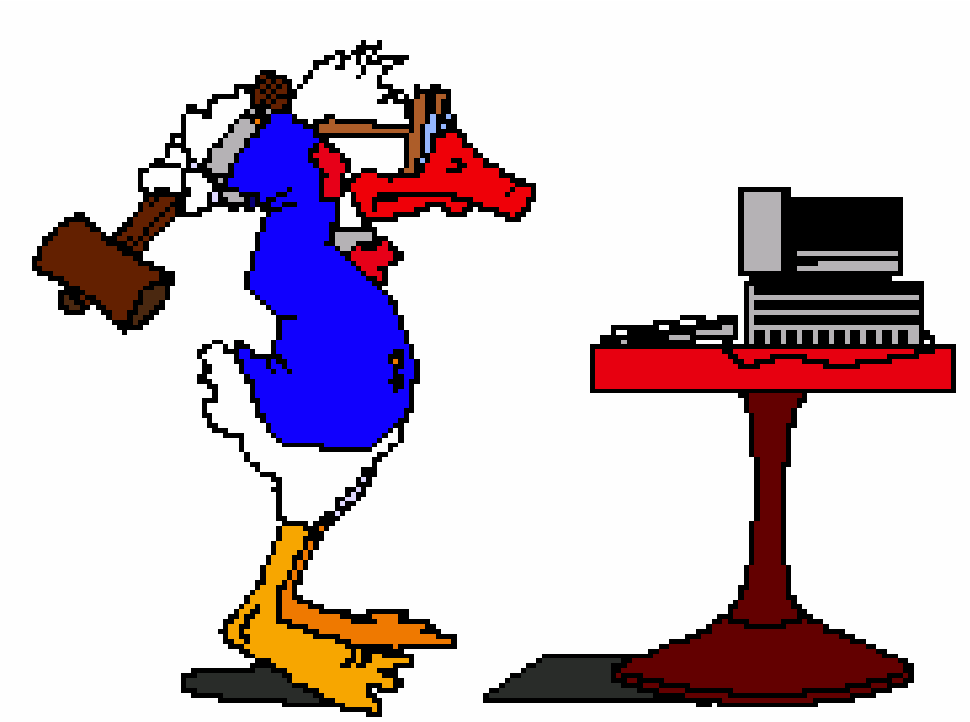
An Introduction to Malicious Code

Agenda

- What is malicious code?
- How do you get malicious software?
- Types of malicious code.
- What is a virus?
- What is a Trojan Horse?
- World Virus Map.
- What is a Worm?
- What is a Logic Bomb?
- Ounce of Prevention.

What is Malicious Code?

- Uninvited software code that is intended to cause harm or mischief.
  - Modifies or destroys data
  - Steals data
  - Allows unauthorized access
  - Exploits or damages a system
  - Does something user did not intend to do
- Malicious code can be a program, part of a program, or can attach itself to an existing program.
- Often exploits system flaws or insecure configurations.
- Writes to files, deletes files, emails, executes and stops programs.



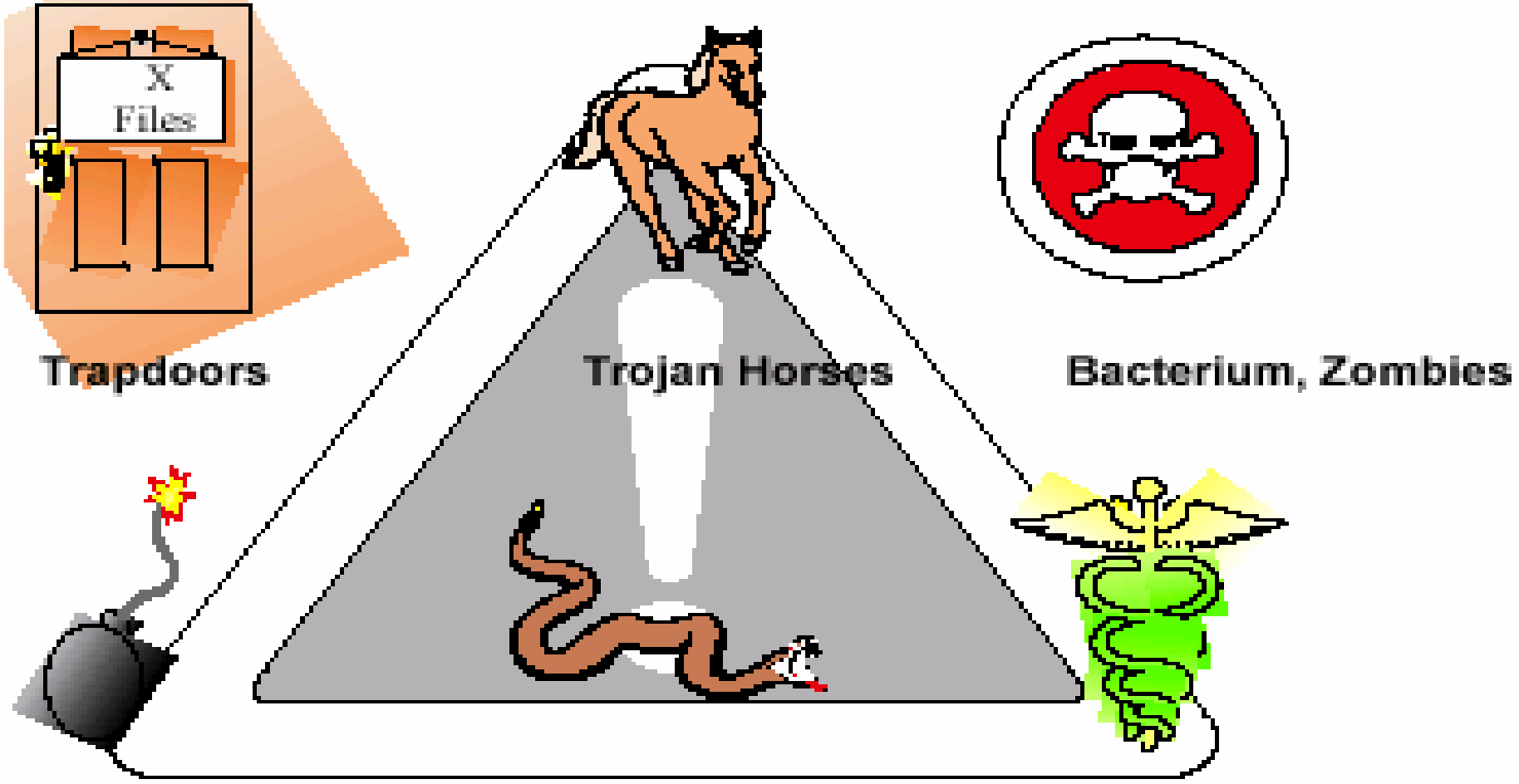
How do you get Malicious software?

- Diskettes
- Email
- Internet
- Pirated Software
- Magazine CDROMs

Types of Malicious Code

- Virus
- **E-mail viruses**
- Trojan Horse
- Worm
- Logic Bomb
- Bacteria
- Trapdoor

MALICIOUS CODE



What is a virus?

- Program that attaches itself to a host program so that when the host is executed, the virus will execute.
- When executed a virus attempts to copy itself to other programs.
- Types – Boot Sector, Multipurpose Viruses, File virus etc.

Object of destruction by virus

- DOS Boot record destructor
- Master Boot Record (Partition Table) destructor
- Specific Data File Destructor
- Fat destructor
- Directory destructor
- Random Sector destructor
- CMOS destructor

Smartness of Viruses

Stealth Technique virus

Virus use some undocumented DOS interrupts/functions to hide from DOS/ Antivirus programs. Or, they take advantage of some loopholes in DOS as well as in Antivirus programs and manage themselves accordingly. These viruses, when in memory, remain safe and undetected by Antivirus programs. Some of these, when in memory, show the original objects instead of the infected ones, when the infected objects are accessed.

Smartness of Viruses

Polymorphic viruses.

These virus encrypt the main part of their own code using a variable key, and leave the decryption routine in an unencrypted form. The encryption key is changed from time to time so as to make it difficult for antivirus programs to use the decryption key for searching virus signature and hence to detect their presence. Due to their complex structure these viruses are difficult to design.

Boot sector Virus

There is no checking either of MBR or of DBR by ROM BIOS loader while the system boots. i.e. the sector (DBR/MBR) is loaded blindly and control is passed to it for execution. BIOS loader is independent of operating system; it only confirms that the sector is executable by checking the two byte signature 55AA Hex in it. Boot sector virus normally store the original DBR or MBR somewhere else on the same disk or use their own DBR/MBR and replace the original sector with their own code. We know that when the system boots the first software executable code is the code in the boot sector (MBR in case of hard disk)). So, if the DBR/ MBR is already infected, the first code to be executed by the system is indirectly the virus itself. Hence these viruses can take control of the system before operating system loads and can have total control of the system and remain in memory all the time. As Antivirus software are loaded after O.S is loaded and as BSVs take system control before O.S. is loaded, BSV infects the disk before antivirus is loaded and also can easily knockout the Antivirus software and forces them to show that system is okay

E- Mail Virus

- An e-mail virus moves around in e-mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book

What is a Trojan Horse

- Apparently useful program containing hidden functions that do things that the user did not intend.
- These programs
- are generally deeply buried in the code of the target
- program
- Games and graphic programs are often used as Trojan horses.
- Carries out a mission that will not be noticed by the user.

Trojan Horse

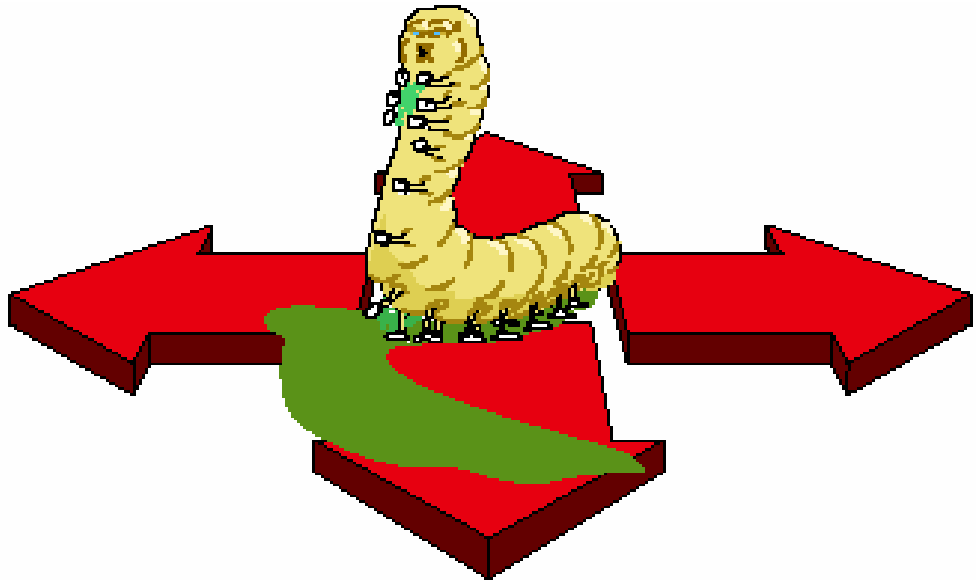
Example:

- “ ***unsuccessful login***” message
- username and password have been captured
- lack of an unsuccessful logon notice would indicate a stolen password!

What is a Worm?

- Program that circulates itself. Uses computer networks and security holes to replicate itself.
- Program that makes a copy of itself and causes the copy to execute as a stand alone program.

Can replicate itself via permanent or dial-up connections.



Def: type of malicious code that propagates from one machine to another, typically through a network connection. Unlike a virus it does not modify a host program to spread, but instead sends its executable to another machine where it is executed using some sort of remote execution facility.

The Great Worm

- November 2,1988, Robert Morris released an unauthorized worm onto the INTERNET.
- Nov. 3: Within 8 hours between 2 and 3 thousand computers were infested causing a massive disruption of services.
- Nov. 4: Worm code was decompiled and it was determined the worm did not modify existing files (not a virus).
- Nov. 6: Most computers were reconnected to the Internet.
- Nov. 12: The Internet E- Mail backlog finally cleared.
- The Great INTERNET Worm was a Program that ran by itself, propagating a fully working version of itself to other machines. The direct and indirect costs from this worm are estimated at over $98 million.

Code Red

Code Red worm replicated itself over 250,000 times in approximately nine hours on July 19, 2001.

- The Code Red worm slowed down Internet traffic when it began to replicate itself.
- Each copy of the worm scans the Internet for Windows NT or Windows 2000 servers that do not have the Microsoft security patch installed (see sidebar). Each time it finds an unsecured server, the worm copies itself to that server. The new copy then scans for other servers to infect. Depending on the number of unsecured servers, a worm could conceivably create hundreds of thousands of copies.
- The Code Red worm attacks Windows NT 4.0 and Windows 2000 servers running Microsoft IIS (Internet Information Server) 4.0 or IIS 5.0. Microsoft released a simple patch that fixes the security loophole used by the Code Red worm

Code Red

- The Code Red worm is designed to do three things:
- Replicate itself for the first 20 days of each month
- Replace Web pages on infected servers with a page that declares "Hacked by Chinese"
- Launch a concerted attack on the White House Web server in an attempt to overwhelm it
- The U.S. government changed the IP address of www.whitehouse.gov to circumvent that particular threat from the worm

Nimda worm

• CERT/ CC Alert 09/ 18/ 01: affects Windows 9x and
NT/ 2000 machines
– Email propagation, IIS vulnerable servers scan, use of Code Red II
and Sadmind back doors;
– No agressive code, modification of HTML web pages and
congestion of networks

What is a logic bomb?

- Program triggered by any combination of conditions – the arrival of a specific data or time, infection of a specific number of files, detection of a predetermined activity.
- More sophisticated attack since there can be delay between preparation and activation.
- Time bomb – set to go off at a specific date and time.

Bacteria

Consume system resources by replication

Trapdoor

Secret entry point into a program to allow unauthorized security access

Viruses Life Phases

- **Dormant phase** – but eventually activated by some event (e.g., date, idle system)
- **Propagation phase** – places identical copy of itself into other programs or system areas
- **Triggering phase** – activation upon certain events and condition (date, etc.)
- **Execution phase** – the function (harmless or destructive) is performed

Types of viruses

- **Parasitic virus** – attaches to executable files and replicates when the infected program is executed
- **Memory-resident virus** – lodges in main memory as part of a resident system program, then infects every program executed
- **Boot sector virus** – infects a (master)boot record and spreads when a system is booted from the infect disk
- **Stealth virus** – explicitly design to hide itself from detection by anti-virus software
- **Polymorphic virus** – mutates with every infection, making detection by “signature” impossible

Once of Prevention

- Purchase virus protection software. Configure your virus protection software to automatically download pattern file updates via the Internet.
- Avoid programs from unknown sources.
- Enable “Macro Virus Protection” in all Microsoft applications.
- Never run executable program attachments received through email.
- Scan all documents and programs before opening or installing.
- Never boot a hard disk system from an unprotected diskette
- Never use untested software (test off line or on a single purpose dedicated system)
- Backup files and programs, securely store and routinely check for infection
- Minimize software sharing within the organization
- Educate users to watch for changes in patterns of system activity
- Install virus detection software