MIT IS MONDOTT? HOGY IS HÍVJÁK?
ELIGAZODÁS A KÁRTEVŐK VILÁGÁBAN

Dr. Leitold Ferenc, fleitold@veszprog.hu

Veszprémi Egyetem – Veszprog Kft.

A világon a legelterjedtebb vírusok legautentikusabb forrása a Wildlist szervezet honlapja, melyen (általában) havonta jelenik meg a legelterjedtebb kártevők listája. Ez a lista a a világ legelismertebb szakértőinek jelentésein alapul és kitűnő információs anyag a szakértőknek. Ők mindig pontosan tudják, hogy melyik vírus melyik. Sajnos az átlagos számítógép felhasználók nem képesek azonosítani a kártevők neveit. A 'description' menüpont alatt némi információ olvasható a vírusokról, azonban ezekkel kapcsolatban néhány probléma adódik:

- Az utolsó elérhető információk már nem aktuálisak.
- Az információk az F-Secure adatbázisán alapulnak, így az elnevezések az F-Secure neveihez kötődnek.
- Néhány esetben nincsen információ egyes elemekhez.
- Néhány esetben azonos információk tartoznak különböző variánsokhoz.

A kártevő nevek egységesítési stratégiák

Jelenleg néhány szervezet foglalkozik azzal, hogy a kártevők neveit megpróblja egységesíteni.

- EICAR (European Institute of Computer Antivirus Reseaerch): a CAMDIER projektje keretében foglalkozik a kártevők neveinek az egységesítésével.
- US-CERT: 2004 novemberében nyilatkozatot adtak ki arról, hogy 2005 első negyedévében megoldást keresnek a problémára. 2005 szeptemberében hoztak létre egy szervezetet (CME – Common Malware Enumeration), mely a legelterjedtebb kártevők közös elnevezésével foglalkozik.

Sajnos a gyakorlatban elképzelhetetlen, hogy a kártevők azonos elnevezését kialakítsuk. Ez abból adódik, hogy a vírusvédelmek azonosítási algoritmusai különbözők. Léteznek olyan kártevők, melyeknek különböző példányait egyes vírusvédelmek különböző neveken illetnek, hiszen például több azonosítási algoritmust használnak. Más antivírusok viszont azonos néven illetik az adott kártevő különböző példányait is. Előfordulhat az is, hogy egy antivírus különböző kártevőket nem különböztet meg, azonos algoritmust használ az azonosításukra. Ebben az esetben a kártevők azonosítására szolgáló nevek átnevezése nem jelenthet megoldást.

Checkvir Real-time AV tesztelés

Ebben a szituációban az egyedüli jó megoldás a kártevők egzakt neveinek kereshető publikálása lehet, amelyek így már használtok azonosításra.

A probléma megoldását egy Real-Time antivírus ellenőrző rendszer adhatja. Ez a rendszer alkalmas arra, hogy az elterjedt vírusokkal, illetve a vírusvédelmek verzióival lépést tartva, **naprakész információkkal szolgáljon a vírusvédelmek által használt elnevezésekről, illetve az antivírusok legfontosabb minősített paramétereikről** valamennyi számítógép felhasználó számára. A rendszer képes arra, hogy észlelje az antivírusok újabb verzióinak a megjelenését és automatikusan az előre elkészített vírusgyűjteményen néhány futtatást (keresést és eltávolítást) hajt végre, az eredményeket kiértékeli és az Interneten elérhetővé teszi. Egy újabb vírus, féreg megjelenésekor is végrehajtódik az ellenőrzés, illetve ennek megfelelően frissítésre kerülnek az adatok. Az így létrejövő adatbázisban megfelelő kereséssel az egyes vírusnevek összerendelhetők és bárki lekérdezheti, hogy a saját számítógépén talált kártékony kód pontosan milyen fertőzést takar. A futtatások során ellenőrizhető az eltávolító algoritmus eljárása: hogyan és milyen módon történik az eltávolítás (törlés, irtás, esetleg nem tudja eltávolítani.

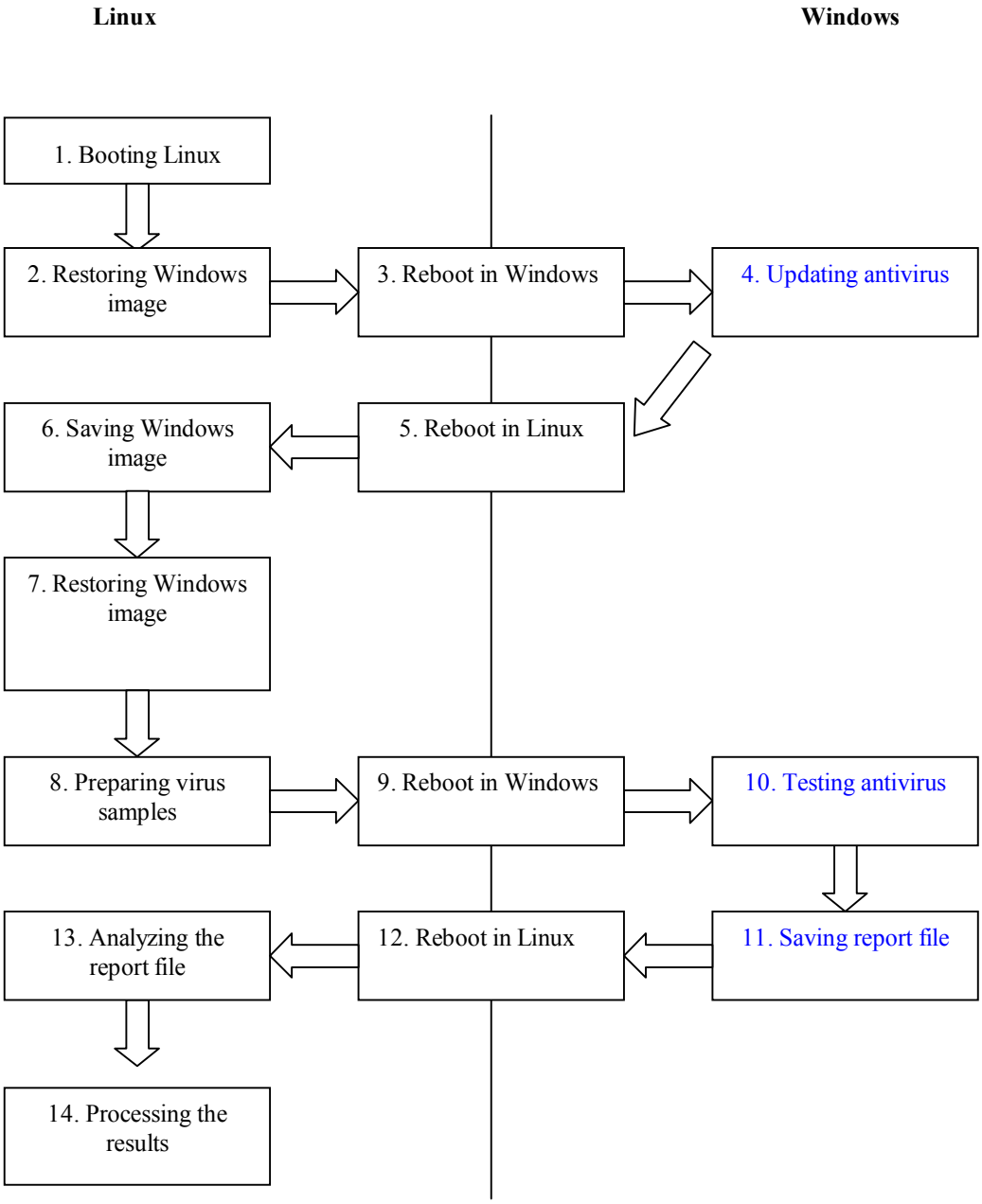
A Real-time antivírus ellenőrzések egzakt információkat biztosíthatnak a kártevők azonosításához, ami magában foglalja az antivírus termék nevét, verzióját, build számát, adatbázis verzióját, … Lehetőség van továbbá korábbi információk keresésére is.

Tesztelési eljárás

A tesztelési eljárás néhány egyszerű lépésből áll, melyek mindegyike automatikusan végrehajtható. Két külön számítógépet használunk a célra. Az egyik feladata, hogy elvégezze a vírusvédelmek frissítését és a frissített antivírushoz tartozó image fájlt elmentse. A másik számítógép az elmentett image-ek felhasználásával képes arra, hogy a teszteket biztonságos körülmények között lefuttassa.

Az eljárás az alábbi lépésekből áll:

1. Linux indítása
2. Windows image visszaállítása (ez tartalmazza a telepített antivírust)
3. Újraindítás Windows-ban
4. Az antivírus frissítése
5. Újraindítás Linux-ban
5. Windows image visszaállítása (ez tartalmazza a telepített antivírust)
6. Windows image visszaállítása biztonságos környezetben
7. Kártevők mintáinak az előkészítése
8. Újraindítás Windows-ban
9. Vírusvédelem tesztelése (on-demand és/vagy on-access)
10. Naplófájl, képernyőkép mentése
11. Újraindítás Linux-ban
12. Naplófájl analizálása
13. Eredmények feldolgozása


Linux
Windows
1. Booting Linux
2. Restoring Windows image
3. Reboot in Windows
4. Updating antivirus
5. Reboot in Linux
6. Saving Windows image
7. Restoring Windows image
8. Preparing virus samples
9. Reboot in Windows
10. Testing antivirus
11. Saving report file
12. Reboot in Linux
13. Analyzing the report file
14. Processing the results

Az alábbi minták néhány speciális esetet mutatnak a tervezet outputra.

W32/Zafi.A

Product name	Version(s)	Virus name(s)
Kaspersky Anti-Virus Workstation	4.5.0.95, 80673 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 82614 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 84230 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 87139 (known viruses)	I-Worm.Zafi
Kaspersky Anti-Virus Workstation	4.5.0.95, 89257 (known viruses)	I-Worm.Zafi
Kaspersky Anti-Virus Personal	5.0.121, 91566 (known viruses)	I-Worm.Zafi
Kaspersky Anti-Virus Workstation	4.5.0.95, 93606 (known viruses)	I-Worm.Zafi.a
Kaspersky Anti-Virus Workstation	4.5.0.95, 96130 (known viruses)	I-Worm.Zafi.a

Product name	Version(s)	Virus name(s)
McAfee VirusScan Enterprise	7.1.0, 4313 (virus definitions), 4.2.60 (scan engine)	New Malware.b (Virus)
McAfee VirusScan Enterprise	7.1.0, 4327 (virus definitions), 4.2.60 (scan engine)	New Malware.b (Virus)
McAfee VirusScan Enterprise	7.1.0, 4339 (virus definitions), 4.3.20 (scan engine)	New Malware.b (Virus)
McAfee VirusScan Enterprise	7.1.0, 4351 (virus definitions), 4.3.20 (scan engine)	New Malware.b (Virus)
McAfee VirusScan	v4.5.1 SP1, 4.0.4360 (virus definitions), 4.3.20 (scan engine)	W32/Zafi@MM
McAfee VirusScan Enterprise	7.1.0, 4367 (virus definitions), 4.3.20 (scan engine)	W32/Zafi.a@MM
McAfee VirusScan Enterprise	7.1.0, 4380 (virus definitions), 4.3.20 (scan engine)	W32/Zafi.a@MM
McAfee VirusScan	v4.5.1 SP1, 4.0.4385 (virus definitions), 4.3.20 (scan engine)	W32/Zafi.a@MM

Product name	Version(s)	Virus name(s)
NOD32 Antivirus System	2.000.9, 1.601 (virdef ver), 4157 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.633 (virdef ver), 4239 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.686 (virdef ver), 4368 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.725 (virdef ver), 4459 (virdef build)	Win32/Zafi.A worm
NOD32 Antivirus System	2.000.9, 1.767 (virdef ver), 4558 (virdef build)	Win32/Zafi.A worm
NOD32 Antivirus System	2.000.9, 1.792 (virdef ver), 4620 (virdef build)	Win32/Zafi.A worm
NOD32 Antivirus System	2.000.9, 1.820 (virdef ver), 4696 (virdef build)	Win32/Zafi.A worm
NOD32 Antivirus System	2.000.9, 1.840 (virdef ver), 4748 (virdef build)	Win32/Zafi.A worm

W32/Sober.E@mm

Product name	Version(s)	Virus name(s)
Kaspersky Anti-Virus Workstation	4.5.0.95, 80673 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 82614 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 84230 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 87139 (known viruses)	I-Worm.Sober.e
Kaspersky Anti-Virus Workstation	4.5.0.95, 89257 (known viruses)	I-Worm.Sober.e
Kaspersky Anti-Virus Personal	5.0.121, 91566 (known viruses)	I-Worm.Sober.e
Kaspersky Anti-Virus Workstation	4.5.0.95, 93606 (known viruses)	I-Worm.Sober.e
Kaspersky Anti-Virus Workstation	4.5.0.95, 96130 (known viruses)	I-Worm.Sober.e

Product name	Version(s)	Virus name(s)
McAfee VirusScan Enterprise	7.1.0, 4313 (virus definitions), 4.2.60 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4327 (virus definitions), 4.2.60 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4339 (virus definitions), 4.3.20 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4351 (virus definitions), 4.3.20 (scan engine)	W32/Sober.e@MM (Virus)
McAfee VirusScan	v4.5.1 SP1, 4.0.4360 (virus definitions), 4.3.20 (scan engine)	W32/Sober.e@MM (Virus)
McAfee VirusScan Enterprise	7.1.0, 4367 (virus definitions), 4.3.20 (scan engine)	W32/Sober.e@MM (Virus)
McAfee VirusScan Enterprise	7.1.0, 4380 (virus definitions), 4.3.20 (scan engine)	W32/Sober.e@MM (Virus)
McAfee VirusScan	v4.5.1 SP1, 4.0.4385 (virus definitions), 4.3.20 (scan engine)	W32/Sober.e@MM (Virus)

Product name	Version(s)	Virus name(s)
NOD32 Antivirus System	2.000.9, 1.601 (virdef ver), 4157 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.633 (virdef ver), 4239 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.686 (virdef ver), 4368 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.725 (virdef ver), 4459 (virdef build)	Win32/Sober.E worm
NOD32 Antivirus System	2.000.9, 1.767 (virdef ver), 4558 (virdef build)	Win32/Sober.E worm
NOD32 Antivirus System	2.000.9, 1.792 (virdef ver), 4620 (virdef build)	Win32/Sober.E worm
NOD32 Antivirus System	2.000.9, 1.820 (virdef ver), 4696 (virdef build)	Win32/Sober.E worm
NOD32 Antivirus System	2.000.9, 1.840 (virdef ver), 4748 (virdef build)	Win32/Sober.E worm

Irodalomjegyzék

Leitold, F.: The solution in the naming chaos Proceedings of the 14th International EICAR Conference, Malta, 2005.

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

Leitold, F.: Independent AV testing Proceedings of the 11th International EICAR Conference, Berlin Germany, 2002.

EICAR Cyber Attack Methods Detection & Information Exploitation Research Project, http://www.eicar.org/camdier/

Order To Come To Virus Naming Chaos, http://www.techweb.com/wire/security/54200541, November 24, 2004