

Viruses, Worms, & Trojan Horses

©July 31, 2004 - material compiled by Bob Carnaghi, www.webpointmorpheus.com

Introduction

This document is one in a series of "Technical White Papers" that attempts to interpret and explain in non-technical language the workings of computers on the Internet. The topic of this document is Viruses, Worms, and Trojan Horses. The presence of these entities within the realm of computers has brought about much grief and expense, and understanding these concepts is crucial to prevention of the effects that they impose. Other documents in this series are mentioned and referenced, and further reading to support the concepts introduced here may be necessary.

Overview

Viruses, Worms, and Trojan Horses are all malicious programs that are purposely written to cause damage to a computer and/or information on the computer. They are also capable of slowing down the Internet, and they can use an individual's computer to spread themselves to friends, family, co-workers, or others. It can be safely stated that an ounce of prevention and some good common sense will go a long way to prevent one from falling victim to these threats. A good metaphor is to compare computer security to locking the front door of a house in order to protect the entire family.

Please keep in mind that the definitions of Viruses, Worms, and Trojan Horses change with their development. A recent ploy of computer virus authors is the combination of two or more viruses together to make a new, stronger virus. The new virus combines the features of each virus into one so that the virus will slip past the antivirus software. It is very important to keep all operating system and antivirus software updated.

Infection Methods

Recent security threats, such as MyDoom, have spread through e-mails disguised as familiar-looking returned-mail error messages. The attached file appeared to be the text of a message recently sent, disguised as a wrong address. However, if opened, one fell victim to the virus. No matter how authentic an e-mail appears to be, know the contents of the attachment before opening it.

Virtually all viruses and many worms cannot spread unless opened or run from an infected program. Worms can spread in insidious manners, but the initial user action is crucial to their deployment.

Detection

Suspicious computer activity is a sign of a virus infection. Consistent computer action beyond the control of the user is to be considered suspicious. If one notices that their email program has just sent out 100 email messages without their consent, there is probably a virus or worm at work.

When one opens and runs an infected program, a contracted virus may not be apparent. The computer may slow down, stop responding, or crash and restart every few minutes. Sometimes a virus will attack the boot files that start the computer. If this is the case, pressing the power button produces only a blank screen.

All of these symptoms are common signs that the computer has become infected by a virus. Another possibility is hardware or software failure, and may have nothing to do with a virus. The symptoms are the same in both cases.

Up-to-date antivirus software installed on the computer is the only sure way to know if there is a virus or not.

Prevention

Although viruses, worms, and Trojan Horses operate differently, there are four main ways to help protect the computer and files:

1. Never open an e-mail attachment from a stranger.
2. Never open an e-mail attachment from known source unless expected, and the contents have been verified.
3. Update antivirus software at least once per week.
4. Keep your operating system software current.

Many of the most dangerous viruses have spread prolifically through e-mail attachments. Viruses, Worms, and Trojan Horses can all be contained in photos, letters written in Microsoft Word, and even Excel spreadsheets. The virus is launched when the file attachment is opened or executed (usually by double-clicking the attachment icon).

If an e-mail arrives with an attachment from an unknown source, delete it immediately. Unfortunately, viruses have the ability to steal the information out of e-mail programs and send themselves to everyone listed in an address book. Even an e-mail from someone familiar can be infected. If an email contains a message that is not coherent, or appears to be gibberish, or has an attachment that wasn't expected, contact the person and confirm the contents of the attachment before opening it.

Beware of messages with a warning that you sent e-mail that contained a virus. A practice known as 'spoofing' permits the forging of return email addresses, and does not mean that the email message came from the origin stated.

Other viruses can spread through programs downloaded from the Internet or from virus-ridden computer disks that were borrowed from friends. Viruses can potentially be contained in the disks bought from a store. These are less common ways to contract a virus. Most viruses come from opening and running unknown e-mail attachments.

Nothing will guarantee the security of a computer 100%. However, by keeping the operating system software up to date, and maintaining a current antivirus software subscription, the chances of remaining virus-free increase dramatically.

Definitions

Virus - A virus is maliciously written code that replicates itself. It may damage hardware, software, or information files. By definition, human interaction is necessary for a virus to spread to another user's files. New viruses are discovered daily.

Most viruses exist simply to replicate themselves. Others can do serious damage such as erasing files or even rendering the computer itself inoperable. Many viruses do a large amount of damage by infecting another program, boot sector, partition sector, or a document that supports macros by inserting itself or attaching itself to that medium.

Worm - A worm is similar to a virus. A worm is designed to copy itself from one computer to another, but it does so automatically (perhaps over a network) by taking control of features on the computer that can transport files or information. This often occurs without the action of humans. Worms are very effective at using e-mail systems and address books to spread. They replicate themselves like viruses, but do not alter files the way that viruses do. The main difference is that worms reside in memory and usually remain unnoticed until their effects become apparent, obnoxious, or overwhelming.

A worm may arrive in the form of a joke program or software of some sort, or by copying itself using email or another transport mechanism. A great

danger of worms is their ability to replicate in great volume. When new worms are unleashed, they spread very quickly, clogging networks and possibly making you wait twice as long to view Web pages on the Internet. This is called a Denial of Service Attack.

The worm may do damage and compromise the security of the computer. Once a worm is in a computer system it can travel alone. Because worms don't need to travel via a "host" program or file, they can tunnel into the system and allow another person to take control of the computer remotely.

To protect against a worm, networked users must keep up with operating system patches and updates as well as anti-virus software, and be aware of any suspicious traffic.

Trojan Horse - A Trojan (or Trojan horse) is a malicious program disguised as a normal application. Trojan horse programs do not replicate themselves like a virus, but they can be propagated as attachments to a virus. Trojan horses cause damage or compromise the security of the computer.

Trojan horses spread when people are lured into opening a program because they think it comes from a legitimate source. But while it runs, it could be allowing "back door" access to the computer by hackers or destroying files on the hard disk. Often an individual emails a Trojan horse-it does not email itself-and it may arrive in the form of a joke program or software of some sort. A recent Trojan horse came in the form of an e-mail that included attachments claiming to be Microsoft security updates, but turned out to be viruses that attempted to disable antivirus and firewall software.

Trojan horses can be included in software that you download for free. Never download software from a source that you don't trust. For protection against a Trojan horse, users must be suspicious of any unknown program and be sure it is safe before running it.

Further Definitions and explanations

Backdoor is a term used to describe a secret or undocumented means of getting into a computer system. Many programs have backdoors placed by the programmer to allow them to gain access to troubleshoot or change the program. Some backdoors are placed by hackers once they gain access to allow themselves an easier way in next time or in case their original entrance is discovered.

Malicious code is a catch-all term used to refer to various types of software that can cause problems or damage a computer. The more common classes

of programs referred to as malicious code are the previously mentioned viruses, worms, Trojan horses, macro viruses, and backdoors. But, malicious code can also be used as a general term to refer to other malicious or destructive programs not covered by those definitions

Heuristics: A method of analysis that uses past experience to make educated guesses about the present. Using rules and decisions based on analysis of past network or email traffic, heuristic scanning in antivirus software can self-learn and use artificial intelligence to attempt to block viruses or worms that are not yet known about and for which the antivirus software does not yet have a filter to detect or block.

Vulnerability: In network security, a vulnerability refers to any flaw or weakness in the network defense that could be exploited to gain unauthorized access to, damage or otherwise affect the network

Firewall: Basically, a firewall is a protective barrier between a computer, or internal network, and the outside world. Traffic into and out of the firewall is blocked or restricted by configuration. By blocking all unnecessary traffic and restricting other traffic to those protocols or individuals necessary, one can greatly improve the security of the internal network.

Denial of Service: A denial of service (DoS) attack floods a network with an overwhelming amount of traffic, slowing its response time for legitimate traffic or grinding it to a halt completely. The more common attacks use built-in "features" of the TCP/IP protocol to create exponential amounts of network traffic

Key Logger: A program placed on a computer to log the keystrokes entered. A hacker then accesses the program to gain account numbers or access illegally.

Spoofing: A method of forging an address in the email system to cloak its true source or sender.

SOURCES:

[University of Hawaii website](#)

[About.com Netsecurity](#)

[Symantec Security Response Documentation](#)

[Microsoft website](#)

Conclusion

This article has covered (briefly and non-technically) the bare essentials of Viruses, Worms, and Trojan Horses. This topic is of a crucial nature, and there are entire sections of the computing industry completely dedicated to dealing with these menaces. The intent of this document has been to inform the reader in a non-technical manner of the generalities of the nature of these entities, and how to prevent oneself from their threat. The ultimate goal has been to edify the reader with enough information to make clear, informed decisions and actions.

Additional

The website process, way the web works, Search Engines, and other web & internet concepts are often very confusing, especially for the typical non-technical person. [webpointmorpheus](http://webpointmorpheus.com) has assembled several documents hoping to simplify these topics. This series of documents are the result of a consistent set of questions posed by current, past, and potential webpointmorpheus clientele. The documents are listed below, and are available online at www.webpointmorpheus.com.

Documents available from [webpointmorpheus](http://webpointmorpheus.com):

- Why Would I Want a Website?
- What's Involved Launching a Website?
- Block view of the Web Site Design Process
- Block View of Typical Web Page Request on the Web
- What is Web Hosting?
- DNS Stands for Domain Name System
- Web & Internet Security Considerations
- E-commerce 101: Is it for me?
- What are Search Engines?
- webpointmorpheus Search Engine Services
- What is PHP Server Side Scripting?
- Databases and the World Wide Web