Virus, Worms and Trojans

Outlines:

- Definition Of a Computer Virus
- History Of Computer Viruses
- The Virus Languages
- Symptoms
- Classifying Viruses
- Classifying virus Categories
- Classifying virus types
- Protection/Prevention
- 9 Antivirus

By: Arash Habibi Lashkari

July - 2010

Introduction

- Computer virus have become today's headline news
- With the increasing use of the Internet, it has become easier for virus to spread
- Virus show us loopholes in software
- Most virus are targeted at the MS Windows OS

Definition

A true virus is capable of self replication on a machine. It may spread between files or disks, but the defining character is that it can recreate itself on it’s own with out traveling to a new host.

On the other word,

A computer virus is a self-replicating program containing code that explicitly copies itself and that can "infect" other programs by modifying them or their environment such that a call to an infected program implies a call to a possibly evolved copy of the virus.

Background

- There are estimated 30,000 computer viruses in existence
- Over 300 new ones are created each month
- First virus was created to show loopholes in software

History

Since the age of technology arose, and the twentieth century of computers came about, there have always been an attempt from those trying to be “smarter” then the average computer, (or computer user, for that matter).

It was the very famous Fred Cohen who "wrote the book" on computer viruses. He was the soul in the development of a theoretical, and mathematical model of computer virus behavior.

He was able to use his logic to test several hypothesis about computer virus’s. Cohen's very own, and well-known, informal definition is "a computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of itself".

This does not mean that a computer has to undergo actual destruction(such as deleting or corrupting files) in order to be classified as a "virus" by Cohen’s definition. Many people use the term "virus" loosely to cover any sort of program that tries to hide its possible destructive functions and\or tries to spread onto as many computers as possible; leaving us with a long list of possibilities to deal with.

Virus Languages

- ANSI COBOL
- C/C++
- Pascal
- VBA
- Unix Shell Scripts
- JavaScript
- Basically any language that works on the system that is the target

Symptoms of Virus Attack

- Computer runs slower then usual
- Computer no longer boots up
- Screen sometimes flicker
- PC speaker beeps periodically
- System crashes for no reason
- Files/directories sometimes disappear
- Denial of Service (DoS)

Classifying Virus - General

- **Virus Information**

  Discovery Date:

  Origin:

  Length:

  Type:

  Sub Type:

  Risk Assessment:

  Category:

Classifying Virus - Categories

- Stealth
- Cavity
- Companion
- Polymorphic
- Armored

Stealth

The STEALTH virus is one that, while "active“ can hide the changes it has made to files or boot records. This is achieved by monitoring the system functions used to read files or sectors from storage media and forging the results of calls to such functions.

In order to do this, the virus must be a resident in memory when the anti virus program is executed and this may be detected by antivirus program.

Cavity

A CAVITY VIRUS is one which overwrites a part of the host file that is filled with a constant (usually nulls), without increasing the length of the file, but preserving its functionality.

The Lehigh virus was an early example of a cavity virus.

Companion

The COMPANION virus is one that, instead of modifying an existing file, creates a new program which is executed instead of the intended program.

On exit, the new program executes the original program so that things appear normal. On PCs this has usually been accomplished by creating an infected .COM file with the same name as an existing .EXE file.

Integrity checking anti virus software that only looks for modifications in existing files will fail to detect such viruses.

Polymorphic

A POLYMORPHIC virus is one that produces varied but operational copies of itself. This is so that virus scanners will not be able to detect all instances of the virus.

One method of evading scan string-driven virus detectors is self-encryption with a variable key. These viruses (Cascades) are not "polymorphic", as their decryption code is always the same. Therefore the decryptor can be used as a scan string by the simplest scan string-driven virus scanners (unless another virus uses the identical decryption routine and the exact identification.)

Armord

An ARMORED virus is one that uses special tricks to make tracing, disassembling and understanding of its code more difficult.

A good example of Armord virus is Whale.

Classifying Virus - Types

- Trojan Horse
- Worm
- Macro

Trojan Horse

A “TROJAN HORSE” is a program that does something undocumented that the programmer intended, but that some users would not approve of if they knew about it.

- Covert
- Leaks information
- Usually does not reproduce

Trojan Horse

- ***Back Orifice***

  Discovery Date: 10/15/1998

  Origin: Pro-hacker Website

  Length: 124,928

  Type: Trojan

  Sub Type: Remote Access

  Risk Assessment: Low

  Category: Stealth

Trojan Horse

- About Back Orifice
  - requires Windows to work
  - distributed by “Cult of the Dead Cow”
  - similar to PC Anywhere, Carbon Copy software
  - allows remote access and control of other computers
  - install a reference in the registry
  - once infected, runs in the background
  - by default uses UDP port 54320
    TCP port 54321
  - In Australia 72% of 92 ISP surveyed were infected with Back Orifice

Trojan Horse

- Features of Back Orifice
  - pings and query servers
  - reboot or lock up the system
  - list cached and screen saver password
  - display system information
  - logs keystrokes
  - edit registry
  - server control
  - receive and send files
  - display a message box

Worms

A computer WORM is a self-contained program (or set of programs), that is able to spread functional copies of itself or its segments to other computer systems (usually via network connections).

- Spread over network connection
- Worms replicate
- First worm released on the Internet was called Morris worm, it was released on Nov 2, 1988.

Worms

- ***Bubbleboy***

  Discovery Date: 11/8/1999

  Origin: Argentina (?)

  Length: 4992

  Type: Worm/Macro

  SubType: VbScript

  Risk Assessment: Low

  Category: Stealth/Companion

Worms

- Bubbleboy
  - requires WSL (windows scripting language), Outlook or Outlook Express, and IE5
  - Does not work in Windows NT
  - Effects Spanish and English version of Windows
  - 2 variants have been identified
  - Is a “latent virus” on a Unix or Linux system
  - May cause DoS

Worms

- How Bubbleboy works
  - Bubbleboy is embedded within an email message of HTML format.
  - a VbScript while the user views a HTML page
  - a file named “Update.hta” is placed in the start up directory
  - upon reboot Bubbleboy executes

Worms

- How Bubbleboy works
  - changes the registered owner/organization
    - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RegisteredOwner = “Bubble Boy”
    - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RegisteredOrganization = “Vandalay Industry”
  - using the Outlook MAPI address book it sends itself to each entry
  - marks itself in the registry
    - HKEY_LOCAL_MACHINE\Software\Outlook.bubbleboy = “OUTLOOK.Bubbleboy1.0 by Zulu”

Macro

- Specific to certain applications
- Comprise a high percentage of the viruses
- Usually made in WordBasic and Visual Basic for Applications (VBA)
- Microsoft shipped “Concept”, the first macro virus, on a CD ROM called "Windows 95 Software Compatibility Test" in 1995

Macro

- ***Melissa***

  Discovery Date: 3/26/1999

  Origin: Newsgroup Posting

  Length: varies depending on variant

  Type: Macro/Worm

  Subtype: Macro

  Risk Assessment: High

  Category: Companion

Macro

- Melissa
  - requires WSL, Outlook or Outlook Express Word 97 SR1 or Office 2000
  - 105 lines of code (original variant)
  - received either as an infected template or email attachment
  - lowers computer defenses to future macro virus attacks
  - may cause DoS
  - infects template files with it's own macro code
  - 80% of of the 150 Fortune 1000 companies were affected

Macro

- How Melissa works
  - the virus is activated through a MS word document
  - document displays reference to pornographic websites while macro runs
  - 1st lowers the macro protection security setting for future attacks
  - checks to see is it has run in current session before
    - HKEY_LOCAL_MACHINE\Software\Microsoft\Office\Melissa = “by Kwyjibo”
  - propagates itself using the Outlook MAPI address book (emails sent to the first 50 addresses)

Macro

- How Melissa works
  - infects the Normal.dot template file with it's own code
  - Lastly if the minutes of the hour match up to the date the macro inserts a quote by Bart Simpson into the current document
    - "Twenty two points, plus triple word score, plus fifty points for using all my letters. Game's over. I'm outta here."

Protection/Prevention

- Knowledge
- Proper configurations
- Run only necessary programs
- Anti-virus software

9 Antivirus

1. PANDA

Panda Antivirus combines anti virus and firewall protection to provide robust security with minimal system impact. Optional script blocking and attachment filtering combined with daily updates helps ensure protection against even new and unknown email threats. Downside: cumbersome custom configuration for scans.

2. NORTON ANTIVIRUS

This latest version of Norton Antivirus offers automatic updating combined with script blocking and outbound worm detection. It also includes protection against IM worms and infected attachments sent via America Online, Yahoo!, and MSN instant messenger programs.

Downside: cumbersome custom configuration for scans.

3. F-PROT

The interface is extremely pleasing - easy enough for novice users to navigate yet sophisticated enough for the more advanced. An excellent addition to any antiviral arenal. Downside: like other Top Picks, excluding folders is a cumbersome task. However, erring on the side of protection is never a bad idea.

4. MCAFEE

MCAFEE provides the protection needed in today's hostile computing environment. Script Stopper technology stops VBScript and JScript worms. Hostile Activity Watch Kernel looks for suspicious activity and stops mass-mailing worms.

Downside: Some reports of incompatibility with ZoneAlarm.

5. NORMAN

Norman with configurable email attachment blocking, decompression module, and sandboxing has earned its second top pick award. The new interface helps better integrate the various modules.

Downside: cumbersome custom configuration for scans.

6. PC-CILLIN

With Micro's best-of-breed anti virus protection features an integrated firewall and extends its scanning to include even web-based email. PC-cillin also provides mobile users the extra protection needed to stay virus-free on the road, including Wi-Fi connection security and PDA synchronization protection.

7. BIT DEFENDER

BitDefender Professional provides filtering of URLs, IP addresses, and ports, as well as seamless signature updates every 8 hours. Also protects against viruses encountered through the use of ICQ, Yahoo! Messenger, NetMeeting, or MSN Messenger.

8. NOD 32

Nod32 continues to be a personal favorite. With a tiny footprint, its presence on the system is barely perceptible yet it packs quite a bit of protection. For older systems.

Downside: inability to exclude folders from scanning.

9. STOPzilla

BLOCK annoying popup-windows for good and forever with STOPzilla!

STOPzilla maximizes your surfing speed by guarding your system against annoying unwanted popup windows. With fully customizable options that allow you to configure STOPzilla to meet your surfing needs, you will never again be smothered in an endless sea of pop-ups!

Questions

Lab 2
Yahoo and MSN sniffing