Tietokoneviruksset ja haittaohjelmat

Mika Hakala

Virustyypit

- Mikä
  - Käynnistyslohkovirukset
  - Virusohjelmat
  - Makrovirukset
- Miten
  - Siirrettävä media
  - Sähköposti / Internet-ohjelmistopalvelimet
  - Verkkomadot
- Mitä
  - Levittyy
  - Tuhoaa
  - Muuttaa
  - Vakoilee / välittää tietoa muualle

Tartunta

- Virus aktivoituu vain ajettaessa
  - aktivoitumisen jälkeen virus voi toimia tausta-ohjelmana
  - virus suorittaa sen jälkeen toimintaansa ohjelmoituja tehtäviä samalla tavoin kuin mikä tahansa muu sovellus
  - Osa sovelluksista voi automaattisesti aktivoida viruksen

Viruksen havaitseminen

- Tiedostot ja keskusmuisti
  - Löytyminen perustuu merkkijono-hakuun
  - Virustunnisteet tallennettuna päivittyvässä tietokannassa
    - Nimi ja tunnistemerkkijono
- Verkkoliikenne
  - Edellisen lisäksi poikkeavat liikennöivät sovellukset ja liikennöinti-protokollat / portit
- Heuristiset menetelmät
  - Varoittavat / estävät normaalista poikkeavia ohjelmistotoimintoja
    - Eli tarkkailevat mm. kiintolevyn / muistin käsittelyä

Hoito tartunnan jälkeen

- Puhdistus, disinfect
  - Pyrkii poistamaan virustartunnan tiedostosta varsinaista tietoa muuttamatta
  - Ei aina onnistu
- Poisto, remove
  - Poistaa tartunnan saaneen tiedoston
  - Voi aiheuttaa ongelmia koneen käytössä
- Osa torjuntasovelluksista sisältää myös karanteenijärjestelmän. Silloin tartunnan saanut tiedosto eristetään kunnes puhdistus onnistuu.

Hoito tartunnan jälkeen

- Jos virus on aktivoitunut, viruksen poistaminen voi olla hankalaa.
  - Puhtaat käynnistysmediat (LiveCD, USB)
- Osa viruksista piiloutuu järjestelmässä alueille, joista tiedostoja ei normaali tilanteissa voi poistaa.

Haittaohjelmistot

- HUOM!! Jako virusten ja haittaohjelmien välillä aika häilyvä ja teennäinen. Lähinnä jako johtuu historiallisista syistä
  - Haittaohjelmat olivat usein alkuaikoina kaupallisia sovelluksia, joissa oli ei-toivottuja ominaisuuksia. Virustorjuntaohjelmistojen valmistajat eivät uskaltaneet näiden toimintaa estää.
- Haittaohjelmistot aiheuttavat järjestelmissä erilaisia ei toivottuja ominaisuuksia
  - Muutokset koneen käytössä
    - Kotisivun muutos, Kuvakkeet työpöydällä
    - Soitto-ohjelmistot, Etähallinta-ohjelmistot, Roskapostin välitys
- Virustorjuntaohjelmistot eivät välttämättä löydä haittaohjelmia. Niiden etsimiseen ja valvontaan löytyy tarkoitusta varten tehtyjä erikoisohjelmia.
  - Mm. Ad-aware ja Spybot
  - Nykyään monissa virustorjuntaohjelmissa mukana, muistettava asennuksissa

Torjuntatekniikat

- Passiivinen
  - Sovelluksella suoritetaan tallennusmedioiden virustarkistus, joko ajastetusti tai manuaalisesti
- Aktiivinen torjunta
  - Käytössä ohjelma, joka tarkkailee järjestelmässä tapahtuvia lataus / tallennus-operaatioita ja pyrkii estämään virusten aktivoitumisen / leviämisen
  - Voi myös tarkkailla verkkoliikennettä, mm. http, smtp, pop3, imap4

Torjuntajärjestelmät

- Työasema / Palvelin
  - Virustorjuntasovellus asennettuna
  - Tunnistusmerkkijonot päivitetty ajan tasalle
- Keskitetty virustorjunta
  - Hallintapalvelin
    - Vastaa asennuksista sekä torjuntasovelluksen asetuksista
    - Vastaanottaa hälytykset keskitetysti
    - Suorittaa tunnistusmerkkijonojen päivitykset keskitetysti

Torjuntajärjestelmät

- Palvelintuotekohtainen virustorjunta
  - Sähköpostijärjestelmät
    - analysoi tulevaa/lähtevää sähköpostia
    - pyrkii estämään virusten leviämisen sähköpostin välityksellä
  - Palomuurit
    - analysoidaan suoraan verkossa tapahtuvaa liikennettä
    - pyritään estämään virusten tulo sisäverkkoon ulkopuolelta