Automatikus vírusvédelmi megoldások az Interneten

Dr. Leitold Ferenc (fleitold@veszprog.veszprem.hu)
Erdélyi Gergely (dyce@veszprog.veszprem.hu)
Laczkó Gábor (tiamat@veszprog.veszprem.hu)

(Az F025166 sz. OTKA támogatás segítségével.)

A számítógépes vírusok manapság egyre nagyobb mértékben veszélyeztetik a számítógépet használók munkáját. A vírusok elleni küzdelem az újabb operációs rendszerek (Windows 95, Windows 98), illetve makrózási lehetőségeket biztosító alkalmazások (Word for Windows, Excel for Windows, …) megjelenésével egyre nagyobb feladatot ró a vírusellenes szakemberekre. Tovább nehezíti a problémát a vírusok folyamatosan növekvő száma, illetve az is, hogy a vírusok készítői újabb és újabb technikákat vetnek be. Ezzel párhuzamosan a vírusellenes kutatások is újabb módszereket dolgoznak ki. Annak érdekében, hogy a vírusvédelem a még ismeretlen vírusokra is kellő gyorsasággal tudjon reagálni az Interneten keresztüli folyamatos kapcsolattartás jelenthet megoldást.

Bevezetés

Az első számítógépes vírus megjelenése óta a vírusok egyre nagyobb mértékben veszélyeztetik a számítógép-felhasználók munkáját. A vírusok elleni küzdelem az exponenciálisan növekvő vírusmennyiség miatt egyre nagyobb feladatot ró a vírusirtókra. További gondot jelent, hogy a számítógépek fizikai korlátai (memória) határt szabnak a nagy számú vírus-információ tárolásának Nagyon nagy szükség van ezért olyan módszerek kidolgozására, amelyek a vírusvédelmet - a nagy vírusszám ellenére - hatékonyan képesek megoldani.

Vírusfertőzési technikák

Az első vírusok tulajdonképpen nem tartalmaztak különösebb álcázási technikákat, egyszerűen csak fertőztek. Általában az eredeti hordozó programot sem tették tönkre, az visszaállítható maradt. Előfordult, hogy a vírus rezidensen a memóriába került, de az is, hogy a szaporodását a memóriában maradás nélkül biztosította. Az előbbi esetben a vírus lényegesen gyorsabban volt képes terjedni, de könnyebben fel lehetett fedezni. Ezzel szemben az utóbbi esetben a vírus ugyan lassabban terjedt, de a felfedezése körülményesebb volt.

A következő csoportba tartozó vírusokat két fő osztályba sorolhatjuk. Egyik osztályukra az jellemző, hogy a lappangási idejük alatt nehezen felfedezhetőek, mivel ezen vírusok már *lopakodó (stealth),* illetve *polimorf* jellegűek.

- **Lopakodó vírusok:** Jellemzőjük, hogy megpróbálnak úgy terjedni, hogy a felhasználó csak nagyon nehezen vehesse észre a vírus jelenlétét. Ennek érdekében például a file végéhez fűződő vírusok esetén, ha azok már bekerültek a memóriába akkor a file-ok eredeti hosszát mutatják, néha még a file eredeti tartalmát is szimulálják. A lopakodó boot-vírusok pedig az eredeti boot-szektort mutatják meg, elfedve vele jelenlétüket.

- **Polimorf vírusok:** Ezek a vírusok nem úgy próbálnak elbújni, hogy szimulálják a gép fertőzésmentes állapotát, hanem önmagukat titkosítják, változtatják megnehezítve ezzel felismerésüket.

A másik osztály a *felülíró (overwrite), gyorsan pusztító vírusok.* Ezek már a hordozó programot is tönkreteszik, így jelenlétük azonnal felfedezhető, de ekkor már többnyire a vírus az állományok nagy részét megfertőzte, azaz tönkre is tette.

- **Felülíró, gyorsan pusztító vírusok:** A *felülíró vírusok* általában azzal okoznak adatveszteséget, hogy a fertőzés előtti állapotot nem tárolják el, hanem egy az egyben felülírják a megfertőzendő programterületet. Ebbe a kategóriába tartoznak a legrövidebb vírusok, hiszen nekik nem kell az eredeti állapotot szimulálniuk.

A vírusok újabb csoportja azt használja ki, hogy a DOS-nak a fentebb említett módokon túl még elég sok kiskapuja van a vírusok számára. Így egy-egy új vírus úgy tud a legkönnyebben megélni, ha olyan módszerrel szaporodik, amit az eddigi vírusvédelmek nem ismernek.

- **CEB vírusok:** Az újabb típusú vírusok legszemléletesebb példája a *CEB (companion)* vírusok megjelenése volt. A CEB vírusok működése azon az elven alapszik, hogy a DOS a futtatható állományokat prioritási sorrendben kezeli. Amennyiben a felhasználó egy program indításánál a kiterjesztést nem adja meg, úgy a DOS a prioritási sorrendben az első létező programot indítja. Ez a prioritási sorrend a kiterjesztések alapján: .**C**OM, .**E**XE, .**B**AT. Így egy CEB vírusnak semmi mást nem kell tennie, mint keresni egy .EXE vagy .BAT kiterjesztésű file-t és ugyanolyan néven, de .COM (vagy .EXE) kiterjesztéssel lemásolnia magát. Ha ezek után az újonnan létrehozott .COM állományt Hidden (rejtett) jelzővel látja el, akkor az a DIR parancsra nem jelenik meg, vagyis a vírus láthatatlan ! Mivel a vírus terjedése egy egyszerű COPY parancsnak fogható fel, nem keltette fel a vírusvédelmek gyanúját sem.

- **Device vírusok:** A device vírusok a device driver-ek működésébe avatkoznak be, a DOS legalsó szintjén dolgoznak, így a vírusvédelmek többsége alá kerülnek. Mivel az operációs rendszer magjába ágyazzák be magukat szinte tökéletesen tudnak lopakodni.

- **ANSI bombák:** Ezek a vírusok azt használják ki, hogy a DOS által a képernyőre kiírt szöveg tartalmazhat olyan vezérlő kódokat amelyek a billentyűzetet átdefiniálhatják, így egy egyszerű TYPE parancs kiadása után egy billentyűlenyomásra elindulhat egy, akár vírusos program is. Ez a módszer csak az ANSI.SYS használatánál lehetséges.

Makróvírusok

Ma a makróvírusok okozzák a legtöbb fertőzést. Számuk 1998 februárjában már meghaladta a 2000-et. Ezek között már megjelentek olyanok is, amelyek képesek Word dokumentumból végrehajtható állományokat, valamint ezekből a végrehajtható állományokból Word dokumentumokat fertőzni.

A makróvírusok fogalma nem új, 1989-ben Harold Highland volt az első aki megjósolta őket. Ekkor születtek az első tanulmányok a makróvírusok írásának lehetőségéről. Joel McNamara 1994-ben egy tanulmányt is írt ezekről a vírusokról, sőt ő maga is készített egy ilyen vírust

DMV néven. Ezt azonban titokban tartotta az első igazi makróvírus a Concept megjelenéséig, ami a megfelelő eszközök és ismeretek hiányában gyorsan elterjedt.

A Concept nagyarányú elterjedése már újabb és újabb makróvírusok megjelenését eredményezte. A makróvírusok megírásához ugyanis nem szükséges a gép mélyebb ismerete. A DOS vírusoktól eltérően a makróvírus nem a gép Assembly utasításkészletéből építkezik, hanem valamely makrónyelv lehetőségeit használja ki, mely a magasszintü programozási nyelvek eszközeivel teszi egyszerűbbé a vírusok készítését.

Elterjedségének másik oka, hogy a Word alatt terjedő vírusok a WordBasic makrónyelv parancskészletét használják. Ily módon függetlenek magától az operációs rendszertől, akár különböző platformokon is terjedhetnek, feltéve ha azokon léteznek kompatibilis WordBasic értelmezők. Például a Word-nek van Macintosh gépeken futó változata is, így ezek a vírusok PC-ről Macintosh-ra, illetve visszafelé is terjedhetnek!

A Concept megjelenése után a vírusirtó cégek is elkezdtek komolyan foglalkozni a makróvírusok kérdésével. A fokozott figyelem ellenére egy másik vírusnak a CAP-nak sikerült ismét széles körben elterjedni. Ez a vírus elsőként valósította meg a teljesen nyelvfüggetlen terjedést. A vírus elterjedéséhez hozzájárulhatott az is, hogy makróit a fertőzött dokumentumban, külön segédeszköz nélkül nem lehet megnézni.

Ezzel párhuzamosan a népszerűbb alkalmazásokra is megjelentek az első makróvírusok, illetve Trójai Falovak (Excel, AmiPro, Lotus, stb.). Ezek száma azonban az Excel vírusok kivételével azóta sem emelkedett.

A következő lökést a “vírusvédelem”-mel ellátott WinWord 8 (WinWord/Office97) jelentette. Ebben a programban kétféle vírusvédelem is jelen van. Az egyik jelez minden olyan dokumentumnál ami makrót tartalmaz, a másik képes néhány Word6/7-es makróvírust a konvertálás során felismerni.

Ezek a védelmek azonban nem érnek túl sokat, a programban megjelent új lehetőségekkel szemben. Ezek közül a legfontosabb, és a legtöbb bajt okozó a makrók konvertálása. Az Office 97-ben mindegyik alkalmazás “egységes” makrónyelvet kapott, azonban a WinWord a kompatibilitás megőrzése miatt képes a régebbi WordBasic-ben írt makrókat átkonvertálni az új Visual Basic környezetbe. Mivel ez automatikusan történik a betöltött vírusból automatikusan keletkezik egy új variáns, ami már képes az új környezetben működni.

Automatikus vírusvédelmi módszerek

Egy új, ismeretlen vírus megjelenésével a szakembereknek el kell végezniük a vírus vizsgálatát, felvételét a vírus-adatbázisba, valamint elkészíteni a vírus ellenszerét. Ez a feladat a naponta megjelenő 5-10 egyre bonyolultabb és bonyolultabb, újabb és újabb technikákat felvonultató vírus esetén rengeteg manuálisan elvégzendő munkafázist jelent. Célszerű ezeket a tevékenységeket automatikus, illetve félautomatikus rendszerek használatával egységessé és ezáltal könnyebben kezelhetővé tenni. Ezen tevékenységek automatizálásában az első lépésünk egy, a vírusok keresési és eltávolítási algoritmusait leíró formalizmus, a VIRSKILL (Virus Searching and Killing Language - Vírus Kereső és Irtó Nyelv) létrehozása volt [1,2,3].

A VIRSKILL formalizmus használatával a vírusok keresési és eltávolítási algoritmusainak a kezelése vált egységessé és így egyszerűbbé, de ez önmagában nem csökkentette a vírusokra

fordított manuális munkát: el kellett végezni a a vírusok vizsgálatát, a keresési és eltávolítási algoritmusok elkészítését, valamint a vírusok felvételét a vírus adatbázisba. Ezen cél megvalósításában hatékony segítséget nyújtott az Automatikus Vírusanalizáló Rendszer (AVAS - Automatic Virus Analyser System) [4,5]. Ez a rendszer már képes arra, hogy a vírusok nagy részének az esetében automatikusan előállítsa az adott vírus keresési és irtási algoritmusát. Ezt nagy számú vírusminta elkészítésével és a vírusmintákból bizonyos következtetések levonásával éri el. Az AVAS rendszer már alkalmas arra, hogy akár az interneten on-line segítséget nyújtson egy esetlegesen még ismeretlen vírussal fertőzött rendszeren a vírus eltávolításában.

Az AVAS célja

Egy vírus vizsgálata során az AVAS az alábbi alaptulajdonságokat állapítja meg:

- a vírus milyen kódterületeket fertőz,
- polimorf, vagy nem polimorf a vírus,
- melyik antivírus milyen néven azonosítja, tökéletesen el tudja-e távolítani,
- szerepel-e már a víruspéldány az adatbázisban.

Elképzelhető, sőt gyakori, hogy egyes (pl. terjedési) tulajdonságok különböző operációs rendszer alatt vizsgálva mások és mások. Így kívánatos a vizsgálatot több operációs rendszer alatt is elvégezni. Ez csak tovább növeli a rengeteg ismétlődő tevékenység számát.

Az alaptulajdonságok megállapítását követően az AVAS képes arra, hogy elkészítse a vírus keresési és irtási algoritmusát VIRSKILL nyelven. Az elkészített algoritmusokat nagy számú vírusfertőzésen ellenőrzi. Ezek után, amennyiben a víruspéldány még nem szerepelt a vírus adatbázisban, úgy a vizsgálat minden eredményével együtt bekerül oda.

Az AVAS működése

Az AVAS két fő fázisban működik: Vírusszaporítás és Analízálás.

A vírusszaporítás a boot és a filevírusok esetén emulált környezetben történik. Attól függően, hogy a vírus mennyire igényel speciális környezetet a szaporodáshoz különböző “szaporító” környezetek állnak rendelkezésre. Amennyiben a vírus a LINUX operációs rendszer alatt futó DOS emulátor alatt képes szaporodni, úgy 5-10 perc alatt képes a vírus szaporítását elvégezni. Amennyiben viszont a vírus az emulált rendszeren nem működik tökéletesen és nem szaporodik, úgy a kétgépes rendszer képes elvégezni a szaporítást. Az AVAS által jelenleg támogatott operációs rendszerek magukba foglalják a vírusok kezdeti célpontját, az MS-DOS operációs rendszereket csakúgy, mint a Windows alapú operációs rendszereket (Windows 95, 98, NT).

A makróvírusok esetén a szaporítás sokkal nehezebben oldható meg. Itt ugyanis nemcsak az operációs rendszert, hanem a „futtató környezetet”, magát a makrókat futtató alkalmazást is emulálni kell. A futtató alkalmazás pedig egyre tágabb körű: Word, Excel, Access, Powerpoint, … .

Irodalomjegyzék

[1] Leitold, F.; Csótai, J.: Virus Searching and Killing Language
Proceeding of the 2nd International Virus Bulletin Conference, Edinburgh, 1992, pp. 159-172.

[2] Leitold, F.: Vírus kereső és irtó nyelv
Proceeding of the HISEC'93 Conference, Budapest, 1993, pp. 253-265.

[3] Leitold, F.: A számítógépes vírusok felismerésének elmélete és gyakorlata
Kandidátusi értekezés, Budapest, 1994

[4] Leitold, F.: Automatic Virus Analyser System
Proceeding of the 5th International Virus Bulletin Conference, Boston USA, 1995, pp. 99-107.

[5] Leitold, F.: Automatikus vírusanalizáló rendszer
Proceeding of the HISEC'96 Confrence, Budapest, 1996, pp. 112-119.