



CSCI 4250/6250 – Fall 2011 Computer and Networks Security

Malware

Goodrich, Chapter 4

Viruses, Worms, Trojans, Rootkits

- ▶ **Malware** = *Malicious Software*
 - ▶ can be classified into several categories, depending on propagation and concealment
- ▶ **Propagation**
 - ▶ **Virus**: human-assisted propagation (e.g., open email attachment)
 - ▶ **Worm**: automatic propagation without human assistance
- ▶ **Concealment**
 - ▶ **Rootkit**: modifies operating system to hide its existence
 - ▶ **Trojan**: provides desirable functionality but hides malicious operation
- ▶ **Various types of payloads, ranging from annoyance to crime**

Insider Attacks

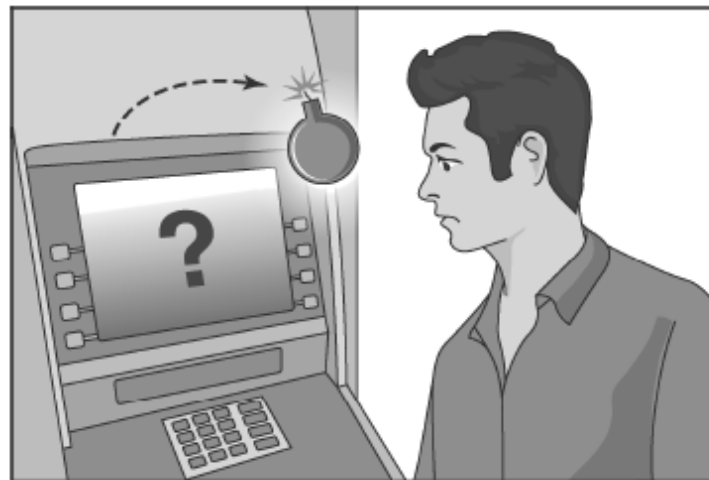
- ▶ An **insider attack** is a security breach that is caused or facilitated by someone who is a part of the very organization that controls or builds the asset that should be protected.
- ▶ In the case of malware, an insider attack refers to a security hole that is created in a software system by one of its programmers.

Backdoors

- ▶ A **backdoor**, which is also sometimes called a **trapdoor**, is a hidden feature or command in a program that allows a user to perform actions he or she would not normally be allowed to do.
- ▶ When used in a normal way, this program performs completely as expected and advertised.
- ▶ But if the hidden feature is activated, the program does something unexpected, often in violation of security policies, such as performing a privilege escalation.
- ▶ Benign example: **Easter Eggs** in DVDs and software

Logic Bombs

- ▶ A **logic bomb** is a program that performs a malicious action as a result of a certain logic condition.
- ▶ The classic example of a logic bomb is a programmer coding up the software for the payroll system who puts in code that makes the program crash should it ever process two consecutive payrolls without paying him.
- ▶ Another classic example combines a logic bomb with a backdoor, where a programmer puts in a logic bomb that will crash the program on a certain date.



The Omega Engineering Logic Bomb

- ▶ An example of a logic bomb that was actually triggered and caused damage is one that programmer Tim Lloyd was convicted of using on his former employer, Omega Engineering Corporation. On July 31, 1996, a logic bomb was triggered on the server for Omega Engineering's manufacturing operations, which ultimately cost the company millions of dollars in damages and led to it laying off many of its employees.

The Omega Bomb Code

- ▶ The Logic Behind the Omega Engineering Time Bomb included the following strings:
- ▶ **7/30/96**
 - ▶ Event that triggered the bomb
- ▶ **F:**
 - ▶ Focused attention to volume F, which had critical files
- ▶ **F:\LOGIN\LOGIN I2345**
 - ▶ Login a fictitious user, I2345 (the back door)
- ▶ **CD \PUBLIC**
 - ▶ Moves to the public folder of programs
- ▶ **FIX.EXE /Y F:*.***
 - ▶ Run a program, called FIX, which actually deletes everything
- ▶ **PURGE F:\ALL**
 - ▶ Prevent recovery of the deleted files

Defenses against Insider Attacks

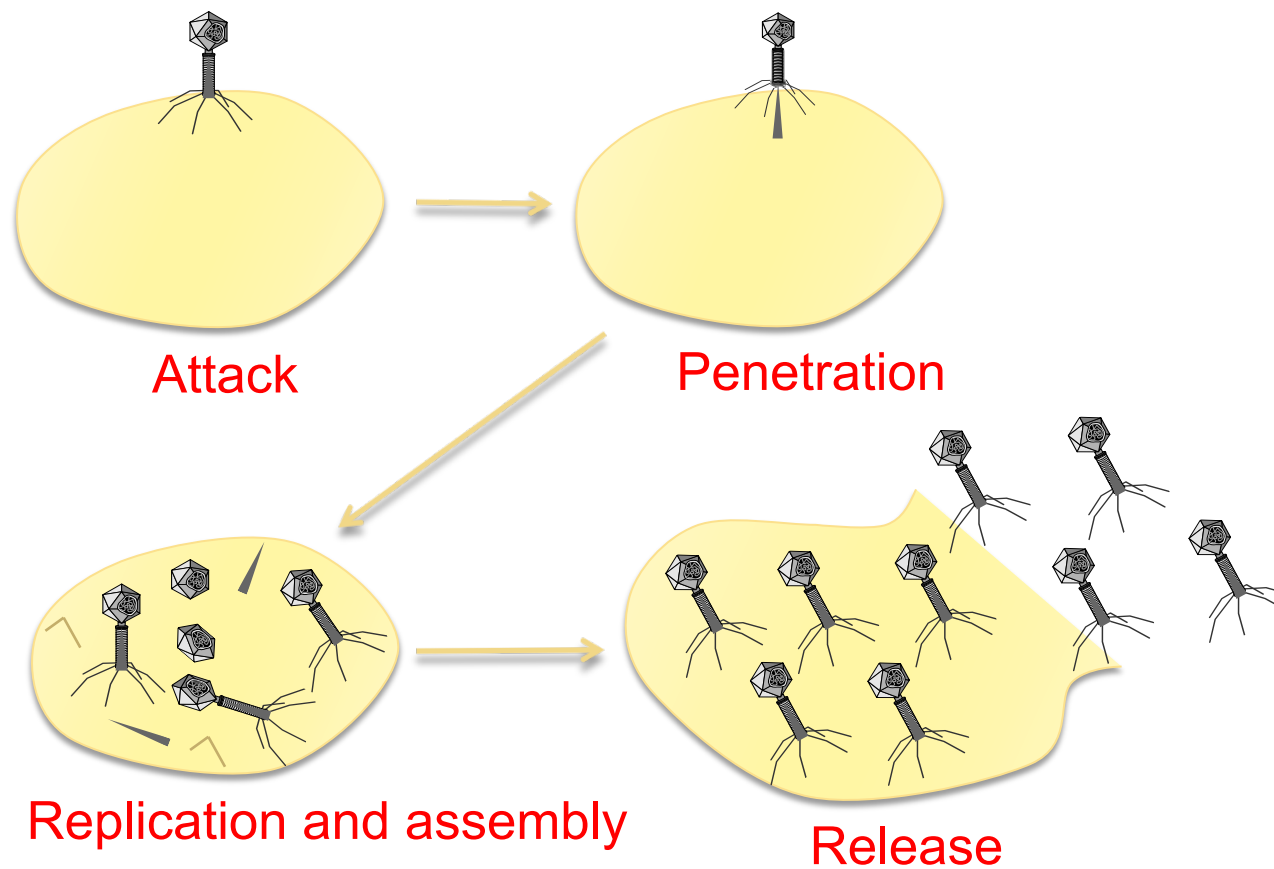
- ▶ Avoid single points of failure.
- ▶ Use code walk-throughs.
- ▶ Use archiving and reporting tools.
- ▶ Limit authority and permissions.
- ▶ Physically secure critical systems.
- ▶ Monitor employee behavior.
- ▶ Control software installations.

Computer Viruses

- ▶ A **computer virus** is computer code that can replicate itself by modifying other files or programs to insert code that is capable of further replication.
- ▶ This self-replication property is what distinguishes computer viruses from other kinds of malware, such as logic bombs.
- ▶ Another distinguishing property of a virus is that replication requires some type of **user assistance**, such as clicking on an email attachment or sharing a USB drive.

Biological Analogy

- ▶ Computer viruses share some properties with Biological viruses



Early History

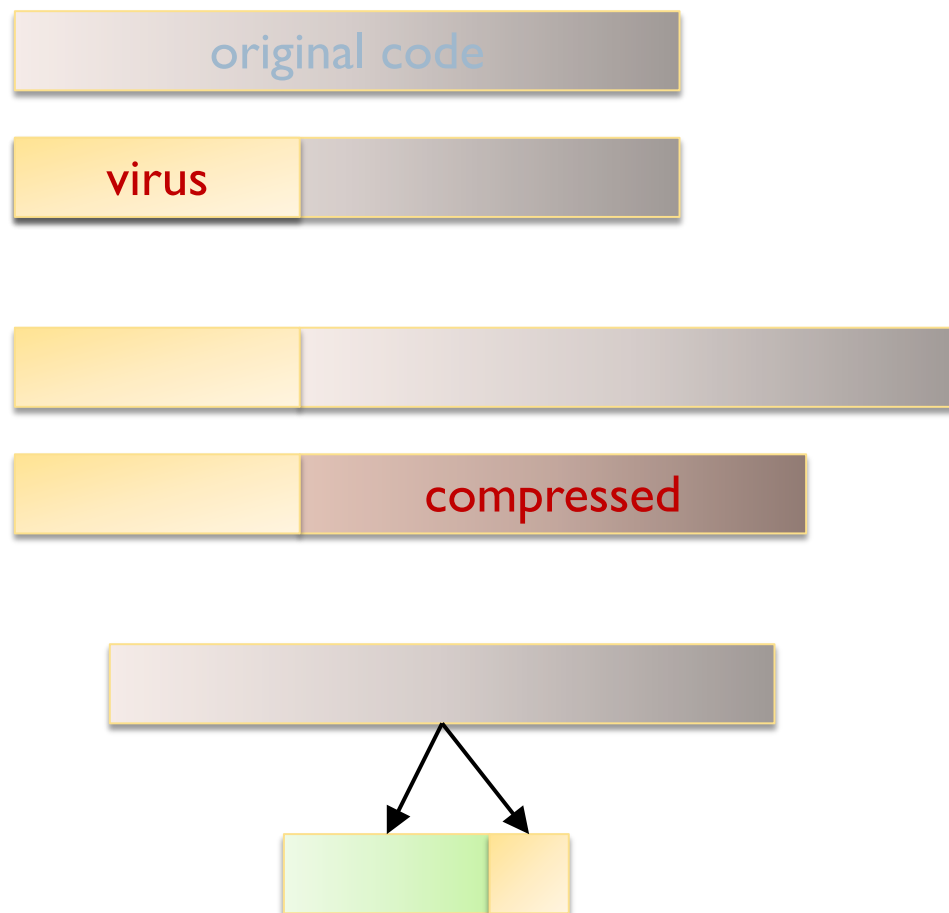
- 1972 sci-fi novel “When HARLIE Was One” features a program called VIRUS that reproduces itself
- First academic use of term virus by PhD student **Fred Cohen** in 1984, who credits advisor Len Adleman with coining it
- In 1982, high-school student Rich Skrenta wrote first virus released in the wild: Elk Cloner, a boot sector virus
- (c)Brain, by Basit and Amjood Farooq Alvi in 1986, credited with being the first virus to infect PCs

Virus Phases

- ▶ **Dormant phase.** During this phase, the virus just exists—the virus is laying low and avoiding detection.
- ▶ **Propagation phase.** During this phase, the virus is replicating itself, infecting new files on new systems.
- ▶ **Triggering phase.** In this phase, some logical condition causes the virus to move from a dormant or propagation phase to perform its intended action.
- ▶ **Action phase.** In this phase, the virus performs the malicious action that it was designed to perform, called **payload**.
 - ▶ This action could include something seemingly innocent, like displaying a silly picture on a computer's screen, or something quite malicious, such as deleting all essential files on the hard drive.

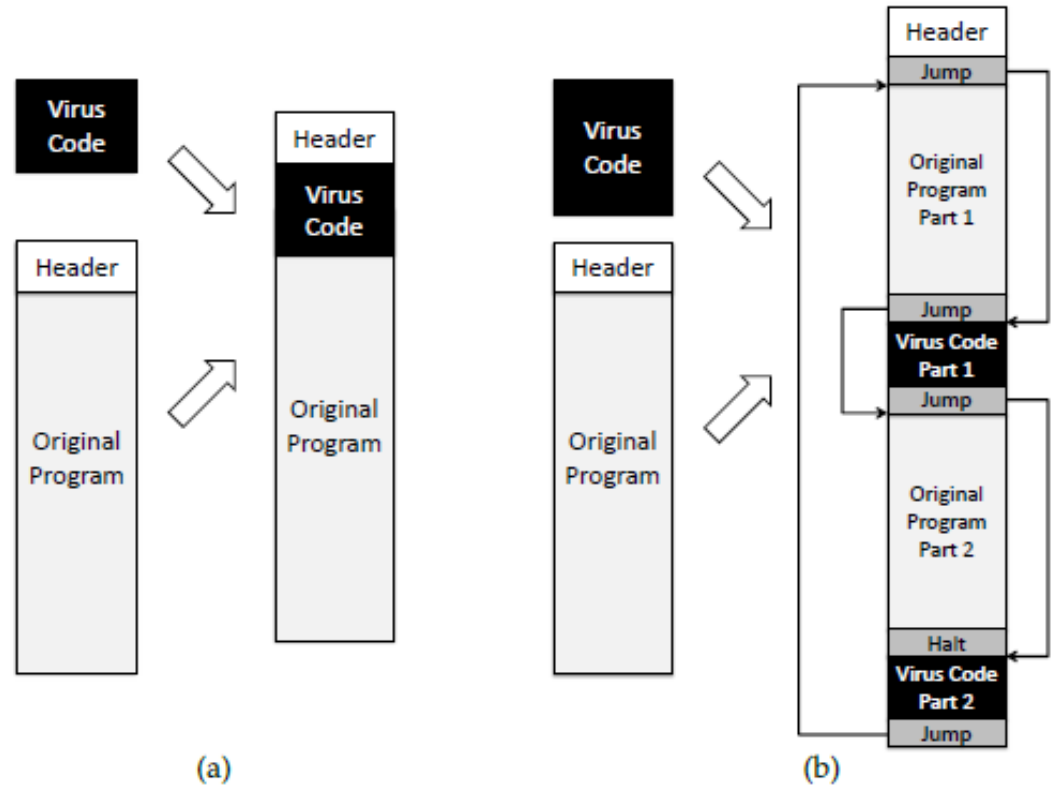
Infection Types

- ▶ **Overwriting**
 - ▶ Destroys original code
- ▶ **Pre-pending**
 - ▶ Keeps original code, possibly compressed
- ▶ **Infection of libraries**
 - ▶ Allows virus to be memory resident
 - ▶ E.g., kernel32.dll
- ▶ **Macro viruses**
 - ▶ Infects MS Office documents
 - ▶ Often installs in main document template



Degrees of Complication

- ▶ Viruses have various degrees of complication in how they can insert themselves in computer code.



Concealment

- ▶ **Encrypted virus**
 - ▶ Decryption engine + encrypted body
 - ▶ Randomly generate encryption key
 - ▶ Detection looks for decryption engine
- ▶ **Polymorphic virus**
 - ▶ Encrypted virus with random variations of the decryption engine (e.g., padding code)
 - ▶ Detection using CPU emulator
- ▶ **Metamorphic virus**
 - ▶ Different virus bodies
 - ▶ Approaches include code permutation and instruction replacement
 - ▶ Challenging to detect

Computer Worms

- ▶ A **computer worm** is a malware program that spreads copies of itself without the need to inject itself in other programs, and usually without human interaction.
- ▶ Thus, computer worms are technically not computer viruses (since they don't infect other programs), but some people nevertheless confuse the terms, since both spread by self-replication.
- ▶ In most cases, a computer worm will carry a malicious payload, such as deleting files or installing a backdoor.

Early History

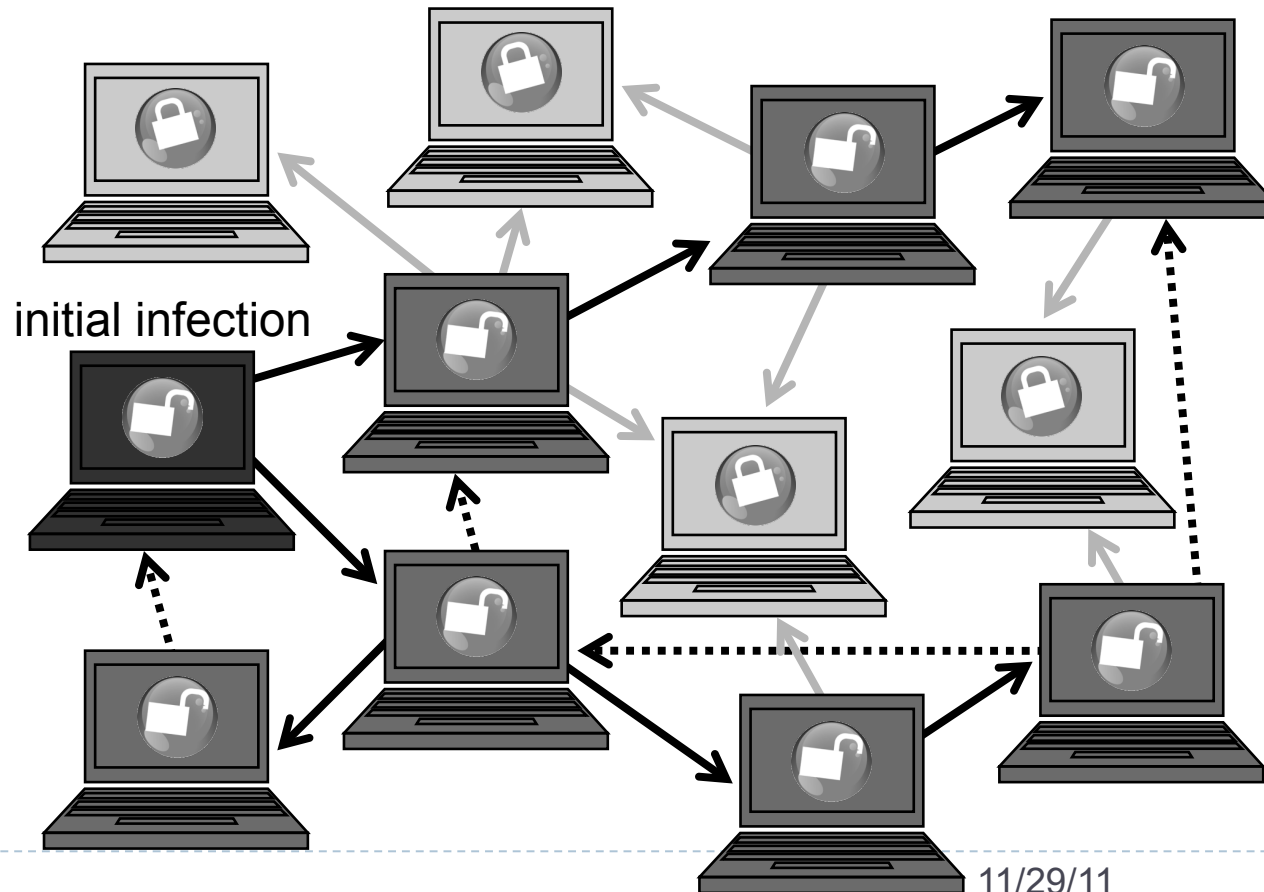
- First worms built in the labs of John Shock and Jon Hepps at Xerox PARC in the early 80s
- CHRISTMA EXEC written in REXX, released in December 1987, and targeting IBM VM/CMS systems was the first worm to use e-mail service
- The first *Internet worm* was the **Morris Worm**, written by Cornell student Robert Tappan Morris and released on November 2, 1988

Worm Development

- Identify vulnerability still unpatched
- Write code for
 - Exploit of vulnerability
 - Generation of target list
 - Random hosts on the internet
 - Hosts on LAN
 - Divide-and-conquer
 - Installation and execution of payload
 - Querying/reporting if a host is infected
- Initial deployment on botnet
- Worm template
 - Generate target list
 - For each host on target list
 - Check if infected
 - Check if vulnerable
 - Infect
 - Recur
- Distributed graph search algorithm
 - Forward edges: infection
 - Back edges: already infected or not vulnerable

Worm Propagation

- ▶ Worms propagate by finding and infecting vulnerable hosts.
 - ▶ They need a way to tell if a host is vulnerable
 - ▶ They need a way to tell if a host is already infected.



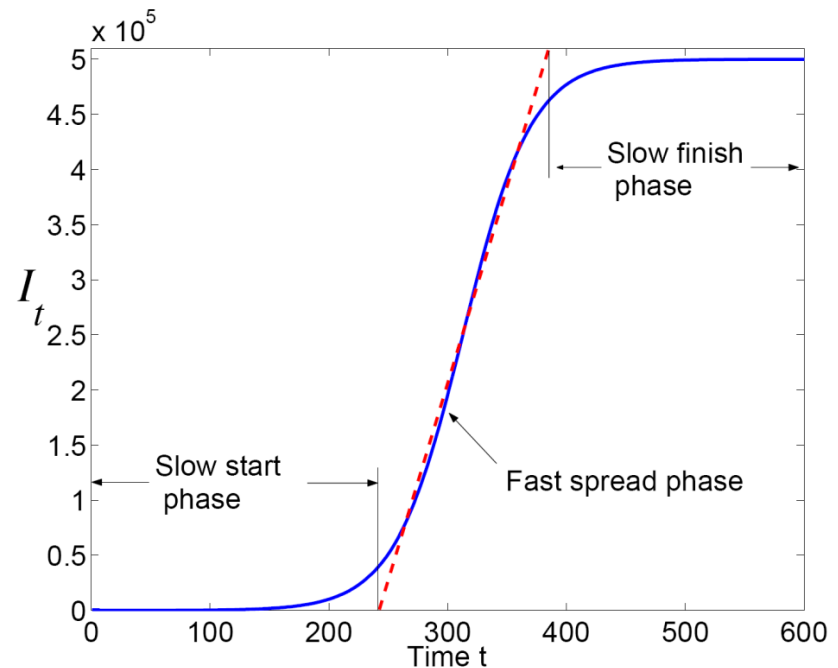
Propagation: Theory

- Classic epidemic model
 - ▶ N : total number of vulnerable hosts
 - ▶ $I(t)$: number of infected hosts at time t
 - ▶ $S(t)$: number of susceptible hosts at time t
 - ▶ $I(t) + S(t) = N$
 - ▶ β : infection rate
- Differential equation for $I(t)$:
$$dI/dt = \beta I(t) S(t)$$
- More accurate models adjust propagation rate over time

Source:

Cliff C. Zou, Weibo Gong, Don Towsley, and Lixin Gao.

[The Monitoring and Early Detection of Internet Worms](#), IEEE/ACM Transactions on Networking, 2005.



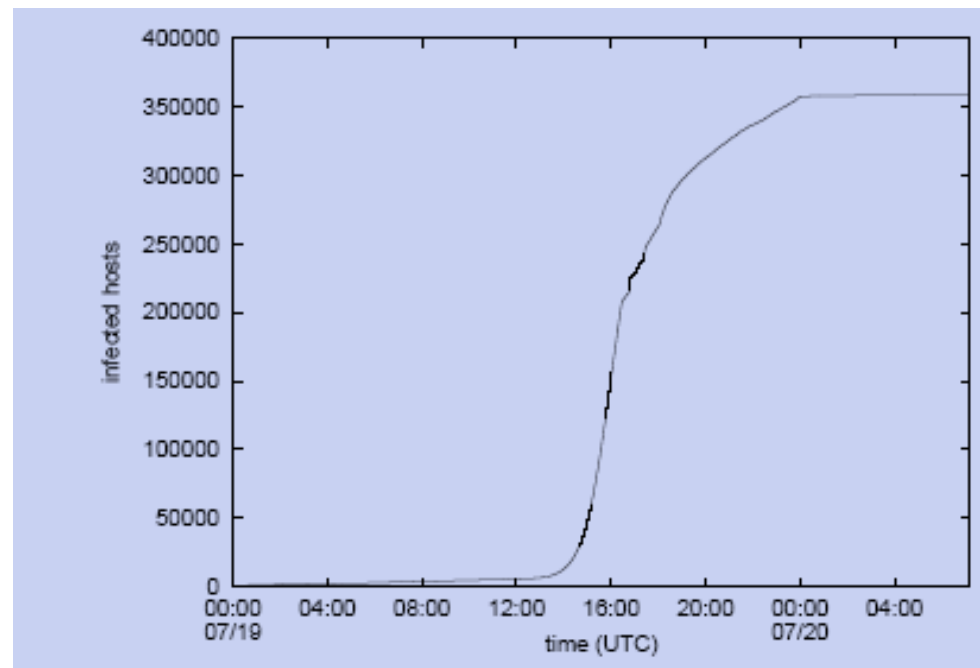
Propagation: Practice

- ▶ Cumulative total of unique IP addresses infected by the first outbreak of Code-Red v2 on July 19-20, 2001

Source:

David Moore, Colleen Shannon, and Jeffery Brown.

[Code-Red: a case study on the spread and victims of an Internet worm](#), CAIDA, 2002

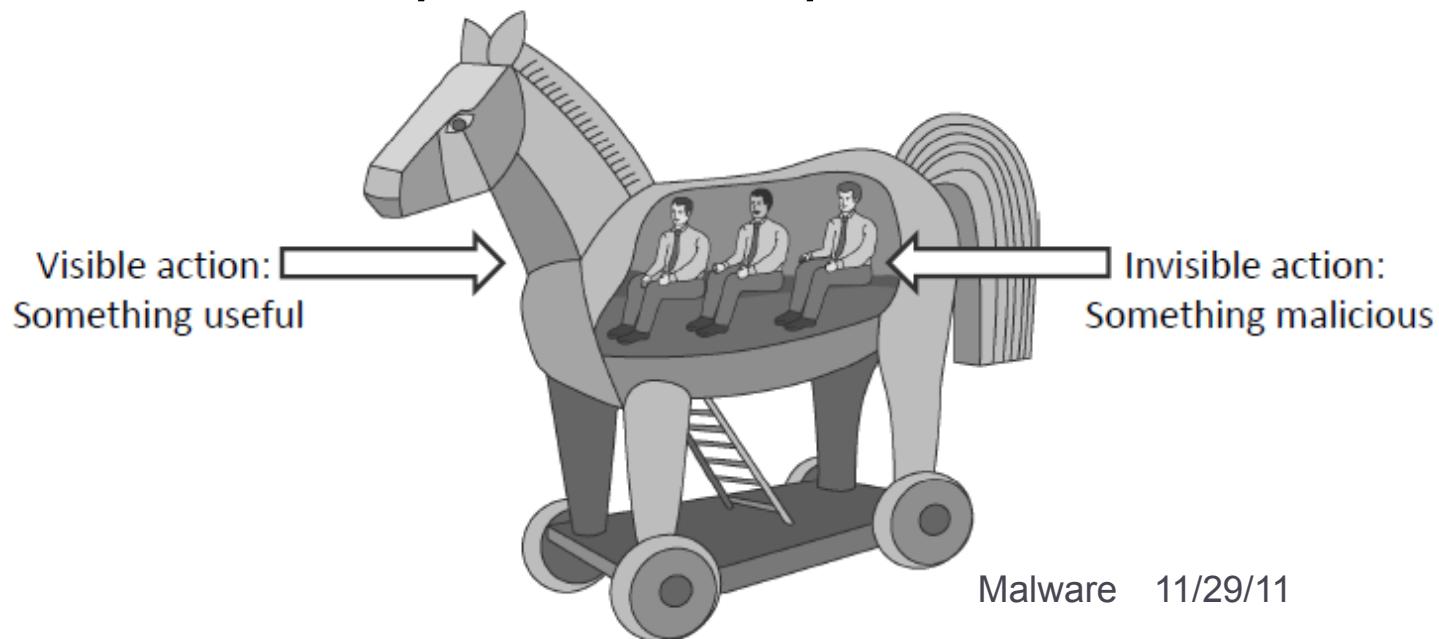


How to Own the Internet in Your Spare Time

<http://www.icir.org/vern/papers/cdc-usenix-sec02/>

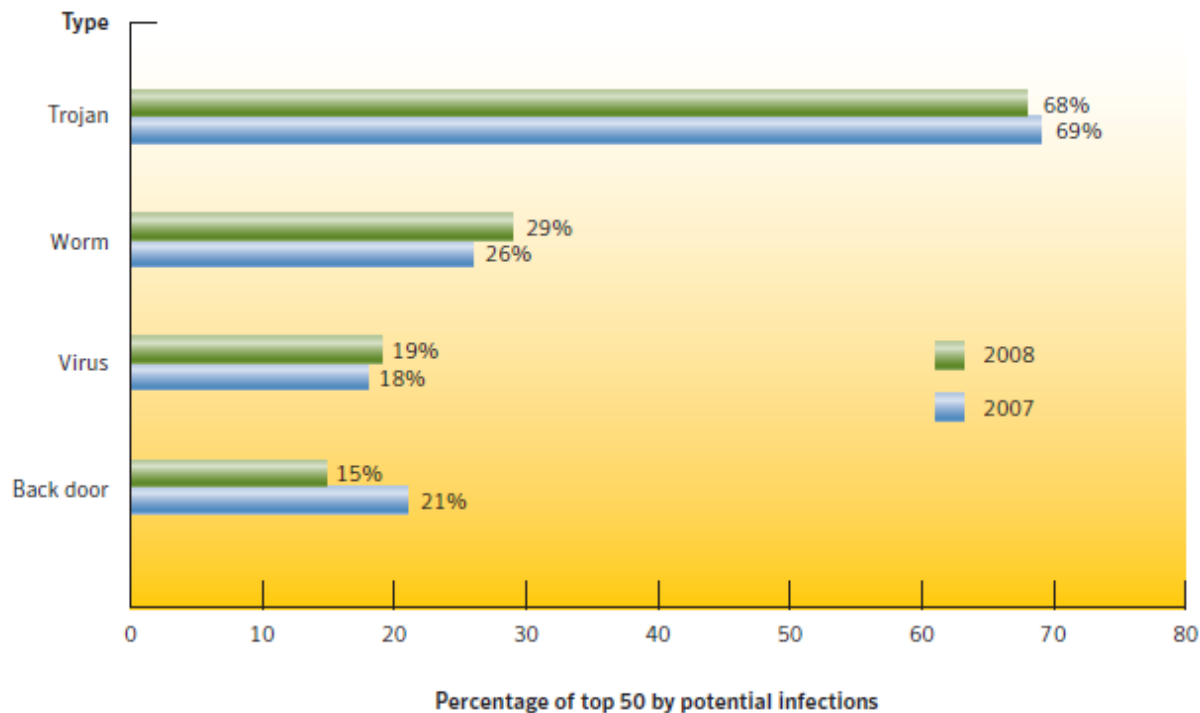
Trojan Horses

- ▶ A **Trojan horse (or Trojan)** is a malware program that appears to perform some useful task, but which also does something with negative consequences (e.g., launches a keylogger).
- ▶ Trojan horses can be installed as part of the payload of other malware but are often installed by a user or administrator, either deliberately or accidentally.



Current Trends

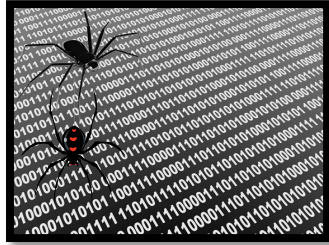
- ▶ Trojans currently have largest infection potential
 - ▶ Often exploit browser vulnerabilities
 - ▶ Typically used to download other malware in multi-stage attacks



Source:
Symantec Internet
Security Threat
Report, April 2009

Adware

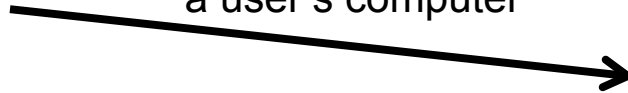
Adware software payload



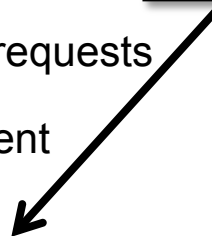
Computer user



Adware engine infects a user's computer



Adware engine requests advertisements from adware agent



Advertisers contract with adware agent for content



Advertisers



Adware agent

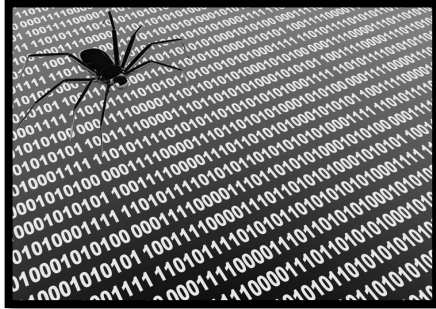


Adware agent delivers ad content to user



Spyware

Spyware software payload



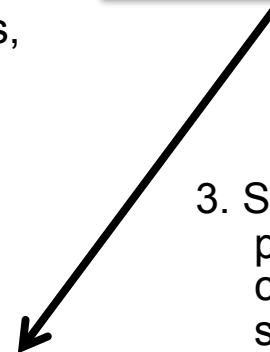
1. Spyware engine infects a user's computer.



Computer user



2. Spyware process collects keystrokes, passwords, and screen captures.



3. Spyware process periodically sends collected data to spyware data collection agent.

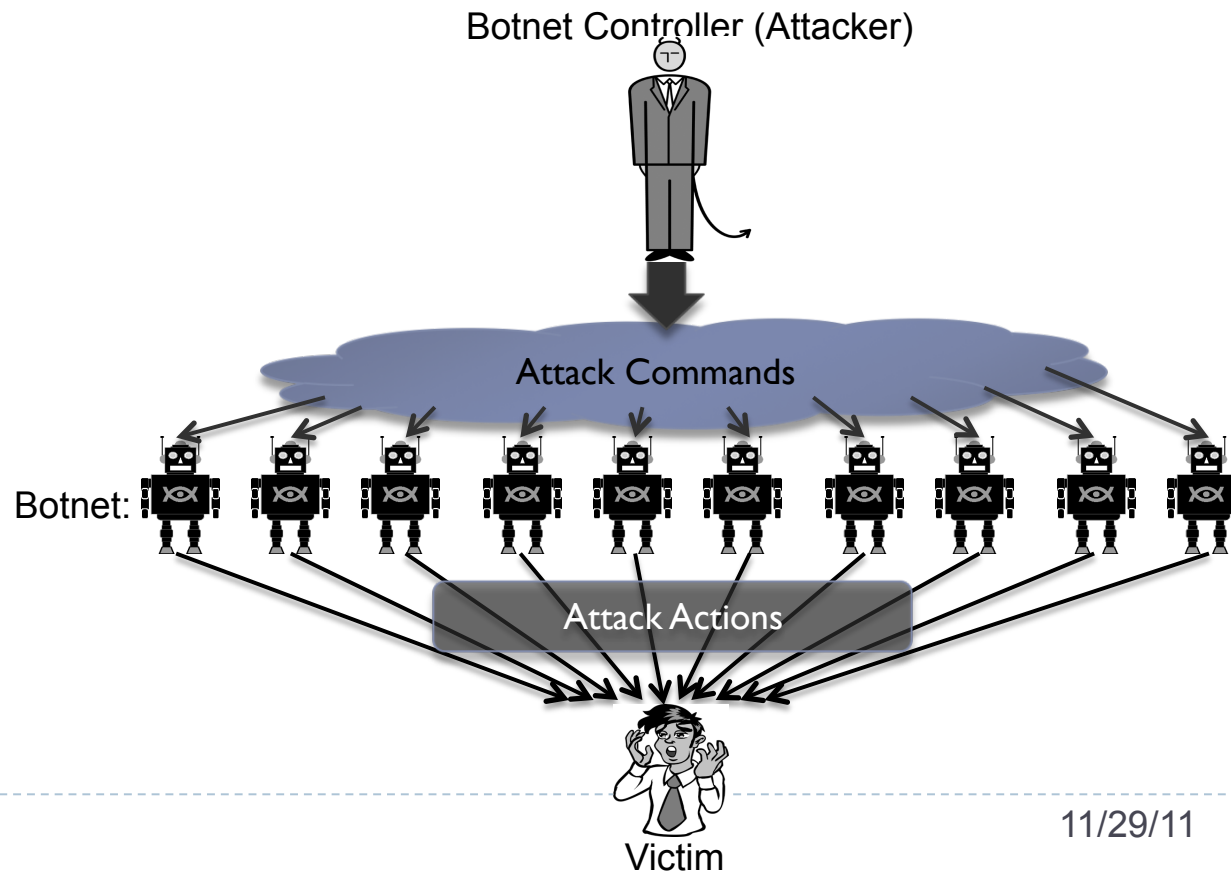
Spyware data collection agent

Rootkits

- A rootkit modifies the operating system to hide its existence
 - E.g., modifies file system exploration utilities
 - Hard to detect using software that relies on the OS itself
- RootkitRevealer
 - By Bryce Cogswell and Mark Russinovich (Sysinternals)
 - Two scans of file system
 - High-level scan using the Windows API
 - Raw scan using disk access methods
 - Discrepancy reveals presence of rootkit
 - Could be defeated by rootkit that intercepts and modifies results of raw scan operations

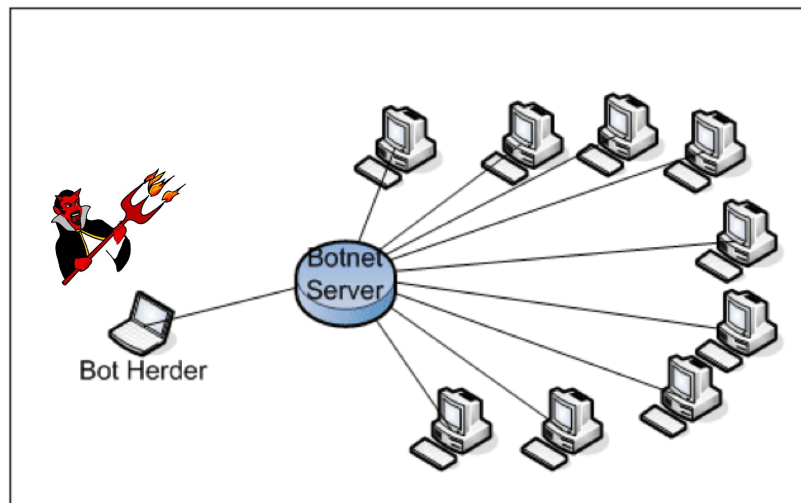
Botnets

- ▶ Malware can turn a computer in to a **bot** (or zombie), which is a machine that is controlled externally to perform malicious attacks, usually as a part of a **botnet**.



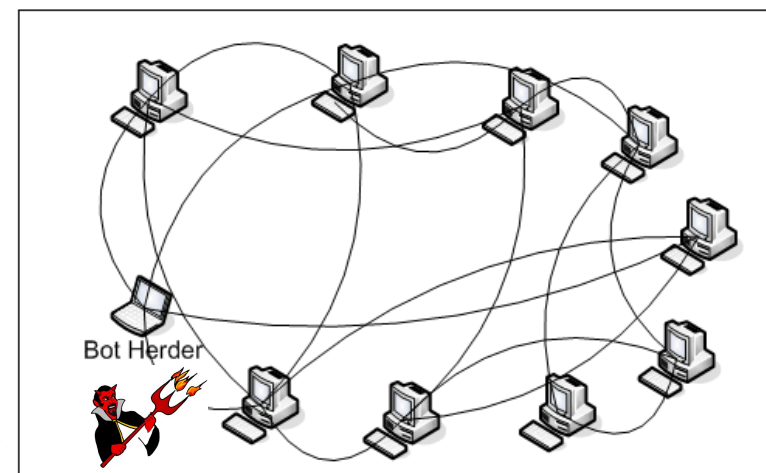
Botnets

- ▶ Groups of bot-compromised machines
 - ▶ Keep in touch with attacker via C&C
 - ▶ Respond to attacker's command in a coordinated way



Centralized

P2P Botnet



Scareware (Fake Avs)

The screenshot shows a Windows Security alert window titled "Scan results" with a red header: "Windows has detected serious threats to your security". The alert text states: "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."

Threat Name	Count	Severity	Description
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

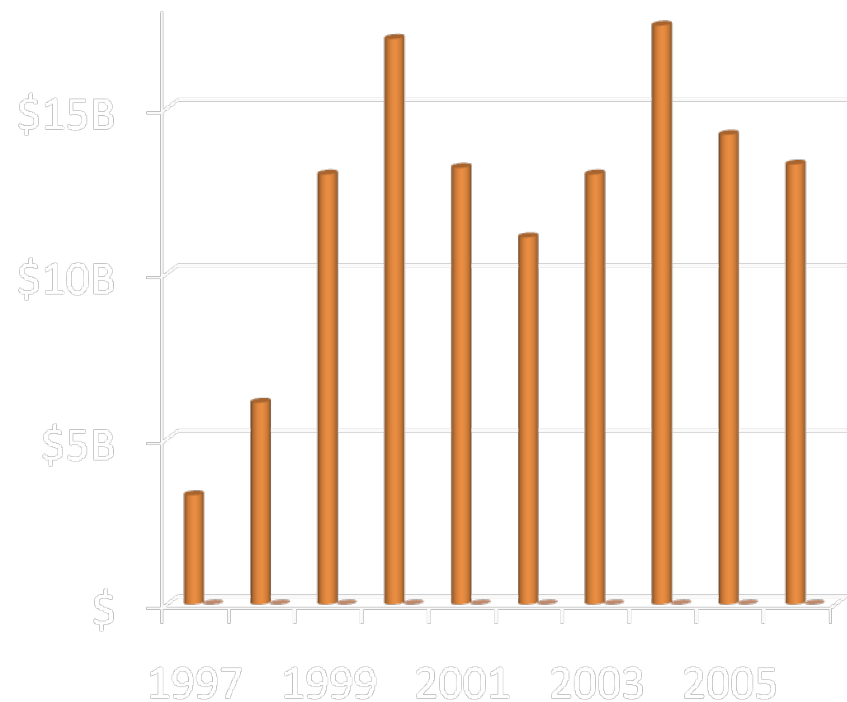
Below the table, it says: "Windows highly recommends you to remove all dangerous threats. Staying unprotected may lead to unprecedented consequences, including complete crash of your PC and operating system."

Overlaid on the alert is a JavaScript warning dialog box titled "JavaScript" from "<ktsoft.eu>". The dialog contains a yellow warning triangle icon and the text: "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". There is a checkbox for "Stop executing scripts on this page" and an "OK" button.

Financial Impact

- Malware often affects a large user population
- Significant financial impact, though estimates vary widely, up to \$100B per year (mi2g)
- Examples
 - LoveBug (2000) caused \$8.75B in damages and shut down the British parliament
 - In 2004, 8% of emails infected by W32/MyDoom.A at its peak
 - In February 2006, the Russian Stock Exchange was taken down by a virus.

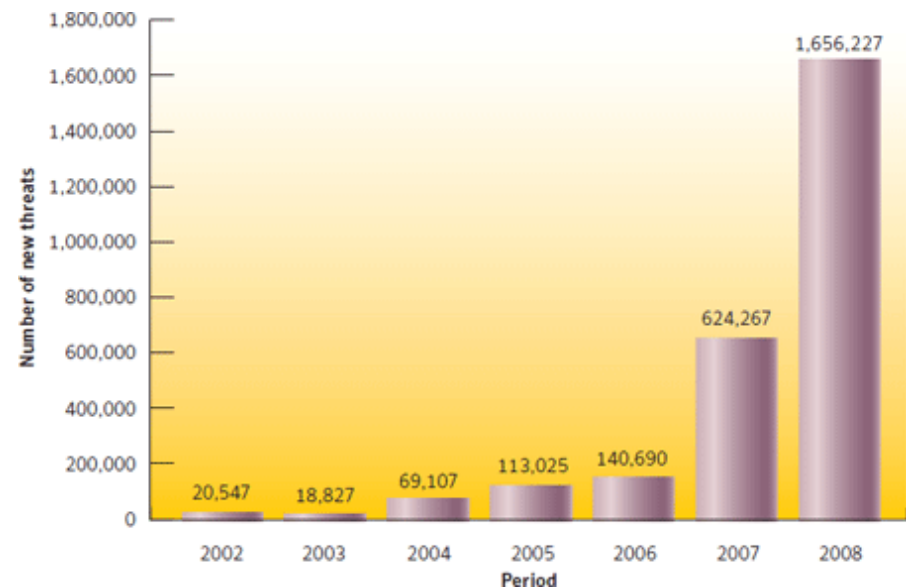
Source: Computer Economics



Economics of Malware

- ▶ New malware threats have grown from 20K to 1.7M in the period 2002-2008
- ▶ Most of the growth has been from 2006 to 2008
- ▶ Number of new threats per year appears to be growing an exponential rate.

Source:
[Symantec Internet Security Threat Report](#), April 2009



Professional Malware

- ▶ Growth in professional cybercrime and online fraud has led to demand for professionally developed malware
- ▶ New malware is often a custom-designed variations of known exploits, so the malware designer can sell different “products” to his/her customers.
- ▶ Like every product, professional malware is subject to the laws of supply and demand.
 - ▶ Recent studies put the price of a software keystroke logger at \$23 and a botnet use at \$225.

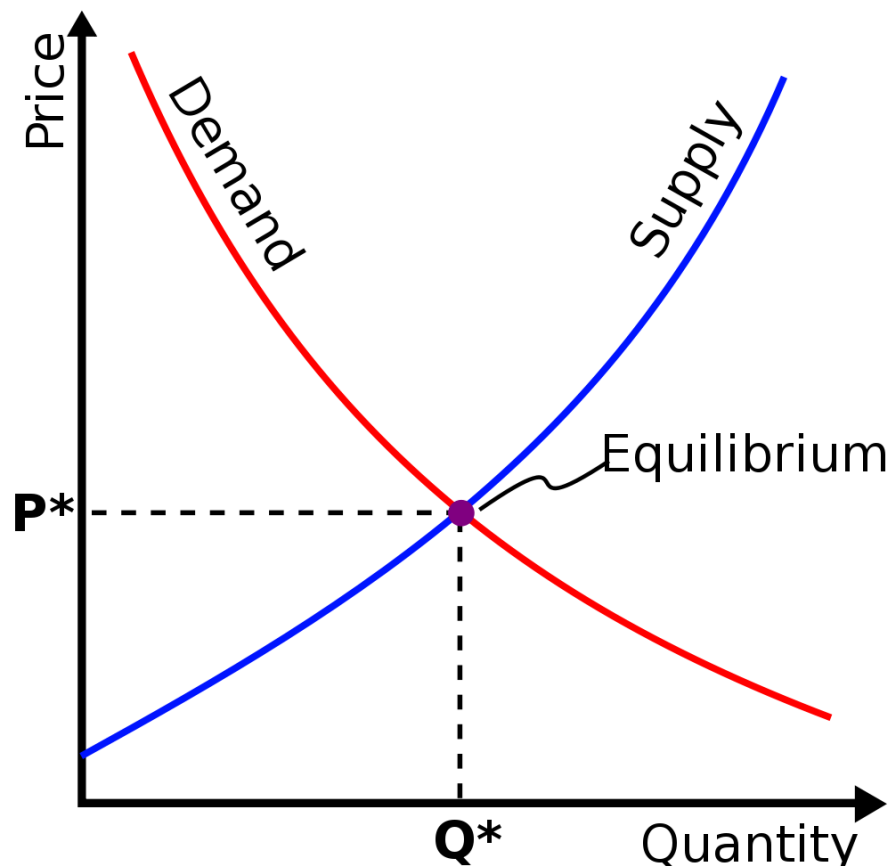


Image by User:SilverStar from <http://commons.wikimedia.org/wiki/File:Supply-demand-equilibrium.svg> used by permission under the *Creative Commons Attribution ShareAlike 3.0 License*

DIY Malware

The image shows the TURKOJAN 4 client interface and its configuration window. The client window has a title bar with "[Aktif PC :deneme]", "Turkojan Client v4.0", and "[Online : 0]". The main window features a header with "Alien Technology" and "TURKOJAN 4" in a stylized font. Below the header is a menu bar with "English", "Editor", "Settings", "About", "Order", and "Port : 15963". A sidebar on the left lists various tools like "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", and "local tools". The main area displays "TURKOJAN v.4" with a 3D alien head icon and the text "TURKOJAN Copyright CigiCigi Online 1997 - 2008 All rights reserved. Made in Turkey". At the bottom, a table shows connection details for a host named "deneme".

Connection ID :	IP Address :	Computer Name :	OS :
deneme	85.109.45.170/192.168.159.130	DEG-B54DA9656F2	WinXP

The "Server Editor" window is overlaid on the client. It contains the following settings:

- DNS - IP (Yours) Address: example.no.ip.biz
- Port No: 15963
- Connection Delay: 2 sec. for connection
- User Name: random
- Copy server to PC
- File Name: mstwain32.exe
- Autostart server
- Registry Name: mstwain32
- Show Message
- Mesaj Title: Bilgi
- Message: Server basariyla kuruldu!
- Mesaj Icon: [Triangle icon]
- Running mode: Help mode (visible), Stealth mode (invisible)
- Icon: [Default icon], [Icon Hunter], [Select Icon]
- Pack server via using UPX v.3.02 [smaller server]
- Progress: 0%
- Save button

At the bottom of the client window, the status bar shows "Ready" and "Status : Passive".

Botnets for sale...

host	count	[controls]
74.63.218.186	81	🔴🔴
apis.videosurf.com	9	🔴🔴
66.218.161.133	6	🔴🔴
safebrowsing.clients.google.com	4	🔴🔴
ocsp.verisign.com	4	🔴🔴
login.hi5.com	4	🔴🔴
baymsg1010711.by2.gateway.edge.messenger.live.com	4	🔴🔴
ocsp.thawte.com	3	🔴🔴
ocsp.comodoca.com	2	🔴🔴
es-ve.hi5.com	2	🔴🔴
foro.mitragus.org	2	🔴🔴
ocsp.godaddy.com	1	🔴🔴
bancolombia.olb.todo1.com	1	🔴🔴
asterixworld.net	1	🔴🔴

I sell Spy Eye Botnet - Acnaz -
22-09-2010 10:37 PM

Hello everybody!
I sell a Spy Eye botnet for 120\$

Please contact me, that we talk over the details.

My Windows Live Messenger:
minigun122@windowslive.com

The SpyEye toolkit is similar to Zeus in a lot of ways. It contains a builder module for creating the Trojan bot executable with config file and a Web control panel for command and control (C&C) of a bot net. Some of the advertised features online are:

- Formgrabber (Keylogger)
- Autofill credit card modules
- Daily email backup
- Encrypted config file
- Ftp protocol grabber
- Pop3 grabber
- Http basic access authorization grabber
- Zeus killer

Signatures:

A Malware Countermeasure

- Scan compare the analyzed object with a database of signatures
- A **signature** is a virus fingerprint
 - E.g., a string with a sequence of instructions specific for each virus
 - Different from a digital signature
- A file is infected if there is a signature inside its code
 - Fast **pattern matching** techniques to search for signatures
- All the signatures together create the malware database that usually is proprietary

White/Black Listing

- ▶ Maintain database of cryptographic hashes for
 - ▶ Operating system files
 - ▶ Popular applications
 - ▶ Known infected files
- ▶ Compute hash of each file
- ▶ Look up into database
- ▶ Needs to protect the integrity of the database

Heuristic Analysis

- Useful to identify new and “zero day” malware
- Code analysis
 - Based on the instructions, the antivirus can determine whether or not the program is malicious, i.e., program contains instruction to delete system files,
- Execution emulation
 - Run code in isolated emulation environment
 - Monitor actions that target file takes
 - If the actions are harmful, mark as virus
- Heuristic methods can trigger false alarms

Shield vs. On-demand

▶ Shield

- ▶ Background process (service/daemon)
- ▶ Scans each time a file is touched (open, copy, execute, etc.)

● On-demand

- Scan on explicit user request or according to regular schedule
- On a suspicious file, directory, drive, etc.

Performance test of scan techniques

- **Comparative**: check the number of already known viruses that are found and the time to perform the scan
- **Retrospective**: test the proactive detection of the scanner for unknown viruses, to verify which vendor uses better heuristics

Anti-viruses are ranked using both parameters:

<http://www.av-comparatives.org/>

Online vs Offline Anti Virus Software

Online

- Free browser plug-in
- Authentication through third party certificate (i.e. VeriSign)
- No shielding
- Software and signatures update at each scan
- Poorly configurable
- Scan needs internet connection
- Report collected by the company that offers the service

Offline

- Paid annual subscription
- Installed on the OS
- Software distributed securely by the vendor online or a retailer
- System shielding
- Scheduled software and signatures updates
- Easily configurable
- Scan without internet connection
- Report collected locally and may be sent to vendor

Quarantine

- A suspicious file can be isolated in a folder called **quarantine**:
 - E.g., if the result of the heuristic analysis is positive and you are waiting for db signatures update
- The suspicious file is not deleted but made harmless: the user can decide when to remove it or eventually restore for a false positive
 - Interacting with a file in quarantine it is possible only through the antivirus program
- The file in quarantine is harmless because it is encrypted
- Usually the quarantine technique is proprietary and the details are kept secret

Static vs. Dynamic Analysis

Static Analysis

- Checks the code without trying to execute it
- Quick scan in white list
- Filtering: scan with different antivirus and check if they return same result with different name
- Weeding: remove the correct part of files as junk to better identify the virus
- Code analysis: check binary code to understand if it is an executable, e.g., PE
- Disassembling: check if the byte code shows something unusual

Dynamic Analysis

- Check the execution of codes inside a virtual sandbox
- **Monitor**
 - File changes
 - Registry changes
 - Processes and threads
 - Networks ports

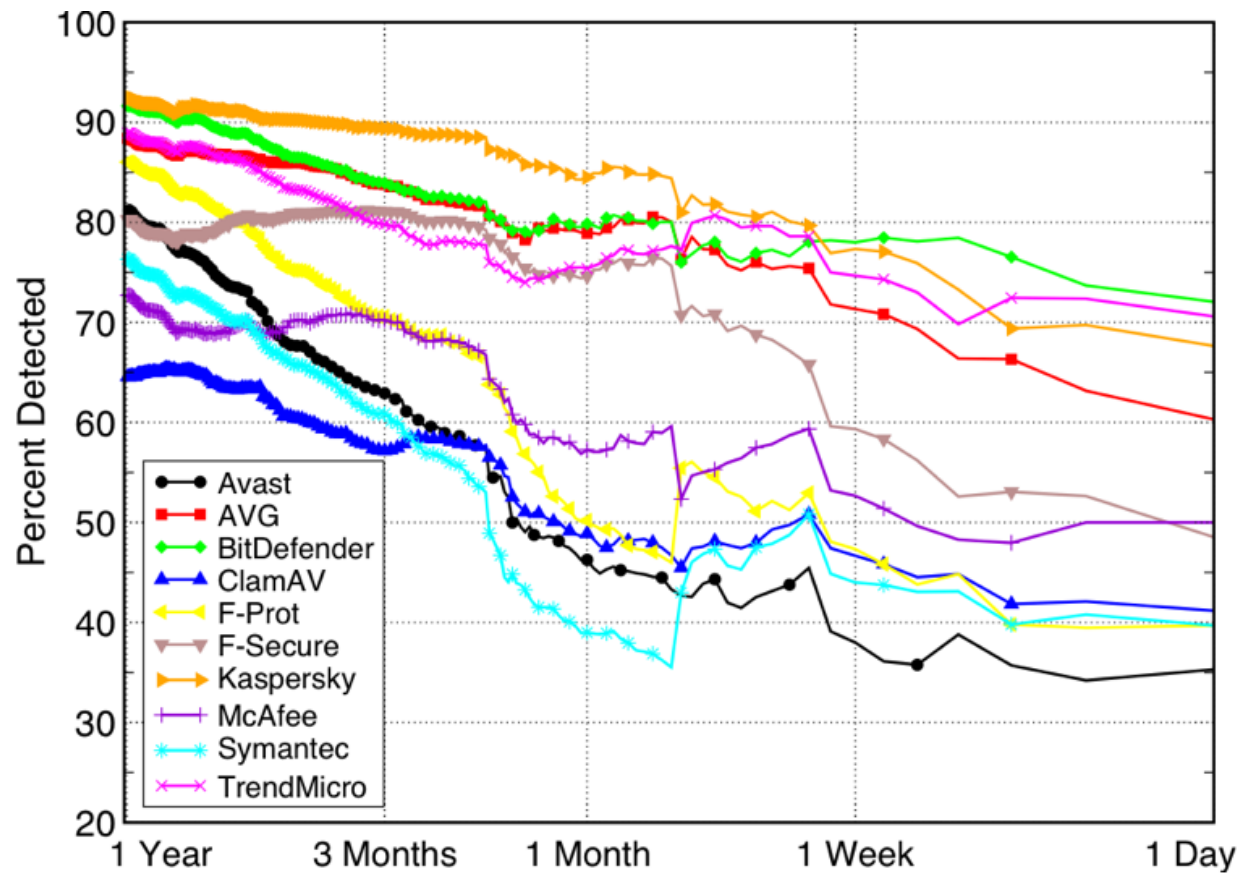
Malware Detection is Undecidable

- ▶ Theoretical result by Fred Cohen (1987)
- ▶ Virus abstractly modeled as program that eventually executes **infect**
- ▶ Code for **infect** may be generated at runtime
- ▶ Proof by contradiction similar to that of the halting problem
- ▶ Suppose program **isVirus** (P) determines whether program P is a virus
- ▶ Define new program Q as follows:
 - if (not **isVirus**(Q))
 - infect**
 - stop
- ▶ Running **isVirus** on Q achieves a contradiction

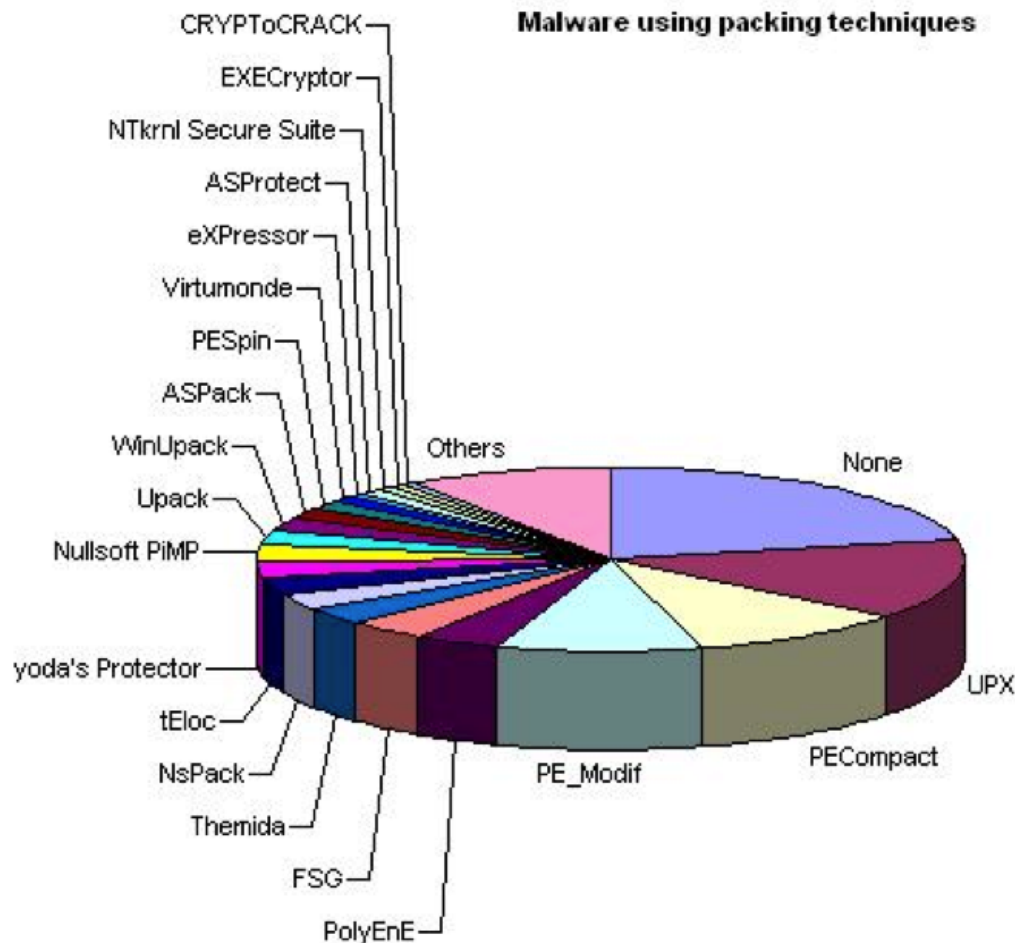
Other Undecidable Detection Problems

- **Detection of a virus**
 - by its appearance
 - by its behavior
- **Detection of an evolution of a known virus**
- **Detection of a triggering mechanism**
 - by its appearance
 - by its behavior
- **Detection of a virus detector**
 - by its appearance
 - by its behavior
- **Detection of an evolution of**
 - a known virus
 - a known triggering mechanism
 - a virus detector

AV tools do not work well



Packers and Cryptors



2K9 www.RDGSoft.Bk.com X

RDG T EJON v0.6 crypter

Private Version

<input checked="" type="checkbox"/> Anti-Debugger	<input checked="" type="checkbox"/> Anti-Anubis
<input checked="" type="checkbox"/> Anti-SandBoxie	<input checked="" type="checkbox"/> DEP - Stolen Bytes
<input checked="" type="checkbox"/> Anti-Virtual PC	<input type="checkbox"/> Checksum-CRC
<input checked="" type="checkbox"/> ReAlign Sections	<input checked="" type="checkbox"/> Anti-DillyDbg
<input checked="" type="checkbox"/> Anti-IDA Debugger	<input checked="" type="checkbox"/> Anti-ThreatExpert
<input checked="" type="checkbox"/> Anti-CWSandbox	<input checked="" type="checkbox"/> Anti-JoeBox
<input checked="" type="checkbox"/> Anti-Norman Sandbox	<input checked="" type="checkbox"/> Anti-VMWare
<input checked="" type="checkbox"/> Anti-VirtualBox	<input checked="" type="checkbox"/> Anti-Debugger 2
<input checked="" type="checkbox"/> Anti-Virtual Machine (Max)	<input type="checkbox"/> + RDG Poly Pack
<input checked="" type="checkbox"/> Anti-SunBelt SandBox	<input checked="" type="checkbox"/> Anti-Deep Freeze
<input checked="" type="checkbox"/> Sleep Sec. <input type="text" value="0"/>	<input checked="" type="checkbox"/> Anti-Returnil V.S
<input checked="" type="checkbox"/> Exceptions N# <input type="text" value="100"/>	<input checked="" type="checkbox"/> Anti-Mal Defender
<input checked="" type="checkbox"/> Get All Privileges	<input checked="" type="checkbox"/> Anti-Wine (Linux)
<input type="checkbox"/> Password protect	<input checked="" type="checkbox"/> Anti-Xen VM
<input type="checkbox"/> Execute w/ Command Line	<input checked="" type="checkbox"/> UnHook All Api
<input type="checkbox"/> Change File Properties	<input checked="" type="checkbox"/> Anti-Attach (Loader)
<input type="checkbox"/> Change Icon	<input checked="" type="checkbox"/> Execute as SYSTEM

Open File **Protect** ?

Resources

- ▶ **Computer Emergency Response Team**
 - ▶ Research center funded by the US federal government
 - ▶ Vulnerabilities database
- ▶ **Symantec**
 - ▶ Reports on malware trends
 - ▶ Database of malware
- ▶ **Art of Computer Virus Research and Defense by Peter Szor**