CSCI 8260 – S16

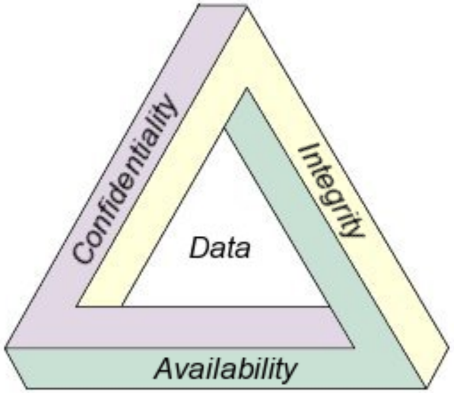
Computer Network Attacks and Defenses

Overview of research topics in computer and network security

Instructor: Prof. Roberto Perdisci

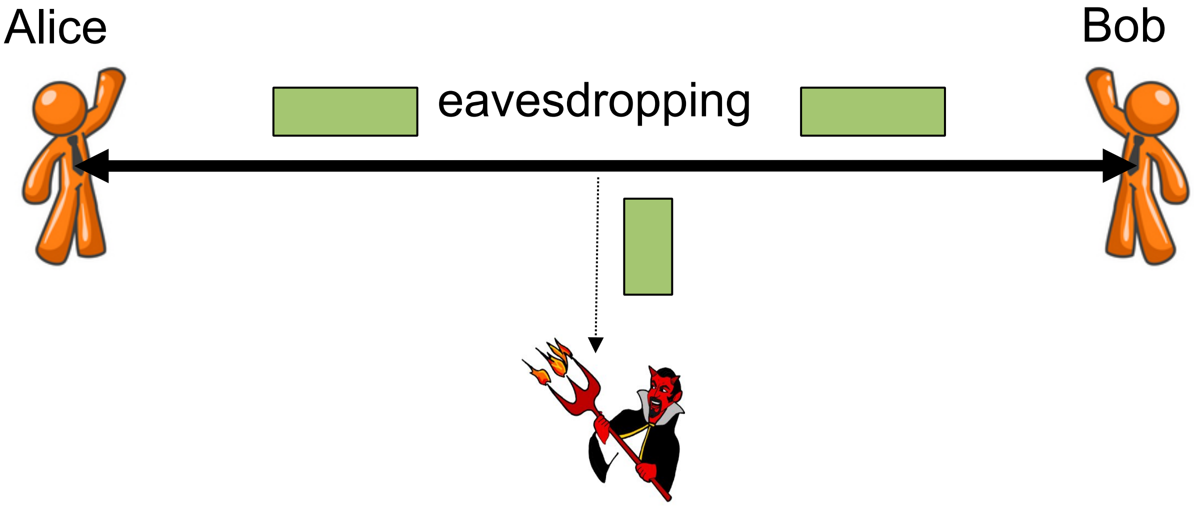
Fundamental Components

- 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

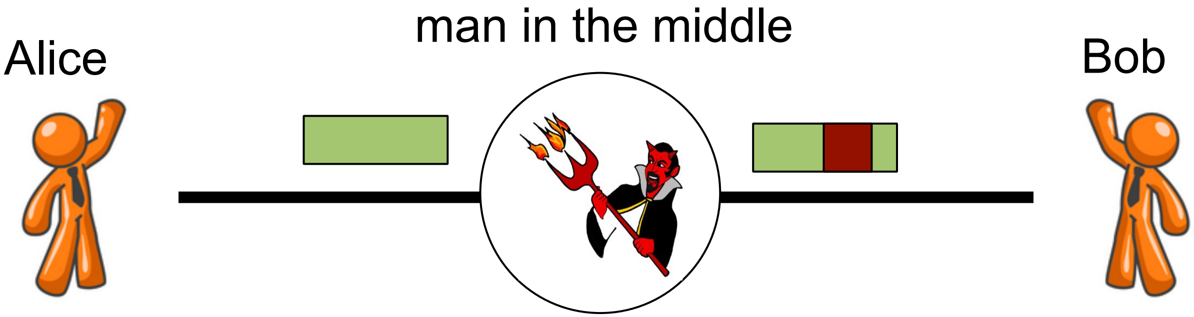


Examples

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

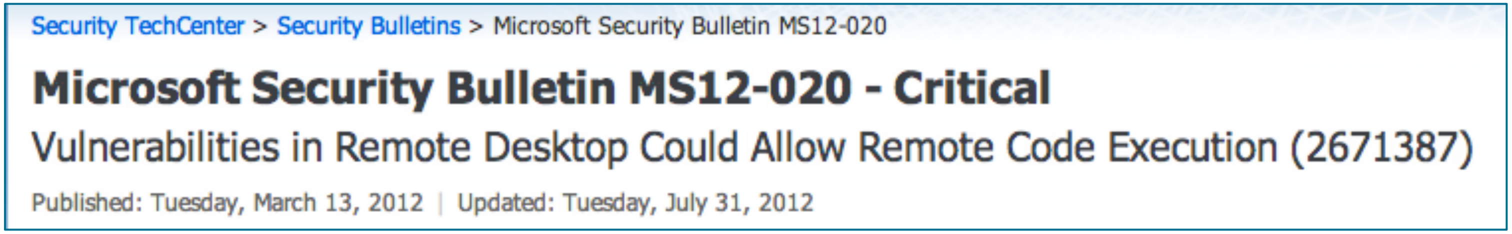
Other Terminology

- ***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 Vulnerability Disclosure



Security TechCenter > Security Bulletins > Microsoft Security Bulletin MS12-020

Microsoft Security Bulletin MS12-020 - Critical

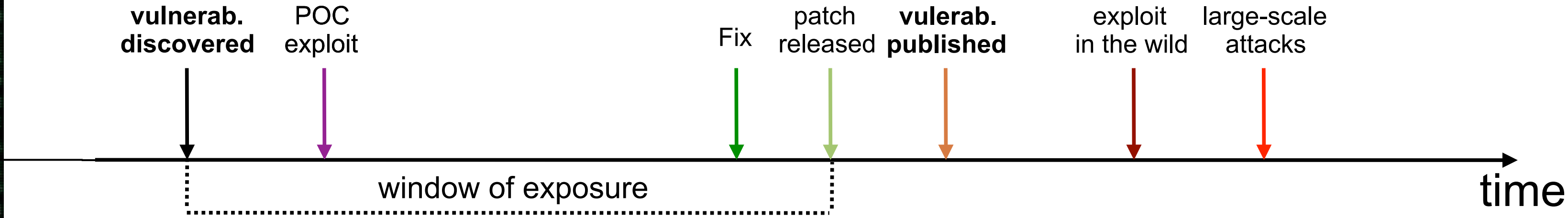
Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)

Published: Tuesday, March 13, 2012 | Updated: Tuesday, July 31, 2012

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

TOP SECRET

Example Scenario (Delayed Disclosure)



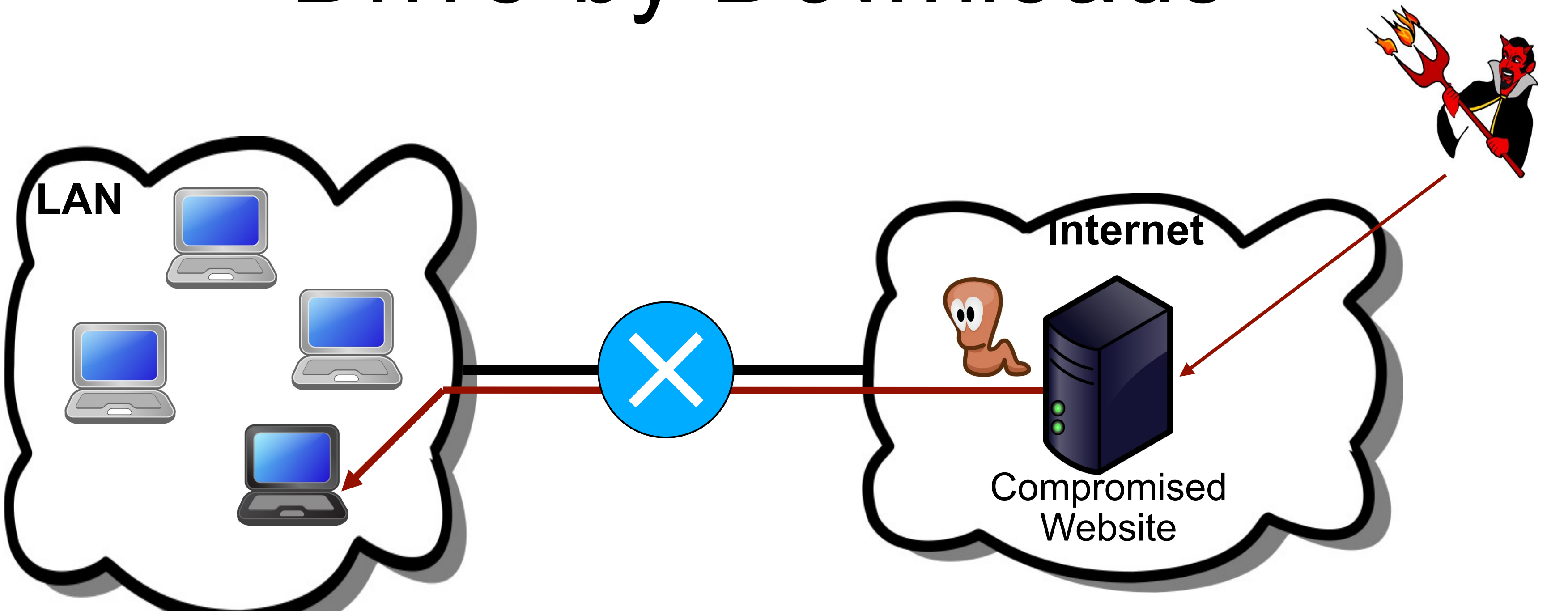
Research Topics

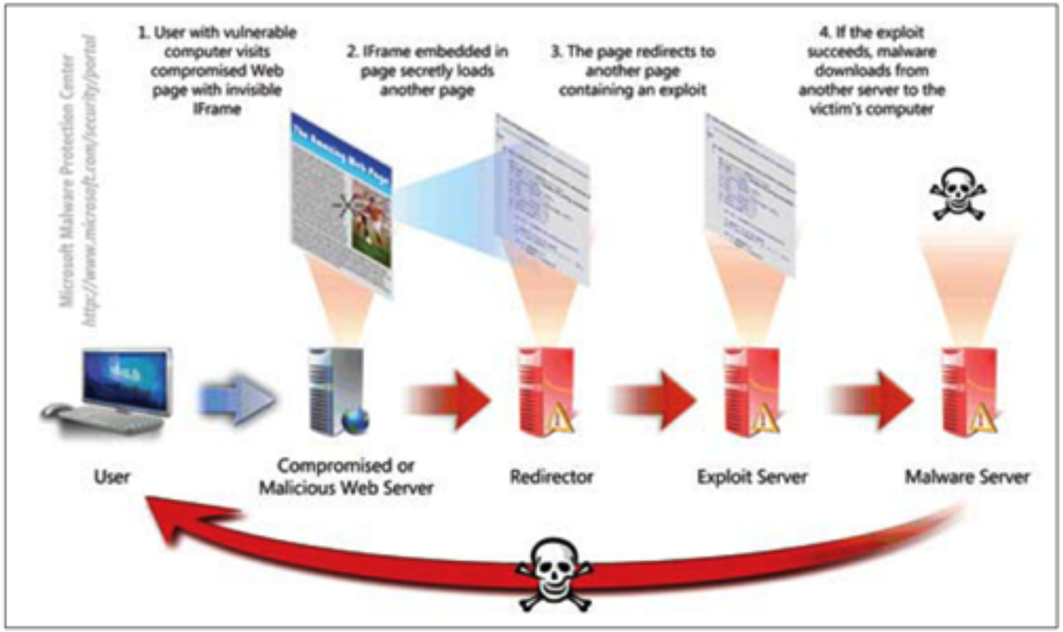
- Malware analysis and detection
- Botnet detection and measurements
- Spam detection
- Intrusion detection
- Automatic vulnerability discovery and protection
- Cloud Security
- Web security
- VoIP security
- Wireless/RFID security
- Privacy and anonymity
- Usable Security
- Physical security
- Cryptography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

Malware

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

Drive-by Downloads

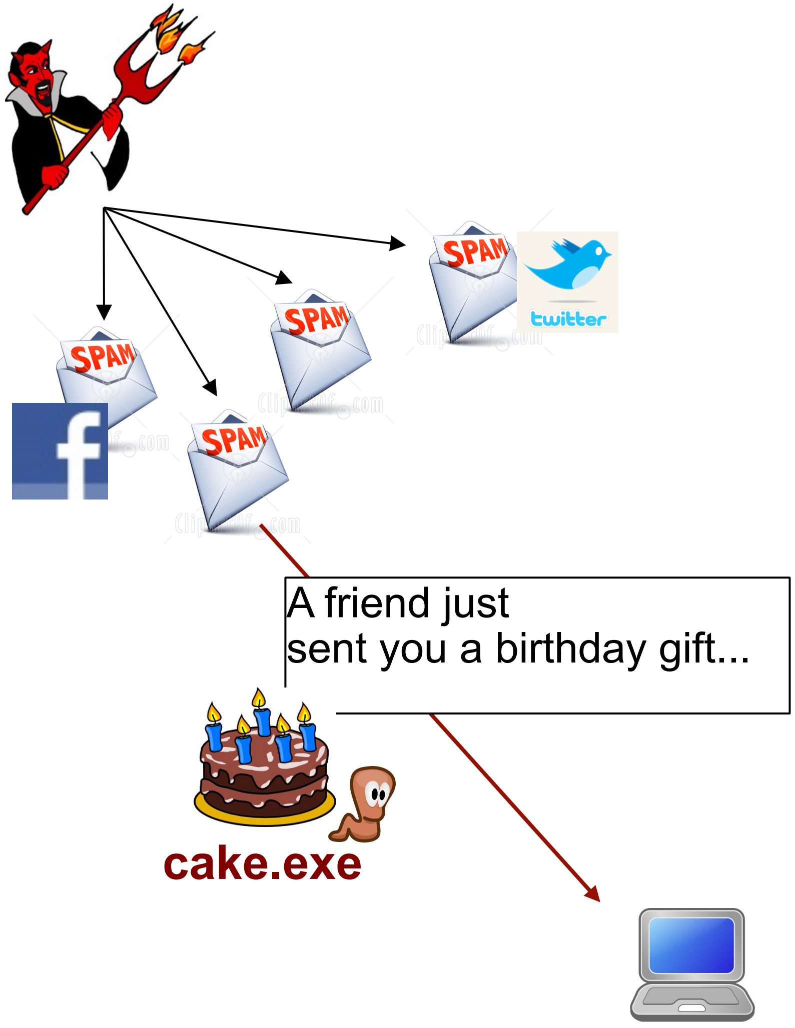



1. User with vulnerable computer visits compromised Web page with invisible IFrame
2. IFrame embedded in page secretly loads another page
3. The page redirects to another page containing an exploit
4. If the exploit succeeds, malware downloads from another server to the victim's computer
User
Compromised or Malicious Web Server
Redirector
Exploit Server
Malware Server

Microsoft Malware Protection Center
http://www.microsoft.com/security/portal

Other Infection Vectors

Social engineering attacks!

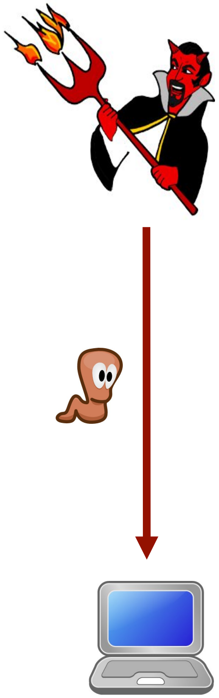


A friend just
sent you a birthday gift...

cake.exe

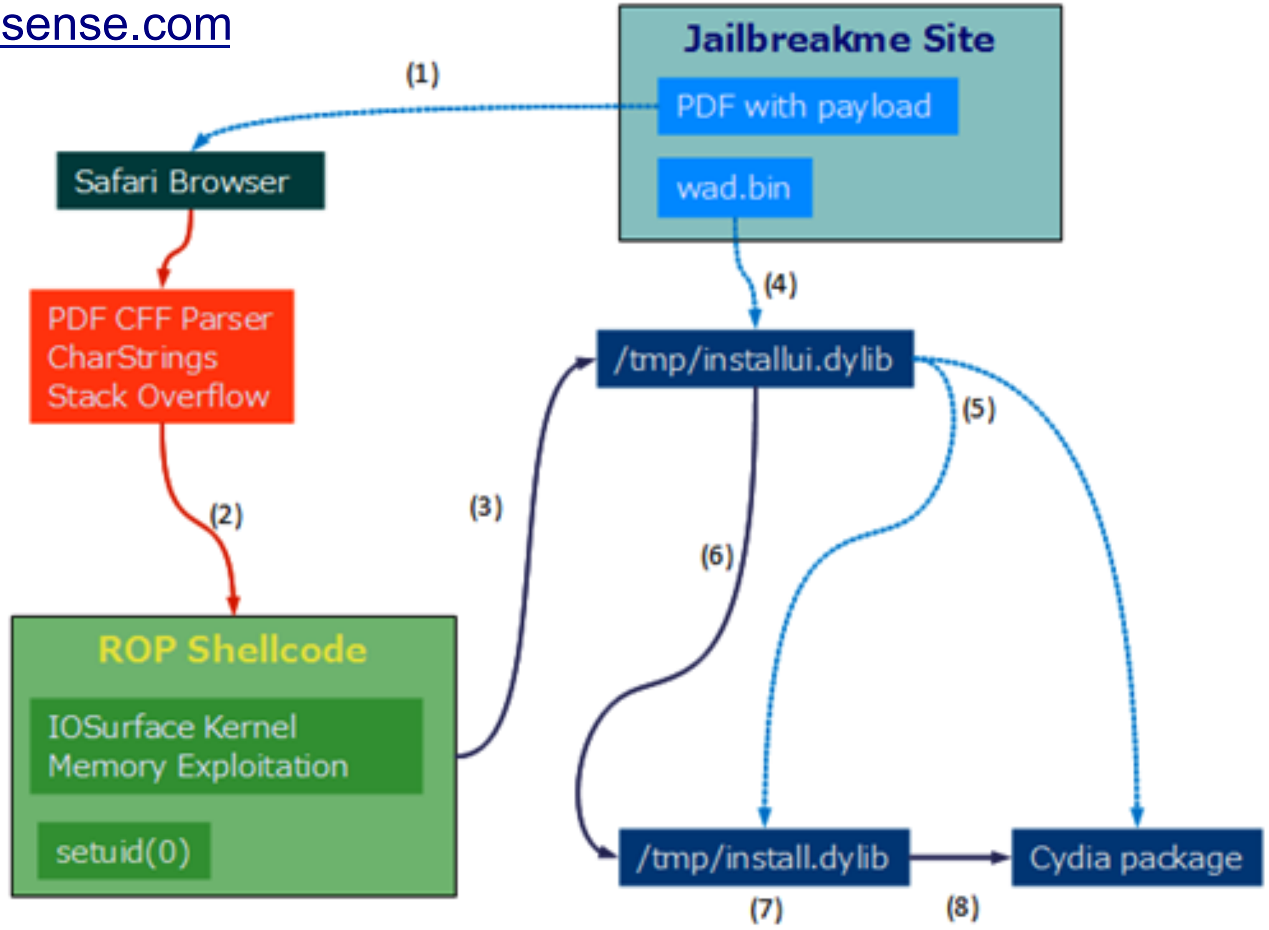
Infected external disk!

Direct *remote exploits*!

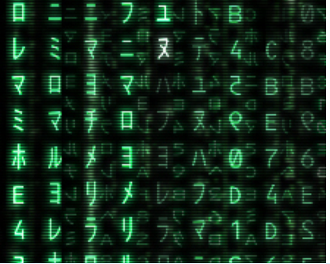


Example of real exploit

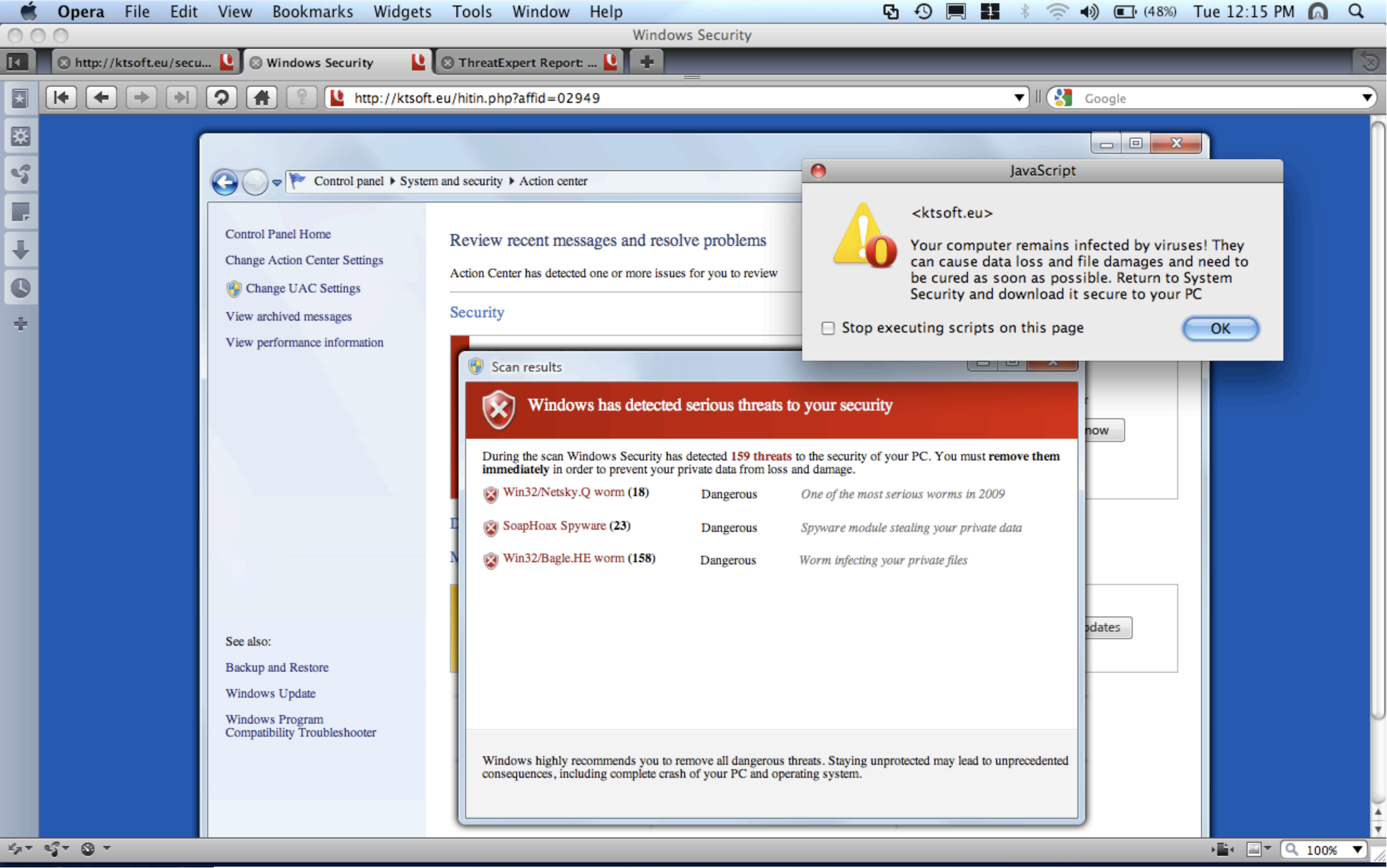
source: websense.com



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



Opera File Edit View Bookmarks Widgets Tools Window Help
(48%) Tue 12:15 PM
Windows Security
http://ktsoft.eu/secu...
Windows Security
ThreatExpert Report: ...
http://ktsoft.eu/hitin.php?affid=02949
Google
Control panel ▸ System and security ▸ Action center
Control Panel Home
Change Action Center Settings
Change UAC Settings
View archived messages
View performance information
See also:
Backup and Restore
Windows Update
Windows Program Compatibility Troubleshooter
Security
now
dates
100%

Review recent messages and resolve problems

Action Center has detected one or more issues for you to review

JavaScript

<ktsoft.eu>

Your computer remains infected by viruses! They can cause data loss and file damages and need to be cured as soon as possible. Return to System Security and download it secure to your PC

□ Stop executing scripts on this page

Scan results

Windows has detected serious threats to your security

During the scan Windows Security has detected **159 threats** to the security of your PC. You must **remove them immediately** in order to prevent your private data from loss and damage.

Win32/Netsky.Q worm **(18)**	Dangerous	*One of the most serious worms in 2009*
SoapHoax Spyware **(23)**	Dangerous	*Spyware module stealing your private data*
Win32/Bagle.HE worm **(158)**	Dangerous	*Worm infecting your private files*

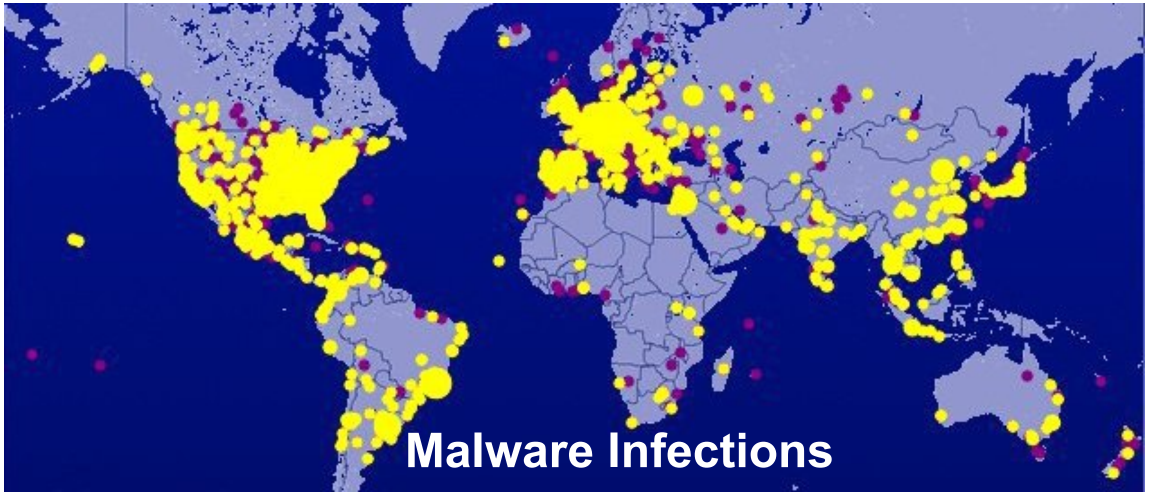
Windows highly recommends you to remove all dangerous threats. Staying unprotected may lead to unprecedented consequences, including complete crash of your PC and operating system.

How bad is the malware problem?

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

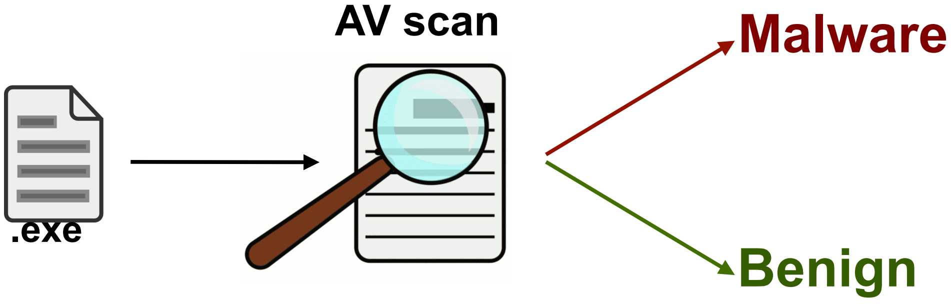
source: CSI/FBI Computer Crime and Security Survey (Dec. 2009)

Operation Aurora



source: shadowserver.org

AVs are loosing the war



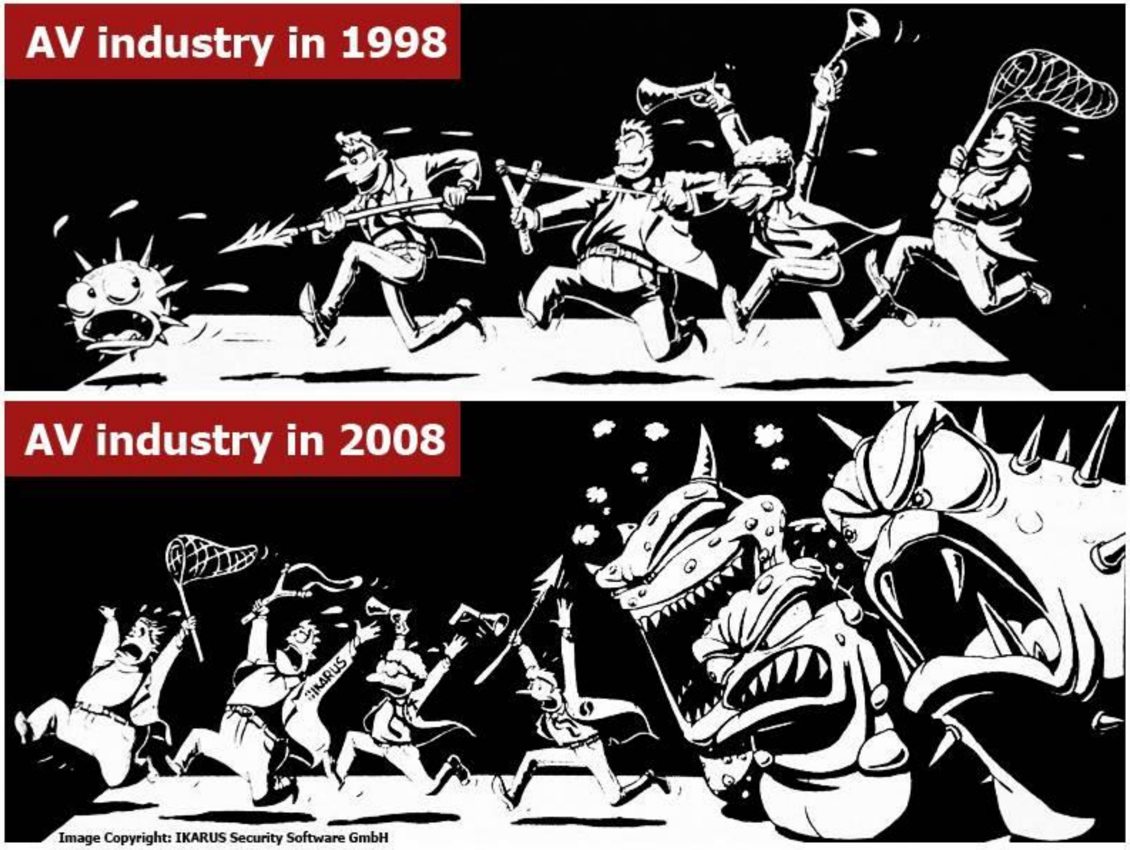
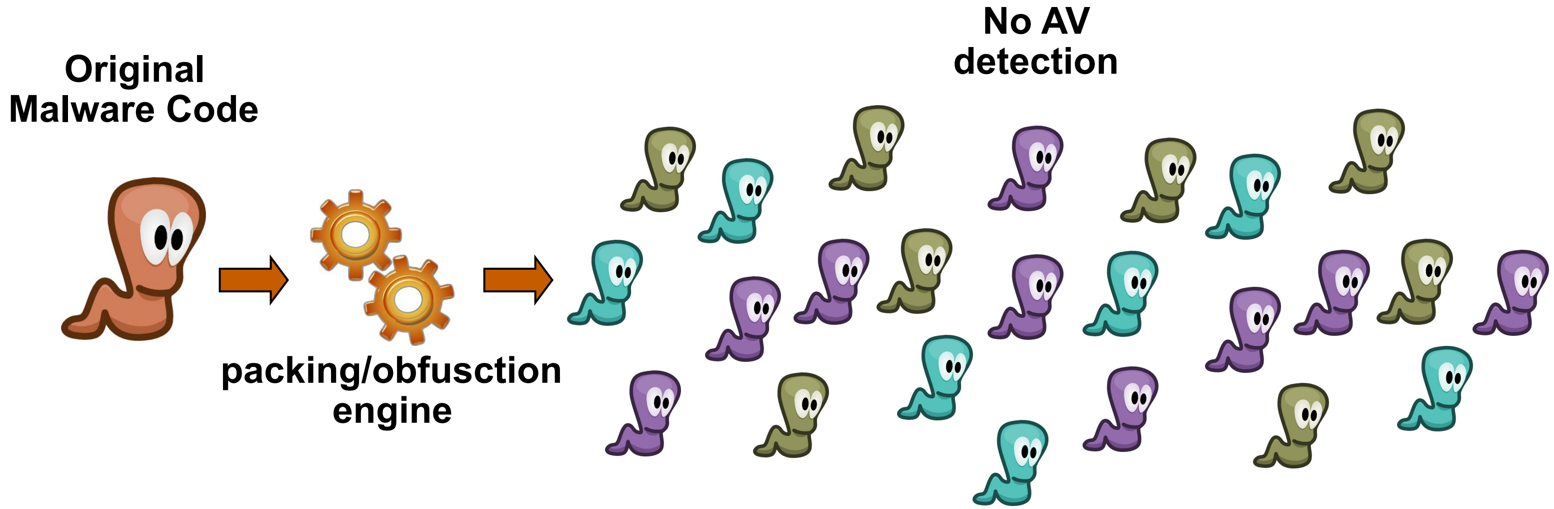


Image Copyright: IKARUS Security Software GmbH

The Packing Problem



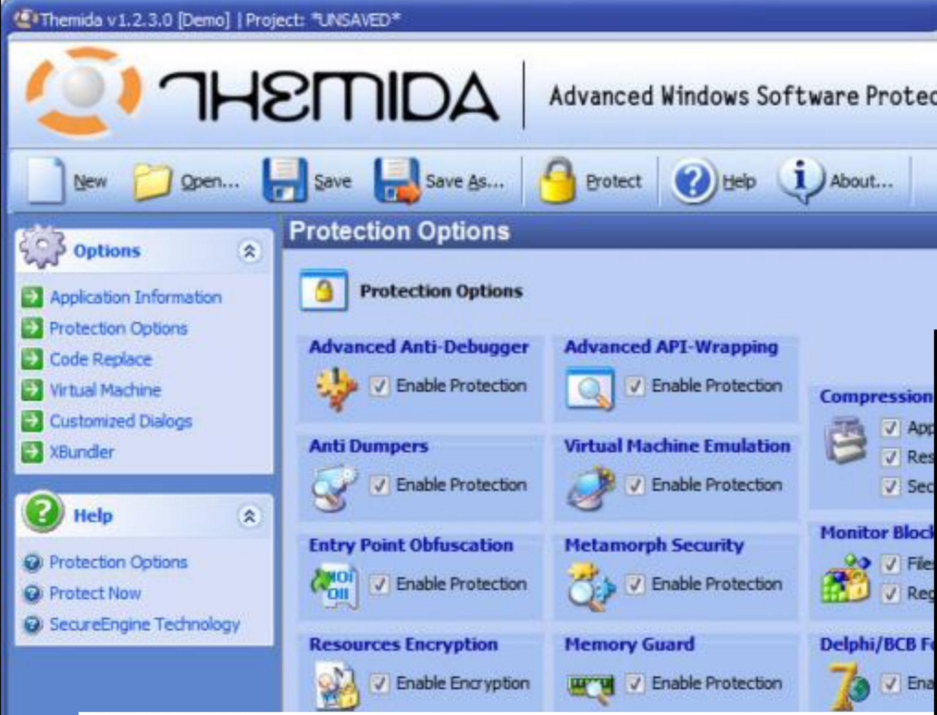
Original Malware Code

packing/obfusction engine

No AV detection

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

Sophisticated Packers


Themida v1.2.3.0 [Demo] | Project: *UNSAVED*

Protection Options

Protection Options

Advanced Anti-Debugger ☑ Enable Protection

Advanced API-Wrapping ☑ Enable Protection

Compression ☑ App ☑ Res ☑ Sec

Anti Dumpers ☑ Enable Protection

Virtual Machine Emulation ☑ Enable Protection

Entry Point Obfuscation ☑ Enable Protection

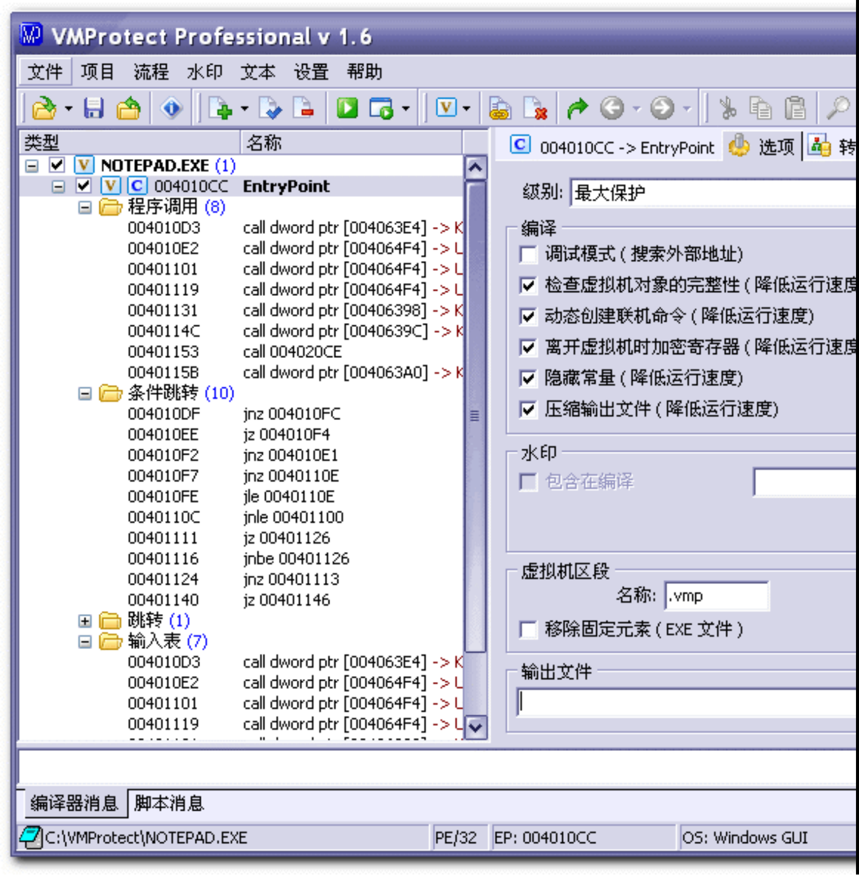
Metamorph Security ☑ Enable Protection

Monitor Bloc ☑ File ☑ Reg

Resources Encryption ☑ Enable Encryption

Memory Guard ☑ Enable Protection

Delphi/BCB F ☑ Ena


VMProtect Professional v 1.6

```
类型                          名称
⊟ ☑ V NOTEPAD.EXE (1)
  ⊟ ☑ V C 004010CC  EntryPoint
     ⊟ 程序调用 (8)
        004010D3    call dword ptr [004063E4] -> K
        004010E2    call dword ptr [004064F4] -> L
        00401101    call dword ptr [004064F4] -> L
        00401119    call dword ptr [004064F4] -> L
        00401131    call dword ptr [00406398] -> K
        0040114C    call dword ptr [0040639C] -> K
        00401153    call 004020CE
        0040115B    call dword ptr [004063A0] -> K
     ⊟ 条件跳转 (10)
        004010DF    jnz 004010FC
        004010EE    jz 004010F4
        004010F2    jnz 004010E1
        004010F7    jnz 0040110E
        004010FE    jle 0040110E
        0040110C    jnle 00401100
        00401111    jz 00401126
        00401116    jnbe 00401126
        00401124    jnz 00401113
        00401140    jz 00401146
     ⊞ 跳转 (1)
     ⊟ 输入表 (7)
        004010D3    call dword ptr [004063E4] -> K
        004010E2    call dword ptr [004064F4] -> L
        00401101    call dword ptr [004064F4] -> L
        00401119    call dword ptr [004064F4] -> L
```

004010CC -> EntryPoint　选项　转

级别: 最大保护

编译
- ☐ 调试模式（搜索外部地址）
- ☑ 检查虚拟机对象的完整性（降低运行速度
- ☑ 动态创建联机命令（降低运行速度）
- ☑ 离开虚拟机时加密寄存器（降低运行速度
- ☑ 隐藏常量（降低运行速度）
- ☑ 压缩输出文件（降低运行速度）

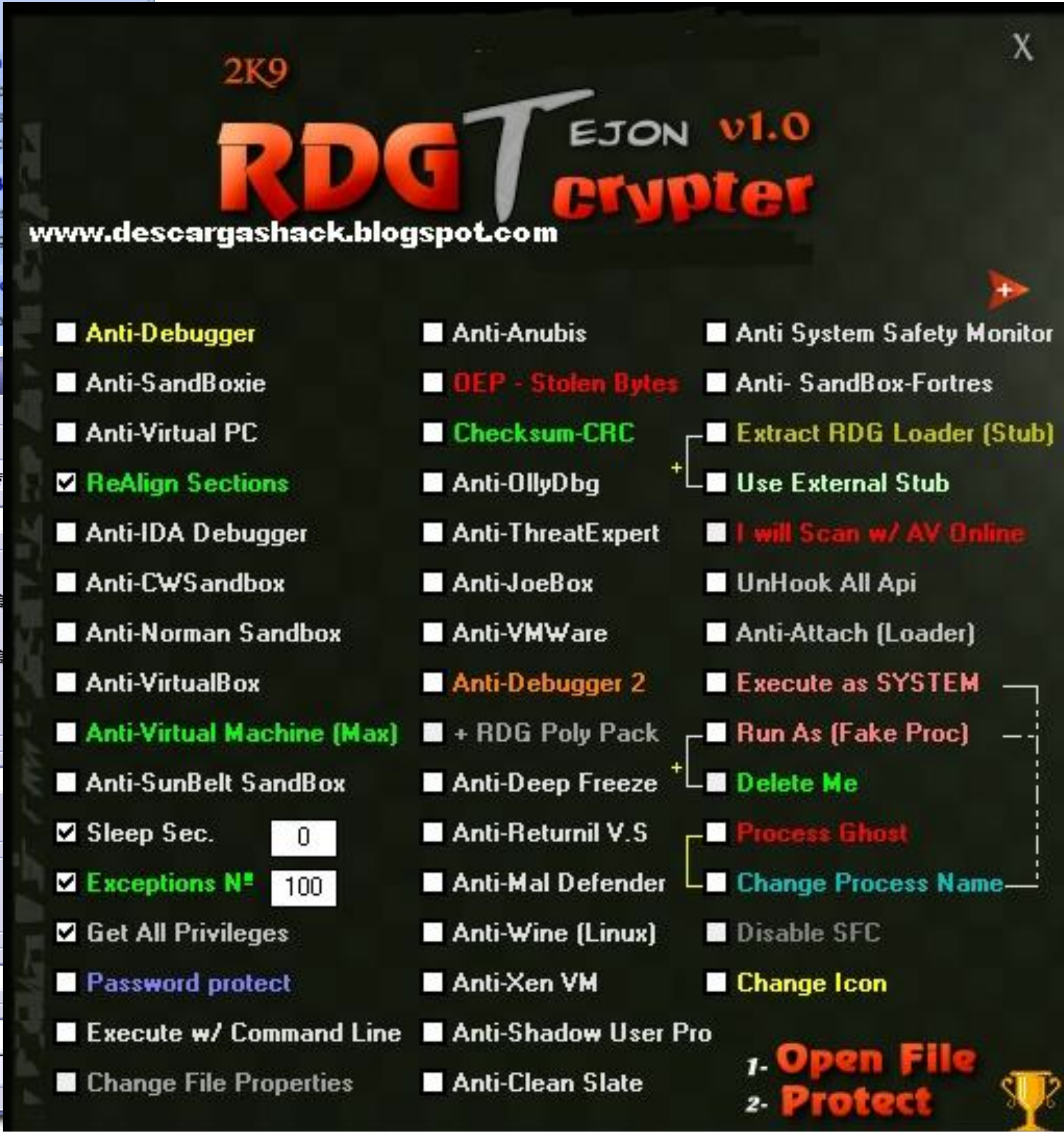
水印
- ☐ 包含在编译

虚拟机区段
名称: .vmp
- ☐ 移除固定元素（EXE 文件）

输出文件

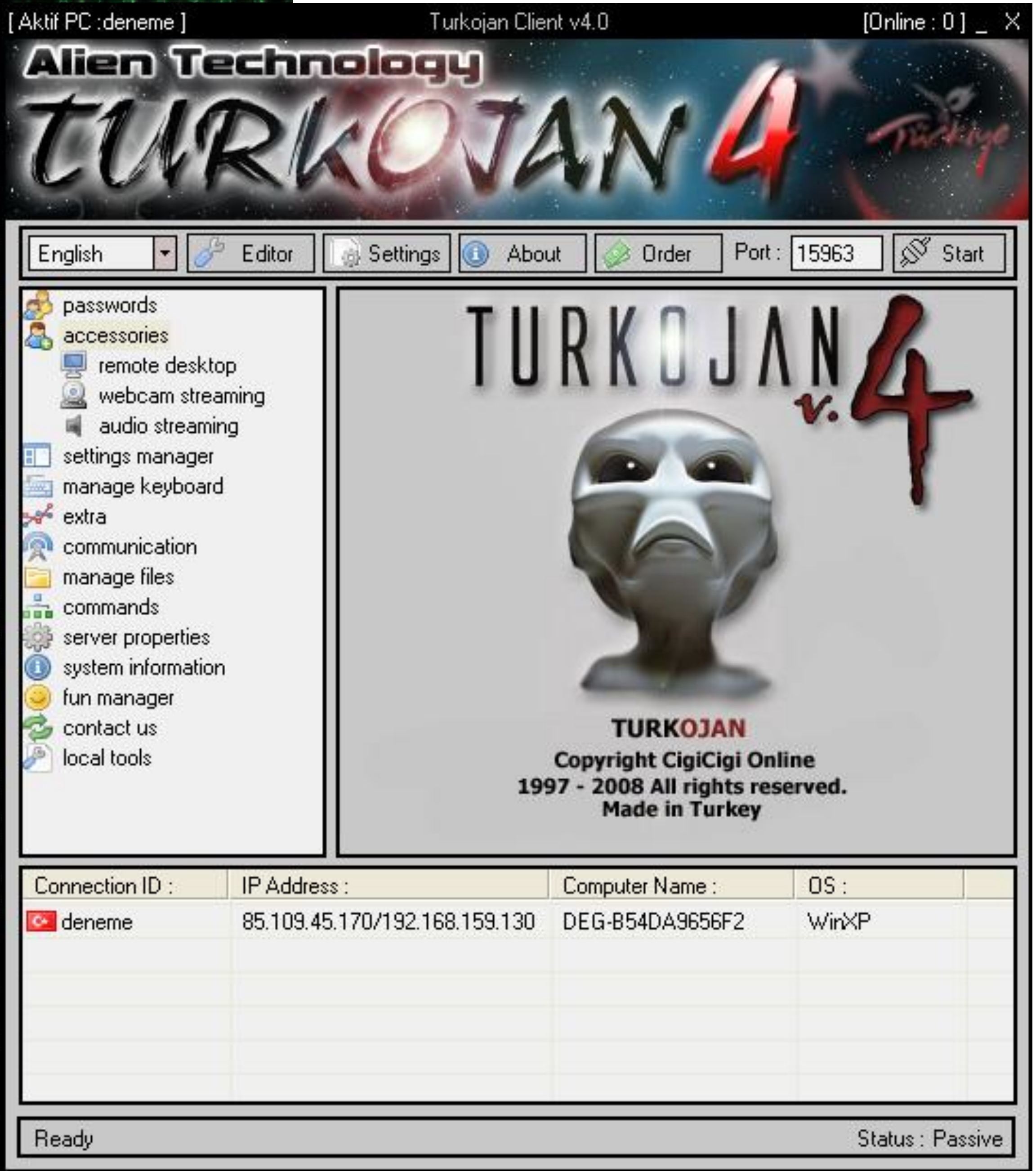
编译器消息　脚本消息

C:\VMProtect\NOTEPAD.EXE　PE/32　EP: 004010CC　OS: Windows GUI



☐ Anti-Debugger	☐ Anti-Anubis	☐ Anti System Safety Monitor
☐ Anti-SandBoxie	☐ OEP - Stolen Bytes	☐ Anti- SandBox-Fortres
☐ Anti-Virtual PC	☐ Checksum-CRC	☐ Extract RDG Loader (Stub)
☑ ReAlign Sections	☐ Anti-OllyDbg	☐ Use External Stub
☐ Anti-IDA Debugger	☐ Anti-ThreatExpert	☐ I will Scan w/ AV Online
☐ Anti-CWSandbox	☐ Anti-JoeBox	☐ UnHook All Api
☐ Anti-Norman Sandbox	☐ Anti-VMWare	☐ Anti-Attach (Loader)
☐ Anti-VirtualBox	☐ Anti-Debugger 2	☐ Execute as SYSTEM
☐ Anti-Virtual Machine (Max)	☐ + RDG Poly Pack	☐ Run As (Fake Proc)
☐ Anti-SunBelt SandBox	☐ Anti-Deep Freeze	☐ Delete Me
☑ Sleep Sec. 0	☐ Anti-Returnil V.S	☐ Process Ghost
☑ Exceptions N° 100	☐ Anti-Mal Defender	☐ Change Process Name
☑ Get All Privileges	☐ Anti-Wine (Linux)	☐ Disable SFC
☐ Password protect	☐ Anti-Xen VM	☐ Change Icon
☐ Execute w/ Command Line	☐ Anti-Shadow User Pro	
☐ Change File Properties	☐ Anti-Clean Slate	

DIY Malware



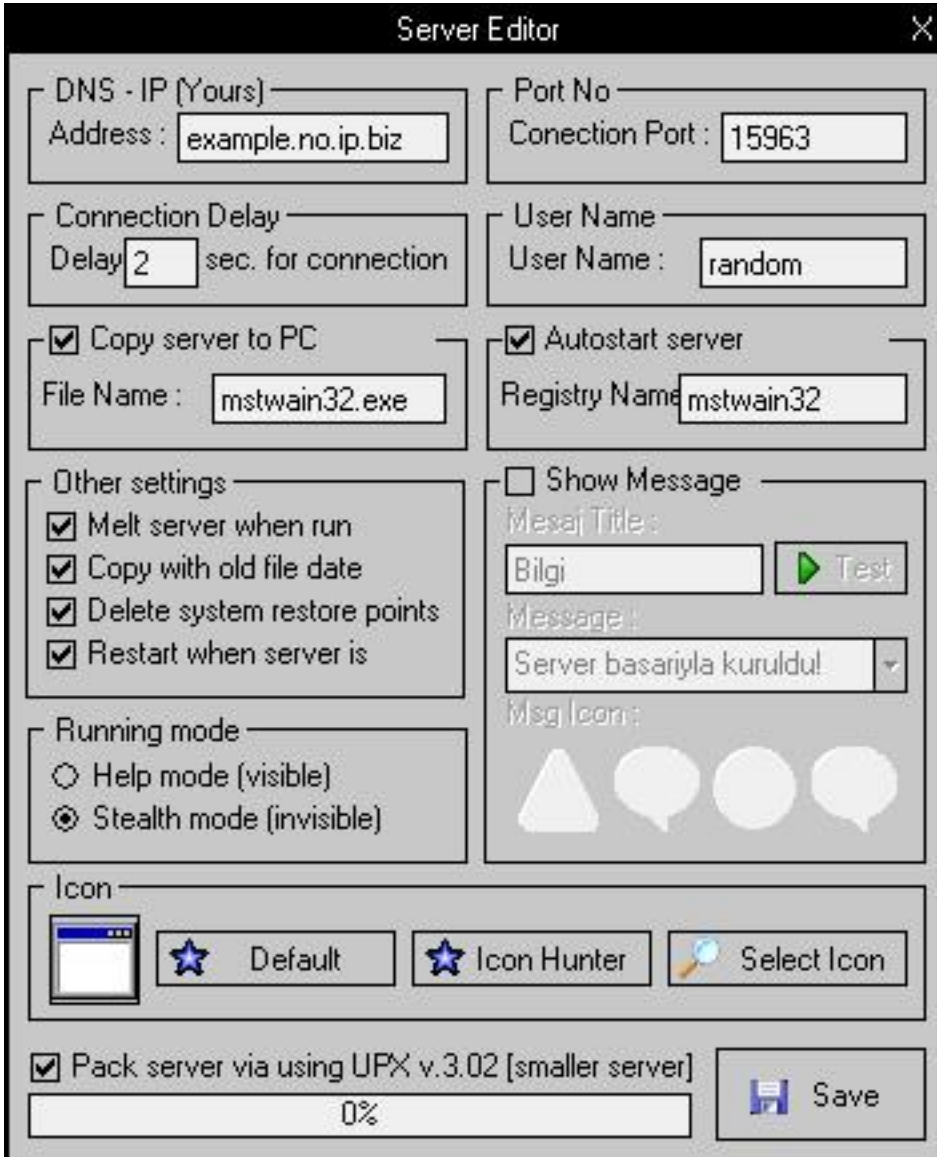
[Aktif PC :deneme]   Turkojan Client v4.0   [Online : 0]

Port : 15963

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
Message :
Server basariyla kuruldu!
Msg Icon :

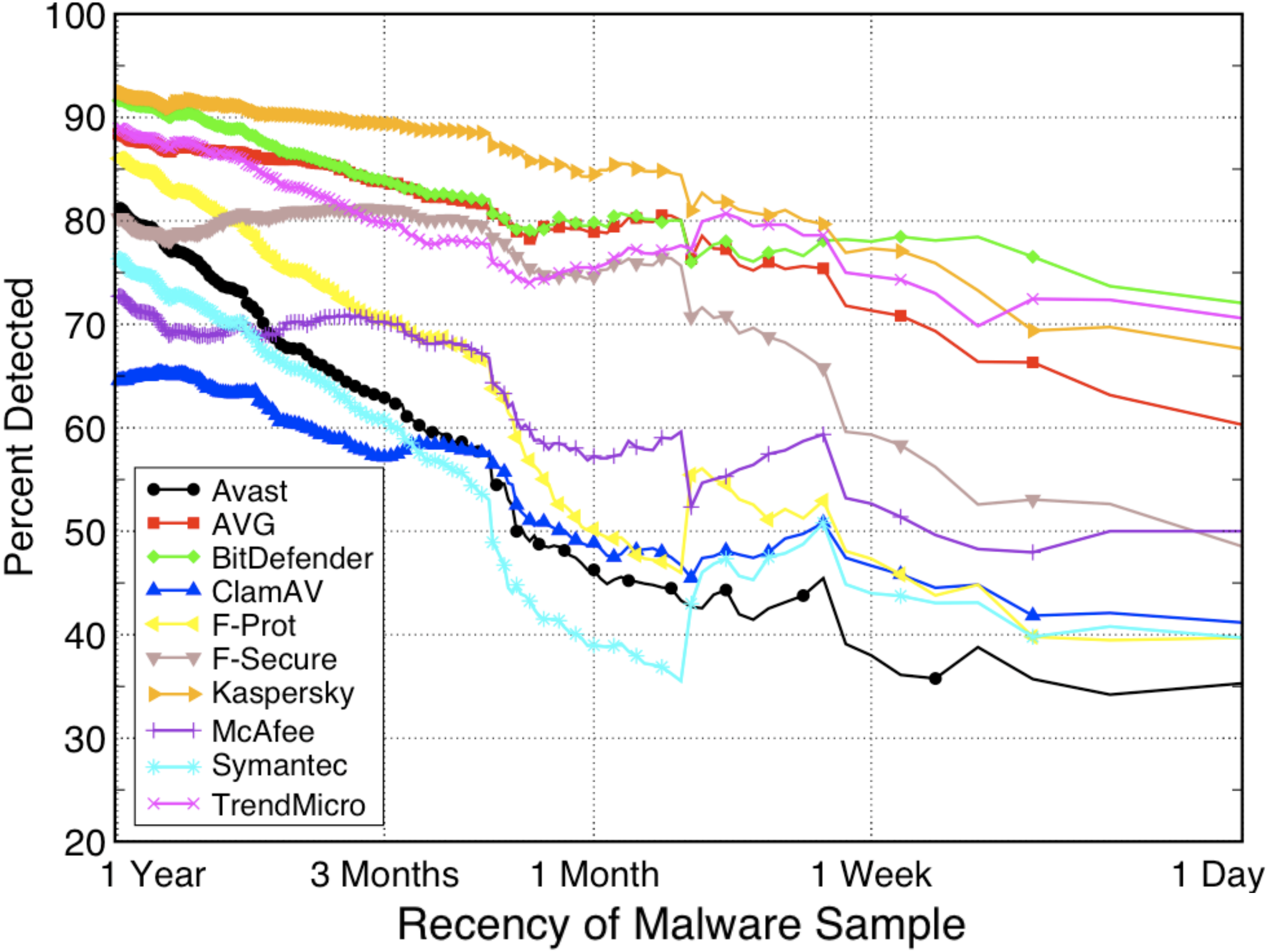
Running mode
○ Help mode [visible]
● Stealth mode [invisible]

Icon

☑ Pack server via using UPX v.3.02 [smaller server]
0%

Measuring AV accuracy

Source: Oberheide et al., USENIX Security 2008

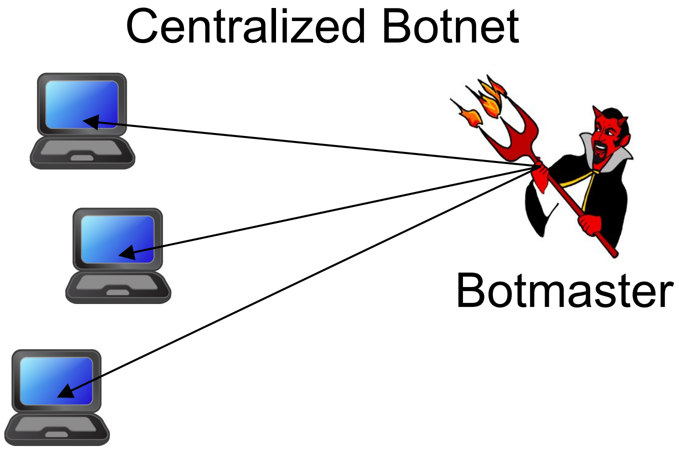


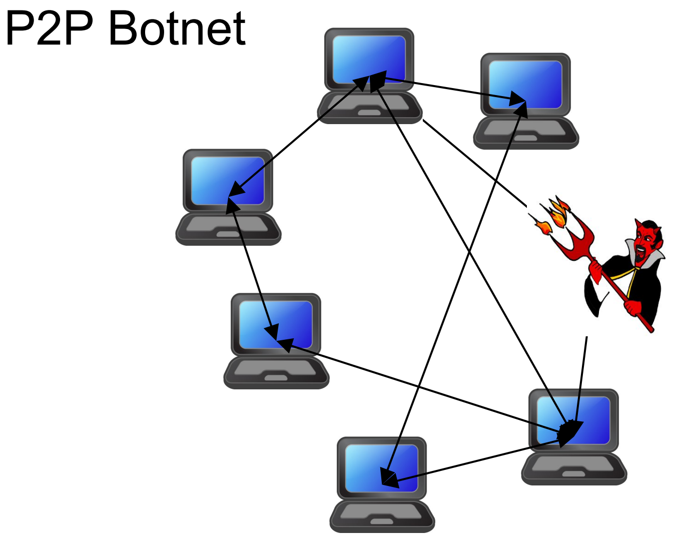
Malware Research

- 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

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

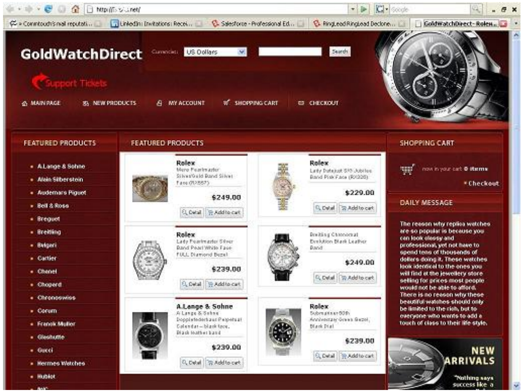
- Different botnets are characterized by differences in
- Number of bots
- C&C architecture
- Propagation strategy
- Kernel/user-level infection
- Main malicious activities
- Preferred packing algorithms

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
  - ...

Spam Detection

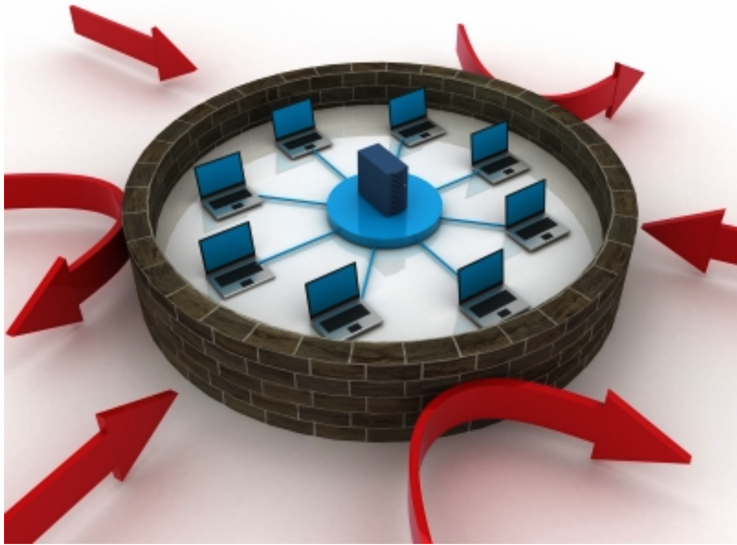
- SPAM = Unsolicited bulk messages
  - email spam, blog spam, **social network** spam
  - new email spam sent via **Gmail/Hotmail**...
- Detection strategies
  - content analysis (headers, body, images...)
  - network-level sender characteristics
    - e.g., IP reputation, sender behavior...



Intrusion Detection

- Detect attempted and successful attacks
- Types of IDS
  - host-based: monitor system events
  - network-based: monitor network traffic
  - signature-based (or misuse-based): rely on attack models
  - anomaly-based: rely on

    a model of normal events
  - hybrid approaches
  - IDS vs. IPS



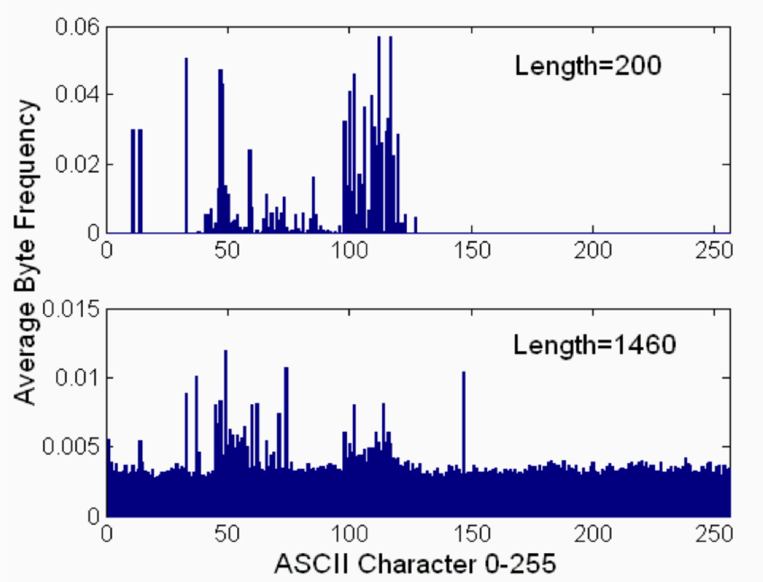
Intrusion Detection

- Example of signature-based network intrusion detection (www.snort.org)

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "MALWARE";
flow: to_server,established; content:"POST"; depth: 4; content:"srng/reg.php HTTP";
within: 50; content:"|0d0a|Host|3a|"; content:"2020search.com"; within: 40;
content:"IpAddr="; nocase; within: 100; classtype: trojan-activity; sid: 2000934; rev:5; )
```

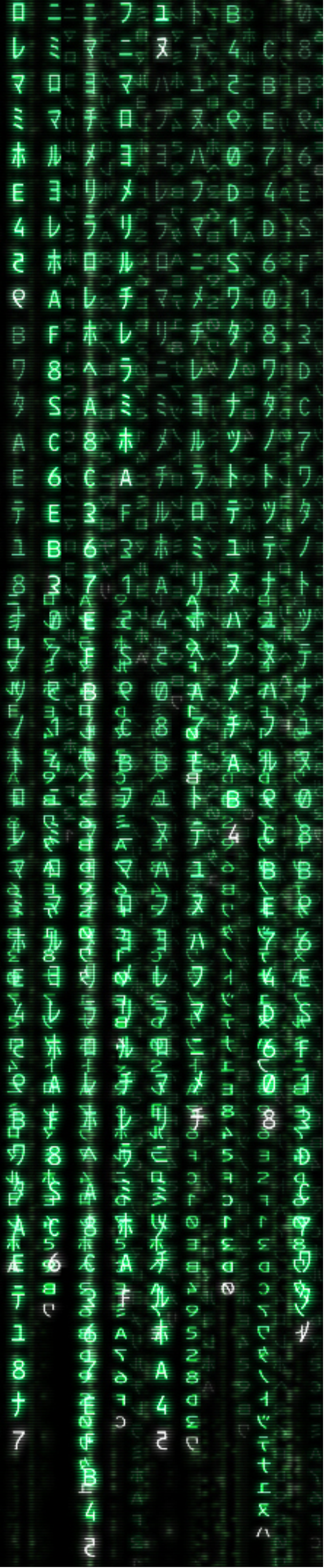
- Example of anomaly-based network intrusion detection system (PAYL)

```
GET /en/html/foo.php HTTP/1.1
User-Agent: Mozilla/5.0 Firefox/1.5.0.11
Host: www.example.com
Accept: text/xml,text/html;
Accept-Language: A{~!b@#9#0)(@>?
Accept-Encoding: gzip,deflate
Connection: keep-alive
Referrer: http://example.com
```



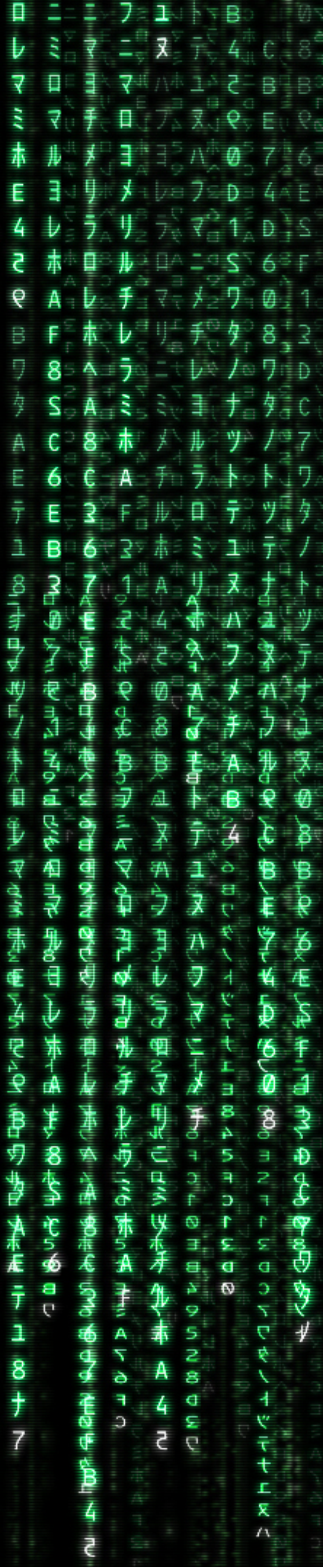
Vulnerability Discovery and Protection

- Automatically finding software bugs
- Automatic construction of vulnerability signatures from exploits
- Automatically building patches
- Patch-based exploit construction
- Improving OS Security (e.g., DEP, ASLR...)
- Sandboxing/Virtualization



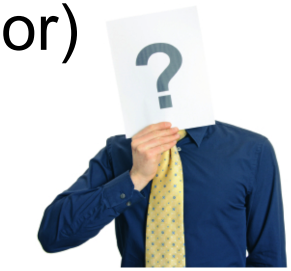
Web 2.0 Security

- Browser architecture/sandboxing
- Browser security policies
- Secure *mashups*
- Javascript security
  - static and dynamic analysis of code
  - e.g., automatic gadget security analysis



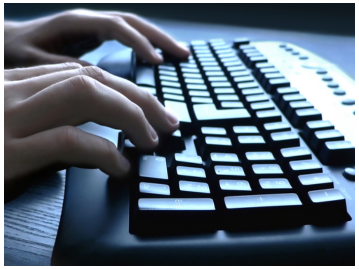
Privacy and Anonymity

- Information leakage in online social networks
- De-anonymizing public datasets
  - Netflix, Genomic Data, ...
- Attacking the confidentiality of encrypted communications
  - Inferring the language in VoIP conversations
  - Inferring content from HTTPS communications
- Communication (de-)anonymization
  - Mix networks
  - Improving/Attacking onion routing (e.g., Tor)
  - Traffic watermarking



Other topics

- Physical Security
  - Identifying keystrokes from audio
  - retrieving encryption keys from memory
  - seeing what other people are watching using reflections
- Wireless/Cellular Network Security
- RFID Security
- VoIP Security
- Cryptography/Crypto-analysis
- Electronic Voting Systems
- ... and many others ...



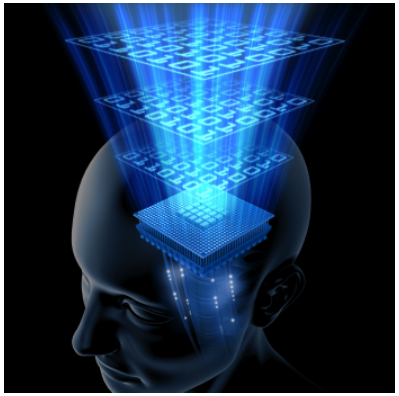
How do we choose a good research topic?

Think!

- What topics inspire you?
- Read as much as you can about them
- Not only academic papers
  - E.g.: interested in malware? Subscribe to malware/security blogs
    - SANS Internet Storm Center
    - Microsoft Malware Protection Center
    - Panda Research Blog
    - Krebs on Security
    - etc.
  - Stay up-to-date with real, current problems

Leverage you knowledge!

- Think about things you are very good at
  - System programming (C/C++, Assembly)?
  - System building?
  - Theory?
  - Algorithms?
  - Machine Learning, AI?



- While reading previous work, think about how your skills could help you solve an open problem

Problems that will likely grow big!

- Nobody can predict the future
- Look at what other people are working on
  - see what people at CMU, Berkeley, Stanford, GaTech, Wisconsin, UCSB, UIUC, etc., are doing
  - if a number of people are working in a particular (sub-)area, it must be of interested
  - try to see whether there is any emerging problem, with a *not too big* list of previous works
  - is there still something we can say about the topic, can we explore the problem from a new angle?
  - Depart from conventional thinking

Some topics are very hot!

- Malware Defense
  - current solutions are failing
  - detection is important
  - defense is even more important!
- Web Security
  - browsers are becoming a platform for applications
  - they are the most common Internet application
  - ... and they expose plenty of vulnerabilities!
- Cloud computing: is this the future?
  - security in the cloud
  - data privacy