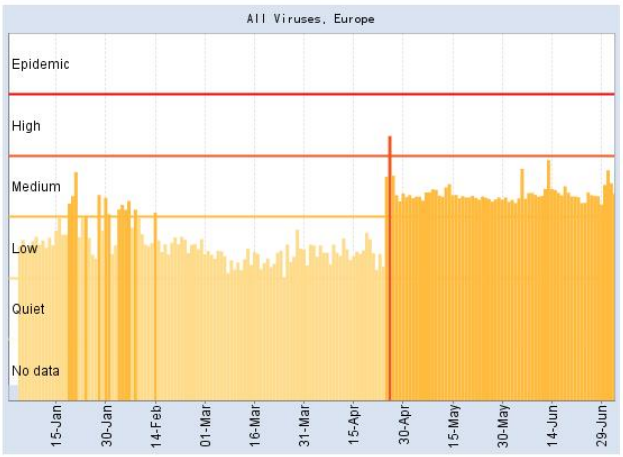
A MULTIMÉDIA ÉS A VÍRUSOK TERJEDÉSE
THE MULTIMEDIA AND THE SPREADING OF COMPUTER VIRUSES

Hermann Péter ***Bencze Katalin*** ***Sándor Tamás***
Pannon Egyetem Georgikon Mezőgazdaságtudományi Kar
8360 Keszthely
Deák Ferenc u. 16.
hermannpeti@yahoo.co.uk *benczekatalin@freemail.hu* *shx1317@mail.datanet.hu*

Absztrakt: Napjainkban a multimédia az élet szinte minden területére kiterjed. Gondoljunk csak a kamerás telefonokra, a digitális videózás elterjedésére, és különösen fontos a számítógépek és az Internet terén. Az internetet nemcsak szöveges adatok továbbítására használják, hanem multimédiás állományok továbbítására is. Viszont a legtöbb felhasználónak komoly gondot okoz, ha a letöltött állomány vírusos. A vírusok terjedése nem kímélte a videó-, kép-, és zenei állományokat sem. Az interneten tulajdonképpen ezen állományok segítségével terjedhetnek a vírusok a legkönnyebben.
A konferencián a vírusok fajtáit próbáljuk röviden bemutatni, különös tekintettel a legújabb álcázási módszerre, amelynek során videó- és képállományok segítségével terjeszthetők a vírusok. A prezentáció során kitérünk a vírusok elleni védekezés lehetőségére. Egy programon keresztül bemutatjuk, hogy hogyan lehetséges úgy védekezni a vírusok ellen, hogy az állomány megmarad a számítógépen és használható is. A vizsgálódás során a hatékonyság mellett a költségeket is fontosnak tartottuk számba venni. Természetesen a jelenlegi helyzet elemzése mellett feltárjuk, hogy a jövőben milyen területen jelenthetnek problémát a vírusok (pl. mobilkommunikáció) és ezek ellen milyenek a lehetőségek a védekezésre.

1. Bevezető

A kártékony kódok készítése napjainkra új gazdasági ágazattá vált. Az eltelt hat hónapban megfigyelhető legfontosabb irányzat a kártékony tevékenységek körének kiterjedése különféle új technológiákra és alkalmazásokra.



1. ábra
Vírusok elterjedése Európában 2007-ben

Fontos tendencia, hogy a vírusok nem csak az Interneten keresztül terjednek, hanem a mobilkommunikációt kihasználva akár MMS-eken keresztül is, valamint az Interneten keresztüli terjedést megkönnyíti a kártékony kódok elhelyezése multimédiás állományokban (pl. képi állományokban). Az ezen támadások mögött álló csoportok látszólag mind nagyobb on-line területeket kívánnak meghódítani, hogy a magánfelhasználók, a cégek és a közszféra elleni célzott támadásokra alapozva erős, önfenntartó fekete-gazdasági ágazatot hozhassanak létre. A tágabb értelemben vett multimédia területe is rendkívül jó táptalajt biztosít a vírusok számára, hiszen újabbnál újabb lejátszóprogramok jelennek meg, melyekben egy tapasztalt vírusíró számára gyerekjáték kártékony kódot elhelyezni, majd ezt letölthető programként teszi fel az Internetre, így biztosítva a vírus terjedését.

2. A vírusok csoportosítása

A vírusok károkozás céljára létrehozott, önreprodukáló programok. Hatásuk a lehető legkülönbözőbb: bizonyos fájlok letörlése, a winchester átkonvertálása, grafikus vagy zenei hatások, dokumentumok váratlan módosulása, gépünkről induló e-mail áradat, stb. Csoportosításuk működésük alapján lehetséges:

Bootvírusok: Ezek a merevlemezek vagy a floppy lemezek boot szektorát fertőzik meg. Normál esetben a boot szektor az operációs rendszer állományainak betöltéséhez szükséges kódot tartalmazza. Egy bootvírus lecseréli a boot szektor eredeti tartalmát saját kódjára és az eredeti tartalmat másutt fogja tárolni. Amikor később egy számítógép egy ilyen floppy lemezről indul el, a vírus átveszi a vezérlést és elrejtőzik a RAM-ban. Ő fogja ezután betölteni és elindítani az eredeti boot szektort és minden normálisnak fog tűnni. Ettől kezdve azonban a számítógépbe behelyezett összes floppy lemezt a vírus meg fogja fertőzni. A '90-es évek közepéig ezen kártevők alig 100-120 fős családja uralta a terepet. Ám a floppy lemezek mint adathordozók visszaszorulásával előbb fokozatosan, majd a végén rohamosan terepet veszítettek.

Fájlfertőzők: Ezek a vírusok általában az állomány végrehajtó programokat, vagyis a .com és .exe kiterjesztésű állományokat fertőzik meg, de időnként megtámadnak más állományokat is. Általános a .dll, az .ovl és az .ovr kiterjesztésűek, de lehetséges akár .jpg fájlok támadása is. Utóbbira példa a JPG Vulnerability Exploit, amely bár 2004 szeptemberében jelent meg, még manapság is okoz problémákat. Ennek oka, hogy a vírusirtó programok nem ellenőrzik automatikusan a .jpg fájlokat, csak ha "kézi ellenőrzésnél" azt állítjuk be, hogy az egész merevlemezt ellenőrizze. A másik gond, hogy mostanra más kópiák is születtek a vírusról, ennek megfelelően azok képesek fertőzni .bmp, .dib, .emf, .gif, .ico, .jfif, .jpe, .jpg, .pcx, .png, .rle, .tga, .tif, .wmf kiterjesztésű fájlokat is. A JPG Vulnerability Exploit akkor aktivizálódik, amikor a felhasználó egy speciálisan szerkesztett JPEG fájlt tekint meg. Ekkor a vírus elindul, és a segítségével a támadók kártékony kódokat futtathatnak le a fertőzött rendszeren. Ezen kódok a legelső változat esetében a következők voltak: Először megpróbálja kihasználni esetlegesen más JPEG állományok sérülékenységét, ezt követően a 64.186.138.100-as IP címről letölt, majd végrehajt egy w.exe nevű fájlt, majd a Windows system könyvtárába létrehoz egy s.exe fájlt. Bár a legtöbb adatbázis szerint a JPG Vulnerability Fájlfertőzőnek számít, az utóbb taglalt hatása (mármint a fájlok letöltése) alapján Trójai programnak is nevezhetnénk.

Trójai programok: Ezek tulajdonképpen hasznos programnak (pl. tesztprogramnak) álcázott pusztító célú programok. Működési elvük a következő: először csak egy kis méretű, gyanúsnak látszó tevékenységet nem végző modul töltődik le. Ez valamilyen jelre nyit egy kiskaput egy vagy több

port megnyitásával. Ezt követően valamilyen jelre vár. Ha ez megérkezik, akkor tölti le a további modulokat, például keyloggereket, programférgeket, backdoor programokat. Utóbbi a leggyakoribb, amivel a trójai program gazdája akár közvetlen utasítások fogadására is felkészíti a kártevőt. Például szabványos IRC programok közvetítésével jutnak el az utasítások a backdoor programhoz, és nagyméretű, akár több millió gépből álló botnet hálózat részévé züllesztik a PC-t. Ezek segítségével később akár webszerverek ellen is intézhetnek támadásokat.

Makróvírusok: A makróvírusokat a Microsoft Office alkalmazásokban használt (általában Visual Basic) makró nyelven írják meg. A makróvírusok jellemzően akkor terjednek, amikor egy fertőzött dokumentumot megnyitunk, vagy egy új dokumentumot elmentünk. Ez azért jelent gondot, mert az Interneten nagyon gyakran töltünk le szöveges állományokat. Ráadásul új makróvírust nagyon egyszerűen készíthetünk.

Companion (társ) típusú vírusok: A fertőzött programok tartalmát nem módosítják, így általában sikerrel kicselezik a változásdetektort alkalmazó vírusvédelmet. Működésük végső soron egy régi CEB szabályként ismert elven alapul. E szerint a .com kiterjesztésű fájlok végrehajtása megelőzi az .exe fájlokét, a sor végén pedig a .bat fájlok állnak. Az ilyen vírusok az .exe fájlokat úgy fertőzik meg, hogy a gazdaprogram mellett elhelyeznek egy azonos nevű .com fájlt, amely így előbb kap vezérlést, és a vírusprogram lefutása után meghívja az .exe gazdaprogramot is. Az előbbinél kissé bonyolultabb megoldásokkal találkozunk a .com fájlokat fertőző companion vírusoknál, hiszen a vírusnak előbb át kell neveznie a gazdafájlt valamilyen egyéb kiterjesztésre, ha rendszeresen vezérléshez kíván jutni.

Férgek: Általában nem szaporodnak, hanem az adott rendszer adataianak (pl. adott felhasználók jelszava) megszerzése a céljuk. Működésük során legfontosabb célkitűzésük, hogy rejtve maradjanak. Feladatuk elvégzése után gyakran megsemmisítik önmagukat. A januárban színre lépett „Small.DAM" a korábbiaknál kifinomultabb megtévesztési módszert alkalmazott. Különféle megrázó eseményekről, többek között az egész Európára kiterjedő viharos időjárásról szóló szalagcímek alá rejtőzve a „Vihar-féreg" ijesztő gyorsasággal, egyetlen éjszaka leforgása alatt elterjedt szerte a világon.

3. Vírusok elleni védekezés

A vírusok csoportosítása után felvetődik a kérdés, hogyan lehet tőlük megszabadulni. Sokan megoldásként törlik a vírusos állományokat, súlyosabb esetekben pedig formattálják a vírusos meghajtót (utóbbi megoldást végső módszerként természetesen napjainkban is alkalmazzák). A probléma ezzel a megoldással az, hogy törlés eredményeként eltűnik az adott állomány, illetve használhatatlanná válik a program. A multimédiás állományok esetében pedig sokszor előfordulhat, hogy nem törölhető pl. az adott képfájl. Gondoljunk csak például egy egyetemi honlap működtetésére, ahol különböző események vannak rögzítve képekben, és gyakori, hogy mindössze 1 gépen tárolják a képeket. Itt az állományok nem törölhetők. Sok esetben megoldható a víruskód kimetszése a fertőzött fileból. Elvileg sikerülhet a fertőzés előtti állapot teljes értékű visszaállítása. Erre antivírus programok zöme kínál lehetőséget. Ilyen program az F-secure Anti-Virus is. Ez egy olyan antivírus szoftver, amelyik több kereső magot tartalmaz (köztük az F-prot és AVP kereső). Segítségével széles körű, valós idejű vírus-felderítési és védelmi rendszer alakítható ki a főbb munkaállomás és szerver platformokon. Azonban az átlagfelhasználó számára fontos tulajdonsága a pozitívumok mellett az is, hogy nem ingyenes a használata. Jelenleg az F-secure anti-virus 2006-os változata (amelyről a frissítés 2007-esre ingyenes) 39,99 €, azaz nagyjából 10.000,- Ft.

2.ábra
F-secure Anti-Virus Működés közben

Főleg otthoni felhasználóknak (például diákoknak) van ingyenes megoldás is. Az avast! Home Edition egy teljesen működőképes csomag, amely kifejezetten otthoni felhasználásra készült. A Home Editiont az ALWIL ingyensen bocsájtja rendelkezésre a fogyasztók számára, így lehetőség nyílik számukra, hogy információkat tudjanak szerezni globális vírusfertőzésekről, a felhasználók véleményéről. Mindkét programhoz folyamatos frissítés is társul, ezáltal mindig felkészültek lehetnek a legújabb vírusokkal szemben, valamint mindkét szoftver magyar nyelvű.

3. ábra
Avast Home Edition 4.7 otthoni felhasználóknak

Természetesen felmerül a kérdés mindenkiben, hogy hogyan is működnek ezen antivírus szoftverek.

4. Antivírus szoftverek felépítése

Az antivírus szoftver három szintből áll, ahol minden szint az eggyel alatta lévőre épül.

Az első szint egy adatbázis (a vírusadatbázis), amely az egyes vírusok tulajdonságait tartalmazza. Többek között megadja, hogy a vírust milyen szekvenciával vagy milyen algoritmussal lehet megtalálni. Az irtás lépései is itt tárolódnak. Az algoritmusok egy virtuális gépen futnak, hogy az adatbázis gépfüggetlen lehessen. Így ha egy új adatbázis jelenik meg, akkor minden ezt használó víruskereső rögtön ismerni fogja az új vírusokat, függetlenül attól, hogy milyen gépen futnak. A

vírusok felismerése pontos kell, hogy legyen. Ezért az adatbázisban a leírás megmondja, hogy a vírus mely bájtjait kell beleszámítani az ellenőrzésbe, és milyen értéknek kell kijönni az ellenőrzőkód képzése után. Fontos, hogy írtást csak egzakt azonosítás után lehet végezni, illetve, hogy a keresés során ne változtassunk meg semmit a fájlokban.

A második szint egy vírusölő függvénykönyvtár, amelynek feladata a fájlokban való víruskeresés, a vírusok kiölése, stb. Annak érdekében, hogy ez a rész hordozható legyen a különböző géptípusok között, a könyvtár C-ben íródik. Az antivírus fájlokat képes keresni, tehát a bootvírust is fájlvírusként kezeli. Ilyenkor a teljes partíció a fájl, a cilinderek, fejek és szektorok száma pedig attributumként kérdezhető le. A fájloknak két típusát különbözteti meg: a primitívek és a konténerek. A primitívek közönséges fájlok, amelyek tartalmazhatnak vírusokat. A konténerek további primitíveket és konténereket tartalmazhatnak. Konténer például a tömörített fájl. A konténer kezelőprogramja biztosítja, hogy a konténeren belüli fájlokat ugyanúgy kezelhessük, mint a közönséges fájlokat. Egy fájl viszont lehet egyszerre primitív és konténer is. Példa erre az önkicsomagoló archív. A mai antivírusok esetében a program tulajdonképpen először csak megkeresi a vírust, majd egy grafikus felületen megkérdezi a felhasználót, hogy kiirtsa-e a vírust.

A harmadik szint az előbbinek megfelelően a felhasználói program. Ez a szint hívja meg a második szint rutinjait. Itt meg lehet adni az antivírus programnak, hogy mit kell ellenőrizni, és a program megadja, hogy az adott célhelyen található-e vírus. Amennyiben igen, akkor a következőket lehet választani: karanténba helyezni a vírusos fájlt, kiirtani a vírust a fájlból, vagy törölje a fájlt. A karanténba helyezés, illetve a törlés főleg akkor javasolt, ha az antivírus nem ismeri fel a vírus konkrét fajtáját, csak észleli. Az F-secure anti-virus ilyenkor a fájl helyreállítása lehetőséget fel sem kínálja, illetve az Avast 4.7 Home esetében fontos megemlíteni, hogy helyreállítást nem végez, csak törölni képes a vírust, valamint karanténba helyezni. A helyreállítás pedig akkor lehet jó, ha ismert a vírus fajtája. Ezen utóbbi megoldással az a gond, hogy a megbecsülhetetlen számú vírusátirat és mutáció miatt az egy „víruscsaládba" tartozó vírusoknak eltérő a mérete, így a vírus eltávolítása után nem biztos, hogy az eredeti, teljesen működőképes programállapotot állítjuk vissza. Egy hibás vírusmentesítés tehát újabb rejtett programhibákat hozhat be a rendszerbe. Súlyosabb esetben a vírus eltávolítása után adatvesztést is tapasztalhatunk. Következésképpen ahogy ezt az antivírus-gyártók is felismerték, célszerű azt megakadályozni, hogy a vírus a gépre kerüljön. Erre a megoldás a rezidens víruskereső (tulajdonképpen ilyen az F-Secure Anti-virus és az Avast 4.7 is), amik a számítógép memóriájában tartózkodnak, és valamennyi fájlműveletet ellenőriznek. Elvileg egyedüli hátrányuk, hogy a számítógép teljesítményét valamelyest visszafogják. További gondot jelent a JPG Vulnerability nevű vírusnál kifejtett probléma.

5. Platformfüggőség

Antivírus szoftvereket gyakorlatilag minden platformra forgalmaznak, bár kétségtelen, hogy Windows alá íródik a legtöbb, de például az F-Secure forgalmaz vírusirtót Linux platformra is. Igaz bár, hogy az OS X platformot nem fenyegetik vírustámadások, de antivírus megoldást azonban még itt is találunk, igaz főleg a Windowsos és Linuxos vírusok lebuktatására. Ilyen például a Sophos Anti-Virus 4.8.12.

6. A mobil eszközök vírusai

Az utóbbi hat hónapban a mobil eszközökre szakosodott vírusgyártók is kártékony kódok világgazdaságának egyre aktívabb résztvevőivé váltak. Az SMS alapú spam, vagyis személyre szabott kéretlen reklámüzenetek telefonos terjesztése említhető kirívó példaként ebben a gyorsan fejlődő csalási ágazatban. Komoly problémát jelentett a CommWarrior elnevezésű vírus, amely Bluetooth kapcsolaton és multimédiás üzeneten (MMS-en) keresztül terjed. Tulajdonképpen minden beérkező SMS és MMS üzenetre automatikusan egy fertőzött MMS-t küld. Az üzenet tartalma olyan, amelyet a vírus a készüléken lévő SMS-ek közül véletlenszerűen kiválaszt. A CommWarrior ezenkívül bármilyen a telefonhoz csatlakoztatott MMC kártyára felmásolja magát. Néhány telefonon a vírus az operátor logót a saját logójára cseréli, ezenkívül megnyit egy Oroszországban bejegyzett weboldalt is. Az utóbbi időben újabb vírusok megjelenését észlelték a kéziszámítógépekben használt Windows Mobile operációs rendszeren és a harmadik generációs Symbian S60 okostelefonokon (utóbbira példa az Appdisabler.R trójai, amely bizonyos segédprogramokat tesz működésképtelenné a telefonon, köztük az Antivírus szoftvert is). Riasztó jelenségként értékelhető, hogy a mobileszközökre készült, mind fejlettebb trójai programokat kereskedelmi vállalkozások fejlesztik, az ebből származó profit pedig a kártékony kódok iparának további növekedését segíti elő.

4. ábra
A CommWarrior vírus hatásai

Az F-secure Mobil Anti-Virus jelenleg a legátfogóbb megoldás az intelligens telefonok kártékony tartalom (például kéretlen üzenetek) elleni védelméhez, mivel a mobil eszközökön futó valós idejű védelmet és automatikus vírusvédelmi frissítéseket biztosít szabadalmaztatott SMS frissítési mechanizmuson és HTTPS kapcsolaton keresztül. Egyedüli hátránya ugyanaz, mint az előnye, mivel valósidejű védelmet biztosít, ezért lassítja a telefont. Viszont egyes készülékek esetében a tapasztalataim azt mutatták, hogy bár elindult az Antivírus szoftver, de működésének köszönhetően gyakorlatilag használhatatlanná vált. Viszont például a CommWarrior képes volt a készüléket megfertőzni (mármint amikor nem volt rajt az Antivírus). Szóval ezen megoldásnak fejlődnie kell, vagy inkább azt mondhatjuk, hogy ezt a problémát vélhetően a telefonok fejlődése fogja az Antivírus szempontjából megoldani.

Összefoglaló

Mint cikkünkből kiderült a vírusok folyamatosan fejlődnek, és alkalmazkodnak az új rendszerekhez és rendszerjavításokhoz. Bár a változatosság gyönyörködtet, ebben az esetben nem tudunk önfeledten örülni a változásoknak. Megoldást a vírusok ellen próbálhatunk keresni antivírus

programok segítségével, de az egyértelmű, hogy az IT-biztonságért folytatott küzdelem eleve védekező harc, amit nem lehet megnyerni, csak folyamatosan leküzdeni a támadásokat.

Irodalomjegyzék:

[1] Farkas Csaba: Windows és Office 2000 felhasználóknak, 55. o.

[2] Computer Panoráma 2007\1, 78. o.

[3] Computer Panoráma 2007\6, 62. o.

[4] Computer Panoráma 2007\7, 68. o.

[3] www.f-secure.com: vírusleírások; antivírus használati útmutató

[4] www.alwil.com: Avast Home Edition 4.7 bemutatása

[5] www.biztonsagportal.hu: vírusleírások

[6] Nagy Ferenc László szakdolgozata: Számítógépes vírusok és védelmi eljárások (www.nfllab.com/szakdoli/szakdoli.html)