CSCI 6900

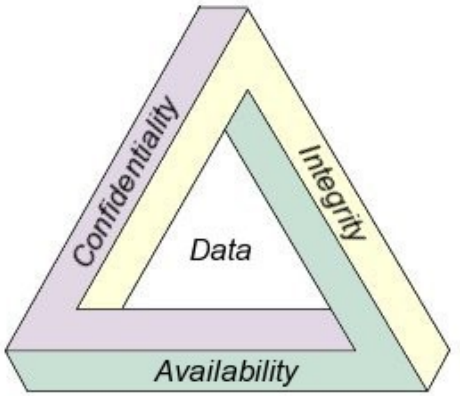
Computer Network Attacks and Defenses

Lecture 2: Overview of research topics in computer and network security (part A)

Instructor: Prof. Roberto Perdisci

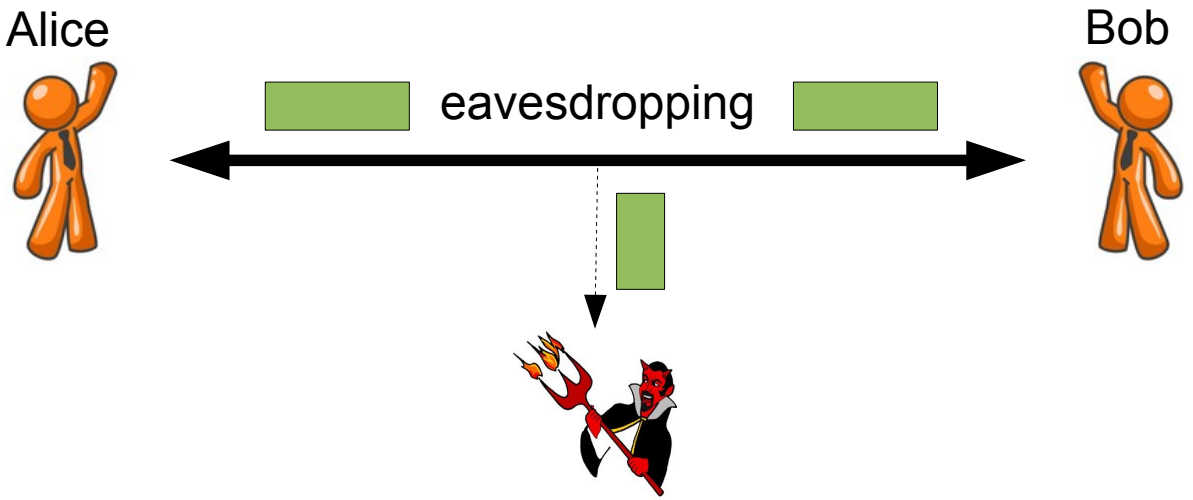
Fundamental Components

- Confidentiality
  - concealment/secrecy of information
    - often achieved using cryptography
- Integrity
  - trustworthiness of data or resources
    - prevention: deny unauthorized changes
    - detection: identify whether data has been changed
- Availability
  - ability to use the desired information or resource



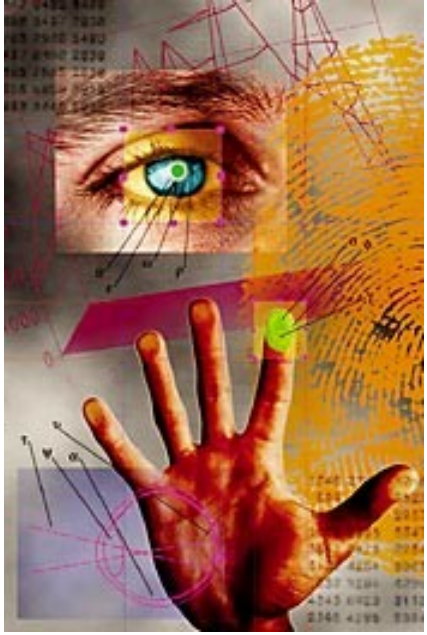
Examples

Attack on Confidentiality



Attack on Confidentiality and/or Integrity

Beyond CIA



- Authentication
  - verification of someone's identity
  - e.g. using password, priv/pub keys, biometrics
- Authorization
  - checking if user is allowed to perform actions
  - ACLs are a common authorization mechanism
- Non-repudiation
  - make a communication or transaction undeniable

Security Policies

- Definition of ***security policy***
  - a statement of what is a what is not allowed
  - partitions the states of a system into *secure* states and *non-secure* or *unauthorized* states
- Definition of ***security mechanism***
  - method or procedure to enforce a policy
- ***Secure system***
  - a system that starts in a secure state and cannot transition to an unauthorized state

Other Terminology

- ***Threat***: possibility of an unauthorized attempt to:
  - access or manipulate information
  - render a system unreliable or unusable
- ***Vulnerability***: known or suspected flaw in *software* or *design* that exposes to
  - unauthorized disclosure of info
  - system intrusion (ability to control system state)
- ***Attack***: execution of a plan to carry out a threat by exploiting a vulnerability
- ***Intrusion***: successful attack

Research in Computer Security

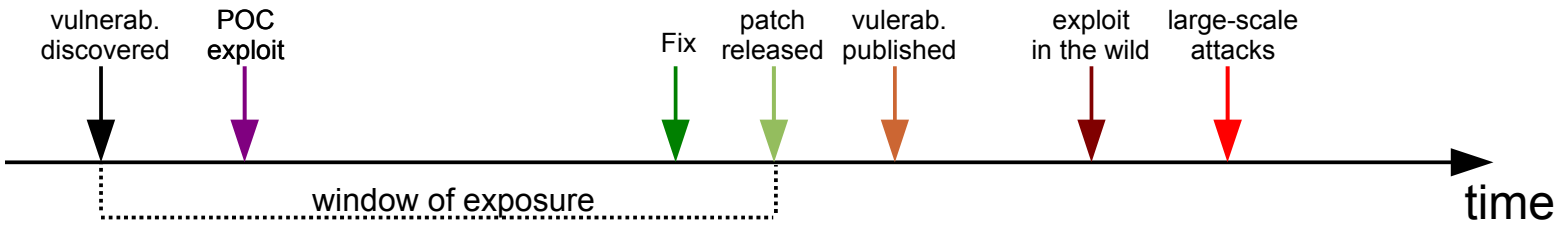
- Most research on computer systems focuses on ***how systems work***
  - features, performance, usability

- Research on computer systems **security** puts a lot of focus on ***how systems fail***
  - what are the weaknesses?
  - how hard is it to exploit the vulnerabilities?
  - if we cannot compromise/own the system, can we render it useless?
  - develop better defenses!

Ethical Disclosure

- How do we disclose vulnerabilities in a responsible way?
- Controversial topic...
  - Security by obscurity (no disclosure)
  - Full disclosure
  - Delayed disclosure

Example Scenario



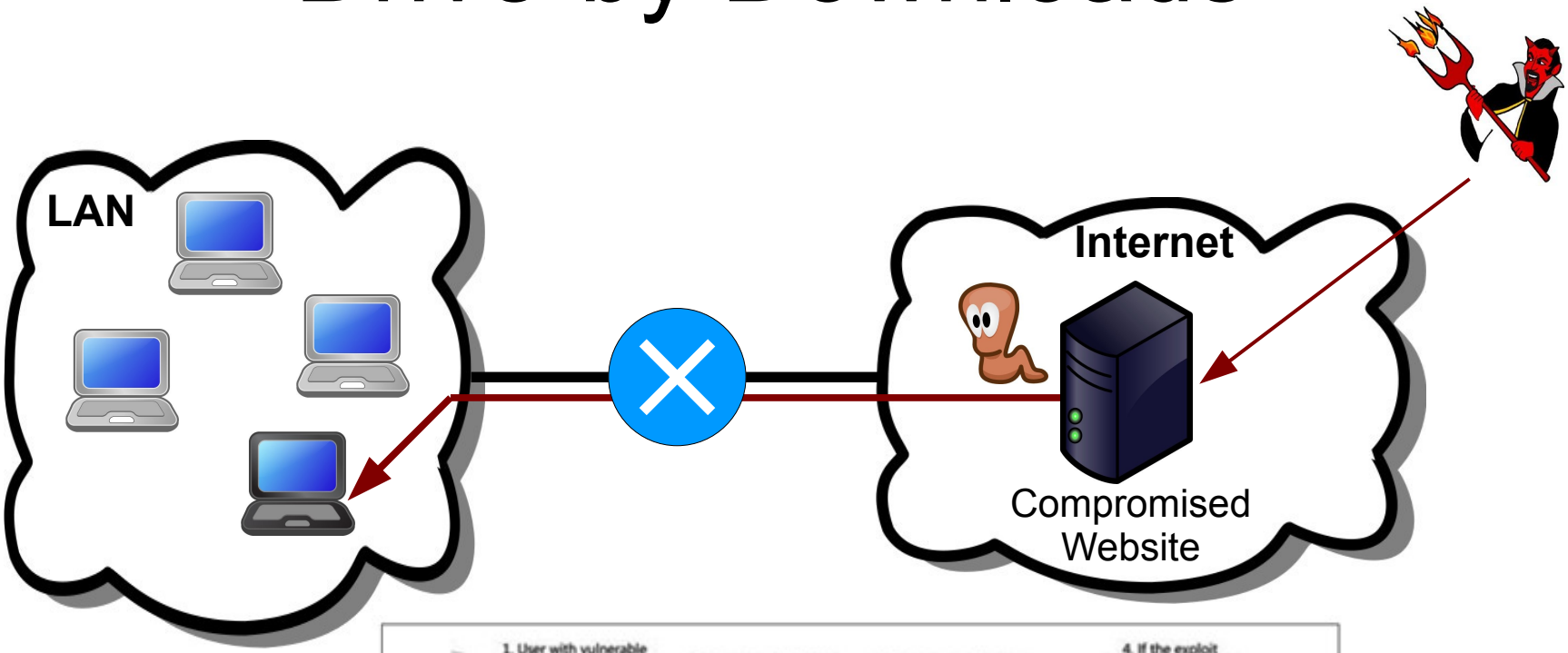
Research Topics

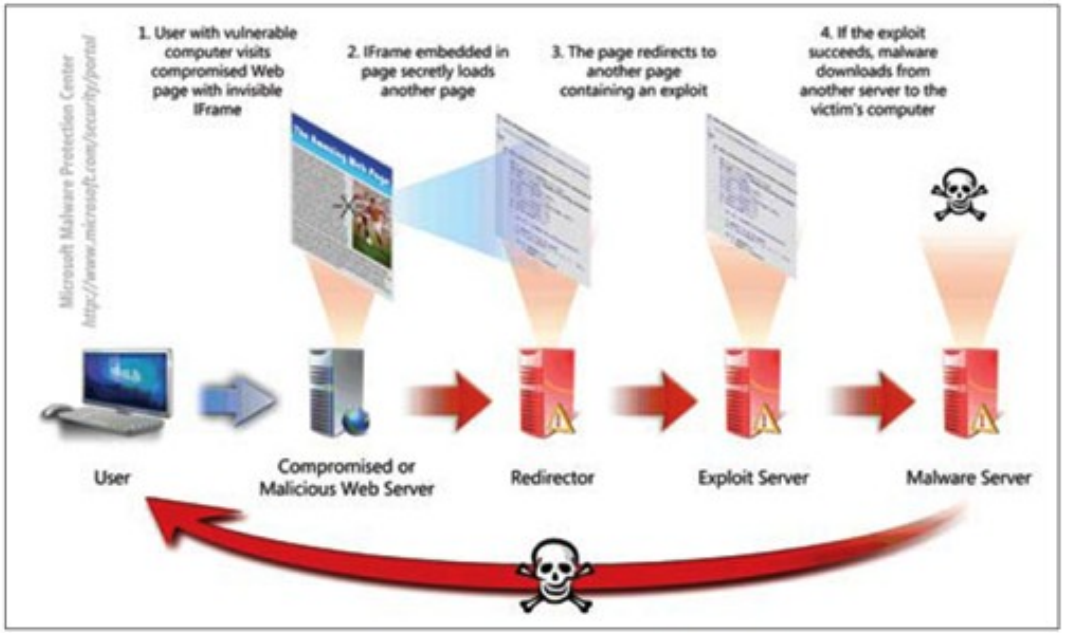
- Malware analysis and detection
- Botnet detection and measurements
- Spam detection
- Intrusion detection
- Automatic vulnerability discovery and protection
- Privacy and anonymity
- Web security
- VoIP security
- Wireless/RFID security
- Physical security
- Cryptography
- ...

Malware

- Generic name for *malicious software*
  - Viruses
  - Worms
  - Trojans
  - Bots
  - Spyware
  - Adware
  - Scareware
  - ...

Drive-by Downloads



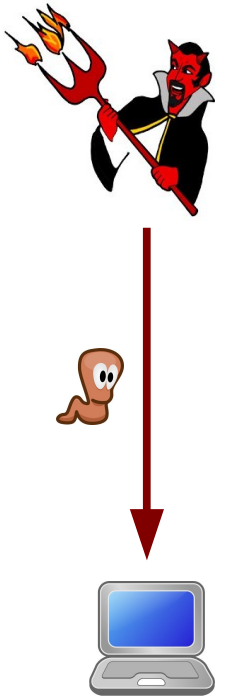


Other Infection Vectors

Social engineering attacks!

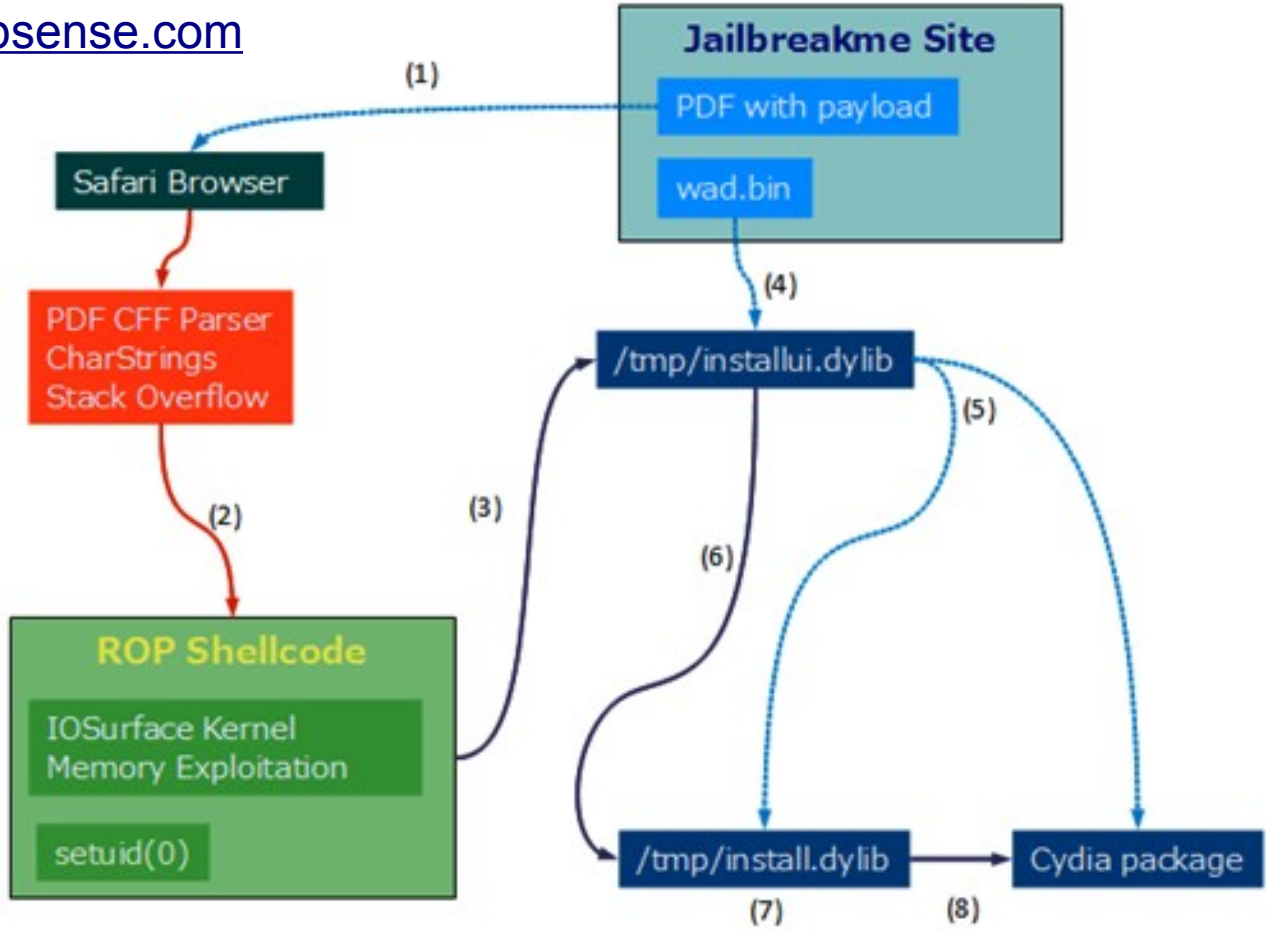
Infected external disk!

Direct *remote exploits*!



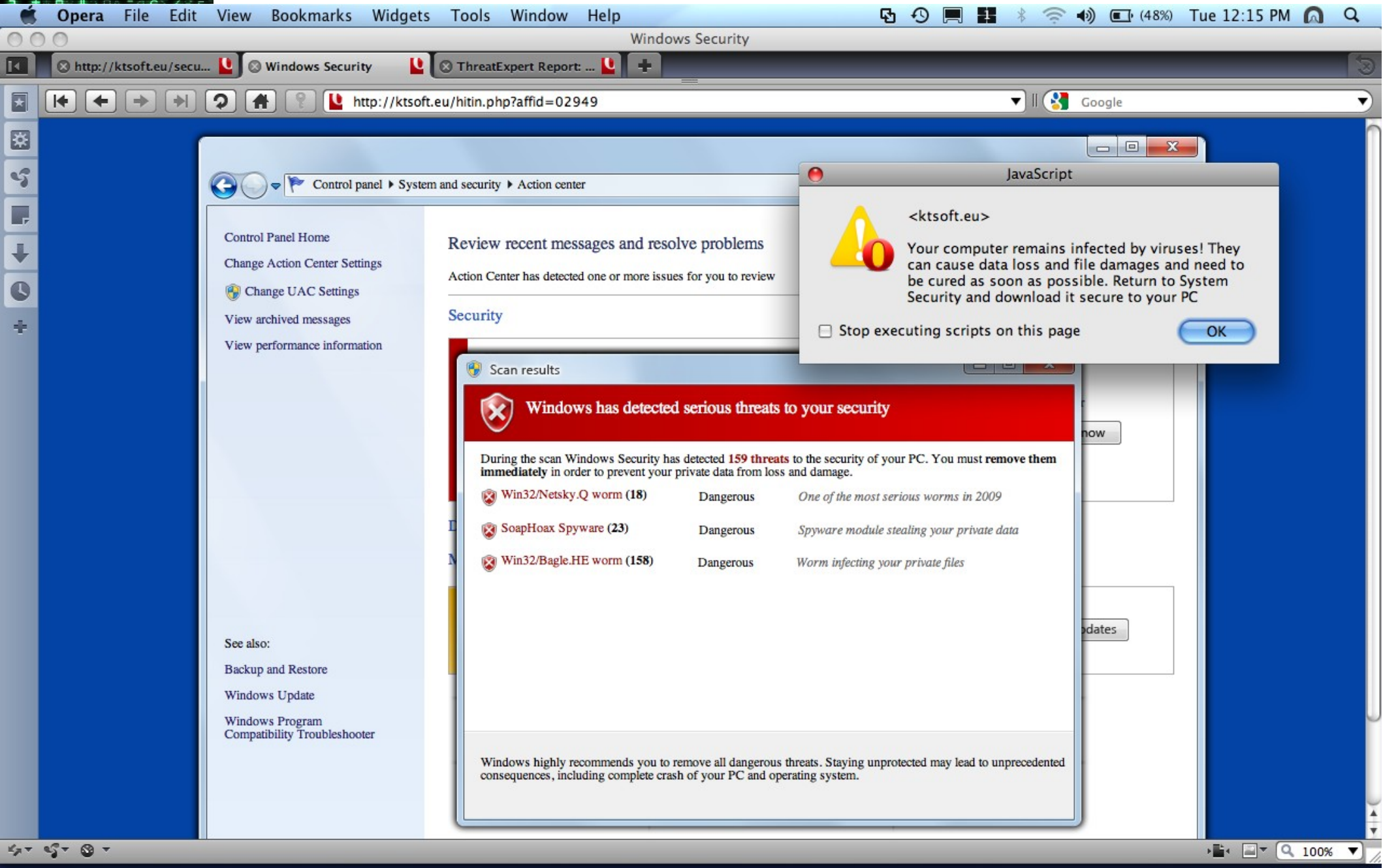
Example of real exploit

source: websense.com



1. The browser downloads the pdf.
2. The CFF CharString payload inside PDF corrupts the stack and control goes to ROP shellcode.
3. After privilege escalation shellcode drops and loads "/tmp/installui.dylib" file. It executes "iui_go" function.
4. "/tmp/installui.dylib" downloads wad.bin from jailbreakme site.
5. Downloaded wad.bin is uncompressed to "/tmp/install.dylib" and Cydia package files.
6. It loads "/tmp/install.dylib" file and executes "do_install" function.
7. "/tmp/install.dylib" modifies the iPhone system files and configurations for jailbreaking.
8. "/tmp/install.dylib" unpacks and installs Cydia.

The Scareware/FakeAV Phenomenon

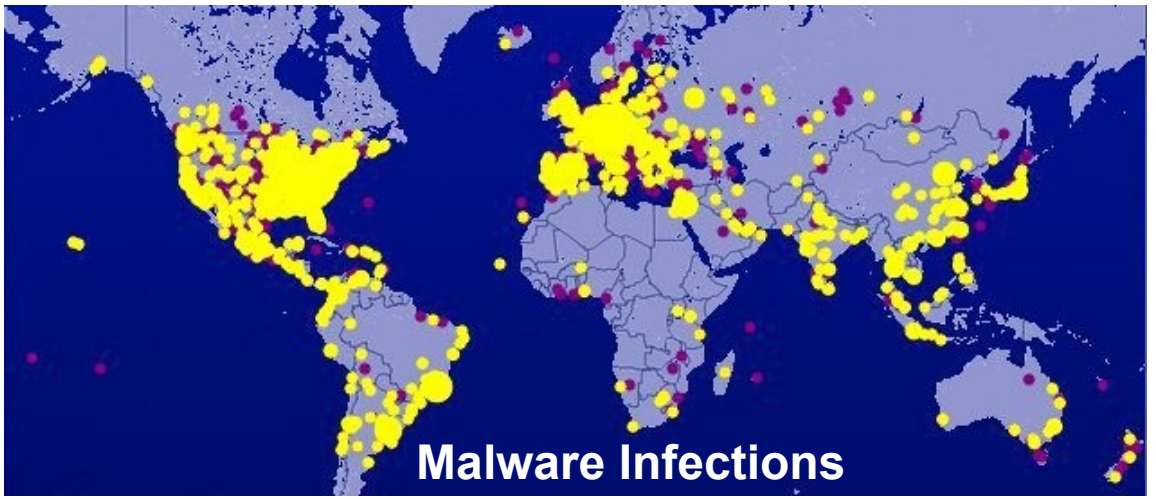


How bad is the malware problem?

The annual financial loss for US organizations amounts to hundreds of millions of dollars.

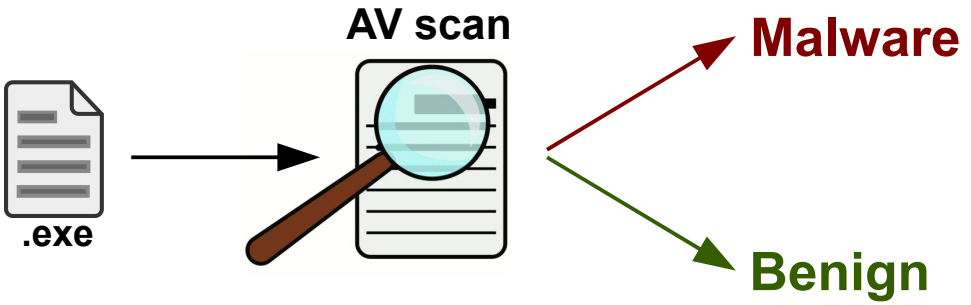
source: CSI/FBI Computer Crime and Security Survey (Dec. 2009)

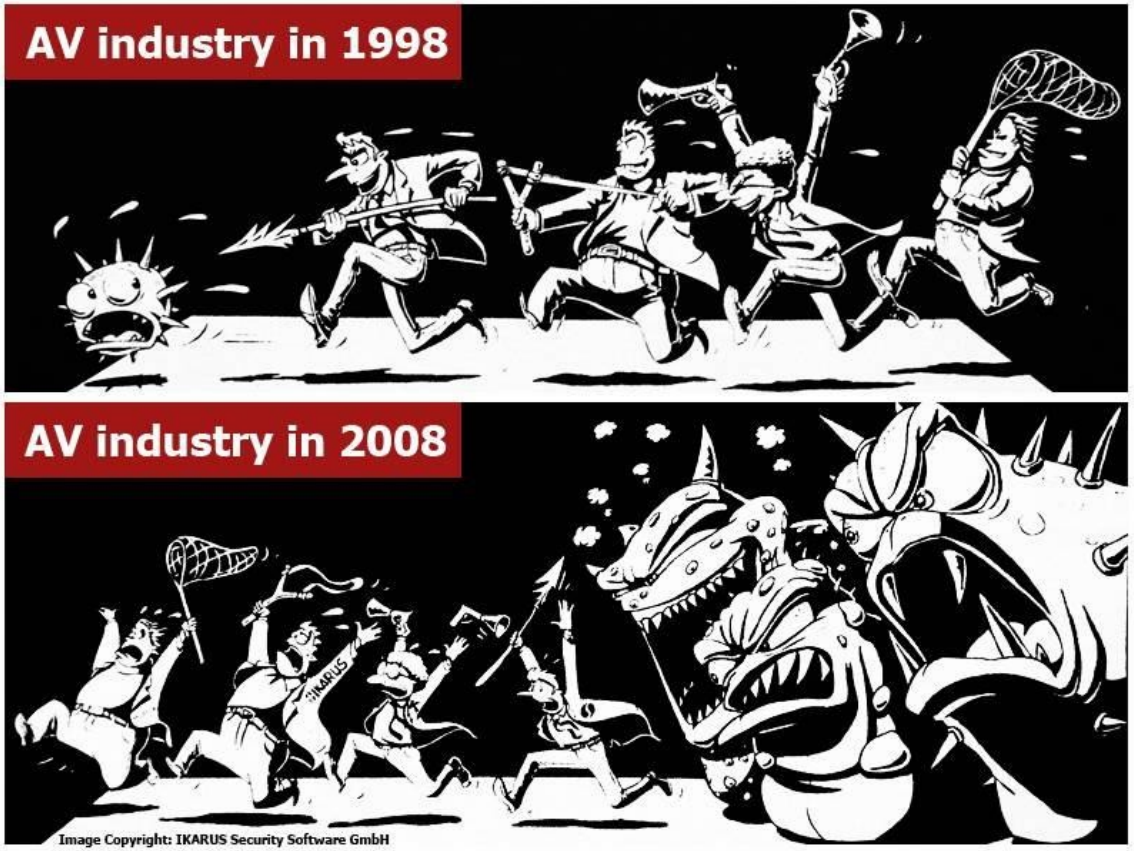
Operation Aurora



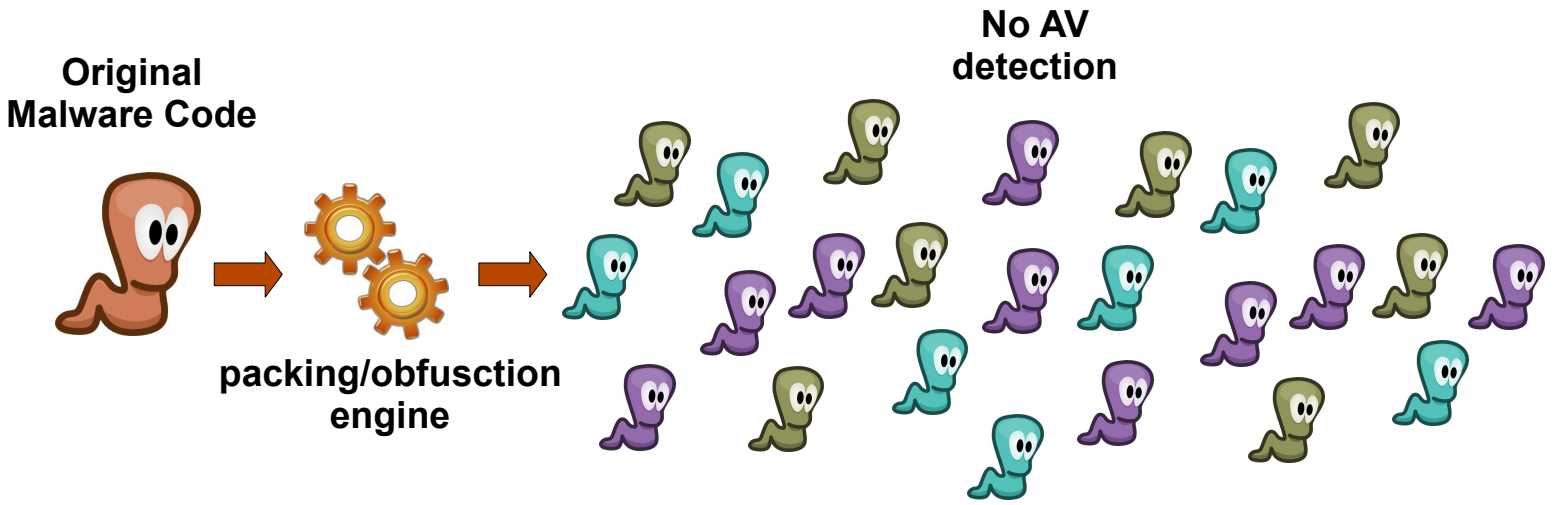
source: shadowserver.org

AVs are loosing the war



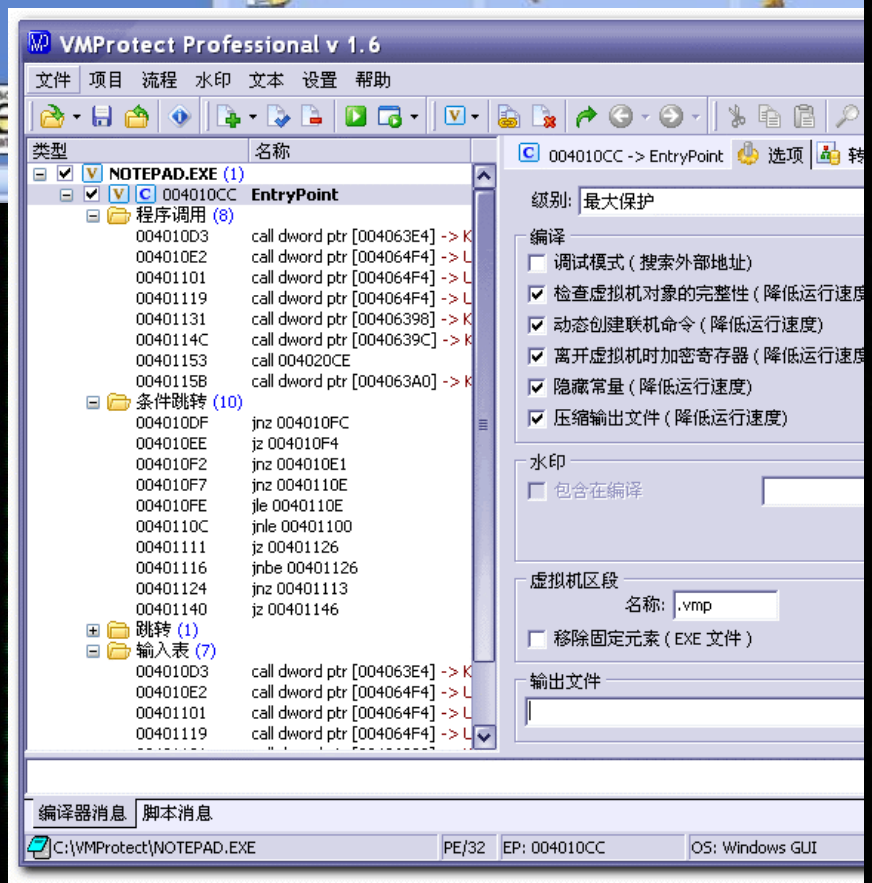


The Packing Problem

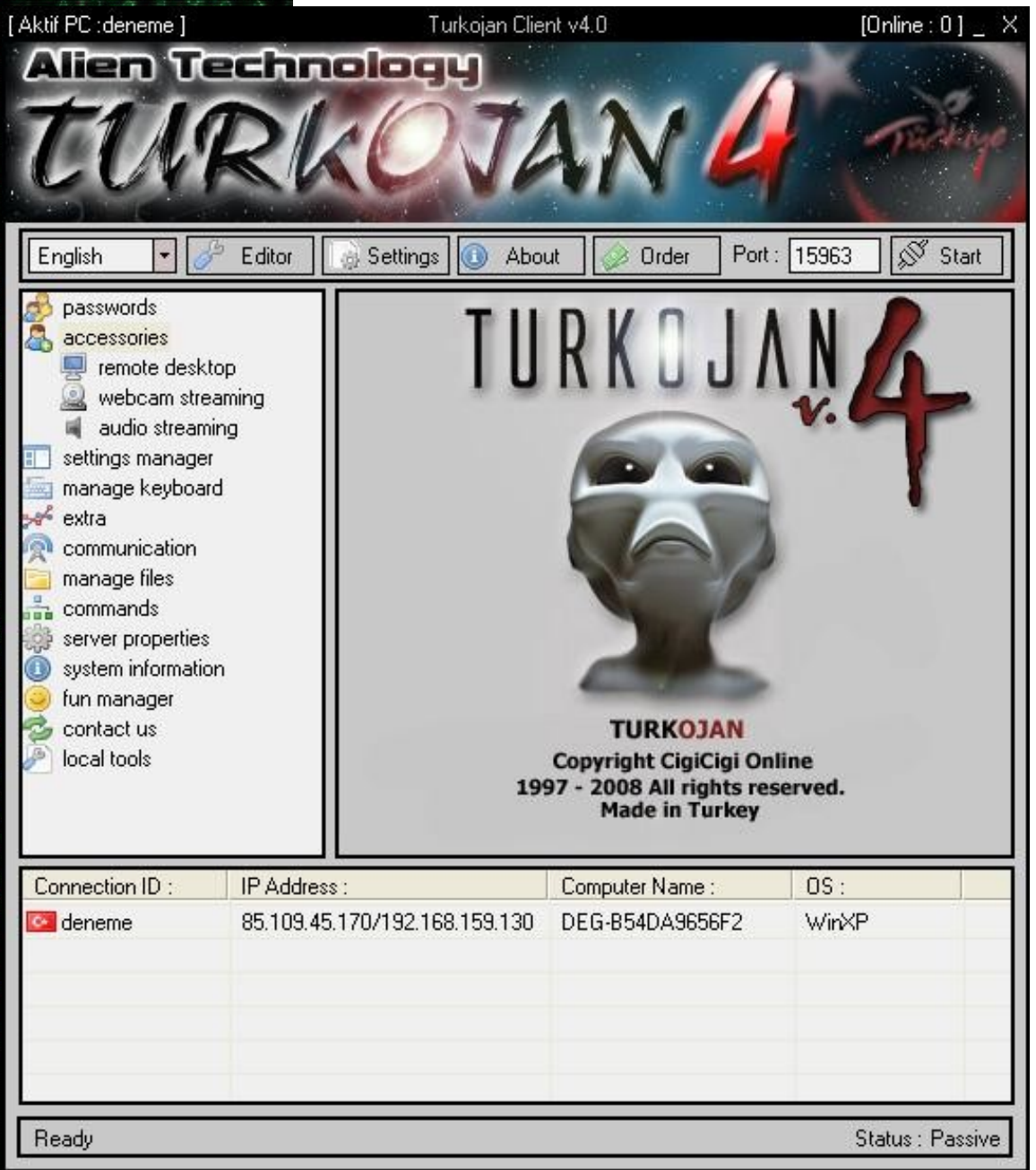


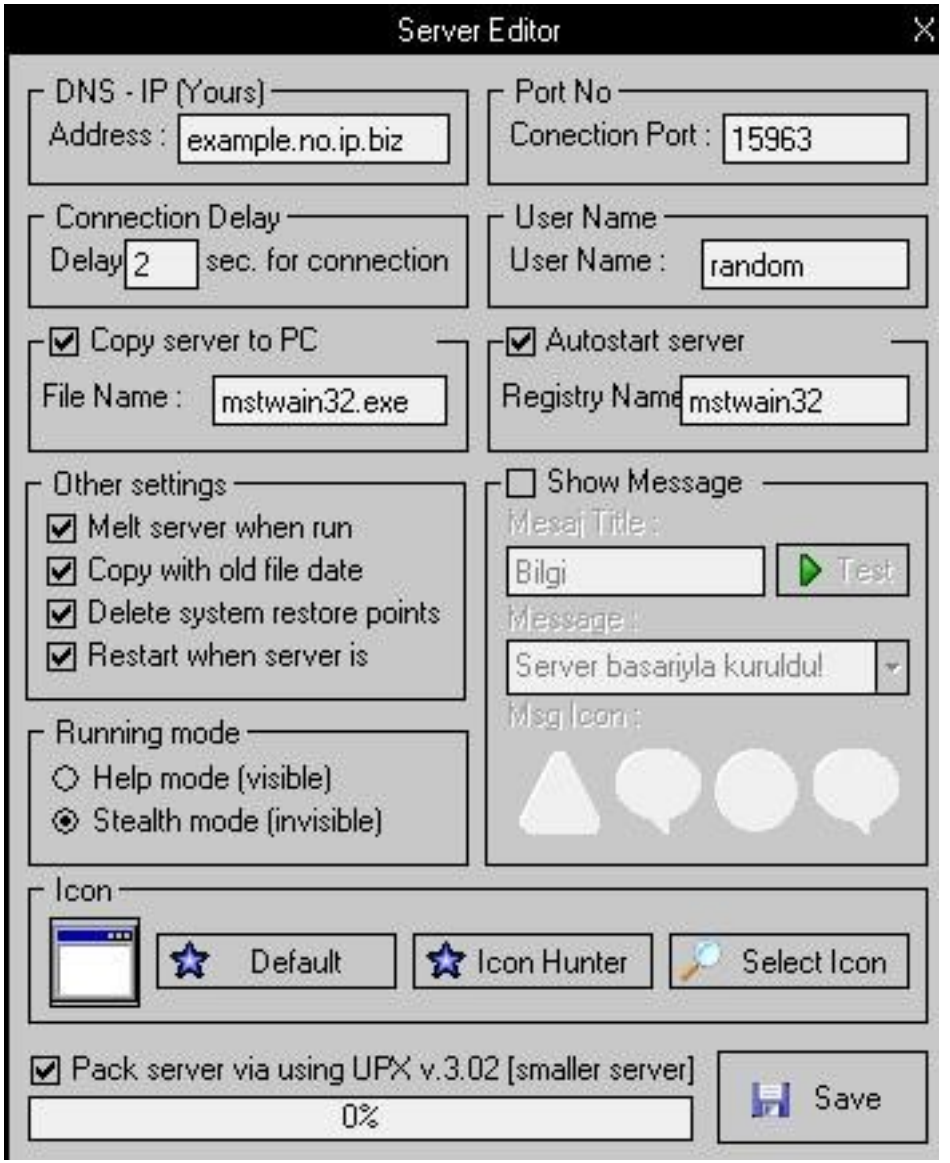
- Hide/obfuscate malware to avoid detection
- Impede malware reverse engineering and analysis

Sophisticated Packers

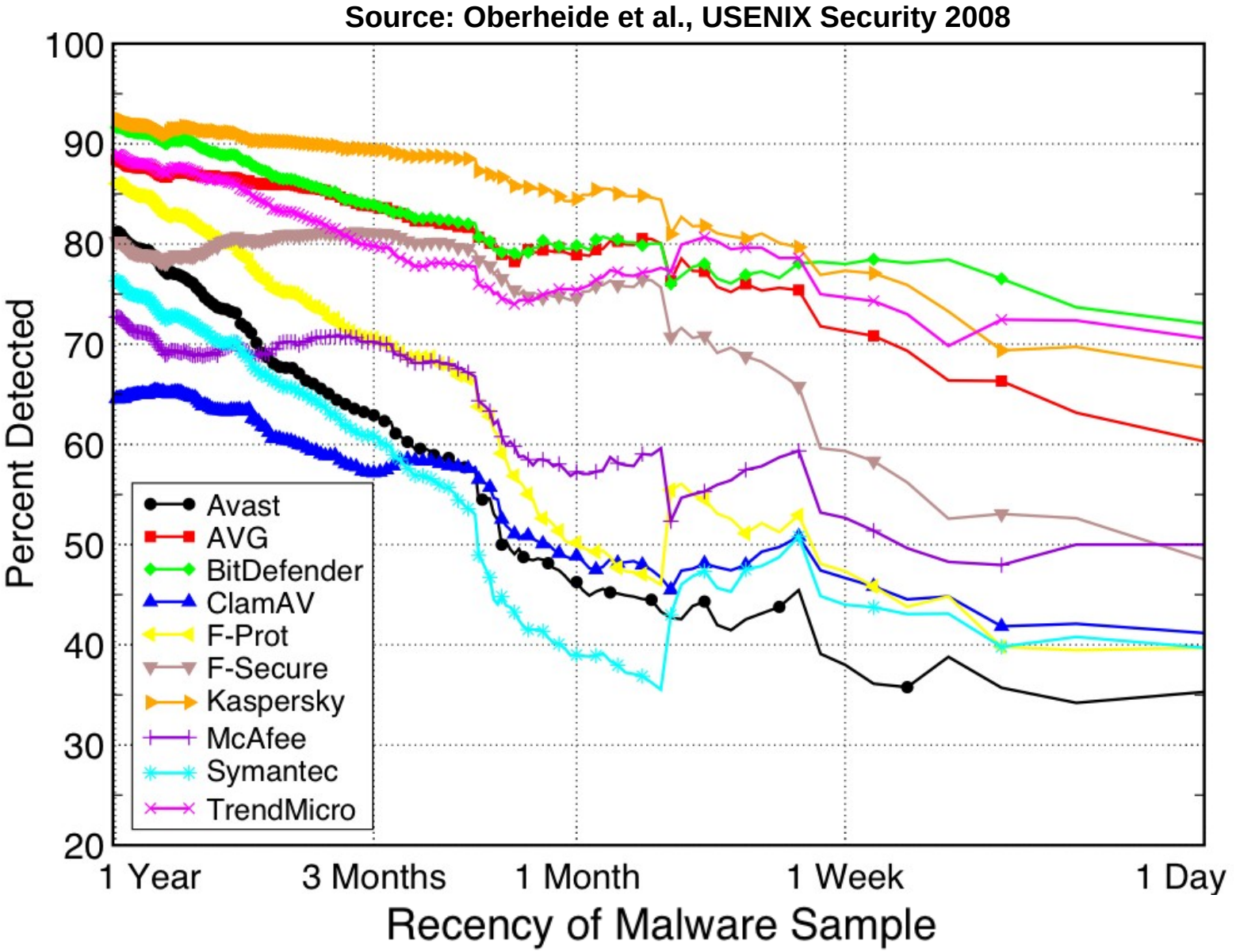


DIY Malware


[Aktif PC :deneme]
Turkojan Client v4.0
[Online : 0]
Alien Technology
TURKOJAN 4
Türkiye
English
Editor
Settings
About
Order
Port : 15963
Start
passwords
accessories
remote desktop
webcam streaming
audio streaming
settings manager
manage keyboard
extra
communication
manage files
commands
server properties
system information
fun manager
contact us
local tools
TURKOJAN v.4
TURKOJAN
Copyright CigiCigi Online
1997 - 2008 All rights reserved.
Made in Turkey
Connection ID :
IP Address :
Computer Name :
OS :
deneme
85.109.45.170/192.168.159.130
DEG-B54DA9656F2
WinXP
Ready
Status : Passive


Server Editor
DNS - IP (Yours)
Address : example.no.ip.biz
Port No
Conection Port : 15963
Connection Delay
Delay 2 sec. for connection
User Name
User Name : random
Copy server to PC
File Name : mstwain32.exe
Autostart server
Registry Name mstwain32
Other settings
Melt server when run
Copy with old file date
Delete system restore points
Restart when server is
Show Message
Mesaj Title :
Bilgi
Test
Message :
Server basariyla kuruldu!
Msg Icon :
Running mode
Help mode (visible)
Stealth mode (invisible)
Icon
Default
Icon Hunter
Select Icon
Pack server via using UPX v.3.02 [smaller server]
0%
Save

Measuring AV accuracy

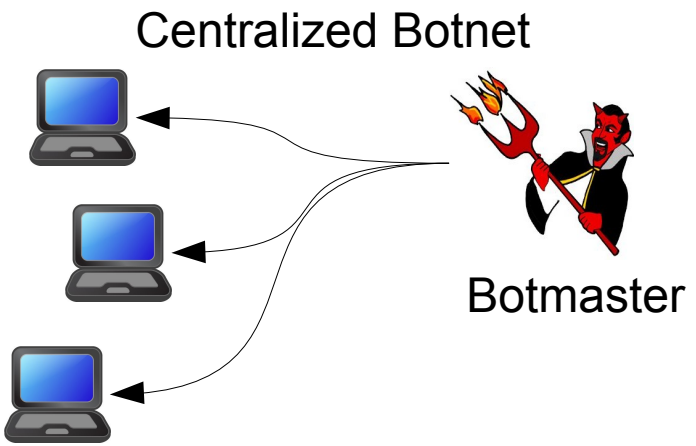


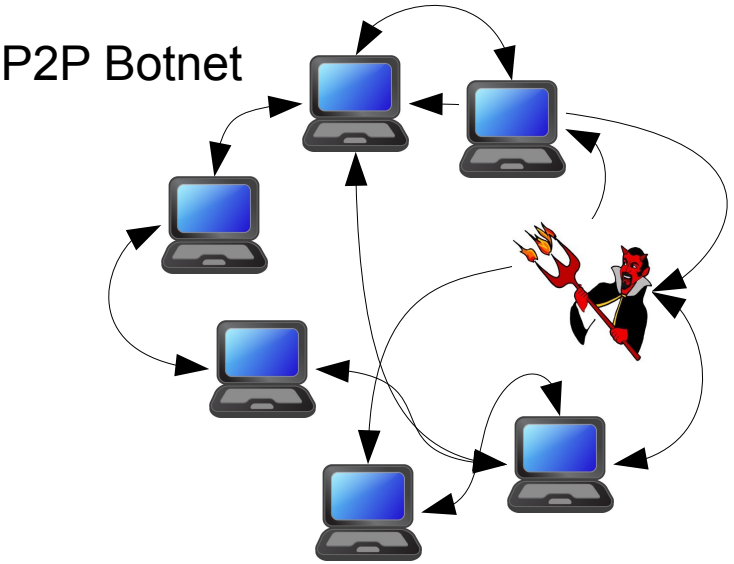
Malware Research

- Analysis
  - Analysis of system and network events
  - Transparent event monitoring
  - Universal unpacking
  - Behavioral clustering and modeling ...
- Detection
  - Detecting malicious system events
  - Detecting malware generated-traffic
  - Preventing infections (e.g., block drive-by downloads) ...

Botnets

- What is a botnet?
  - group of malware-compromised machines (bots)
  - can be remotely controlled by an attacker through a command and control (C&C) channel
  - bots respond to the attaker (the botmaster) commands in a coordinated way





Typical Botnet Activities

- Send spam
- Distributed Denial of Service Attacks
- Phishing/Scam infrastructure
  - e.g., building Malicious Fast-Flux Networks
- Information stealing
  - online banking info, identity theft
- Scanning/searching for new victims
- Massive exploits
  - e.g., massive SQL injection attacks
- Breaking CAPTCHAs

(in)famous botnets

- Storm
- Mega-D
- Zeus
- Waledac
- Bobax
- Kraken
- Torpig/Sinowal
- Srizbi
- ASProx
- Koobface
- Confincker
- Mariposa

- Different botnets are characterized by differences in
  - Number of bots
  - C&C architecture
  - Propagation strategy
  - Kernel/user-level infection
  - Main malicious activities
  - Preferred packing algorithms

Botnet Research

- Analysis
  - C&C protocol reverse engineering
  - Botnet hijacking/infiltration
  - Botnet measurements
  - ...
- Detection
  - netflow-based detection
  - detection based on message-sending patterns
  - DNS-based detection
  - ...

Logistics

- Classroom changes: GSRC 208 (M), HH 101 (TR)
- About paper reviews
  - They are intended to be “mini” reviews
  - The load is not as bad as it may sound
- Reminder
  - Please send me an email with
    - Name, PhD/MSc, year, advisor
    - Email needed to send out last-minute announcements
- **Choose 3 papers from the following list by 8/20**
  - http://www.cs.uga.edu/~perdisci/CSCI6900-F10/Paper_List.html
  - Notice the website is now at www.cs.uga.edu/~perdisci/CSCI6900-F10/
  - Send me your choices via email. **First come, first served!**

Next Time

- Next Time
  - BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection
  - Read the paper (no review required)

- Monday 8/23
  - Behavioral Clustering of HTTP-based Malware and Signature Generation using Malicious Network Traces
  - Read the paper (no review required)