MALICIOUS APPLICATIONS

Objective

- What malware are
- How do they infect hosts
- How do they hide
- How do they propagate
- How to detect them
- Worms

What is a Malware ?

- Malware in short known for malicious software.
- It is a software designed to gain access to a computer system without the owner's informed consent.
  - Includes computer viruses, worms, Trojan horses, rootkits, spyware and Adware
- Designed to find and steal confidential information stored on your computer

What it is good for ?

- Steal personal information
- Delete files
- Click fraud
- Steal software serial numbers
- Use your computer as relay

The Malware Categories

- Virus
- Backdoor
- Trojan horse
- Rootkit
- Scareware
- Adware
- Worm

What is a Virus ?

- Program that can infect other programs by modifying them to include a, possibly evolved, version of itself

Some Virus Type

- Polymorphic : Uses a polymorphic engine to mutate while keeping the original algorithm intact (packer)
- Metamorphic : Change after each infection

What is a Trojan

- Describes the class of malware that appears to perform a desirable function but in fact performs
  - Undisclosed malicious functions that allow unauthorized access to the victim computer

What is rootkit

- A root kit is a component that uses stealth to maintain a persistent and undetectable presence on the machine

What is a Worm

- A computer worm is a self-replicating computer program.

- It uses a network to send copies of itself to other nodes and do so without any user intervention.

Image courtesy of: Tech Tips.com

History

- 1981 First reported virus : Elk Cloner (Apple 2)
- 1983 Virus get defined
- 1986 First PC virus MS DOS
- 1988 First worm : Morris worm
- 1990 First polymorphic virus
- 1998 First Java virus
- 1998 Back orifice
- 1999 Melissa virus
- 1999 Zombie concept
- 1999 Knark rootkit
- 2000 love bug
- 2001 Code Red Worm
- 2001 Kernel Intrusion System
- 2001 Nimda worm
- 2003 SQL Slammer worm

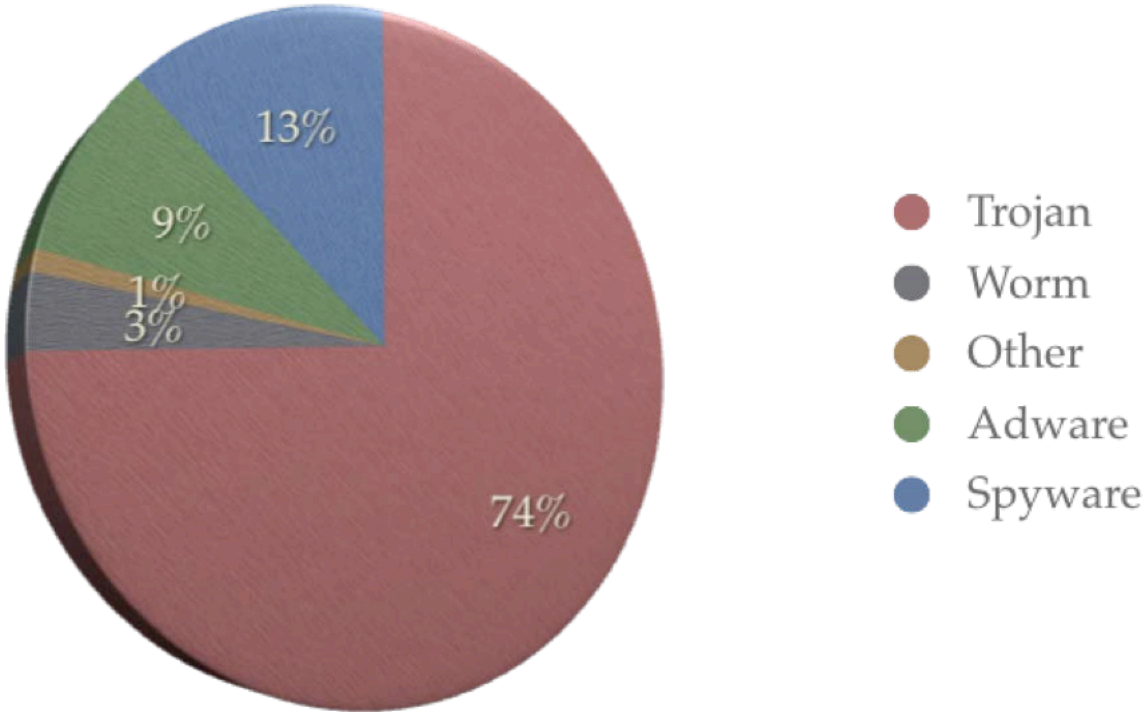
Melissa spread by email and share

Knark rootkit made by creed demonstrate the first ideas

love bug vb script that abused a weakness in outlook

Kernel intrusion by optyx gui and efficent hidding mechanims

Malware Repartition



Infection methods

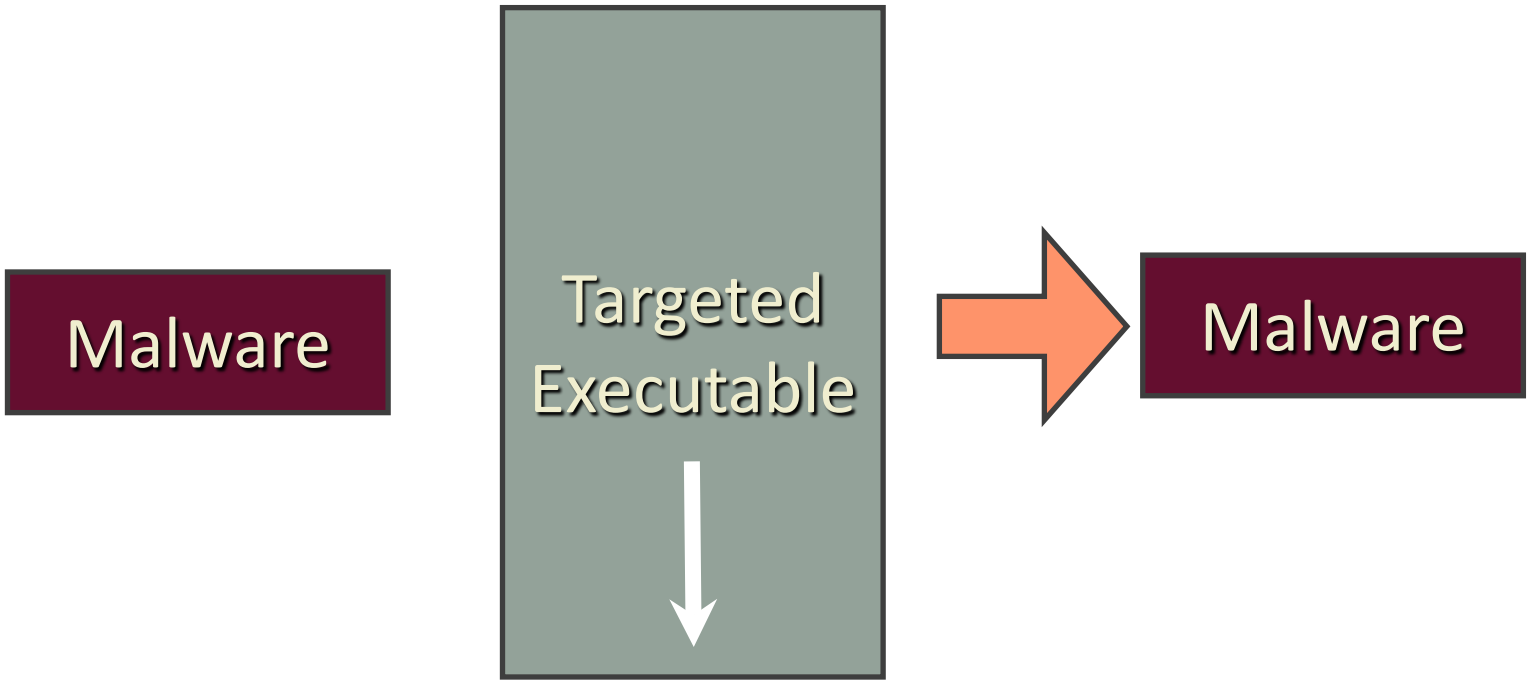
Outline

- What malware are
- How do they infect hosts
- How do they propagate
- How to detect them
- Worms

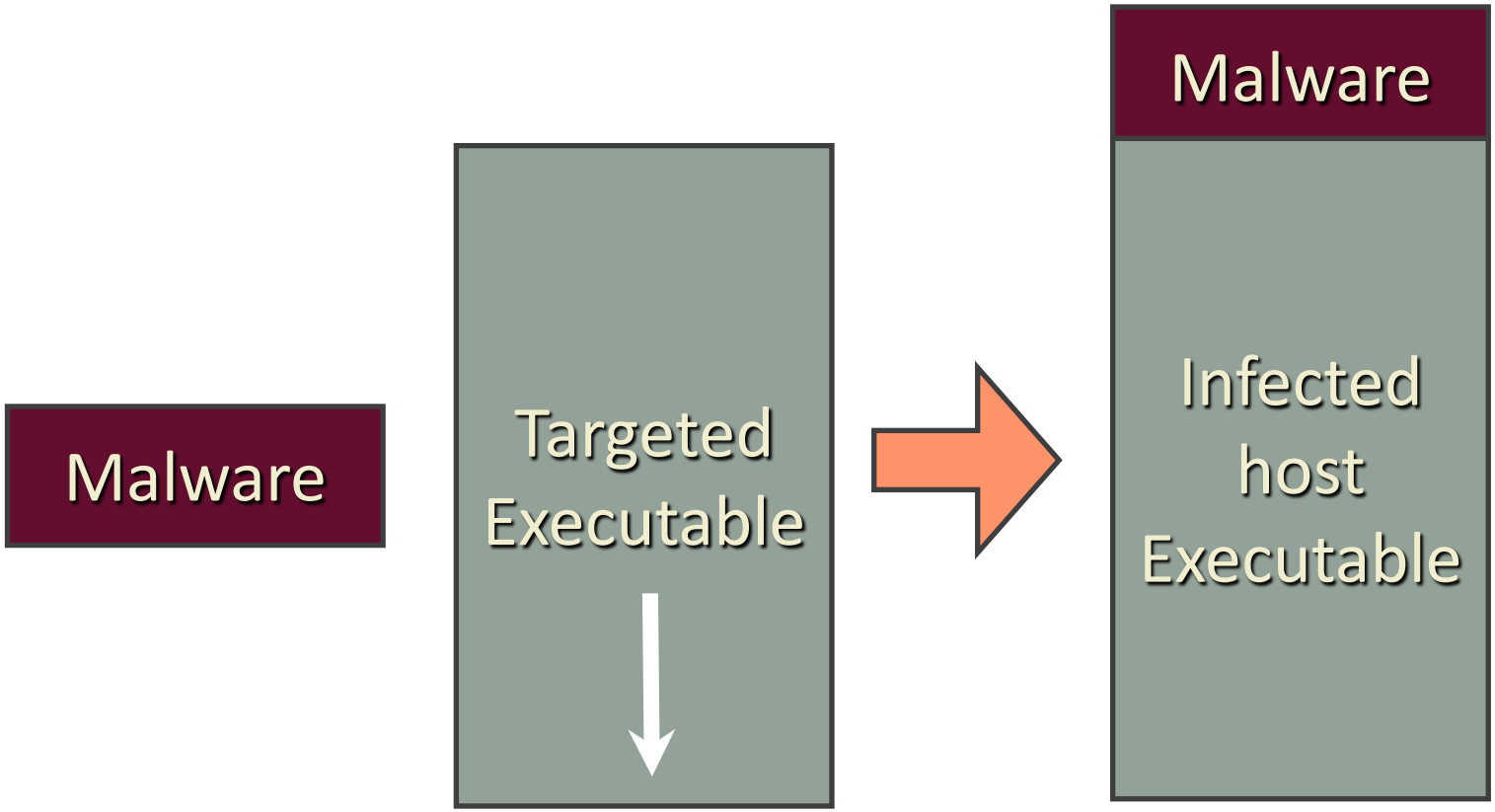
What to Infect

- Executable
- Interpreted file
- Kernel
- Service
- MBR
- Hypervisor

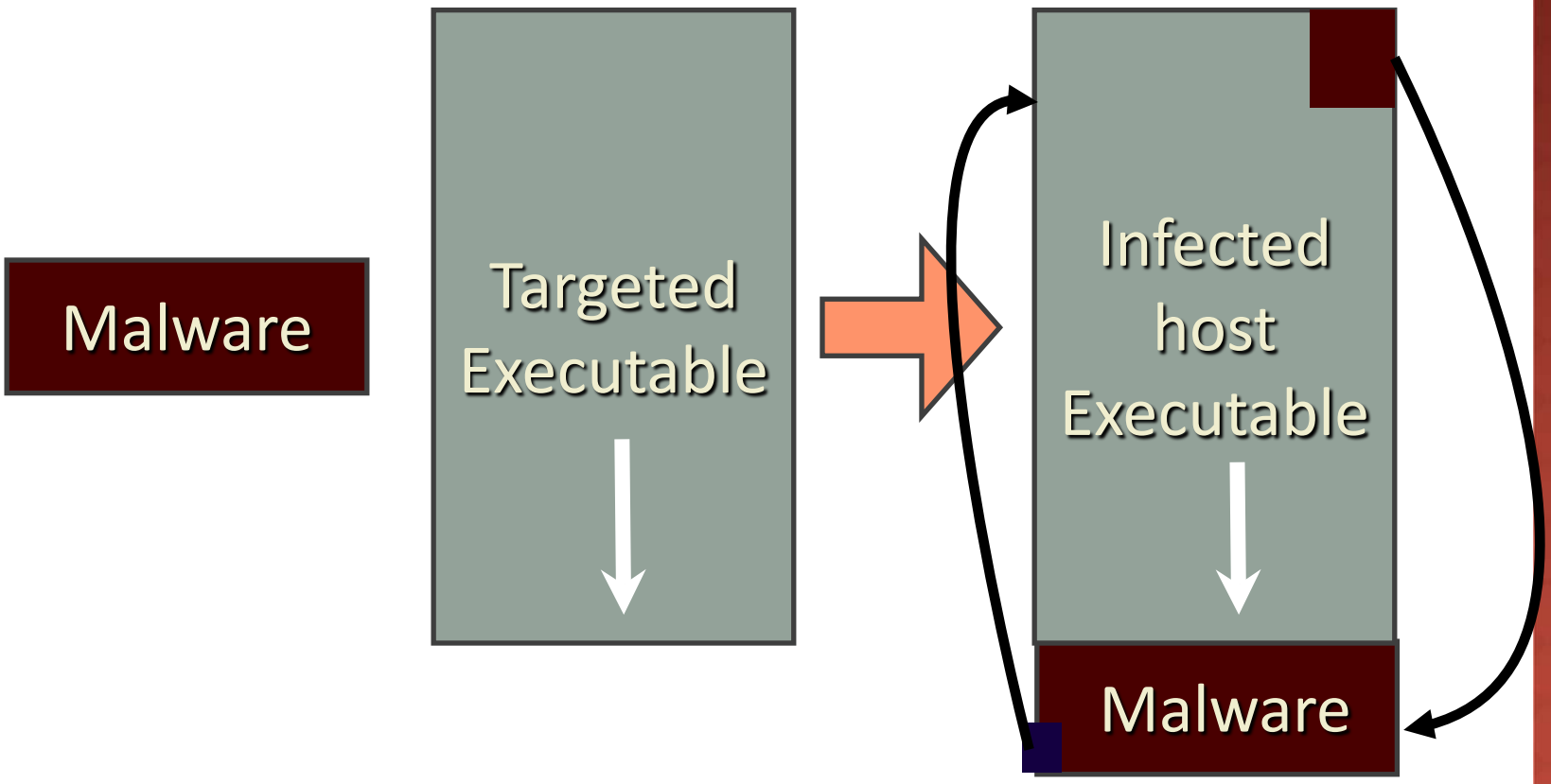
Overwriting Malware



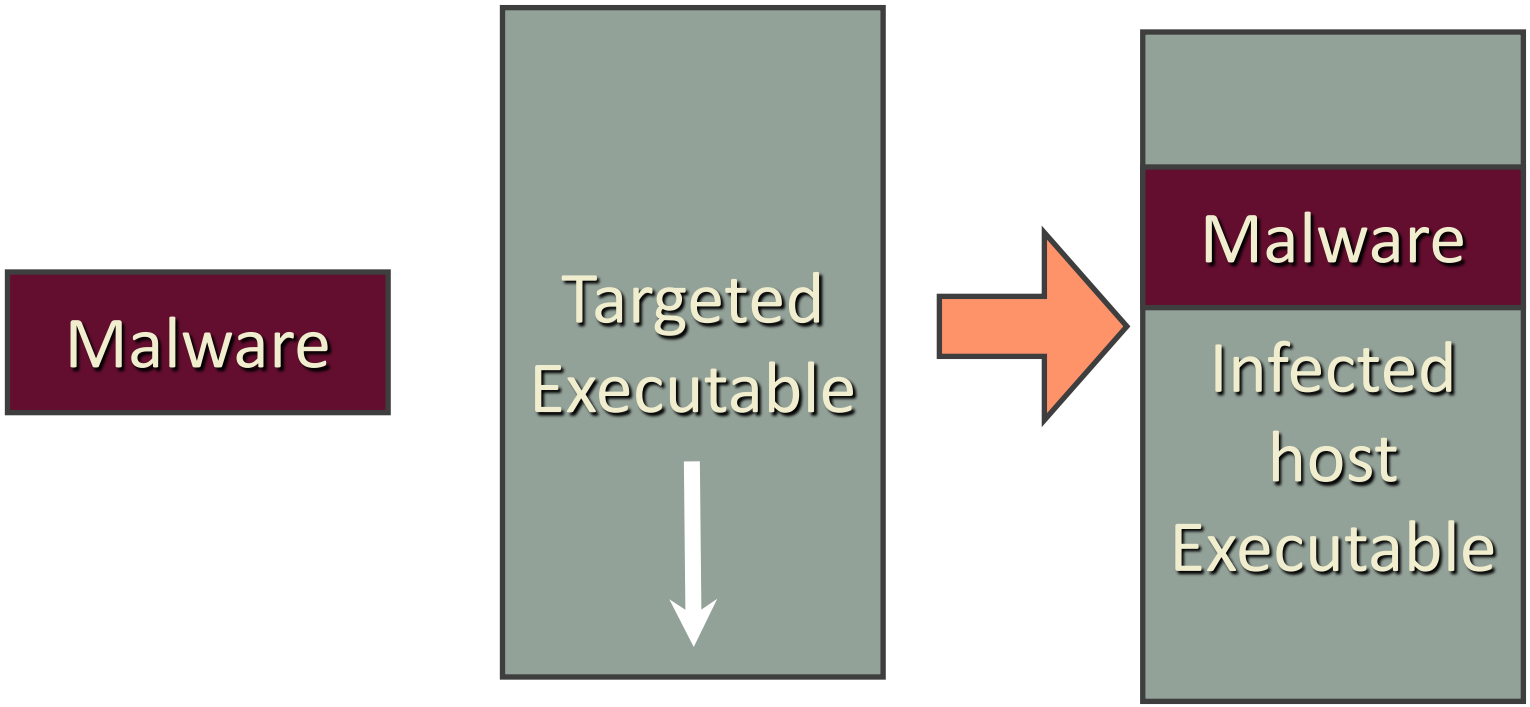
Prepending Malware



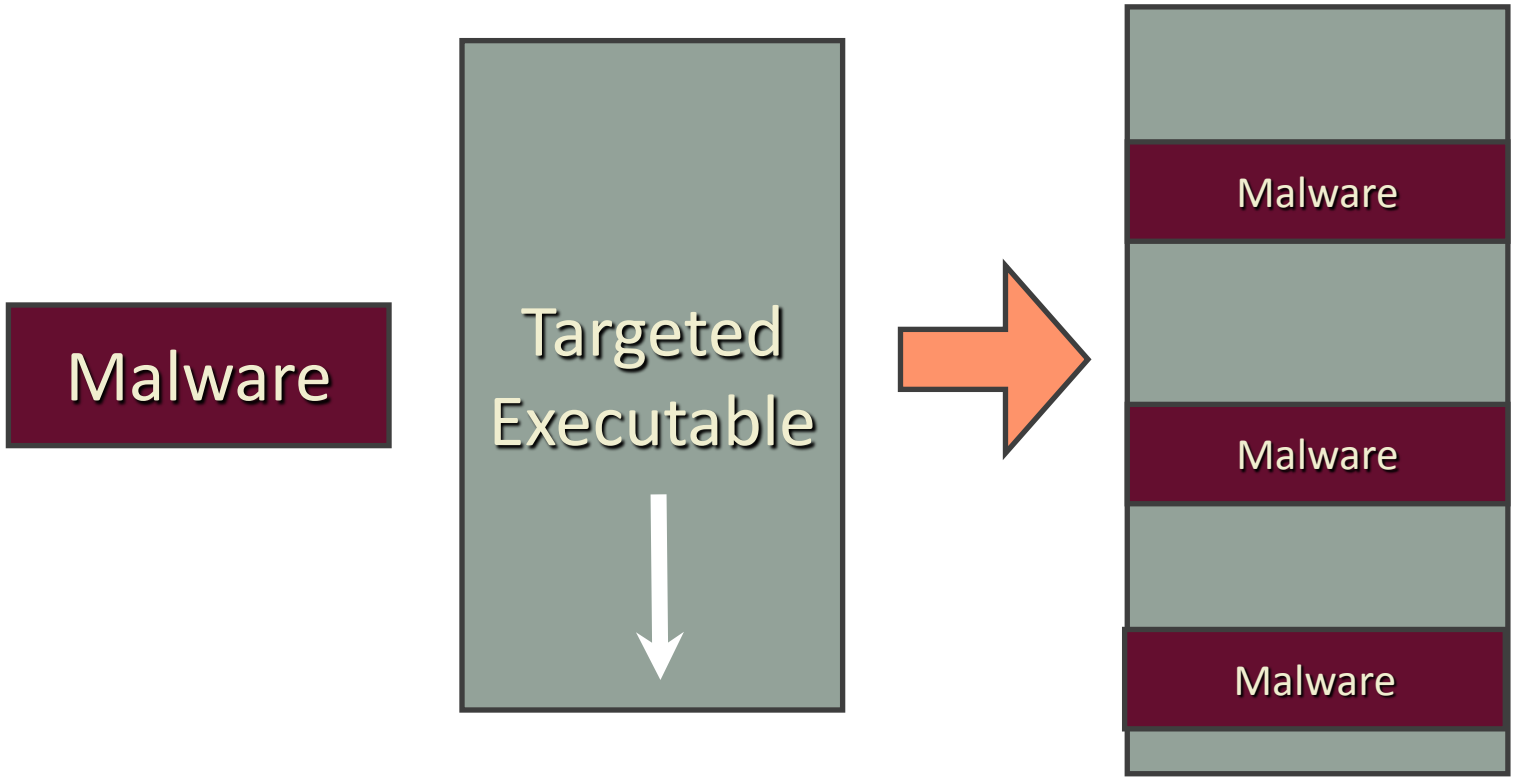
Adding Malware



Cavity Malware



Multi-Cavity malware



Auto Start

- Folder auto-start : C:\Documents and Settings\[user_name]\Start Menu\Programs\Startup
- Win.ini : run=[backdoor]" or "load=[backdoor]".
- System.ini : shell=”myexplorer.exe”
- Wininit
- Config.sys

Auto Start Cont.

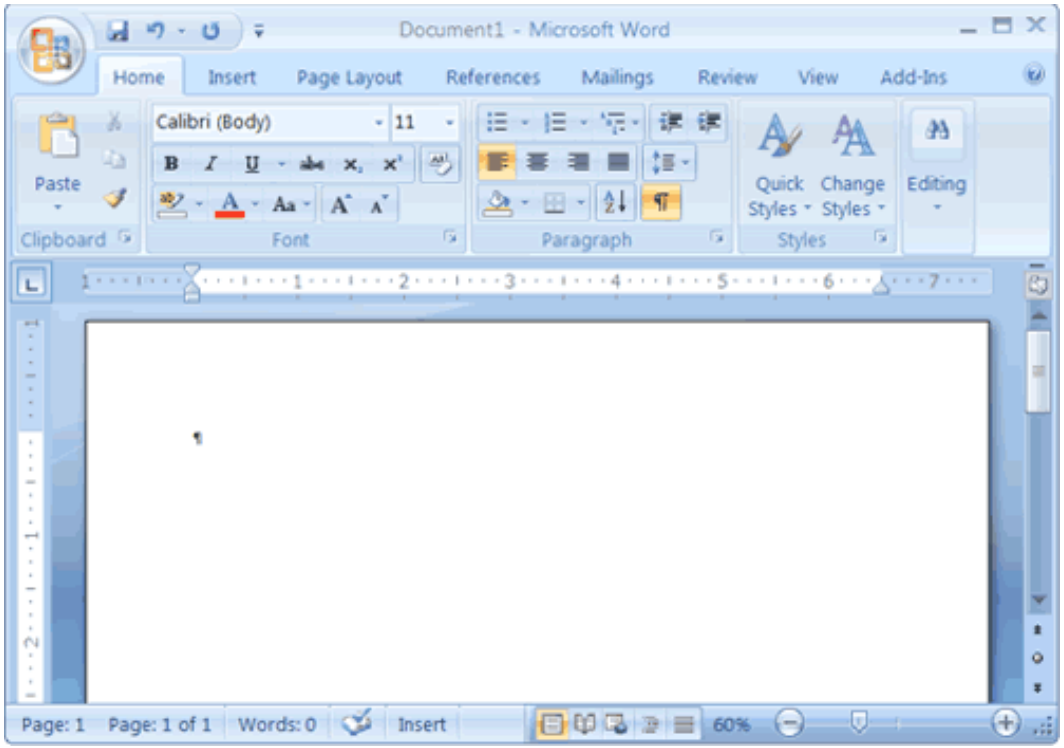
- Assign know extension (.doc) to the malware
- Add a Registry key such as *HKCU\SOFTWARE\Microsoft\Windows \CurrentVersion\Run*
- Add a task in the task scheduler
- Run as service

Macro virus

- Use the builtin script engine
- Example of call back used (word)
  - AutoExec()
  - AutoClose()
  - AutoOpen()
  - AutoNew()

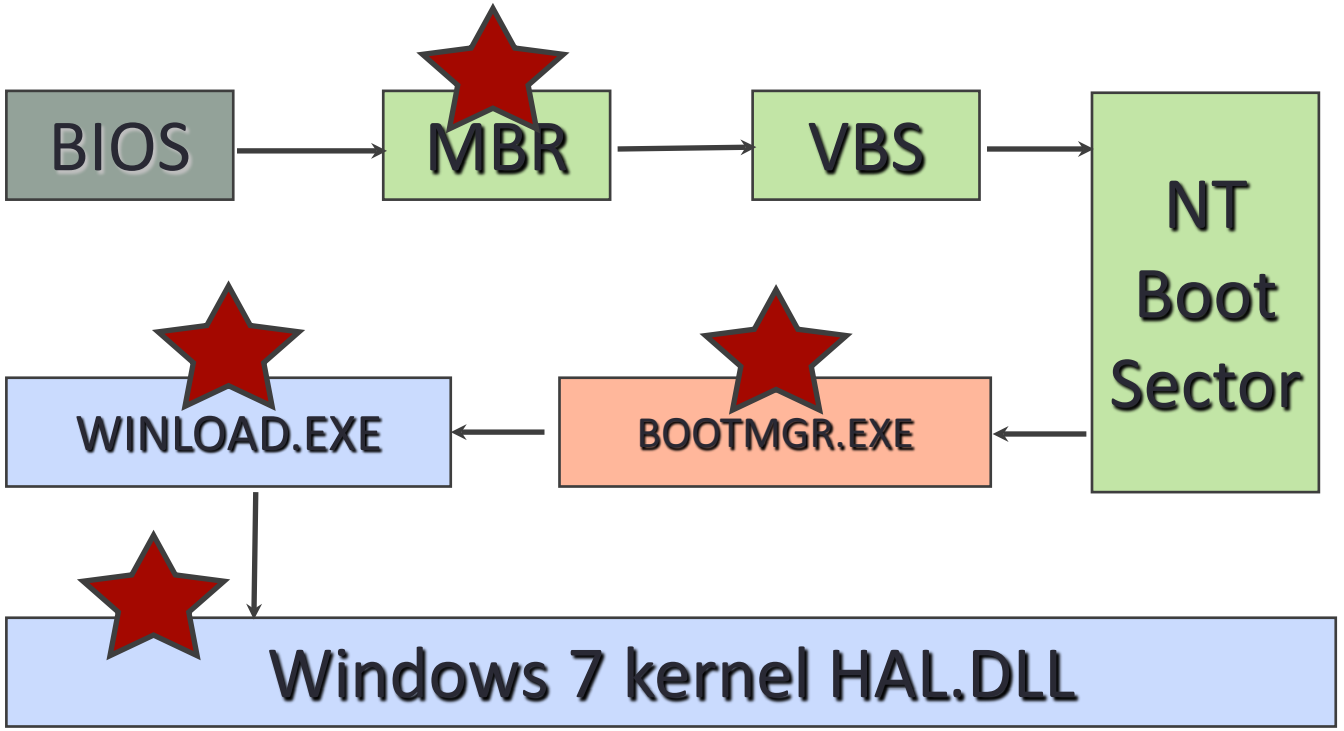
Document based malware

- MS Office
- Open Office
- Acrobat



MBR/Bootkit

- Bootkits can be used to avoid all protections of an OS, because OS consider that the system was in trusted stated at the moment the OS boot loader took control.

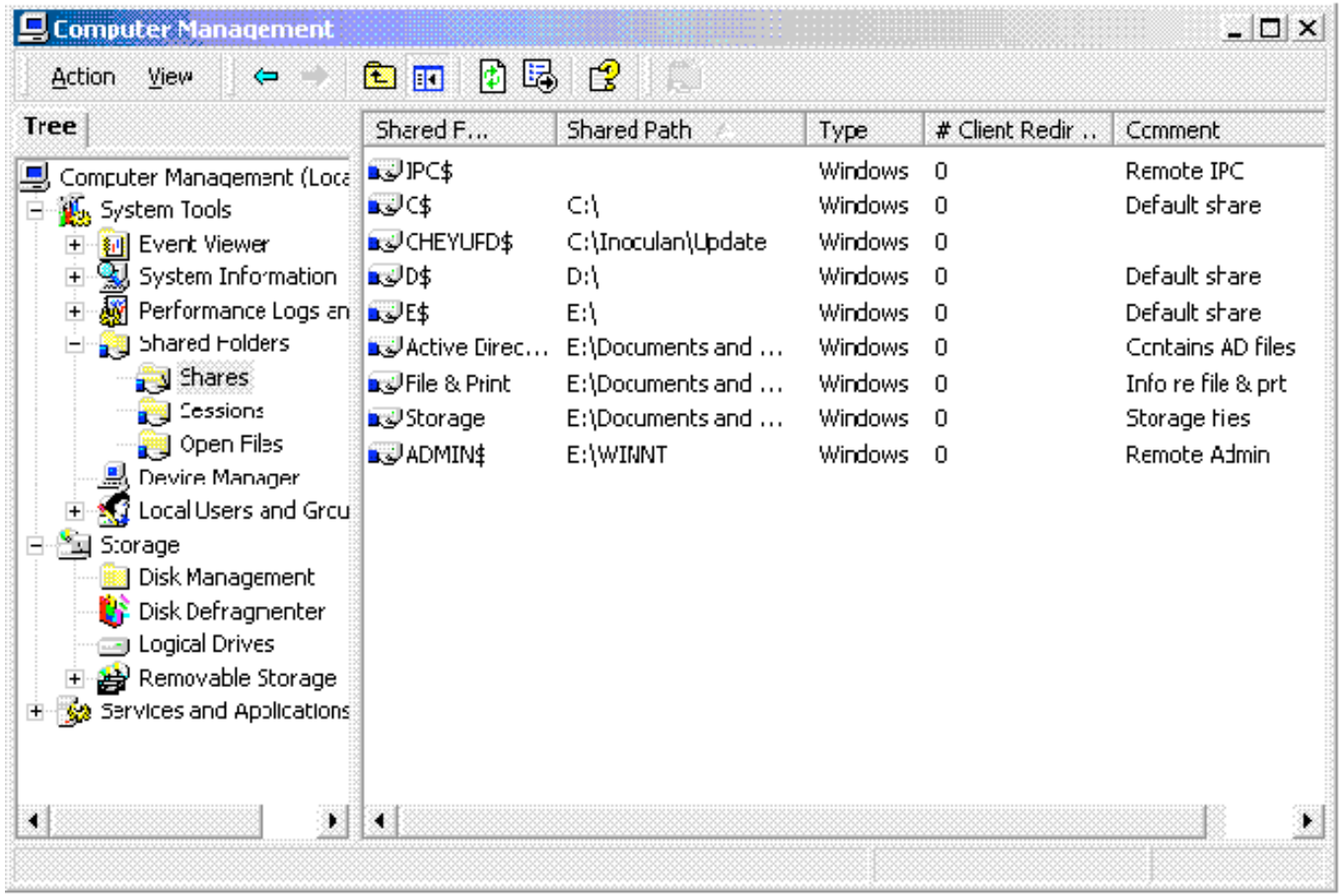

BIOS
MBR
VBS
NT Boot Sector
WINLOAD.EXE
BOOTMGR.EXE
Windows 7 kernel HAL.DLL

Vboot

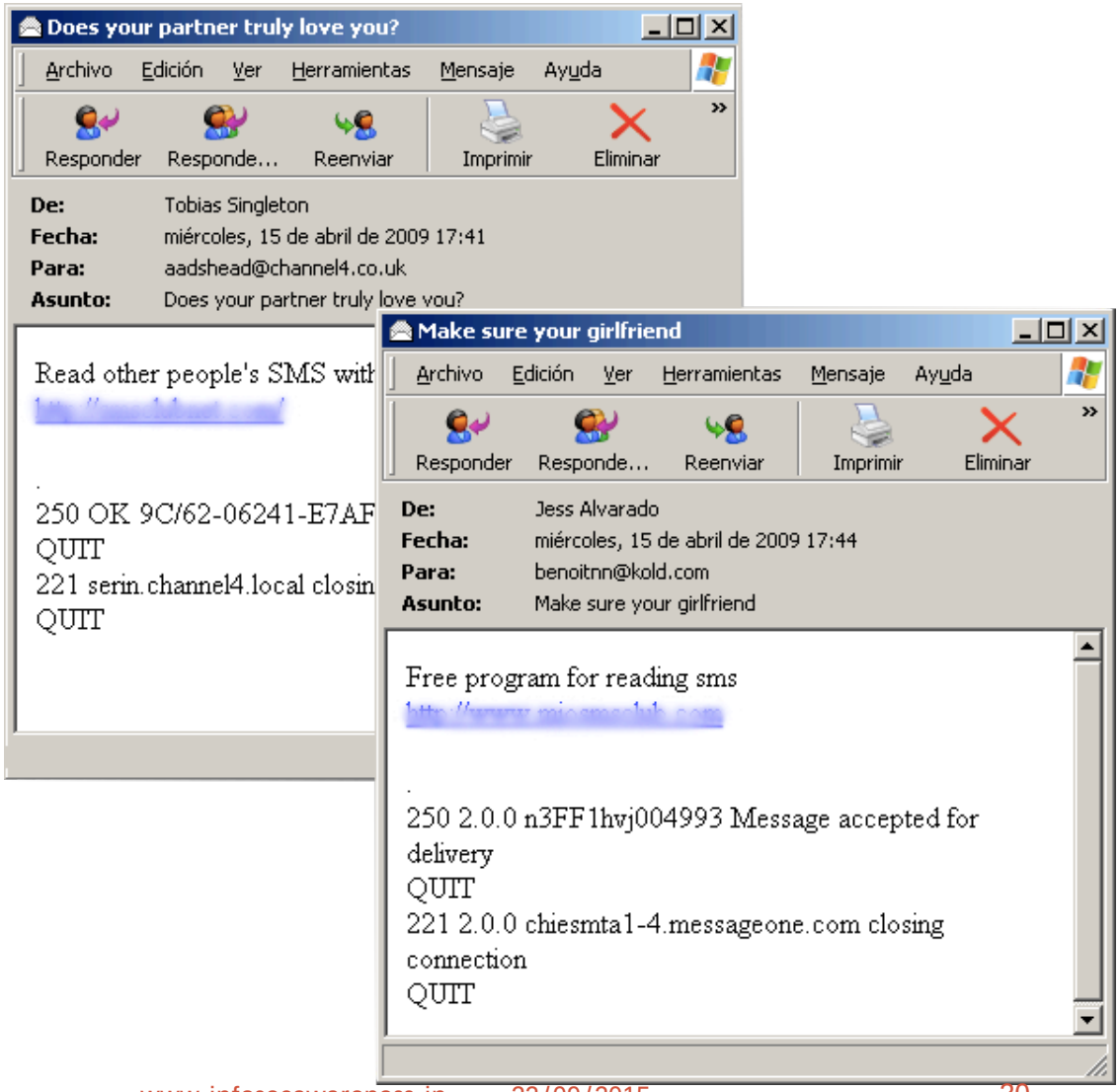
- Work on every Windows (vista,7)
- 3ko
- Bypass checks by letting them run and then do inflight patching
- Communicate via ping command

How do they propagate

Shared Folder

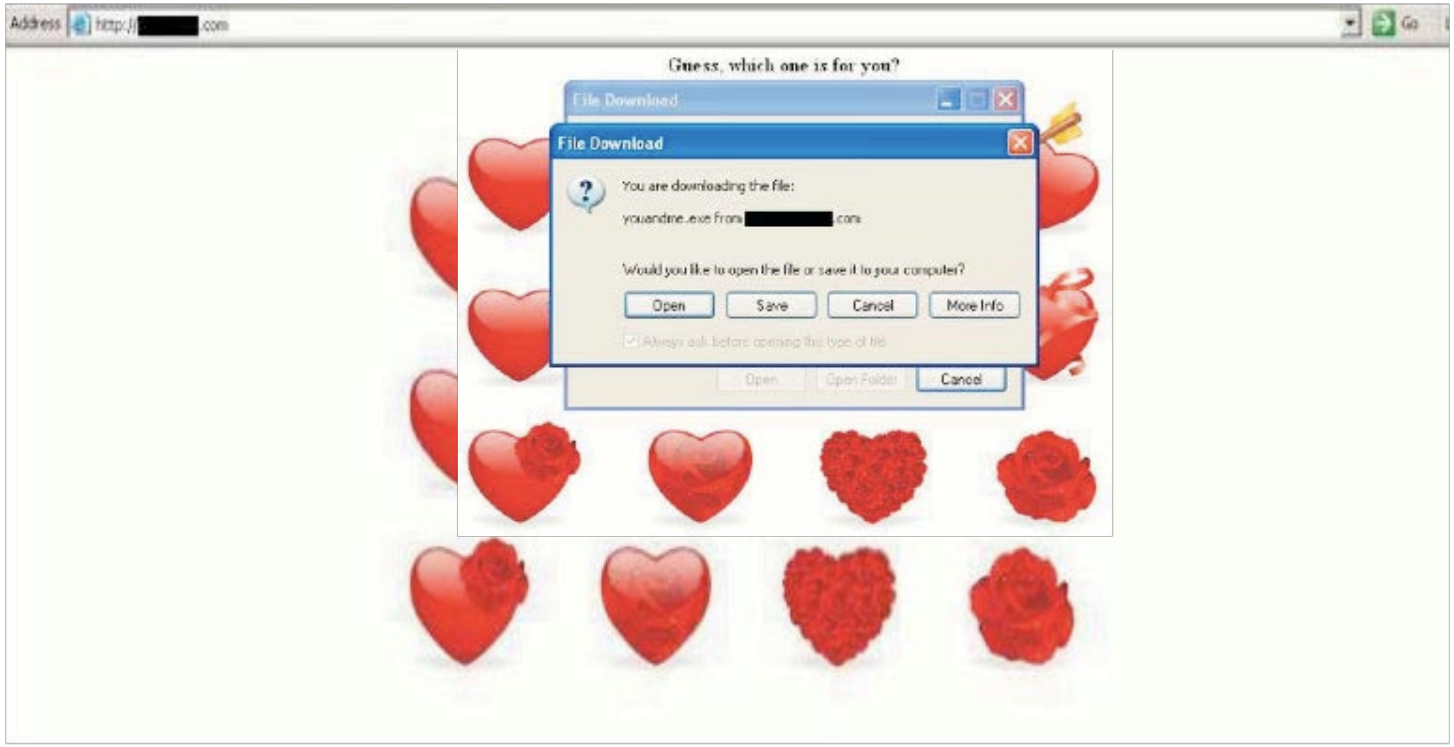


Email Propagation



from pandalab blog

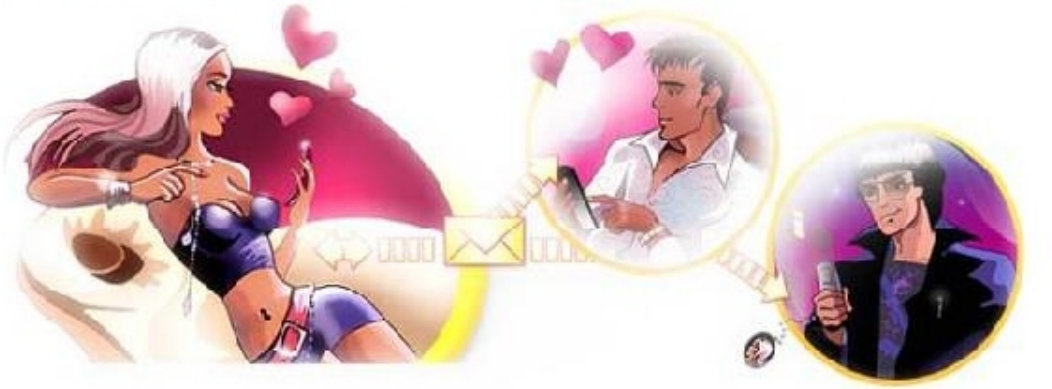
Valentine Day ...



- Waledac malicious domain from pandalab blog

Email again

Are you interested in reading other people's sms?



Get Your Free 30-Day Trial!

Do you want to test your partner or just to read somebody's SMS? This program is exactly what you need then! It's so easy! You don't need to install it at the mobile phone of your partner.
Just download the program and you will able to read all SMS when you are online. Be aware of everything! This is an extremely new service!

http://[Removed].com/freetrial.exe

Download Free Trial
© SMS Spy. All rights reserved

Symantec 2009

Fake Codec

QuickTime™ and a
GIF decompressor
are needed to see this picture.

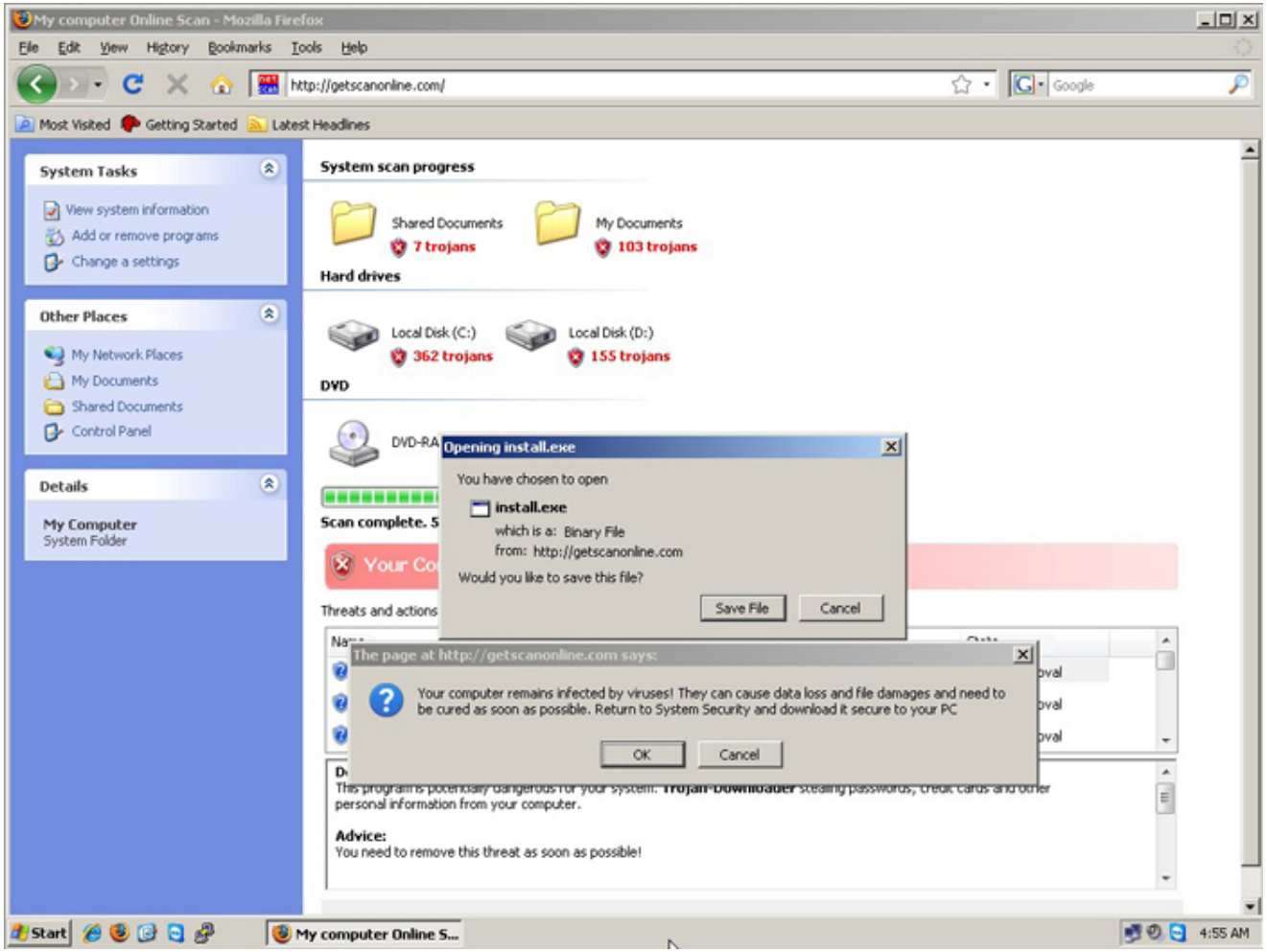
Fake Antivirus

from pandalab blog

Hijack You Browser

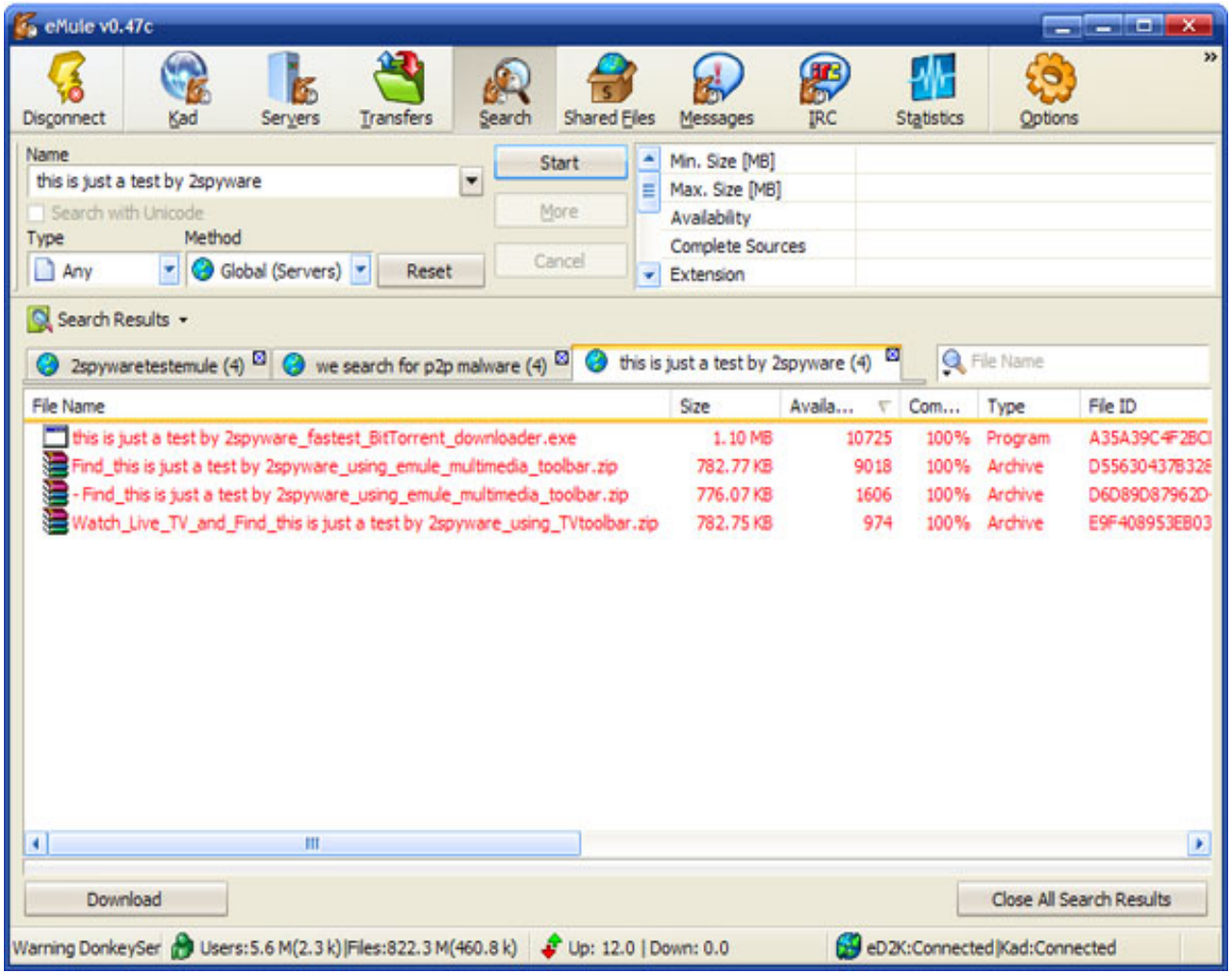
from pandalab blog

Fake page !



from pandalab blog

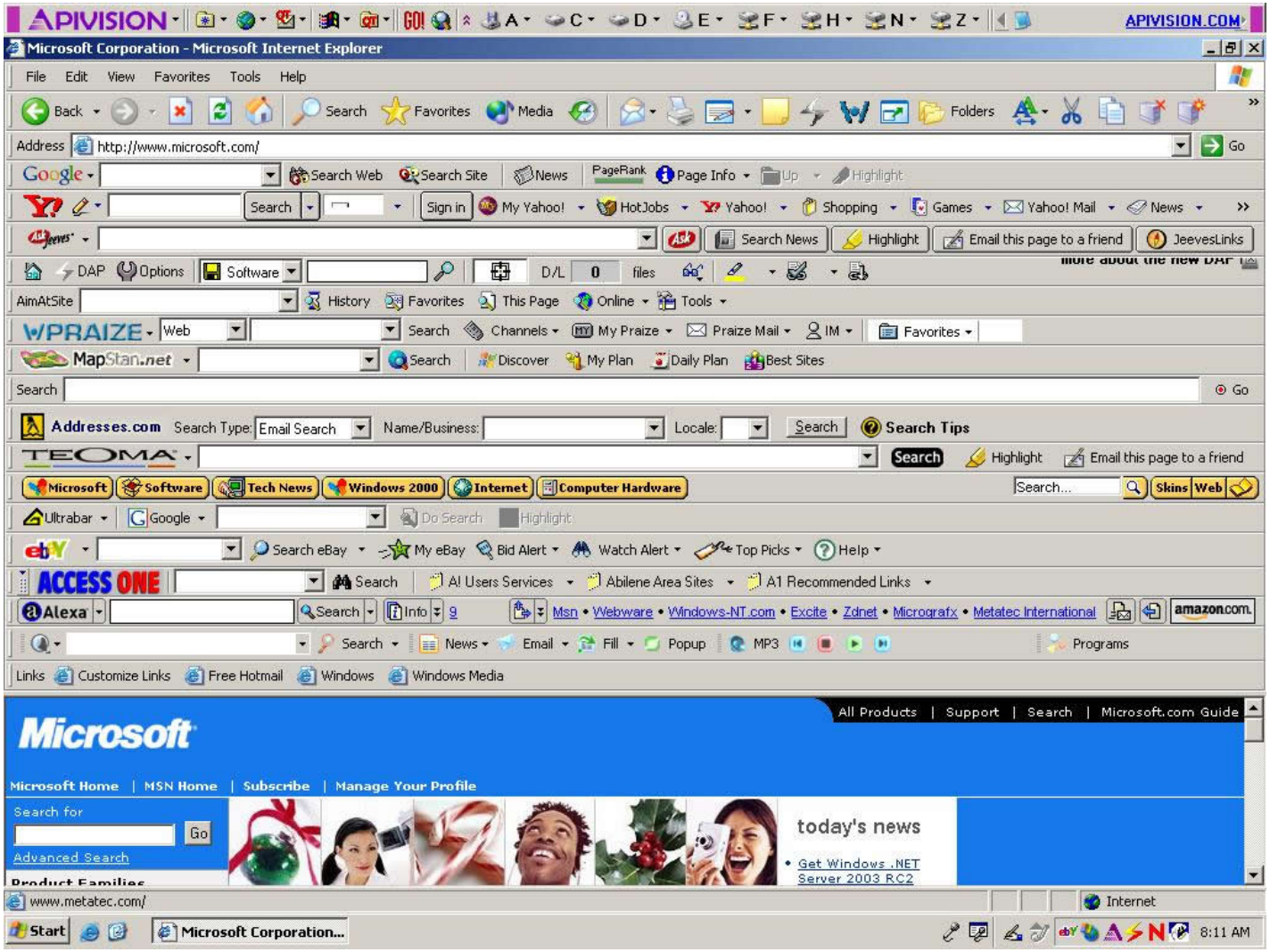
P2P Files


eMule v0.47c
Disconnect
Kad
Servers
Transfers
Search
Shared Files
Messages
IRC
Statistics
Options
Name
this is just a test by 2spyware
Search with Unicode
Type
Any
Method
Global (Servers)
Reset
Start
More
Cancel
Min. Size [MB]
Max. Size [MB]
Availability
Complete Sources
Extension
Search Results
2spywaretestemule (4)
we search for p2p malware (4)
this is just a test by 2spyware (4)
File Name
File Name
Size
Availa...
Com...
Type
File ID
this is just a test by 2spyware_fastest_BitTorrent_downloader.exe 1.10 MB 10725 100% Program A35A39C4F2BC
Find_this is just a test by 2spyware_using_emule_multimedia_toolbar.zip 782.77 KB 9018 100% Archive D5563043 7B32
- Find_this is just a test by 2spyware_using_emule_multimedia_toolbar.zip 776.07 KB 1606 100% Archive D6D89D87962D
Watch_Live_TV_and_Find_this is just a test by 2spyware_using_TVtoolbar.zip 782.75 KB 974 100% Archive E9F408953EB03
Download
Close All Search Results
Warning DonkeySer
Users:5.6 M(2.3 k)|Files:822.3 M(460.8 k)
Up: 12.0 | Down: 0.0
eD2K:Connected|Kad:Connected

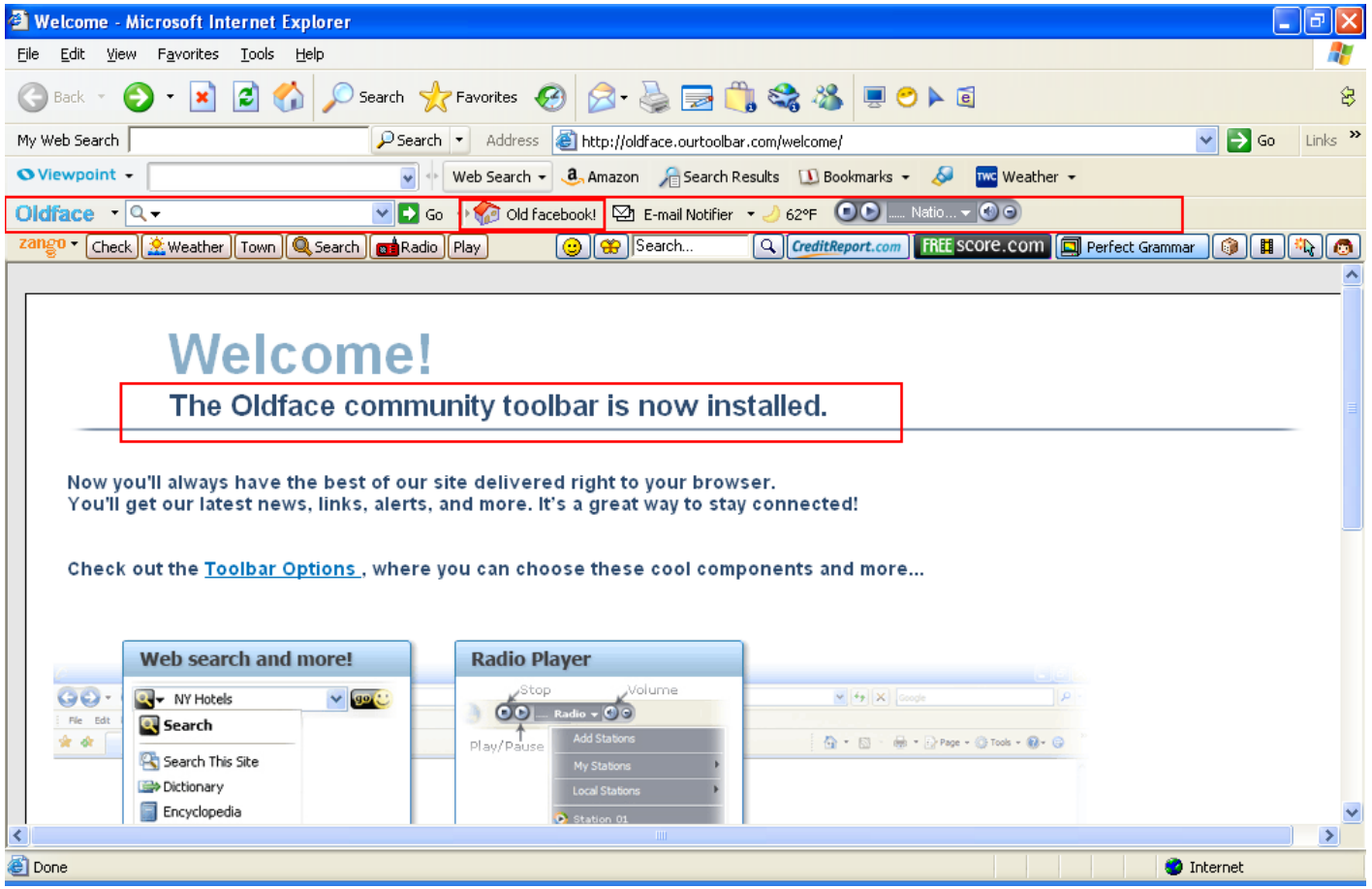
Adware


Free connection
Free modem
Click here to find out more
BT
INSWEB
Lower your insurance costs.
Enter to WIN!
XEROX
WIN an $11,000 USD
Business Upgrade Package or a Xerox Phaser® 8400 Color Printer
World's fastest color printer for under $1,000 USD.
Phaser 8400
Color Printer
$999
TRY 2 RISK-FREE ISSUES!
Netscape What's New
Science Proves It: Drinking Causes...
Teen Girls Beware: Popular Boys Do THIS
Look What Was Found in Stone Age Cave
Strange Space Object Mystery Deepens
Did You See What Bush Dared to Wear?
If You Get This E-Mail Scam, Delete It
15 FREE POWER GUIDES
Home-Owners Click Here
AMERIQUEST MORTGAGE COMPANY®
Before you go, did you know....
You can add AOL® for Broadband to any high-speed cable or DSL connection!
Works with and enhances any basic high-speed connection
Built-in protection for you and your family
The best on-demand and exclusive programming online
GET A FREE TRIAL!
Upto 45 days FREE
Click here for details
Are You Paying Too
Rates are at Hist
Get cas
your h
HomeLoanCenter.com
TRAVELZOO
This Week's
on the Interne
Released APRIL 14
Song
CheapCaribbean.c
ReliaQuot
A better way to buy life insura
Take this free test!

Browser Toolbar ...

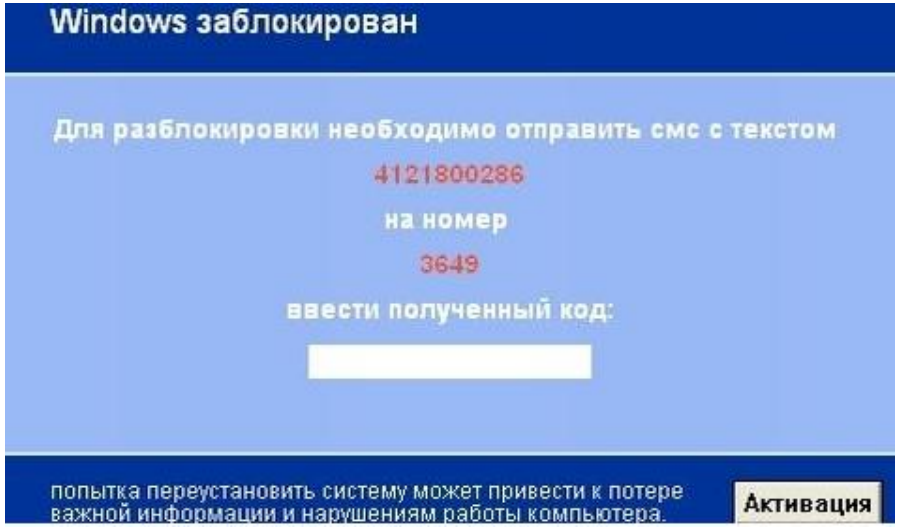


Toolbar again



Ransomware

- Trj/SMSlock.A
- Russian Ransomware

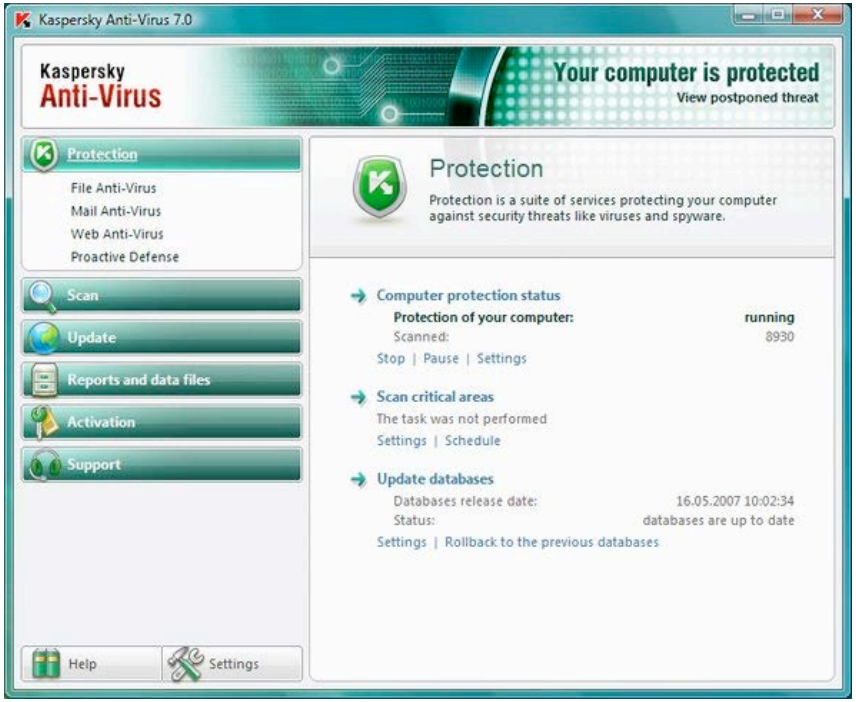


To unlock you need to send an SMS with the text4121800286to the number3649Enter the resulting code: Any attempt to reinstall the system may lead to loss of important information and computer damage

Detection

Anti-virus

- Analyze system behavior
- Analyze binary to decide if it a virus
- Type :
  - Scanner
  - Real time monitor



Worm

- A worm is self-replicating software designed to spread through the network
  - Typically, exploit security flaws in widely used services
  - Can cause enormous damage
    - Launch DDOS attacks, install bot networks
    - Access sensitive information
    - Cause confusion by corrupting the sensitive information

- Worm vs Virus vs Trojan horse
  - A virus is code embedded in a file or program
  - Viruses and Trojan horses rely on human intervention
  - Worms are self-contained and may spread autonomously

Cost of worm attacks

- Morris worm
  - Infected approximately 6,000 machines
    - 10% of computers connected to the Internet
  - cost ~ $10 million in downtime and cleanup
- Code Red worm
  - Direct descendant of Morris' worm
  - Infected more than 500,000 servers
    - Programmed to go into infinite sleep mode July 28
  - Caused ~ $2.6 Billion in damages,
- Love Bug worm: $8.75 billion

  - Statistics: Computer Economics Inc., Carlsbad, California