

Beware of Your Inbox!

Beware of Your Inbox!

Robert B. Fried, BS, MS

Abstract

This paper focuses on Internet and electronic mail based viruses and worms and how they function. Moreover, the languages in which these viruses are written and distributed, specifically Microsoft's Visual Basic Scripting (VBS) and Hyper Text Markup Language (HTML), and examples of each are discussed in detail. In addition, mechanisms for defense and prevention against such viruses and worms are also evaluated.

Introduction

Imagine a plague that only exists virtually. In reality, computer viruses, worms and other forms of malicious code exist; often, they hamper the security of our data and computer related experiences. Recently, a new trend among virus writers has emerged. The utilization of the Internet, specifically the use of electronic mail, has brought about a new and unique generation of computer viruses and worms. The authors of these annoying critters are learning new computer languages and scripts. As a result, virus writers are becoming more clever and creative. Furthermore, viruses and worms are becoming more disguisable.

For Starters

In order to properly understand computer viruses and worms, it is important to accurately define and distinguish them from one another. When one thinks of the term virus, memories of a high school or college biology class probably begin to spark. In humans, "viral infections are spread by the virus (a small shell containing genetic material) injecting its contents into a far larger body cell. The cell is then infected and converted into a biological factory producing replicants of the virus" [1]. Computer viruses operate in a very similar fashion.

There are many known definitions with respect to the term computer virus. However, Dr. Fred Cohen's definition is widely accepted. Cohen asserts that a computer virus is "a program that can 'infect' other programs by modifying them to include a possibly evolved version of itself" [2]. Computer viruses are interesting in that they tend to hide copies of themselves within 'normal running' programs.

Computer worms are different than computer viruses. Computer worms are "programs that can run independently and travel from machine to machine across

network connections; worms may have portions of themselves running on many different machines." Furthermore, it is known that "worms do not change other programs, although they may carry other code that does, such as a true virus" [1]. Although viruses function in different manners, they both have the possibility to become a nuisance and a source of heartache to the users of the computers they infect.

The Evolution of the Internet

Imagine what the world would be like without the presence of the Internet. In 1969, the ARPANET network was installed at the University of California at Los Angeles. Its primary function was to allow for information exchange amongst academic institutions [3]. Its no wonder, a little more than two decades later, such a network evolved globally. Today, the Internet has the capacity and ability to reach billions of individuals in all sectors of society. A simple setup, inclusive of a computer system and a modem/network card will do the job. Although some Internet Service Providers (ISPs) charge subscribers usage fees, there are many (ISPs) that allow users to connect for free. Regardless of the connection method or costs involved; millions of new subscribers are signing onto the Internet each year.

Microsoft's Visual Basic Scripting Language

As the computer community continues to soar, the need for more user-friendly interactive software applications exists. One language that attempts to bridge software applications with the World Wide Web is Microsoft's Visual Basic Scripting. According to Microsoft, Visual Basic Scripting language is a subset of Microsoft's Visual Basic programming language. Visual Basic Scripting language allows for the Microsoft Windows Operating system environment to perform such tasks as "file access, registry manipulation, running other programs, email and Internet access, etc" [4]. These features however, can only be performed if the Windows Scripting Host is installed during the installation of the Windows 98/2000 operating system or Microsoft's Internet Explorer version 5.0 or higher. The Windows Scripting Host allows the operating system execute files written in VBS language [4].

The Birth of Viruses Utilizing VBS Language

Seeing the power within the scripting language, and the potential it gives in terms of exploitation, virus writers decided to use what they knew, in conjunction with what the software had to offer, to have a little fun. Two of the most well known critters written in VBS were VBS/LoveLet-A, which first appeared in May 2000 and VBS/Bubbleboy, which first appeared in November 1999. Although written in the same language, these two critters are distinct in their methods in which they are placed onto a computer system.

VBS/LoveLet-A is a critter that utilizes Microsoft Outlook, an e-mail management program that supports VBS, to propagate. The virus arrives in an e-mail containing various subject headers such as: " ILOVEYOU" and "susitikim shi vakara kavos

puodukui". The message also carries with it an attached file. If only the e-mail message is opened, there is no damage done to the computer. However, if the recipients of the e-mail go as far as downloading and executing the attached file, then they can consider themselves victims.

Victims of VBS/LoveLet-A find that many files containing extensions such as JPEG and MP3 are overwritten and manipulated. Furthermore, the critter utilizes the Internet to allow the computer to send confidential information within the computer to be transferred to an e-mail address. Moreover, the critter utilizes the infected computer user's Microsoft Outlook's address book, to e-mail a copy of itself to all the e-mail addresses that are listed, therefore allowing it to spread [5].

When the first warnings on VBS/LoveLet-A were publicized, proper precautions had been taken by many. However, it is no surprise that VBS/LoveLet-A infected tens of thousands of computer systems. Due to the lack of common sense, on the part of the e-mail recipients, as well as the cleverness of the virus writer, VBS/LoveLet-A found its place in computer virus history.

At first glance, the e-mail message containing VBS/LoveLet-A appears to be from a trust worthy source. The author of the e-mail appears to be an individual with whom the recipient is familiar. As a result, many recipients may deem it safe to open the e-mail, download the attached file and then execute that file. Furthermore, although many computer users are skeptical regarding the downloading of attached files, the way in which critters such as VBS/LoveLet-A cleverly disguise themselves as text files, fools many into thinking the file is safe to execute. Moreover, many people simply become overwhelmed by the curiosity of receiving an e-mail of this nature that they don't think twice as to whether or not the attachment is unsafe. In addition, "many versions of Windows as default strip off the file extension of the file association is known. This resulted in the file appearing to be "LOVE-LETTER-FOR-YOU.txt (leaving out the true VBS file extension), which many user's happily double clicked" [6]. Finally, the icons of a txt and a VBS file within the windows operating system that the average computer user would most likely fail to notice the difference between the two [6].

While, VBS/LoveLet-A involves the user downloading and executing an attached file to infect a computer system, VBS/Bubbleboy does not. In fact, according to Sophos, a leader in anti-virus products, " VBS/BubbleBoy is the first virus to infect users when recipients read an email. It does not depend on the user opening an attachment" [7]. This virus is unique because the HTML file that contains the Visual Basic Script virus is actually embedded within the e-mail message. As a result, a simple motion or click over the hypertext link in Microsoft Outlook, is all it takes for this critter to infect a computer user's system [7].

Once a computer system is infected with the VBS/Bubbleboy, several things follow. The critter places a file within the Windows/Startup directory. The next time the Windows operating system is booted up, the critter edits the system registry files to allow the virus to copy and send itself to all the entries in the computer user's Microsoft

Outlook address book [7]. VBS/Bubbleboy apparently does not do any damage. However, if the user's address book is large enough, the amount of e-mails the critter generates can be large enough to cause severe amounts of traffic on a corporate network server [7].

Classification Confusion?!?!

There are clear and distinct differences within the various types of VBS critters; however, there is still some confusion as to how to go about classifying the various types that exist. Some claim that they should be classified as computer viruses. On the other hand there are many individuals who would argue that they are characteristic of computer worms. Stephen Wing provides some insight regarding this matter.

Wing asserts "a virus is a malicious code that spreads from file to file, usually attaching itself to the host file. It usually requires some user interaction" [6]. On the other hand, "a worm is malicious code that spreads from computer to computer without any user interaction" [6]. Based on Wing's definition of a virus, it is safe to assume that VBS/LoveLet-A is characteristic of a computer virus. Furthermore, Wing's interpretation of a worm, leads one to assume that VBS/Bubbleboy can be classified as a computer worm.

This all seems pretty logical right? Well, according to Fred Kerby, "as the majority require the user to perform some task, e.g. opening an e-mail, these should actually be classified to as viruses" [6]. However, the virus companies don't share this belief. "Some virus manufacturers such as Sophos and Symantec class most VBS malware as worms, do to that fact that these 'viruses' do not infect other files, only the computer itself" [6]. No matter how VBS malware is classified, one thing is certain; these types of critters can all be categorized under 'annoyance'.

Hyper Text Markup Language

Hyper Text Markup Language (HTML) is utilized for publishing hypertext in cyberspace. This language is based upon the Standard Generalized Markup Language (SGML). Documents containing HTML, such as websites, can be created with the help of web authoring tools found within many popular software suites. As the Internet continues to expand, many new deviations of HTML such as What You See is What You Get (WYSIWYG) are being developed [8]. Furthermore, because of the popularity of the Internet, many virus writers are utilizing HTML to create new critters.

The Birth of Viruses Utilizing HTML

Its no wonder that within time the language of the web would become exploited. The first of the so-called HTML viruses appeared in November 1998. To help better

understand the nature of such viruses and their potential threats, it is important to discuss the three well-known viruses of this kind: HTML/Internal, HTML/Prepend.1670 and HTML/ReDirect.

HTML/Internal was the first HTML to be discovered. It can be viewed as a rather simple virus. Essentially, the virus is transmitted to a computer user who has visited a particular website. However, accessing the website does not do any harm to the visitor's computer. The virus will only begin to impact a computer system if the Microsoft Explorer's security features are improperly configured. If this is the case and the computer user clicks a dialog box that grants permission to view the content on the site, that user has just fallen into the trap. What the website visitor probably didn't know was that the web site contains inline script routines written in Visual Basic [9]. With the virus now on that user's system, the virus begins to unload. Basically, what happens is that when run from the local hard drive, the virus' visual basic script contains instructions to allow the virus to overwrite files on the infected user's computer hard drive. The files that become affected are those that are in the same directory as the virus and that are written in HTML format [4]. Although, the virus does a little tinkering with the files on the infected computer, this virus is not viewed as a serious threat [4].

Why stop when your having fun? This was probably the question in the mind of the author who created HTML/Internal. So, what did this virus writer do? He created HTML/Prepend.1670. This virus is not very different than its predecessor. Classified as a "true prepending virus", HTML/Prepend.1670 operates in a very similar fashion to HTML/Internal. A prepending virus is one that attaches itself to the beginning of files. As is the case with HTML/Internal, this particular virus does not appear to be a serious threat [10]

Some virus writers just can't get enough. Probably wanting to gain more attention than fame, the virus writer decided to create another critter. HTML/Redirect is deemed a "companion type" virus. Again, this virus operates in a very similar manner to both HTML/Internal and HTML/Prepend.1670. A companion virus is one that infects a file type by renaming it and copying it to the program, which this file uses to execute itself. It should also be noted that this virus does not appear to be a serious threat [10].

As a result in the similarities between the viruses discussed, it was not important to go through the latter of the two. However, in discussing HTML/Internal an important point was made. It was noted that the virus was in the form of an HTML file; however, the virus actually operates according to VBScripts contained within that file. In reality, "an 'HTML virus' is distributed in an HTML and targets files of this format, but its code is written in VBScript and not in the HTML language itself. This means that these viruses will affect users of browsers supporting VBScript written code - i.e. mainly those running Internet Explorer" [10]. Although, these viruses appear to be no serious threat at this time, it is uncertain what dangers the future will bring as computer languages are integrated with one another.

Mechanisms of Defense

In his textbook *A Short Course on Computer Viruses*, Dr. Fred Cohen provides a solution to the computer virus epidemic. Cohen asserts that if computer users eliminate certain high-risk activities then they can consider themselves immune to computer virus infection. According to Cohen, high-risk activities include: sharing, programming and changes [11]. In an ideal and perfect world this may be achieved. However, in reality, people need and want computers to perform all these tasks. As a result, mechanisms for defense need to be created.

Mechanisms of Defense for VBS Viruses and Worms

When one begins to think of how to prevent viruses in general, the first thing that comes to mind is the utilization of anti-virus software. As more and more individuals begin to venture off into cyberspace the need for viral protection is essential. Anti-virus software aids in the detection and prevention of computer viruses. However, anti-viral software programs are only effective if they are regularly updated [6].

Anti-virus software should not be a computer user's only means of defense against a computer virus. Computer viruses can hit the computer community at any time. Authors of viruses can decide to unleash their critters at any time. With all the new types of viruses and languages being used to create viruses these days, it is hard to be one hundred percent immune. Many anti-virus programs do their best in trying to keep up with the never-ending battle. Although, these companies try to update their products whenever a potentially threatening virus is expected to appear, they may not always be able to find the antidote before the virus strikes. Furthermore, although many anti-virus companies claim to update their virus definitions regularly, there may still be some uncertainty as to the effectiveness of the product. This uncertainty existed when several VBS viruses and worms first appeared. It is known that at least one anti-virus company was known to have updated their virus libraries to include VBS viruses/worms; however, the mechanisms utilized to help detect these viruses were never added to the product. As a result, virus writers got busy and created even more viruses of this sort [6].

So, if computer users shouldn't fully trust anti-virus packages, what other options for defenses are available? Well, many anti-virus vendors, governmental agencies and other related organizations exist to help keep the computer community informed and alert. Preparation and awareness are vital components in fighting any battle.

In trying to help fight the battle against VBS viruses, Microsoft has issued many patches, which fix some of the vulnerabilities that exist in many of their products utilizing Visual Basic Scripting Language. One such patch, "scriptlet.TypeLib/EyeDog", eliminates the security vulnerability within Microsoft Internet Explorer. With this patch, automatic execution of e-mails as seen in VBS/Bubbleboy will be prevented. Furthermore, Microsoft also issued a patch, the Outlook E-mail Security Update, to prevent the sending or receiving of potentially threatening executable files. Unfortunately, this patch does not fully compatible with several other e-mail management programs on the market [6].

Besides anti-virus software and vendor issued patches, there are other ways to prevent infection by a VBS virus or worms. User manipulation of system settings and configurations can also help defend against these critters. For example, the user can allow for file extensions to appear within the Windows environment. Furthermore, many users can make use of utilities that help to detect the presence of VBS files attached to an e-mail message. Moreover, users can eliminate the Windows Scripting Host, which is automatically placed onto a system during the installation of Windows and newer versions of Internet Explorer. If users are still uncertain as to whether their systems are vulnerable, all associations of VBS files with Windows should be deleted [6].

Mechanisms of Defense for HTML Viruses

Members of the anti-virus industry claim that HTML viruses pose no serious threat. However, these critters are still considered an annoyance and should proper measures should be taken to avoid infection. The first phase of defense is to increase the level of security within Microsoft's Internet Explorer web browser. Research shows that the virus is specific to only Internet Explorer and not the competitor, Netscape Navigator/Communicator. Allowing for a stricter security setting allows for more user interactivity in regards to information being downloaded onto a computer system while on the World Wide Web. For, those who do not wish to sacrifice their ability to conveniently browse the web, using common sense is recommended. If an unfamiliar dialog box appears, the user should not be quick to click. Taking these precautions, as well as the utilization of an up to date anti-virus program, infection by HTML viruses can be easily avoided [4].

Summary, Conclusions, and Further Work

It is evident that computer languages utilized by and integrated with the Internet are being exploited. Virus writers are finding ways to write viruses using Visual Basic Scripting. Virus writers are using Hyper Text Markup Language to distribute these critters. Mechanisms of defense in helping to prevent infection from such viruses/worms are currently available. Some require the addition of a patch or the manipulation of system files; while others require the use of anti-virus program.

The use of common sense is probably the best defense against computer viruses of this sort. Virus writers prey on those computer users that are most vulnerable. These people are the types of individuals who are joining the computer community each day. As the masses continue to sign on to the cyberspace and continue to prevent the stop of sharing, programming and transitivity, viruses will continue to plague the computer world.

In an article entitled "the Future of Viruses on the Internet, by David Chess, a member of IBM Research Team, the role of the Internet in regards to spreading viruses is discussed. According to Chess, "The Internet currently plays a comparatively small role in the spread of viruses. No common virus today is network-aware; all of them require

help (generally accidental help) from users in order to spread" [12]. Chess' words speak so much truth.

So, what can be done to aid in the prevention of such viruses and the exploitation of Internet associated languages? The answer is rather complex. There needs to be a network of individuals from corporate, public, private, and academic sectors of society. This network of individuals will help to effectively communicate the needs and concerns of each represented group. It would be through this network that people could gain information and education in regards to various types of vulnerabilities that exist in the computer world.

There is still much research to be done. New viruses are being created daily. Virus writers are becoming more curious and clever. Software and computer language exploitation is on the rise. The computer community continues to grow with each passing day. The technology of today should be experienced with as little annoyances as possible. Computer viruses won't go away anytime soon. Until an antidote is found, think before you click. Most importantly, beware of your inbox!

References:

[1] Denning, Peter J. "A Computer Virus Primer." Computers Under Attack: Intruders, Worms, and Viruses. ACM Press, 1990, ISBN 0-201-53067-8, pages 316-355.

[2] Cohen, Fred. "How Does a Virus Spread Through a System." A Short Course On Computer Viruses. ASP Press, 1990, ISBN 1-878109-01-4, page 11.

[3] Denning, Peter J. "The Worldwide Network of Computers." Computers Under Attack: Intruders, Worms, and Viruses. ACM Press, 1990, ISBN 0-201-53067-8, page 01.

[4] <http://www.avertlabs.com/public/datafiles/valerts/vinfo/htmvir.asp>

[5] <http://www.virusbtn.com/VirusInformation/lovelet.html>

[6] Wing, Stephen. "Why and How Do They Spread So Quickly?" <http://www.sans.org/infosecFAQ/malicious/VBS.htm>

[7] <http://www.sophos.com/virusinfo/articles/bubbleboy.html>

[8] <http://www.w3.org/MarkUp/>

[9] <http://www.avp.ch/avpve/script/INTERNAL.stm>

[10] <http://www.vet.com.au/html/faq/faq/FAQ-SCANNING-208.html>

[11] Cohen, Fred. "High Risk Activities." A Short Course On Computer Viruses, ASP Press, 1990, ISBN 1-878109-01-4, page 34.

[12] Chess, David. "The Future of Viruses on the Internet".
<http://www.research.ibm.com/antivirus/SciPapers/Chess/Future.html>

About the Author

Robert Fried holds a B.S. and an M.S. in Forensic Science with a concentration in Advanced Investigation. He also holds Certificates in Law Enforcement Science, Forensic Computer Investigation, and Information Protection and Security from the University of New Haven and SEARCH. Fried has extensive knowledge of forensic science, however, most recently he has worked extensively in the developing field of "digital forensics" and has published in this area by organizations such as the SANS Institute. He is also a member of the NorthEast chapter of the High Technology Crime Investigation Association (HTCIA).