Viruses, exploits, rootkits
the inside view from an AV producer

(based on real facts)

Short summary

- Intro
  - Hello :)
- Malware
  - Types of threats
  - So... what does AV cover ?
- What’s next ?

secure your every bit

Common terminology ?

(from dict.org)

virus: a program or segment of program code that may make copies of itself (replicate), attach itself to other programs, and perform unwanted actions within a computer; also called {computer virus} or {virus program}. Such programs are almost always introduced into a computer without the knowledge or assent of its owner, and are often malicious, causing destructive actions such as erasing data on disk, but sometime only annoying, causing peculiar objects to appear on the display. *The form of sociopathic mental disease that causes a programmer to write such a program has not yet been given a name*.

Common terminology ?

(from wikipedia)

virus: a self-replicating computer program that spreads by inserting copies of itself into other executable code or documents. A computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells. Extending the analogy, the insertion of a virus into the program is termed as an "infection", and the infected file, or executable code that is not part of a file, is called a "host". Viruses are one of the several types of malicious software or malware. In common parlance, the term virus is often extended to refer to worms, trojan horses and other sorts of malware; viruses in the narrow sense of the word are less common than they used to be, compared to other forms of malware

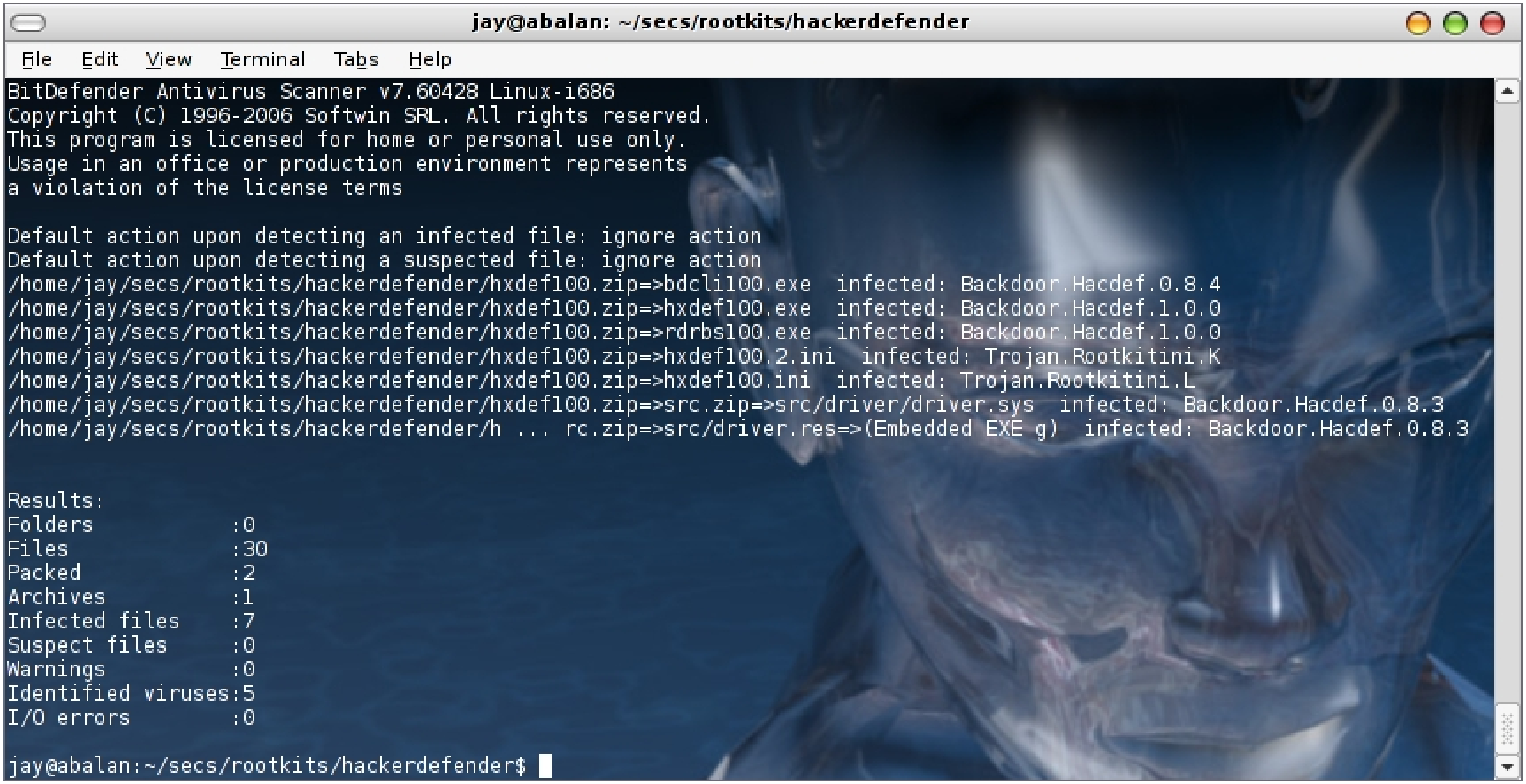
Common terminology ?

Exploit: a piece of software, a chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in order to gain control of a computer system or allow privilege escalation or a denial of service attack.

Rootkit: a set of software tools frequently used by a third party (usually an intruder) after gaining access to a computer system. These tools are intended to conceal running processes, files or system data, which helps an intruder maintain access to a system without the user's knowledge. Rootkits are known to exist for a variety of operating systems such as Linux, Solaris and versions of Microsoft Windows. A computer with a rootkit on it is called a rooted computer

Backdoors

HackerDefender



```
BitDefender Antivirus Scanner v7.60428 Linux-i686
Copyright (C) 1996-2006 Softwin SRL. All rights reserved.
This program is licensed for home or personal use only.
Usage in an office or production environment represents
a violation of the license terms

Default action upon detecting an infected file: ignore action
Default action upon detecting a suspected file: ignore action
/home/jay/secs/rootkits/hackerdefender/hxdef100.zip=>bdcli100.exe  infected: Backdoor.Hacdef.0.8.4
/home/jay/secs/rootkits/hackerdefender/hxdef100.zip=>hxdef100.exe  infected: Backdoor.Hacdef.1.0.0
/home/jay/secs/rootkits/hackerdefender/hxdef100.zip=>rdrbs100.exe  infected: Backdoor.Hacdef.1.0.0
/home/jay/secs/rootkits/hackerdefender/hxdef100.zip=>hxdef100.2.ini  infected: Trojan.Rootkitini.K
/home/jay/secs/rootkits/hackerdefender/hxdef100.zip=>hxdef100.ini  infected: Trojan.Rootkitini.L
/home/jay/secs/rootkits/hackerdefender/hxdef100.zip=>src.zip=>src/driver/driver.sys  infected: Backdoor.Hacdef.0.8.3
/home/jay/secs/rootkits/hackerdefender/h ... rc.zip=>src/driver.res=>(Embedded EXE g)  infected: Backdoor.Hacdef.0.8.3


Results:
Folders           :0
Files             :30
Packed            :2
Archives          :1
Infected files    :7
Suspect files     :0
Warnings          :0
Identified viruses:5
I/O errors        :0

jay@abalan:~/secs/rootkits/hackerdefender$
```

Backdoors

- HackerDefender
  - executable morphing tools
  - process hiding tools
  - small remote shell (including connectback)
  - if combined with a sniffer and keylogger, you won't even feel your private data and conversations being delivered on daily basis to a remote attacker

Backdoors

- Trojan.Ardamax.A

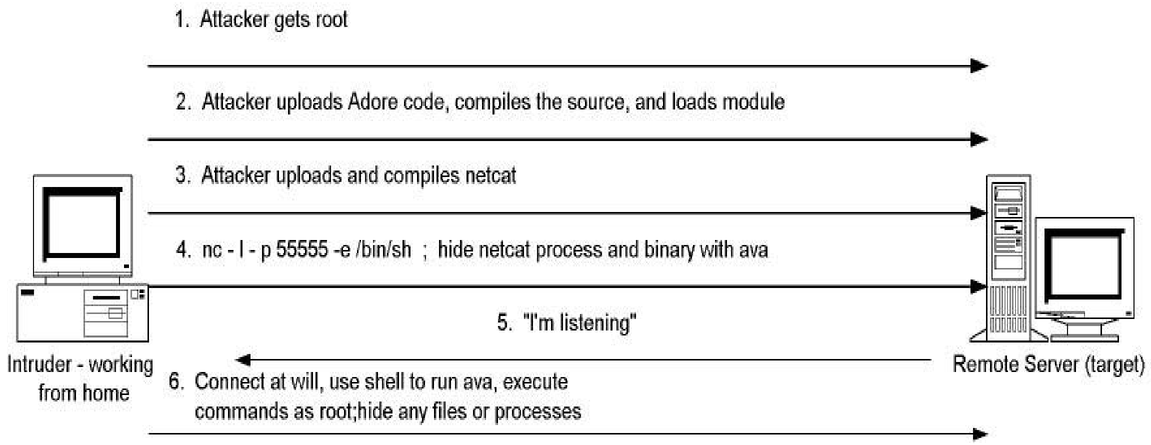
“Hi man, I finnaly found some time to give you the program i kept telling you about. I'll give you the IP addresses you have to put in. Give me a buzz whenever you get online and we'll talk. http://[REMOVED]/vladutz2006/client.zip”

  - pretends to be a hacking tool but actually is a commonly known keylogger
  - steals icq, skype, msn, gtalk, ym, miranda and qip passwords and delivers them to an e-mail address defined by the attacker

The mighty adore

by team-teso

- Known to be the most advanced rootkit in the wild
- LKM based (hint! load it as a NIC driver)
- One of the releases managed to defeat all known AV engines and rootkit hunters



1. Attacker gets root
2. Attacker uploads Adore code, compiles the source, and loads module
3. Attacker uploads and compiles netcat
4. nc - l - p 55555 -e /bin/sh ; hide netcat process and binary with ava
5. "I'm listening"
6. Connect at will, use shell to run ava, execute commands as root;hide any files or processes

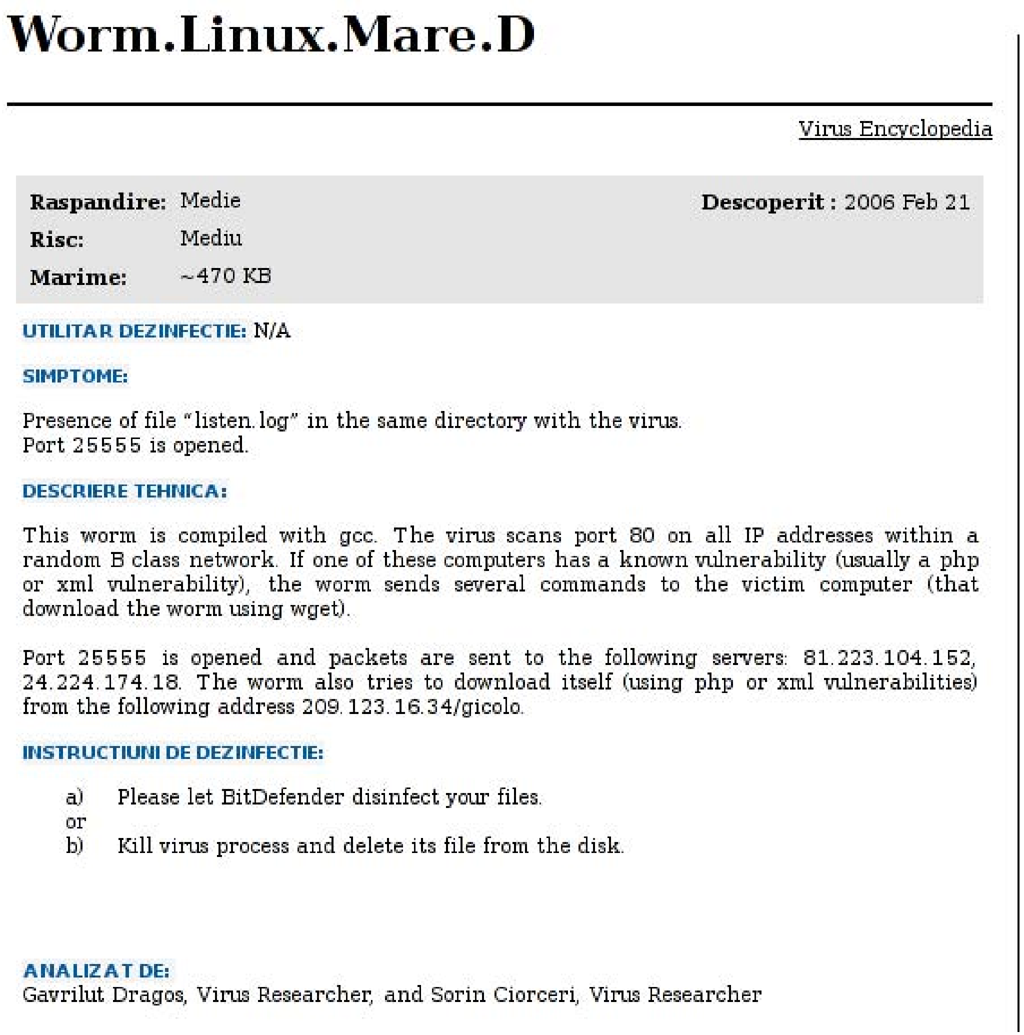
SucKIT

by sd & devik

- Description also available in Phrack issue 58, article 0x07 ("Linux on-the-fly kernel patching without LKM")
- Loaded through /dev/kmem
- Provides a password protected remote access connect-back shell initiated by a spoofed packet (bypassing most of firewall configurations), and can hide processes, files and connections.

Exploits

- Tools that usually don't do any harm to your system but can be used to intrude into others
- Target vulnerable services (web servers, php flaws, windows RPC, etc..)
- Very popular and easy to find in the wild
- Main reason why every teenager with a computer and a need to prove himself can become a l33t h4x0r



Worm.Linux.Mare.D

Virus Encyclopedia

Raspandire: Medie		**Descoperit :** 2006 Feb 21
Risc: Mediu		
Marime: ~470 KB		

UTILITAR DEZINFECTIE: N/A

SIMPTOME:

Presence of file "listen.log" in the same directory with the virus.
Port 25555 is opened.

DESCRIERE TEHNICA:

This worm is compiled with gcc. The virus scans port 80 on all IP addresses within a random B class network. If one of these computers has a known vulnerability (usually a php or xml vulnerability), the worm sends several commands to the victim computer (that download the worm using wget).

Port 25555 is opened and packets are sent to the following servers: 81.223.104.152, 24.224.174.18. The worm also tries to download itself (using php or xml vulnerabilities) from the following address 209.123.16.34/gicolo.

INSTRUCTIUNI DE DEZINFECTIE:

a) Please let BitDefender disinfect your files.
or
b) Kill virus process and delete its file from the disk.

ANALIZAT DE:
Gavrilut Dragos, Virus Researcher, and Sorin Ciorceri, Virus Researcher

Viruses

- Win32.Polip.A
  - File infector
  - Loads and resides in volatile memory when an infected file is executed
  - Encrypted
  - Includes polymorphic combined with junk code generator to fool debuggers and emulators

Most dangerous malware

- It's a combination of all mentioned so far and more
- Almost impossible to detect and disinfect
- Can disable ANY antivirus or security solution
- Mostly targeted through social engineering
- Creates holes in any firewall
- Ignores and gets by any company security policy
- Eventually delivers one way or the other, any confidential or private data to a remote attacker...

The User

The dilema

- When it comes to security, windows people have all the “fun”
  - AV industry provides them with protection from rootkits, viruses, and almost all known threats
  - AV industry provides them with firewalls
  - Some AV vendors even provide “Intrusion Detection Systems”
- For UNIX based systems, administrators have to rely on other tools or software
  - IDS/IPS
  - File Alteration Monitors
  - etc..

The dilema (the Q/A part)

- Should the security industry be divided between
  - Linux – Windows ?
  - Viruses – rootkits – other hacking tools – IDS ?
- Should AV companies provide firewalls for Linux servers like they do for windows desktops ?
- Should AV companies provide signatures for Linux rootkits like they do for windows ?
- OT: Do you feel that a kernel module for on-access AV scanning would be intrusive ?