Computer Viruses and Worms

CMP103

Definition of Virus

- "A computer virus is an exact cybernetic analogy to its biological reference"

Computer Virus

- Replicate itself in order to carry out a mission.
- Be dependent on a "host" to carry out the mission.
- Create damage to the computer system "infected".

VIRUS EFFECTS

- Trivial, simply reproduces or displays messages.
- Minor, alters or deletes infected files.
- Moderate, wipes out entire disk drive.
- Major, slowly corrupts data with pattern, making restoration difficult.
- Severe, slowly corrupts data without pattern, making restoration impossible.
- Unlimited, virus which discovers system administrator's password and mails it to one or more users, tempting them to use it for illegal purposes.

Worms

- **Worm** - is a self-replicating program, similar to a computer virus. A virus attaches itself to, and becomes part of, another executable program; however, a worm is self-contained and does not need to be part of another program to propagate itself.

History of Worms

- The first worm to attract wide attention, the Morris worm, was written by Robert Tappan Morris, who at the time was a graduate student at Cornell University.
- It was released on November 2, 1988
- Morris himself was convicted under the US Computer Crime and Abuse Act and received three years probation, community service and a fine in excess of $10,000.

- Xerox PARC

Worms…

- **Worms** – is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.
- They are often designed to exploit the file transmission capabilities found on many computers.

Zombies

- Infected computers — mostly Windows machines — are now the major delivery method of spam.
- Zombies have been used extensively to send e-mail spam; between 50% to 80% of all spam worldwide is now sent by zombie computers

Typical things that some current Personal Computer (PC) viruses do

- Display a message
- Erase files
- Scramble data on a hard disk
- Cause erratic screen behavior
- Halt the PC
- Many viruses do nothing obvious at all except spread!

Distributed Denial of Service

- A **denial-of-service attack** is an attack that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.

How it works?

- The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.
- Victim's IP address.
- Victim's port number.
- Attacking packet size.
- Attacking interpacket delay.
- Duration of attack.
- MyDoom – SCO Group

MyDoom

- **26 January 2004:** The Mydoom virus is first identified around 8am. Computer security companies report that Mydoom is responsible for approximately one in ten e-mail messages at this time. Slows overall internet performance by approximately ten percent and average web page load times by approximately fifty percent

TYPES: Executable Viruses

- Traditional Viruses
- pieces of code attached to a legitimate program
- run when the legitimate program gets executed
- loads itself into memory and looks around to see if it can find any other programs on the disk

OTHER TYPES

- BOOT SECTOR
- MULTI-PARTITE
- POLYMORPHIC
- META

Boot Sector Viruses

- Traditional Virus
- infect the boot sector on floppy disks and hard disks
- By putting its code in the boot sector, a virus can guarantee it gets executed
- load itself into memory immediately, and it is able to run whenever the computer is on

POPULAR VIRUS ATTACKS

- **1. Mydoom – $38 billion**
- The worst computer virus outbreak in history, Mydoom caused estimated damage of $38 billion in 2004, but its inflation-adjusted cost is actually $52.2 billion. Also known as Novarg, this malware is technically a “worm,” spread by mass emailing. At one point, the Mydoom virus was responsible for 25% of all emails sent.

Melissa virus

- March 1999
- the Melissa virus was the fastest-spreading virus ever seen
- Someone created the virus as a Word document uploaded to an Internet newsgroup
- People who downloaded the document and opened it would trigger the virus
- The virus would then send the document in an e-mail message to the first 50 people in the person's address book

I LOVE YOU – $15BILLION

- The year 2000’s ILOVEYOU virus worked by sending a bogus “love letter” that looked like a harmless text file. Like Mydoom, this attacker sent copies of itself to every email address in the infected machine’s contact list. Shortly after its May 4 release, it had spread to more than 10 million PCs.
- The virus was created by a college student in the Philippines named Onel de Guzman. Lacking funds, he wrote the virus to steal passwords so he could log into online services he wanted to use for free. He reportedly had no idea how far his creation would spread. This virus is also known as Loveletter.

WANNA CRY? – $4 BILLION

- The 2017 WannaCry computer virus is ransomware, a virus that takes over your computer (or cloud files) and holds them hostage. The WannaCry ransomware ripped through computers in 150 countries, causing massive productivity losses as businesses, hospitals, and government organizations that didn’t pay were forced to rebuild systems from scratch.

TROJANS

- Computer Trojans are simply malicious computer programs disguised as something useful.
- THE STORY OF TROY

DIFFERENCE

- The major difference between viruses and Trojans is that viruses reproduce, while a Trojan is just a one time program which executes its payload as soon as the Trojan is executed. Trojans are the most common way of bringing a virus into a system. **A current example of a Trojan is a program called pkz300b.exe which disguises itself as an archiving utility, but when run it will delete your entire hard drive.**

Prevention

- Updates
- Anti-Viruses
- More secure operating systems
  e.g. UNIX

ADDITIONAL NOTES

- CYBER SECURITY (C.I.A)
- PHISHING

- READ ON THEM

Reference

- http://mirror.aarnet.edu.au/pub/code-red/newframes-small-log.gif
- http://www.factmonster.com/ipka/A0872842.html
  http://www.faqs.org/faqs/computer-virus/new-users/
- http://www.mines.edu/academic/computer/viri-sysadmin.htm