CERT Advisory CA-2000-04 Love Letter Worm

Original release date: May 4, 2000
Last revised: May 9, 2000
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Microsoft Windows with Windows Scripting Host enabled

Overview

The "Love Letter" worm is a malicious VBScript program which spreads in a variety of ways. As of 5:00 pm EDT(GMT-4) May 8, 2000, the CERT Coordination Center has received reports from more than 650 individual sites indicating more than 500,000 individual systems are affected. In addition, we have several reports of sites suffering considerable network degradation as a result of mail, file, and web traffic generated by the "Love Letter" worm.

I. Description

You can be infected with the "Love Letter" worm in a variety of ways, including electronic mail, Windows file sharing, IRC, USENET news, and possibly via webpages. Once the worm has executed on your system, it will take the actions described in the
Impact section.

Electronic Mail

When the worm executes, it attempts to send copies of itself using Microsoft Outlook to all the entries in all the address books. The mail it sends has the following characteristics:

- An attachment named "LOVE-LETTER-FOR-YOU.TXT.VBS"
- A subject of "ILOVEYOU"
- The body of the message reads "kindly check the attached LOVELETTER coming from me."

People who receive copies of the worm via electronic mail will most likely recognize the sender. We encourage people to avoid executing code, including VBScripts, received through electronic mail regardless of the sender without firsthand prior knowledge of the origin of the code.

Internet Relay Chat

When the worm executes, it will attempt to create a file named *script.ini* in any directory that contains certain files associated with the popular IRC client mIRC. The script file will attempt to send a copy of the worm via DCC to other people in any IRC channel joined by the victim. We encourage people to disable automatic reception of files via DCC in any IRC client.

Executing Files on Shared File Systems

When the worm executes, it will search for certain types of files and replace them with a copy of the worm (see the Impact section for more details). Executing (double clicking) files modified by other infected users will result in executing the worm. Files modified by the worm may also be started automatically, for example from a startup script.

Reading USENET News

There have been reports of the worm appearing in USENET newsgroups. The suggestions above should be applied to users reading messages in USENET newsgroups.

II. Impact

When the worm is executed, it takes the following steps:

Replaces Files with Copies of the Worm

When the worm executes, it will search for certain types of files and make changes to those files depending on the type of file. For files on fixed or network drives, it will take the following steps:

- For files whose extension is *vbs* or *vbe* it will replace those files with a copy of itself.
- For files whose extensions are *js*, *jse*, *css*, *wsh*, *sct*, or *hta*, it will replace those files with a copy of itself and change the extension to *vbs*. For example, a file named *x.css* will be replaced with a file named *x.vbs* containing a copy of the worm.
- For files whose extension is *jpg* or *jpeg*, it will replace those files with a copy of the worm and add a *vbs* extension. For example, a file named *x.jpg* will be replaced by a file called *x.jpg.vbs* containing a copy of the worm.
- For files whose extension is *mp3* or *mp2*, it will create a copy of itself in a file named with a *vbs* extension in the same manner as for a *jpg* file. The original file is preserved, but its attributes are changed to hidden.

Since the modified files are overwritten by the worm code rather than being deleted, file recovery is difficult and may be impossible.

Users executing files that have been modified in this step will cause the worm to begin executing again. If these files are on a filesystem shared over a local area network, new users may be affected.

Creates an mIRC Script

While the worm is examining files as described in the previous section, it may take additional steps to create a mIRC script file. If the file name being examined is *mirc32.exe*, *mlink32.exe*, *mirc.ini*, *script.ini*, or *mirc.hlp*, the worm will create a file named *script.ini* in the same folder. The *script.ini* file will contain:

```
[script]

n0=on 1:JOIN:#:{
n1=  /if ( $nick == $me ) { halt }
n2=  /.dcc send $nick DIRSYSTEM\LOVE-LETTER-FOR-YOU.HTM
n3=}
```

where DIRSYSTEM varies based on the platform where the worm is executed. If the file *script.ini* already exists, no changes occur.

This code defines an mIRC script so that when a new user joins an IRC channel the infected user has previously joined, a copy of the worm will be sent to the new user via DCC. The *script.ini* file is created only once per folder processed by the worm.

Modifies the Internet Explorer Start Page

If the file *\WinFAT32.exe* does not exist, the worm sets the Internet Explorer Start page to one of four randomly selected URLs. These URLs all refer to a file named *WIN-BUGSFIX.exe*, which presumably contains malicious code. The worm checks for this file in the Internet Explorer *downlo ads* directory, and if found, the file is added to the list of programs to run at reboot. The Internet Explorer Start page is then reset to "about:blank". Information about the impact of running *WIN-BUGSFIX.exe* will be added to this document as soon as it is available.

Sends Copies of Itself via Email

The worm attempts to use Microsoft Outlook to send copies of itself to all entries in all address books as described in the Description section.

Modifies Other Registry Keys

In addition to other changes, the worm updates the following registry keys:

```
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\*
```

Note that when the worm is sending email, it updates the last entry each time it sends a message. If a large number of messages are sent, the size of the registry may grow significantly, possibly introducing additional problems.

III. Solution

Update Your Anti-Virus Product

It is important for users to update their anti-virus software. Some anti-virus software vendors have released updated information, tools, or virus databases to help prevent and combat this worm. A list of vendor-specific anti-virus information can be found in Appendix A.

Disable Windows Scripting Host

Because the worm is written in VBS, it requires the Windows Scripting Host (WSH) to run. Disabling WSH prevents the worm from executing. For information about disabling WSH, see:

http://www.sophos.com/support/faqs/wsh.html

This change may disable functionality the user desires. Exercise caution when implementing this solution.

Disable Active Scripting in Internet Explorer

Information about disabling active scripting in Internet Explorer can be found at:

http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps

This change may disable functionality the user desires. Exercise caution when implementing this solution.

Disable Auto-DCC Reception in IRC Clients

Users of Internet Relay Chat (IRC) programs should disable automatic reception of files offered to them via DCC.

Filter the Worm in E-Mail

Sites can use email filtering techniques to delete messages containing subject lines known to contain the worm. For sites using unix, here are some possible methods:

Sendmail

Sendmail, Inc. has published information about blocking the worm in incoming email at:

http://www2.sendmail.com/loveletter

PostFix

Add the following line in /etc/postfix/header_checks:

```
/^Subject: ILOVEYOU/ REJECT
```

The main Postfix configuration file must contain the following line to enable the check :

header_checks = regexp:/etc/postfix/header_checks
Postfix must also be reloaded after this information is added.

Exim

A generic Windows-executable content-blocking filter has been produced for Exim. This will block messages with attachments whose extensions are *vbs*, as well as several other types that Windows may consider executable by default. The filter, which includes some supporting installation documention within the filter file itself, can be found at:

ftp://ftp.exim.org/pub/filter

Procmail

This procmail rule also deletes any messages with the Subject: line containing "ILOVEYOU":

```
:0 D
* ^Subject:[[tab] ]+ILOVEYOU
/dev/null
```

Note that in all of these examples, [tab] represents a literal tab character, and must be replaced with a tab for them to work correctly.

It is important to note that these three methods, as described, do not prevent the worm from spreading if the Subject: line of the email has changed. Administrators can use more complicated procmail rules to block the worm based on the body of the email, but such methods require more processing time on mail servers, and may not be feasible at sites with high volumes of email traffic.

Exercise Caution When Opening Attachments

Exercise caution with attachments in email. Users should disable auto-opening or previewing of email attachments in their mail programs. Users should never open attachments from an untrusted origin, or that appear suspicious in any way.

Appendix A. Anti-Virus Vendor Information

Aladdin Knowledge Systems

http://www.aks.com/home/csrt/valerts.asp

Command Software Systems, Inc.

http://www.command.co.uk/html/virus/love.html
http://www.commandcom.com/virus/love.html

Computer Associates

http://www.ca.com/virusinfo/virusalert.htm

F-Secure

http://www.f-secure.com/download-purchase/updates.html

Finjan Software, Ltd.

http://www.finjan.com/attack_release_detail.cfm?attack_release_id=34

McAfee / Network Associates

http://vil.nai.com/villib/dispVirus.asp?virus_k=98617
http://www.cert.org/advisories/CA-2000-04/nai.dat

Proland Software

http://www.pspl.com/virus_info/worms/loveletter.htm

Sophos

http://www.sophos.com/virusinfo/analyses/vbsloveleta.html
http://www.sophos.com/virusinfo/analyses/trojloveleta.html

Symantec

http://www.symantec.com/avcenter/venc/data/vbs.loveletter.a.html

Trend Micro

http://www.antivirus.com

A

The CERT Coordination Center has received reports of worm

J

o

This variant changes several refer

encesto*LOVE-LETTER-FOR-YO*inthesourcecodeto*VeryFunny*.Thisprim*VeryFunny.vbs*.Theem

The subject of this variant is "Thanks for your purchase!" and the body of the em