Malicious Logic

Dr. Ahmad Almulhem

Computer Engineering Department, KFUPM

Spring 2008

Outline

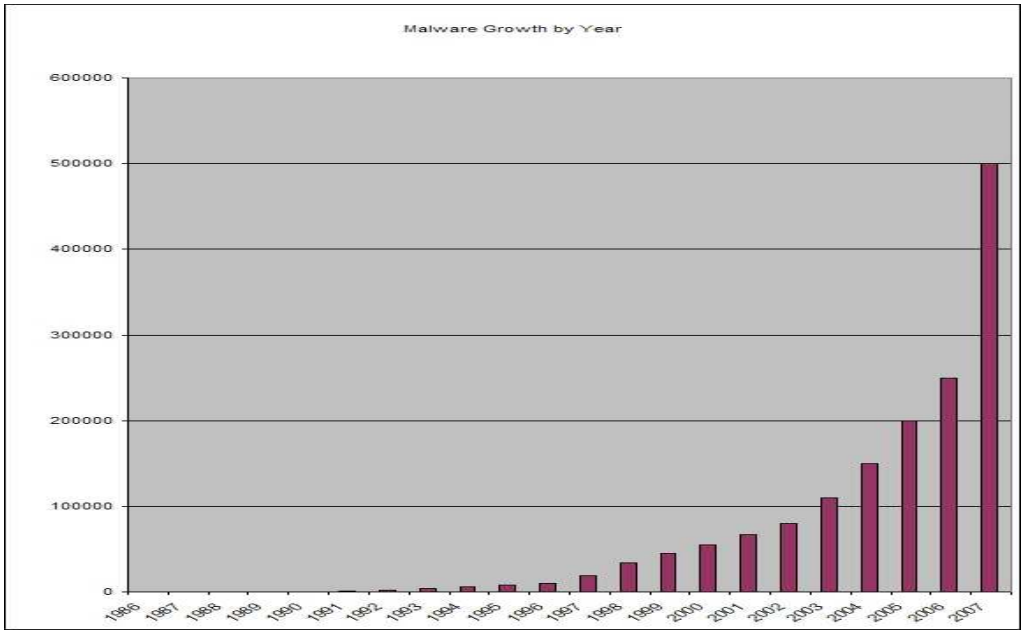
Malicious Logic

Definition (Malicious Logic)

A set of instructions that cause site security policy to be violated

- Also called *Malicious software (malware)*
- Incorrectly called "computer viruses"
- Based on intention (e.g. `rm -fr *`)
- Should not be confused with defective software (bugs)

Malicious Logic



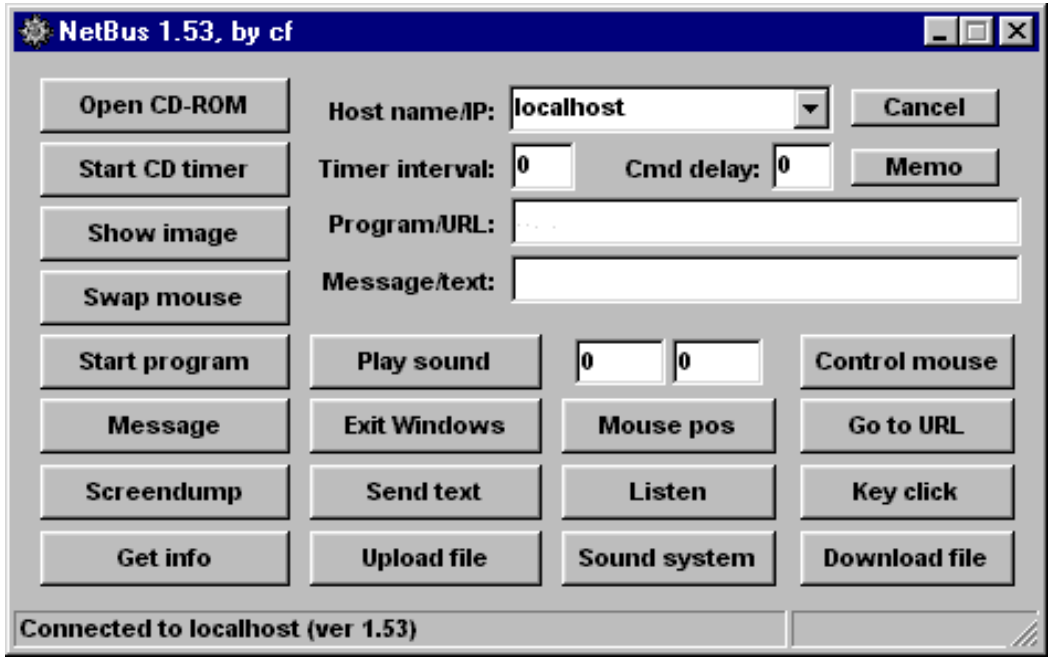
src: http://www.f-secure.com/

- Most of released code today are malicious
- F-Secure: 25,000 malware samples every day!
- Symantec: web-based malware instead of direct attacks
- Delivered through the Internet, by email and websites

Trojan Horses

- Program with an overt purpose (known to user) and a covert purpose (unknown to user)
- Usually superficially attractive (eg game, s/w upgrade etc)
- The covert purpose is done by a hidden payload:
  - Remote Access
  - Data Destruction
  - Downloader
  - Server Trojan(Proxy, FTP , IRC, Email, HTTP/HTTPS, etc.)
  - Security software disabler
  - Denial-of-service attack (DoS)

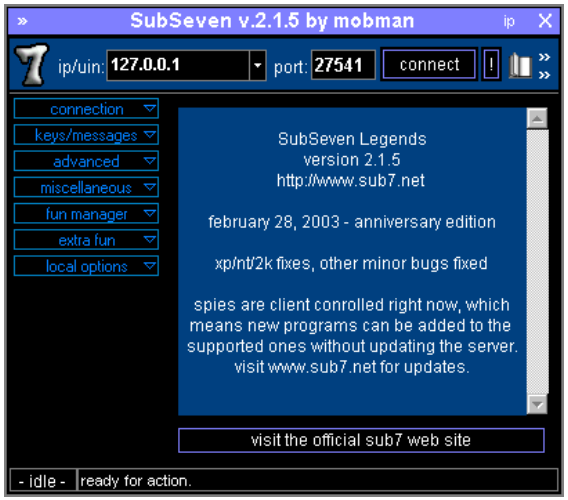
Trojan Horses: Examples



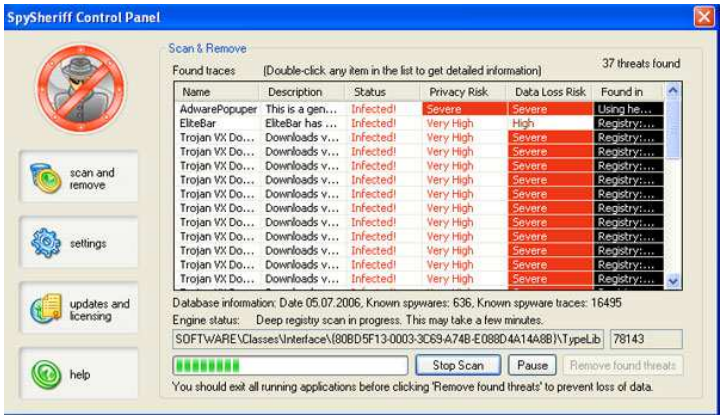
NetBus

- client-server architecture
- Designed for Windows system (1998)
- Server must be installed (usually disguised as a game)
- Client is a GUI with many functions!
- NetBuster/NetBusterBuster can be used to attack back!

Trojan Horses: Examples



- Back Orifice
- Sub7
- NetBus
- SpySheriff (anti-spyware program!)
- Prorat
- Vundo trojan (popups and advertising)
- Trojanizary



Viruses

- Program that inserts itself into one or more files and performs some action
  - *Insertion (infection)* phase is inserting itself into file or disk
  - *Execution* phase is performing some action
- Spreads without permission or knowledge of the user
- Requires a host (program) to spread

Trojans vs Viruses

- Trojans have an overt (good) purpose and a covert (bad) purpose
- Viruses have only one purpose

Types of Viruses

- Boot sector viruses
  - A virus that inserts itself into the boot sector of a disk
  - Executed when system boots
- Executable viruses
  - A virus that infects executable programs (eg .exe)
- Multipartite viruses
  - A virus that can infect either boot sectors or executable
  - Contains a boot sector infector and executable infector
- Memory-resident (TSR) viruses
  - A virus that stays active in memory
- Stealth viruses
  - A virus that conceals infection of files
  - Intercepts system calls
  - Example: Request for file length: return length of uninfected file

Types of Viruses

- Encrypted viruses
  - A virus that is enciphered except for a small deciphering routine
  - Uses random key; harder to detect!
- Polymorphic viruses
  - A virus that changes its form each time it inserts itself into another program
  - Use different instructions with same effect (eg add/subtract/xor 0)
  - Harder than encrypted viruses
- Macro viruses
  - A virus composed of a sequence of instructions that are interpreted rather than executed directly
  - Code is platform independent (eg MS Word/Excel)
  - Melissa virus (MS Word)

Worms

- A program that copies itself from one computer to another
- Spreads over a network
- Morris Internet worm in 1988
  - Written by Robert Morris (Cornell University student) and launched from MIT
  - Targeted Berkeley, Sun UNIX systems
  - Disabled several thousand systems in about 6 hours
  - Used virus-like attack to inject instructions into running program and run them
  - To recover, had to disconnect system from Internet and reboot
  - Led to creation of CERTs

Worms vs Viruses

Worms spread through network $\leftrightarrow$ Viruses spread through files

Worms harm network bandwidth $\leftrightarrow$ Viruses corrupt or modify files

Rabbits/Bacteria

- A program that absorbs all of some class of resources

Example (Unix Shell script)

```
while true
do
      mkdir x
      cd x
done
```

Logic Bombs

- A program that performs malicious actions when specified conditions are met:
  - presence/absence of some file
  - particular date/time
  - particular user
- When triggered typically damage system
  - modify/delete files/disks, halt machine, etc

Other Malware types

The list goes on . . .

- Malware for profit
  - spyware
  - adware
  - botnet
  - key-loggers
- rootkits
- zombies
- backdoor

Countermeasures

- Best countermeasure is prevention
  - Don't allow a virus to get in
- Prevention in general is not possible
- Hence need to do one or more of:
  - detection - of viruses in infected system
  - identification - of specific infecting virus
  - removal - restoring system to clean state
- Advances in viruses and anti-virus technology go hand in hand!
- Earlier viruses were easier to detect

Anti-Virus Software

1. First-generation (simple scanners)
   - Uses virus signature to identify virus
   - Detect changes in length of programs
2. Second-generation (heuristic scanners)
   - Uses heuristic rules to spot viral infection
   - Uses checksum/hash of program to detect changes
3. Third-generation (activity traps)
   - Memory-resident programs identify virus by actions
4. Fourth-generation (full-featured protection)
   - Packages with a variety of anti-virus techniques
   - eg scanning & activity traps, access-controls

Summary

- Malware
- Malware types: Trojan horses, viruses, worms, logic bombs, etc
- Malware defenses: anti-virus generations