



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

"ILOVEYOU" Worm

Tracey Whalen

September 9, 2000

Computer viruses and worms have probably become the most widely known Security problem dealing with computers. They have inundated news stories of top wire companies. ⁽⁷⁾ They can wreak havoc and affect the work force, and are always changing in order to bypass current anti-virus software. One of the most wide spread worms that caused damage to date was the Love Letter; along with its variants, Love Bug, Very Funny, and Mothers Day. ^(1, 7, 9)

According to sources, there were over 29 versions of this worm, ⁽⁷⁾ which affected at least 650 different sites and over 500,000 individual systems. ⁽¹⁾ This program not only damaged systems, it also caused network degradation. ⁽¹⁾ The worm was a Visual Basic script and spread through the world within hours of its release. ^(6, 7)

Overview

The Love Letter Worm was reported to anti-virus agencies by early morning on May 4, 2000. ⁽⁸⁾ Unlike other worms, which cause damage to one file, the ILOVEYOU worm caused damage to many areas of each machine it infected. Many people called the Love Letter a virus, but it was actually a worm. Defining the term 'worm' and differentiating it from virus is important. According to Symantec, "worms replicate from one machine to many others, using a network medium (e.g. email or TCP/IP). The goal of a worm is to infect as many machines on a network as possible." ⁽⁷⁾ A virus, on the other hand, needs "human help" to propagate a malicious code. ⁽⁷⁾

The ILOVEYOU worm spread and contaminated the machines of its victims primarily through email. The recipient of an email would receive a subject line of "ILOVEYOU" ^(1, 6, 7, 9) from someone they knew (it was automatically propagated through address books of its victims). There was also an attachment named "LOVE-LETTER-FOR-YOU.TXT.VBS" with the text of the message stating "kindly check the attached LOVELETTER coming from me" ^(1, 6, 8). The attachment would be launched, which would cause the following problems:

1. Opening the attachment replaced files using the following extensions: .vbs, .vbe, .js, .jse, .css, .wsh, .sct, .hta, .jpg, .jpeg, .wav, .txt, .giv, .doc, .htm, .html, .xls, .ini, .bat, .com, .mp3, and .mp2. ^(1, 6, 7) *Note that the .mp3 and .mp2 files are not replaced or deleted, they just become hidden. ^(1, 3, 4, 6, 7, 9)
2. Opening the attachment created a mIRC Script to send the virus to any user that does not have a script.ini file. ^(1, 2, 6, 7, 9)
3. Modification of the "Start" page in Internet Explorer to send the user to a URL that provides them with another damaging file "WIN-BUGSFIX.EXE". ^(1, 6, 9)
4. Sends copies of the original message to EVERYONE within an Outlook email account. ^(1, 2, 5, 6, 7, 9)
5. Modifies Registry settings including: ^(1, 6, 8)

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32

HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Win32DLL

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX

HKCU\Software\Microsoft\Windows Scripting Host\Settings\Timeout

HKCU\Software\Microsoft\Internet Explorer\Main\Start Page

HKCU\Software\Microsoft\WAB*

The worm spread quickly as users address books were copied and all their recipients address books were copied, etc. In fact, during that time any file shared or sent with the affected extensions mentioned previously would also spread the virus. Social engineering also played a hand in the spread of this worm. The "Love Letter" subject sent by someone the recipient knew would entice the recipient to open the message and attachment ^(4, 7). One user from the German computer gaming magazine PC Player was quoted on May 4 as saying "This morning at 10:37 am, I received a mail with the subject ILOVEYOU. Everybody wants to be loved, so I opened it, revealing the message

'kindly check the attached LOVELETTER coming from me' plus a little image with a gray tilde. No macro virus, no executable file – can't be a virus. Wrong!" (2)

Clean Up

Most of the "clean-up" needed after the virus was publicized came through anti-virus software. Due to the destructive nature of this worm, separate software was needed to flush out the worm from the system and restore the registry settings to what they needed to be. The following are some of the different companies that provided solutions to the "ILOVEYOU" bug: Alladin Knowledge Systems, Command Software Systems, Computer Associates, F-Secure, Finjan Software, McAfee/Network Associates, Proland Software, Sophos, Symantec, and Trend Micro. (1, 6, 9)

Although the worm was targeted primarily at Microsoft products (Internet Explorer, Microsoft Outlook, Microsoft registry keys, etc.), it did affect other systems such as UNIX and MAC. Although these systems were not affected as badly as Microsoft, if an infected file was sent to a UNIX or MAC user, they could potentially spread the virus by forwarding an infected file to someone else.

Protecting Against Worms

How can we stop the spread of worms? It seems it will get worse before it gets better. According to Symantec, worms will probably become more widespread than viruses' (8). Possible suggestions for reducing the amount of damage caused by worms include keeping anti-virus protection up to date, planning, implementing, and maintaining malicious code detection on networks and hosts attached to the internet, and Intrusion Detection when and where available. (8) As worms increase in complexity and speed, technology will have to grow as well. Keeping up to date with Security Advisories and trends will help reduce the damage a worm can cause. Unfortunately, anti-virus software and IDS systems are more defensive than offensive in nature. Therefore they can only react to a new worm, not prevent a new code. Most proactive stances any individual user or corporation can take are the best defense they can have. Proactive stances include Security advisories, updated software, education of users, and policies written and adhered to for types of software, use of, and reactions to virus and worms.

References

1. CERT Advisory. "CERT Advisory CA-2000-04 Love Letter Worm." 4 May 2000. URL: <http://www.cert.org/advisories/CA-2000-04.html> (September 8, 2000).
2. Finley, Michelle. "Techies: Victims of Love." 4 May 2000. URL: <http://www.wired.com/news/lovebug/0,1768,36125,00.html> (September 8, 2000).
3. King, Brad. "Love Bug Only Hides MP3s." 5 May 2000. URL: <http://www.wired.com/news/lovebug/0,1768,36164,00.html> (September 8, 2000).
4. King, Brad. "Love Bug: The Conspiracy." 6 May 2000. URL: <http://www.wired.com/news/lovebug/0,1768,36166,00.html> (September 8, 2000).
5. Reuters. "Suspect Charged in Love Bug Case." 8 September 2000. URL: <http://www.wired.com/news/lovebug/0,1768,37322,00.html> (September 8, 2000).
6. Symantec. "'ILOVEYOU' Worm Wreaks Havoc Worldwide." 16 May, 2000. URL: <http://enterprisesecurity.symantec.com/article.cfm?articleid=97.html> (September 9, 2000).
7. Symantec. "VBS.LoveLetter.A." 9 May 2000. URL: <http://www.symantec.com/avcenter/venc/data/vbs.loveletter.a.html> (September 8, 2000).
8. Symantec. "Worms and Your Network" 29 August 2000. URL: <http://enterprisesecurity.symantec.com/article.cfm?articleid=245> (September 9, 2000).
9. Trend Virus Encyclopedia. "VBS_Loveletter." 4 May 2000. URL: http://www.antivirus.com/vin...sencyclo/default5.asp?Vname=VBS_LOVELETTER.html (September 8, 2000).

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive