TOP 10 VIRUSES :

1. W32.Navidad
2. W95.MTX
3. W32.Hybris
4. VBS.KakWorm
5. VBS.LoveLetter Family
6. W97M.Melissa.BG
7. W32.Prolin
8. W97M.Marker Family
9. W32.Funlove
10. W95.CIH

Common Name(s):	The Love Bug, I loveYou
Aliases:	VBS.LoveLet.A, VBS.Lovel, I- Worm.LoveLetter, VBS.LoveLetter.A@mm.Worm
Variants:	*Please refer to the Variants sectior*
Type:	Visual Basic Script worm
Author:	Unknown
Discovered:	05/04/2000
Origin:	Manila, Philippines
Risk:	High
Damage:	High
Distribution:	High
Encrypted:	No
Resident:	No
Stealth:	No
Vulnerable:	Windows 95/98/NT/2000
Profile Updated:	11:00PM GMT 05/05/2000

Infection

The worm itself is a 10KB Visual Basic Script named LOVE-LETTER-FOR-YOU.TXT.vbs. As with any other VBS worm, a user must manually trigger VBS.LoveLetter.A by running the script.

Affected Systems

The worm runs using the WSH (Windows Scripting Host) program, which is installed by default in Windows 98 and Windows 2000. WSH is not normally present on Windows 95 or Windows NT unless Internet Explorer 5 is installed. On any Windows platform, it is possible to disable WSH, in which case the worm is rendered harmless.

Local Self-Distribution

When the worm is first run it drops copies of itself in the following places:
C:\WINDOWS\WIN32DLL.VBS
C:\WINDOWS\SYSTEM\LOVE-LETTER-FOR-YOU.TXT.VBS
C:\WINDOWS\SYSTEM\MSKERNEL32.VBS
It then creates a number of registry entries to execute these programs when the machine restarts. These entries are:
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
MSKernel32=C:\WINDOWS\SYSTEM\MSKernel32.vbs
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
Win32DLL=C:\WINDOWS\Win32DLL.vbs

Downloading a Trojan

The worm then tries to download and install an executable file called WIN-BUGSFIX.EXE from the Internet. In order to facilitate this download the worm sets the start-up page of Microsoft Internet Explorer to point to the web page containing the password stealing trojan. It randomly selects on of the four following URL's:

http://www.skyinet.net/~young1s/JKhjn... ...jbvYT/WIN-BUGSFIX.exe
http://www.skyinet.net/~angelcat/kladj... ...kqj4w/WIN-BUGSFIX.exe

http://www.skyinet.net/~koichi/f6TRj... ...3Vbvg/WIN-BUGSFIX.exe
http://www.skyinet.net/~chu/dgfhj... ...7thjg/WIN-BUGSFIX.exe

According to Ronald Elciaro, a network administrator with Skyinet.net, the above web pages have been taken down. Further, the Phillipines based ISP has been out of service for most of today. Theoretically though, when a newly infected user runs Internet Explorer for the first time, they would automatically begin the process of downloading WIN-BUGSFIX.EXE, otherwise known as Troj.LoveLetter.A, a trojan horse password stealer.

Troj.LoveLetter.A

When this trojan is first run, it creates the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
WinFAT32=C:\WINDOWS\SYSTEM\WinFAT32
The trojan then copies itself to \Windows\System\ directory as WINFAT32.EXE and then runs the file from that location. The above registry key modification makes the trojan become active every time Windows starts.
When run, the trojan attempts to send an email containing information on the user's hostname, username, host IP address, remote access passwords, and cache passwords to a Phillipine email account.

Housecleaning

The next time the worm is executed, it will skip over the portions of code that attempt to download the trojan. Instead, it sets the following registry key so that WIN-BUGSFIX.EXE is always run on startup:
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ WIN-BUGSFIX=downread&"\WIN-BUGSFIX.exe
Then it cleans up after itself by changing the Internet Explorer startup page to blank via the following registry key:
HKCU\Software\Microsoft\Internet Explorer\Main\ Start Page=about:blank

Infecting Files

The worm then attempts to infect select files on all local and networked drives. The worm replaces the following files with copies of itself and it adds the extension .VBS to the original filename:
*.JPG *.JPEG *.MP3 *.MP2
The worm also overwrites the following files with copies of itself and renames the files' extensions to .VBS:
*.VBS *.VBE *.JS *.JSE *.CSS *.WSH *.SCT *.HTA

Infecting Email

The email component of the worm is only functional if Microsoft Outlook is present.

If so, after a short delay, the worm uses MAPI calls to Outlook and creates messages by iterating through all the address in the Microsoft Outlook Address Book. The worm marks these recipients using the registry in attempt to only send them the mail once.

The subject of the email is: ILOVEYOU

The body of the email is: kindly check the attached LOVELETTER coming from me.

Attached to the email is the 10KB file: LOVE-LETTER-FOR-YOU.TXT.vbs

Since the attachment has a "double extension", mailers which suppress well-known extensions such as .vbs may present this file as LOVE-LETTER-FOR-YOU.TXT, which appears more innocent.