F-Secure silmitsi maailma e-kurjusega

16. oktoober 2007 - 0:00 Autor: AM

(Arvutimaailm 10/07)

Kaido Einama

Võiks arvata, et F-Secure´i kontor on samasugune igav tarkvarafirma büroo nagu enamus teisigi – tõsised tarkvaraprofid arvutite taga antiviiruseid kirjutamas ja kuskil klaaskapis varitseb nende ülemus, et majandustulemused head püsiksid. F-Secure aga on panustanud ka välisesse hiilgusse – juba fuajees tekib mulje, et maailm on üks küberkuritegevuse sõjatanner, mida jälgitakse siit, F-Secure´i kõrgtehnoloogilisest staabipunkrist.

Suur ekraan sekretäri pea kohal näitabki selle lahinguvälja ülevaadet. Samasugust pilti epideemiakolletega maakera eri paigus võib imetleda ka F-Secure´i kodulehel, kuid suurel ekraanil on see muidugi palju efektsem.

Mida sealt siis näha? Eks ikka seda, et USA lääneranniku käib aktiivne seltsielu nii uss- kui muudel viirustel ja Euroopa pole ka parem koht: punaseid täppe tekib ja kaob üsna kiiresti just läänepoolses osas. Rääkimata Aasiast, mille kõrgtehnoloogilised tiigrid arenevad üheskoos maailma moodsaimate viirustega. Nende keerukusest annab selgust kohe sekretäri kõrval seinal rippuv maal. See pole taies mõnelt tuntud Soome kunstnikult, vaid ühe keerulise ussiviiruse – Sobig.f struktuur. Kui keegi tahab teada, mismoodi viirused siis tegelikult välja näevad, siis just see vurrikujuline rägastik ongi kõige parem seletus.

[---]

Valgete kitlitega viirusetõrjujad

Raske otsustada, kas edasine ringkäik F-Secure peakontoris on osavalt lavastatud *show* või ongi antiviirustefirmas elu nagu Hollywoodis. Nimelt kohtume me valgete kitlitega nagi kõrval antiviirusemaailma guru Mikko Hypponeniga, kelle edasine tegutsemine, nagu hiljem selgub, on detailideni põhjalikult ette valmistatud ja kordub erinevate gruppidega üsna täpse stsenaariumi järgi.

Valged kitlid nagis on pigem PR-komponent kui praktiline vajadus, näib puldiga avatavate klaasuste taha jõudes, sest "suletud tsoonis" on näha liikumas täiesti tavalisi itimehi kampsunites ja T-särkides. Hypponen avab "kinnise tsooni" uksed ja selgitab: tsoon on suletud sellepärast, et keegi siit kogemata mõnd nakatunud arvutit, mälupulka või CD-d välja ei viiks ja viirust igale poole laiali ei levitaks.

Istume seepeale maha suure kolmnurkse laua taha hämaras ruumis, mis on varustatud ühe suure ja kahe väiksema ekraaniga. Vasakpoolsel keerleb taas *Bagle*-nimelise ussviiruse ruumiline skeem ja parempoolsel vilguvad rohelised-punased tulukesed maailmakaardil. Keskmisel suurel tööekraanil hakkab Hypponen näitama, kuidas viirused kinni nabitakse.

Ta avab kõigepealt Google Earthi gloobuse ja seletab, et kui veel mitmed aastad tagasi olid viirusekirjutajad peamiselt üksiküritajad, siis praegu tegutsetakse organiseeritud kampadena. Kõik mäletavad 2001.-2003. aastal maailma laastanud hiigel-epideemiaid, kui paljud viirused (alates Melissast) saavutasid kähku ülemaailmse leviku, nüüd enam selliseid asju ei juhtu. Kas maailm on vahepeal turvalisemaks läinud?

Hoopiski mitte, kummutab Hypponen kõik lootused. Vastupidi – pahalasi on liikvel enam kui kunagi varem. Viirusetõrje on aga aja jooksul tõhustunud.

Et asjale interaktiivset maiku lisada, võetakse lahti hetkel saabunud pahalaste päritolukohad. Hollywoodilikult lavastatud stseen sisaldab endas viiruseallika kindlaks tegemist IP aadressi järgi ja siis selle kaudu geograafilise asukoha määramist. Suumime Google Earthiga kiiresti sisse ühte USA linna ja ristike jääb pidama ühel suvalisel parkimisplatsil. Kuskilt sealt parklast viirus lahti pääseski, teatab Hypponen võidukalt. Siis sõidame satelliidipildiga edasi kuhugi Siberi tööstuslinna, kust ka just olevat hakanud levima midagi kahtlast.

Hoopis vajalikum tööriist viiruseuurijatele on aga virtuaalmasina failidest joonistatud graafilised "tornid". Need värvuvad triibulisteks, kui arvuti mõne viirusega nakatada. Punaseks läinud failid tähistavad seda, et miskit neis peale nakatumist muudeti. Nüüd on viiruseuurijatel lihtsam vaatama hakata, mis muudatusi pahalane siis tegi.

(edasi loe juba oktoobri Arvutimaailmast...)

- Tegijad
- Turvalisus