ISSN 0956-9979 FEBRUARY 2001

VIRUS BULLETIN

THE INTERNATIONAL PUBLICATION ON COMPUTER VIRUS PREVENTION, RECOGNITION AND REMOVAL

IN THIS ISSUE:

• **Five minutes of fame:** the News page features stories on the latest threats that are making headlines around the world. See p.3 for details.

• **Miscellaneous musings:** three very different Opinions cover such diverse topics as email worms, Venture Capital and *MS Exchange*, starting on p.6.

• **ME, ME, ME:** a first for *Virus Bulletin*, this month's Comparative Review puts seventeen anti-virus products for *Windows ME* through their paces. The action starts on p.17.

CONTENTS

COMMENT

Great Big Expectations

“ Customers want to come to a one-stop shop … ”

I joined the AV industry a comparatively short time ago at the beginning of 1997. Needless to say, since then the industry has changed beyond recognition. There were many contributing factors: new operating systems, new versions of *MS Office* and some other software, an exponential increase of global connectivity – all of which produced new types of malicious threats, not to mention the fact that the virus writing (or rather malicious code writing) community is better organised than ever, thanks to exactly the same contributing factors. Many smaller AV companies were acquired by larger software vendors with different degrees of success, which should have simplified the picture; instead it was made even more complex.

Service requirements became much tougher. If, four years ago, weekly or bi-weekly virus signature updates were good enough, now we recommend they are performed daily. Viruses are not geographically isolated any more – what happens in the US is repeated two hours later in Australia. So we have the ‘follow the sun – help me now’ AV support issue. This fact alone puts serious strain on smaller AV companies, but falls into the ‘business as usual’ category for the larger ones. While viruses and other malicious threats have become more complex and tend to ‘learn’ one from another, they take new technical avenues which sometimes come as a surprise. So this leads me to another point – the necessity for serious pre-emptive research, because a reactive collection of new viruses and their variants is not good enough any more. Supporting research teams with an average research project cycle of several months is much easier for the larger vendors, and becomes more difficult for the smaller ones.

We have also come to understand that our customers, especially larger ones, don’t want to go to different places for different products (in our case, security solutions). Potentially this creates compatibility, service and support problems. Customers want to come to a one-stop shop and acquire a firewall, AV protection for their desktops, servers and gateways, intrusion detection software, access control and audit logging tools and of course, VPN, to accommodate their mobile users. Not many companies on the market can offer even two products from this list, which is why larger vendors command so much attention the world over.

Along with many other security vendors, we found it impossible to build security bastions around large company networks without taking care of small office and home (SOHO) users. This way or that way the threats would find their way from unprotected sources into even the most secure sites (human error is one of the ways). So, we decided that the best way to protect SOHO users is to provide very affordable software for them, using our research facilities which we have to have anyway to take care of our larger customers. At some overhead cost we can prove that we are good corporate citizens and at the same time improve our customers’ corporate security protection by supporting safe computing environments around the globe.

It is a widespread misconception that all security software vendors are in fierce competition with each other and therefore they don’t work together and don’t talk to each other. Well, one thing is perfectly clear, if the task of providing a secure computing environment worldwide is to be taken seriously, it is a must that all security vendors work together, most importantly at research and interoperability levels. To facilitate these communications it is incredibly important to have bodies like the *ICSA* or *Virus Bulletin*. Communicating with or via these bodies and cooperating with governing authorities in different countries definitely creates an environment in which the malicious code-writing community is antithetical. Does this spell death to smaller security vendors? Definitely not – there will always be market niches where they can happily fit. What I really wanted to show is that larger companies are not necessarily guided only by profit margins and revenue figures. We do care about safer computing environments everywhere and we support both communication and cooperation.

Dr Eugene Dozortsev, Asst Vice President R&D, Computer Associates International, Australia

NEWS

Melissa Macs a Comeback?

When will a well-known *Word* macro virus not be detected by several scanners? One answer many people discovered on 17 January is 'When it is in a *Word 2001 for Macintosh* format file'. Officially known as Melissa.W, this variant caused a minor outbreak, the reports of which suggest was mainly centred around UK sites.

The problem this incident exposed is that the recently released version of *Word* for the Macintosh has a small document file format change. This does not affect the ability of other versions of *Word* to read *Word 2001* documents successfully. However, it does prevent several virus scanners from handling such files properly. The undocumented change to the file format (a DWORD was changed to a WORD) means the code in many scanners that locates the p-code representation of a document's macros will fail – and if their p-code cannot be seen, viruses cannot be detected by scanners dependent on p-code analysis.

Melissa.W becomes immediately recognisable when it replicates to a *Word 97*, *98* or *2000* form from a *Word 2001* document. However, because the originally opened document is the one Melissa attaches to its outgoing email, the initial *Word 2001* document that started this outbreak may just keep on going and going and going … Most scanners with a weakness in handling *Word 2001* format files should have engine updates available soon ▮

Ramen Around

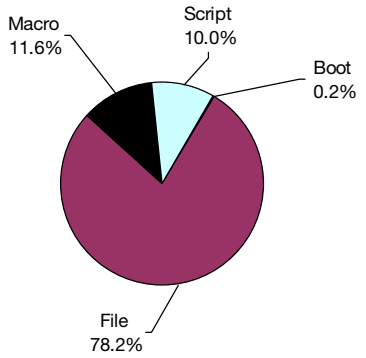
The *CERT Coordination Center* has issued a warning about the widespread distribution of the Ramen worm. The worm is a series of scripts and executables that take advantage of three old, but commonly unpatched, security vulnerabilities in services shipped in several popular *Linux* distributions. Ramen probes the network for potentially vulnerable hosts and when one is found, launches its remote root exploits against it. Should one of these exploits succeed, that machine connects back to the host launching the attack, downloads the worm kit from it (via a service the worm runs for this purpose), unpacks the archive file and runs the worm's 'installer'. Ramen also replaces any INDEX.HTML files it may find with its own. For more details see the Web site http://www.cert.org/.

Towards the end of January, Ramen was confirmed to be in the wild. Texas A&M University and a *NASA* site were reportedly hit, while fears are that the worm is quite widespread due to the number of inexpertly installed and maintained *Linux* machines out there. However, contrary to reports by some AV vendors, Ramen is not the first *Linux* worm and it is certainly not the first *Linux* worm in the wild. We ran an analysis of the under-reported Admw0rm back in August 1998 ▮

Prevalence Table – December 2000

Virus	Type	Incidents	Reports
Win32/MTX	File	1261	27.3%
Win32/Navidad	File	1190	25.7%
Win32/Hybris	File	502	10.9%
Win32/Prolin	File	447	9.7%
Kak	Script	286	6.2%
LoveLetter	Script	156	3.4%
Divi	Macro	140	3.0%
Laroux	Macro	88	1.9%
Marker	Macro	69	1.5%
Win32/QAZ	File	65	1.4%
Win32/Ska	File	50	1.1%
Ethan	Macro	42	0.9%
Win32/Funlove	File	36	0.8%
Thus	Macro	26	0.6%
Tristate	Macro	22	0.5%
Stages	Script	21	0.5%
Myna	Macro	18	0.4%
Cap	Macro	17	0.4%
Melissa	Macro	17	0.4%
Win32/Pretty	File	14	0.3%
Win32/Plage	File	13	0.3%
Class	Macro	12	0.3%
Win95/CIH	File	12	0.3%
Jini	Macro	8	0.2%
Story	Macro	8	0.2%
Win32/BleBla	File	8	0.2%
Others		94	2.0%
Total		**4622**	**100%**

[1] The Prevalence Table includes a total of 94 reports across 33 further viruses. A complete listing is posted at http://www.virusbtn.com/Prevalence/.



LETTERS

Dear Virus Bulletin

Help vs Hype

[*Having received a press release from* Norman Data Defense Systems *warning 'against over-reaction to deluge of new virus warnings', I asked the Manager of* Norman Virus Control's *engine development to give his opinions on this sensitive issue. Ed.*]

Norman Data Defense Systems issues warnings rather rarely in comparison with some other companies. This is an intentional policy which is elaborated on in the following URL:http://www.norman.no/technical_alertroutines.shtml.

Our way of doing things is not necessarily always the correct one, and fixed criteria on exactly what to alarm on do not exist. On the other hand, we do have some guidelines on how to act in a possible alert situation. This basically boils down to a discussion between analysts, support and the Development Manager on whether the virus in question has one or more of the following:

- new techniques that set it apart from others, and that require attention and/or special security measures to avoid
- large destructive potential (not enough *per se*, but carries weight in combination with other factors)
- high ability to propagate (analysis judgement)
- high actual spread (support input, cross-company cooperation)
- high attention level in media (sometimes we have to make statements to calm users).

If some of these factors are present we make a joint decision on whether we should issue a warning. All implicated persons are aware that if a warning is issued when it shouldn't have been (for example on something that we've seen only once and that has no spread potential), that may reflect badly on us personally and as a company, and may cause our warnings to carry less weight in the future.

What's the downside? Well, obviously, in the cases where we have ultrafast spreaders, they may infect everyone in the country while we are in discussion. That does not happen very often though – last time it happened was in the LoveLetter incident, and then no-one was in any doubt. The decision to alert was made instantaneously.

Another possibly worse effect is that a spread of a certain virus may be *just* below alarm level until it actually is a real problem. This has happened in our history, but we do try to keep track of the spread to see if it rises above a certain level.

There is a notable difference between virus alerts and virus information. Personally, I do not have any problem with frequent virus info; as long as it comes with a level-headed spreadability/damage assessment based on actual data.

Snorre Fagerland
Norman Data Defense Systems
Norway

Lone Hoax Ranger

Like Larry Friddle (see *VB*, January 2001, p.4), I'm tired of virus alerts – the innumerable Wobbler hoax variants; the hoaxes that ascribe mythological properties to real malware; the unsolicited alerts that address real problems but are so inaccurate or just so vague as to be useless, and that give the sender a warm feeling of having done their civic duty and scored brownie points with the recipients.

However, I don't think it's unreasonable to ask the IT team to do some first-line handling of alerts. I'd argue that an IT team that doesn't have someone on board who can recognize more than 70% of current hoaxes as hoaxes the first time they see them may need a radical sanity check. If they're responsible for anti-virus administration and incident management, make that 90%. As for hoaxes and the non-geek majority, the industry is psychologically stuck in the mid 1990s. Not all hoaxes are illiterate Wobbler/Good Times and the heuristics of 1997 aren't infallible or universally applicable.

Many of the things we all once said viruses don't do *are* done by current malware. Even http://www.vmyths.com can't teach a computer-illiterate to recognise 100% of alarmist drivel. What the average hoax victim wants is someone to verify alerts for them, and ask if they should be forwarded. (Oddly enough, the answer isn't always no.) I long ago gritted my teeth and accepted the role of sacrificial goat within the organization I work for. Anyone who gets an alert is supposed to mail it to me, not the rest of the known universe.

Over time, the incidence of alerts passed on willy-nilly has declined dramatically, and people have learned to recognise more hoaxes all by themselves. When they do send a request for verification, it's often enough to reply 'Yes/no, it is/isn't a hoax', and this way I often get to see hoaxes that aren't to be found on sites that offer hoax databases. It still costs my employers a percentage of my salary to deal with this stuff, but it doesn't appreciably slow down people whose workload shouldn't include trawling through various Web sites.

Lately, I've 'extended my perimeter' by offering a somewhat abbreviated but similar free service to people outside my organization. Not only does this choke on entry some of

the dross that would formerly have spread through my organization, but it's proving to have some potential as a research tool. This theme is explored further and can be viewed at http://www.security-sceptic.org.uk/.

David Harley
Imperial Cancer Research Fund
UK

100% Proof

Having read Eugene Bytschkow's letter in the January issue of *Virus Bulletin*, and having worked in the AV field for not exactly 10 but 6 years, I started to ask myself what precisely is the reason why we haven't reached 100% perfect detection of all known and unknown viruses, as Mr Bytschkow suggested.

However, unlike Mr Bytschkow, my wondering was short-lived. From the point of view of a developer and anti-virus researcher I think I'm entitled to know best what would be better or worse for the user and thus I do know why anti-virus products are still unable to detect every possible virus written or unwritten.

A theoretician in the field would point Mr Bytschkow to Dr Fred Cohen's 1987 (more than 10 years old!) paper 'Computer Viruses: Theory and Experiments'. Or he could see the more modern interpretation – 'Undetectable Computer Viruses' – shown to the public at the VB2000 International Conference in Orlando by David Chess and Steve White. As my two above-named colleagues say, 'dismiss without detailed study any claim that some method correctly detects "all possible viruses known and unknown"'.

However, even without using the mathematical interpretation regarding computer viruses, I say that the main practical reason we are not yet detecting all possible computer viruses can be regarded in the same way as the reason for which we are not yet curing all forms of cancer or AIDS. Of course, we should have been able to cure those diseases after 10 years.

Regarding the political question issued by Mr Bytschkow, 'Why do we not get 100%?', I must say that above all, even if virus detection is still the most important part, it is not the be-all and end-all of what you have to provide to a user. Even if anti-virus products did achieve the perfect 100% detection rate, I think that wouldn't mean the end of the industry, since users will always need more than just detection. And a product which has 100% perfect detection would not need updates, right? But what happens when the conditions of the system in which the product is operating change? The study of 'Theory of Systems' provides the answer: the product needs to be updated with regard to the new conditions of the system.

Therefore, even if a product has a 100% detection rate of all known and unknown viruses, it will still require updates to deal with a new code interchange format, or with new features of the operating system, or new communication protocols. And this is before thinking about new processors, or new hardware, or bugs.

Of course, if users would stop running pirated software, stop clicking the attachments they receive, only use text files to exchange information and never ever make any mistakes of any kind, then yes, maybe we'd live in a world without virus problems. However, I doubt the users are willing to pay that price for a life without viruses. Compared to that, I think today's image of the IT world is worth paying the price of still not having 100% detection of all possible known and unknown viruses.

Coming to the part of the letter where Mr Bytschkow regards the AV industry, hackers and virus writers as one big family working together *against* the user, I must say that this opinion is not new. Mainly, it is sustained by the presence in the AV industry of some companies that care less about ethics, and more about their profits.

Which outlines again the great importance of computer ethics, which is not as alien a subject to us as Mr Bytschkow seems to think – it's an integral part of our work and research. So, even if we haven't yet reached perfection with our technologies, I'm sure that at least we are doing our best to achieve it. And if Mr Bytschkow doesn't believe me, I invite him to Prague for the VB2001 conference to watch the latest advances in this domain, and I also encourage him to read Steve White's keynote speech in the VB2000 proceedings – as everyone can see, if things like 100% perfect detection are not yet out there, well, let's check again in 10 years.

Costin Raiu
Kaspersky Lab
Romania

Standard Sense

Stories on VBS/Davinia being 'potentially more dangerous than LoveLetter' according to one AV vendor could be found on mainstream news Web sites during the week of 14 January, 2000. These stories quickly turned into pieces on whether the virus was really a risk and if a particular vendor was just crying wolf. Unfortunately, another more important message got lost in the shuffle – the need for a standardized threat assessment system. With a standard metric system, customers could more easily compare how AV vendors' threat opinions differ. Today, vendors can independently help consumers by publishing how they calculate their threat rating. At *Symantec*, we use a rating scale of 1 to 5 which is based on wildness, distribution method, and damage. This makes the perceived threat of malware more objective. Through this system and the fact that VBS/Divinia requires *MS Word 2000*, one could easily conclude that VBS/Divinia would not be 'potentially more dangerous than LoveLetter'.

Eric Chien
SARC
Netherlands

OPINION 1

Long, Thin, Slimy Ones

Nick FitzGerald
Computer Virus Consulting, New Zealand

A bit of an odd title, but I was at a loss for an entry to this article, until I remembered a silly song from my childhood about eating worms:

> Nobody likes me, everybody hates me,
> I'm going down the garden to eat worms.
> …
> Long, thin, slimy ones slip down easily,
> Short, fat, fuzzy ones don't.
> …

Then it struck me that the latest rash of mass-mailing worms are the digital world's 'long, thin, slimy ones'. Why? Because despite a significant period of bad news, ill tidings and warnings about running unbidden email attachments, this batch of worms has 'slipped down easily'.

Users have gladly clicked up a storm. Looking back a week at a time from when this was written, we see (with scarcely a break week on week) W97M/Afeto and Win32/Music, Win32/BleBla (aka Win32/Verona), Win95/Hybris, Win32/Navidad, Win32/Sonic, and Win95/MTX. During that period there was also heightened VBS/LoveLetter activity reported, particularly VBS/LoveLetter.AS (aka Colombia and Plan). This last week it was Win32/ProLin and Win32/XTC… [*This article was originally prepared in early December for inclusion in the January issue. Ed.*]

Some of these are parasitic viruses that also have mass-mailing capabilities, but regardless of that, all stirred up some activity. Several have become quite widespread. With the exception of BleBla, all require their recipients to choose to execute unbidden email attachments. (BleBla depends on a security hole in *Internet Explorer* to drop and run its code when its messages are read in email clients using *IE* to parse HTML-format messages.)

Has the World Gone Mad?

The seemingly crazy behaviour of running unbidden attachments continues despite the warnings, leading many computer experts to pose some questions. Are computer users really that stupid? Perhaps a fit of collective insanity has hit them? Perhaps computers are just too hard to understand sufficiently for most people to be able to use them safely?

These questions have an implicit assumption – the users are somehow at fault. We (the experts) have warned them, but still they do it. We warned them again and they continued doing it. Some people have been hit more than once (*usually* by different worms) but still they open unbidden attachments – ordinary folk must be really stupid to avoid the best efforts of the experts… But maybe the users are not the problem. Maybe the problem is the experts? Maybe the experts make things too hard for ordinary folk?

In the early days of what is now called 'human factors engineering', car manufacturers were not beyond designing clutches or brakes that were too heavy for women of average build (and thus also a goodly proportion of men) to operate safely and comfortably. Was the reaction to suggest that women who wanted to drive these cars take body-building courses at the local gym? No. Rather sensibly, the car manufacturers started to take note of such issues, took measures to avoid such problems in future designs and offered free upgrades, refits and so on to remedy such problems in existing models.

When it comes to PCs, neither the user nor manufacturers currently see computer security and maintaining computer system integrity as anywhere near as critical as safety issues have been in the car industry. Hopefully this will change in the future, but what can be done in the meantime?

Educate, Educate, Educate

Security experts seem particularly scathing of the idea that users can be taught to take a more informed and responsible approach to the issue of avoiding malware. As these same technologists have still failed to provide vaguely adequate technological solutions to the problem, I question whether their opinion here is relevant.

There *are* good examples of user education reducing malware incidents and the previous unthinking spreading of hoaxes. One example I am often reminded of is the effort at the University of Texas (UT). There, a small IT support team runs a successful information and education campaign among the widely diverse academic and support staff. Coming from IT admin in a university environment myself, I appreciate the constraints that maintaining academic freedom can place on such IT administrators.

Yet, as Paul Schmehl from UT often describes in messages to newsgroups such as alt.comp.virus, by developing an air of local authority over malware matters, seldom posting alerts and continually reinforcing their constituents for desirable behaviour, his team has reduced real incidents and hoax mailings to virtually zero.

UT users seeking to check virus and hoax stories with the appropriate local IT support staff are praised for doing so (no matter how onerous it is for the support staff to debunk Good Times or BudFrogs for the umpteenth time) and reports of 'suspicious' computer activity are closely followed up whether they really are malware-related or not. Both actions strengthen the relationship between the

support staff and their clients. In turn, this enhances the effectiveness of the educational material, and rare malware warnings posted by the UT support staff. Such results are achieved on shoestring budgets and low staffing levels compared to large corporate sites.

But suggesting education is the answer still addresses the 'problem' as if it is sited in the users. Better informed users will help, but suggesting education alone is 'the solution' is akin to suggesting there was nothing wrong with those early cars but the women wanting to drive them were at fault for not being strong (or heavy) enough to apply the brakes properly. It may be acceptable in a few specially designed cars (say for racing) to expect 'unusual' strength and/or weight in the driver, but a car 'for the ordinary person' should be a car an 'ordinary person' can drive. Shouldn't the same go for computers intended for personal use?

If we need to educate people specially before they become safe computer users, are we not admitting that computers really are not that much of a general purpose tool yet? And if users need special training, should they not be required to obtain that *before* being allowed out on the 'information superhighway', much as we require automobile users to pass driving competency tests and obtain a licence before being allowed out, unaccompanied, on our roads?

Redesign for Safety

So can we learn anything from the car designers of old? To answer this, we should first look at some similarities and differences between cars and computers. Used poorly, a car will readily injure, maim or kill many people other than its driver. While this can be true of computers, in general it is not. This is one reason there has been no political movement to enforce (or even suggest) usability, security and other standards on computer designers, and licensing on users. However, used poorly, a car can easily cause very extensive property damage and, depending on your definition of property, this is equally true of computers. The difference between these two examples may explain why most countries do have laws against unauthorized data modification that have broad scope in many computer-related crimes.

Typical cars are expensive relative to typical computers and an interesting psychological effect may come into play as a result. There is a strong belief among many people that great events require great causes. An often-cited example of this is that many people do not accept the 'lone gunman' explanation of Kennedy's assassination because the scale of the event (or, more precisely, the scale of its consequences) 'requires' a greater cause than a single, disillusioned sniper. What happens if we apply this in reverse? Computers are cheap and everyone has one, therefore they cannot be much cause for concern.

There are more differences between cars and computers and our attitudes to them and their use, but the only other one we'll consider now is that (ignoring environmental effects) cars only impact their immediate locale. With computer security this is often not the case. A poorly managed machine may be compromised and a DDoS agent installed, but the computer keeps working, so what is the 'damage'? In a sense there is none until the compromised machine is used as part of an attack network. Even then, the damage to the poorly managed machine or its local network may be imperceptible. Two expressions spring to mind – 'What the eye doesn't see the heart can't grieve over' and 'Out of sight, out of mind'. Unfortunately, these seem to be a mantra for too many system administrators.

'The Boeing Effect'

Imagine what happens when one very large site is hit by something new before its scanners are updated and then widebands the infection to perhaps 10% of other large corporate sites. Because that site is huge, it is more likely to be hit; because it is huge it is more likely to have your company's address in its corporate email address lists, and, if it is a technology company, victims downstream of it (including some of your staff) are more likely to drop their guard with attachments from it.

This is a very chilling illustration of why individuals who are not well-versed in deciding what code to run should be removed from that decision process. Although we have seen precisely this type of thing happen to *Boeing* (including ProLin), the US Department of Defense and some others have been equally involved in the early, widespread distribution of other email worms. So, how do you avoid being hit by what I have heard called 'the Boeing effect'?

Education can help, but it cannot be the entire solution. It seems we have adopted, and now fail to question, many assumptions about how computers should be. We downplay the negative side-effects in terms of security, and system and data integrity, that arise from these unquestioned yet not necessarily unavoidable assumptions.

In the past we built safer cars. Can we really not build and run computer systems that are safer and can be configured to prevent 'ordinary users' from having to make mission critical integrity decisions? If we cannot remove that need entirely, can we not reduce the rate at which they need to be made? Desktop computers have opened the doors to the power and flexibility of data processing we now take for granted. However, if used carelessly, their globally interconnected nature means they also readily open the doors to the company's secrets for many undesirables.

You cannot prevent the 'Boeings' of the world accidentally shooting at you, but you can work to ensure your system integrity management is only done by those acquainted with the peculiar (and complex) aspects of that task. You can save yourself hassles along the road to achieving that by stringently filtering all 'executable' code out of incoming email and other sources of external code arriving at your network boundary. You *must* stop assuming that if virus-specific scanners don't stop something then it is OK.

OPINION 2

What Price Progress?

Richard Ford
Cenetec LLC, USA

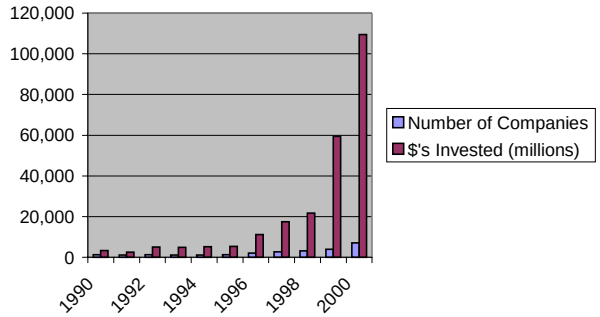
Nobody would debate that the last several years have seen an exceptional growth in the stock market. A strong technology sector, on-line trading, and an economic upswing have allowed some companies to grow from startup to multi-billion dollar behemoths almost overnight. While this has led to the rapid uptake of new technologies, some have argued strongly that it has actually hurt the security of companies, and therefore our nations, in many subtle ways.

In this article I will examine some of these arguments, and portray what I believe to be a fair perspective on the likely outcome of this sudden growth. While things still look fairly positive with respect to the market, we are certainly in danger of reaping the harvest of the seeds sown in the nineties. What kind of harvest will it be?

The Dotcom Revolution?

One reason the role of security in the new economy is so important to me is that after leaving *IBM's* anti-virus team, I found myself at a fledgling dotcom company, working on a large (it later turned out to be the largest in the world) Web hosting system. From there, a short stint in the Venture Capital (VC) industry led me to my current position as CTO of *Cenetec LLC*, a technology accelerator. From *VB* Editor to Venture Capitalist may seem like a long journey but in fact, in many ways, a VC exists by applying many of the same business principles required to run a business like *Virus Bulletin*.

To many outsiders, the role of Venture Capital (VC) is poorly understood at best. Essentially, VC provides an important source of 'smart' money for companies – smart because the VC also brings with it many other benefits, such as contacts and direction. VC investment statistics show a large increase over the last few years (see graph).



While most people think of a VC investment only in terms of a young startup company, VC monies can also be used to help a company grow to a size where it can be acquired, or go through an IPO. Finally, a VC can also invest in a company that needs financial help (known as turnaround or recapitalization financing). In each instance, however, the VC is driven by profit, hoping that the equity acquired in the company can later be resold at a profit.

As seen in the graph, VC investments have undergone a rapid expansion over the last few years, after a period of relative stability in the mid-1990s. This curve has been partially driven by the success of the Internet-centric NASDAQ-100, which swung upwards almost un-stoppably until lately. This huge influx of money, and the rapidity of IPOs that seemed to leave all investors clearly in profit have created a 'built to flip' culture, not to mention a raft of new millionaires. All is well, or so it seems on the surface.

Unfortunately, the real picture may be somewhat different. One has only to chart several of last year's 'hot stocks' to see how quickly an industry or market segment can lose the market's favour. 'Time to market' is king, and getting products to market is more important than ever. In the last several months, this has become even 'truer' (if possible) as the decline in Internet stocks has made several capital-intensive ventures tighten their belts.

What does all this have to do with security and, more particularly, what does it have to do with anti-virus security? The key is in the previous paragraph, or even in just three little words: '*time to market*'.

When money is tight, competition is fierce, and time is the ultimate enemy, there is an incredible pressure to get products 'out of the door'. This pressure can lead to a lack of focus on certain foundational elements – sometimes security, sometimes platform, and sometimes scalability.

Given the huge pressure on startups to bring products to market, coupled with the lure of quick turnover of companies for cash, it seems inevitable that certain facets of the business could get overlooked. Functional 'insurance' like security systems or anti-virus policy can be overlooked in the name of speed. As many viruses do not carry particularly unpleasant payloads, some have even taken a purely reactive approach to the problem, dealing with outbreaks as they occur, rather than adopting a proactive stance.

More disturbingly, the focus on functionality can encourage the creation of new products that are fundamentally insecure in design. Even large established companies are not immune to this syndrome – the original *Word* viruses had the ability to function silently, because of the functionality built into *Word*. Later versions implemented some protection against the abuse of embedded macros, but the

principle is there – functionality is sometimes put in place instead of security. In an arena where 'time to market' is king, functionality is queen.

The Solution

All is not lost in the new economy, but without some careful planning now, there are likely to be some pretty large lumps and bumps. Most importantly, the concept of 'built to flip' is probably not going to be as prevalent – the new maxim could well be more along the lines of 'built to last and built to scale' and that means foundations.

Perhaps the biggest hurdle to be overcome is raising the importance of 'designed in' security – that is, security incorporated from the design stage, not retrofitted as problems arise. The concept of treating security as a risk avoidance feature must be replaced with the idea of security *as a feature*. This is a major paradigm shift, and one that will take time, but it is likely to be a transition which startup companies undergo, given the high-profile failures of security in mission-critical systems lately.

Ultimately, the startup market represents capitalism in action; thus, until the consumer places a high value on security, the market will not place a high value on security. Part of this lack of value relies upon the fact that many people think of security as simply protecting one's systems from the wily hacker – this is not the case. Security encompasses the areas of confidentiality, availability and integrity; when illustrated this way, suddenly the importance of security becomes much more immediate. While the hacker seems dim and distant, the degradation of any of the preceding factors is unacceptable; security should be seen as a competitive advantage.

The foregoing should certainly not be taken to indicate that all startups do not have their collective eyes on the ball. Just as there are good and bad anti-virus products, some companies do value and construct security adequately, and some do not. Certainly, the tighter market conditions have lead designers to examine the longterm goals of design decisions, not just the 'time to market' considerations. A liquidity event is now more likely to be further out and based upon not just release into the market but also market success. Thus, while many readers may well have lost money (and lots of it!) in the technology stock correction, they are also significantly more likely to see stronger, leaner, more functional companies develop.

Action Items

A solid understanding of the preceding issues allows one to take several different precautions to prevent the most common mistakes. Small companies, for example, recognize that the technology decisions executed now are still likely to be in effect many months or even years hence. Thus, one must build both technology and procedures early on in the development process if large-scale success is to be achieved. Process cannot be ignored – if one does not put it in place initially, one may well find putting it in place later many times more difficult and expensive. Even more importantly, investors are becoming better educated concerning the downstream consequences of inappropriate or inadequate planning and architecture.

For the average investor, the results are equally fundamental – solid research must be carried out to ensure that the real architectural and security needs of a company are being addressed. While the market may have allowed some technologies to 'slip through the net', such an approach is not one upon which one should ever rely. It is a far better policy to make sure that the fundamentals are addressed in the rush to market.

Due to the difficulties many companies have during the critical architectural stage, the need for a more structured yet rapid approach to creating products/services led to the formation of *Cenetec*, the company for which I now work. During my brief VC stint, I observed that money was, in many ways, the least valuable resource we were able to bring to bear – most valuable was experience and focus. Thus, *Cenetec* was born – a combination of money and services, as it were.

In this model, companies spend resources planning the overall architecture of a product, and examine how the proposed solution would impact the security, usability and cost effectiveness of the product. Then, and only then, is the product built. This approach may seem obvious (indeed, it represents many years of industry best practice), but this longer-term focus is often hard to obtain in the controlled chaos that is a startup.

So, the *Cenetec* approach (among others) helps to provide the business entrepreneur with a 'big picture' view of a market. While this is not the only way to succeed, we have seen that there are many advantages to this approach, which allows companies to come to market not just quickly but also securely.

Conclusions

In many ways, one could argue that the rapid rise of Internet stocks has lead to a distinct focus *away* from traditional computer security. Increased pressure on 'time to market', and the ability to achieve liquidity with little or no proven market success led to a culture where the focus of developers was on features, appearance and overall 'time to market'. Fortunately, this economic boom seems to have slowed down and more rational approaches should, over time, prevail.

Those startups that concentrate on building products which have a strong longterm position in the market are likely to be successful, while 'slash and burn' development will become increasingly hard to sustain. Finally, continuing focus from the user perspective on computer security issues ultimately drives the market; if consumers value the security of their data highly enough, so will the investors.

OPINION 3

In Exchange for Protection

Péter Agócs
VirusBuster Ltd, Hungary

Regarding last year's virus incidents, it is indisputable that the threat caused by 'Internet-ready' mailware was and is the primary concern. Electronic mail is the main vector for these viruses, and that is why mail servers form the front-line defences of the battle fought against them. Based on conventional warfare strategies, the obvious solution would be to build up a strong defence at these strategic points. Considering this, the solution may seem simple, as the protection of strategic points is provided by installing the appropriate product from a reputable manufacturer on the mail server and by making the proper adjustments. This would seem to be the most simplified theoretical approach, but let's see how theory meets experience in the case of *Microsoft Exchange* servers.

There are several technical possibilities to protect *Exchange* servers, which result in a wide range of solutions with varying degrees of efficient defence. One of these solutions is *AVAPI*, which, as its name implies, has been developed to attach to anti-virus solutions. I considered it a fortunate initiative from *Microsoft* to have developed the *AVAPI*, as it finally suggests that valuable developer capacities are not just taken up with superfluous research and experimentation, but actual, effective development tasks as well.

AVAPI came out in *Exchange 5.5 Service Pack 3*, while in *Exchange 2000* it is an included accessory. Recent service packs include the correction only of initial, basic deficiencies – they do not provide a solution for fundamental problems. But we shall not look that far; let's see what experiences we had with *AVAPI's SP3* version.

First Impressions Last

We began to examine the package trustingly, and at first we were delighted to see that it contained official documentation, though it was not to perfect technical specifications. Of course, only those who have had experiences with, for example, the IFS Kit can understand the importance of this. Nevertheless, a good look at the documentation decreased our enthusiasm as it turned out almost at once that possibilities are limited to a narrow range.

Having examined it thoroughly, we were led to the recognition of serious problems and deficiencies. Among others, substantial data on the examined object is not available, which makes it impossible to identify its actual connections. This literally means that only the name (and the length, but it is irrelevant here) of the file given for inspection is known, but its connection to another object (email, folder) is not.

If I were a system operator who got a message like this 'The XYZ.DOC file is infected with "Any" virus and is therefore moved to quarantine' in an organization with several thousands of users, I would probably feel very frustrated if I had to find out who the sender or the recipient was. This also means that the sender is not warned about the fact that he keeps on sending infected files, neither is the recipient informed that the attachment was infected but has been disinfected. The fact that carrying out a timed or manual scan is only possible inside *AVAPI* by using a 'DIY' solution is almost not worth mentioning. If we look at it strictly, we can say that these are important but not critical features, and that virus protection software can perform its essential function without them.

After having tackled the initial problems, we proceeded with further analysis and developed the integration of our scanner with the interface, hoping that no further serious errors would come to light.

Curiouser and Curiouser

Well, unfortunately we were wrong. After installation the *Exchange* store loads the AV extension without any problems, that is unless someone thinks about giving a value in the proper place different from the vendor string given in the sample Registry data. If that happens, the AV extension will not be loaded and what is more there is no warning of that fact. After a successful load the stored files scan begins, but only if this is the first occasion on which the program is loaded, or if the version number has changed in the AV extension descriptor.

Getting enthusiastic about the signs of operation, we increased the number of files to be scanned. However, we experienced a strange phenomenon concerning the scan of an incoming email's attachments. The point is that although the email arrives in the recipient's mailbox, the scan is not immediately performed – it occurs some time later. If the opening of a message is initiated before the completion of the scan, first a neat little message window informs you 'Could not open one or more attachments'. If the user happens to be unable to find out exactly which attachment could not be accessed, then the following 'The request operation failed' message will inform them about the naked truth after the unsuccessful attempt. I would be surprised if this reminded anyone of the 'Scanning in progress, please wait …' message.

The situation is even more serious when the email transfer happens during the full re-scan, which – as I have already mentioned – is performed automatically after the refresh. Whenever this happens, the incoming or outgoing email's attachment gets to the end of the queue, which also means that if the scan of the previous messages has not been

performed in the pre-set time interval, the message will be classified as undeliverable email. Then the sender's mailbox will get a 'The following recipient(s) could not be reached …' warning message, which – to be quite frank – is not even close to the truth.

The thing that I really can't understand is that it is suggested that the scan interface is multi-thread safe, which leads us to assume that the scan can be initiated through several threads. The truth is that we were not able to find even an indication of multi-thread execution. I think that this is a 'reserved for later development' feature, just as I cannot believe that the queuing problem mentioned earlier isn't easy to fix somehow.

Problems, Problems

If a file contains a virus that cannot be disinfected by the AV scanner or simply looks suspicious to heuristics, another interesting problem is raised. Generally, the action to be performed in such a case can be adjusted differently in different AV products.

Let's look at the scenario of choosing the 'warn only' option. There is a problem with both incoming and outgoing emails here – the AV extension is not able to send a message, since it does not know where to send it. It can only send a message by overwriting the attachment's content and type – this results in saving the original attachment in the quarantine, where it can only be identified if someone asks for the lost file. If the file happens to remain unaltered then there is no problem with incoming emails, since access to the attachments is denied with the usual message.

In contrast to this, with regard to outgoing emails, with access to the attachment denied the server cannot send the message at all. The user will get the usual 'The following recipient(s) could not be reached …' warning message. And since there is no information available on the inspected object, whether it is attached to an incoming or an outgoing email, the administrator's attempts to find the option mentioned above would probably be in vain, as its implementation is 'suspended due to technical reasons'.

The main reason for these annoyingly trivial problems is that we want to pack our messages with various kinds of attachments, both large and small. Actually, the simplest way to ensure that we will not become the victims of such glitches is not to use attachments at all. That's right – but why do we need mail protection then?

One of the reasons is that *Exchange* approaches HTML-based messages from a very interesting aspect. Why? These messages are handled not as attachments, but as HTML-based message bodies, and as such they are not scanned at all because the AV extension only gets attached files for scanning – and we have established that these are not attached files. That means if the HTML message happens to include embedded Visual Basic Scripts, then they will pass the protection line without any difficulties. This is a serious problem – remember BubbleBoy?

Last, but not least, the first version of *AVAPI* had a small but not negligible surprise in store for us. The store could hardly tolerate the presence of the AV extension and after a while, due to considerable deterioration of its condition, it was compelled to turn to its medical advisor, *Dr Watson*.

Where To Now?

As I have already mentioned, we gathered these experiences during the development of the first version of *AVAPI*. Of course, we did not want to write off valuable time and work invested, so we began a long series of experimentation to find the way out of this 'dark tunnel'. I put every existing contact of mine to use, to track down information on possible solutions.

If you're expecting dramatic news, you are wrong: I was unsuccessful. Not surprisingly, we put the product aside – although we have finished it meanwhile – and began to search for another solution. The service packs which came out in the meantime seem to support our conclusion, and though they include the correction of a significant proportion of the problems, the essential ones have not been solved. Let's look more closely.

Having armed our server with *SP4*, I checked the above problems and I was delighted to see that there are signs of improvement in the operation of the AV extension. The stability problem and the multi-thread scan issue have been addressed, thus decreasing the chance that the scan will not be executed in the specified time when opening a message. With respect to the mail opening request, the store now initiates the scanning of attached files immediately, so it only depends on the server's load as to whether it can manage to do so in the time available. To this end, two parameters have been introduced for the attempts in addition to the option to adjust timed intervals.

However, it can do nothing with the attachments which have been marked as infected, so there has been no improvement in this field. (Which reminds me – the AV extension has the opportunity to return virus information to the store, but it is unclear to me where it is used and what for, so if someone would be so kind as to give me information on that, I would be very grateful.)

In my opinion all the corrections are limited to little annoyances, except for the stability problems. The essential problems like HTML email scanning or the access to the files' connections have not been solved yet. In the light of this, *AVAPI*'s capability in its actual form is highly questionable. According to my (admittedly very limited) information, *AVAPI*'s second version, which is just being developed, will contain several essential changes greatly improving its applicability. Considering my experiences, I am a little bit sceptical, but who knows? One day we may complete the unfinished project.

FEATURE

Paddy Whacks the Virus

Berni Dwan
Freelance technology writer, Ireland

It is said that St Patrick banished all snakes from Ireland in the fifth century. What kind of snakes they were I do not know, and how they survived the cold, damp climate up to then I cannot imagine. Notwithstanding, we ambled along quite nicely over the centuries until worms, Trojans and variants with an equally slippery disposition reappeared in the late 20th century.

Big e-Business

Now, if in the meantime Ireland had not become the e-commerce hub of Europe and the largest exporter of software goods in the world after the USA, the computer virus phenomenon might not be of much interest to us. But the landscape, metaphorically speaking, changed dramatically during the 1990s as we moved from an agrarian (well, kind of!) to a cyber society (I'm exaggerating for effect here), and the reappearance of slippery characters will require not the intercession of a saint, but the intervention of the technologically astute. Failing the frequent and cheap availability of supersonic air travel, our only direct means of contact with the rest of the planet is through our information and communications technology.

Increasing the levels of international bandwidth has been a crucial step on the part of the Irish government in ensuring that Ireland remains at the forefront of e-Business activities in Europe and further afield. Lower communication costs, hugely increased capacity and state-of-the-art connectivity was assured with an $80 million agreement between the Irish government and *Global Crossing* to build the *Irish Ring*. This undersea fiber optic cable will seamlessly link Ireland to 36 major European cities and trade centres as well as the United States through the *Telco* network.

However, being the e-Commerce hub of Europe is merely a decorative title if integrity is not an intrinsic part of the model. Last year, the Electronic Commerce Bill (which allows for the introduction and maintenance of a voluntary accreditation scheme and a supervision scheme for the issuers of electronic signatures) was signed into Irish law which, according to the Minister for Public Enterprise, would add trust and certainty to the existing Irish electronic commerce system.

In a 1998 piece on Ireland in *Wired News*, Vint Cerf said the island nation is 'in line to capitalise on a "first to market" advantage that could be gained if vigorous action is taken during the next six to twelve months'. The adroit moves regarding international bandwidth and the e-Commerce Bill were a major part of that affirmative action.

This island nation with a population of 3.5 million is responsible for producing over 40% of all PC package software sold in Europe. The software industry in Ireland consists of 550 companies employing more than 15,000 people. The 120 overseas software companies based here cover a wide brief, including core software development, product customisation, software testing and fulfilment.

The software that is wholly developed in Ireland covers a wide range of applications including mobile communications, electronics, engineering, enterprise resource planning, database management, banking, insurance and Internet security systems. It doesn't stop at testing and development. Consultancy service and systems integration companies are using Ireland as a base to support international business clients and a growing number of companies are also providing worldwide tech support via toll-free call centres.

While computer viruses to date have been analysed to death, their vocabulary hackneyed and worn, there is one sure thing – new threats, including malicious mobile code, and distributed denial of service attacks will continue to evolve through the efforts of 'script kiddies' or astute, yet dark, programmers. They will meander through the global network leaving minor annoyances to national incidents in their slippery wake.

Alec Florence, CEO of *Priority Data Systems* (specialists in e-security issues) sees local support as being the vital key in this precarious climate. For his company this is provided through a permanently manned virus support help desk, while they also offer an anti-virus health check service to clients, whereby a team goes on site and checks software for any degradation before optimising it.

It is bad enough when the economic wellbeing of a company or organisation is adversely affected by a particularly sinister virus infection, but if a nation comes into this category, well, it is worse than bad. I hesitate in using the word catastrophic, as the battle of wits between the virus and anti-virus writers remains on a somewhat even keel. Sure, the virus writers always get to move the pawn or the knight first, but the anti-virus response, while not always instant, is generally effective.

In November 1999, the Funlove virus felled operations in *Dell's* Irish plant in Limerick for two days. After discovering the virus in the system used to load software into desktop and laptop computers they were forced to recall 12,000 units. Despite the fact that no viruses were found in the recalled units, valuable production time and millions of pounds were lost.

This example of a major multinational company working out of Ireland shows what could happen on a larger scale if a particularly debilitating virus managed to inveigle its way

into the nation's fileservers. Not only would it be a company issue, it could also be a national issue in this, the 'European software capital'.

Talking Tactics

I spoke with David Bolger from *Entropy Limited*, a wholly Irish-owned firm which provides IS infrastructure services and plans to launch an outsourced Managed Security Service (MSS) across Europe in the near future. We covered some of the important issues relating to the virus threat in Ireland, bearing in mind its somewhat unique position. Regarding strategy, the trend in Ireland as elsewhere is to protect the gateway and scan all email (encompassing anti-virus and content management), Internet connections and file transfers through some form of proxy or anti-virus engine before it ever reaches the desktop. Perimeter protection, therefore, is the desired goal.

Irish-based offices linked to foreign branches or headquarters via private leased lines or WAN links pose a particular challenge. As Bolger points out, they both transfer email without going through the Internet. If any of the foreign-based offices do not have a policy for scanning all inbound email from the Internet they could receive virus-infected email and transfer it over the internal network to the Irish office. The Irish office will already have Internet email scanning set up but will have no scanning procedures in place for private leased lines or WAN link email.

Not wishing to seem too laborious about this, one can see how the Irish office is probably wasting its time scanning only Internet email if, in tandem with this, it simply trusts the integrity of the seemingly safer email coming in over the private lines. This encouraged *Entropy's* implementation of groupware scanning, which goes back a step further than the gateway and concentrates on the central server that holds all email regardless of its incoming route, before passing it to the desktops.

Bolger says that we need more products that cover desktop, gateway, groupware and the corporate server as opposed to just covering the desktop and the gateway, with central deployment being paramount. This is the trend now anyway, and I can immediately think of several products off the top of my head, which meet this requirement.

However, it is not necessary to take one or several products from a single stable to build your own motte and bailey against the viral hoards. *Entropy's* own strategy is to pick 'best of breed' products for each separate entity requiring protection, and to build a suite with these. So, the product protecting your desktops could be from a completely different stable to the one protecting your gateway.

It would seem that so far, user policies are not yet strongly enforced in Ireland and as Bolger observes, 'products only implement what the policy dictates. In many cases where a new virus or threat is discovered the anti-virus software cannot detect it, therefore you are still relying on the rules in the security policy to protect the organisation. Users need to be educated on the policy and the risks.'

While the more behemoth-like corporate policies tend to be guarded and locked away, thus escaping any chance of being updated, application policies, defined by configuring the product, are shorter and more manageable. They have a much better chance of grabbing the attention of and being implemented by company departments. A human resources department, for example says Bolger, should only receive CVs in their email, so all file attachments that do not have a .DOC extension should be blocked. 'Lovebug would not have been a big hit if policies had been strictly adhered to. This was a VBS file and no one should have been able to receive it unless they were developers.'

Despite warnings though, users continued to receive unwelcome Christmas presents including Hybris.B, Prolin and Navidad, which according to John Mooney of *Renaissance Limited* (a company which provides Irish computer users with a range of computer security products and services) are increasingly using psychology to tempt users to open attachments.

'Everyone's New Year resolution should be to do a double take before they double-click', Mooney says. Acknowledging that most monthly virus alerts are repeats or copies of previous viruses, he adds, 'when a new virus is seen as a real threat we notify customers immediately so that they can take appropriate action.' Mooney is happy and confident that Ireland has the technical expertise to cope with old and new virus threats, however he recognises that it is a learning process for everyone.

Hoaxes are almost as interesting as viruses themselves, and can cause the same downtime and loss of productivity. Bolger knows of cases where the affected company faced with the albeit hoax threat, pulled all external connections rather than risk any more 'infected' email coming in or going out. In some cases, this may have been a policy decision anyway, especially if the hoax had a file attachment but where such a drastic move is not feasible, Bolger suggests quarantining, not to mention diligent and frequent checking of hoax lists.

Alec Florence sees containment as part of an outbreak management system where, for example, the file server would be knocked off and the network manager alerted if ten emails with the same file attachments come in within a few minutes. Bolger agrees, 'Ireland being an e-Commerce hub of Europe means that we will probably become more prone to receiving malicious code across our networks. We are more susceptible.' He advises Irish companies engaged in e-Commerce to 'put in as much technology as you can to enforce what you want and keep up to date with developments. If you can afford outside experts to do it for you, then all the better.' And people do appear to be listening. More and more Irish companies are concentrating on the business of their Web sites while outsourcing IT security to specialist companies.

FEATURE SERIES

The Usual Suspects – Part 3

Andreas Marx
University of Magdeburg, Germany

This concludes our look at the commonly encountered problems thrown up when testing anti-virus software.

Password-protected Office documents

Microsoft Office documents can be password-protected. For *Office 95*, the content of the document and all *Word 95* macros are stored in encrypted form (*Excel* macros are not). However, this encryption is easy to break and it is no big deal to find out if a macro virus is inside it. The encryption has changed in higher *Office* versions and cannot be broken in real-time any more, but the macro modules are no longer encrypted and can be scanned easily.

If the AV program is capable of scaning inside password-protected files like .DOC, .XLS and .PPT, all well and good, but some cannot or do not want to break *Office 95* encryption. If this is the case, a warning message (to the effect that the file is password-protected and cannot be scanned) should be displayed and put in the report file.

Run-time Compressed Files

Script kiddies tend to compress well-known backdoors, worms and other malware to avoid easy detection by the scanners. Under DOS it was relatively easy to decompress the files in memory and check if they looked dangerous. However, in these Win32 times it has all changed – compression, encryption and other protection programs are common and the files can be very large.

It usually takes considerable amounts of time and memory to decompress such files, not counting the time taken to develop a solution for a single compression method of a special version. We are still playing the 'we can't win' battle against viruses; every new virus will get its own signature, so why can't we develop decompression routines for the most common Win32 compressors too? Only a few programs are able to scan such files – this has not changed for a long time now, while the problem gets more significant every day. Another idea would be to compress any known Win32 malware using all known packers and include them into the virus database. This is a very complex process and may be impossible if there are too many different variations of compression programs and malware.

Scan Time and Speed

For a long time, it was thought that only the scan time of an uninfected PC was important, since this would be the standard scenario for an AV scanner. The situation has

changed now, especially on a mail server – since everyone can send infected emails over it, it is important to scan the files fast enough to find viruses. Moreover, cleaning is usually enabled which takes additional time until the email can be delivered.

There are some ItW viruses around which require significant scan time – Win32/Fono is a good example. Large and complex documents with fragmented OLE2 structures need longer still. The interesting question is what happens if several of these files reach the server at the same time? We tried it – some programs experienced a slow-down, but about half crashed after about 30–50 infected files, which would constitute a nice DoS (Denial of Service) attack. With cleaning enabled, it only took half that number.

However, our *Exchange* and *Notes* test system – a *Pentium III 800* with 384 MB RAM – did not slow down. One idea would be to improve the scan time for problem files – not possible without major changes. A more suitable solution would be to implement a better handling of 'in-progress' emails which are currently being scanned or are next in the queue. It also makes sense for customers to switch off disinfection and only quarantine attachments, since disinfection causes its own kind of trouble (see below).

Updates

It is a fact that users want to have an easy Internet download function for updates. However, most still want to be able to download updates separately, when necessary. An offer of regular program updates and upgrades on CD is a good idea.

If a user buys an AV program in a shop, it is often weeks or months old and has to be updated first. Less understandable is if someone downloads a program from the Web and this version is very old too. Why not keep it up to date?

Internet updates seem to be easy – one button has to be pressed and the download starts. However, in our tests, at least one program consistently forgot the proxy settings and in some, neither name nor password for the proxy server was specified. Another problem is caused by programs which always download all files first – after they have finished it looks like something completely new. Another program always downloads the complete databases, after it has checked if they are newer than the last version. Both cause the 'high network traffic' problem for both retail and corporate users. This could easily be avoided.

Newer implementations only download the changed part of files, which requires some extra programming but the downloads are much smaller and faster. After the download, all the changed files are patched and they look like they would after a complete download. One solution would be cumulative and regular small updates loaded directly by the program. However, this requires more memory at run-time and after a while a big new update will have to be released.

Often, like with outbreaks or other dangerous situations, it is useful to be able to have very small update files. In the best case these would be readable ASCII files, which can either be downloaded or sent by email or maybe even fax. Since they are very small, clients can be updated very fast without high network usage and even in an outbreak situation the vendor's Web server may still be fast enough.

One thing we have seen several times is the possibility of updating the engine and the program separately. However, the program can usually only update the signature files, but the engine has to be downloaded and installed separately. In the real-world we foresee a big problem here: many people only download new signatures, not engine updates.

Since AV developers do not test all the possible variations of signature and engine versions (a nearly impossible task), strange things can happen after an update – like system hang-ups or the overwriting of system areas. A better idea would be simply to implement a feature to download engine updates as well as the usual pattern updates, if a new engine is available. After all, the engine update has to implement new detection routines for new sorts of malware which cannot be found with the old engine. The user can have the latest signature file and the program can say it is up to date, but the scanner will only detect a subset of new viruses.

Banana Software

Some updates look like 'banana software', which matures when it is with the customer. It is understandable that not every last detail can be tested on every platform with every software release. However, we cannot see why there have been – for example – so many false positives every now and then on standard applications like DOS 6.22, *Office 97*/*2000* and *Microsoft's* Java implementation.

It is a fact that proper testing requires a lot of time and it can only show if there is an error, not if there isn't. Since updates are released daily or weekly, it is important to test everything sufficiently speedily. Some say that a slight change in the signature file cannot cause problems, but we have seen some, such as the misidentification of viruses which causes a wrong repair routine to be called, or buffer overflows etc. Even minor changes can have significant effects. Another example was the boot-up scanner of one program which ceased to work after a signature update as there was no longer sufficient memory available.

It is a good thing that anti-virus tests can be performed on a parallel basis – the more PCs and humans, the faster the tests. These do not include detection tests, where scanners have to find at least the number of viruses from the last update and then the newly implemented detection, and only then perform disinfection. As mentioned above, no code change does not mean no problem with disinfection – the disinfected files still have to be checked to ensure that they are the same as in the last disinfection tests. Stability (some corrupted files, as well as other kinds of data trash and very large files should be tested), speed (the decrease caused by the new signatures should be minimal and unnoticeable) and all the other software quality criteria have to be tested.

Boot viruses on floppies and hard disks should not be forgotten. Our last test showed the lack of detection of boot viruses in a few products. One program was able to handle Unicode directories and files correctly, but the next version of it was not. It also seems that some developers only test their archive detection against the *EICAR* test file and not against large real-world archives.

It should be noted that we recorded minor differences on the different *Windows* platforms (*98*, *NT*, *2000*) in our last batch of tests and some dramatic differences on *NetWare* (*4.11*, *4.20*, *5.00*, *5.10*) which are all reproducible. The same problem happened with the English but not the German version of *NetWare*.

Memory Detection and Disinfection

A big problem seems to be the detection and disinfection of active malware. Most scanners show that they scan the memory, when most only look for boot and old DOS file viruses in the first 640 KB of it. If so, most of today's viruses will be missed, since they have been written for Win32. If such a virus is active in memory and the user scans all files, it has a good chance of infecting everything.

However, some scanners do this for Win32/CIH – they scan everything, infect everything and clean everything, leaving the infection marker 'U' before the PE header starts (which is not a bad idea). This cleans the system completely but it is not an ideal solution. A better one would be to detect at least all the top twenty non-macro ItW malware in memory and clean them. For viruses this is tricky, but worms can usually be removed using some simple *Windows* functions. Some special disinfection programs and developer freebies can do this easily, but usually the main virus scanner cannot, which begs the question 'why not?'.

Some special malware, such as the Win32/PrettyPark worm or the Win32/SubSeven backdoor, uses a tricky way to hinder an easy disinfection. In the Registry, they change the entry which governs how to start EXE files so that the virus will be started first, which will run the requested executable file. There could be a problem caused by an active resident virus protection – it denies access to a detected malicious program, no other programs can be started any more, and in most products the resident protection cannot be switched off in such a situation. Under DOS, worm parts can only be deleted, and after such a 'repair' programs will not run since the Registry is still unfixed. Only one program avoided this problem, replacing the virus parts with a program that starts the EXE files the usual way and the system still runs.

Back to *Windows* – the problem is first that the Registry fix (including a possible Autostart entry) has to be made and second that the malware files have to be removed, but they are usually active and cannot be deleted. Only one program was able to do it this way – most removed the malware parts but then the system stopped running.

Another example of tricky disinfection would be that of Win32/Ska (aka Happy99) which changes WSOCK32.DLL. While disinfecting, the file has to be replaced by a backup copy from the installation CD or by a backup copy the worm creates during infection. However, only a few programs do this – most delete WSOCK32.DLL or leave it in a modified state. A well-known ItW worm with backdoor functions is Win32/QAZ. With this worm, the file called NOTE.COM must be renamed NOTEPAD.EXE (after deleting the viral NOTEPAD.EXE) but only one program did this in our last test. Only two programs were able to remove the Autostart entry – out of 13 scanners tested. AV companies should not document large disinfection instructions with up to 20 difficult steps if they can be automated.

Of course, users should be warned in the case of a critical disinfection and also if a virus like Ripper or XM/Compat has infected the system, since these two viruses change the user's data randomly. Win32/MsInit (aka RC5) causes a problem, too – one part of it is a harmless program, but the user should know about its installation and resource consumption. Maybe a macro virus warning feature can be restored in the Registry too, or the program can display a warning about it.

File and Macro Disinfection

Disinfection of DOS viruses did not often result in problems – sometimes files were simply a little bit longer, since the virus did not store the original length. With Win32 it is a very complex task to restore everything so that the program is still able to run. This can easily be seen by comparing the disinfected files of different programs – usually no two repairs are identical (for DOS, it is). This also causes the problem of a scanner creating a new variant of an existing backdoor or worm program when it cleans it the virus incorrectly and does not check for further infections or cannot find the wrong, cleaned malware program any more. There are many examples of this, such as a Win32/CIH-infected Win32/Back_Orifice backdoor.

Macro disinfection is a complex task too, especially if the program tries to keep the user macros intact. More than half the programs we tested had problems with this, however the results looked better after every test. Most are just inconvenient, such as error or macro virus warning messages while opening a disinfected *Office* document or while opening the VBA Editor even if no macro is inside the file. In some cases this is easy to avoid – *Office 95* files can be cleaned very easily so that neither *Office 97* or *2000* displays a virus warning message.

It is more difficult to clean *Office 97* or *2000* files correctly and after we compared disinfection methods we can say that every company's methods differ slightly, with better or poorer results. There were only two programs which cleaned the files so 'well' that they could only be opened with many error messages on an English version of *Office*, and not at all on a localized German version.

We keep testing all possibilities of parasitic and non-parasitic DOC and XLS infections. The first problem occurs while scanning parasitic infections: some programs are unable to detect the virus any more, even if the program is still working fine. The second problem is the disinfection: sometimes user macros are removed (in the case of parasitic macro viruses this is OK), sometimes the ThisDocument stream is destroyed, sometimes the modules are corrupted and sometimes the file or the VBA editor cannot be opened nor could macros be created or started. More than one program had a nice idea for disinfection: all macros (sometimes including the user macros) were shortened – only the 'Sub <Name>', some spaces and 'End sub' were left – with interesting results, if the virus uses functions like FileSaveAs…

Conclusion

This series has covered only a number of important issues concerning the oft-encountered problems of anti-virus programs. There are a lot of others, such as a good central administration program, but much has been written on this. There are still many improvements needed for groupware anti-virus software, for example, not only allowing black-listing, but also white-listing of file types using smart scanning. It should also be noted that anti-virus programs cannot constitute the future in our connected world, but together with other kinds of software, like desktop firewalls and content filtering programs they may help to make the problem easier to handle.

I'd like to thank the people who gave me comments and suggestions for this articles and our tests, especially Sarah Gordon, Eugene Kaspersky, Igor Muttik, Petr Odehnal and Costin Raiu. Readers are asked to refer to our exhaustive comments on disinfection results for current tests on our newly-designed Web page http://www.av-test.org.

COMPARATIVE REVIEW

Look at ME!

Matt Ham

Since the last Comparative in these hallowed pages, back in the November issue, there has been change in the world. Most noticeably, to the outside world at least, a relative host of executable viruses descended upon the WildList in a plague of biblical proportions, replacing the recent deluge of script viruses. These introduced an extra extension to scan – the .CHM used by the W32/BleBla worm – an event which always brings uncertainty into the results of the Comparative tests. For further possibilities of the unexpected, the platform tested this month – *Windows ME* – is one which has never before been used in *VB* testing.

The general scientific method of testing is of changing only one variable at a time, though having changed two thus far it seemed a good time to change everything else as well. In truth, the change of hardware was inevitable, since the venerable test machines have been taking an intolerable length of time to complete tests recently, and did not have sufficient hard drive space to install *Windows ME* and all the required test-sets. Details of the exact hardware used can be found, as ever, at the end of this review.

Test Procedures

With all this remodelling out of the way the test procedure itself was the final area where changes occurred, though in this case perhaps codification was more the order of the day. The overall gist of the VB 100% testing regime has been clear since its inception – test the software in its default settings for detection and false positives. With the addition of several new parts to the test, however, combined with there being many different ways to prove that a product can detect a virus in a specific file, there have been several occasions when this has been too vague – thus the following clarification.

In order to be given a VB 100% award a product must detect, in its default setting, all viruses on the top half of the WildList during the month prior to its test. 'Default setting' refers to such selectable affairs as sensitivity of detection, scanned extensions and the use of heuristics. Settings not related to detection *may be changed* in order to facilitate the production of realistic results. This full detection must be demonstrated both on-access and on-demand.

For on-demand testing, results are preferably taken by parsing of log files, with the setting of 'report only' selected. Network and CD scanning has been seen to introduce sporadic errors into the test results and thus this is performed upon a copy of the test-sets on a local hard drive. It has, however, been the case in many products of late that log files are either useless for *VB* results or that the taking of log files causes the scanner to crash after a certain size is reached. In such cases, the preferred method is to run a scan selecting 'delete' as the option, followed by another choosing 'quarantine' and another scan to check that no further files are being detected as viral. Those files remaining are regarded as misses.

For on-access testing, a tool is used which seeks through the test-sets recursively, opening each file in turn. Scanners are set to block access on opening of an infected file and a tool generates a log of those files opened. For products which scan on 'file close' rather than 'open' a different method is used. Under operating systems where such a function is available natively, the test-set is copied using a command which allows the blocking of individual copy operations. In this test the XCOPY command was used for this purpose.

For false positive detection, the scanners are required to produce no false positives on the OLE and Clean test-sets. Many products declare files to be suspicious which is *not* considered to be a false positive but is registered as having occurred in the table of results. If archive scanning is implemented it is activated, if 'off' by default it is only run during the scans involving archived files. These latter tests are not used for the determination of false positives.

A healthy dose of preamble out of the way, the results are to come. With despair, frustration and explosions in store for the reader, who could resist the wonders that await ?

Aladdin eSafe Desktop v3

ItW Overall	99.6%	Macro	96.8%
ItW Overall (o/a)	31.3%	Standard	97.0%
ItW File	99.6%	Polymorphic	89.3%

A strange set of results from *Aladdin* saw an impressive improvement in the on-demand results in comparison with the November tests on *NT*, with only two files undetected in the wild and overall several hundred more viruses detected.

There was, however, a downside to this with macro detection seeming to be partially disabled on-access. This was most noticeable with *Word 97* files, with other macro containing objects being somewhat affected. Though it is probably fair to assume this to be a momentary, if worrying, blip in the detection, the developers have reasons to be both pleased and displeased alike with this result.

Also of interest was *eSafe's* behaviour on the scan speed tests. On several occasions the scanner gave the message 'skipped xx files' where xx was a number ranging from 2 to 32. This behaviour was not explained further in any way and was in addition to three false positives.

On-demand tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Aladdin eSafe Desktop	0	100.00%	2	99.65%	99.66%	125	96.80%	322	89.32%	73	97.01%
Alwil AVAST32	0	100.00%	2	99.53%	99.55%	25	99.32%	8	95.36%	12	99.03%
CA InoculateIT	0	100.00%	2	99.53%	99.55%	0	100.00%	9	98.87%	2	99.61%
CA Vet Ant-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	268	93.73%	2	99.96%
DialogueScience DrWeb	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
FRISK F-Prot	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.98%	8	99.15%
GDATA AntiVirusKIt	0	100.00%	2	99.53%	99.55%	0	100.00%	0	100.00%	0	100.00%
GeCAD RAV	0	100.00%	1	99.77%	99.77%	0	100.00%	0	100.00%	1	99.90%
Grisoft AVG	0	100.00%	2	99.53%	99.55%	8	99.79%	124	92.01%	30	98.67%
HAURI ViRobot	10	52.38%	194	78.14%	77.42%	1229	67.56%	10904	27.83%	735	58.23%
Kaspersky Lab KAV	0	100.00%	2	99.53%	99.55%	0	100.00%	0	100.00%	0	100.00%
NAI VirusScan	0	100.00%	1	99.91%	99.91%	0	100.00%	19	97.86%	7	99.86%
Norman Virus Control	0	100.00%	1	99.77%	99.77%	0	100.00%	618	92.43%	23	98.87%
Sophos Anti-Virus	0	100.00%	2	99.53%	99.55%	13	99.65%	191	95.24%	37	99.15%
Symantec Norton AntiVirus	0	100.00%	0	100.00%	100.00%	17	99.53%	0	100.00%	16	99.46%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	2	99.93%	15	98.70%	5	99.61%

Alwil AVAST32 v3.0

ItW Overall	99.5%	Macro	99.3%
ItW Overall (o/a)	100.0%	Standard	99.0%
ItW File	99.5%	Polymorphic	95.3%

The first to fall victim to samples of W32/Blebla.B and .C, *Alwil's AVAST32* failed to detect the two .CHM files in the ItW set. Detecting these would not have been enough to gain a VB 100% award, however, due to the scanner's behaviour in the OLE Clean set. The scanner hung repeatedly on an *Excel* file.

In any case a true speed of scanning figure could not be determined and *AVAST32* is rated as 'not tested' for the two OLE-related speed tests. It also proved impossible on several occasions to stop a scan job permanently; only pausing seemed to work and this prevented exiting the application via any normal means as this paused job was pending. *AVAST32* also gained frustration points due to its somewhat impenetrable interface, which has an impressive number of controls yet manages to hide away some of those required for logging or actions to take on infection.

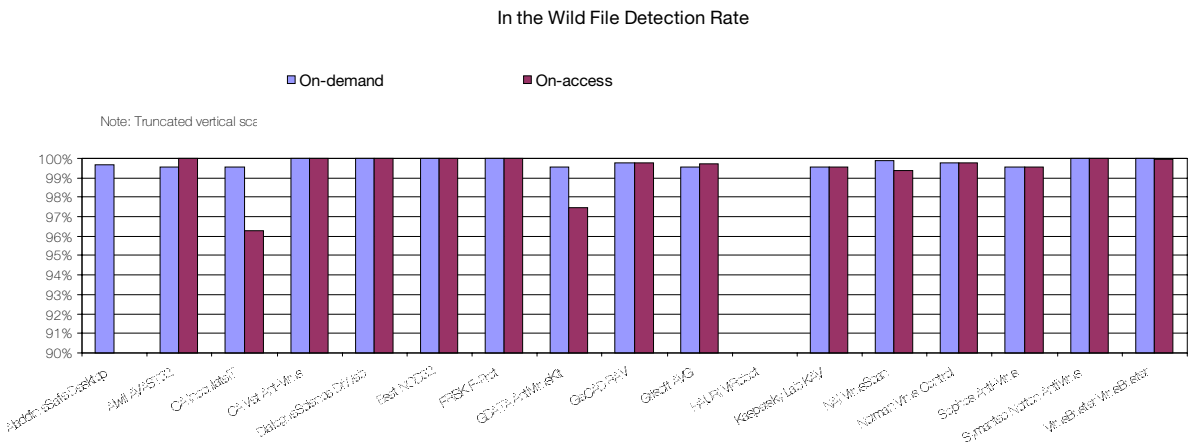
On-access scanning was performed by means of XCOPY, as there is no detection on 'file open'. The on-access scanner did manage, however, to deny reboots based upon a non-bootable CD being in the drive.

CA InoculateIT v4.53 build 524

ItW Overall	99.5%	Macro	100.0%
ItW Overall (o/a)	96.2%	Standard	99.6%
ItW File	99.5%	Polymorphic	98.8%

InoculateIT seemed to be having problems adapting to the new operating system, showing a downturn in detection since the latest *Windows NT* and *Windows 98* tests. Most surprising was the non-detection of Michaelangelo in the on-access sets. There were also extension list problems on-access with .SCR files being passed over.

One possible cause for alarm here was the patch supplied with the product which claimed to address VBS security hazards. This resulted in declaring all files with the .VBS extension to be possibly viral. While not a totally outra-



geous idea, it must be noted that standard *Windows ME* installations contain six .VBS files by default, and thus this patch almost guarantees false positives on a basic machine. Although the Clean set does not currently contain .VBS files, this particular patch seems destined to spur the addition of visual basic scripts to the Clean set.

CA Vet Anti-Virus v10.2.5.2

ItW Overall	100.0%	Macro	100.0%
ItW Overall (o/a)	100.0%	Standard	99.9%
ItW File	100.0%	Polymorphic	93.7%

Faring rather better in this test than its sister product *Vet* claims another VB 100% award as a result of its consistency. This was one of the first products examined and the first to demonstrate the blue screen warning from the OS upon removal of a disk from a floppy drive when *Windows ME* is not expecting it, in the same way that CDs cause this effect in *Windows 98*. This obvious change in the handling of floppy accesses did not, however, alter *Vet's* behaviour.

Misses for *Vet* were almost entirely to be found within the Polymorphic set, though small differences in on-access and on-demand scanning saw a slight advantage emerge for the former. One area where *Vet* has definitely lost ground is scan speed. Where once it was undisputed king of speed it now puts in a good performance on the OLE files but is only average on the executable Clean set.

DialogueScience DrWeb v4.22

ItW Overall	100.0%	Macro	100.0%
ItW Overall (o/a)	100.0%	Standard	100.0%
ItW File	100.0%	Polymorphic	100.0%

The second product to offer no default on-access scanning for 'file opens', *DrWeb* was tested using XCOPY. The on-access scanner showed a smattering of misses in the Standard set, though elsewhere and on-demand detection was perfect. That a certain degree of *DrWeb's* efficiency was due to heuristics was hinted at by the only fly in the ointment, a large number of warnings of suspicious files in the speed tests. These were not quite at the level of false positives, and thus a VB 100% was deserved and granted.

On an aesthetic note the alerts for on-access scanning are of a decidedly DOS-inspired nature and both unpleasant to look at and obtrusive. This cannot be held against *DrWeb* as alerts should be difficult to avoid – other products were cursed with 'ignorable alerts', a much greater problem.

Eset NOD32 v1.58

ItW Overall	100.0%	Macro	100.0%
ItW Overall (o/a)	100.0%	Standard	100.0%
ItW File	100.0%	Polymorphic	100.0%

A product which does not change is often a bad thing, though in the last Comparative *NOD32* took a turn for the worse by missing out on a VB 100% award. This review showed a return to what *Eset* must consider the good old days with full detection across the board combined with a lack of any false positives – worthy of a VB 100% award again.

With no misses and an excellent overall scanning speed, there is little in the way of comment to make which is not blatantly obvious to even the most myopic observer. The interface does, in the hunt for notable changes, appear to have undergone some minor tweaking. This results in more control available than in the deep and distant past, while the artwork still ranks as a personal favourite.

FRISK F-Prot v3.08

ItW Overall	100.0%	Macro	100.0%
ItW Overall (o/a)	100.0%	Standard	99.1%
ItW File	100.0%	Polymorphic	99.9%

It has been some time since *F-prot* has been seen in its naked form, rather than clothed in the garments of *F-secure*. Given *F-Prot's* good reputation for its macro detection capabilities

On-access tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Aladdin eSafe Desktop	0	100.00%	634	29.42%	31.38%	3475	10.81%	690	73.54%	75	96.76%
Alwil AVAST32	0	100.00%	0	100.00%	100.00%	17	99.53%	28	95.36%	11	99.08%
CA InoculateIT	1	95.24%	28	96.28%	96.25%	17	99.64%	255	98.00%	59	97.22%
CA Vet Ant-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	268	93.73%	0	100.00%
DialogueScience DrWeb	0	100.00%	0	100.00%	100.00%	1	99.98%	0	100.00%	9	99.81%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
FRISK F-Prot	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.98%	22	98.84%
GDATA AntiVirusKIt	21	0.00%	8	97.44%	94.73%	0	100.00%	0	100.00%	4	99.64%
GeCAD RAV	0	100.00%	1	99.77%	99.77%	0	100.00%	292	89.47%	2	99.71%
Grisoft AVG	21	0.00%	2	99.73%	96.95%	29	99.31%	292	89.47%	47	97.11%
HAURI ViRobot	21	0.00%	194	78.14%	75.96%	1229	67.56%	10904	27.83%	735	58.23%
Kaspersky Lab KAV	0	100.00%	2	99.53%	99.55%	0	100.00%	0	100.00%	0	100.00%
NAI VirusScan	0	100.00%	4	99.40%	99.42%	3	99.97%	34	97.69%	10	99.63%
Norman Virus Control	0	100.00%	1	99.77%	99.77%	0	100.00%	616	92.44%	23	98.87%
Sophos Anti-Virus	0	100.00%	2	99.53%	99.55%	14	99.60%	191	95.24%	37	99.15%
Symantec Norton AntiVirus	0	100.00%	0	100.00%	100.00%	17	99.55%	0	100.00%	16	99.46%
VirusBuster VirusBuster	3	85.71%	1	99.96%	99.56%	8	99.82%	15	99.44%	5	99.61%

there was potential for a surprise if results for the scanner were not good. Surprises were not to be had – *F-Prot* easily qualified for the fourth VB 100% award in this review. The misses for *FRISK's* offering were a handful of standard and polymorphic files with no real shocks among them.

The only odd behaviour of note came in the on-access floppy scan tests, where the declaration of infection was made twice for each disk scanned. This made for a confusing test, but again, too many alerts is substantially better than too few.

GDATA AntiVirusKit v10.0.1.0

ItW Overall	99.5%	Macro	100.0%
ItW Overall (o/a)	94.7%	Standard	100.0%
ItW File	99.5%	Polymorphic	100.0%

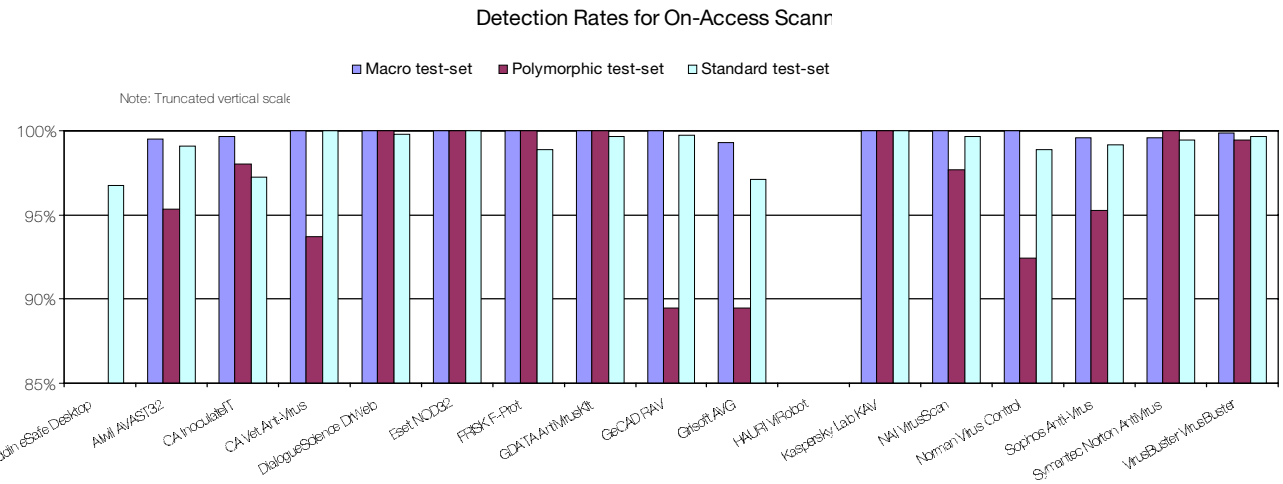
Having recovered from its non-scanning of macros in the last Comparative, or perhaps having slyly transferred this problem to *Aladdin*, *AVK* had a much better showing on this outing. ItW on-demand the two W32/Blebla.CHM files proved to be unsurprisingly undetectable. More odd was that the .EXE parts of this worm, in its .B and .C variants, were detected on-demand but not on-access, the on-access scanner also failing to detect a pair of W32/MSInit variants also in the wild.

No other problems were encountered except in the matter of log files, which at first appeared to be as required, but failed due to the inclusion of page numbers interspersed with the scan data. On-demand detection ratings were thus judged by the deletion and quarantine method.

GeCAD RAV v8.1.5.28

ItW Overall	99.7%	Macro	100.0%
ItW Overall (o/a)	99.7%	Standard	99.9%
ItW File	99.7%	Polymorphic	100.0%

Though in the final stages of beta in the last review, *RAV* was definitely finished and in an improved state in this test. Like several other products, *RAV* sports a dual mode, with 'advanced' and 'simple' being freely interchangeable once



the relevant button has been located. On the detection front for files, results were impressive, only JS/Unicle preventing 100% detection ItW.

On-access there were problems – with a full log and monitor enabled the scanner was not entirely stable, while the floppy scans verged on the invisible on occasion due to being non-modal and not always in the foreground. On-demand, the floppy scans managed to declare two scans for each disk, one of which always declared 'no infection' while the other proved accurate. A worthy product, it seems likely that these small issues will be attended to by the next review, though the heuristics are still more than a little fierce during the scan speed tests.

Grisoft AVG v6.0.226

ItW Overall	99.5%	Macro	99.7%
ItW Overall (o/a)	96.9%	Standard	98.6%
ItW File	99.5%	Polymorphic	92.0%

The ancient adversary that is JS/Unicle was also the only file missed in the wild for *AVG* – another in a long line of steady improvements. The *Grisoft* scanner also shared a predeliction for finding viruses where there were none in the Clean set, mostly in cases where the scanned files would be decompressed upon execution.

Floppy scanning is the prime area of concern for *AVG* – absent in the on-access field and very cumbersome in the on-demand scanner. On speed of scanning of OLE files, however, *AVG* is the undisputed champion and can boast a good detection rate in addition to raw speed.

HAURI ViRobot 2000 v3.0

ItW Overall	77.4%	Macro	67.5%
ItW Overall (o/a)	75.9%	Standard	58.2%
ItW File	78.1%	Polymorphic	27.8%

The arrival of a newcomer to the *VB* Comparatives is always a nervous time. As far as ease of operation and scan speed went, however, *ViRobot* was a pleasant product and an early sigh of relief was breathed. There were some ominous signs though – a very small extension list and a scan rate almost too fast to be true being the main concerns.

Analysis of the results showed these concerns to be valid, with heavy misses across the board. Detection rates were slightly better for wild viruses than in other sets, and *Excel* files were better detected than the other *Office* formats. This is not surprising – *Word* is not at all popular in *HAURI's* native Korea, being supplanted by local products better able to deal with the hangul character set. *Excel*, on the other hand, is as popular as elsewhere. There is definitely room for improvement, and other developers will testify that inauspicious beginnings can be overcome in time.

Kaspersky Lab KAV v3.5.133.0

ItW Overall	99.5%	Macro	100.0%
ItW Overall (o/a)	99.5%	Standard	100.0%
ItW File	99.5%	Polymorphic	100.0%

A nominally new product that will nevertheless be recognised by all regular readers, *KAV* once more falls short of a VB 100% award by the slightest of margins. This is again an extension issue, with the W32/Blebla .CHM files proving *KAV's* undoing. The 'scanner formerly known as AVP' presence of *KAV* was made more obvious by the parenthetic insertion of *AVP* in the 'help about' field of the program, though other than the name, few changes seem to have been made to the application itself.

As with other products though, there were some oddities with *Windows ME's* floppy operations, with disk changes causing strange messages to pop up on occasion, though this had no effect upon detection rates.

NAI VirusScan v5.15.0002.1

ItW Overall	99.9%	Macro	100.0%
ItW Overall (o/a)	99.4%	Standard	99.8%
ItW File	99.9%	Polymorphic	97.8%

Hard Disk Scan Rate	Executables			OLE Files			Zipped Executables		Zipped OLE Files	
	Time (s)	Throughput (kB/s)	FPs [susp]	Time(s)	Throughput (kB/s)	FPs [susp]	Time (s)	Throughput (kB/s)	Time(s)	Throughput (kB/s)
Aladdin eSafe Desktop	885	618002	3	24	3305574		300	531389	32	2331484
Alwil AVAST32	535	1022303		n/t	n/t	1	197	809221	n/t	n/t
CA InoculateIT	121	4520101		9	8814863		74	2154278	17	4388676
CA Vet Ant-Virus	356	1536326		14	5666698		105	1518253	21	3552738
DialogueScience DrWeb	334	1637521	[25]	35	2266679	[1]	147	1084467	25	2984300
Eset NOD32	80	6836652		16	4958360		71	2245304	14	5329107
FRISK F-Prot	200	2734661		22	3606080		95	1678069	33	2260833
GDATA AntiVirusKIt	495	1104913		37	2144156		103	1547734	23	3243804
GeCAD RAV	1308	418144	2[47]	20	3966688		187	852495	39	1913013
Grisoft AVG	262	2087527	4 [2]	115	689859		99	1610269	18	4144861
HAURI ViRobot	62	8821487		39	2034199		147	1084467	47	1587394
Kaspersky Lab KAV	181	3021725		27	2938288		88	1811552	19	3926710
NAI VirusScan	156	3505975		21	3777798		108	1476080	29	2572672
Norman Virus Control	366	1494350		21	3777798		159	1002620	19	3926710
Sophos Anti-Virus	185	2956390		24	3305574		73	2183789	20	3730375
Symantec Norton AntiVirus	438	1248704		68	1166673		444	359046	35	2131643
VirusBuster VirusBuster	408	1340520		28	2833349		221	721342	14	5329107

A host of problems were noted in the *NT* Comparative relating to *VirusScan's* performance, which are still clearly evident in the current, more retail-oriented product tested this time round. Scanning of infected files was atrociously slow, despite the upgraded hardware. A scan which took at the most an hour on any of the other products (barring *Norton AntiVirus*, of which later) was still meandering its merry way along on *VirusScan* some *forty* hours later. This seemed almost certainly due to the log file, recompiled after every few detections, and as a result detection was ultimately performed by deletion. Even then, time problems were not solved totally, with W97M/Splash proving more time-consuming for each sample than some scanners found the entire test-set.

The scanning engine staff might rightly blame the front-end designers for the first of the problems, and vice versa for the second affliction. Whatever the burden of responsibility, there will be many years in Beelzebub's company for those responsible if there is any justice in the afterlife.

The infected files which caused *VirusScan's NT* incarnation to crash still did so, incidentally, so that I feel justified in ignoring the very decent detection rates in order to be harsh about *VirusScan's* shortcomings.

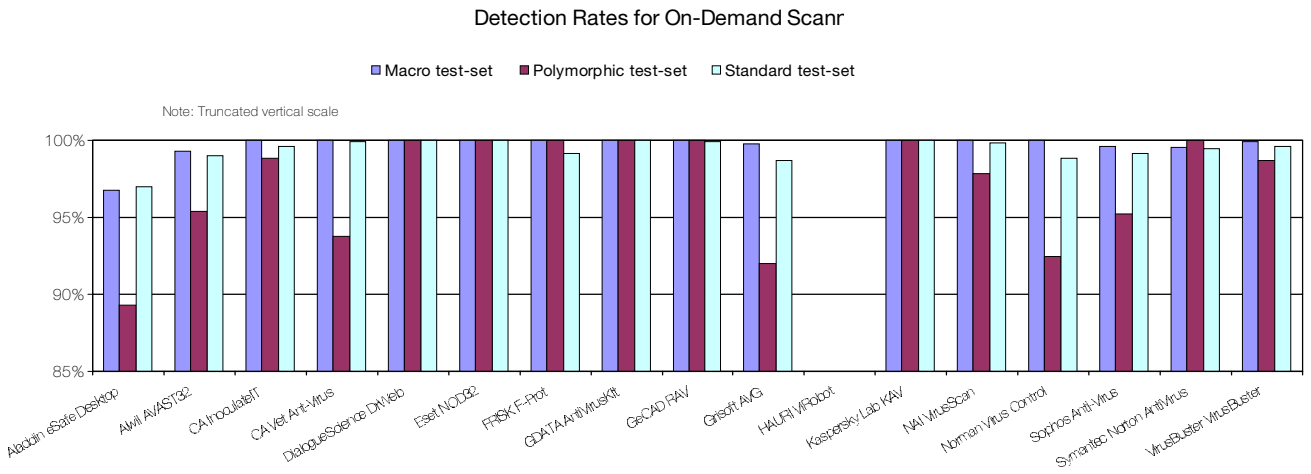
Norman Virus Control v5.00.18

ItW Overall	99.7%	Macro	100.0%
ItW Overall (o/a)	99.7%	Standard	98.8%
ItW File	99.7%	Polymorphic	92.4%

In contrast to the last product, the developers at *Norman* apologised in advance for any instability or detection problems that might arise from their new release – and, thankfully, none were at all apparent. ItW detection stood at 100% but for the .CHM sample of W32/Blebla.B, which was all that denied a VB 100% award to *Norman Virus Control* (*NVC*).

The new design of *NVControl* was not all milk and honey, though. The construction of tasks is a somewhat drawn out and less than intuitive affair, and tasks are required for all but the simplest procedure.

Scanning of floppies required numerous actions, with no chance of a continuous scan, while other tasks had to be constructed in one place and activated from another. There may be a simpler way through all of this, though it is not obvious, but hopefully these are constraints which will be overcome as the product matures.



Sophos Anti-Virus v3.41

ItW Overall	99.5%	Macro	99.6%
ItW Overall (o/a)	99.5%	Standard	99.1%
ItW File	99.5%	Polymorphic	95.2%

Sophos Anti-Virus suffered in the last review from having an extension list a week or so out of date, and thus lacking .PIF files, and repeated this with .CHM files on this occasion, again just missing out on a VB 100% award by this one omission. Other than the two W32/Blebla.CHM files, the misses were the traditional few for *SAV*, encompassing the ACG.A and ACG.B polymorphics and a collection of files in the Standard set.

With the product having had much the same front-end for a considerable time now, there are few other areas to comment upon, though lovers of trivia might wish to know that of the products tested *SAV* is the only one to record files in its log in 8+3 format rather than as long file names.

Symantec Norton AntiVirus v7.50.846

ItW Overall	100.0%	Macro	99.5%
ItW Overall (o/a)	100.0%	Standard	99.4%
ItW File	100.0%	Polymorphic	100.0%

Such was the power of *Norton AntiVirus* that shortly after testing the product one of the machines gave up the ghost in a manner which involved smoke, flashes and loud noises. Not wishing to be afflicted with the same end, I'll tread lightly and state that *NAV's* problems with stability and logging apparent in the *NT* comparative remained in this review.

Instability was decidedly rampant on the on-demand scan and thus detection was performed by deletion on the test-set. The on-demand floppy scan did not provide relief, as it involved a tedious rigmarole which might well prove a fitting activity for those found worthy of a cruel and unusual punishment. These problems aside, *NAV's* detection rates were again more than admirable, and the product picks up another VB 100%.

VirusBuster VirusBuster v3.0

ItW Overall	100.0%	Macro	99.9%
ItW Overall (o/a)	99.5%	Standard	99.6%
ItW File	100.0%	Polymorphic	98.7%

An admirable achiever on-demand, *VirusBuster* was let down by its on-access woes which, as luck would have it, were concentrated in the ItW set. The primary cause for concern, however, was in the on-access boot tests, where detection was very difficult to achieve. Operating system changes are consistently responsible for such problems and the tests performed involved all those permutations which allow feisty scanners to detect boot sector infectors on-access. Despite this, misses remained. One can hope that these are easily remedied, for if they are *VirusBuster* will be in with a good chance of a VB 100% in the near future.

Conclusions

All the changes mentioned in the introduction taken into account showed that the products themselves remained the one real constant. Improving products continued to improve, though in some cases there is little room for it; unlucky products missed out on VB 100% awards by the slightest of margins; the 'big two' (*VirusScan* and *NAV*) continued to be beset with problems of overzealous logging; many products suffered on-access boot problems.

Ever in search of some thrill to titillate the jaded appetite, the next Comparative will focus on *Windows 2000*. Will that be different enough to shake things up? I for one certainly hope so, though the developers might be less keen.

Technical Details

Test Environment: Three 750 MHz AMD Duron workstations with 64 MB RAM, 8 and 4 GB dual hard disks, CD-ROM, LS120 and 3.5-inch floppy, all running *Windows ME*. The workstations were rebuilt from image back-ups and the test-sets restored from CD after each test.

Virus Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/NT/2000/11test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.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 Sth Audubon Road, Wakefield, MA 01880, USA

Tel (781) 2139066, Fax (781) 2139067

END NOTES AND NEWS

The 10th Annual *EICAR* conference, also known as the 2nd European Anti-Malware conference, is to be held in Munich, Germany from 3–6 March 2001 at the Hilton Munich City Hotel. **For more information about the programme and registration details see http://www.eicar.org/.**

***Sophos* is to host a two-day Anti-Virus Workshop on 22 and 23 March 2001** at the organization's training suite in Abingdon, Oxfordshire, UK. For more details about the different courses and training days available, or to reserve your place, contact Daniel Trotman; Tel +44 1235 559933, or email courses@sophos.com.

InfoSec 2001, Europe's largest IT security event, is to take place from 24–26 April 2001 in the National Hall, Olympia, London, UK. See the Web site http://www.infosec.co.uk, or find out more about the event by emailing infosecurity@reedexpo.co.uk.

***Norman Data Defense Systems* announces the release of *Norman Virus Control* version 5.** For more information about this latest release, contact Dawn Cooke; Tel +44 1908 520900 or visit the Web site http://www.norman.com/.

iSEC Asia 2001 is to be held at the Singapore International Convention and Exhibition Centre from 25–27 April 2001. The conference and exhibition covers IT security topics from anti-virus through encryption to biometrics and digital signatures. For more information and a booking form contact Stella Tan; Tel +65 322 2756 or email stella@aic-asia.com.

F-Secure's Instant Security Alert Service uses *EnvoyWorldWide's EnvoyXpress* in order to send subscribers immediate information about the latest virus threats. US$200 buys a year-long subscription to the service. For details see the Web site http://www.F-Secure.com/. The Finland-based AV company's products are now available electronically from the Scandinavian PC-Superstore's Web shop. For details visit the Web site http://pcsuperstore.fi/.

InfoSec Paris 2001, the 15th information systems and communications security exhibition and conference, will take place at CNIT, Paris-La Défense, France from 29–31 May 2001. Companies wishing to participate in the exhibition are encouraged to contact the organisers; Tel +33 0144 537220, or email salons@mci-salons.fr.

iSEC Australia will take place in Halls 5 & 6 of the Sydney Convention & Exhibition Centre from 6–8 August 2001. For information on how you can be a sponsor, exhibitor or delegate, visit the Web site http://www.isecworldwide.com/isec_aus2001/. Alternatively contact Chris Rodrigues; Tel +61 2 9210 5756.

Russian-based anti-virus company *Kaspersky Lab* invites *Virus Bulletin* readers to visit http://www.kaspersky.com/ to see a full year's end review of the 2000 anti-virus scene. Topics include: the anticipation of cell phone viruses, coverage of VBS/LoveLetter, the state of *Linux* against malware, the evolution of worms and the diversification of viruses.

Peapod*, the UK-based e-initiative company, is to distribute *HackerShield, *BindView's* Internet security scanner. The product is available at £2,152 for 100 IP addresses. For more information contact *Peapod*; Tel +44 20 8606 9990 or see http://www.peapod.co.uk/.

***Symantec* has made an advance announcement of the availability at the year's end of *CarrierScan Server 2.0*.** The product will allow Internet companies to integrate *Symantec's* AV protection into Web-based applications and will be available for *Solaris 2.6* and after, *Windows NT* and *Windows 2000*. See http://www.symantec.com/ for more details.

Davinia, the much-hyped email worm, is the first of its kind to use the *Office 2000* UA Control Vulnerability to disable macro security in *Word 2000*. It poses no serious threat to users who employ regularly updated, reputable anti-virus products. We will feature a commentary and analysis of this worm in the March issue.