Antivirusni programi na Linux platformi

DORS & CLUC 2004

Ivan Guštin
ivan@elin.hr

ELIN, HULK

Uvod

- Sadržaj:
  - zašto antivirusna zaštita na Linuxu
  - izvedbe antivirusne zaštite na Linuxu
  - open source rješenja
  - komercijalna rješenja
- ovlašteni partner za komercijalni AV
- bez informacija o kvaliteti detekcije pojedinih AV
- situacija: početak travnja 2004.

Izvorni virusi za Linux

- zbog različitog imenovanja, teško je dobiti njihov točan broj
- procjene govore da se radi o oko 40-tak *native* Linux virusa, a tek se poneki raširio
- to je tek oko 0.05% ukupno poznatih virusa i njihovih varijanti
- trojanaca i crva ima više
- porastom broja korisnika Linuxa, očekuje se rast broja virusa

Izvorni virusi za Linux

- prema podacima jedne komercijalne AV tvrtke, u njihovoj bazi uzoraka postoji za Linux (uključujući sve varijante):
  - 55 virusa
  - 16 crva
  - 73 trojana
  - ukupno: 144

Virusi na Linuxu?

- neki od prvih: Staog i Bliss, pravi virusi koji se “zalijepe” na izvršne programe
- suprostavljena dva mišljenja:
  - na Linuxu neće i ne može biti virusa
  - na Linuxu može i bit će sve više virusa
- Security Focus, listopad 2003.
  - Scott Granneman objavio članak: “Linux vs. Windows Viruses”, izazvao velike polemike
  - reakcija VirusBulletina i drugih kolumnista

Virusi na Linuxu?

- broj virusa za DOS/Windows:
  - 1987. - 10
  - 1990. - 220
  - 1993. - oko 3.500
  - 2002. - oko 65.000
- broj virusa za Linux:
  - 2002. - oko 130 (Virus Bulletin)
  - 2004. - oko 150 (ESET)

Zašto AV programi na Linuxu?

- Linux je danas u heterogenim mrežama:
  - file server
  - mail server
  - Internet gateway
- rastući broj korisnika Linuxa
  - povećava interes autora virusa
  - povećava broj žrtava zbog lošeg updatea i veće neopreznosti
  - *Does anybody have a fix for the human stupitidy bug?*

Zašto AV programi na Linuxu?

- postoje slični rizici:
  - socijalni: Windows+ Linux+
  - aut. attachmenti: Windows+ Linux+
  - brisanje podataka: Windows+ Linux+
  - propusti u browseru: IE+ Mozilla+
- postoje razlike:
  - brisanje OS-a: Win 9x/ME+ Linux-
  - default root/admin: Win XP+ Linux-
    - iznimka: Linspire (ex Lindows OS) koristi root po defaultu, i njegov password kao opciju!

Zašto AV programi na Linuxu?

- brzina ispravaka popularnijih paketa mjeri se satima kod developera, ali...
  - ima slučajeva “prebrzog izlaska” i nedovoljnog testiranja (Samba, OpenSSH...)
  - distributeri kasne s patchom nekoliko dana do nekoliko tjedana, a enduseri ovise o njima
- uz sve tehničke prednosti Linuxa, i open sourcea općenito, rizici postoje i rasti će povećanjem broja korisnika Linuxa

Izvedbe AV zaštite na Linuxu

- On Demand file skeneri
- On Access skeneri
- Mail server skeneri
- Proxy (gateway) skeneri

On Demand file skeneri

- klasični file skeneri, nemaju ugrađenu on-access mogućnost, niti skeniranja mailova
- većina proizvođača AV softvera najprije je izdalo takve AV programe za Linux, jer je to bilo najlakše i najbrže za portanje
- na Linuxu se i takve AV programe lako iskoristilo za file, mail i proxy skeniranje

On Access skeneri

- mora raditi na kernel razini
- neki su to riješili kroz Sambu
  - ograničeno na datoteke dijeljene kroz Sambu
- rješenje: Dazuko modul za kernel
  - interface za kontrolu pristupa datotekama od strane drugih programa izvođenih u *userlandu*
  - započeli: H+BEDV Datentechnik GmbH
  - verzija 2.0.1, za Linux 2.2 – 2.6 i FreeBSD 4/5
  - izdano pod GPL i BSD licencama
  - SUSE ima i binary modul out-of-the-box

Mail server skeneri

- MailScanner (Perl skripta) + AV file skener
- http://www.mailscanner.info/
- prednosti: cijena on-demand AV programa je značajno manja od AV programa za Mail Server koji se plaća po mailoboxu
- posljedica: licence za neke on-demand AV programe ne dozvoljavaju skeniranje mailova na takav način
- popularan je i AMaViS

Proxy (gateway) skeneri

- Viralator (Perl) + Squid + AV file skener
- http://viralator.sourceforge.net/
- skenira http promet tako da sa wget najprije skine datoteku na serveru, provjeri je AV programom, te ako je čista proslijedi klijentu

Virus Bulletin testovi

- Virus Bulletin test 4/2002 – SUSE Linux
  - 11 prijavljenih AV programa
  - nitko nije dobio certifikat VB100%, jer nisu imali on-access modul
- Virus Bulletin test 5/2003 – RedHat Linux
  - isti broj prijavljenih, prošao samo Alwil avast!
  - on-access modul imao je još i H+BEDV Antivir, ali nije prošao na testovima detekcije
- Virus Bulletin test 4/2004 – RedHat Linux
  - prošla većina programa

Open Source rješenja

- OpenAntivirus (razvija se kao platforma)
- ClamAV
- iako imaju zanimljivih prednosti, problem su zajedničke mane:
  - loša detekcija
  - spori updateovi
- za sada se ne preporuča u produkcijskim korporativnim okruženjima

Komercijalna AV rješenja na Linuxu

- Kaspersky
  - WS/server, Samba, mail
  - Webmin modul
- Network Associates (McAfee)
  - desktop, file server, command-line modul
- Sophos
  - WS/server on-demand, mail, SAV engine
- Trend Micro
  - WS/server, za Lotus Notes

Komercijalna AV rješenja na Linuxu

- Softwin
  - Samba, mail
- Symantec (Norton)
  - CL file skener, Domino
- ESET
  - file server, mail
- Grisoft
  - WS/server, mail

Reference (članci, časopisi)

- Virus Bulletin 4/2002
- Virus Bulletin 5/2002
- Virus Bulletin 8/2002
- Virus Bulletin 4/2003
- Virus Bulletin 5/2003
- Peeling, Satchell; QinetiQ: “Analysis of the Impact of Open Source Software”
- Radoslav Dejanović: “Viruses on Unix systems”
- Larry Boettger: “The Morris Worm: how it Affected Computer Security and Lessons Learnd by it”

Reference (Web)

- http://www.theregister.co.uk
- http://www.securitymap.net
- http://www.securityfocus.com
- http://www.dazuko.org/
- http://www.virusbtn.com
- http://www.wildlist.org
- http://www.openantivirus.org
- http://viralator.sourceforge.net
- http://www.clamav.net/