VIRUS ANALYSIS 1

When Love came to Town

Nick FitzGerald
Computer Virus Consulting, New Zealand

Few virus dates really stick in my mind. 6 March is the annual reminder of the Michelangelo fiasco. 26 April has been 'CIH day' for a couple of years, but will not last. 26 March 1999 delivered Melissa madness whose importance may be more enduring than CIH's.

After dining with my parents and spending a couple of hours trying to fix a knotty problem with their PC and printer, 4 May 2000 seemed fairly ordinary. Arriving home, however, everything changed. There were more than 200 new messages in alt.comp.virus. I had 120–130 new email messages – the number I receive overnight on a really busy day, virus-wise, in the Northern Hemisphere. Something was clearly afoot …

Give Me Good Loving

That much correspondence typifies a 'normal day'. Why had it been generated in the time I was away from my computers – approximately four hours? Further, these were the 'early-through-mid-morning' hours in Europe – the US East Coast was just rising and barely anyone was at work there yet. Most of the message flood was about a new, mass-mailing, VBS virus being referred to as ILOVEYOU, LoveLetter and, particularly in the media, 'the Love Bug'. At four hours old it was a media darling already!

From much of this early reporting, things sounded dire and the virus seemed to have spread further and much faster than Melissa. The half dozen samples in my email were all the same and a quick glance at the code showed it was straight, standalone VBS script. This was something of a relief as it ruled out a few suggestions already floating around that LoveLetter may have been 'Kak on steroids'.

The rest, as they say, is history. By the time you read this, much more of the LoveLetter story will have unfurled, as this was written a bare week after love came to town. Now the *FBI* and other such agencies have made their arrests and are talking about the possibility of extradition. The authorities in the Philippines, where the writer(s) of LoveLetter reside, are struggling to find suitable laws to charge the suspects with breaking. With these interesting elements yet to unfold, and the best part of three columns yet to fill, I had better get into the analysis.

What is this Thing called Love?

About thirty LoveLetter variants existed when this article was submitted. Specific details in this analysis, such as file names, are those of VBS/LoveLetter.A and are different in some variants. As a virus, LoveLetter is a trivial VBS overwriter with most variants also including two methods to transfer themselves to other hosts. One of these is a mass email routine very similar to that of Melissa. The other distribution mechanism is via DCC file transfers on IRC, if an infected machine runs the popular *mIRC* client. Some variants retain only one of these functions.

Although not necessitated by its dual distribution approach, LoveLetter transfers its code in different forms with each method – as a VBS file attached to email and as a script embedded in an HTML file over IRC. Neither transfer mechanism results in the virus automatically being run on recipient machines. As with traditional viruses and most recent mass-mailers, the victim must deliberately run the virus – be it the VBS attachment from an email message, or the HTML file received via IRC.

When the VBS form of the virus is run, the script copies itself to the files MSKERNEL32.VBS and LOVE-LETTER-FOR-YOU.TXT.VBS in the *Windows* system directory and to the file Win32DLL.VBS in the *Windows* installation directory. Two of these are set to run at startup and log-in by creating the Registry values MSKernel32 and Win32DLL in the Run and RunServices keys respectively, under the … \Software\Microsoft\Windows\CurrentVersion key. The Registry value … \Software\Microsoft\Windows Scripting Host\Settings\Timeout is set to zero if it is greater than or equal to one. Zero is the default timeout value, and prevents the scripting host from aborting a script, no matter how long it runs. If *Internet Explorer's* (*IE*) 'Download Directory' setting is not configured, it is set to 'C:\'. This is important to one of LoveLetter.A's payloads.

An HTML form of the virus' code is also written to the file LOVE-LETTER-FOR-YOU.HTM in the system directory. This is a dropper for the main VBS form of the virus. Few of the variants have modified this aspect of LoveLetter.A, apart from removing the function altogether. Thus, most variants retaining this function drop and spread the .A variant that spreads via *mIRC*.

When run in its standalone VBS form, LoveLetter also traverses the directories of all non-removable and network drives overwriting VBS and VBE files with copies of itself. This is its main viral replication mechanism. Meanwhile, it looks for MIRC32.EXE, MLINK32.EXE, MIRC.INI, SCRIPT.INI and MIRC.HLP. When any of these files are found, a SCRIPT.INI is created in the file's directory and a sequence of *mIRC* scripting commands written to it. This causes LOVE-LETTER-FOR-YOU.HTM to be sent via DCC to others joining the infected user's current IRC channel. A series of comments suggest *mIRC's* author wrote the script and that system problems will arise if it is altered – an attempt to dissuade the inquisitive but naïve.

Love Hurts

LoveLetter has several payloads. One attempts to install a password-stealing Trojan Horse. Fortunately, this program was removed from the hosting Philippino ISP early in the outbreak and few infected users saw this payload succeed. Removal of those files has prompted some of the variant makers to delete this functionality from the VBS script code. If present, the function checks the existence of WinFAT32.EXE in the *Windows* system directory. If it is not there, one of four URLs to WIN-BUGSFIX.EXE on www.skyinet.net is randomly chosen and *IE's* 'start page' is set to that URL. However, if the file WIN-BUGSFIX.EXE exists in *IE's* download directory, the Registry is altered to run it at startup and the *IE* start page is set to a blank page.

In changing the default *IE* start page, LoveLetter expects the file WIN-BUGSFIX.EXE to be downloaded and run. When executed, this password-stealing Trojan checks whether it is running from the system directory. If not, it copies itself there as WinFAT32.EXE and sets a Registry 'Run' value to execute that copy of itself at startup. This Trojan runs in a hidden window, not appearing in the Task List but remaining resident nonetheless.

Should its host have an Internet connection, the Trojan emails some information about the host machine and username/password combinations from *Windows'* authentication caches. These messages are sent directly via the smtp.super.net.ph server to mailme@super.net.ph. The values 'HideSharePwds' and 'DisablePwdCaching' are also deleted from network policies sections in the registry. As the Trojan depends on network interfaces not present in the original *Windows 95*, it fails to run under that OS unless the appropriate system updates have been installed.

The payload that probably gained more of the victim's attention was the deletion and apparent deletion of all files of several popular types. As LoveLetter.A searches for VBE and VBS files to infect, it also looks for CSS, JPEG, JPG, JS, JSE, HTA, MP2, MP3, SCT and WSH files. MP2 and MP3 files are hidden and files of the same name plus '.VBS' are created and the virus' code written to them. Early reports of LoveLetter's payload were very confused about this aspect of the code, often claiming these files were deleted. Of course, panicked users were rushing around double-clicking their 'lost' music files, running the virus over and over.

This payload also affects other file types. JPEG and JPG files are overwritten with the virus code, deleted and then files of the same name plus '.VBS' created and the virus' code written to them – for example, THIS.JPG would be replaced with a copy of the virus' VBS form as THIS.JPG.VBS. Files of the other types are overwritten with the virus' code, then deleted. This approach makes file recovery more difficult and therefore less likely to succeed. Overwriting a file typically replaces critical data in the directory record of the original, such as its size and its initial cluster. Worse still, all the file writing activity increases the likelihood of clusters from the deleted files being re-written. Deletion of CSS files (HTML cascading style sheets) has serious side-effects on the active desktop option in *IE*. The file types affected and precise details are different among the variants.

Love is in the Air

What made LoveLetter (in)famous was its mass-mailing payload. As with Melissa, this payload triggers when the virus first runs. Although the payload code seems 'inspired' by Melissa's, there are some important differences. Melissa sent a copy of itself to everyone in each accessible address list, or to the first 50 addresses, whichever was smaller. LoveLetter sends its message to every address accessible in each list. Possibly accounting for some of its apparently greater performance hits on mail servers, LoveLetter sends a message per address, whereas Melissa sent one message per address list.

Also unlike Melissa, LoveLetter's payload is not a run-once affair. LoveLetter keeps track of the addresses to which it sends itself so as to avoid re-sending. Thus, it can send itself to addresses added to *Outlook's* address lists since its previous run. This is achieved by storing each address list entry as a value at … \Software\Microsoft\WAB. In corporate LANs with large address lists, this 'scorecard' could cause performance and stability problems with Registry filesize blow-outs. LoveLetter.A's email message is simple, with a subject of 'ILOVEYOU' and a message body of 'Kindly check the attached LOVELETTER coming from me.' A copy of the virus' code is attached in the file LOVE-LETTER-FOR-YOU.TXT.VBS.

Little was learned, or at least retained, from the Melissa incident. LoveLetter may have had more impact because more people have susceptible machines. *Windows Scripting Host* may now be installed on more machines than *Word 97* was a year ago, and most email programs probably give less warning about running attachments than *Word* does about opening macro-carrying documents. And maybe, just maybe, what the world needs now, is love, sweet love…

VBS/LoveLetter	
Alias:	LoveLet, ILOVEYOU, Love Bug.
Type:	VBS overwriter with mass-mailing and *mIRC* distribution.
Self-recognition in Files:	None – it repetitively overwrites targets.
Payloads:	Overwrites files of many types. Some variants set hidden attribute of some file types and some attempt to down-load and install a password stealer.
Removal:	Delete all copies of the virus' script files and remove password stealer. Remove or reset Registry values as appropriate.