ISSN 0956-9979 JUNE 2000

VIRUS BULLETIN

THE INTERNATIONAL PUBLICATION ON COMPUTER VIRUS PREVENTION, RECOGNITION AND REMOVAL

IN THIS ISSUE:

• **All you need is love:** software manufacturers, IT security watchdogs, AV consultants and concerned users all have their say about what went wrong on Thursday 4 May. The love-in starts on p.2.

• **May the work-force be with you:** Nadir Karanjia saw 'Star Wars' 27 times. As far as he's concerned the aliens have taken over the AV reseller's market in India. Darth Vendors battle VARs on p.10.

• **Education, education, education:** this month's Tutorials come from two IT security specialists who hold opposing ideas on the value of AV education for users. *Microsoft's* Randy Abrams kicks off the debate on p.14.

CONTENTS

COMMENT

“ Our industry failed today … ”

Denial of (Anti-Virus) Service

VBS/LoveLetter.A presented a perfect opportunity for *WarLab* to cut its teeth on. *WarLab* (*Wells Antivirus Research Laboratory*) does not develop or support any anti-virus products; our primary focus is on product-neutral services. Since we do not have to pour resources into product design, development, testing, or support, we’re free to step back and decide where research is needed. Our normal, day-to-day operations involve monitoring both the perception and the reality of the virus problem, as well as the anti-virus industry’s response to the problem.

Back in early 1999, anti-virus was still a product. Then W97M/Melissa.A forced anti-virus to become a service. Suddenly, the services provided by the industry became paramount – services like providing immediate updates, instant information, and 24x7 support. Then, on 4 May, 2000, VBS/LoveLetter.A stress-tested the anti-virus industry.

Early in the day (Nevada time), while we were monitoring VBS/LoveLetter.A, an unforeseen issue became extremely obvious – the anti-virus industry as a whole was being pushed to new limits. We quickly realized that this was a golden opportunity to test that which was normally untestable. Therefore, we set out to test the anti-virus industry’s ability to function in the midst of an unprecedented crisis. To this end, we spent most of the day monitoring several key factors – doing so only intermittently so as not to add to the problems we found.

Here’s what we monitored – reports on the spread of the VBS/LoveLetter.A; anti-virus update availability; anti-virus update accessibility; anti-virus tech support accessibility; the efficiency of real-time product updating.

The results of our day of stress-testing the industry were disheartening. It was evident that the industry was unprepared for an event of this magnitude. Sadly, users were undoubtedly encountering the same problems we were. The bigger US anti-virus research and information Web sites were simply unavailable at first. We couldn’t get to *SARC*, *AVERT*, or *Trend* at all for much of the day. This changed by quitting time in the western USA (after European and most US businesses were closed).

The same was the case for the tech support phone lines, which were either busy or had long waits (we chose not to wait since real users needed help). Interestingly, we called one tech support line and got a recorded message that ‘a new virus’ had greatly increased wait times. Callers were told to go to a specific Web site which, of course, was inaccessible. When we tested real-time virus updating we were successful, but the downloads were painfully slow. Such systems seemed to be the only recourse we could deem successful.

Yet even then, one update we downloaded automatically (at 1pm Pacific Standard Time), did not detect VBS/LoveLetter.A. Since tech support was out of the question, we made a personal call to someone we knew in the lab. We were told that the correct update was going up as we spoke. Pity the poor user who assumed their successfully downloaded file would protect them.

Now, if we extrapolate our results to users in general, an ominous image takes shape. Users were hit today and many had no way to get help. Those who needed to download updates in order to stop their local epidemic were doomed to failure. Assuming an update was actually available, it was inaccessible. Even assuming some persevered in their calls to tech support and got through, how would they get the all-essential update?

We have a problem. By extension, our users have a problem. Our industry failed today to protect many of those who depend on us. The problem is one of accessibility of services. Therefore, we as an industry must provide a solution to this new problem.

Joe Wells, WarLab
Thursday, 4 May, 2000

VIRUS BULLETIN **©2000 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. / 2000/$0.00+2.50**

NEWS

Love's Labours Lost

VBS/LoveLetter.A crippled businesses worldwide and hit the headlines on Thursday 4 May. By mid-month the *FBI* (in association with various authorities) had detained a young man and his sister in Manila. With many of the major AV vendor Web sites unable to cope due to sheer numbers of panicking customers, this month *VB* looks at whether this worm really was 'more dangerous than Melissa' (as the media reported) and if there was anything that could have been done to prevent the damage ▮

Class-ic Case

Many thanks to the guys at *Norman*, who tipped us off that the May 2000 issue of *Microsoft Office & Visual Basic for Applications Developer* includes the full, commented source of the W97M/Class virus in its cover feature 'Anatomy of a Macro Virus: Understanding the Enemy'. At the time of writing, the article is not on the magazine's Web page (www.officevba.com/) which, while some may think this is a blessing, may not be. Several years back we saw a huge flurry of Wazzu variants when a German magazine did a similar thing. People had to type the code in and, of course, there were not only the usual typos to contend with but also the 'creative urges' of questionable types who knew not what they were doing – or worse, did, and thought it would be cool to have their 'own' virus variant ▮

Media'che

In the early hours of Friday 19 May (GMT) a new worm surfaced – VBS/NewLove. The American media, still on edge from the LoveLetter incident, sprang into action immediately, reporting thousands of infections across the US and triggering analysts around the globe to implement its detection. This seems a tad hysterical given that, in comparison to VBS/LoveLetter, in-the-wild reports of NewLove were few and far between.

A mass-mailer with a destructive payload, VBS/NewLove uses a few simple, yet effective, tricks in order to make it polymorphic. The subject line and attachment filename are derived from the name of a randomly selected file from the … \Windows\Recent folder on the infected machine. The VBS code itself mutates upon each infection, with the insertion of spaces and randomly generated comment lines. Watch this space for a full analysis soon ▮

VB2000 Sponsors

Virus Bulletin is pleased to announce that VB2000 in Orlando, Florida on 28 and 29 September is to be sponsored by *McAfee*, *Sophos* and *Symantec*. Many thanks to these AV companies for their generous support ▮

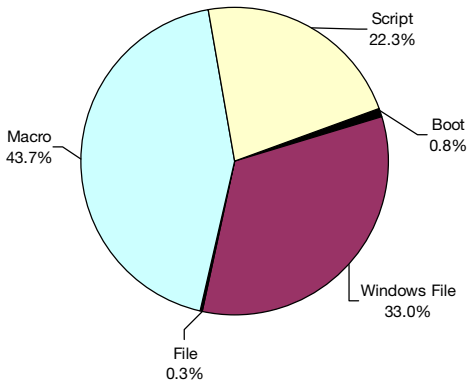
Prevalence Table – April 2000

Virus	Type	Incidents	Reports
Kak	Script	229	17.9%
Win32/Pretty	File	206	16.1%
Win32/Ska	File	153	12.0%
Laroux	Macro	96	7.5%
Marker	Macro	84	6.6%
Ethan	Macro	79	6.2%
Service	Macro	64	5.0%
Freelinks	Script	53	4.2%
Thus	Macro	37	2.9%
Class	Macro	30	2.4%
Win32/Fix	File	28	2.2%
Win95/CIH	File	25	2.0%
Melissa	Macro	22	1.7%
Story	Macro	21	1.6%
Tristate	Macro	17	1.3%
Cap	Macro	14	1.1%
Pri	Macro	14	1.1%
ColdApe	Macro	13	1.0%
IIS	Macro	9	0.7%
Proverb	Macro	6	0.5%
AntiCMOS	Boot	5	0.4%
Divi	Macro	5	0.4%
Win32/ExploreZip	File	4	0.3%
Others [1]		62	4.9%
Total		1276	100%

[1] The Prevalence Table includes a total of 62 reports across 37 further viruses. Readers are reminded that a complete listing is posted at http://www.virusbtn.com/Prevalence/.

In order to avoid a distortion of the figures, data for the 'self-reporting' W97M/ColdApe virus (totalling 762 reports in April) have been omitted from the table this month.

Distribution of virus types in repor



LETTERS

Dear Virus Bulletin

WarLab & Peace

The March 2000 WildList was not published. Its nonexistence made it impossible for certification agencies to perform their regular monthly tests. While no excuse can change things now, there are some things that the *WLO* would like its readership and Participants to understand.

First and foremost, on behalf of the *WLO*, I would like to offer an apology to all those who rely so heavily upon the WildList. As I seem to be the person most responsible for its compilation, I can only say that it was not my intention to cause inconveniences.

What happened? Well, a few different 'things' – both foreseen and unforeseen. Ignoring those things that have little relevance to the anti-virus industry, and focusing only on those that do, please allow me to explain further.

Wells Antivirus Research Laboratories (*WarLab*) is a small startup company. Being a new business, there is (still) much to do. Because, among other things, there were employees to train, my energy had to be focused elsewhere. The work at *WarLab* took precedence over something that is still, after all, a non-profit, volunteer project. I will also mention that *Trend Micro – WarLab's* parent company – had nothing to do with our prioritization of activities. As I've told many people, I continue to believe strongly that *WarLab* will have a positive impact on the *WLO*.

Both Joe and I knew that getting *WarLab* going was something that would take a toll on the March WildList. We knew that it might cause delays. What we didn't count on were the several other mishaps, all of which, when combined, made it impossible for us to finalize the March WildList. (The other things included a broken computer critical to WildList work, a medical emergency, an out-of-state trip, and my house, which is still in the process of being built.)

Now, on the heels of VBS/LoveLetter, the situation with the March WildList is somewhat similar to the 'Denial of (Anti-virus) Service' Comment appearing on p.2 of this issue. That is, we became overloaded and couldn't provide the monthly service to which so many people have become so accustomed.

The *WLO* believes it has taken at least one step necessary to alleviate this type of problem. We brought in a greater number of volunteers for the arduous process of compilation. It is a step that we *had* to take, mostly because of the ever increasing amount of activity and reports that we are receiving each month. Whereas last year at this time we would see an average of 50–75 samples per month from the Participants, we now see an average of 300–350 samples per month. In the time currently allotted, this is simply too much work for one person to hope to do well.

While unexpected problems can arise at any time, the *WLO* does not see a recurrence of the events that occurred in March. We therefore hope to move peacefully back to the usual 15th-of-the-month release of all future WildLists. Thank you for your patience, continued support, and understanding.

Shane Coursen and the rest of the WLO
WildList Organization
USA

Taken with a Pinch of Smiley

Normally, I feel I shouldn't get involved in discussions about *VB* articles once they are published. I would hate to have my opinions mistaken for those of my employer and as Technical Editor of *VB* I get to have my 'go' at the proof reading stage, but as I had discussed this with Francesca before publishing, she suggested that I share my thoughts.

So, taking my industry hats off, I'm still a computer user – I use computers in my after-hours life, and security issues in general, and viruses in particular, are parts of my leisure interests. That's why I read Lucijan Caric's article in last month's issue with great interest. The kidnapping of the AV industry by the marketing hype, scare tactics, unsubstantiated press releases, shifting the focus of the industry from the customers to the shareholders are all issues that I am also concerned with. I read eagerly, looking forward to Lucijan's suggestions and possible directions that might lead us towards the light at the end of the long dark tunnel that we all seem to have wandered into.

To my disappointment, Lucijan took the easy way out, turning a serious problem into sarcasm and escaping the serious issue by making a joke instead. And I think I know why – he probably doesn't know of a solution. So why does this article annoy me? Because I can't see a solution either. I appreciate irony as an anti-virus researcher, but as a reader and a user I expected some solutions or suggestions. Since none were even attempted, the whole article should be clearly accompanied by 'the big smiley'. Good on'ya Lucijan – at least for a moment I was entertained by the thought of some anti-virus producer taking your advice seriously. My only hope is that no one ever uses this article to substantiate claims that anti-virus companies do write their own viruses.

Lejla Pavlov's letter reflecting on the last *InfoSec* ('Watch Out Pigeons – Here Comes Kitty!') was not so entertaining and made me rather angry. I don't believe the world is black

VIRUS BULLETIN **©2000 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. / 2000/$0.00+2.50**

and white, and I don't believe all hackers and virus writers should burn in hell or even go to jail but Lejla's attempts to define ethical hackers based on the content of the sites they hack is completely unreasonable: 'They target child pornography sites and Nazi sites. Come on, you've got to agree that it is ethical hacking! Anyone who has kids would definitely agree.' Does that mean that childless people wouldn't agree? Will breaking into a site of a big American sportswear producer using cheap labour in poor countries be alright too? Government sites of countries with bad human rights records? Abortion clinics? Still good hacking or not?

Reading further: 'Since no one had bothered to admit the obvious, I thought I'd thank Sir Dystic for BackOrifice and pointed out there were a lot of administrators out there who do use it… I got a little applause too.' I think it would be interesting to ask those applauding how many of them insist that their AV products still detect BackOrifice and other backdoors (like NetBus) as something undesirable on their company networks.

And the very next paragraph: 'Let's face it. If there weren't hackers, regardless of whether they are "dark" hackers or "ethical" hackers and "proof of concept" virus writers or "meanie" virus writers, there would be no security industry.' This argument is misconceived and is usually purported by someone with little computer education. It's surprising that this misleading idea is promoted by someone who cannot see themselves 'being in any other field in IT'.

What about the security of the sensitive data (e.g. protection of medical records, financial transactions) or network administration issues (account management, application and data distribution) or secure data storage and backups? 'Unethical hackers' and viruses are just some of the issues the security industry have to deal with.

And finally: 'So let's swallow our ideals and thank these people for making our jobs and giving us a little bit of excitement in our daily routine!' Why should we swallow our ideals – these are the last things we should give up. What else would we have left? If we owe our living to virus writers, and (quoting Lucijan) we 'are bending lower and lower before the dollar God' – the only thing that can possibly get us out of here are our ideals. And as far as a 'bit of excitement' goes, I hope Lejla had plenty of fun with the LoveLetter worms.

Jakub Kaminski
Australia

Bias is Bull!

It was with wry amusement that I have been following the recent fracas in alt.comp.virus concerning a poster, allegedly working for *Trend Micro*, who has 'discovered' that 'VB is Sophos' and implies that it is therefore useless as a review body. First let me bring any reader into the dreadful realization: *Virus Bulletin* and *Sophos* are sister companies. 'Oh my!', I hear you cry …as if this fact has ever been an issue, or ever even disguised. The same folks who decided to become interested in viruses years ago also chose to launch a magazine about them. Shocking!

Some have therefore drawn the conclusion that *VB* is biased toward *Sophos*. I'd like to show what a ridiculous piece of logic this is, in a few points:

1. *VB* has a wide advisory board, comprising some 14 people representing 14 *different* AV companies. Not the best platform from which to pitch one's product!
2. *VB* reviews show remarkable correlations to other professional AV reviews. An analysis of past Comparatives shows incontrovertible consistencies.
3. No attempt has been made to hide the link between *Sophos* and *VB* – again, hardly a sensible move if the intent was to deceive.
4. I have been a *VB* Editor – I hope that those who have met me know that my name and integrity is worth more than any job. The same is true of all Editors past. The current team is just as professionally honest as any in the past. By insulting *VB's* integrity you are directly insulting theirs.
5. *VB* has always given the opportunity for a vendor to show how results obtained for tests are false, and when any test I was involved in was proved in error, VB has *always* either amended the article if the magazine had not gone to print, or printed a correction as soon as possible.

This most recent attack reminds me of another such claim, made to me at an *EICAR* conference. At the Gala Dinner it was my distinct displeasure to be railed upon by a somewhat drunk, terribly obnoxious and *extremely* loud representative of an anti-virus company which, by way of good grace, I shall not name. This 'gentleman' regaled the table with his obscenity-laden litany that consisted primarily of saying that *Virus Bulletin's* independence was a sham. Between each spittle-inflected part-sentence, I asked him the same question I now ask the author of the posts in a.c.v: put up or shut up! Show me the bias … All I got for my position was another barrage of verbiage with no actual fact to back it up with.

The mud being thrown in public is of no benefit to anyone; only truth supported by facts can hope to create a dialogue which produces more light than heat. The strongest argument for *VB's* value is the accuracy of its reviews. This latest round of mud-slinging has gone on far too long, and the veracity of claims made or, worse yet, things merely implied, needs to be proved. There is really only one way to do this: one knows the tree by the fruit it bears. The reviews I have seen are accurate, biting, and above all else, useful to the user. Good fruit, from a good tree.

Dr Richard Ford,
CTO, Cenetec LLC
USA

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.

VIRUS ANALYSIS 2

Rare Beasts

Andy Nikishin & Mike Pavluschick
Kaspersky Lab, Russia

A macro virus researcher's life is actually quite boring and not as varied as people think. Every day we have to deal with dozens of new macro viruses that are as similar as two teardrops (remember the hundreds of Wazzu, Laroux, Ethan and Class variants?). It is very, very seldom that we meet really interesting viruses, unique infection methods, funny payloads, or something that commands attention. Unfortunately (or fortunately, depending on your point of view), viruses like these very rarely spread worldwide and get into wild or prevalence lists, but nevertheless we are going to talk about them here.

O97M/Carpe

This was the very first cross-platform macro virus to infect not only *Word* documents and *Excel* spreadsheets but *Project* documents as well. Its infection technique resembles that of O97M/Triplicate (see *VB*, March 1999, p.11). Carpe uses an original technique to hide its code, setting a 'white on white' colour scheme in the VBA Editor. During activation, the virus saves its code into a file called C:\WRDVBS.EXP. Then it creates C:\WINDOWS \Start Menu\Programs\Startup\Reminder.VBS. Upon rebooting, this script runs (it was placed in the *Windows* startup folder) and infects *Word's* normal template (NORMAL.DOT) area using the previously saved file (WRDVBS.EXP) which contains the virus body.

After this, the virus saves any active documents as C:\CDLIST.RTF and creates a C:\WINDOWS\ZIPINF.BAT file with instructions to write an infected .RTF document into every ZIP archive in the Windows\Desktop location. Finally, Carpe starts this .BAT file. If the virus was activated from an *Excel* spreadsheet, and it is the first half of January, the virus shows a series of messages with New Year congratulations. It also creates and starts a .BAT file that shows the messages: 'No Religion, No Gods, No Masters', 'Begin this new age in a new light', 'After all we will all die eventually', and 'and Life isn't all about how much suffering we can endure… is it ???'.

W97M/Blink

This virus is not a pure macro virus – it is a specially prepared 'sandwich' that contains *Word* documents and a Win32 executable. The .EXE file is written to the end of the document. The macro part activates when infected documents open. During the activation phase, Blink saves the active (i.e. infected) *Word* document as BLINK.DOC, allocates 8 KB of memory, reads part of the .DOC file into the allocated memory and then saves this data to a file called BLINK.EXE. To do this, the virus uses the Win32 functions _lopen, _lcreat, _llseek, GlobalAlloc, CopyFileA, _lread, _lwrite and _lclose from KERNEL32.DLL. Finally, the macro part runs the dropped .EXE file.

Now it is time for the EXE part. This finds RAR archives on all directories beginning at the root directory on the current disk and adds the BLINK.DOC file to the archives.

W97M/Ipid

This is a very ordinary and badly coded virus, but it has one interesting feature – during activation, it copies a file (\\ESM-CPD\E$\IPID.EXE) from the network drive to the *Windows* directory and runs it. We can only guess why it needs to do this. This file may be a Trojan or a virus or even a special spy tool. Or maybe it was the revenge of a fired administrator – who knows?

As an extra feature the virus also displays some stealth techniques by hiding the Tools_Macro menu as well as its submenu. However, this feature only works with the Spanish version of *Word*.

W97M/Damon

This virus is a very interesting and rare specimen, especially when you try to catch it by opening a number of documents and trying to see macros within them. You cannot see the code because this is not a pure virus – this is a worm which creeps over from one document to another.

Damon infects one of the opened documents (which the virus chooses, depending on a random generator) and deletes its code from the host document. So, only one document on your computer is infected. Potentially, a user could never know that his or her computer is (or was) infected if the infected document gets deleted.

W97M/Trojan.NPR

Usually, *Virus Bulletin* does not feature analyses of Trojans (password stealers). However, we permit ourselves to break this rule and try to draw your attention to this 'macro-horse' – this 'thief' was written in VBA (as far as we know, this is the *first* macro password stealer).

What unusual behaviour does this Trojan exhibit? This piece of malware is a classic Trojan – it pretends to be a useful utility doing some helpful work. The useful part recovers a forgotten password from *Netscape Communicator* and shows it in a new document (it shows a version of *Netscape Navigator*, a number of users and mail accounts, and for every account it shows profile and user names, POP3 addresses and passwords).

To do this, the Trojan registers the hot key Alt-F1. During its first execution on a user's computer, the Trojan saves its body as a macro module, called MSPlus, to the global template (NORMAL.DOT). To prevent repeated infection, it checks the macro module's name. When the user closes *Word*, the Trojan checks the internal counter which it places in C:\WINDOWS\LOGOW.SYS offset 76989 and, depending on the counter and the current day, collects and sends account data to the malefactor.

Let us review this data-sending procedure a little more closely. First of all, the Trojan checks connections and if the computer does not connect to the Internet, it stops its work. To check connections, the Trojan finds a window with the title <Connect to> (in English or Russian). It is worth remembering that it always checks Russian and English messages and window titles.

After this, the Trojan starts the standard Telnet application (TELNET.EXE) and tries to connect to one of 5 SMTP servers (though it contains a list of 10 such servers). After connection, it prepares to send a message to its master using SMTP protocol commands. This information will make its way to kashek@usa.net and the sender becomes master@myself.com. The Trojan collects information about the victim's Internet account (login and password) by creating its own temporary file with a random name and .ENG extension in the C:\WINDOWS directory.

It finds the C:\WINDOWS\EDIALER.INI file (the Internet dialler's .INI file), reads the password and user login from it, and saves this data into the Trojan's temporary file. After this, it checks the SYSTEM.INI file's (Password Lists) section and stores the password file's name (with a .PWL extension) into its temporary file. Then the Trojan sends the data to its master by converting its own temporary file and .PWL files into text format (using the BASE64 encoding procedure), attaching the converted data to an email message and deleting the temporary file.

Consequently, the email message contains a number of attachments that contain the user's login and password to connect to the Internet provider. Finally, it stores the current date to C:\WINDOWS\LOGOW.SYS offset 76989. W97M/Trojan.NPR has some stealth functions – it intercepts the ToolsOptions() function and, before showing *Word's* Option dialog, switches on *Word's* macro virus protection and switches it off again afterwards.

W97M/Bridge

This is a very interesting virus in that it uses an unusual event handling mechanism. The virus appears to be a 'bridge' between two technologies: old – using automacros, and new – using classes and objects events handling.

Bridge contains two modules – a class module and an ordinary module. The first one is called 'Contec'. This contains the public object variable Acol of the .DOC type declared using the 'WithEvents' keyword. Such a declaration allows the write handle procedure for any object event to be stored in the variable. This variable is then used as a bridge. Actually, the only handle procedure implemented is Acol_Close. It handles the Close event of documents associated with the Acol variable and contains the main virus code. The Acol_Open procedure is also present in the class module, but it has no code.

The second module, named 'MdCont', contains the declaration of the class variable and the AutoOpen() procedure. Since the class variable is declared with the 'New' keyword in the global namespace, it creates the class exemplar at the moment of project initialization. The AutoOpen procedure only does one thing – it initializes the class module's public variable with an active (i.e. just opened) document. From this moment on, the virus controls the document's behaviour with events handle procedures in the class module.

If the AutoOpen () procedure is placed in a document, *Word* executes it only at the time that document opens. If the same procedure takes place in the normal template, it executes *each and every* time a document opens. So, if Bridge executes from a document, it only hooks that same document, but if it runs from the normal template, it hooks the most recently opened document.

On closing the hooked document, *Word* executes the Acol_Close procedure in the class module and the virus code gets control. At first, the virus infects the normal template area. Before this, it checks if the normal template is already infected or not by looking for the 'Contec' module. If it is not found, the virus creates two modules in the normal template (again, an ordinary and a class module) and copies its own code into them. It takes the same steps to infect an active document.

There is a potential problem for the virus if the AutoOpen procedure is already present in a project. If this is the case, then the VBA compiler will generate an error message. If virus writers find a way to avoid this, virus technology will begin a new era. At the moment, usually only one macro virus can exist in a document because most of them lay exclusive claim to procedure names like Document_Close, Document_Open, etc. Ordinary, modern macro viruses remove all existing code from modules before infection to avoid a global names conflict. With new technology this may not necessarily be a requirement. Potentially therefore, a lot of viruses could be present in the document at the same time without any conflicts or problems. The event handle procedures would execute one by one in a registration queue (objects creation).

Last Words

We have one cherished desire – that one day we come to work and find that there are no more new macro viruses out there at all. However, we guess that this wish will never come true. So, every day we get sent dozens of new macro virus beasts – fortunately, there are some interesting specimens among them.

FEATURE

On the Indian Frontier

Nadir Karanjia
N&N Systems and Software Pvt Ltd, India

No grandiose orchestral strains wafting out of *Dolby* systems or eclectic space vehicles chasing each other across wide expanses of the starry firmament; no lasers or phasers blasting holes in battle-scarred hulls; no intergalactic escape pods liberating themselves from star-freighters to hide in desert planets buffeted by swirling space dust; no dynamic, rascal/rogue pilots or Jedi Knights and Masters to inject wisdom in maddening times; no intelligent droids and dreamy galactic princesses to rescue; no Spielberg as I engage to fight my… price wars.

Darth Vendor takes on VAR

The country is India, the war is over anti-virus software and the market is, to put it in perspective, as saturated as the fat in a greasy spoon café. The reason behind this energetic environment is that hidden-in-the-shadows force: the Darth Vendor.

In the early years – the good ol' days of *Dr Solomon's* – when there were only one or two serious players in the field, there remained a semblance of control in the structure of the distribution chain and processes governing the sale of AV products. One had the luxury of making a presentation of some quality, grandly proclaiming all the features and functions of the products that one sold; destroying any meek query from the customer about a competitive product with a disdainful, sardonic glance and issuing wild challenges to any other dealer or VAR (Very Agonized Reseller) to stand forth and subject his product to the full blast of that digital rapier of justice… the Virus Collection.

There were seldom any takers. Those foolhardy enough to try were forever routed in the eyes of the customer, doing such damage to themselves in the process of misguided bravado that no option remained worthy in the customer's esteem but the excellent *Dr Solomon's* anti-virus product range of which we were distributors in India.

So what if it was often twice the price of others? So what if the representative did not 'drop his pants' (if you will be so kind as to pardon the phrase) at the customer's price request? This AV product was the most important purchase to secure one's networks and data, considered a strategic acquisition worthy of the costs.

Moreover, it was not enough just to buy the product – you had to buy the services too! Implementation, installation, emergency support, 24-hour help lines, outstation support, training, updates and upgrades provided on floppy disks (as were the default media in those days) etc, etc, etc. All these goodies came at a price and customers recognized the fact that service worth having was service worth paying for. In other words, 'You pay peanuts – you get monkeys.'

'Those were the days my friend, we thought they'd never end…' (hmm, think I heard those words in a song sometime) but alas, all good things must come to an end. Just when you think it's perfect, it seldom is. Apply one of Murphy's many laws – choose whatever reason you wish – the harsh reality is that today we are in the middle of price wars and we have, among other reasons, the Darth Vendor to thank for it.

In the mad scramble for market-share and the hunger for turnover in the 'most important quarter, which is the quarter you are in' as one Darth Vendor so succinctly put it, nothing is too chaste to sacrifice. No goat is too precious to bring to the almighty altar of NASDAQ – always push the quarter, always push the growth curve, always stuff the channel. Grow, grow, grow … until the bubble, finally and inevitably, bursts.

The Return of the Reseller

Today, the anti-virus market in India is in a shambles. The market churns out volumes which contribute heftily to turnover and top line, with wafer-thin contributions to bottom line profitability of an enterprise. This may not seem as bad as it sounds in a developed market where it is understood that there is a line that divides products from value-added services.

In a market like India, however, this is something that has completely slipped through the cracks with regards to anti-virus value-added and emergency services. Customers are not willing to pay charges for services and they expect hefty discounts off the printed list price at the same time in order to close the sale.

The most absurd thing of all is that the customer is *not* being as unreasonable as the case may seem; they are merely doing what they have been taught to do by vendors and dealers alike. The worst thing about a price war is the fact that it is like a treadmill and once on, you cannot get off that easily, if at all. Vendors saturate the market with agents, dealers, representatives, distributors-who-think-they-are-resellers, distributors-who-think-they-are-bazaar-stalls, resellers, casual resellers. *Anybody* who wants to sell *anything* is awarded the status of 'partner' by Darth Vendor.

This results in an energetic environment initially, but to call upon the Marxist philosophy of 'dialectical change', one can extrapolate the reasoning that the system which grows as a result of chaos has within it the seeds of its own destruction. It writes its own destiny which inevitably culminates in an implosion of sorts that destroys the entire

VIRUS BULLETIN **©2000 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. / 2000/$0.00+2.50**

core. In our situation, this means *all* the vast pool of channels selling Darth Vendor's products end up doing so not on a basis of technical or marketing excellence but on one issue alone, that being the bogey of price.

Alas, but the Darth Vendor is not really happy either. The first few months after the initiation of the wars, the Vendor sees his volume of sales increase; he is delighted and thinks that his wonderful strategy has paid rich dividends. Two quarters down, the Vendor is wondering what in heaven's name he started – all day, all night, all the time he is inundated by calls, emails, communications for bid requests, price discounts etc. All he seems to be doing with his time is addressing conflicts in his channels, answering embarrassing questions on transfer prices, filling out RFPs (requests for pricing), juggling distributors, agents, resellers, VARS, general resellers, customers and the like.

Sometime past the third quarter of the price wars, Darth Vendor's country manager finds his infrastructure loaded with unprocessed requests and his pipelines clogged with administrative bottlenecks. To top it all, the 'suits' above him in the corporate hierarchy see volume increases in the territories and heap more and more targets on him in their ever-hungry bid to push the corporate counter on the mighty NASDAQ.

The result is more pressure down the ranks, more saturation, further trouser-dropping by everyone until it feels like the first thing one does at a customer's site is to remove all one's clothes and sit down with only a tie around the neck at each customer meeting. Then, one need not discuss anything – it is all too obviously evident which course of action will be taken.

The Vendor Strikes Back

Finally, Darth Vendor's representative goes berserk; one morning he wakes up and feels that jumping out of the window of his plush office (where he has spent the night trying to sort out all the price-bid requests) is a more appealing option than facing another day of *MS Outlook* inbox phenomena; he gamely decides to bring some order into the chaos that has been sown.

His boss flies down from Corporate HQ in his Lear Jet or whatever means he utilizes to get to the battle-zone. Lord and vassal alike survey the carnage and with a flurry of activity set about announcing lofty proclamations, peppered with reassuring phrases such as 'price control will be enforced', 'understand your concerns', 'sort out the mess', 'you have my word' and 'raising comfort levels.'

Of course, at the end of the day, it is quite needless to say that everything just gets worse as people who start to believe the propaganda (ha ha!) end up with the short end of the stick. They lose a few accounts as a result of keeping their clothes *on* for a change (I speak figuratively, of course) and come back into the fray with a vengeance – the metaphorical equivalent of removing even the tie this time round – and descend into that gray area called 'strategic negative selling'.

India has reached the pinnacle of its price wars where we now have the experience of being told our transfer prices from Darth Vendor to VAR by the customer, who then tells us how much we should be making on the deal, based on others making that much or less. I stress again, it is not the customer's fault (and I say this not because I am a believer in the Gandhian ideal of 'the customer is always right') because the customer's job is to get the best deal for his company from the market.

It is the hand of Darth Vendor – his agents, representatives, his dealers, his partners, his structures, his management – that is responsible for the mayhem. In place of a structured approach aimed at fostering sustainable growth of a market, and an equitable system of reward for excellence which should determine the transfer margins and thus the depth of each channel's pocket when it comes to wanton discounting, Darth Vendor chooses the route of chaos over ordered sanctity.

The Phantom Menace?

Price, price, price – that ubiquitous benchmark of qualification that exists in our nation; price – that great leveller of vanities, that usurper of thrones, that king of confusion, that source of systematic dilution of skill and knowledge base; price, that definer of performance – how much it has hurt to fight these price wars.

Our company tired of this. Hence, almost two years ago, at the peak of our success in anti-virus solutions, we re-invented ourselves as a network security and network management products, services and consultancy outfit. We have already seen tremendous success in these growth areas as a result of almost two full years of building knowledge bases and excellence. Today I may even whisper a small 'thank you' to the price wars – they forced us out of our comfort zone and made us venture into a new world.

OPINION 1

Do you really Love Me?

Robert Vibert
Segura Solutions, Canada

It was Thursday, 4 May, and I was starting to write a short piece on how managers seem to ignore the whole anti-virus issue until they simply cannot avoid it. I thought I would check my email in the background while I composed. Out of the corner of my eye, I watched as the number of incoming email messages climbed higher than usual. Hmm, I wondered, what is the story here?

The Cobbler's House

Turns out I was getting a bunch of emails from an anti-virus company with the subject 'ILOVEYOU'. And, if you have been following the news at all, you will have heard all about this Son-of-Melissa and its kissing cousins. I watched as the reports trickled in from folks analysing the critter and spent a few minutes reading the cries for help in the newsgroups. Some said it was spreading faster than Melissa and could have greater impact. In my case, four people from a well-known anti-virus company had been infected with it, and were sending out the virus to all and sundry. What is the old saying? In the cobbler's house the children run barefoot …

A detailed analysis of this virus can be found on p.6 of this issue, so I will not get into that here. In any case, my original topic is now all the more interesting, given that the management at lots of organizations seem to have missed the point of Melissa and been smacked again.

Unfortunately, they will continue to get hit again and again, but how many times does it take for them to realize what is going on? I was having a nice email chat the other day with the head anti-virus honcho at a major communications company when he dropped an interesting comment on me, to wit, that his management did not care about the anti-virus issue unless it made them look good.

He went on to tell me about approaching the CEO of *MegaDataCorp* and asking which division would entertain the thought of integrating malware scanning tools into the Internet infrastructure. The idea was, shall we say, filed for further study.

Oh, *MegaDataCorp* does have enterprise-level anti-virus protection installed, including scanning on their Internet gateway, and they have reduced the number of viruses arriving at the desktop dramatically. In April of this year, they stopped over 4,400 inbound viruses from the Internet while over 2,200 internally circulating viruses were caught. And, by the end of the first day of the love-in, they had snagged over 11,000 copies of LoveLetter at the gateway.

Minimum Funding, Maximum Results

The problem is that while the anti-virus technicians toil on, they typically get little, if any, management support. The main question my friend at *MegaDataCorp* gets asked when he proposes improvements to their anti-virus defences is 'Who gets credit for this?'.

As the managerial types who would like the credit would have a hard time explaining what 'they' have done to deserve it, the whole topic gets put onto the proverbial backburner. At least, that is until things like Melissa or LoveLetter come calling.

Another anti-virus warrior at *MegaElectroCorp* told me that 'management wants maximum protection with zero cost', and 'if we have paid so much and have deployed the best protection for our environment, why are we still finding thousands of viruses every month?'.

The AVicious Circle

So the circle goes round and round. Management ignores the anti-virus issue as much as possible for as long as possible (since it is not a particularly sexy topic unlike hackers or MP3 files). They quibble over the costs of anti-virus software and services. They ignore and drag their feet on the advice of the specialists they hire.

Then something nasty and very public comes along, like LoveLetter, and their systems go down for the count. It is then that they crack the whip and emit quotable sound bites for the radio and TV crews while their technicians scramble to get fixes in place.

For how long will managers pay attention to each anti-virus crisis? Only until something else comes along that is more interesting and with career-enhancing possibilities.

I have seen a few cases of organizations which temporarily 'got religion' about anti-virus, but usually it takes a high level manager embarrassing himself by sending out a virus to his staff and peers before anyone makes a serious move.

Far too many are like the Canadian bank which switched suppliers from an experienced anti-virus reseller to one with some greenhorn cowboys who claimed they could do just as good a job – all for the sake of 'saving' about a dollar per machine per year. Anyone with a long-term view (say a year at a time) would realize that all it takes is a single big incident to wipe out any such savings.

So the question on the lips of all corporate anti-virus technicians as they face their managers on the morning after LoveLetter and kin finally fade away, will undoubtedly be 'Do you really love me?'. Let's hope that this time the replies they get are not empty promises.

VIRUS BULLETIN **©2000 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. / 2000/$0.00+2.50**

OPINION 2

Cleaning up the Kak

Paul Baccas
Sophos Plc, UK

I have noticed a disturbing trend in virus-related mails and posts to various locations lately. Within days of 4 May alt.comp.virus had around 1,400 posts a day, many of them highlighting issues that had been waiting to solidify.

Knowledge is Power

Two of the most recent fast, large-scale infectors – Kak and LoveLetter – have been written in easily understandable code. All you need to see it is access to a text viewer/editor. Kak is slightly more complex to analyse, but a precocious twelve-year old could understand it. Looking at some of the postings of fixes and descriptions, perhaps these mythical twelve-year olds have already had a go!

Power Corrupts

The relative ease of analysis of Kak and LoveLetter has led to a veritable agony of self-proclaimed anti-virus experts. From the dubious moral characters of those posting commented virus source code in the interests of security, to show how clever they are, or for plain one-upmanship, to the plethora of 'fixes' for the damage these viruses can do – the range and diversity is unbelievable. Some of them are obviously more dangerous than others and even some reputable experts have got things wrong.

Each of the fixes suggested alter the Registry of the affected machine, but they are proposed with a lack of fundamental understanding that is frightening. A cavalier approach to the Registry is ill-advised – *Microsoft* warns not to 'play' with the Registry without some degree of expertise. In fact, whenever possible, you should use the GUI application to alter its own Registry entries.

Unfortunately, at least one major AV vendor's Web site, in providing a fix for Kak, contained misleading information. The fix's author seemed to forget that, of the five static roots in the Registry, only two are true – the others are merely reflections of their component parts – and suggested more modifications than necessary.

The Registry is a database that, like *Word* with 'Fast Save' turned on, adds the changes made to the bottom. The Registry can only be compacted manually, via a complex routine, and is only of finite size. For LoveLetter, this can be particularly salient, as it can write to the Registry numerous times. A report to *NTBugtraq* suggests nearly six thousand keys added and modified. Extra modifications to the Registry will leave you, at some time in the future, with a corrupt Registry.

Systems Administrators are faced with the dilemma of a financially expedient solution versus a possible data integrity corruption. To whom do they turn for advice? They turn to the security industry in general and the AV industry in particular. How have these people responded?

Absolute Power Corrupts Absolutely

Someone at *AN Other* 'AV vendor' publicly misinterpreted their rather ropey analysis of LoveLetter by claiming that 'you could be infected by previewing an email containing Loveletter in the same way as Kak'. This suggestion muddied the already murky waters and caused resources to be completely tied up. The similarities between Kak and LoveLetter concern the use of *Windows Scripting Host* and email. A recent, unhelpful press release from a UK security company at the perimeter of the AV industry has perpetuated this myth.

The balance between brief and verbose descriptions is a difficult one to find. The trick to giving all the relevant information necessary, i.e. what it does but not how it does it, without leaving ambiguity, is not easy. The rapid dissemination of good information is essential in a volatile arena like the AV industry. The self-confessed anti-virus expert, the media, and the marketing departments are not particularly interested in the 'truth'. They are interested in kudos, newsworthiness and good spin – all of which make the issues 'as clear as mud' in the minds of the public. For example, one vendor claimed that they 'saw' their first sample of LoveLetter ten hours before other vendors began getting fixes out.

The question is, where can we get good, reliable information? I have touched upon the problems of 'fixing' the Registry but both the viruses discussed alter other things. While 'fixing' these other things is less fraught with danger, it is currently left up to the user to do so. In large user environments we will increasingly see 2-bit fixes based on the viral code. The less proficient the twelve-year old, the more likely we are to have viral fixes. How many of the current macro viruses are fixed this way?

One UK computing weekly devoted eight articles to LoveLetter in the second week of May. None mentioned anyone from the AV industry. The views and opinions expressed suggested a lack of information about the virus and its related issues. When the dust finally settles on LoveLetter, we will probably be discussing 'the Hype and the Glory' – who gained the most, or rather, who did not lose in this incident. We are like citizens of Naples waiting for our Pompeii. The nature of the AV industry's relationship with its customers is one in which the latter believe in the former's omnipotence; 'I have anti-virus software, my email is checked, therefore it is safe to…'.

TUTORIAL 1

If I told you ILOVEYOU would you Educate Me?

Randy Abrams
Microsoft Corporation, USA

I once heard a saying that went something like this: 'Would those of you who say it can't be done please get out of the way of those of us who are doing it'.

I have no doubt that a great many quitters and misinformed people are going to point to the VBS/LoveLetter worm as proof that education does not work. It is not uncommon for people to mistake 'I don't know how' for 'It can't be done'. The fact is that poor quality education simply does not work.

A poor quality education will turn out bad doctors, incompetent engineers, and uninformed computer users. Education can be quite effective, but it needs to be done just right.

Good Teaching Works

For a very long time a small group of people advised users not to open suspicious attachments. Then Melissa hit and a larger group of people told many more people not to open suspicious attachments. Even the first groups of so-called 'students' who were taught not to open suspicious attachments opened Melissa.

When the ExploreZip worm landed, the much larger group of people who were taught not to open suspicious attachments opened ExploreZip and these people were once again reminded not to open suspicious attachments. Now the VBS/LoveLetter worm has come and the huge audience who were taught from ExploreZip not to open suspicious attachments did so. Proof that education does not work? It might be an excuse to quit trying, but it is *not* proof that education does not work. It is, however, proof that bad teaching is ineffective.

Anti-virus is a particularly challenging subject to teach. Up until the past year or so anti-virus software was the one thing that the aliens in the movie 'Independence Day' wished they had, but viruses were still a rarity to the common user outside of the realm of the large corporation or the silver screen.

This means that for many people viruses are essentially theoretical in nature. This applies even to uneducated users who have launched Melissa, but do not have any notion of how a program works – it is fairly close to theoretical stuff, or black magic perhaps. Theoretical materials tend to be more challenging to teach. Most people learn better from what they can see, hear, or touch. When we couple obscurity with vagueness and mix it with a subject that normal people read about to combat severe bouts of insomnia, we have a subject that is, at the very least, a challenge to teach. I maintain that this is not an insurmountable task.

In order to teach the subject of anti-virus we must keep the following criteria in mind.:

1. The subject must be perceived as relevant to the audience.
2. The subject must be presented at the audience's skill level.
3. The subject must be made to be interesting. The more visual your examples the better your chances are of making a lasting impression on most people.

Tried and Tested Techniques

I'll share with you some of the techniques I have found to be successful. It is good practice to define the terms you will use before teaching the subject.

I let the audience know it was OK for them not to know what a virus is because the experts do not all agree on what a virus is either! To support this contention I show a few definitions of a 'virus'. Ultimately, I end up showing the definition from *Dr Solomon's Virus Encyclopedia*: 'A program that replicates itself'. This is truly what the target audience needs to understand, so I contrast this with examples and definitions of Trojans and hoaxes.

Much of teaching anti-virus is teaching best practices. This includes dealing with attachments. One of the best practices I teach is to obtain files from their source whenever possible. To tie together virus, hoax, Trojan, and the best practice of getting your programs from the source, I use the 'Frog-in-the-Blender' program which you can get from http://www.joecartoon.com/.

The example was set up first by showing a frog who gets the 'wart' virus. The students can see the wart attached to the frog. Next, the frog swims with his buddies in the same pond and they all get the 'wart' virus. Rather than give another visual of a worm, I simply point out how the *virus* attached itself to the host program (or frog) and became a part of it, whereas a worm does not. I remind my students that they have all seen a dog with worms and suggest it might be better to leave the visual alone at this time.

The next slide shows our frog, sans wart, in front of a really fancy door. Above the door is a sign that reads 'Welcome to Paradise'. Here is the Trojan. The frog believes that he is entering Paradise only to find out that 'click' – he is the frog in the blender! As the frog spins around and around I explain that a Trojan might do this (scrambling) to your

data. As the frog guts fly out of the top of the blender I observe that nothing about the frog will ever replicate again, and *viruses* replicate. The use of humour and a visual makes for a very effective means of conveying the information in a memorable format.

After the class has recovered from the display of frog entrails, I take the time to tie in hoax, joke, and a best practice. The 'Frog-in-the-Blender' is a joke program. The email warning that went around saying that this was infected with a virus that would kill your computer was a hoax. If you downloaded it from www.joecartoon.com you knew you were getting a safe program, but if a friend of yours ran it on an infected computer and then sent you the executable…

Attach with Care!

Perhaps the weakest part of most anti-virus education has to do with email attachments. Time and time again we see proof of this. Incredulous administrators will throw their hands up and proclaim that they told the stupid users not to open suspicious email and they opened it anyway.

During my last presentation I asked how many users were ever told not to open suspicious email or a suspicious attachment. Virtually everyone raised his or her hand. I then asked how many people were told what suspicious means with respect to email. Not a single hand went up.

A definition of terms is critical. You cannot hope to teach a subject if the term you use has an entirely different meaning from that which your students use it for. You have to define 'suspicious' in context. There is nothing suspicious about receiving email from people you know. What I teach is that it is the email and not so much the sender that is, and must be, viewed with suspicion.

An example I use is the potential to receive plain text email from a convicted murderer and the ExploreZip worm from your own mother. It isn't *who* sent the email; it is what is in it. I then explain that today you must look at the email suspiciously. If I send you an email proclaiming that the attached is a document that I promised you, but I never promised such a document, it is suspicious. You cannot trust that the email came from me and you have to be suspicious of the attachment.

I was once fortunate enough to have a perfect example of a suspicious email which came in the day before a presentation. The email came from an account called 'Microsoft Direct Access'. I explained to my class that I did not expect this email, so even though it came from my own company, or at least appeared to, it was suspect already.

After verifying that the alias used actually even existed, I went on to the attachment-handling phase. At this point I explained that if you do not need the attachment the safest thing to do is simply to delete it. Here, you have to be a realist. It is like the argument for sex education. People are not going to stop having sex if they are not told about it. Similarly, people should be told how to handle attachments in the safest possible way if they are going to open them.

I always explain that if you are determined to open the attached RTF (Rich Text Format) document, the proper steps would be to save the file to disk and verify that it is what you think it is. That is, if it has a picture icon, it must not have an .EXE extension. If it is supposed to be an RTF, then when you save it to disk it had better have an .RTF extension. Once the file is saved to disk, a virus scan is in order. In this case, the attachment is an RTF file, so the next appropriate move would be to open *Word* and verify that the security is set appropriately.

Only after these steps can you then proceed to open the document. I could have told the students not to open a suspicious email, but showing them a suspicious email, the steps used to identify it as suspicious, and how to deal with it are much more effective than just telling a story.

Make it Memorable

Another part of a successful anti-virus education includes teaching people about their anti-virus scanner. Most users are simply told to keep their anti-virus software up to date. For some people you may as well have told them to keep the debris out of their particle accelerator. Show your users how to launch their scanner, where to find out how current it is, and both *where* and *how* to update it.

I'm not going to say that teaching users about anti-virus is simple. You will always find some who refuse to learn, are unable to learn, or need medication to control their inclinations to double-click on anything that appears upon their desktop. You will also find that if you present the information in a meaningful and entertaining way you can reach your audience. People generally do not like to hurt other people. Once a person understands that a virus like Melissa can actually cause their friend's or business associate's confidential information to be broadcast publicly, they tend to see personal relevance and become more interested in anti-virus education.

Do not give up on your users. Provide resources where people can go to enhance their education. Some may argue that if people were truly interested they would go find the information themselves but if you are willing to make it easy for people to find the information to start with some of them will get 'hooked' and continue to learn on their own. I point people to http://claws-and-paws.com/virus and also http://antivirus.about.com. These sites do a good job of presenting information for beginners.

My presentation takes 90 minutes. The students feel it is a very good use of their time. Keeping people interested is the hardest part of the battle. If I can keep the audience interested in AV for 90 minutes then I am confident that anti-virus education is possible. If you don't think it can be done then kindly get out of my way… I am doing it.

TUTORIAL 2

Safe Hex in the 21st Century: Part 1

Martin Overton
ChekWARE, UK

Remember the Chinese curse – 'May you live in interesting times'? Well, we are living in very interesting (and busy) times – consider yourself cursed!

A Safe Hex on You

With the boundaries between data and executables becoming ever more blurred, and the Internet and email becoming an integral (and indispensable) part of everyday life, many are feeling that what was once considered safe to use is becoming increasingly fraught with unexpected dangers. Are the following fears real or rubbish?

- Emails that trigger payloads on preview or opening, people clicking on email attachments that promise love, free sex site codes, or whatever.
- The threat from a boot sector virus still haunting us almost 10 years after its creation.
- *Excel* spreadsheets fast becoming one of the main infection vectors within many companies.
- Drawing files that contain macro viruses.

It is no wonder many believe the hoax virus messages that circulate in many companies. Fact and fiction are getting mighty close! How can the users (and even the security officers) ever expect to learn about the growing number of threats in terms that they can understand?

This article aims to offer advice and suggest tools or methodologies that can be used in organisations that are battling with the scenarios outlined above.

Let's Start at the Very Beginning

Some people argue that technology is to blame, or that *Microsoft* is responsible for putting functionality before security. However, you must remember that it is ultimately (in most cases) a human being pressing the buttons, and this is the root of the problem.

I think we can all agree that *Microsoft* and other software vendors are partially responsible, but remember that we (the consumers) have helped make them what they are by our constant 'need' for improved usability and integration when it comes to technology. In effect, we have created a monster, and now we have to pay the price – bring out your Internet and computer virgins and offer them up to appease the beast!

Many people think that user education is the key to dealing with malware issues. At VB'96 in Brighton, I came to the following sad conclusion: 'You may think that trying to educate your staff about the risk of viruses is like trying to nail jelly to a wall, and about as rewarding, and in most cases you are right. Your non-IT staff will generally be either blasé, paranoid or simply ignorant about viruses. They simply see it as not being their problem.'

Last year's appearance of Melissa and last month's fiasco with 'The Love Bug' aka VBS/LoveLetter.A (and its many offspring), have forced me finally to acknowledge that anti-virus software is at least partially responsible for the 'it-can't-happen-to-me' attitude of users!

Why? Ask a user why they will read almost any email sent to them (no matter how suspect or frivolous it appears), and in many cases even blindly run attachments, with hardly a second thought. Are they really so insecure, desperate for attention, or careless? No! They think they are safe *because they run anti-virus software* – 'the panacea for all that ails!' How else can you explain why normally intelligent and otherwise savvy people risk opening the electronic version of a mail bomb?

I know some of you will disagree with my conclusion that user AV education is generally a waste of time. However, in my defence I would like to enter the following. Your PC Support and other technical staff *are* worth educating as they tend to understand the technology better and actually might be interested in what you have to offer.

Some of them may want to penetrate the mystic aura surrounding viruses and AV, and may believe you when you tell them it does not require them to chant strange incantations over the entrails of viral samples [*or frogs! Ed.*], and attend secret meetings at nodal points during the year. (Well, at least they might believe the incantations part!) If nurtured correctly this interest may actually blossom and you could end up with another valuable member of your security or anti-virus function or team. If nothing else, it might help to spread the burden and the skills.

Well, enough ranting (for now). Let us have a look at the problems and some suggestions on how they might be reduced or neutralised.

Know thine Enemy

Continuing on the education theme, obviously most of you (who are still awake) reading this are very interested in keeping up to date with new threats, viral techniques, and protection methodologies. Well, let us look at the best ways to 'know thine enemy', because if you understand your enemy, you understand what drives them and more importantly, their Achilles heel.

Most, if not all, anti-virus (and other security) companies offer 'Email Alert Lists'. These can be an excellent way to keep up to date. Try to pick a good cross-section of mailing lists, from those that post 'at the drop of a hat' to the other end of the spectrum, those (few) that post about 'in-the-wild viruses' when they are actually in the wild.

What a Load of Bulletins

Another useful tool for the security managers and their staff are the numerous security bulletins, including the rather busy 'Microsoft Security Bulletin' pages on their Web site. These can warn of new security loopholes and if they are acted on can help to thwart new malware attacks that use the published exploits. A good example is the extremely widespread Kak worm and the earlier BubbleBoy virus, which uses the 'eyedog' exploit. *Microsoft* (for all its failings) posted a fix for this on 31 August 1999, yet today the Kak worm is still the most frequent virus I see trapped by many email scanners. Why?

Do very few IT or security staff monitor this useful site and the many others which feature known exploits for products used in numerous companies, or is it just a case of 'it-can't-happen-here' syndrome? I know some of you monitor these sites and some of you act on the information that you find. What are the rest of you doing – fighting and cleaning up the malware that uses these exploits?

Did you Myth Me?

How can virus hoaxes, other hoaxes, myths, chain letters, etc be defused successfully? This is a difficult, but not insurmountable problem. I do not know about you but I used to spend more time debunking and dealing with hoaxes than dealing with real viruses. Please note the past tense, as this is not the case now. How this state of affairs was turned around is revealed below.

Here are some guidelines as well as some useful links. As mentioned before, information and a good security policy can go a long way to managing this problem. However, information and a few savvy members of staff are probably the most important factors in the never-ending battle against the hoax email. The problem has got somewhat worse over the last eighteen months or so, as we have started to see malware that does what we always told our users could not be done.

Simply reading an email is no longer perfectly safe. HTML mail, along with Visual Basic Scripting (also known as *Windows Scripting Host*), JavaScript, and *LotusScript*, and possibly others, have shown that we must be careful. What we say is safe today may well be dangerous tomorrow. So, now let us get on to some possible useful methodologies for you to consider.

Set up a good hoax policy and get it endorsed by your board. Once approved, send it to all your staff, either electronically or as an addendum to their terms and conditions of employment. (You might want to check out the legal implications of this!) An example might look like this: *'If information about a new virus threat is received this must be passed to Security [or a named contact] for verification. They will then decide if a general alert should be posted, which will include a confirmation or denial of the reported threat and any further steps that are required. Only Security [or named contact] is authorised to distribute virus alerts. Failure to follow this policy may result in disciplinary action.'*

If you run an Intranet, put a link from your home page to a good virus hoax site, e.g. http://www.kumite.com/myths, or to just about any AV company on the Web. Or, I give you my permission to re-post the hoax and myths information pages from the *ChekWARE* site on your own Intranet. You can find this at http://arachnophiliac.com/hoax/.

The above simple recommendations have cut the re-posting of hoaxes by around 80% in one company. It has also significantly reduced the number of calls that the company's help desk receives about hoaxes and other related electronic ephemera.

Still Putting the Boot In

Why is the Form virus still a problem in many companies and how can the threat from it finally be eradicated? This venerable boot sector virus is still a regular in the *Virus Bulletin* Prevalence Table and has hardly been out of it since Form was released. Why are we *still* seeing infections from this non-Internet, non-File, sneaker-net-dependent virus? A simple and cost-free change on any PC built in the last five or six (or maybe more) years can render Form incapable of infecting.

To take the sting out of Form and other boot (DOS Boot Record) and partition (Master Boot Record) sector-infecting viruses, simply change your CMOS boot-up sequence from the usual default of A: drive then C: drive to C: drive then A: drive. This means that if you accidentally have a floppy infected with a DBR virus like Form or an MBR virus like Parity_Boot, you could boot by default from drive C instead, thus robbing the boot sector virus of its ability to infect another system. If you do occasionally need to boot from a floppy disk, then the CMOS can be quickly switched back to the default A: drive then C: drive (but do not forget to switch it back again). This simple trick will defeat all pure boot and partition-infecting viruses, but not multi-partite samples in their boot sector-infecting state.

In Summary

Hopefully this has given you something to think about. I welcome feedback and comments, both via *Virus Bulletin* or private email (martin@arachnophiliac.com). The next part of this article will deal with what can be done to minimise or neutralise the risks from the greatest threats to many companies – emails, attachments and the scourge of Macros, VBA, *WSH*, etc.

PRODUCT REVIEW 1

F-Secure Anti-Virus v5.01 Part 2

Last month, we looked at the installation and central management of *F-Secure Anti-Virus* (*FSAV*). In this second and final instalment, we look at the client-side component of the package, specifically its operation and performance.

Installation

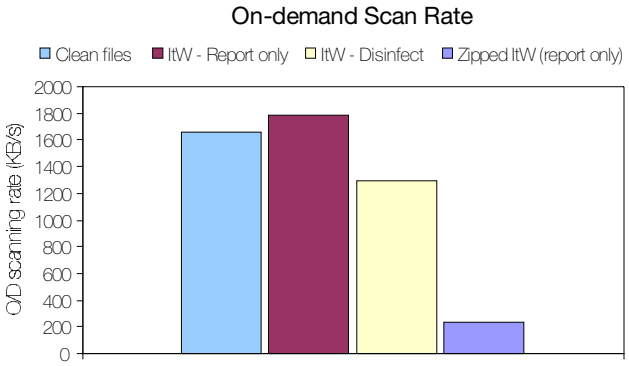
FSAV can be pushed onto workstations from the central management server using *F-Secure Administrator* (*FSA*), or it can be installed directly onto the workstations as a standalone application. The former method was used during testing for both the installation and updating of *FSAV*. Virus signature updates for each of the constituent virus engines (*AVP* and *F-Prot*) were downloaded from the *F-Secure* Web site and centrally distributed to the client scanner.

Once installed, access to *FSAV* is enabled via the *F-Secure Manager* (*FSM*) icon in the taskbar, via context menus within *Explorer*, or from the *Windows* Start Menu. The level to which users can see and control the *FSAV* settings is determined by the centrally-administered policy (for centrally-managed *FSAV* installations that is).

Three property pages comprise the body of the client-side *FSAV* scanner. The visibility and adjustability of the two that are used for configuring and controlling real-time and on-demand scanning are governed by the central policy settings (for centrally-managed installations). Thus, a typical configuration may therefore entail users having the ability to configure and initiate on-demand scans, but no means of disabling or configuring real-time protection. A third property page presents the real-time scanner statistics, and a fourth, presenting manual scan statistics, appears transiently during an on-demand scan.

Performance

On-demand scanning speeds were determined for scanning various file sets, some containing clean files, some infected files. The throughputs returned across the various sets are presented for comparison in the graph below. When set to disinfect the ItW sample set, the observed throughput dropped accordingly – *FSAV* reported 747 of the 788 samples to have been successfully disinfected, although the 'work done' during disinfection was not quantified. Finally,



the archive scanning rate was investigated by setting *FSAV* to scan a single ZIP archive containing the entire ItW set. A throughput of approximately 250 KB/sec was observed.

The overhead of the on-access scanner (*Gatekeeper*) was then measured. For this, sets of files were copied between directories on the local hard disk. The overheads presented here were obtained by comparing the average times observed with *Gatekeeper* enabled, to those with it disabled. *FSAV* is one of the relatively few AV products to offer users the facility of on-access ZIP archive scanning – the overhead of which is also presented below.

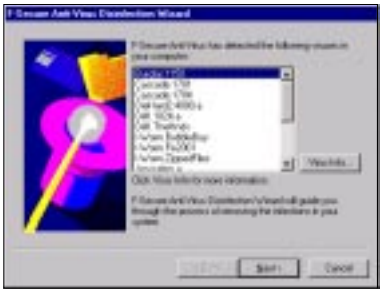
The overheads observed were typical of those observed in previous Comparative Reviews – a touch larger than those observed with some other AV products, attributable in part to the use of two virus engines in *FSAV*.

File set	Percentage Overhead
Executable/OLE2 files	140%
ZIP'ed executable/OLE2 files	657%

Detection Results

The test-set used for detection rate tests is detailed at the URL listed at the end of this review. The test-sets were constructed immediately prior to obtaining the signature updates, and, importantly, the contents of the In-the-Wild (ItW) set were aligned to the April 2000 WildList (see http://www.wildlist.org/).

On-demand detection rates were determined from the scanning logs produced by *FSAV* – which are now in HTML format, providing convenient links to the on-line *F-Secure* virus encyclopaedia. Upon finding infected files, *FSAV* presents the user with the *Disinfection Wizard* – a utility that provides options



to delete, rename or disinfect the infected files. For networked installations, the utility may not start if the action to take upon detecting an infection is fixed via a centrally-managed policy.

As has often been noted in past Comparative Reviews, *FSAV* reaps the benefit of utilising two well-ranked virus engines (*F-Prot* and *AVP*) when attention is focused upon detection rates. During testing, *FSAV* maintained this reputation in only missing a few viruses across the entirety of the test-sets. By default, only files of specific extension are included in on-demand scans. This resulted in various samples being rather needlessly missed – for example, the extensionless *Excel* files infected with variants of O97M/Tristate, and a series of batch files associated with the recent BAT/Firkin worm. Additionally, neither *Windows* help (HLP) nor ActiveX control (OCX) files are included in the default extension list, and so samples infected with Win95/Babylonia and Win32/Flcc were missed from the ItW set. Pleasingly, on-access results mirrored those observed during on-demand scanning.

With *FSAV* set to include all files in both on-demand and on-access scanning, only samples associated with two viruses were missed. These samples were the HTA file that is dropped into the *Windows* startup folder by JS/Unicle.A (a recent, and perhaps 'surprise' newcomer on the April WildList), and the PIF files associated with 911/Firkin – not in themselves viral, but constituent parts of this multi-part worm, responsible for launching other batch files.

Summary

One of the most significant changes introduced in this latest incarnation of *FSAV* is the slimmed down client-side component. And the result? For the administrator – easily configurable, tamper-proof AV scanner roll-outs. For the user – a simple-to-use interface, which (as is the way for most AV scanners nowadays) is pretty much 'invisible' to the user but for the taskbar icon.

FSAV behaved impeccably throughout testing, and no real surprises were uncovered – two engines returning high detection rates, at a small cost to performance. The only complaint is one associated with the HTML formatted scanning logs, which tend to become quite cumbersome thanks to the plethora of HTML tags within.

Technical Details
Product: *F-Secure Anti-Virus*
Version: *FSAV v5.01.5364, FSA v4.02.861, FSMA v4.02.830*
Test Environment: *Server*: 450 MHz AMD *K6* with 128 MB of RAM, 8 GB hard disk, running *Windows NT 4.0 (SP5), and Internet Information Server 4.0*.
Workstations: Three 166 MHz Pentium-MMX workstations with 64 MB RAM, 4 GB hard disks, running *Windows NT 4.0 (SP5)*.
Detection Rates: On-demand and on-access results were as follows: ItW – 99.3%, Standard – 99.5%, Macro – 99.7%, Polymorphic – 100.0%.
Test-Sets: Complete listings of the test-sets can be found at: http://www.virusbtn.com/Std/200006/test-sets.html

PRODUCT REVIEW 2

Norman Virus Control for Lotus Notes v4.73

The second review this month takes a look at *Norman's* groupware product for the *Lotus Notes* platform – '*Norman Virus Control for Groupware with Lotus Domino Plug-In*' (hereafter referred to as simply *NVC*).

The Package

Contrary to the customary submission of products clad in their full packaging, *NVC* was submitted entirely electronically – the 'package' comprising the core installation files, an engine update, recent signature files, and a patch to fix a minor bug (associated with on-demand scanning).

A PDF of the user manual was included within the installation files, which detailed the installation, configuration and administration of *NVC*. A quick flick through the manual suggested that it is perhaps time for it to be reviewed. At least one comment – '*Mail scanning involves scanning of attachments, not the actual message body, which cannot carry viruses*' – is misleading and should be removed, with the recent increase in script-based malware, and the potential vulnerabilities of *Notes* hotspots and scripts.

Installation

NVC has to be installed on the *NT* server running *Lotus Domino*, whilst logged in as administrator. Remote installations are not possible – something of a drawback when that server is deep within a murky server room. Prior to commencing with the installation, the *Notes* directory on the *Domino* server must be included in the path and system environment variables. This satisfied, the installation proceeds via a standard *InstallShield* interface. File copying is completed in seconds – only just over 5 MB of files are written to the server in total. Finally, a message box reminding the administrator to restart the *Domino* service for real-time scanning to be enabled, is shown.

The front-end module alone can be installed to workstations in order to allow remote configuration by the administrator. No consideration as to how to install the front-end on workstations is given in the manual or help, but simply copying the executable file associated with the module (NVCGW.EXE), together with other identically stemmed files (CNT, HDR, GID and HLP) proved to be sufficient. The front-end module could then be launched by simply running the NVCGW.EXE executable. If someone other than the administrator tries to run the module, then upon attempting to connect to the *Domino* server, access is denied and a warning box stating the need for administrative privileges is shown.

NVC Architecture

Three components comprise *NVC* – the graphical user interface (the 'front-end' module discussed above) for configuration, the *NT* service module, and the on-demand and real-time plug-in modules. Amongst other things, the service module is responsible for communication with the *NT* Registry. Configuration settings which can be manipulated via the front-end module are written to the Registry by the *NVC* service module.

Some other AV products interface more closely to the *Notes* environment than *NVC* chooses to. Instead of using a *Notes* database through which the scanner can be configured and enabled, *NVC* adopts a 'plug-in' approach (hence the rather long product name). Operating as an *NT* service, *NVC* hooks all 'open' events in the NSF subsystem. Thus, incoming and outgoing mail is scanned when it is written to the MAIL.BOX database. Outgoing mail is also scanned when written to the MTA queue databases.

To ensure the real-time hook is started with the *Domino* service, a pointer to the real-time hook DLL is added to the NOTES.INI file during installation (hence the need for restarting the *Domino* service following installation).

For products that utilise a *Notes* database for configuring and enabling the scanner, access to the relevant database (required for remote administration) is controlled by the *Notes* Access Control Lists (ACLs). With the approach taken by *NVC*, remote configuration is governed by *NT*-controlled user access. Assuming administrator privileges are available, *NVC* can be configured, updated or used to produce logs from any workstation on the same network as the *Domino* server. Multiple *Domino* servers can be administered from a single workstation – upon loading the front-end module, the administrator is prompted for the identity of the target server.

Administering NVC

The *NVC* service module is installed with automatic start-up and so will start when the server is restarted. Subsequently, the service can be stopped/restarted either from the command line, using the *NVC* front-end module or via the *NT* control panel.

The *NVC* front-end module presents the administrator with a simple and straightforward interface, and 'mission-critical' information (service status, virus signature file dates, and number of infected files found) is displayed in the main window. The interface bears a clear family resemblance to other *Norman* AV products. Buttons on the toolbar enable the user to select the target server, stop/start the service, alter scanning options, view statistics or the viewing log, and initiate an on-demand scan. Access to the same facilities is also provided via the drop-down menus.

Configuration changes are made through four pages containing scanning, infection, alarm and logging options. A button to reset the options to the 'out-of-the-factory' defaults is provided. Peculiarly, *NVC* does not separate the real-time and on-demand scanning options into separate pages – all configurable options are bundled together within the four property pages. Certain options (e.g. 'scan within archives' or 'clean infected attachments') apply to both the on-demand and real-time settings. A certain amount of flexibility is therefore removed – it is not possible to set the real-time configuration and then set temporary configurations for on-demand scans for example.

Aside from the fact that the on-demand and real-time configuration settings are shared, the options are as might be expected. By default all *Notes* documents which contain no mail properties are not scanned. (The mail-determining criteria used by *NVC* are the 'SendTo', 'CopyTo' and 'BlindCopyTo' fields of the document – if all of these fields are blank, then, by default, the message is not scanned.)

The Enemy Within

It is imperative for gateway and mail-server AV products to be able to scan within compressed or packaged files. A variety of archive formats must be handled, as should a (growing) number of 'package' formats. To investigate the capabilities of *NVC* in this area, a file set based on the EICAR test file in its various archived, encoded and packaged incarnations was used.

As can be seen from the table within this review *NVC* lets itself down somewhat in terms of archive and package handling. Only PKZIP and ARJ compression formats were handled, and none of the tested encoded or package formats were handled whatsoever. This included the *Microsoft* 'Scrap Object' format (SHS) which is known to have been exploited recently by Trojans and viruses. Within multi-tier AV deployments, the area where there is a real need to handle a wide variety of package and archive formats is at the mail-server or firewall scanner. This issue is one that requires attention from the *Norman* developers.

Password-protected ZIP files pose something of a problem to mail-server AV scanners. From the manual it appears that *NVC* approaches the problem in a similar manner to other products – the encrypted archive can be removed. However, even with *NVC* configured to perform this action, such behaviour was not observed. Instead the encrypted archive was successfully delivered and the scanning log registered the file as clean, as if successfully scanned.

File format	Handled?
ZIP	✓
Nested ZIPs	✓
ARJ	✓
GZIP	✗
RAR	✗
LZH	✗
TAR	✗
UUE	✗
XXE	✗
MIME-64	✗
CAB	✗
SHS	✗

Specific to the *Notes* platform are threats associated with hotspots. From *Notes v4.5*, hotspots support the use of @Commands, enabling a variety of operations such as executing external programs or composing/printing documents. Perhaps more susceptible to exploitation is the support for a full object-oriented programming language, *LotusScript* – in a sense, the *Notes* equivalent to VBA. AV scanners truly native to the *Notes* environment should offer the facility to scan documents for malicious hotspot and script content. Sadly, at this point, *NVC* does not offer this.

Dealing with Infections

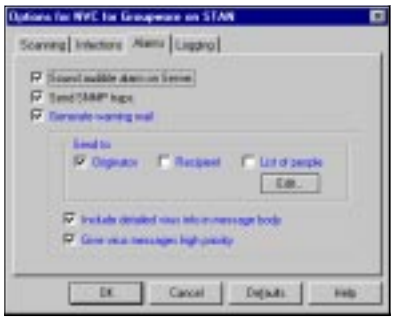
The action to take upon detecting an infection can be set from within the scanning options property pages. By default, an attempt to clean infected files is made, and if disinfection is unsuccessful, the attachment is removed.

Infected attachments are also copied to a quarantine directory on the *Domino* server, and renamed with a '_n' suffix (EICAR.COM is renamed to EICAR.COM_0 for example). *NVC* provides no facility to delete, re-route or continue the delivery of attachments that have been copied to the quarantine.

Alerting & Logging

Three alerting mechanisms upon finding an infection are provided by *NVC* – SNMP traps, email notification and an audible alert on the server. By default, email notifications are sent to the sender, but the intended recipient and additional people can also receive notifications if desired. Since *NVC* makes no distinction between incoming and outgoing mail, administrators should obviously be cautious before configuring *NVC* to send notifications to the recipient!

NVC can log service information and infection reports to three locations – the *NT* event log, the server console, and the *NVC* service's log file. Four levels of information can be logged:

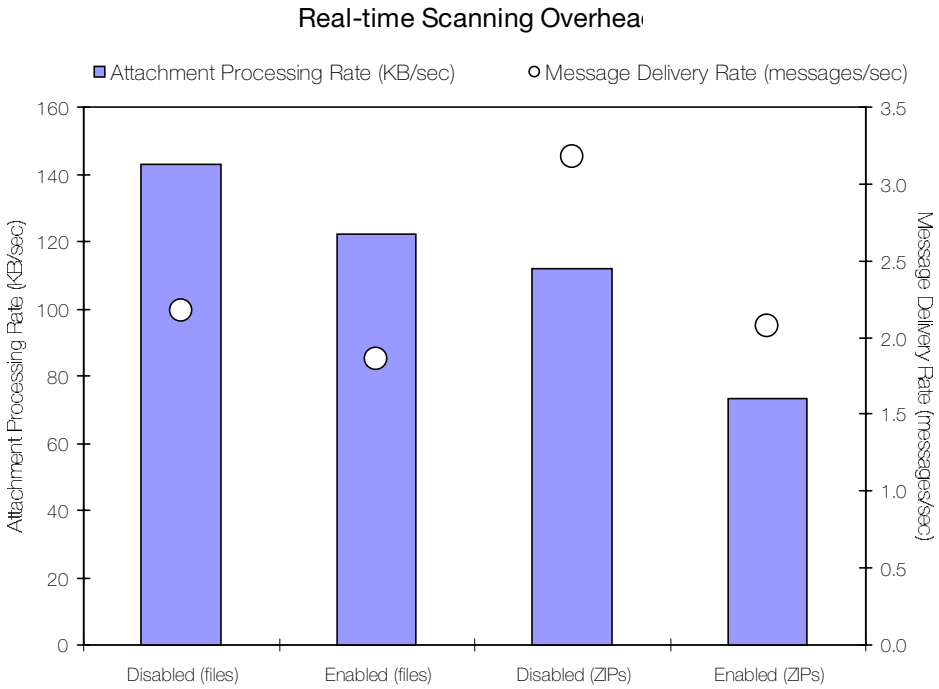


infections (infected files, virus name, database name etc), errors (system errors), warnings (when *NVC* fails to perform a task) and general information (details of the tasks performed). Additionally, an option to perform verbose logging is presented, which results in extremely detailed logs (which can grow to quite a size very quickly). To combat oversized log files, *NVC* provides the option to create a new log file each day, a full history of the daily logs preserved.

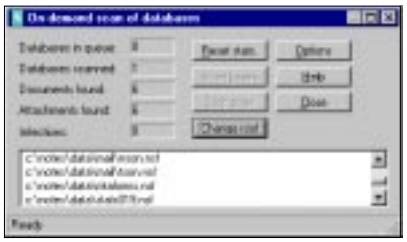
A button on the toolbar within the front-end module gives access to the statistics *Window*. Only a brief statistics summary is presented, lacking the sophistication of some of the statistics presentations in other AV products. Only four pieces of data are displayed – total files scanned, number of infected files, the name of the last virus and the date and time of the last alarm.

On-Demand Scanning

An essential component of any mail-server AV product is an on-demand scanner, capable of searching within the constituent databases of the specific mail system. Duly, *NVC* provides an on-demand scanning facility, accessible from the front-end module. On-demand scanning is controlled from a very simple console – a specific directory (the 'root') is selected, and all the NSF databases within that directory are shown in the lower panel. The databases to



scan can then be selected, and the scan initiated. The console includes a link to the shared scanning options property pages, and a brief summary of the on-demand scan statistics (which are resettable).



The on-demand scanning speed of *NVC* was measured by setting it to scan a mailbox containing a series of messages, each bearing a single, clean file attachment. The process was repeated for compressed (PKZIP) file attachments.

Target File Set	Scanning Rate (KB/sec)
Clean Executables	1044.6
Zipped, Clean Executables	134.8

Performance

The final two areas of performance investigated in this review are real-time scanning overhead, and virus detection rates. The real-time scanning overhead was measured by comparing the message delivery rates for a series of 1000 emails (each bearing a single, clean, executable file attachment) with and without *NVC* installed. The process was then repeated using a stream of emails bearing the same files, but this time compressed using PKZIP. Message delivery rates were determined with reference to the routing logs on the *Domino* server. The rate of message delivery has been expressed in terms of average attachment processing rate (KB/sec) and message delivery rate (messages/sec) within this review. As can be seen from the graph, *NVC* imposes a measurable overhead upon the message delivery process. In terms of attachment processing rate, *NVC* imposed overheads of 14% and 34% for real-time scanning of emails bearing the clean and zipped, clean executable files respectively.

The detection capabilities of *NVC* have been assessed using a utility running on a *Linux* box, which was used to generate Internet mail. The utility opened an SMTP session with the *Domino* mail server, and, for each file within a directory tree, generated a single email bearing that file. In this way, a stream of emails, each bearing a single file from the customary *VB* test-set (bar the Polymorphic set), was generated. Importantly, the ItW set was aligned to the April 2000 list. Complete listings of the test-set contents can be found at the URL listed at the end of this review.

NVC was configured to remove infected attachments throughout the detection rate tests, and so missed samples were evident as attachments within the target mailbox. All detection rates were confirmed by reference to the *NVC* log files as well. Observed detection rates were respectable, if not quite at the level that *Norman* products typically perform in *VB* Comparatives. Failure to detect HyperText Application (HTA) files infected with VBS/BubbleBoy, JS/Kak.A and JS/Unicle.A prevented complete detection against the ItW set. Misses associated with HTA files continued in the Standard set – all the HTA files infected with variants A-through-F of JS/Kak were missed, yet the related HTM files were detected. A small handful of infected VBS files were also missed from the Standard set. Results were best in the Macro set, where the only misses were a proportion of the MDB samples infected with the A and B variants of A97M/Accessiv.

Summary

In many ways *NVC* proved to be a pleasant product to test. Its installation was straightforward and problem-free, and no peculiar behaviour was observed throughout testing. In terms of virus detection, the weakest area appeared to be against script viruses – a selection of VBS viruses and infected HTA files being missed. Nonetheless, the observed detection rates were still high. On-demand and scanning performance was on a par with competitor products (if a little slow with archive scanning).

Sadly, *NVC* does lack some of the features that other products offer. Mail-server AV products are well complemented by some form of content control. The benefit of such a feature is exemplified by the recent experiences with mass-mailers such as VBS/LoveLetter – in the interim period between the outbreak and the obtaining/distribution of signature updates, a number of administrators combat such malware by blocking mail at the server using subject and body content filtering. *NVC* would also benefit from slightly more sophisticated alerting mechanisms. Administrators may not want to receive email notification of each and every infection, but they may want to receive an alert if say, more than 10 infections are reported in a 30 minute period. Putting bonus or 'add-on' features aside, *NVC* also failed to cope with a sufficient range of archive and packaging formats – something that needs to be addressed.

Finally, one is left with mixed feelings about this product. The *Norman* virus engine at its heart provided the expected detection rates, and no actual problems were experienced. However, there are a few areas in which the product is found wanting. One suspects that the next revised version will remedy some of these problems, thereby producing a more well-rounded and better equipped product.

Technical Details
Product: *Norman Virus Control for Groupware with Lotus Domino Plug-In*
Version: *NVCgroup* service 4.73, Engine 4.70.56, Virus signatures 4.70 (27/04/2000)
Test Environment: *Domino Server*: 450 MHz AMD *K6* with 128 MB of RAM, 8 GB hard disk, running *Windows NT 4.0 (SP5), and Lotus Domino 4.6a*. *Workstations*: 166 MHz Pentium-MMX workstations with 64 MB RAM, 4 GB hard disks, running *Windows NT 4.0 (SP5)*.
Detection Rates: On-demand and on-access results were: ItW – 98.7%, Standard – 97.7%, Macro – 99.8%.
Test-Sets: For listings of the test-sets & detection results see: http://www.virusbtn.com/Domino/200006/nvc.html

PRODUCT REVIEW 3

Complex Associations

In January 1999, *Computer Associates* acquired the Australian *Cybec Vet Anti-Virus* product developer. Subsequently, they distributed the *Cybec* product, free to home users, from their own Web site – rebadged as *InoculateIT Personal Edition* (*IPE*). Additionally, the original *Cybec* product is still sold, now under the name *Computer Associates Vet Anti-Virus* (*Vet*) – the name under which it features in *VB* Comparatives. A spate of enquiries to *Virus Bulletin*, coupled with a recent thread on alt.comp.virus, have prompted this review, which will outline any differences between *IPE* and *Vet*, two seemingly identical products.

The Packages

The 'fully boxed' product of *Vet* was used for testing, exactly the same product that was submitted (on 26 April) for testing in the next Comparative Review. A self-extracting executable comprising *IPE* was obtained by download from the *Computer Associates* web site at the same time.

Installation

The products both use an *InstallShield* interface to aid installation, installing by default to the locations 'C:\Vet' and 'C:\Program Files\InoculateIT PE' for *Vet* and *IPE* respectively. *Vet* provides an option to perform a master installation – designed for administrators needing to roll-out installations to many workstations across a network. Because *IPE* is distributed for individual use, it does not provide this option. To protect the configuration settings, *Vet* offers a password protection facility that is configured during installation. With *IPE*, this option is enabled once the product is installed, and not during installation.

The final part of installation is the same for both products; the user is prompted for start-up options, real-time settings and the option to create boot sector templates. Finally, the user is prompted to restart the machine.

Both products, unsurprisingly, imposed similar footprints in terms of file space. Slightly more files were installed with *Vet* – this fact is attributable to a handful of files associated with an HTML page and its associated GIFs. For this review, three DAT files were copied from the *Vet* installation to that of *IPE*, such that the same signature files were used for testing both products, although it should be noted that each had slightly different virus engine versions.

Using the Products

Following installation (assuming that the option to add an icon in the taskbar was not disabled), the status of the products is displayed upon holding the pointer over the icon. Both products can be loaded from the start menu or from the taskbar icon, and file scanning can also be initiated from context menus within *Explorer*.

The configuration settings are accessible from the drop-down menus, and, logically, are divided amongst program (on-demand), real-time and alerting options. For the most part, the options available are identical for *IPE* and *Vet*. The options selected by default are almost the same as well. There are some important differences however:

- *Vet* offers two levels of scanning – 'Fast' (entry-point scanning, the default) and 'Full' (a grunt scan). *IPE* offers only entry-point scanning.
- *Vet* caters for scanning of files on network drives. The tested version of *IPE* had this facility disabled for both on-demand and real-time scanning.
- By default, *Vet's* real-time scanner includes all files, whereas *IPE's* includes only 'program files'.
- *IPE* can only handle archives of ZIP format, whereas *Vet* handles a wide variety of archive and package formats including ZIP, ARJ, GZIP, UUE, MIME, and CAB (see *VB*, April 2000, p.17).

Performance Summary

During the detection rate tests, the above differences between *IPE* and *Vet* clearly manifested themselves in the observed results. On-demand results were identical (despite the engine versions differing slightly), but *Vet* outperformed *IPE* during on-access scanning, thanks to *IPE* ignoring certain file types. Were the two products tested under the usual *VB* Comparative 'default configuration' rule, differing percentages would be reported for each, despite using identical virus signatures.

Is it fair to extrapolate *Vet's* Comparative Review results to its *IPE* blood-brother? Assuming that the same engine and signatures files are used, and you pay attention to the configuration settings and con-figure the products identically, then yes, it is fair. Not all the differences can be corrected with tweaking though –most significant is *IPE's* inability to scan network drives and handle the range of archives and package formats that *Vet* does.

Technical Details
Products: *Computer Associates Vet Anti-Virus* (*Vet*), *Computer Associates InoculateIT Personal Edition* (*IPE*).
Versions: *Vet* v10.1.8.6, *IPE* v5.1.0.6
Signature Files: Major v300, Minor v339, Macro 26/04/2000
Test Environment: *Workstations*: 166 MHz Pentium-MMX workstations with 64 MB RAM, running *Windows 98*.
Detection Rates: For on-demand & on-access results see: http://www.virusbtn.com/Std/200006/vet_ipe.html
Test-Sets: Complete listings of the test-sets can be found at: http://www.virusbtn.com/Std/200006/test-sets.html

SUBSCRIPTION RATES

Subscription price for 1 year (12 issues) including first-class/airmail delivery:

UK £195, Europe £225, International £245 (US$395)

Editorial enquiries, subscription enquiries, orders and payments:

Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP, England

Tel 01235 555139, International Tel +44 1235 555139
Fax 01235 531889, International Fax +44 1235 531889
Email: editorial@virusbtn.com
World Wide Web: http://www.virusbtn.com/

US subscriptions only:

VB, 50–S Audubon Road, Wakefield, MA 01880, USA

Tel (781) 213 9066, Fax (781) 213 9067

END NOTES AND NEWS

VB2000, *Virus Bulletin's* 10th international conference, is to take place on Thursday 28 and Friday 29 September 2000 at the Hyatt Regency Grand Cypress Hotel in Orlando, Florida. The full colour conference brochure contains programme details of the line-up of technical and corporate sessions, evening social events, the concurrent exhibition and accommodation information. To reserve your copy or to enquire about exhibition opportunities at the event, contact Karen Richardson; Tel +44 1235 544141, email VB2000@virusbtn.com or visit http://www.virusbtn.com. The Web site also contains details of the new subscriber bonus open to VB2000 delegates.

***Symantec's Norton Anti-Virus* now scans and analyses files in ELF format** – the format used by the *Linux* platform – in anticipation of the creation of Linux viruses. In an unrelated announcement, the company confirms that it has been granted a **patent for technology to speed up the process of scanning files on PCs and servers as well as those sent over the Internet.** A modification of the old method of intermittent file content snapshots in the new technology eliminates redundant scans and reduces waiting times. For further information contact Lucy Bunker in the UK; Tel +44 1628 592222 or visit http://www.symantec.com/.

Sophos* will host a two-day Anti-Virus Workshop on 18 and 19 July 2000** at the organization's training suite in Abingdon, Oxfordshire, UK. Contact Daniel Trotman for details; Tel +44 1235 559933, or email courses@sophos.com. The company has also recently announced **a technological partnership with *SendMail to protect *SendMail* enterprise and service provider customers from Internet-borne viruses. *Sophos Anti-Virus Interface* (*SAVI*) is to be integrated with products in the *SendMail Switch* range, scanning incoming and outgoing messages, accelerating performance and providing IDs for virus information messages. For further details visit the Web site; http://www.sophos.com/.

The 17th world conference on Computer Security, Audit and Control focuses on all aspects of e-commerce. **CompSec 2000 takes place from 1–3 November 2000 at the Queen Elizabeth II conference centre in Westminster, London, UK.** There are still exhibition opportunities available for this show. For details visit the Web site http://www.elsevier.nl/locate/compsec2000 or contact Gill Heaton; Tel +44 1865 373625.

The 16th Annual Computer Security Applications Conference (ACSAC) will take place from 7–11 December 2000 in New Orleans, Louisiana, USA. Visit the Web site http://www.acsac.org for more information or email publicity_chair@acsac.org.

***Kaspersky Lab* announces the availability of its new product *AVP for QMail*.** Aimed at the business sector, *AVP for QMail* features anti-virus filtering capabilities for both internal and external (incoming and outgoing) email passing the gateway. A beta version is available for download free of charge from http://www.kasperskylab.ru/.

***Norman Data Defense Systems* announces the launch of *Norman Internet Security*.** The product combines *Norman Virus Control* and *Norman Privacy* as one exclusive package especially aimed at addressing the home worker's Internet security issues. It is available for £49 +VAT for a single user including all updates, upgrades and technical support. For details email Dawne_Cook@Norman.com or visit http://www.norman.com/.

Dr Solomon's* (a business unit of *Network Associates Inc*) has included the core technologies *Dr Solomon's ePolicy Orchestrator* and *Anti-Virus Informant products in the *Dr Solomon's Active Virus Defense* (*AVD*) *Suite* to benefit e-businesses and managed service providers. The *AVD Suite* costs $30 per node at 5000 nodes. Also aimed at the e-business market is ***Dr Solomon's AVERT WebImmune* service** which provides Web-based virus research, offering instant cures and information. For more details visit http://www.nai.com/.

***F-Secure* has launched the *F-Secure Policy Manager* for the management of multiple applications on multiple operating systems from a central location.** This 'blanket security' extends from traditional LAN-based machines to smart phones and PDAs. For further information email Pirkka.Palomaki@F-Secure.com or visit the Web site http://www.F-Secure.com/.

In the wake of the LoveLetter virus episode, *Microsoft* issued an update for *Outlook* on 22 May. The patch warns users when a program is trying to access their address books or send email on their behalf. It also switches the default Internet setting from 'trusted' to 'restricted' and limits the types of file attachments it can open, including .VBS, .EXE and .BAT files. As yet, *Microsoft* has no plans to release a patch for *Outlook Express*.