Information Systems Security

Lecture 2

Malicious Software

Dr. En. Bader Ahmad

Outline

1. Malicious code
2. Trojan horses
3. Viruses
4. Worms
5. Other malicious codes
6. Countermeasures

1. What is Malicious Code?

- Any code which:
  - Modifies or destroys data
  - Steals data
  - Allows unauthorized access
  - Exploits or damages a system
  - Does something user did not intend to do
- **Malware** is a MALicious softWARE
- Malware can be any things: viruses, worms, trojan horses, etc.

2. Trojan Horse

- **A Trojan horse** is a program that appears to be useful or harmless but that contains hidden code designed to exploit or damage the system on which it is run.
- Originally Trojan horses were not designed to spread themselves.
- A Trojan horse tricks user into executing malicious code.
- Examples:
  - A simple example of a Trojan Horse would be a program named “Bush.EXE" that is posted on a website with a promise to be a fun animation.

Trojan Horse

- Windows configured by default to hide filename extensions
  - 'Readme.txt → Readme.txt.exe.
- On the Microsoft Windows platform, an attacker might attach a Trojan horse with an innocent-looking filename to an email message which entices the recipient into opening the file.

- Downloader-UA.h
  - On the McAfee web site
  - Discovered in May 2008
  - Downloader-UA.h trojans are fake music and video files associated with fastmp3player.com.

Trojan Horses: How do we avoid getting infected?

Some practical tips to avoid getting infected:

1. NEVER download blindly from people or sites which we aren't 100% sure about.
2. Even if the file comes from a friend, we still must be sure what the file is before opening it
3. Beware of hidden file extensions
4. NEVER use features in our programs that automatically get or preview files.
5. Never blindly type commands that others tell us to type, or go to web addresses mentioned by strangers, or run pre-fabricated programs or scripts.
6. Don't be lulled into a false sense of security just because you run anti-virus programs
7. Finally, we must avoid any download of executable programs.

Trojan Horses: How do We get rid of Trojans?

1. **Clean Re-installation**:
   - Back up our entire hard disk,
   - Reformat the disk,.
   - Re-install the operating system and all our applications from original CDs,
   - Restore our user files from the backup if we're certain they are not infected.

2. **Anti-Virus Software**:
   - Can handle most of the well known trojans, but none perfect,
   - Must be updated

Trojan Horses: How do We get rid of Trojans?

- is not as evolved fast as trojans
- Some times give false sense of security
- Effective AVs: AVP, PCcillin, and McAfee VirusScan

3. **Anti-Trojan Programs**:
   - The Most effective against trojan horse attacks
   - A popular choice is The Cleaner,
   - update with all security patches, then we must change all our passwords because they may have been seen by every "hacker" in the world.

Trojan Horses: Back Orifice 2000

- Presented as a remote administration tool.
- It is composed of 3 parts:
  - Server Side Program (112 KB)
  - Configuration tool (Automatic Installation)
  - Client Side Tool (User Friendly)
- It provides more than 77 Functionalities. For example:
  - Restart the Computer Remotely
  - Lock the Computer Remotely
  - Detect the Passwords Remotely
  - Collect Information Remotely

3. Virus

- A **virus** uses code written with the express intention of replicating itself.
- A virus attempts to spread from computer to computer by attaching itself to a host program.
- It may damage hardware, software, or data.
  - When the "host" is executed, the virus code also runs, infecting new hosts and sometimes delivering an additional malicious actions.

Virus Operation

- During its lifetime, a typical virus goes through the following four phases:
- • Dormant phase: virus is idle, waiting for trigger event (eg date, program or file , disk capacity). Not all viruses have this stage
- • Propagation phase: virus places a copy of itself into other programs / system areas
- • Triggering phase: virus is activated by some trigger event to perform intended function
- • Execution phase: desired function (which may be harmless or destructive) is performed
- Most viruses work in a manner specific to a particular operating system or even hardware platform, and are designed to take advantage of the details and weaknesses of particular systems.

Virus Structure

1. Replicator
2. Protector
3. Payload
4. Trigger

```
Program V:=
{goto main;
   1234567;
   subroutine infect-executable :=
   {loop:
   file := get-random-executable-file;
   if (first-line-of-file = 1234567)
        then goto loop
   else
        Compress file
        prepend V to file;
   subroutine do-damage :=
     {what ever damage to be done}

   subroutine trigger-pulled :=
   {return true if some condition holds}

Main: main-program :=
   {infect-executable;
    if trigger-pulled then do-damage;
   goto next;}
next:
}
```

Virus Structure

The replication mechanism of a virus consists simply of computer executable instructions, or code, that enables the virus to attach itself to another

The protection mechanism is another attribute of a virus. It has the ability to attempt to hide from detection (by compression or encryption).

Trigger events or conditions that activate the virus.

The payload is defined as what the virus do in addition to replication

Types of viruses

1. File virus, also called **parasitic virus**.
2. **Boot sector infectors**: Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.
3. Memory-resident virus: lodges in the main memory and infects every program that executes
4. **Stealth virus**: a form of virus explicitly designed to hide itself from detection by antivirus softwares.
5. **Polymorphic virus**: a virus that mutates with every infection, making its detection impossible.

Types of viruses

6. **Macro virus**: infects macro programming environment (e.g., Microsoft office application such as Word) rather than specific operating systems .
   - ***A macro*** is a an executable program embedded in a word processing document or other types of files.
   - A macros is an executable file that can modify commands within the application menu.
   - Macro virus infects data files rather than executable files.
7. Email Virus: spread using email with attachment containing a macro virus
   - triggered when user opens attachment/message
   - usually targeted at Microsoft Outlook

Signs of viruses

- Indicators on the presence of virus:
  - The computer runs more slowly than normal
  - The computer stops responding or locks up often
  - The computer crashes and restarts every few minutes
  - The computer restarts on its own and then fails to run normally
  - Applications on the computer don't work correctly
  - Disks or disk drives are inaccessible
  - We can't print correctly
  - We see unusual error messages
  - …

How to Protect Ourselves from Viruses

- Avoid programs from unknown sources
- Disable floppy disk booting
- Make sure that Macro Virus Protection is enabled in all Microsoft applications,
- NEVER run macros in a document.
- Update the antivirus software, and perform a thorough scan of the computer.
- Download, install, and run the Malicious Software Removal Tool (for Microsoft Windows XP or Windows 2000 users especially).

4. Worms

- A **worm** uses self-propagating malicious code that can automatically distribute itself from one computer to another through network connections.
  - *i.e.*, Worms can execute and spread without user intervention.

- A worm can take harmful actions, such as:
  - consuming network or local system resources
  - causing a denial of service attack.
  - deleting data, spying users, …

Worm Operation

- worm phases like those of viruses:
  - dormant
  - propagation
    - search for other systems to infect
    - establish connection to target remote system
    - replicate self onto remote system
  - triggering
  - execution

Morris Worm

- best known classic worm
- released by Robert Morris in 1988
- targeted Unix systems
- using several propagation techniques
  - simple password cracking of local pw file
  - exploit bug in finger protocol,
  - exploiting a trapdoor in the debug option of the sendmail mail daemon.
- if any attack succeeds then replicated self

The Code Red Worm

- Self-replicating malicious code that exploits a known vulnerability in Microsoft servers
  - Appeared in July 2001.
- Proceeds as follows:
  - Infect a web server and replicate attack programs
  - From the infected web server, the code red infects other web servers and replicate attack programs
  - Damages:
    - Defacement of infected servers
    - Infected servers launch DOS attack against IP a particular IP address (the white house web site)

5. Other malwares

- **Trap door (or Back door)**: a secret entry point into a program that allows someone that is aware of the trapdoor to gain access without going through the usual security procedures.

- **Logic bomb**: is a code embedded in some legitimate program that is set to explode when certain conditions are met (time, or data).

- **Zombie**: is a program that secretly takes over another Internet-attached computer and then uses this computer to launch attacks

Other malwares

- What is not malware?!!!
  - Spyware (also called *spybot* or *tracking software)*. programs that conduct certain activities (collecting personal information) on a computer without obtaining appropriate consent from the user.
  - Adware: pop-up advertisements
  - Spam: is unsolicited e-mail generated to advertise some service or product
  - Scams: An e-mail message that attempts to trick the recipient into revealing personal information that can be used for unlawful purposes

6. Virus countermeasures

- The antivirus approach: the ideal solution to the threat of viruses is prevention:
  - Don't allow malware to get into the system
    - This is difficult (even impossible) to achieve
- Follow the following approach:
  - Detection: once the infection has occurred, locate the virus.
  - Identification: identify the specific virus that has infected a program.
  - Removal: remove all traces of the virus from the infected program and restore it to its original state.
- Follow Virus Alert's website: (eg, next slide)
- Example:
  - The Windows case (the antivirus Defense-in-Depth Guide, Ch4)

Learn More

Current Malware

	Date Published
GPCoder.h	16 Jul 2007
W32/Zhelatin.gen!eml	04 Jul 2007
Phish-BuyPhony	01 Jul 2007
W32/Stration.gen.dldr	07 Nov 2006
PWS-Banker.gen.ac	17 May 2006

- See Recent Malware
- View Malware Threat Key
- Search Threat Library

Top Potentially Unwanted Programs (PUPs)

	Date Discovered
Generic PUP.g	05 Feb 2007
Dialer-315	25 Jan 2007
Adware-Mirar	29 Mar 2005
Spyware-Webhancer	19 Jan 2005
with fishy extension	04 Aug 2004

- See Recent PUPs
- Search Threat Library

Virus Map

Get a real-time, bird's-eye view of where computers around the globe are detecting viruses.

Current Vulnerabilities

	Date Public
MS07-060 MS Word Mem..	09 Oct 2007
MS07-061 URI RCE	01 Sep 2007
MS07-042 XML Core	14 Aug 2007
MS07-039 Active Dir ..	10 Jul 2007
MS07-031 MS SChannel	12 Jun 2007
MS07-059 SharePoint ..	04 May 2007
MS07-029 MS DNS RPC	12 Apr 2007
MS07-057 IE onload S..	23 Feb 2007
MS07-054 MSN RCE	31 Jan 2007

- See Recent Vulnerabilities
- View Vulnerability Threat Key
- Search Threat Library

Latest Spam Activity

Current Spam Categories

Tips to Avoid Spam

View Top 10 Spam Subject Lines

Top Phish scams

Suspension Notice
eBay New Unpaid Item Message
You have 1 new secure message
Amazon.com - Critical Account Information
Sparkasse Internet Banking

View Top 10 Phish Scams

Top 10 Threat Predictions for 2008

As 2007 comes to a close, it's a good time to reflect on the current threat landscape. McAfee Avert Labs has identified ten noteworthy trends that we expect to unfold in 2008.

McAfee Avert Labs Blog

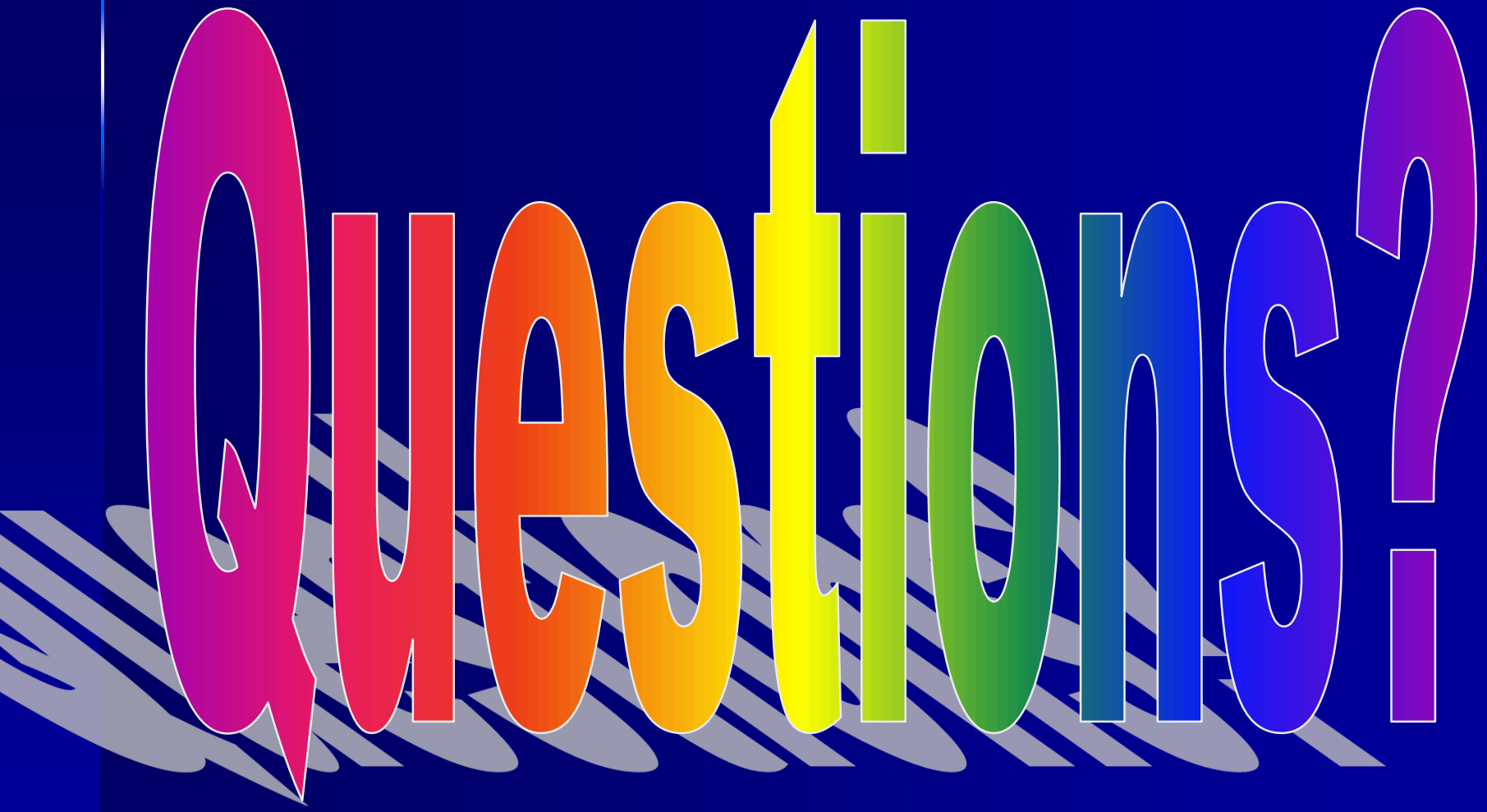
Read about security research as it happens

McAfee Avert Labs Security Advisories

Sign up here to receive free

Windows's antivirus Defense-in-Depth Guide

1. Active processes and services
   - Task Manager, Ps Tools, Process Explorer
2. The local registry
   - Regedit (the registry editor)
3. Files in the Microsoft Windows system folders.
   - Use the "Windows Search"
4. New user or group accounts, especially with Administrator privileges
5. Shared folders (including hidden folders).
6. Newly created files with normal looking file names but in unusual locations
7. Opened network ports
   - Netstat, FPort


Questions?