Kahjurvara

- Viirused — teisi programme nakatavad programmid
- Ussid — iseseisvalt edasi tungivad programmid
- Trooja hobused — reeglina ei levi ise, aga teevad kurja või avavad tagaukse hilisemaks juurdepääsuks ründajale
- Loogikapommid — legaalsetes programmides olevad dokumenteerimata võimalused, mis turvaauke tekitavad
- Pipetid — trooja hobuste, viiruste jms levitamiseks kasutatavad peibutusprogrammid
- Pettus (*hoax*) — inimesi nakatav "viirus"

Viiruste liigitus

- Failiviirused — nakatavad käivitatavaid programme
  - Mitteresidentsed
  - Residentsed
- Kaasfailiviirused
- Alglaadesektori viirused
- Hübriidviirused
- Peit- (*stealth*) ja soomusviirused (*armoured*)
- Polümorfsed viirused
- Vaktsiinihävitusviirused
- Võrguviirused
- Makroviirused!
- Pseudoviirused

Makroviirused

- Tänapäeval valdavad
- Kasutavad ära võimalust, et mõnedesse andmefailidesse saab lisada programme
- Word & .doc — Concept 1994
- Iga makrokeelt sisaldav dokumendiformaat on potentsiaalne ohuallikas
- Algkäivitusmakrodest hoidumine pole piisav
- Automaatselt käivitatavatest makrodest hoidumine on kohati piisav
- Mitmeid trikke makrokaitsest mööda hiilimiseks

Viiruste vastu

- Mitte käivitada mitteusaldusväärsest allikast pärit aktiivsisu!
- Koolitada kasutajaid potentsiaalset aktiivsisu ära tundma
- Seadistada tarkvara aktiivsisu mitte automaatselt käivitama
- Käivitamise vajadusel kontrollida antiviirusega
- Antiviirust rakendada perimeetri kõigis punktides (meilisüsteem, veebivahendaja, sissetoodud flopid, . . .)
- Võimalusel mitte kasutada makrosid sisaldavaid formaate
- Kaitsta käivitatavad failid kasutajatepoolse muutmise eest
- Kontrollida regulaarselt failide autentsust (kontrollsummad jms)

Ussid

- Levivad iseseisvalt võrku mööda
- Nakatavad arvuteid (ühekomponendilised) või võrke (mitmekomponendilised)
- Robert Morrise Internet Worm 1988
- "Jänesed" — korraga üks eksemplar liigub ringi
- Nakatavad kindlat platvormi (platvorme)
- Kasutavad ära teenuste turvaauke nakatatavates arvutites
- Kasutavad ära meiliprogramme ja veebibrausereid (nii turvaauke kui kasutajate rumalust)

Usside levimine

- Suudavad levida väga kiiresti
  - Iseseisvalt teenuse aukude kaudu levides mõne päeva kuni mõne tunniga kogu Internet, teoreetiliselt veerand tunniga
  - Meili teel levivad aeglasemalt (vajalik kasutaja sekkumine igal sammul)

Trooja hobused

- Ründajal tuleb trooja hobune kõigepealt rünnatavasse masinasse sokutada (pipetid, brauserite turvaaugud, *social engineering*)
- Levinud on ründajale juhtimiskanalit pakkuvad troojalased (varem eriti IRC võrgu kaudu, tänapäeval oma kanalid kuni P2P võrkudeni välja)
- RAT — *Remote Access Tool*
- Nn. *rootkitid* on samuti trooja hobused
- Tihti kasutatakse trooja hobuseid vallutatud arvutitest edasiste rünnakute tegemiseks (näiteks DDoS, rämpsposti saatmine)
- Lunavara (*ransomware*)
- Kaugekõnede võtjad

Pipetid

- Pipettideks on igasugused peibutised
  - Igasugu (interaktiived) animatsioonid ("viruta Bill Gatesile tordiga!")
  - Väidetavalt uued versioonid levinud programmidest (antiviirused!)
  - Microsofti/Adobe/Oracle/... turvaparandused
  - Hirmvara (*scareware*)
  - Eesti mäng.exe
  - Lahe mobiilimäng, mis nõuab kõikvõimalikke õigusi
- Põhiline, et kasutaja nad käima paneks

Loogikapommid

- Autori poolt meelega lisatud võimalused, mis teevad kasutaja arvutis midagi, mida kasutaja tegelikult ei taha
- Tagauksed
- Krüptosüsteemide nõrgendamine (salakanalid võtmete jaoks jne)
- Andmete kogumine, nuhkvara (*spyware*)
- Avatud lähtekood aitab siin

Tõrjumine

- Esiteks, **KOOLITAGE KASUTAJAID!**
- Jäävad turvaauke kasutavad ründeprogrammid
  - Aktiivsisu filtreerimine
- Antiviirustest on kasu, aga neile loota ei tasu
  - Nad on alati ajast maas
  - Nad võitlevad tagajärgede, mitte põhjustega, ja sedagi alles pärast ohu levimist
- Antiviirustele on enamasti ka levinumad ussid ja trooja hobused selgeks tehtud
- Hakatakse aru saama, et ka nuhkvara, reklaami näitajad jms kuuluvad samasse patta
- Seni on nende eemaldamiseks siiski eraldi programmid