioista.

2 Erilaisia haitallisia ohjelmatyyppejä

Haitallisia ohjelmia voidaan jakaa niiden toiminnallisuutensa perusteella useisiin eri luokkiin. Alan kirjallisuudessa ei kuitenkaan ole päästy täysin yhteisymmärrykseen, missä kunkin luokan rajat kulkevat. Tästä syystä alla jaotellut luokat ovat ehkä joiltain osin hieman päällekkäisiä ja joidenkin rajatapauksien luokitteleminen voi ylipäätään olla hyvin vaikeaa. Asioiden selventämiseksi ohjelmatyypit on kuitenkin jaoteltu tavalla, jota läpi kirjoituksen seurataan.

2.1 Kaniinit ja bakteerit

Kaniinit (*rabbit*) ja *bakteerit* (*bacterium*) ovat itsenäisesti toimivia ohjelmia, joiden tarkoituksena on heikentää jonkin tietokoneen resurssiluokan toimintaa [Bis02]. Molemmat ohjelmatyypit estävät siten järjestelmää tarjoamasta jotain tiettyä palvelua (ns. *denial of service attack*). Tyypillisesti kaniinit ovat ohjelmia, jotka kuluttavat yhden järjestelmän sisällä kaikki resurssit tekemällä itsestään äärettömästi kopioita [WKC89]. Bakteerit sitä vastoin pyrkivät kopioitumalla levittäytymään muille käyttäjille tai muihin järjestelmiin ja niitä ei välttämättä ole suunniteltu näännyttämään kaikkia järjestelmän resursseja [WKC89]. Ohjelmointivirheiden voisi kuvitella aiheuttavan järjestelmille samankaltaisia ongelmia kuin kaniinit ja bakteerit voivat aiheuttaa. Kumpikaan, kaniinit tai bakteerit, eivät tartuta muita ohjelmia [ViG05]. Seuraavassa on esiteltynä

kaniiniksi luokiteltava komentokielinen lause, joka voisi mahdollisesti ehdyttää UNIX-järjestelmän levytilan tai inode-taulun [Rit79].

```
while true
do
  mkdir x
  chdir x
done
```

2.2 Tietokonevirukset

Yleisimmillään *tietokonevirusten* (*computer virus*) voidaan ajatella olevan ohjelmia, jotka tarttuvat muihin ohjelmiin muuntamalla ne sisältämään version itsestään [Coh86] mahdollisesti samalla aiheuttaen vahinkoa isäntäohjelmalle tai –järjestelmälle [Ant05a]. Tässä merkityksessä tietokonevirus on siis vain pieni ohjelmapätkä, joka käyttää loisen kaltaisesti muita ohjelmia hyväkseen. Kuitenkin on myös olemassa tietokoneviruksia, jotka luovat rinnakkaisen ohjelman, joka vain käynnistetään ’saastuneessa’ ohjelmassa tai levyn *käynnistyslohkossa* (*boot sector*) [Hel94]. Tällaisissa tapauksissa virusohjelma ei siis välttämättä muuta muita ohjelmia, joten yllä esitetty määritelmä ei täysin kata kaikkia tapauksia.

Tietokoneviruksen elinkaaren voi jakaa kolmeen osaan [Jär90]. Ensimmäisessä vaiheessa virus tarttuu uuteen kohteeseen ja pyrkii piiloutumaan sinne. Toisessa vaiheessa virus pyrkii levittäytymään mahdollisimman laajalle. Lopuksi virus aktivoituu ja tekee mahdollisesti haitalliset toimenpiteensä.

Tietokoneviruksia voidaan luokitella toimintansa perusteella muun muassa seuraaviin kategorioihin [Bis02, Hel94, Jär90, Sym04]. *Käynnistyslohkovirukset* (*boot sector infectors*) piiloutuvat nimensä mukaisesti levyillä käynnistyslohkoon, josta ne pääsevät tietokoneen muistiin heti, kun levy luetaan tai kone käynnistetään. *Tiedostovirukset* (*executable infectors*) ovat viruksia, jotka tarttuvat suoritettaviin ohjelmiin. Tiedostovirukset pääsevät muistiin, kun viruksen saanut ohjelma käynnistetään. *Moniosiovirukset* (*multipartite viruses*) ovat viruksia, jotka osaavat toimia sekä käynnistyslohko- että tiedostoviruksen tavalla. *Muistiin jäävät virukset* (*terminate and stay resident viruses*) voivat pysyä muistissa aktiivisina, kunnes tietokone sammutetaan. Muistiin jäävät virukset voivat olla sekä käynnistyslohko- että tiedostoviruksia. *Sovellusohjelmavirukset* (*macro viruses*) tehdään jonkin sovellusohjelman omalla makro- tai ohjelmointikielellä, jolloin ne leviävät vain kyseisessä ohjelmassa käytettäviin tiedostoihin. Lisäksi on olemassa kehittyneempiä viruksia, jotka osaavat naamioida itsensä antamalla järjestelmälle virheellistä tietoa esimerkiksi sieppaamalla käyttöjärjestelmän tiedostonlukupyynnön (*stealth viruses*), voivat salakirjoittaa suurimman osan

ohjelmakoodistaan hämätäkseen viruksentorjuntaohjelmia (*encrypted viruses*) tai pystyvät muuttamaan muotoaan jokaisella uudella tartuntakerralla (*polymorphic viruses*).
Seuraava pseudokoodi havainnollistaa, miten yksinkertainen tietokonevirus toimii [Bis02].

```
beginvirus:
   if spread-condition then begin
      for some set of target files do begin
          if target is not infected then begin
             determine where to place virus instructions
             copy instructions from beginvirus to endvirus into target
             alter target to execute added instructions
          end;
      end;
  end;
  perform some action(s)
  goto beginning of infected program
endvirus:
```

2.3 Troijan hevoset

Troijan hevoseksi (*Trojan horse*) kutsutaan ohjelmaa, joka näyttää ulospäin houkuttelevalta ja viattomalta, mutta sen sisälle on lisätty ylimääräinen ja usein käyttäjälle näkymätön pätkä ohjelmakoodia [Jär90, WKC89]. Tämä ylimääräinen koodi saattaa esimerkiksi lähettää salaa ohjelman käyttäjän tietoja Troijan hevosen tekijälle, lisätä kyseenalaisten käyttäjäryhmien oikeuksia järjestelmässä tai vain tyhjentää koko ohjelman käyttäjän kiintolevyn. Viruksista poiketen Troijan hevoset eivät pyri lisääntymään levittämällä itseään uusiin tiedostoihin [Jär90, Sym04].
Loogiset pommit (*logic bomb*) ovat Troijan hevosten erikoistapauksia, joissa vahinkoa aiheuttava ohjelmakoodi on kätkettynä ohjelman sisään sillä tavalla, että se suoritetaan vasta, kun ohjelmoijan asettamat ehdot täyttyvät [Jär90, WKC89]. Näitä ehtoja voivat olla esimerkiksi jokin tietty päivämäärä, tietyn käyttäjän kirjautuminen sisään järjestelmään, levyn täyttöaste, ohjelman ajokertojen määrä tai tietyn toimintosarjan suorittaminen ohjelmassa [Bis02, Jär90, WKC89].
Takaovet (*trap door, back door*) ovat myös erikoistapauksia Troijan hevosista. Takaovet ovat ohjelmoijan tahallisesti jättämiä ja piilottamia oikopolkuja ohjelman koodiin esimerkiksi siten, että takaovelliseen järjestelmään pystyy kirjautumaan sisään ilman valideja tai dokumentoituja käyttäjätunnuksia [Wik05a, WKC89].

2.4 Madot

Perinteisesti *madot* (*computer worm*) ovat ohjelmia, jotka pystyvät itse verkon välityksellä lisääntymään hyödyntäen yleisesti käytetyissä ohjelmissa ja järjestelmissä olevia turva- ja toimintaperiaatepuutteita [KiE03, WPS03]. Viruksista poiketen madot pystyvät siis monesti

levittäytymään ilman käyttäjän tekemiä toimintoja (esimerkiksi ilman tiedoston suorittamista) ja ne eivät usein tarvitse ollenkaan isäntätiedostoa toimiakseen [Ant05b, Sym04].

2.5 Tiedon urkinta- ja vakoilumenetelmät

Eräs merkittävästi yleistyvä muoto Troijan hevosista ovat *tiedon urkinta- ja vakoilumenetelmät* (*spyware*) [Ant05c]. Vaikka kyseessä on vain jossain määrin erikoistapaus Troijan hevosista, tulee niitä käsitellä hieman tarkemmin niiden ajankohtaisen luonteen takia.

Yleisesti tiedon urkinta- ja vakoilumenetelmillä tarkoitetaan ohjelmistoja, jotka keräävät, usein salaa, tietoa käyttäjän järjestelmästä sekä järjestelmän käytöstä ja välittävät kerätyt tiedot takaisin jollekin kolmannelle osapuolelle [SGL04]. Tällä tavoin kolmas osapuoli pystyy esimerkiksi räätälöimään mainontaansa käyttäjäkohtaisesti, keräämään tietoja käyttäjän näppäimen painalluksista tai ilmoittamaan käyttäjän järjestelmässä olevista tietoturvapuutteista [Ant05d, SGL04].

Tiedon urkinta- ja vakoilusovellukset leviävät tyypillisesti vertaisverkko-ohjelmistojen, www-sivuilta, jopa automaattisesti, asennettavien laajennuksien (*browser helper object*) ja muiden epäilyttävien ohjelmien asennusten yhteydessä [Ant05d, SGL04]. Lisäksi yhteistyötä tekevät www-sivustot pystyvät *jäljittävien keksien* (*tracking cookie*) avulla keräämään tietoa käyttäjän käyttäytymisestä www-sivuillaan ja *piilojäljitteiden* (*web bug*), www-sivuilla olevien pienten näkymättömien kuvien, avulla käyttäjän tietojen kerääminen on mahdollista ilman käyttäjän tietämystä [SGL04].

3 Haitallisten ohjelmien ja virustentorjunnan kronologia

Haitallisten ohjelmien juuret juontavat pitkälle menneisyyteen, aina lähelle ensimmäisten tietokoneiden syntyä. Haitallisten ohjelmien kehityshistoria näyttää muutenkin seuranneen hyvin tarkasti eri ajanjaksoina käytettyjen tietokoneiden ja järjestelmien kehitystä sekä levinneisyyttä. Seuraavassa on melko kattava kuvaus haitallisten ohjelmien ja niitä vastaan tehtyjen virustentorjuntaohjelmien kehityksestä ja historiasta. Vuosien varrella haitallisten ohjelmien määrä on kasvanut niin suureksi, että kaikki niitä ei ole pystynyt historiikkiin sisällyttämän. Pääpainotukseksi onkin valittu uudenlaisia kehityssuuntauksia tuoneet tapahtumat, jotka eivät välttämättä mediassa ole saaneet sen suurempaa huomiota.

3.1 Varhainen historia

Tietokonevirusten idean uskotaan syntyneen vuonna 1949, kun matemaatikko *John Von Neumann* esitti ideansa automaattisesti itseään monistavista ohjelmista [Ant05e, Vir05]. Vuoteen 1951

mennessä hän olikin jo kehittänyt ehdotuksensa, kuinka kyseisiä automaattisia toimintoja voisi luoda. Vuonna 1959 matemaatikko *Lionel Penrose* jalosti vielä Von Neumannin ideaa pidemmälle esittämällä rakenteen, joka pystyisi aktivoitumaan, monistautumaan, muuntautumaan ja hyökkäämään. Penrosen mallia testattiin käytännössä myös *IBM 650* –koneella. Vaikka kyseiset ehdotukset luotiinkin parantamaan ihmisten käyttämää teknologiaa, on näin jälkikäteen sanottuna yhteys tietokoneviruksiin varsin selvä. [Vir05]

Ensimmäiset ohjelmat, jotka käyttivät automaattisesti monistautuvan ohjelman ideaa olivat *Darwin* vuonna 1962, *The Creeper* 1970-luvun alkupuolella, *Rabbit* vuonna 1974 ja *Pervading Animal* vuonna 1975. Darwin oli vain tietokonepeli, jossa pelaajien ohjelmat yrittävät tuhota vastustajan ohjelmia monistuen samalla itse mahdollisimman laajalle. Sen perusideaa on kuitenkin mahdollista käyttää aivan toisenlaisiin tarkoituksiin. The Creeper voidaan jo luokitella tietokonevirukseksi tai jonkinasteiseksi madoksi. Se levisi *ARPANET*:ssa, Yhdysvaltojen armeijan sisäisessä verkossa, käytetyissä *Tenex*-käyttöjärjestelmissä kopioimalla itseään etäkoneisiin. Varsinaista tuhoa Creeper ei kuitenkaan aiheuttanut. Se vain tulosti saastuneessa koneessa tekstin: ”*I'M THE CREEPER : CATCH ME IF YOU CAN.*” Vielä mielenkiintoisammaksi asian tekee se, että Creeper-ohjelman jälkeen julkistettiin ohjelma nimeltä *The Reeper*, joka myös levisi pitkin sisäistä verkkoa, mutta tarkoituksenaan Creeper-ohjelmien tuhoaminen. The Reeper –ohjelmaa voidaan siis pitää ensimmäisenä *virustentorjuntaohjelmana* (*anti-virus program*). Rabbit oli myös haitallisiin tarkoituksiin tehty ohjelma. Se ei tehnyt muuta kuin monisti itseään mahdollisimman paljon haitaten järjestelmän toimintaa (kts. kappale 2.1 kohta ”kaniinit”). Pervading Animal –peli aiheutti ehkä ensimmäisen ’virusepidemian’. Se toimi *Univax 1108* –järjestelmissä. Pelissä oli tahallinen tai tahaton sivuvaikutus, joka aiheutti pelin tekemään itsestään kopioita käyttäjän järjestelmään vieden paljon levytilaa [Bis02, Vir05]. Peli saattoi siis olla ensimmäinen Troijan hevonen. Toisaalta joidenkin lähteiden mukaan peli yhdisti kopioitaan suoritettavien tiedostojen perään [ViS05], ollen näin ehkä enemminkin tietokonevirus. [Vir05, ViS05]

80-luvun alkupuolella mikrotietokoneiden yleistyessä yhä useammat yksityishenkilöt rupesivat tekemään omia ohjelmiaan. Myös telekommunikaatiolaitteiden kehittyminen ja *purkkien* (*Bulletin Board System*) käyttäminen auttoi omalta osaltaan virusepidemioiden syntymistä. Ilmeisesti ensimmäiset mikrotietokoneille ohjelmoidut haitalliset ohjelmat tehtiin 80-luvun alkupuoliskon aikaan hyvin yleisessä käytössä olleelle *Apple II* –tietokoneelle [Bis02]. Tunnetuin näistä lienee tietokonevirus nimeltä *Elk Cloner*, jota pidetään ensimmäisenä viruksena, joka pääsi vapaasti leviämään myös synnyinympäristönsä ulkopuolella [Ant05e]. Kyseinen virus oli ensimmäisiä käynnistyslohkoviruksia. Koska Apple II –tietokoneissa käyttöjärjestelmä ladattiin aina levykkeeltä,

pääsi virus koneen muistiin joka kerta, kun kone käynnistettiin. Muistissa ollessaan virus tartutti jokaisen levykkeen, joka laitettiin koneeseen sisälle. [Vir05, ViS05]

Virallisesti termi ”tietokonevirus” (computer virus) syntyi vasta vuonna 1983 Etelä-Kalifornian yliopistossa, jossa *Len Adleman* kutsui tietokonevirukseksi oppilaansa *Fred Cohenin* tekemää Troijan hevosta [Bis02]. Termiä käytettiin ensimmäistä kertaa akateemisessa julkaisussa Fred Cohenin seuraavana vuonna kirjoittamassa artikkelissa nimeltä ”*Experiments with Computer Viruses*”. Artikkelissa tietokoneviruksia kuvattiin ohjelmina, jotka ovat tahallisesti tehty haittaamaan tai tuhoamaan muita ohjelmia tai järjestelmiä [Wik05b]. Kuitenkin aiemmin, jo 70-luvun puolivälin tieteiskirjallisuudessa, *David Gerroldin* teoksessa ”*When H.A.R.L.I.E. Was One*” esiintyy ohjelma nimeltä ”*Virus*”, joka toimi oikean biologisen viruksen tavoin [Wik05b]. Samassa teoksessa esiintyi Virus-ohjelmalle myös vastaohjelma ”*Antibody*”. Lisäksi vuoden 1973 elokuvassa ”*Westworld*” käytettiin termiä tietokonevirus kuvaamaan huvipuiston järjestelmässä olevaa haitallista ohjelmaa ja myös sarjakuvalehdessä vuodelta 1982, ”*Uncanny X-men*”, termiä tietokonevirus käytettiin jo nykyisessä merkityksessään [Wik05b]. Termi tietokonevirus on siis epävirallisesti keksitty jo paljon aiemmin, itse asiassa melko pian ensimmäisten haitallisten ohjelmien synnyn jälkeen. Termi mato esiintyi myös kirjallisuudessa jo varhaisessa vaiheessa. *John Brunnerin* vuoden 1975 romaanissa ”*The Shockwave Rider*” kuvataan matoja ohjelmina, jotka leviävät verkossa tuhoten tietoa [Wik05b]. Brunner tosin kutsui kyseisiä matoja nimellä ”*Tapeworms*”.

3.2 Haitallisten ohjelmien määrän kasvu ja kehitys

Vuonna 1986 havaittiin ensimmäistä kertaa *IBM PC* -tietokoneiden kanssa yhteensopiva tietokonevirus [esim. Bis02, Jär90]. Tämän kyseenalaisen kunnian sai osakseen tietokonevirus nimeltä *Brain*. Joidenkin lähteiden mukaan kyseinen virus oli myös ensimmäinen *naamioituvatietokonevirus* (kts. kappale 2.2 kohta ”stealth viruses”) [SuL01, Vir05, ViS05]. Brain oli käynnistyslohkovirus, jonka arvellaan tartuttaneen yli 300 000 levykettä [Jär90]. Kasvavien virustartuntojen määrä selittynee sillä, että IBM PC –koneissa yleisesti käytetyn *MS-DOS* –käyttöjärjestelmän suosio kasvoi tuolloin kovaa vauhtia [Ant05e]. Samana vuonna saksalainen ohjelmoija *Ralf Burger* esitti maanalaisessa tietokonealan harrastajien tapaamisessa tietokoneviruksensa nimeltä *VirDem*, joka pystyi tekemään kopioita itsestään liittäytymällä kiinni muihin ajettaviin tiedostoihin [Hel94, Vir05, ViS05]. Ohjelma herätti hakkereiden keskuudessa suurta kiinnostusta [Vir05]. Myös ensimmäinen varsinainen Troijan hevonen havaittiin vuonna 1986 [Ant05e]. Ohjelman nimi oli *PC-Write*. Se esitti olevansa ilmaiseksi jaettava versio

tekstinkäsittelyohjelmasta ja olikin sitä, mutta kuitenkin käytettäessä se samalla tuhosi ja korruptoi tietoa kovalevyltä [Ant05e].

Vuosi 1987 oli varsin synkkä tietokoneiden käyttäjille. Tällöin ohjelmoijien kiinnostus haitallisten ohjelmien tekemiseen varsinaisesti heräsi [Hel94]. Vaikka suurin osa hyökkäyksistä kohdistuikin nyt IBM PC -koneisiin, raportoitiin useista tapauksista myös Apple-, Amiga- ja Atari ST –koneille. Yllä esitelty Ralf Burger julkaisi vuonna 1987 kirjan "*Computer Viruses: A High-Tech Disease*", jossa hän esitti tarkat kuvaukset, miten tietokonevirus nimeltä *Vienna* tehtiin toimintakyvyttömäksi. Teos ei kuitenkaan ollut pelkästään edeltäjänä virustentorjuntaohjelmille, vaan se toimi valitettavasti myös innoittajana virusten ohjelmoimiseksi, koska siinä kuvattiin hyvin tarkasti, miten tietokoneviruksia tehdään. Vuonna 1987 havaittiin myös ensimmäinen osaksi *salakirjoitettu tietokonevirus* (kts. kappale 2.2 kohta "encrypted viruses") nimeltä *Cascade*, ensimmäinen tietoa levyltä tuhoava virus nimeltä *The Lehigh* ja ensimmäinen kokonainen virusperhe nimeltään *Suriv*, jossa viruksen alkuperäiseen koodiin tehtiin muutoksia uudenlaisen viruksen luomiseksi (*variants*) [Hel94, Vir05, ViS05]. Lisäksi samana vuonna levisi ympäri maailmaa ensimmäinen eri verkkojen välityksellä sähköpostitse levinnyt haitallinen ohjelma nimeltänsä *Christmas Tree* [Jär90, Vir05, ViS05]. Ohjelmaa ajettaessa se tulosti joulutervehdyksen ruudulle, mutta myös samalla tutki käyttäjän elektronisen postiluettelon ja lähetti itsestään kopion kaikille listassa mainituille henkilöille. Neljässä päivässä koko verkko oli täynnä kopioita ohjelmasta. Kyseessä oli siis Troijan hevonen sekä yksi ensimmäisistä madoista [KiE03]. [Vir05, ViS05]

Ensimmäiset varsinaiset virustentorjuntaohjelmistot näkivät päivän valon vuonna 1988 [Hel94, Vir05, ViS05]. Virustentorjunta perustui tunnettujen merkkijonojen etsintään ja ohjelmien muuntamiseen niin, että tietokonevirukset luulivat ohjelmassa olevan jo tartunta [Hel94, Vir05]. Samana vuonna perustettiin myös ensimmäinen virusturvaa käsittelevä *elektroninen keskustelupalsta Usenet*-verkkoon [Vir05]. Myös haitallisten ohjelmien rintamalla tapahtui. Ensimmäinen mato, joka käytti käyttöjärjestelmässä olleita turva-aukkoja hyväkseen syntyi [KiE03]. Madon nimi oli *Morris* (tunnettu myös nimellä *Internet Worm*). Se levisi pääosin sähköpostien kautta, kuten aiemmin esitetty Christmas Tree, mutta se käytti myös hyväkseen Unix-käyttöjärjestelmässä löytyneitä tietoturvapuutteita ja salasanalistoihin perustuvaa salasanojen arvaamista [Jär90, KiE03, Vir05, ViS05]. Vuonna 1989 puolestaan havaittiin mato nimeltä *Wank*, joka levisi *VAX/VMS*-koneissa *SPAM*-verkossa muuttaen järjestelmien salasanat symboleiksi [Vir05]. Kaikki symboliset salasanat mato lähetti eräällä saman verkon käyttäjälle. Vuodelta 1989 olivat myös tietokonevirus nimeltä *Disk Killer*, joka oli ensimmäisiä Suomessa havaittuja viruksia [Jär90] sekä *Harold Josephin* esitysmielessä tekemä, todennäköisesti kaikista ensimmäinen,

sovellusohjelmavirus. Josephin sovellusohjelmavirus oli suunnattu toimimaan *Lotus 1-2-3* –ohjelmassa [Bis02].

Ensimmäinen polymorfinen virus havaittiin vuonna 1990 (kts. kappale 2.2 kohta ”polymorphic viruses”) [Hel94, SuL01, Vir05, ViS05]. Virus oli osuvasti nimeltään *Chameleon* (suom. kameleontti). Virustentorjuntaohjelmille tämä aiheutti suurta päänvainaa, koska entinen merkkijonoihin perustunut virustentorjunta ei enää ollut riittävää [Hel94, Vir05, ViS05]. Tarvittiin uusia erikoistuneita algoritmeja polymorfisten virusten tunnistamiseksi [Hel94, Vir05]. Vuonna 1990 havaittiin myös ensimmäinen moniosiovirus [SuL01] sekä aikansa ehkä aktiivisimman virustenkirjoittajan, *Dark Avengerin*, monia tuotoksia [Vir05, ViS05]. Samana vuonna perustettiin myös ensimmäinen virusten vaihtoon tarkoitettu purkki [Vir05, ViS05]. Purkin välityksellä kuka tahansa ympäri maailmaa pystyi lähettämään ja lataamaan uusia viruksia. Dark Avengeria epäillään purkin todennäköiseksi perustajaksi [Vir05].

Vuonna 1992 ilmestyi ensimmäinen *mutanttikone* (*MtE, Self Mutating Engine*) [Hel94, Vir05, ViS05]. Mutanttikoneen tarkoituksena oli tehdä kaikille virustentekijöille polymorfisten virusten luominen mahdollisimman helpoksi. Ohjelman luoja oli kukapas muu kuin Dark Avenger. Dark Avengerin mutanttikone toimi esikuvana monille muille mutanttikoneille. *Eugene Kaspersky* onnistui kuitenkin kehittämään tehokkaan tavan polymorfisten virusten havaitsemiseksi. Hän kehitti ohjelman, joka emuloi prosessoria polymorfisen viruksen konekoodien selvittämiseksi. Tämä tarkoitti sitä, että jos virustentorjuntaohjelma onnistui tunnistamaan yhden mutanttikoneella tehdyn viruksen, se pystyi tunnistamaan kaikki viruksen eri variaatiot [Hel94]. Vuonna 1992 ilmestyivät myös ensimmäiset virukset, jotka yrittivät tavalla tai toisella häiritä virustentorjuntaohjelmien toimintaa ja ensimmäinen virus *Windows*-käyttöjärjestelmälle. Tästä alkoi jossain määrin uusi aikakausi haitallisten ohjelmien tekemisessä. Windowsista oli tulossa ensisijainen hyökkäysten kohde. [Vir05, ViS05]

Vuosina 1993-1996 ei tapahtunut mitään kovin mullistavaa haitallisten ohjelmien kehityksen kannalta. Taistelu virustentorjunta- ja haitallisten ohjelmien välillä tosin kiihtyi ja useat uudet tietokonevirukset olivat yhä ammattimaisemmin tehtyjä. Kuitenkin *CD-levyjen* käytön yleistyminen vuonna 1994 lisäsi merkittävästi virusten leviämistä, koska CD-levyltä ei virusta pysty poistamaan itse levyä tuhoamatta ja sovellusohjelmavirusten kasvava määrä vuonna 1995 asetti virustentorjuntaohjelmien tekijöille uusia haasteita. Kokonaisuudessaan haitallisten ohjelmien lukumäärä oli kasvanut noin kolmesta sadasta (vuonna 1991) moniin tuhansiin (yli 10 000 vuonna 1997 [Tyn04]). [Vir05, ViS05]

3.3 Viime vuosista tähän päivään

Vuosi 1997 oli astinkivenä verkon välityksellä tarkoitettujen haitallisten ohjelmien todelliselle esiinmarssille. *ShareFun* oli ensimmäinen sovellusohjelmavirus, joka pyrki leviämään myös sähköpostien liitetiedostojen kautta [KiE03, Vir05, ViS05]. Mikäli koneessa oli käytössä Microsoft Mail -sähköpostiohjelma, virus yritti lähettää sähköpostiviestin, jonka liitetiedostona oli saastunut Word-dokumentti, kolmelle paikallisesta MS Mail -nimiluettelosta satunnaisesti löytämälleen henkilölle [FSe05a]. *Homer* puolestaan oli ensimmäinen mato, joka levisi käyttäen FTP-protokollaa [Vir05, ViS05]. Se kopioi itsensä kaikkiin etäkoneisiin, johon käyttäjä oli ottanut yhteyden. Samana vuonna syntyivät myös ensimmäiset *internetin keskustelukanavien* (*Internet Relay Chat, IRC*) kautta leviävät madot ja muut haitalliset ohjelmat [Vir05, ViS05]. Lisäksi vuodelta 1997 on ensimmäinen havaittu tietokonevirus Linuxille. Viruksen nimi oli *Linux Bliss* [Vir05, ViS05].

Trendi jatkui samana seuraavanakin vuonna. Tuli yhä selvemmäksi, että haitallisten ohjelmien tekijöiden kiinnostus oli suuntautumassa verkkopohjaisiin ohjelmiin. Vuonna 1998 ilmaantui muun muassa *BackOrifice* niminen haitallinen ohjelma. Se mahdollisti koneen hallitsemisen salaa etäkoneesta käsin. Haitallisten ohjelmien tekijät huomasivat myös mahdollisuutensa WWW-sivujen aktiivisten komponenttien hyväksikäytössä. Ensimmäinen haitallista koodia sisältävä ajettava *Java*-moduuli nimeltään *StrangeBrew* havaittiinkin elokuussa 1998. Myöhemmin samana vuonna havaittiin myös ensimmäiset *HTML*-virukset. Virukset käyttivät hyväkseen HTML-koodiin upotettua *Visual Basic* –skriptiä [FSe05b, Vir05, ViS05]. Haittaa ne kuitenkin aiheuttivat vain silloin, kun saastunut sivu tallennettiin ja avattiin paikalliselta levyltä [FSe05b]. [Vir05, ViS05]

Vuonna 1999 havaittiin sähköpostimato nimeltään *Bubbleboy*, joka pystyi tarttumaan käyttäjän koneeseen välittömästi, kun saastunut sähköpostiviesti avattiin [KiE03, Vir05]. Se oli ensimmäinen mato, joka ei tarvinnut sähköpostin liitetiedoston avaamista käyttäjän koneen saastuttamiseksi. Mato hyödynsi Microsoftin sähköpostiohjelmassa ollutta tietoturva-aukkoa [KiE03, Vir05], joka tosin pikaisesti paikattiin. Vuoden 1999 joulukuussa löydettiin myös ensimmäinen tietokonevirus, joka pystyi päivittämään itseään verkkoyhteyden välityksellä. Virus oli nimeltään *Babylonia* ja se yritti aika ajoin ladata japanilaiselta palvelimelta itselleen tuoreempia moduuleita toimintansa muuttamiseksi. Samalta vuodelta oli myös mato nimeltä *ExploreZip*, joka levisi lähiverkossa automaattisesti hyödyntäen Windows-käyttöjärjestelmän tiedostojen jakamiseen tarkoitettuja protokollia [KiE03]. Se oli ensimmäinen mato, joka osasi hyödyntää tätä turvallisuusaukkoa tartuttaen kaikki lähiverkon suojaamattomat tietokoneet [KiE03]. [Vir05]

Ensimmäinen kämmentietokoneille kirjoitettu haitallinen ohjelma löydettiin vuonna 2000 [FsD01, Vir05]. Ohjelma tarttui PalmOS-käyttöjärjestelmiin ja oli nimeltään *Liberty* [FsD01, Vir05].

Samana vuonna esiintyi myös *Timofonica* niminen mato, joka käytti ensimmäisenä hyväkseen matkapuhelimia [Vir05]. Timofonica-mato tosin lähetti vain kantaaottavia tekstiviestejä erään palveluntarjoajan sattumanvaraisiin puhelinnumeroihin [Vir05].

Vuodesta 1999 eteenpäin haitallisten ohjelmien kirjoittajien mielenkiinto perinteisten tiedostojen kautta leviävien tietokonevirusten tekemiseen oli hiljalleen häviämässä. Haitallisten ohjelmien kirjoittamisen pääpaino siirtyi lopullisesti internetissä käytettävien toimintojen, kuten esimerkiksi sähköpostin, vertaisverkkojen, www-sivujen ja IRC:n, hyväksikäyttämiseen. Madoista ja erilaisista Troijan hevosista oli tullut suurimmat tietokoneen käytön arkipäivän viholliset. Laajoja epidemioita ympäri maailmaa ovat aiheuttaneet lukuisat joko sähköpostitse ja/tai erilaisia tietoturva-aukkoja myöten levinneet madot, joista tunnetuimpia ovat *Happy99* ja *Melissa* vuodelta 1999, *LoveLetter* vuodelta 2000, *CodeRed* ja *Nimda* vuodelta 2001, *Slammer*, *Blaster* ja *Sobig* vuodelta 2003 sekä *Bagle* ja *Sasser* vuodelta 2004 [KiE03, SeF04, Sul01, Vir05]. Useista näistä madoista on myös olemassa lukuisia myöhemmin ilmaantuneita hieman muunneltuja variaatioita. Vaikka kaikki yllä mainitut ja muutenkin suurin osa matojen hyökkäyksistä olikin kohdistunut Microsoftin käyttöjärjestelmiin, oli myös esimerkiksi Linux-käyttöjärjestelmä matojen hyökkäysten kohteena. Esimerkiksi *Ramen*-mato vuonna 2001 pääsi leviämään useiden yritysten, kuten esimerkiksi *NASA*:n, verkkoon. [Vir05]

Vuosien 2001-2004 uutuutena haitallisten ohjelmien saralla oli tiedon urkinta- ja vakoilumenetelmien (kts. kappale 2.5) todellinen esiintulo [SGL04]. Koska perinteiset virustentorjuntaohjelmat eivät tunnistaneet tämän kaltaisia uhkia, syntyi markkinoille useita uusia ohjelmia, joiden nimenomaisena tarkoituksena oli kyseisten haitallisten ohjelmien toiminnan estäminen. Perinteisistä haitallisista ohjelmista erityisesti erilaiset madot kehittyivät kyseisen ajanjakson aikana yhä moninaisemmiksi ja taidokkaimmaksi. Yhä useampi mato osasi käyttää useita erilaisia tapoja levitäkseen ja monet matojen tekijöistä oppivat toisiltaan uusia tekniikoita käyttöjärjestelmissä olevien haavoittuvuuksien hyödyntämiseksi [KiE03, Vir05]. Lisäksi matojen kylkiäisinä oli usein Troijan hevosia tai tietokoneviruksia, jotka pystyivät siten leviämään madon mukana räjähtävällä nopeudella. Joitakin uudistuksia syntyi myös perinteisempiin haitallisiin ohjelmiin. Ensimmäiset *Tiedostottomat madot* (*fileless worms*) havaittiin vuonna 2001. Nämä madot pystyivät toimimaan tietokoneen keskusmuistissa kokonaan ilman levyllä säilytettäviä tiedostoja ja ne pystyivät leviämään pelkkien data-pakettien avulla. Tiedostottomat madot aiheuttivat erityistä päänvaivaa virustentorjuntaohjelmien kehittäjille. Vuonna 2001 ilmestyi myös haitallisille ohjelmille uusi tartuntatapa. Selaimissa olevien turvallisuusaukkojen avulla saastunut internet-sivusto saattoi tartuttaa sivujen käyttäjän pelkän sivustolla tapahtuneen vierailun aikana. Vuonna 2003 puolestaan syntyi uusi haitallisten ohjelmien käytön trendi. Roskapostittajat rupesivat

tekemään yhteistyötä haitallisten ohjelmien kirjoittajien kanssa [Fse03, Vir05]. He alkoivat käyttämään Troijan hevosten saastuttamia tietokoneita apuvälineenä sähköpostien lähettämiseen. Lisäksi todennäköisesti ensimmäinen todellinen matkapuhelimille tehty haitallinen ohjelma havaittiin vuonna 2004. Ohjelma oli mato nimeltään *Cabir*, joka pystyi leviämään avoimen *Bluetooth*-tiedonsiirtoyhteyden avulla matkapuhelimissa käytetyissä *Symbian*-käyttöjärjestelmissä [Fse05c]. Vuosien saatossa haitallisten ohjelmien lukumäärä oli kerinnyt kasvamaan, kaikki variantit mukaan lukien, jo noin sataan tuhanteen (90 000 vuonna 2003 [Fse03], tiedon urkinta- ja vakoilumenetelmien määrää ei ole laskettu lukuun mukaan). [Vir05]

4 Yhteenveto

Erilaisista haitallisista ohjelmista on kehittynyt arkinen uhka kaikille tietokoneiden käyttäjille. Haitallisten ohjelmien historian kehityksen huomioon ottaen on selvästi odotettavissa, että ongelman suuruus vain kasvaa kasvamistaan. Internetin laajuuden ja tietoliikenneyhteyksien määrän räjähtänyt kasvu on ollut omiaan edesauttamaan tämän ei-toivotun tilanteen paisumisessa. Nykyään ilman asianmukaista palomuuri- ja virustentorjuntaohjelmistoa ei kukaan ole haitallisilta ohjelmilta turvassa, oli asuinpaikka sitten missä päin maailmaa tahansa.

Haitalliset ohjelmat ovat viime vuosina aloittaneet leviämisen myös kämmenmikroihin sekä matkapuhelimiin. Vielä kyseisiä laitteita voi melko huoletta käyttää ilman pelkoa tartuntavaaroista, mutta on todennäköisesti vain ajan kysymys, koska haitallisten ohjelmien tekijöiden mielestä esimerkiksi kämmenmikroista löytyvä tieto on varastamisen arvoista tai matkapuhelimia pystyy jotenkin käyttämään taloudellisen hyödyn tavoittelussa hyväksi [Vir05]. On myös mahdollista, että muidenkin kodinkoneiden, kuten esimerkiksi *digiboksien*, kehittyessä ei tulevaisuudessa voi haitallisilta ohjelmilta välttyä yhdessäkään tilanteessa, jossa ollaan tekemisissä tekniikan kanssa. Haitallisista ohjelmista on selvästi muodostunut yksi aikakautemme ikävimmistä vitsauksista ja tilanne voi vuosien saatossa vielä pahentua entisestään.

Lähteet

Ant05a Antivirus World – Your Source About Computer Safety, What is a Computer Virus? **URL http://www.antivirusworld.com/articles/computer-virus.php** [27.01.2005].

Ant05b Antivirus World – Your Source About Computer Safety, What is a Computer Worm? **URL http://www.antivirusworld.com/articles/computer-worm.php** [27.01.2005].

Ant05c Antivirus World – Your Source About Computer Safety, What is a Trojan Horse? **URL http://www.antivirusworld.com/articles/trojan-horse.php** [27.01.2005].

Ant05d Antivirus World – Your Source About Computer Safety, Spyware and What You Should Know About It? **URL http://www.antivirusworld.com/articles/spyware.php** [27.01.2005].

Ant05e Antivirus World – Your Source About Computer Safety, History of Computer Viruses. **URL http://www.antivirusworld.com/articles/history.php** [27.01.2005].

Bis02 Bishop, M., Computer Security: Art and Science. *Addison-Wesley*, Chapter 22, Pages 613–644, December 2002.

Coh86 Cohen, F., Computer Viruses. *PhD Dissertation, University of Southern California, ASP Press (PO Box 81270, Pittsburgh, PA 15217 USA)*, 1986.

FsD01 Foley, S. N. ja Dumigan, R., Are Handheld Viruses a Significant Threat? *Communications of the ACM*, *Volume 44*, *Issue 1*, Pages 105–107, January 2001.

Fse03 The Year of the Worm, *F-Secure Corporation's Data Security Summary for 2003*. **URL www.f-secure.com/2003/f-secure_corporation_data_security_summary_for_2003.pdf** [27.01.2005].

FSe05a F-Secure - Viruskuvaukset, Sharefun. **URL http://www.f-secure.com/v-kuvaus/sharefun.shtml** [27.01.2005].

Fse05b F-Secure - Viruskuvaukset, HTML Virus. **URL http://www.f-secure.com/v-descs/html.shtml** [27.01.2005].

Fse05c F-Secure - Viruskuvaukset, Cabir. **URL http://www.f-secure.com/v-descs/cabir.shtml** [27.01.2005].

Hel94 Helenius, M., Tietokonevirukset ja Virustentorjunta. *B-1994-3, Tampereen yliopisto*, Tammikuussa 1994.

Jär90 Järvinen, P., Tietokonevirukset, Toinen Painos. *WSOY*, Vuonna 1990.

KiE03 Kienzle, D. M. ja Elder, M. C., Recent Worms: A Survey and Trends. *In Proceedings of the 2003 ACM Workshop on Rapid Malcode*, Pages 1–10, Washington, DC, United States, October 2003.

Rit79 Ritchie, D., On the Security of UNIX. *UNIX System Manager's Manual*, pp. SM17: 1–3, 1979.

SeF04 SecurityFocus, A Short History of Computer Viruses and Attacks. **URL http://www.securityfocus.com/news/2445** [27.01.2005].

SGL04 Saroiu, S., Gribble, S. D. ja Levy, H. M., Measurement and Analysis of Spyware in a University Environment. *In Proceedings of the First Symposium on Networked Systems Design and Implementation*, Pages 141–153, March 2004.

SuL01 Subramanya, S. R. ja Lakshminarasimhan, N., Computer Viruses. *Potentials, IEEE, Volume 20, Issue 4*, Pages 16–19, 2001.

Sym04 Symantec, What is the Difference Between Viruses, Worms and Trojans? **URL http://service1.symantec.com/SUPPORT/nav.nsf/docid/1999041209131106** [27.01.2005].

Tyn04 Tynan, D., Viral Scourge 101: Not-So-Great Moments in PC History. *PC World*, **URL http://pcworld.about.com/news/Oct292003id113177.htm** [27.01.2005].

ViG05 Virus Glossary. **URL http://members.fortunecity.com/weihsin/glossary.html** [27.01.2005].

Vir05 Viruslist.com – All About Internet Security, History of Malicious Programs. **URL http://www.viruslist.com/en/viruses/encyclopedia?chapter=153280684** [27.01.2005]

ViS05 ViruScan Software, The History of Computer Viruses. **URL http://www.virus-scan-software.com/virus-scan-help/answers/the-history-of-computer-viruses.shtml** [27.01.2005]

Wik05a Wikipedia – The Free Encyclopedia, Backdoor. **URL http://en.wikipedia.org/wiki/Backdoor** [27.01.2005].

Wik05b Wikipedia – The Free Encyclopedia, Computer virus. **URL http://en.wikipedia.org/wiki/Computer_virus** [27.01.2005].

WKC89 White, S. R., Kuo, C. J. ja Chess, D. M., Coping with Computer Viruses and Related Problems. *IBM Los Angeles Scientific Center*, *Research Report Number RC 14405*, January 1989. **URL http://www.itmweb.com/essay503.htm** [27.01.2005].

WPS03 Weaver, N., Paxson, V., Staniford, S. ja Cunningham, R., A Taxonomy of Computer Worms. *In Proceedings of the 2003 ACM Workshop on Rapid Malcode*, Pages 11–18, Washington, DC, United States, October 2003.