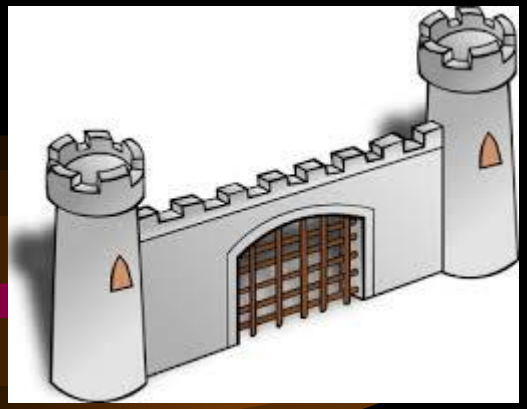
InfoComm Security fundamentals

Topic 2
Client Security
(Malware)

Objectives

- Identify different kinds of malware
- List different client side attacks
- Securing with Anti-Malware Software
- Describe the types of social engineering attacks

Operational Security



- For many years …

protection = **prevention**

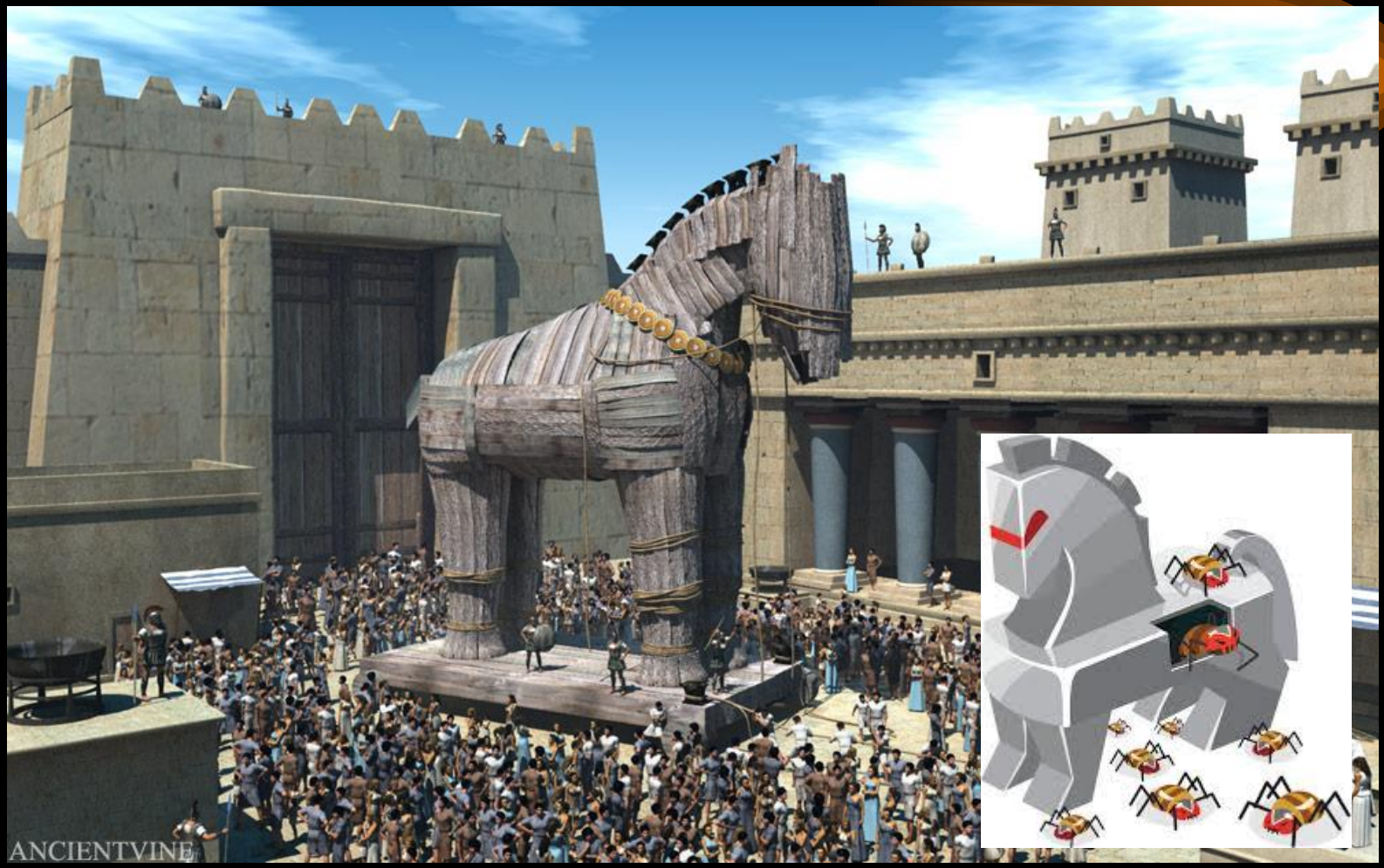
- Regardless of how well people seem to do in prevention technology, somebody always seems to find a way around safeguards.

- Therefore, **multiple prevention** techniques and technology are required to alert when prevention has failed and to provide ways to address the problem.

How to attack this castle?

- By the front
- Infiltration
- Attack from Inside

A trojanhorse



Operational Model of Computer Security

- The **operational model** of computer security includes two additions to the original security equation:

Protection = Prevention + (Detection + Response)

- Every security technique and technology falls into at least one of the three elements of the equation.

Operational Model of Computer Security

Protection = Prevention + (Detection + Response)

- Access controls
- Firewalls
- Encryption

- Audit logs
- Intrusion detection systems
- Honeypots

- Backups
- Incident Response Teams
- Computer Forensics

Attacks Using Malware

- Malicious software (malware)
  - Refers to a wide variety of damaging or annoying software
  - Enters a computer system without the owner's knowledge or consent

Virus

- computer code that attached to files;
- relies on user action to spread; and
- cannot be remote control.

- Types of computer viruses
  - Program: Infects executable files e.g. (.exe and .com)
  - Macro: Executes a script (e.g. VBA in .doc)
  - Resident: Virus infects files opened by user or operating system
  - Boot virus: Infects the Master Boot Record of a hard disk
  - Companion virus: A copycat version of a legitimate program, e.g. NOTEPAD.COM

Worm

- Exploits application or operating system vulnerability
- Uses the network to travel from one computer to another. No user action needed
- Allows remote control of a computer by an attacker

I Love You

- Macro Worm released on 5 May 2000
- 50 million infections within a week
- Mail attachment with a file
  Love-Letter-For-You.TXT.vbs
- a VBScript program that, when opened, finds the recipient's Outlook address book and re-sends the note to everyone in it. It then overwrites (and thus destroys) all files of the following file types: JPEG, MP3, VPOS, JS, JSE, CSS, WSH, SCT and HTA.

Virus versus Worm

Action	Virus	Worm
How does it spread to other computers?	Because viruses are attached to files, it is spread by a user transferring those files to other devices	Worms use a network to travel from one computer to another
How does it infect?	Viruses insert their code into a file	Worms exploit vulnerabilities in an application or operating system
Does there need to be user action?	Yes	No
Can it be remote controlled?	No	Yes

Difference between viruses and worms

SPYWARE

- Spyware refers to programs that use your Internet connection to send information from your personal computer to some other computer, normally without your knowledge or permission.

- This information is a record of your ongoing browsing habits, downloads, or it could be more personal data like your name and address.

Spyware Effects and Behaviors

- A spyware infestation can create significant unwanted CPU activity, disk usage, and network traffic.
- Stability issues, such as applications freezing, failure to boot, and system-wide crashes, are also common.
- Spyware, which interferes with networking software commonly causes difficulty connecting to the Internet.

Types of Spyware

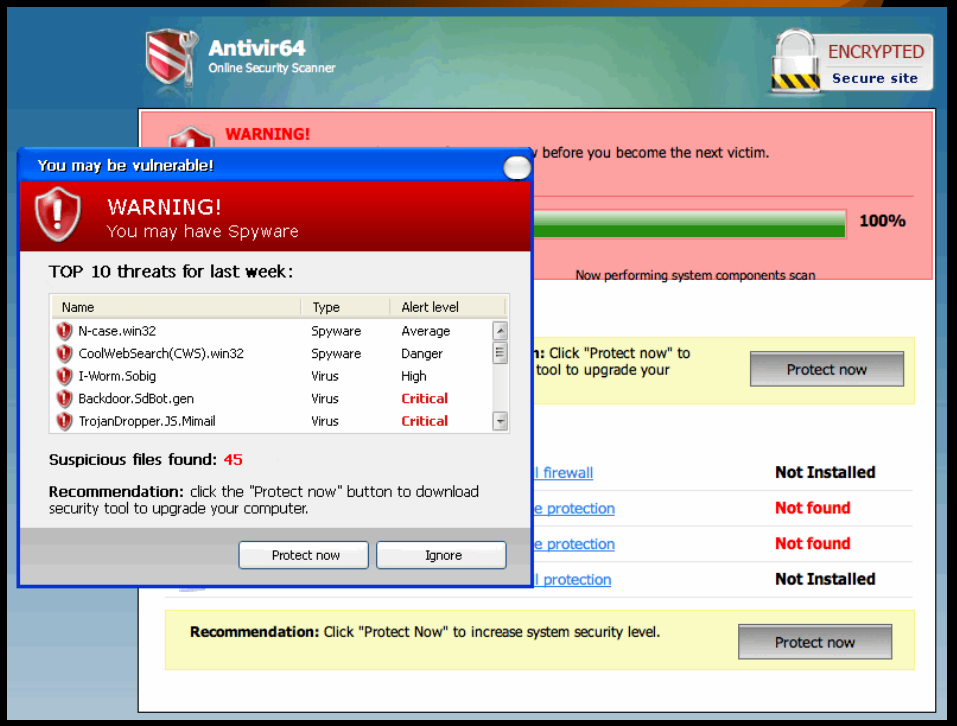
- Some types of spyware disable software firewalls and anti-virus software, and/or reduce browser security settings, thus opening the system to further opportunistic infections, much like an immune deficiency disease.
- Some other types of spyware use rootkit like techniques to prevent detection, and thus removal.

Remedies and Prevention

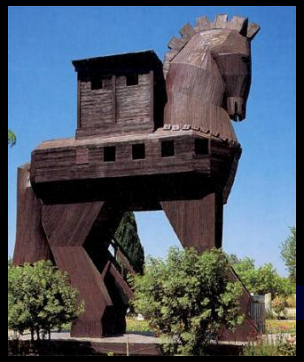
- Spyware is constantly evolving, meaning remedies can vary from different types of spyware.
- If programs do not work to rid the computer of the infected then a full system reinstall would be needed.
- Most big anti-virus firms have added anti-spyware to their anti-virus packages. (Such as Mcafee and Symantec)
- Read forums to get latest spyware info - http://www.spywareinfoforum.com/

Examples of Spyware Programs

- CoolWebSearch
- Internet Optimizer
- HuntBar
- Movieland
- MyWebSearch
- Zango
- WeatherStudio

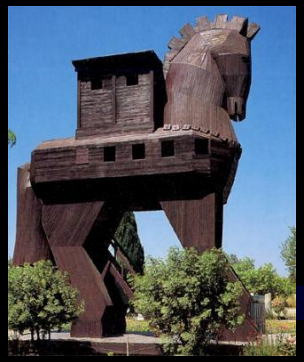


http://www.2-spyware.com/news/



Trojans

- Program that does something other than advertised
- Typically executable programs
- Sometimes made to appear as data file
- Example
  - User downloads “free calendar program”
  - Program scans system for credit card numbers & passwords
  - Transmits information to attacker through network

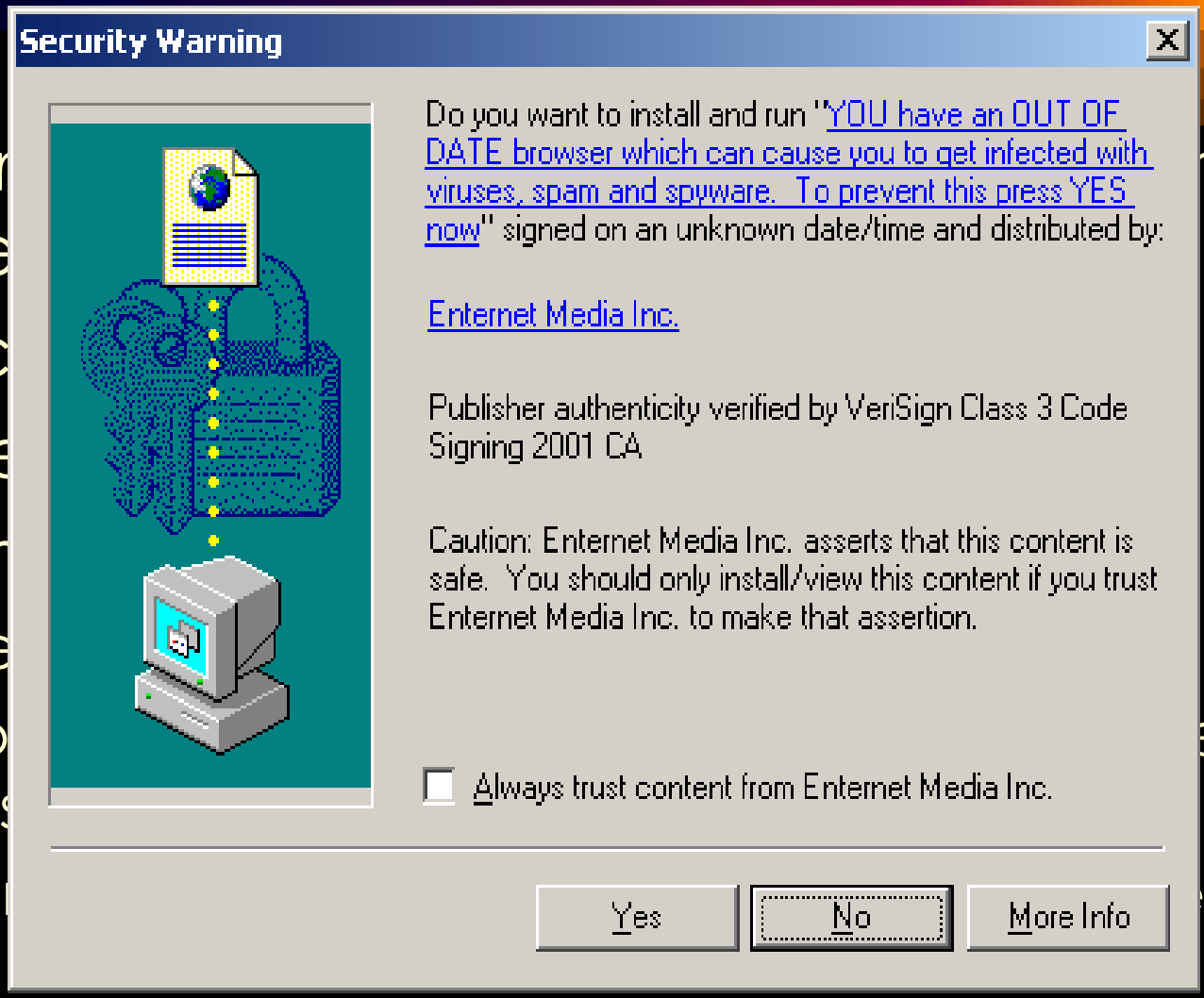


Trojans

- Progr
  adve
- Typic
- Some
- Exam
  - Use
  - Pro
    pas
  - Tra

ers &

twork



Rootkits

- Software tools used by an attacker to hide actions or presence of other types of malicious software
- Hide or remove traces of log-in records, log entries
- May alter or replace operating system files with modified versions:
  - Specifically designed to ignore malicious activity

Rootkits

- Rootkits can be detected using programs that compare file contents with original files
- Rootkits that operate at operating system's lower levels:
  - May be difficult to detect
- Removal of a rootkit can be difficult
  - Rootkit must be erased
  - Original operating system files must be restored
  - Reformat hard drive and reinstall operating system

Logic Bombs

- Computer code that lies dormant
  - Triggered by a specific logical event
  - Then performs malicious activities
- Difficult to detect before it is triggered
- Sometimes used by legitimate software companies to ensure payment for their software.

Botnets

- Infected computer called a **zombie**
- Groups of zombie computers together called **botnet**
- Attacker is knows as a **bot herder**
- Computer is infected with program that allows it to be remotely controlled by attacker
  - Often payload of Trojans, worms, and viruses
- Early botnet attackers used Internet Relay Chat to remotely control zombies
  - HTTP is often used today

Botnets

- Botnets operate in the background commanding thousands of zombies to send massive amounts of spam
- Some of the data that spam mail may track:
  - timestamp when email gets opened and read
  - duration of reading the e-mail; (Read/Skimmed/Glanced)
  - who did the reader forwarded the e-mail
  - location/country (ip address) origin of the reader

Keyloggers (Spyware)

- Hardware Keyloggers
  - A small hardware device inserted between the keyboard connector and computer keyboard port.
  - Monitors each keystroke a user types on the computer's keyboard. As the user types, the keystrokes are collected and saved as text
- Software keyloggers
  - Programs that silently capture all keystrokes, including passwords and sensitive information
  - Hide themselves so that they cannot be easily detected even if a user is searching for them

Hardware Keylogger

HOW TO OVERCOME KEYLOGGER?

Objectives of malware

1. Spreads

2. Conceals

3. Profits

Viruses Trojans Worms Rootkits Botnets Keyloggers
Logic Bombs

Objectives of malware

1. Spreads

- Viruses
- Worms

2. Conceals

- Trojans
- Rootkits
- Logic Bombs

3. Profits

- Botnets
- Keyloggers

Viruses Trojans Worms Rootkits Botnets Keyloggers Logic Bombs

E-Mail Attacks

- SPAM
  - Unsolicited emails
  - Use Spam filters to look for specific words and block emails
- Malicious attachments
  - Email distributed viruses
- Embedded hyperlinks
  - Trick users to be directed to the attacker's "look alike" web site.

Anti-Malware

- Anti-virus
- Anti-Spam
- Pop-up blockers

Anti-virus

- Software that examines a computer for infections
- Scans new documents that might contain viruses
- Searches for known virus patterns
- Weakness of anti-virus
  - Vendor must continually search for new viruses, update and distribute signature files to users

Anti-virus

How Antivirus works?

1. Examining files to look for known viruses by means of a virus dictionary.
   - When the anti-virus software examines a file, it refers to a dictionary of known viruses that have been identified by the author of the anti-virus software. If a piece of code in the file matches any virus identified in the dictionary, then the anti-virus software can then either delete the file or quarantine it.
2. Identifying suspicious behaviour from any computer program which might indicate infection.
   - The suspicious behaviour approach monitors the behaviour of all programs. If one program tries to write data to an executable program, for example, this is flagged as suspicious behaviour and the user is alerted to this, and asked what to do.

reference: http://www.antivirusworld.com/articles/antivirus.php

Anti-Spam

- Anti spam software filters prevent all unwanted spam and junk email from entering your inbox
  - Norton, Trend Mirco, McAfee

Figure 2-3 GIF layering

- However, attacker can use anti-spam mail techniques to overcome filter
  - GIF Layering
    - Image spam divided into multiple images
    - Layers make up one complete legible message
  - Word Splitting
    - Horizontally separating words
    - Can still be read by human eye
  - Geometric variance
    - Uses speckling and different colors so no two emails appear to be the same

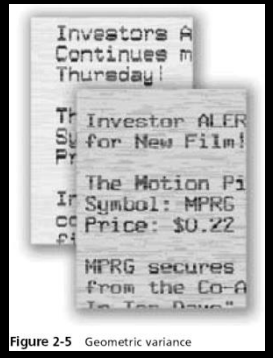


Figure 2-5 Geometric variance

Pop-up blockers

- Separate program as part of anti-spyware package
- Incorporated within a browser
- Allows user to limit or block most pop-ups
- Alert can be displayed in the browser
  - Gives user option to display pop-up