DIGITÁLIS KÁROKOZÓK HOLNAPUTÁN

Csiszér Béla

doktorjelölt, Budapesti Műszaki és Gazdaságtudományi Egyetem
Innovációmenedzsment és Technikatörténet Tanszék
bela.csiszer@sicontact.hu

A számítógépes vírusok témaköre folyamatosan változó, nagyon érdekes terület. Sokan például nem is sejtik, hogy annak ellenére vírusokról beszélünk a szak- és a köznyelvben egyaránt, hogy *a szigorú értelemben vett számítógépes vírusok mára gyakorlatilag kihaltak. Manapság vírusok helyett leginkább férgekkel, trójai, reklám- és kémprogramokkal találkozhatunk*.

Ez a változás többek között azért tapasztalható, mert a vírusok „élettere", a számítógépes környezet is folyamatosan és alapjaiban alakult át az elmúlt két évtized alatt. Gyökeresen más például a manapság használt hardver- és szoftverkörnyezet, mint a kezdetekben, ráadásul napjainkban a személyi számítógépek már nem önálló munkaállomások, hanem az internet elterjedtségének köszönhetően egy világméretű hálózat részei.

Vegyük például az első dokumentált PC-s vírust, a *Brain*-t, amely 2006-ban ünnepelte huszadik születésnapját, és terjedéséhez kizárólag az 5,25"-os, 360 kilobájtos floppylemezek bootszektorát fertőzte meg. Mivel mára az 5,25"-os hajlékonylemezek gyakorlatilag eltűntek (a köznyelvben floppy alatt is a 3,5"-os adattárolót értjük), továbbá a mai modern számítógépek már floppymeghajtót sem tartalmaznak, ezzel a vírussal már csak vírusgyűjteményekben találkozhatunk.

Az ősi számítógépes vírusok terjedési sebességét jellemzi egyébként, hogy Magyarországra négy év alatt jutott el a *Brain* vírus – szemben minden idők leggyorsabb számítógépes kártevőjével, a *Slammer*-rel, amely a 2003. január 25-i kitörése alkalmával körülbelül negyed óra alatt körbejárta a világot. Érdekes a párhuzam az előbbi lassú terjedéses példával: a 2004 júniusában felfedezett, első mobiltelefonos féreg, a *Cabir,* amely kizárólag Bluetooth kapcsolaton terjed, ráadásul a hibásan megírt algoritmus miatt csak elég lassan (ezt az algoritmust a *Cabir* néhány későbbi változatában lecserélték). A „modern" PC-s kártevők terjedési sebességét megközelítő mobiltelefonos károkozó jelenleg még nem létezik, és véleményem szerint csak akkorra várható, amikor a mobiltelefonok többsége állandó internetkapcsolattal rendelkezik majd.

A jövő számítógépes vírusaira véleményem szerint – ellentétben a néhány évvel ezelőtt tapasztalható trenddel – elsősorban *nem a gyors terjedés lesz jellemző*. 2005-ig például a sajtó rendszeresen tudósított hatalmas víruskitörésekről (féregjárványokról), amelyek megbénították a számítógépes rendszereket, és világméretű fertőzéseket okoztak. Ilyen hírhedt kártevők voltak többek között a *Melissa,* a *Klez,* a *Bugbear,* a *Sobig,* a *Mydoom,*

a *Netsky* vagy a *Bagle.* Az elmúlt két évben érdekes módon már nem tapasztalhattunk az előbbiekhez hasonló méretű kitöréseket – *manapság (és a jövőben is) inkább kisebb, célzottabb támadásokra számíthatunk*, elsősorban azért, mert így a vírusirtó cégek feladata nehezebb (kisebb fertőzés esetén kisebb a „lebukás" veszélye), és a kártevők hosszabb ideig tudnak „életben maradni". Ráadásul a mai „modern" kártevők már általában nem is terjednek maguktól (hiszen nem ez az elsődleges céljuk), csak *az irányítást veszik át a számítógép felett*.

A mai, modern károkozók a fent említettek miatt például *már nem e-mailben érkeznek, hanem egyszerű böngészés útján kerülnek számítógépünkre*. Ez azt is jelenti, hogy nem lehet ellenük központosítva, a levelezőszervereken védekezni, hanem valós időben, a munkaállomáson kell megoldani a védelmet – ez lényegesen nehezebb feladat, hiszen a munkaállomások nem lassulhatnak le a víruskeresés miatt (ha egy e-mailt pár perc késéssel kapunk meg, az nem annyira zavaró, mint ha a böngészés lassulna le lényegesen). Tehát *minden eszközzel optimalizálni kell a víruskeresést*, ami nagyon nehéz feladat a rohamosan bővülő kártevőszám mellett.

A számítógépes kártevők folyamatosan változnak ma is, ám nemcsak technikai szempontból alakulnak át: a kezdeti, öncélú rombolás helyét átvette az üzleti alapú vírusírás – kevesen tudják, hogy a mai vírustámadások hátterében a kéretlen reklámlevelek és felbukkanó hirdetések állnak. A megfertőzött és így távolról irányítható számítógépek ezrei óriási, elosztott számítástechnikai kapacitást jelentenek a számítógépes vírusok készítői számára; kéretlen reklámlevelek küldésére, célzott internetes támadásra lehet ezeket a hálózatba foglalt, fertőzött gépeket felhasználni.

Mivel a megfertőzött és távolról irányítható számítógépek a bűnözők számára nagy értéket képviselnek, a mai modern kártevők (és véleményem szerint ez *a jövő vírusaira is igaz lesz*) *megpróbálnak minél tovább észrevétlenek maradni, az operációs rendszer legmélyére beépülni* – éppen ezért az úgynevezett *rootkit* technológiákat alkalmazó károkozók száma az utóbbi időkben drasztikusan emelkedett, ami komoly fejtörést okoz a biztonságtechnikai cégek számára. A Microsoft egyik szakértője, Mike Danseglio például arra hívja fel a figyelmet, hogy a legjobb védekezés egy ilyen rejtőzködő kártevő ellen a rendszer teljes újratelepítése.

Véleményem szerint *a jövő digitális károkozói is döntően üzleti alapon íródnak majd*, bár természetesen megmarad a későbbiekben is az ún. *proof-of-concept* irányvonal, vagyis minden programozható rendszerre megpróbálnak majd vírust írni, még akkor is, ha a kártevő soha nem fog tudni igazából elterjedni. Talán az egyik legjobb példa erre a *MenuetOS,* amely egy pár ezres felhasználói táborral rendelkező operációs rendszer, mégis írtak már rá két vírust is, az *Oxymoron*-t és a *Tristesse*-t.

A jövő digitális károkozói lényegesen kifinomultabbak lesznek, mint mai társaik, elsősorban az antivírusiparral való kiéleződő verseny miatt. Biztos vagyok benne, hogy megváltozik majd a kártevők támadási technikája is – ma elsősorban az operációs rendszer sebezhetőségeit használják ki a vírusok, *a jövőben a független gyártók alkalmazásai lesznek az elsődleges célpontok, hiszen azokra kevesebb figyelmet és energiát fordítanak, mint az operációs rendszerre*. A különböző kártevők közti határok elmosódnak, nem lehet egyértelműen osztályozni és csoportosítani őket (például: vírus, féreg) – már ma is olyan „hibrid" kártevőkkel

találkozunk, amit az angol szaknyelv „vírus" helyett inkább *threat*-nek nevez.

Egy dolog biztosan nem fog változni: *mindenképpen értenünk kell a számítástechnikához*, ráadásul naprakész információkkal kell rendelkeznünk a számítógépes biztonságtechnika területéről, hogy elfogadható biztonságban tudhassuk a munkánkat – *a technika* (vírusirtó programok, tűzfalak) *önmagában sajnos nem fog megvédeni bennünket*.

Kulcsszavak: *vírus, féreg, rootkit, kártevő, jövő*

IRODALOM

Farmosi István – Kis J. – Szegedi I. (1990): *Víruslélektan*. Cédrus, Budapest (http://mek.oszk.hu/03100/03153/03153.pdf)

F-Secure leírás a Brain vírusról, http://www.f-secure.com/v-descs/brain.shtml (2007. 01. 16)

F-Secure leírás a Slammer féregről, http://www.f-secure.com/v-descs/mssqlm.shtml (2007. 01. 16)

F-Secure leírás a Cabir féregről, http://www.f-secure.com/v-descs/cabir.shtml (2007. 01. 16)

Ismeretlen szerző: Who Wrote Sobig?, http://spamkings.oreilly.com/WhoWroteSobig.pdf (2007. 01. 16)

A MenuetOS operációs rendszer honlapja, http://www.menuetos.net/ (2007. 01. 16)

„Microsoft Says Recovery from Malware Becoming Impossible", http://www.eweek.com/article2/0,1895,1945808,00.asp (2007. 01. 16)