# Bevezető helyett

## Kiadói beszélgetés Szőr Péterrel, a vírusvédelem művészével

*Habent sua fata libelli, azaz minden könyvnek megvan a maga sorsa. Szőr Péter Magyarországon kezdett el foglalkozni a vírusok és a férgek elleni védekezéssel, majd az Egyesült Államokban, a legszélesebb nemzetközi szinten folytatta. Ismereteit, tapasztalatait összefoglalta a* Vírusvédelem művészete *(The Art of Computer Virus Research and Defense) című könyvében. Ez a könyv először angolul jelent meg, majd csehül és lengyelül, később kínaiul is. Végül, ha lassan is, de a magyar nyelvű változat is elkészült. Jobb későn, mint soha. De nem késett el ez a kiadás?*

Természetesen nagyon örülök, hogy a könyv végre a magyar olvasókhoz is eljuthatott. Amikor 2004-ben eldöntöttem, eljött az ideje, hogy könyvet írjak a vírusokról, főként az motivált, hogy úgy láttam, a vírusok fejlődése eljutott egy olyan komplex szintre, amelyet már nehéz meghaladni. Vagyis nehéz volt elképzelni, hogy ezen a területen „lesz még új a nap alatt". A könyvben igyekeztem úgy írni, hogy az olvasó végig érezze: a könyvben az ismertetett programok és technikák lényegében függetlenek attól a környezettől, amelyben futnak. Ugyanakkor az is célom volt, hogy bemutassam: a környezet olyan változásai, mint a biztonsági funkciók, az antivírusok megjelenése az operációs rendszerekben, milyen hatással van a kártékony programokra, és hogyan fejlődik az idők során egymásra hatva mind a két oldal.

Az utóbbi pár évben természetesen új környezetek jelentek meg, ezekben pedig vírusok, férgek és egyéb trójai programok. Kijött például az Apple iPhone-ja, és annak ellenére, hogy az Apple nem engedi meg az ismeretlen programok futtatását, hekkerprogramok ma már ki tudják iktatni az Apple védelmét, így lehetővé teszik, hogy a telefont más hálózatokon is lehessen használni az eredetileg engedélyezetthez képest. Ezt az ügyes programozó hekkerek olyan *exploitokkal* oldották meg, amelyek eredetileg egy képmegjelenítő funkció hibáját használják ki. Az exploitokat a könyv részletesen tárgyalja, továbbá bemutatja, hogy minden adatfájl, így egy képfájl is, veszélyes lehet egy adott környezetben. Érdekesség, hogy ennek ellenére az Apple iPhone-non a vírusok csak a feltört verziójú rendszereken vannak jelen, ahol más hibákat, például az SSH-háttérprogram hibáit, is ki tudják használni. Az utóbbi időben nagyon elterjedtek a facebookos kártékony programok is, hiszen a felhasználók milliói regisztrálták magukat az efféle rendszerekben. Az ilyen vírusok azt használják ki, hogy láthatók az emberek közötti kapcsolatok, így bizonyos felhasználói köröket könnyebb beugratniuk.

Teljesen beigazolódott az a tendencia is, amelynek a kezdetét már 2003–2004 körül éreztük. A vírusírás tökéletesen megváltozott, a hobbifejlesztésből a professzionális maffia szintjére került. Tényleg úgy működik minden, mint a maffiánál, hiszen a programozókat megfizetik a kártékony programok megírásáért, ezeket megint csak más emberek továbbadják olyanoknak, akik ezeket több ezer gépen, úgynevezett bot networkökön (automatikusan vezérelt hálózatokon) keresztül széles körben elterjesztik. Máskor az a cél, hogy személyre szabott támadást hajtsanak végre. A legtöbb kártékony program csak néhány, legfeljebb néhány tucat gépen van jelen. Így az a régi modell, amely arra épült, hogy minél több gépet vegyenek egyszerre célba, nagyon megváltozott. Néha egy-egy kártékony programot csak azzal a céllal írnak meg, hogy egy adott cégtől adatokat szerezzenek. Jó példa erre a Google ellen elkövetett kínai támadás, ezt a Google néhány gépén elhelyezett backdoorral oldották meg. Ugyanezt aztán több mint 30 másik mamutcégnél is megtették. Az ilyen támadásokat sokkal nehezebb észrevenni. Végül a pénzt a főnökök inkasszálják az ellopott adatok, a hitelkártyaszámok, a bankszámlaszámok, a kulcsszavak, az ellopott PIN számok révén. Ez ma milliárdos üzlet.

Amikor a víruskutatást elkezdtem, csak néhány tucat vírus volt ismeretes. El sem tudtam képzelni, hogy a vírus elleni védekezés jelentősége világméretűvé fog nőni az évek során. Az utóbbi években a kártékony programok fejlesztése, terjesztése és az adathalászat is milliárdos üzletté vált. Nagyon lényeges, hogy az ellenfél is motivált lett üzletileg, ugyanis ezen a ponton még nehezebbé válik a védekezés. A gyakorlatban hosszú távon a támadás sokkal gazdaságosabbá válik, mint a védekezés. Az utóbbi években „bűnbandák" ezzel a motivációval évente több millió kártékony kódot írtak. A védekezés pedig egyre nehezebb. Az antivírusprogramok nagy változásokon mennek át, és a fejlesztés főleg a kártékony funkciókkal szembeni viselkedésalapú (behavior blocking) védekezésre épül. Emellett megjelent az antivírusprogramokban a hálózatalapú védekezés, amely gyakorlatilag „pillanatra kész" adatbázist biztosít a felhasználóknak. Ez az antivírus-adatbázis nagy részét, a több millió azonosítórekordot egy szerveren tárolja, és a fájlokról készített „ujjlenyomat" alapján vagy akár a futó programnak egy távoli szerverre való teljes elküldésével összeveti a gépen futó programokkal. Ezekre a megoldásokra azért van szükség, hogy az antivírusprogramok ne lassítsák tovább a gépeket azzal, hogy az egyre jobban növekvő adatbázisokat a memóriában tartják.

És persze megjelentek új operációs rendszerek, például a Windows Vista, a Windows 7, amelyek új védekezési eljárásokat tartalmaznak. Ezek nagy részét a könyv, más környezetekben ugyan, de részletesen tartalmazza.

*A vírusírás bizonyos mértékig az egyéniség szabadságáról szól, éppúgy, mint a hekkelés. Sokan ezzel akarják megmutatni, hogy vannak olyan okosak és ügyesek, mint a sok pénzért dolgozó fejlesztők, sőt egy lépéssel előttük tudnak járni. Úgy tűnik azonban, hogy nemcsak a vírusírás, hanem a vírusok elleni védekezés is mintegy a hobbitevékenységből fejlődött ki. Milyen csoportok foglalkoznak ma a vírusvédelemmel, és hogyan áll a vírusírók és a vírusirtók versenye?*

Ez nagyon igaz. Azt mondanám, hogy akik régebben hobbivírusírókká váltak volna, ma inkább a rendszerbiztonságra koncentrálnak, és exploitokkal foglalkoznak. Ezt alapvetően azért teszik, hogy saját képességeiket bizonyítsák, de emellett támogatják a védekezést, és mindezt leggyakrabban fizetés nélkül. Vigyázni kell azonban, hogy ezek a kódok ne kerüljenek hamarabb a köztudatba, mint a védelmek. Jó példa erre a CodeRed és a Slammer férgek, amelyek percek alatt fertőztek meg több százezer számítógépet, és kódjuk publikus exploitokon alapult. Persze a hekkerek azt állítják, hogy nélkülük a hiba felfedezésére soha nem került volna sor, és ebben sok igazság van. Ám emellett etikailag is fontos, hogy ezeket a demonstratív exploitkódokat milyen módon terjesztik, mert hamarabb ki tudják használni őket támadásokra, mielőtt egy cég, például a Microsoft, egy adott hibát ki tud javítani a rendszerében. Ez különösen olyan esetekben nehéz, mint a Windows, amelynek sok nyelvre lefordított változata, kódja van, és ez megemeli a hiba elhárításának és tesztelésének az időigényét.

A vírusvédelem területére nagyon sokan érkeznek ilyen háttérrel, de egy magára valamit is adó antivíruscég ügyel arra, hogy senkit ne alkalmazzon, aki bármilyen formában „a sötét oldalról" jött. Nagyon sok programozó tanul bele a védelemfejlesztésbe, de ez olyan terület, ahol a támadásokat is részletesen ismerni kell. Nagyon sokat változott a világ az utóbbi 20 évben. Nagyon sok az érdeklődő, aki kihívást lát a védelem fejlesztésében, és „felveszi az odadobott kesztyűt".

*A könyv első kiadása óta eltelt öt év. Nyilván sok minden megjelent azóta, amivel frissíteni lehetne a leírtakat. Mivel erre sem idő, sem tér nincs, kérlek, röviden jellemezd, mi az, ami újdonság a víruskészítők térfelén, és mivel tudtak erősíteni a biztonságunkért dolgozók? Csak címszerűen: mi az, ami igazán hiányzik a most közreadott a szövegből?*

A védekezés oldalán nagyon fontos lenne írni arról, hogy a felhőalapú keresők hogyan hatnak a védelemre, és melyek a hibáik. Erről nem szól a könyv. Utoljára 2009-ben tartottam előadást Budapesten, a CARO szervezésében. Arról beszéltem, hogy az egyik prominens antivíruskereső hálózatalapú védelmében baljós hibát találtam, amellyel a keresőt a hálózaton kívülről ki lehetett iktatni, mintegy a „man in the middle attack" keretében. Ezekről a tanulságokról nagyon szeretnék még később írni. Tervezem, hogy írok egy második, kisebb kötetet a könyvhöz, amely ezeket az újdonságokat ismerteti.

A támadási oldalon a legérdekesebbnek azt az elméletet tartom, amelyet Dr. Chris Adamival együtt gondoltam végig. Chris biológus kutató, az evolúcióval foglalkozik, és ezt igyekszik prezentálni programkörnyezetben. A Virus Bulletin konferenciáján bemutattuk, hogy a vírusok a jövőben saját magukat fejleszthetik úgy, hogy még a saját szerzőjük sem tudja, hogyan kerülik ki a védelmeket. Mindezt az igazi evolúció működéséhez hasonlóan teszik. Persze elméletben mutattuk be ezt a lehetőséget, szimulációs környezetben, de biztó-

sak vagyunk abban, hogy megvalósítható. A védelmi programok például gyakran ellenőrzik, hogy egy programnak van-e felhasználói felülete. Ha van, akkor valószínűleg nem kártékony program (bár esetleg ez is lehet vírussal fertőzött). Szóval, amikor a vírusvédelem úgy dönt, hogy egy programot nem érdemes a fertőzött programok közé sorolni, ezt gyakran valami efféle egyszerű heurisztika alapján teszi. Képzeljünk el egy olyan programot, amely véletlenszerűen használja a Windows programozói interfészét, és egy adott ponton egy olyan rutint ír magába, amely megjelenít egy láthatatlan ablakot, amely felhasználói felületnek tűnik. Ezen a ponton a támadó program kicselezte a védekező programot, bár erről fogalma sem volt. Mivel az evolúció a működő dolgokat preferálja, automatikusan ilyen vírusokat fog ezután produkálni, és vigyáz arra, hogy ez a funkció sokáig, több generáción keresztül megmaradjon a vírus mutációiban.

Rengeteg analógiát lehet erre a természetben tálalni. Vannak például olyan hangyák, amelyek ha megfertőződnek egy vírussal, akkor úgy néznek ki, mint egy gyümölcs. A gyanútlan madarak megeszik, és megfertőződnek. Majd a vírus az elpottyantott ürülékkel távozik a madárból, ezt egy hangya elkapja, és minden kezdődik elölről. Ez az egész körforgás azon alapul, hogy a fertőzött hangya véletlenül gyümölcsre hasonlít. Sem a vírus, sem a hangya, sem a madár nincs ennek tudatában.

*Nagyjából megismerkedve a könyv témáival és szövegével, az a benyomásom támadt, hogy ez az írás nemcsak biztonságtechnikai információkat tartalmaz, hanem ennél általánosabban, sokat mond a programfejlesztés technológiájáról, a kód és az ember kapcsolatáról, a programozás pszichológiájáról. Ilyen értelemben a tanulságai túlmutatnak az eredeti célján. Mint professzionális oktató, kihasználhatónak látod a vírusépítő és a védekezési technológiák tapasztalatainak általánosítását a programozók tudásának a fejlesztésében?*

Igen, nagyon örülök, hogy ezt észrevetted. Számomra a víruskutatás mindig izgalmas párbaj volt: jön a program, majd az ellenprogram, és mindezt más és más számítógépeken lehet eljátszani. A játékelmélet erősen hat ezen a területen, szóval nagyon izgalmas az egész. Úgy gondolom, hogy minden programozónak tudnia kell, hogy a hibákat mások ki tudják használni. Ennek felismerése automatikusan jobb programozókat eredményez, akik többet törődnek a kódjuk helyességével.

*Végül, nemcsak a könyveknek, hanem a szerzőknek is megvan a maguk sorsa. Úgy hallottam, módosítottad a pályádat. Ez annyit jelent, hogy a vírusírók fellélegezhetnek?*

2009 végén sikerült begyűjtenem az „Év víruskeresője" trófeát a Symantec AntiVirus számára, Andreas Clementi tesztjén. Ezen a ponton úgy véltem, az utóbbi 10 évben a Symantecnél mindent megtettem azért, hogy a védekezési rendszerüket a középmezőnyből az élvonalba vigyem. És végre úgy gondoltam, hogy legalábbis egy kis időre lezárhatom ezt a témát, hogy valami más

érdekes dologgal foglalkozhassak. 20 év sok idő egy területen, és a rendszerbiztonság a „szívem csücske" marad. Így 2010-ben új céget alapítottunk a barátaimmal, és a Windows felgyorsításán fáradozunk. Furcsa az élettől, hogy ebben szerepet játszanak a lassúbb víruskeresők is, de mi az egész rendszer felgyorsításával foglalkozunk, azt kutatjuk és fejlesztjük, hogy mely programoknak van szerepük a számítógép helyes működésében, és melyek azok, amelyekre nincs szükség. Ez sokkal nagyobb probléma, mint a vírusos programok felfedezése, mert itt minden programot a működése alapján próbálunk kategorizálni. Célunk az is, hogy a hibás programokat javítani tudjuk. Ez lenne az úgynevezett „öngyógyító" szoftverkörnyezet, amelyben úttörő szerepet játszanak korábbi víruskutatók, például Dr. Steve White az IBM-től, de a jól ismert dr. Simonyi Károly professzor is foglalkozik ezzel a területtel *(http://www.hewettresearch.com/insider/doc/simonyi-2003.pdf)*.

Ehhez a projekthez anyagi támogatást kaptunk, így kis csapatunk lelkesen halad előre, és remélhetőleg a jövő év elején már a piacon lesz a termékünk. Az érdekes az, hogy a programok lassú működésének vizsgálata kapcsán gyakran találunk kártékony programokat is, így ez egyfajta közvetett védekezést jelent. Sokszor fedezünk fel olyan programokat, amelyek abban a környezetben, ahol több védelmi program is fut, hátsókaput (backdoor) rejtenek magukba. Ez nagyon érdekes és tanulságos nézőpont számomra. Egyszóval a jobb védelem kifejlesztése örök célom marad.