APRIL 2007

virus BULLETIN

Fighting malware and spam

CONTENTS

ISSN 1749-7027

IN THIS ISSUE

FUTURE TESTING

What lies ahead for anti-virus testing programmes with the introduction of new protection schemes that move away from scanner-based detection? Richard Ford and Attila Ondi look to the future of AV testing.

page 6

ESTABLISHED RESPONSIBILITIES

Who is responsible when a person uses a computer that is infected with malicious software? Can the user be liable even when unaware of the infestation? Can the user be liable even if they do not own or control the computer? Patrick Knight considers what is needed to achieve justice in the digital age.

page 9

VB100 ON LINUX

In this month's VB100 test John Hawes put 16 AV products through their paces on *SUSE Linux*. Find out how each of them fared.

page 11

vbSpam supplement

This month: anti-spam news & events, and Martin Overton catalogues some of the changes that have been seen in the 419 scam over the last few years.

virus BULLETIN COMMENT

'The anti-malware industry has the habit of developing solutions that detect malicious or unwanted activity.'

Righard Zwienenberg, Norman

MAGICAL LIGHTS SHINE ON YOU

In February, the light of a 'magic lantern' shone once again, this time on computer users in Germany. 'Magic lantern' is the term that has been adopted by the anti-malware industry to describe a trojan that is planted (without the user's consent) on a system by an official intelligence agency or criminal investigator in order to gather evidence relating to the user's activities.

The magic lantern idea is not new. The use of trojans to gather evidence has previously been proposed by law enforcers in Sweden, the Netherlands, Denmark and the USA. The first time the magic lantern idea came to light was in 2001, when there was rumoured to be in existence a key logger, created by the FBI, which could be installed remotely via an email attachment or by exploiting vulnerabilities in the operating system. (Code Red was first discovered in July 2001 – was it a trial run?)

However, there is something of an obstacle for all magic lantern projects: the anti-malware industry has the habit of developing solutions that detect malicious or unwanted activity. And we are getting better and better at doing so in a generic way, using heuristics or behavioural analysis. Therefore there is a very high likelihood that at least one anti-malware product or forensic tool will be able to detect the malicious nature of the code (which, at least from the user's point of view is unwanted), thus revealing the presence of the trojan to the user. This would put the evidence gathering at risk: a criminal who detects a surveillance trojan on his system would likely then delete all the evidence before the investigators have obtained it. Extremely counterproductive!

To get around this problem, the intelligence agencies will have to ask the anti-malware industry *not* to detect their magic lantern trojans. To ask one company for cooperation would seem reasonable, but to get the entire anti-malware industry to agree *not* to detect a piece malicious code (whose origin and purpose is irrelevant for analysing engines) would be a utopia.

The anti-malware industry as a whole has, in fact, already agreed to make one exception to its detection rules: almost all anti-malware products detect and treat as malicious the (clean) EICAR test file (see http://www.eicar.org/anti_virus_test_file.htm). However, in the case of the magic lantern trojan, even if the majority of vendors agreed not to detect the trojan, it is likely that there will always be one or two (if not more) vendors who choose to detect it. This may be for ethical reasons, it may be because the vendors are new to the market and unaware of the non-detection agreement, it may be for PR reasons (making such an exception would get the company a lot of press coverage), or it may simply be because the vendor has updated its behavioural analysis module, with the result that the trojan has become detectable.

For the sake of this article, let's assume that it *is* possible to have a global non-detection agreement for a magic lantern trojan. The next problem is that the trojan can only be used once. Criminals may have backups which are not discovered and confiscated at the time of their arrest. These could then be analysed by the criminals or their associates, and information about the trojan would quickly become freely available. Even if the established anti-malware industry didn't detect it, there would be a market for one-off scanners, detecting just this instance of the 'magic lantern trojan'. So, for every instance in which an agency wants to deploy a magic lantern trojan, a new one would have to be made – and in every instance it would require the agreement of all anti-malware and forensic utility vendors not to detect it. World peace would be easier to accomplish.

As for whether such a magic lantern does exist and has ever been used, I am not aware of one, and I don't believe such a thing has ever been deployed (yeah, right!). If I at least plead ignorance in public, it might save me from being taken away in a dark-windowed car by men in black suits and sunglasses.

NEWS

VB2007 CONFERENCE PROGRAMME REVEALED

VB has revealed the conference programme for VB2007, Vienna.

Once again, the three-day conference programme boasts an exceptional line-up of anti-malware and anti-spam expert speakers and caters for both technical and corporate audiences. More than 40 presentations will cover subjects including: automated analysis, rootkits, malware in the gaming world, malware on mobile devices, anti-malware testing, spam and phishing trends and techniques, spyware, forensics, legal issues and much more. In addition to the scheduled traditional 40-minute presentations, a portion of the technical stream is set aside for brief (20-minute) technical presentations, dealing with up-to-the-minute specialist topics. Proposals for the 'last-minute' presentations must be submitted two weeks before the start of the conference (details of how to submit proposals will be announced in due course). The schedule for the last-minute presentations will be announced shortly before the start of the conference.

VB2007 takes place 19–21 September 2007 in Vienna, Austria. Online registration is now available. For the full programme see http://www.virusbtn.com/conference/vb2007/programme/.

THIRD ROUND FOR US ANTI-SPYWARE BILL

Anti-spyware legislation was presented for the third time in the US House of Representatives last month. The proposed 'Spy Act' ('Securely Protect Yourself Against Cyber Trespass Act') would make it unlawful to install software that gathers information, monitors usage, serves up ads or modifies browser and other settings on the computer without the user's consent. The legislation would afford the Federal Trade Commission (FTC) wider scope to pursue those responsible for spyware, broadening the definition of spyware and allowing the FTC to impose fines of up to $3 million per violation of the act.

However, the Spy Act has twice before been passed by the US House (in 2004 and 2005), but on both occasions faltered once it reached the Senate thanks to opposition from the advertising industry. With the increasing proliferation of spyware, as well as extensive media coverage of legal cases involving spyware (see *VB*, March 2007, p.12), it is hoped by many that it will be third time lucky for the passing of the Spy Act.

Prevalence Table – February 2007

Virus	Type	Incidents	Reports
W32/Netsky	Worm	2,076,653	30.11%
W32/Mytob	Worm	1,695,000	24.58%
W32/Bagle	Worm	886,328	12.85%
W32/MyWife	Worm	737,206	10.69%
W32/Virut	File	454,248	6.59%
W32/Zafi	File	416,147	6.03%
W32/Lovgate	Worm	195,217	2.83%
W32/Mydoom	Worm	142,380	2.06%
W32/Bagz	Worm	60,811	0.88%
W32/Tenga	File	52,323	0.76%
W32/Funlove	File	30,300	0.44%
W32/Parite	File	26,002	0.38%
W32/Klez	File	22,402	0.32%
W32/Womble	File	16,063	0.23%
W32/Bugbear	Worm	15,699	0.23%
W32/Mabutu	Worm	14,474	0.21%
W32/Valla	File	9,995	0.14%
VBS/Redlof	Script	7,412	0.11%
W32/Stration	Worm	6,763	0.10%
W32/Sality	File	5,610	0.08%
W32/Sober	Worm	4,771	0.07%
W32/Yaha	File	3,438	0.05%
W32/Maslan	File	2,255	0.03%
W32/Dref	File	1,913	0.03%
W32/Dumaru	File	1,292	0.02%
W32/Elkern	File	1,280	0.02%
W97M/Thus	Macro	1,123	0.02%
W32/Plexus	File	1,074	0.02%
W95/Tenrobot	File	1,011	0.01%
W95/Spaces	File	795	0.01%
W32/Darby	File	748	0.01%
W32/Mimail	File	685	0.01%
Others[1]		4,808	0.07%
Total			100%

[1]The Prevalence Table includes a total of 4,808 reports across 40 further viruses. Readers are reminded that a complete listing is posted at http://www.virusbtn.com/Prevalence/.

VIRUS ANALYSIS

WORMHOLE ATTACKS SOLARIS STATION

Costin Ionescu
Symantec, Ireland

Looking at the title of this article, you might be forgiven for thinking that you were about to read the script of an episode of *Star Trek*. Well, maybe next time – for now it is just the story of the Wanuk/Froot worm, or what is more widely known as the Solaris Telnet worm.

The number of threats designed to work on *Solaris* is quite small, and these consist mostly of tools used to perform DoS attacks, although we can also add to that a fine share of UNIX-compatible threats. Writing a worm for a more common platform like *Windows* does not seem as 'exotic' as writing one for *Solaris*, and this was probably one of the reasons for this unnecessary creation. Of course, other reasons include the fact that the vulnerability is trivial to exploit and it was disclosed before a patch was available.

If there were a Hollywood equivalent for the virus-writing industry, that is where this virus would have been produced – it has all the hallmarks of a 'wanna-be'. In the movie industry the following can be seen as a recipe for success: take an interesting book (it's easier than spending time and effort creating a new story), make a small change to the meaning that the author of the book wanted to express, add some shiny visual effects and voilà – a blockbuster!

Now, for the virus-writing equivalent: substitute a vulnerability advisory/disclosure for the interesting book, change its original meaning (instead of aiming to improve the security of the affected product, the vulnerability is exploited) and then add the final touch – an extravagant payload. This seems to be the norm for worms that use exploits to spread. Furthermore, worm writers are usually lazy enough to wait for a working proof-of-concept (PoC) exploit that achieves remote code execution after the vulnerability is disclosed. It's very hard (if not impossible) to find a worm that exploits a previously unknown vulnerability. In fact, recently we have seen only a small number of targeted attacks with true zero-day exploits and those used backdoors or trojans rather than worms. In Wanuk's case, the fact that the Telnet vulnerability was so trivial to exploit spared the author some time because there was no need to wait for a further PoC.

THE VULNERABILITY

You can find a fully detailed explanation of the vulnerability in the published advisories [1]. It is a design vulnerability that has existed for a long time, but which became very dangerous when a new command line switch (*-f*) was made available to the login utility to allow 'pre-authenticated' users to log in without being prompted for a password. The Telnet daemon takes whatever string was sent as the user name and passes it to the login. This way, passing '*-f[username]*' will cause the login to consider '*username*' as authenticated.

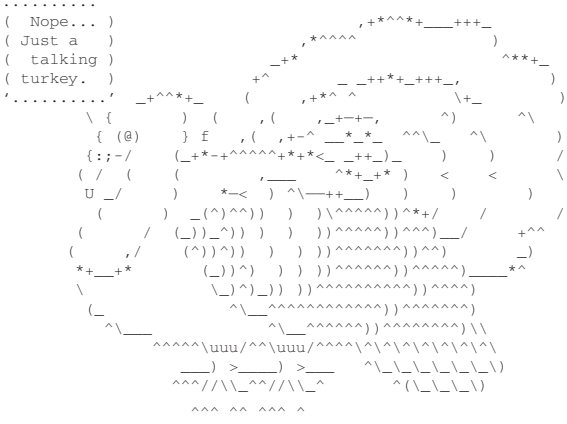
INSTALLATION

The first thing the threat does when executed is to re-spawn itself like a daemon (new session, all standard input/output redirected to /dev/null, signals hooked for a graceful silent exit). If the time is between 1:00 AM and 5:59 AM on the 13th of the month, there is a one in three chance that the payload will run. It waits for noon to broadcast to all users logged onto the server (by using the *wall* utility) either some ASCII art text or, ironically, the patch for the vulnerability that it exploits (in *diff* format). It also has a message, for the faint-hearted users, that displays a fake output of the command to erase the whole file system:

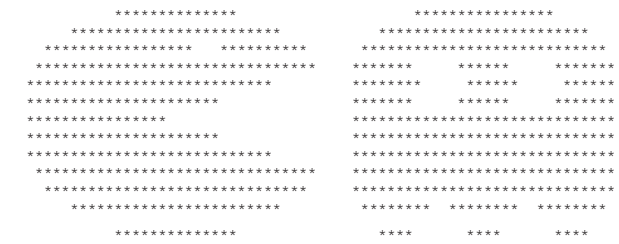
```
# rm -rf /* &
23858
# rm: Unable to remove directory /dev/fd: Device busy
rm: Unable to remove directory /dev: File exists
rm: Unable to remove directory /devices: Device busy
rm: Unable to remove directory /etc: File exists
rm: Unable to remove directory /home: Device busy
rm: Unable to remove directory /lib: File exists
rm: Unable to remove directory /net: Device busy
rm: Unable to remove directory /opt: Device busy
rm: Unable to remove directory /proc: Device busy
rm: Unable to remove directory /system: File exists
rm: Unable to remove directory /tmp: Device busy
rm: Unable to remove directory /usr/openwin: Device
busy
rm: Unable to remove directory /usr: File exists
```

Among the art messages we find:

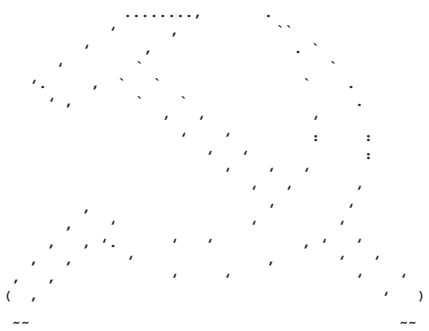
- A talking turkey



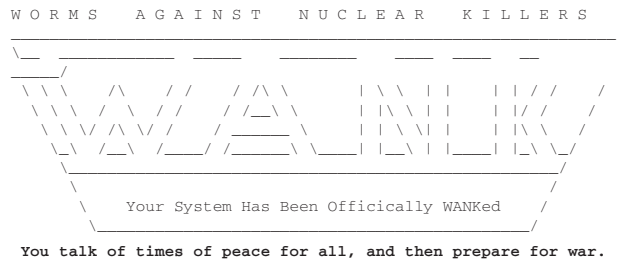
- Pacman's revenge



- A greeting to all the comrades out there



- A bit of self-justifying philosophy/smut



- A party teaser

In two other messages, the author diverts his ASCII drawing talents against Theo deRaadt (founder of OpenBSD) and Gadi Evron, not forgetting to feed us a fake confession, in which he claims to be *Sun* developer Casper Dik [2]:

```
Hi, I'm Casper, I am a bored Sun developer and I
wrote this piece of code.
```

The two out of three times that the threat does not run the payload between the hours of 1:00 AM and 5:59 AM on the 13th of the month, it instead gathers some statistics with IP address ranges that are used for the non-local networks configured on the server and also any IP addresses that are accessed. These statistics are generated by parsing the output of two commands:

- `/usr/sbin/ifconfig -u4a`
- `/usr/bin/netstat -f -inet -rn`

SPREADING

First, the worm creates a thread to deal with the information that it gathered from the statistics above. For each range of IP addresses, it chooses a random address in the range and tries to attack it. It then increments the IP until it reaches the end of that range. In parallel, the worm creates 66 threads to generate random IP addresses (using a predefined list for the most significant byte in the IP address to increase the accuracy), and then it attempts to attack them.

The attack consists of an attempt to connect on TCP port 23 (the standard port for the Telnet service), where it passes the user name -fadm. Upon successful connection, the worm checks that the computer it has connected to is *Intel* or *SPARC* and that the operating system is *Solaris 10* (*SunOS 5.10* or *5.11*).

Next, it creates the directory /var/adm/sa/.adm where it transfers in uuencoded form the two worm bodies (one for *Intel*, one for *SPARC*), saving them as .i86pc and .sun4. The worm then overwrites /var/adm/.profile with a short shell script to be executed on login.

To complete the installation of the worm on the compromised computer, it attempts to copy the worm file to the computer architecture as a name selected randomly from the following list:

devfsadmd	dladm	logadm
svcadm	bootadm	nlsadmin
cfgadm	routeadm	sacadm
kadmind	uadmin	syseventadmd
zoneadmd	acctadm	ttyadmd
sadm	cryptoadm	consadmd
sysadm	inetadm	metadevadm

This copy, which will look like a legitimate process at first glance, is then added as a *cron* job to be executed every day at 1:10 AM. To speed up the spreading process it also executes the newly created copy.

The same attack as described above is performed again in order to open a small back door that just provides a shell to the attacker on TCP port 32982. For this attack, the worm uses the user name lp for the Telnet connection. The directory for installing this threat is /var/spool/lp/admins/.lp and the file names are .lp-door.i86pc and .lp-door.sun4. Again, it will install a *cron* job for the corresponding backdoor copy which can be named any of the following:

lpshut	lpfilter
lpsystem	lpstat
lpadmin	lpd
lpmove	lpsched
lpusers	lpc

CODING SKILLS

Unlike most malware writers, the author of this worm paid a lot of attention to detail with his creation, and included error checks at each step. Even I/O operations on files and sockets are wrapped in nice routines that use timeouts to avoid having the worm hanging on a faulty connection. You rarely see this kind of dedication from virus writers – they are not renowned for writing good quality code. This tends to support the idea that the author of Wanuk may be a professional developer, probably with too much time on his hands.

However, in spite of all the precautions taken by the author, at least one bug slipped through. The bug is in the routine that launches 66 threads for generating random IP addresses to attack and one thread to attack the nearby networks. Before launching the threads, the virus allocates an array of 67 integers to store the thread IDs, but when it creates the thread for attacking nearby networks it attempts to use index 67 for storing the thread ID, instead of 66 (random IP attack threads use indexes 0 to 65).

One more interesting feature is that the author included code to have the worm run in test mode, which was probably used during development. If there is an environment variable named *M*, the worm will use that variable's value as the IP address to attack instead of generating random IP addresses to attack. Also, when running in test mode the payload is disabled (I guess the author got sick of all that ASCII art after a while).

CONCLUSION

Even though we did not see a significant epidemic as a result of this worm (after all, how many people still use Telnet?), this threat showed once again that an increasing number of different platforms are being targeted by malware writers.

Another trend highlighted by this worm is the improved adaptability of malware to multiple architectures (which can easily be achieved for Wanuk, just by recompiling the worm and backdoor source code).

REFERENCES

[1] Sun Solaris Telnet remote authentication bypass vulnerability. http://www.securityfocus.com/bid/22512.

[2] The author feeds us a fake confession, in which he claims to be *Sun* developer Casper Dik. http://www.securityfocus.com/archive/1/459993/30/0/threaded.

FEATURE 1

TESTING TIMES AHEAD?

Richard Ford, Attila Ondi
Florida Institute of Technology, USA

Product reviewing has a long and sometimes contentious history in the anti-virus world. Furthermore, unlike word processors or video games, a user of an anti-malware product is ill-placed to measure the utility of the particular protection scheme, for although its usability and performance can readily be determined, the crucial question of how much protection a product provides is elusive.

As if this were not enough, new developments in anti-malware research mean that this problem could worsen considerably, leaving not only users but reviewers confounded when attempting to evaluate new product developments. As forewarned is forearmed, this article outlines some of the history of anti-virus product reviews and certification, and highlights some of the challenges new technology could bring with it.

THE GOAL OF THE TESTER

The goals of the product tester vary dramatically depending on the audience of the tests. Despite these variations, testing an array of products usually involves either putting them through some sort of 'pass/fail' tests (like product certification schemes), or ranking them in an ordinal way – usually by deciding which is best when measured against a particular set of criteria.

To date, tests of anti-virus software have evolved greatly from their fairly simple beginnings. Whereas initially products were ranked based only on raw detection scores, added emphasis was soon placed on the detection of viruses 'in the wild' (though the concept of 'in the wild' has become increasingly dated with time, and it is no longer entirely representative of the threats facing users), response time, and the overhead the product imposed on the host operating system.

Clearly, how one balances the importance of different areas is somewhat subjective – for example, is missing one zoo virus 100 times less important than missing one wild virus? Most people are fairly comfortable reading these kinds of tests, simply because they are so common.

However, one of the important things to realize is that current tests are easy because the information provided by the products has always essentially been binary: products

generally detect an object or they don't. Thus, it has been easy to count false negative and false positive rates, and provide readers with good, useful data.

The binary nature of traditional anti-virus software – detect or not – meant that there really wasn't much meaning in any middle ground. Files detected using heuristics or other 'softer' techniques generally count toward detection, so reviewers have not had to deal with *degrees* of detection in any great way.

In addition, tests can usually be performed using just one or two machines; complex networks are seldom required. The benefit of the anti-virus software is measurable at the individual machine level: the better-protected a single machine is, the better for all. Thus, our review criteria are geared toward classifiers that are single-unit centric.

COMING TO A MACHINE NEAR YOU…

It would be wonderful if reviewers could continue these reviewing practices for the foreseeable future, but the truth is that as new threats evolve, new protection paradigms also emerge.

For example, in the anti-spam world, several different products have investigated the use of throttling techniques to limit the number of spam messages a user receives. Such a product never actually determines whether or not an individual message is spam. Instead, as mail from a particular endpoint exceeds some threshold or other metric, a delay is injected into the processing of subsequent messages.

This technique can be extremely effective, but its *local* impact is hard to measure without some understanding of the global picture. If a customer implements the system, what levels of spam reduction might (s)he expect? Testing the system against a corpus of spam/non-spam messages is meaningless; only by understanding the dynamics of the whole system can one determine the expected outcome.

Similarly, a product that works by the throttling of network traffic for worm limiting is difficult to evaluate: from the perspective of a single computer, protection is not provided. Holistically, however, the speed (and therefore, ultimately, the magnitude) of outbreaks can be shifted radically. This is in step with biologically inspired systems, for example, which are relatively accepting of sacrificing single units or cells for the good of the whole.

Other new technologies in the anti-virus world are equally challenging for reviewers, as they break away from single machine solutions. Essentially, anything that doesn't operate at the level of a classifier ('run this, don't run that') is well outside the reach of current reviewing methodologies.

LOOKING AT THE BIG PICTURE

While it would be nice to ignore these issues, doing so tends to exacerbate the anti-virus industry's legendary resistance to new ways of doing things. New ideas that emerge need to be compared meaningfully to current best practice.

However, if we need to examine the system as a whole, testing becomes a whole lot more difficult as it's not practical to do this for real. Instead, we need some way of creating our own reality for the purpose of experimentation. That means either an analytical model, a testbed, or a simulation; unfortunately, there's no obvious right answer, as each solution has its own problems.

Simplistically, a testbed seems like the most attractive approach, as it's really quite close to what reviewers do already. A test environment is created and the products are tested under 'real world' conditions. Unfortunately, for products that act more systemically, that's a tall order. Many thousands of nodes might be required to really understand how the product would fare under typical scenarios. Furthermore, generating realistic conditions (for example, realistic simulation of a user browsing the web) is non-trivial.

Analytical models are attractive in that they are elegant and provide a clean way of calculating how a product might fare. Unfortunately, anything but the simplest scenarios lead rapidly to intractable mathematics. Furthermore, most systems incorporate a large amount of randomness. Consider an email worm, for example, which hits a large mailing list by chance early on in its spread. Such a worm would likely be more widespread than one which initially was 'unlucky' in spread.

Getting such data from analytical models is difficult, but an important question for those interested in a product's effectiveness. It's much more useful, for example, to know that 90% of the time the solution works fine, but in 10% of the cases all machines get infected, than it is to know that 30% of machines get infected *on average*.

The last approach is simulation. Up front, we should disclose that we have a certain amount of bias: Florida Tech has spent a lot of time developing Monte-Carlo-based simulators of virus/worm spread. However, this choice of platform was based upon a careful assessment of the needs for the solution. Simulation provides a relatively cost-effective way of determining the likely range of results from a prevention technique, and can be reconfigured rapidly to explore the effect of different parameters.

WE NEED HELP!

Regardless of what technique is chosen, products that affect the population dynamics of spread must be evaluated in

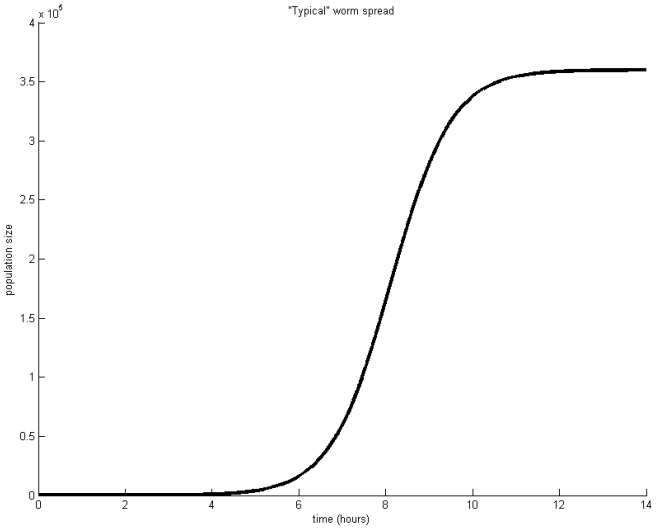


Figure 1: The 'S' curve often seen by virus researchers illustrating the spread of a 'typical' worm.

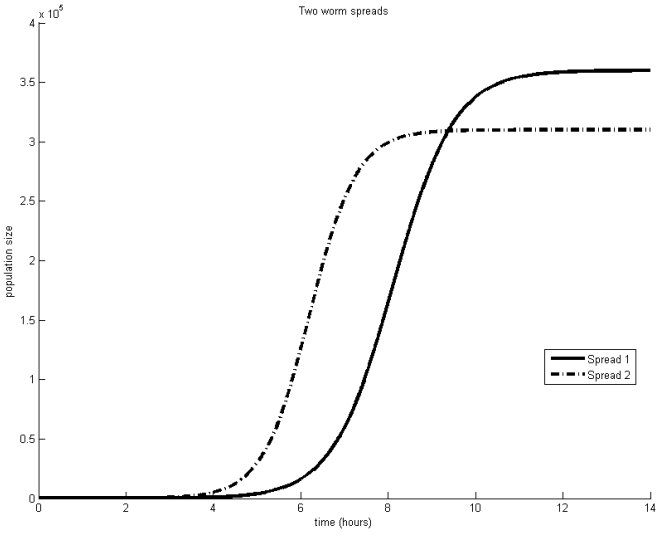


Figure 2: Two different worm outbreaks plotted as a function of time. Which curve is more desirable?

terms of those dynamics. Here, a new issue emerges: there is no real agreement on how to compare different spread dynamics.

Virus researchers will be very familiar with the 'S' curve shown in Figure 1 illustrating the spread of a 'typical' worm over time. Essentially, these curves differ in terms of speed of spread and overall magnitude. However, real-world viruses and worms don't necessarily follow these curves at all. Different spread methods and preventatives all affect the shape of the spread. How can one compare the spread shapes meaningfully? Figure 2, for example, shows two different worm outbreaks plotted as a function of time. Which shape is more desirable from the perspective of a defender? Are they both bad or is one indicative that a particular product is better than another?

Part of the challenge is that no protection scheme can be evaluated *in vacuo*. That is, a protection scheme which slows down a virus/worm outbreak is only meaningful if the slowdown is sufficient to allow other protection schemes to be deployed. For example, slowing the global spread of a worm by one minute will have relatively little impact, but slowing it by three days is more significant if users are able to react in this timeframe. If the delay is sufficient, other defences can be put in place; below a certain amount of time, some slowdown makes no real difference to the size of the outbreak.

Part of the challenge for reviewers in the future will be quantifying 'how much is good enough'. Furthermore, in order for the reviewer to avoid the pitfalls of subjectivity, there will have to be some globally accepted models of reaction times and modification times. How does the public change its behaviour in the face of a particularly nasty worm? These and other difficult questions will have to be explored in order really to compare products which are not simple virus detection engines.

LOOKING TO THE FUTURE

New protection schemes will cause fairly significant problems for those involved in product reviews and certification. In particular, products that move away from binary 'good/bad' classification, and which benefit the system macroscopically instead of microscopically, are well beyond the current experience both of reviewers and certification bodies.

This is not ideal for anyone; at best, it leaves users with no information regarding product effectiveness. At worst, it discourages early adopters and could blunt the penetration of innovations which really do benefit the community as a whole. That's bad for everyone, because at the end of the day the security of the Internet is literally becoming a matter of life and death.

As researchers, as users, and as developers, we need to start thinking about how and why we test products, and how we can prepare for the next wave of innovation. Not doing so is simply shortsighted.

FEATURE 2

(IN)JUSTICE IN THE DIGITAL AGE

Patrick Knight
Authentium, USA

By now many of you will have heard of the court case involving the Norwich, Connecticut, substitute teacher Julie Amero (see *VB*, March 2007 p.12). She was convicted on 7 January on four counts of 'risk of injury to a minor, or impairing the morals of a child' after a malware-infested classroom computer that she was using displayed a barrage of porn-related pop-up windows.

In October 2004, Amero was called to substitute a seventh grade Language Arts class. Reports of the case indicate that a computer in the classroom, which was running *Windows 98* with *Internet Explorer 5*, was used by Amero to browse the Internet and to check email. At some point a website related to hairstyles was accessed either by the teacher or by students. The website contained code that caused a flood of porn-related pop-ups which the teacher could not control. The prosecution in the case claimed that Amero had 'physically clicked' on porn links to cause the pop-ups, which then exposed the children to adult pornography.

Further reports from the trial indicate that the prosecution suppressed critical evidence that would have mitigated the case against her. The forensics investigator for the prosecution admitted that he had not scanned the computer's hard drive for malicious software. The defence hired an independent computer forensics investigator who found several malicious code samples, including code within the hairstyle web page which caused the porn pop-ups. Unfortunately, the jury was not presented much of this evidence because the defence had failed to bring up the topic of malware during the trial's discovery phase.

Testimony also pointed out that since Amero had no credentials to log onto the computer, the regular teacher had logged on with his own credentials and instructed her not to turn off the computer as she would be unable to log back in. This was the reason she gave for not having turned the computer off as a means to protect the children from exposure to porn.

Some serious questions were raised during the trial: why was the teacher accessing her own email from school? Was she browsing the Internet during class time when she should have been teaching? Why did she not do more to shield the children from viewing the images? Who actually accessed the hairstyle website: Amero or a student? All of these are valid questions that demand answers.

In the end, based on the evidence presented during the trial, a jury of Connecticut citizens decided that a 40-year-old female substitute teacher who was four months pregnant had actively surfed the Internet for pornography during class time. Evidently the jury found this to be more believable than a much more difficult explanation involving malicious software, outdated security products, and other computer forensics mumbo jumbo.

CONCERNS

The Amero case has raised a number of concerns regarding computer security, investigation and liability. Who is responsible when a person uses a computer that is infected with malicious software? Can the user be liable even when unaware of the infestation? Can the user be liable even if they do not own or control the computer?

We live in a world where technology is the tool of choice for criminals who want to make money at any cost. The malicious software industry is out to make money and those behind it do not care whose lives are destroyed in the process.

Who is pursuing the author of the website that injected code to cause the pop-ups on the computer in Ms Amero's classroom? Why is this person not liable? What is the liability of the school district that chose to use old computers running outdated content filters and outdated anti-virus software? Does the school district have any responsibility to protect the teachers and students from this type of prosecution by providing safeguards? What about the responsibility of the manufacturer of the web browser to protect users from these types of threats?

The power to legislate and prosecute these crimes is placed in the hands of people who, generally, have no clue about the technology involved. In July 2006 US Senator from Alaska, Ted Stevens, famously described the Internet as a 'series of tubes' and later went on to say: '[I] just the other day got an Internet ... sent by my staff at 10 o'clock in the morning on Friday and I just got it yesterday [*sic*].' Statements like these might be considered laughable if Stevens were not the Chairman of the US Senate Committee on Commerce, Science, and Transportation – which oversees legislation concerning, among other things, interstate commerce, science, technology and telecommunications (e.g. the Internet). From his statements we must presume that he is in no way qualified to make critical decisions regarding technology, and that in order for him to make informed decisions regarding Internet issues he must rely on well-financed lobbyists who have traditionally demonstrated their lack of concern for the greater good.

Criminal prosecutors are no more equipped to discern how technology can be manipulated in a criminal case. Complicating this are methods used by computer forensics investigators who are well trained in file system forensics, but who are not always trained to look for and analyse

malicious software. Many computer forensic investigations include some form of virus scan of the digital data in question. However, if the virus scan does not identify an infection the evidence is submitted as 'clean'. In fact, a result of 'nothing found at this time' might be more accurate. This type of result can easily be manipulated by prosecutors to effectively rule out the possibility of the presence of malicious software.

FORENSICS

More and more criminal trials include evidence that requires some sort of computer forensics examination even if the digital information is not the central theme of the trial. Take the 2004 trial of Scott Peterson who was convicted of killing his wife and unborn son in 2002. The Peterson's home computer was examined for any evidence regarding the disappearance of his wife. Evidence of web browsing was found on the computer. The time of the browsing activities reportedly took place after the time at which police believed Mrs Peterson had disappeared, thus presenting the investigation timeline with a question of whether she was, in fact, still at home or whether Scott was browsing the web after her disappearance. The computer evidence was minor considering the mountain of DNA evidence and other physical evidence against Peterson, but computer investigation was necessary to complete the criminal investigation. If this were another case with an innocent defendant, legal fees including the cost of a computer forensics investigation would surely mount.

Let's examine another hypothetical, but realistic scenario. Suppose a customized trojan infects a PC and deletes, alters or plants email evidence that is somehow used to incriminate an innocent victim. Only the most sophisticated heuristic virus scanner may be able to detect that this trojan is malicious. If such a malware sample is found the forensics investigator must be equipped to analyse it. However, with the volume of data involved in most modern computer forensics investigations, it is not unreasonable to expect that the investigator will not analyse such an application if it is not picked up by the virus scanners.

One might expect that additional evidence would likely exonerate the victim. To this, I simply point back to the Julie Amero case. There was such evidence, but a combination of failures from the defence counsel and improper investigations led to a conviction that many believe is false.

RAISING THE BAR ON FORENSICS

We are creating a society where average citizens must live in fear that their personal computer or the computers they use at work can be used for crime or have evidence planted on them that can destroy their life. The culpability is placed on the user, even when they do not own the computer.

For anyone who handles malicious software it is easy to imagine customized applications that are designed to perform a specific job that might otherwise not find their way into the sample collection of an AV company. Customized trojans need not replicate, open back doors or be found by the hundreds to be malicious. How about a trojan designed to alter timestamps on specific files on a file system? If this trojan does not further open an IRC backdoor or mass mail itself to other machines it may never be picked up by an anti-virus scanner. It is not unusual these days to see this type of malicious software used against another individual or company. In fact, the number of customized trojans is growing as targeted attacks become more common.

This raises the bar for anyone whose primary job is to perform computer forensics or otherwise to analyse malicious software. In a world of incomplete legal representation the stakes are high regarding high-tech investigations. Incomplete investigations or poor defence lawyers can stand between acquittal and a prison sentence.

Computer investigations like this are also quite expensive. Some victims will find themselves forced into a situation where it is financially preferable to make a plea deal with prosecutors than to go broke paying for defence costs and risk greater jail time despite being innocent of the charges against them. There are some organizations, though, that will take on pro bono cases and provide computer forensics examinations. One such organization is the Computer Forensic Volunteer Project which provides computer forensics investigation support for people who are unable to pay for expensive investigations.

More and more, computer forensics and malicious software analysis go hand in hand. In fact, many virus analysts also have forensics backgrounds. Many virus analysts in the AV industry already find themselves helping law enforcement authorities take down bot nets or spam networks. These tasks require a great deal of time and effort on the part of virus analysts as well as law enforcement personnel to gather and present evidence. This effort illustrates the active battle that the AV industry is waging against the malware industry, which goes beyond the passive battle of malware detection.

Lawmakers and law enforcement authorities are in many ways outdated in their abilities to counter malware threats and to protect innocent people. The response of the AV industry to legal investigations is increasing due to the sheer volume of malicious software and how it is being used by criminals. The anti-virus community is well positioned and well equipped to provide the expert testimonies in cases that involve computers and to go after the real criminals.

COMPARATIVE REVIEW

NOVELL SUSE LINUX ENTERPRISE SERVER 10

John Hawes

I approached my first attempt at VB100 testing under *Linux* with a little more than the usual trepidation. Despite some experience of running the open-source UNIX clone, my knowledge of anti-virus products for the platform was limited mainly to the exasperated rantings I had read in previous *VB* comparative reviews. The simple command-line scanners of old, I assumed, were fast becoming a thing of the past, with ever more sophisticated systems now providing the on-access detection that forms a central part of the VB100 testing methodology.

Alongside these advances I expected updating systems to keep products in touch with the latest discoveries in their base labs in the blink of an eye, and for the more corporate-oriented products I expected complex network administration and reporting systems to provide admins with control over the security of their many systems. As I embarked on the testing I could only hope that the baffling installation processes, obscure, incomplete or misleading documentation and generally bizarre behaviour reported by my predecessor would have long since been eradicated.

PLATFORM

The *Linux* operating system continues its steady movement into the mainstream, pushing its unruly way into the media and public consciousness with ever-growing compatibility, efficiency and usability. Novice-friendly distributions provide simple, out-of-the-box installation and a colourful and streamlined user experience, while server platforms – which have long been the most common implementation – have acquired the support and backing of major global concerns, even those that own and promote their own competitive UNIX flavours. Of course, for the legions of admins who prefer to get their hands dirty tinkering merrily under the bonnet, more serious distributions and bespoke versions are as popular as ever.

At the desktop level penetration remains fairly low, with most estimates placing *Linux* on less than 5% of systems. Servers, on the other hand – particularly web and mail servers – are much more likely to be running some kind of *Linux* implementation, with probably more than a quarter based on the open source alternative to UNIX, *NetWare* or *Microsoft*'s offerings.

SUSE (formerly *SuSE*) emerged in Germany in the 1990s and soon rose to prominence as one of the most widespread commercial distributions, particularly in Europe where it has long been the main rival to *Red Hat*'s global domination. While the fedora-themed distributor has blossomed in its own right as provider of a solid and supported platform, *SUSE* was acquired in early 2004 by *Novell*, and has since been marketed heavily and positioned as a solid base for a corporate network, with many of the tools and services provided by *Novell*'s other server platform, *NetWare*, ported across to *SUSE*-based systems.

The positioning of *SUSE* in the heart of the enterprise brings us to the basis of this comparative review. The old chestnut about *Linux* users not needing protection from malware doesn't cut it at the enterprise level, where file servers store and share data across networks dominated by more vulnerable *Windows* systems at the desktop level, serve up websites and process email for users around the world. More powerful server systems are a crucial layer of defence against infection, with on-access protection preventing uploading of dangerous files and scheduled scanning out of hours allowing more in-depth checking of shared data.

Installing *SUSE* has, for some time, been a simple and painless process, with a clearly designed GUI leading the user gently by the hand through the partitioning of drives and selection of software. The YAST management system, and its offspring, the YOU updater, provide similarly easy-on-the-brain methods of organising things, while the more technically minded can always get their hands dirty tinkering with config files and the like.

With the base systems set up and sharing some drive space via *Samba*, the other piece of software I expected to make extensive use of was the open-source *Dazuko* driver, developed by *Avira* and adopted by many other products for their file-hooking needs. With the kernel sources and other requirements in place, *Dazuko* proved easy and speedy to put in place, and the systems were imaged with a version precompiled as a kernel module and ready to insert at will.

TEST SETS

The latest WildList available at the deadline set for this test (1 March) was the December list, released in mid-February. Of the fair number of new samples added since the previous test, there were few surprises.

Another large swathe of W32/Stration variants joined their relatives in the set, along with a few more W32/Sdbot, W32/Bagle, W32/Feebs and W32/Areses. There were fewer than the usual number of W32/Mytob and W32/Rbot variants, a single nasty W32/Rontokbro, and a couple of new names offering pretty similar functionality. Beyond the worms, there were also a handful of W32/Looked variants, which vary between voracious infectors of just about anything they can find and more choosy types.

On-access tests	ItW		File infector		Macro		Polymorphic		Worms & bots		DOS		Linux		Clean set	
	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	False positives	Susp.
Alwil avast!	0	100.00%	13	98.18%	18	99.56%	301	79.98%	1	99.57%	246	99.32%	8	83.33%		4
Avira Antivir	0	100.00%	0	100.00%	0	100.00%	3	98.72%	0	100.00%	32	99.78%	3	86.67%		
CA eTrust	0	100.00%	3	99.33%	12	99.82%	20	92.15%	0	100.00%	367	99.57%	12	53.33%	3	
CAT Quick Heal	0	100.00%	22	96.28%	73	98.23%	370	76.21%	0	100.00%	1120	90.75%	7	60.00%		
Doctor Web Dr.Web	3	99.64%	3	98.72%	19	99.61%	9	96.15%	6	98.70%	0	100.00%	4	76.67%		2
ESET NOD32 for Linux Server	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	32	99.78%	0	100.00%	1	
Frisk F-Prot Anti-Virus	15	99.88%	0	100.00%	0	100.00%	0	100.00%	1	99.57%	0	100.00%	0	100.00%		
F-Secure Linux Server Security	0	100.00%	3	98.72%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	5	73.33%		2
Grisoft AVG	0	100.00%	17	96.13%	0	100.00%	190	75.64%	2	99.42%	663	97.33%	7	65.00%		1
Kaspersky Anti-Virus for Linux	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
McAfee LinuxShield	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	64	99.85%	0	100.00%		3
Microworld eScan AntiVirus for Linux File Servers	2	99.76%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	2	
Norman Virus Control	0	100.00%	11	98.46%	0	100.00%	217	85.53%	0	100.00%	118	99.74%	6	66.67%		
Sophos Anti-Virus for Linux	0	100.00%	12	97.95%	0	100.00%	0	100.00%	0	100.00%	2	99.78%	7	71.67%		
Symantec AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	5	99.97%	0	100.00%		
VirusBuster VirusBuster for Linux	0	100.00%	11	97.95%	3	99.93%	98	87.64%	0	100.00%	142	99.32%	9	66.67%		

In the other sets, the gradual revamping of the layout has seen a fairly major step this month. To link up with last time's rebranding of the 'standard' set as 'file infectors' to better reflect its contents, a new set of worms and bots has been added, populated so far with a selection of nasties removed from the old set and a few more recent additions. It is expected that this set will see a steady enlargement as samples of these common threats are acquired and added.

A second set also makes its first appearance this time, although with less up-to-the minute contents. Responding to recommendations that the many DOS samples in our test sets be removed (being of only minor significance these days), a sizeable chunk of these older threats have been plucked from their long-term positions. Abandoning them completely seemed a little extreme however, and would surely deny avid readers the valuable reflection of the in-depth strength of products – so they have been placed in a new set of their own, with a handful of additions thrown in to make good use of some stock waiting to be introduced. The decision to keep the DOS threats was justified by the reappearance, for the first time in many months, of DOS malware in last month's *VB* prevalence table – in very small numbers but from two separate data providers, indicating that some people at least are still exposing themselves and their precious data to these aged dangers.

As usual, the main bulk of the tests were carried out using the products' default settings. However, since some products ignore certain file types in their default settings, where possible, the archive speed tests were performed with archive scanning switched on (although, regrettably such an option was not always available, or at least not easily found). The aim was to compare like with like, and since the concept of 'default settings' is less clear with these predominantly command-line driven products, which expect plenty of qualifiers to tell them what to do, it seemed fair to tweak the settings upward rather than down, for those that needed it.

As a reflection of the increasing speed and capacity of modern hardware and scanning software, on-demand test results are presented this month in megabytes per second. In a further tweak to the presentation of figures, the on-access 'slowdown' figures are now calculated as the lag time added when accessing files. As the measurement is that of the time taken simply to open a file, and does not pretend to represent the overall system-wide effect of on-access protection, it is hoped that presenting the results in this way will provide a more useful indication of a product's overhead. Of course, any criticisms or suggestions regarding the data gathered and presented in these reviews is welcome (email john.hawes@virusbtn.com).

As a final nod to this month's specialist platform, *VB*'s set of *Linux* malware was revived, and alongside a few additions to the false positive set sits a batch of *Linux* files to add to the speed figures, the contents of the /bin, /sbin, /opt and a few other pivotal locations having been copied onto the scanning share. The on-access speed results for this special test set are a little problematic, as such files are

unlikely to be accessed from *Windows* clients in this way, and the large number of very small files results in a far greater scanning overhead relative to the size of the set. To allow the other data to be presented more clearly, the graph for this speed test is presented separately.

With all preparations completed, it was time for testing to commence.

Alwil avast! 4 v. 3.0.1

ItW	100.00%	**Macro**	99.56%
ItW (o/a)	100.00%	**Polymorphic**	79.98%
File infector	98.95%	**Worms & bots**	99.57%
DOS	99.32%	**Linux**	83.33%

Alwil provides its product in the form of rpm installers or more simple gzipped sets of files. I used the rpm method without problem, although this left me somewhat at a loss as to where the files had installed themselves. A brief search located them, with some simple documentation describing the use of the command-line scanner and the implementation of the *Dazuko*-based on-access component.

After a quick look through the usage guide, scanning was straightforward to implement, and detections zipped up the terminal window at an impressive pace.

Implementation of the on-access scanner failed silently at first, with no warning given that *Dazuko* needed to be inserted manually, but once up it seemed reliable and set a pleasing pace. Detection in both modes was reasonably thorough, with none of the new additions appearing among the smattering of misses.

The default setting for processing archive files, however, seemed to balk at anything too large or too deeply nested – to the extent of suggesting that several corrupted files could be 'decompression bombs'. Apart from this, a 'joke' program also found in the clean set was the only other issue, and with better results in the WildList set than in some of the more obscure collections, the product earns a VB100 award.

Avira AntiVir 2.1.9-37

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Polymorphic**	98.72%
File infector	100.00%	**Worms & bots**	100.00%
DOS	99.78%	**Linux**	100.00%

Not surprisingly, as its original developer, *Avira* also makes use of *Dazuko* in on-access mode. *Antivir* comes as an rpm, with a post-install configuration script to guide the user through the basic selection of settings. These include a request for the location of a ready-compiled *Dazuko* module, which is made use of when required.

Like most of the *Dazuko*-based products, on-access scanning is set on selected directories, rather than provided on the machine as a whole with exclusions needed for secure or sensitive locations, and these settings are adjusted in a configuration file.

Antivir also includes a graphical interface, which required a Java environment. Once this hurdle was overcome, the GUI proved pretty sophisticated, providing a thorough range of configuration options and scanning power, although on-access scanning could not be activated or switched off from here. There is also a rather clever graphical display of how many files have been 'guarded'.

The testing was carried out from the command line, a utility provided with a broad range of options; I was a little thrown at first until I realised that scanning did not recurse into subdirectories by default, but everything else was clear, and logging was laid out very simply and logically.

Scanning speeds were excellent, and only one particularly tricky member of the new set of DOS samples brought detection figures below 100%. With a full house of WildList detections, and no false positives, *Antivir* earns itself another VB100 award.

CA eTrust r.8.1.5310

ItW	100.00%	**Macro**	99.82%
ItW (o/a)	100.00%	**Polymorphic**	92.15%
File infector	99.85%	**Worms & bots**	100.00%
DOS	99.57%	**Linux**	80.00%

CA's product was the first to stray from the path of *Dazuko* and break its own ground for on-access scanning. It was also the first with rather grander pretensions, eschewing the simplicity of the command line and the config file for a system integrating with its cross-platform, centrally managed ITM system. Anticipating the benefits of familiarity, I was somewhat disappointed to find myself struggling with a rather tricky system.

The submission came in the form of the full contents of the distribution CD for *Linux*, UNIX and *NetWare* products. Browsing to the *Linux* section, I found an install script which, after making it executable and running it, took me through a sizeable installation process (including several EULAs which required scrolling all the way through before they could be accepted). Options for install locations etc. were run through, and the installation took place – a fairly

On-demand tests	ItW		File infector		Macro		Polymorphic		Worms & bots		DOS		Linux		Clean set	
	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	False positives	Susp.
Alwil avast!	0	100.00%	12	98.95%	18	99.56%	301	79.98%	1	99.57%	246	99.32%	8	83.33%		4
Avira Antivir	0	100.00%	0	100.00%	0	100.00%	3	98.72%	0	100.00%	32	99.78%	0	100.00%		
CA eTrust	0	100.00%	1	99.85%	12	99.82%	20	92.15%	0	100.00%	367	99.57%	8	80.00%	3	
CAT Quick Heal	0	100.00%	20	96.79%	73	98.23%	370	76.21%	0	100.00%	1120	90.75%	7	60.00%		
Doctor Web Dr.Web	3	99.64%	3	98.72%	19	99.61%	9	96.15%	6	98.70%	0	100.00%	4	76.67%		3
ESET NOD32 for Linux Server	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	32	99.78%	0	100.00%	1	
Frisk F-Prot Anti-Virus	15	99.88%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
F-Secure Linux Server Security	0	100.00%	3	98.72%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	5	73.33%		2
Grisoft AVG	0	100.00%	0	100.00%	0	100.00%	190	75.64%	2	99.42%	663	97.33%	7	65.00%		1
Kaspersky Anti-Virus for Linux	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
McAfee LinuxShield	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	64	99.85%	0	100.00%		3
Microworld eScan AntiVirus for Linux File Servers	2	99.76%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	2	
Norman Virus Control	0	100.00%	9	98.97%	0	100.00%	217	85.53%	0	100.00%	0	100.00%	0	100.00%		
Sophos Anti-Virus for Linux	0	100.00%	12	97.95%	0	100.00%	0	100.00%	0	100.00%	2	99.78%	7	71.67%		
Symantec AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	5	99.97%	0	100.00%		
VirusBuster VirusBuster for Linux	0	100.00%	8	99.23%	0	100.00%	98	87.64%	0	100.00%	142	99.32%	5	86.67%		

lengthy process. Browsing through the area mentioned in the installer, I found a command-line interface, which seemed inoperative, complaining about missing libraries. Checking the manual, I found much information on the centralised management utility, how to control vast networks of systems, but little on accessing any kind of client-end tools (although the broken command-line scanner was mentioned in passing).

I managed to find the ITM manager, a complex and bewildering thing, by checking some config files for the right port to point my browser at. I was able to sort out my on-access needs from there, but on-demand scanning seemed only to be available as scheduled scans – unsuitable for my speed test needs.

On contacting the product's creators, I was given the secret access point for the client end, which was familiar from previous tests on other platforms, and I managed to perform some more tests from here. Also familiar was the progress bar which dragged along each time a button was clicked, and I soon grew tired of it. I eventually found the missing libraries, enabling the command-line scanner and running the speed tests much more efficiently (and fairly) from there.

All tests recorded a good solid level of detection, and highly impressive speeds. In the clean set, however, something of an upset occurred, with no less than three files alerted on, all apparently infected with 'Antipas.653'. This was enough to deny *CA* a VB100 this time around, rendering all my struggles somehow all the more futile.

CAT Quick Heal 2007 v.9

ItW	100.00%	**Macro**	98.23%
ItW (o/a)	100.00%	**Polymorphic**	76.21%
File infector	96.79%	**Worms & bots**	100.00%
DOS	90.75%	**Linux**	60.00%

Quick Heal offered a pleasant return to the more simple side of things, and to *Dazuko*. Installation took the form of a simple zip file, with an install script within. This shepherded me through the setup process comfortably, and left me in no doubt as to how to go about running things. There is even a GUI, this time QT-based and requiring no further software to power it, providing clear and basic access to configuration and scanning.

There seemed to be few options regarding the on-access side of things, however, beyond the most basic on and off settings. As a result, *Quick Heal*'s on-access times are excluded from the archive table, which endeavours to compare like with like by running all products with archive scanning enabled, where possible. Nevertheless, decent speeds and reasonable detection were combined with a lack of false positives and exemplary coverage of the WildList set, thus qualifying *Quick Heal* for a VB100 award.

Doctor Web Dr.Web 4.33

ItW	99.64%	**Macro**	99.61%
ItW (o/a)	99.64%	**Polymorphic**	96.15%
File infector	98.72%	**Worms & bots**	98.70%
DOS	100.00%	**Linux**	76.67%

From a single file to many; *Dr.Web*'s installation was a rather more complex process, with several rpms provided to install the various components. Fortunately, a simple manual, as well as some tips from the developers, led me through the process of setting up the various daemons, scanners, another straightforward GUI, and the *Samba* integration. This was, it emerged, the first of several products to make use of the VFS functionality added to *Samba* in recent years to allow for file hooking, with a simple entry in the *Samba* configuration file directing all requests to the application of one's choice.

At this point the manual became less than helpful, the English version at least not having kept up with the latest increments to *Samba*; a table, matching up the pile of drivers provided by *Dr.Web* with the appropriate *Samba* versions, didn't include the version I had on my bare *SUSE* install. However, a little trial and error and the consultation of some logs soon had things moving.

The GUI was little help here, focusing mainly on the on-demand end, and as little control of logging was provided from here either, I stuck with the more fine-tunable command line for much of the testing.

On demand, speeds were a little less zippy than the previous few, and on access this was exaggerated, with the connection dropping occasionally and my file-opening utility reporting many files not opened. Running several retries and checking through the logs showed that none of these errors had been due to a false positive, although a couple of items were labelled as undesirable and another as adware.

More seriously, however, three separate variants of W32/Sdbot were missed from the WildList set, thus spoiling *Dr.Web*'s chances of a VB100 award.

ESET NOD32 for Linux Server 2.70.4

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Polymorphic**	100.00%
File infector	100.00%	**Worms & bots**	100.00%
DOS	99.78%	**Linux**	100.00%

Installation of *NOD32* was pleasingly well-designed, with an install script which made sense, and set things up just so. I barely even needed the simple instructions provided along with the product submission.

Once set up, the overall user experience was equally well thought out. While many of the other products in this review dropped their components into obscure locations with convoluted and unpredictable filenames, here I speculatively typed 'nod32' and got a nice polite response, urging me to provide some more specific options, while a standard –h call gave lucid and detailed information on usage.

Similarly, the on-access component was controlled by a proper init script in the standard location, responding to the standard instructions. *NOD32* was another product using *Dazuko* for its file hooking, and like the others in this class the on-access component was simple to set up, fast and efficient. The speeds recorded were even more eyebrow-lifting than usual, with the screen a blur of detections.

Sadly for *ESET*, my usual pleasure in using their product was marred, initially in a very minor way by missing one of the added sets of DOS samples (a strangely appropriate 32 samples, in fact), which spoiled a flawless record held by the product for some time now. More seriously, a false positive was generated in the older part of the clean set, caused by an apparently accidental upward tweak to the heuristics settings for DOS files in this build of the *Linux* product. Although the use of 'probably' in the log alert made the decision less than straightforward, rescanning the clean set with auto-deletion switched on resulted in the loss of the file in question, and combined with the commonness of 'probably' detections in *ESET*'s heuristic-heavy product, this was adjudged too severe to be classed as a mere 'suspicious file', resulting in *NOD32*'s first failure to achieve the VB100 for five years – its last having been the last time *VB* conducted tests on *SuSE Linux* in 2002 (see *VB*, April 2002, p.16).

Frisk F-Prot Anti-Virus 6.2.0

ItW	99.88%	**Macro**	100.00%
ItW (o/a)	99.88%	**Polymorphic**	100.00%
File infector	100.00%	**Worms & bots**	100.00%
DOS	100.00%	**Linux**	100.00%

F-Prot was another nice, simple product, with its files simply unzipped into /opt. *Dazuko* was again required for on-access scanning, although the absence of the module was not alerted on when running the product. Again, everything was simply configured via config files and scanning run from a pared-down command-line interface.

Speeds were fairly reasonable, and detection thorough almost across the board; unfortunately for *FRISK*, that thoroughness did not extend quite far enough, with one of the new variants of W32/Looked missed entirely while scanning the WildList set. The absence of any false positives more significant than the labelling of a *Sysinternals* tool as

On-demand throughput	Executables and system files		Media and documents		Linux		Other file types		Archive files	
	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)
Alwil avast!	147	11.07	24	51.89	86	9.40	24	0.57	32	22.96
Avira Antivir	83	19.57	21	57.20	61	13.15	13	1.00	87	8.41
CA eTrust	79	20.58	25	49.39	76	10.54	20	0.68	161	4.56
CAT Quick Heal	94	17.26	584	2.09	626	1.29	23	0.59	219	3.35
Doctor Web Dr.Web	259	6.27	267	4.57	308	2.61	68	0.20	342	2.15
ESET NOD32 for Linux Server	124	13.11	23	52.34	69	11.60	17	0.79	63	11.64
Frisk F-Prot Anti-Virus	158	10.25	37	33.29	33	24.30	12	1.09	76	9.60
F-Secure Linux Server Security	278	5.83	223	5.46	251	3.20	40	0.33	487	1.51
Grisoft AVG	163	9.97	35	34.77	144	5.59	17	0.79	159	4.62
Kaspersky Anti-Virus for Linux	229	7.10	154	7.93	243	3.31	25	0.53	454	1.62
McAfee LinuxShield	232	7.00	48	25.59	148	5.44	24	0.55	248	2.96
Microworld eScan AntiVirus for Linux File Servers	206	7.88	176	6.95	234	3.44	26	0.52	464	1.58
Norman Virus Control	909	1.78	24	50.96	218	3.68	41	0.32	135	5.43
Sophos Anti-Virus for Linux	97	16.74	26	47.24	57	14.03	10	1.40	93	7.91
Symantec AntiVirus	113	14.36	22	55.47	106	7.59	16	0.84	33	22.24
VirusBuster VirusBuster Scanner for Linux	166	9.76	94	13.00	139	5.80	23	0.59	70	10.52

undesirable could not redeem *F-prot* sufficiently to achieve a VB100 award.

F-Secure Linux Server Security 5.50

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Polymorphic**	100.00%
File infector	98.72%	**Worms & bots**	100.00%
DOS	100.00%	**Linux**	73.33%

F-Secure's product had a more professional feel than many, with some serious and thorough documentation. Installation took the form of a zip and an install script, featuring a selection of languages, EULA and licence code acquisition. There is also a web interface, which was typically crisp and austere, although some rather small fonts proved a little painful on the eye at the resolution setting I was using.

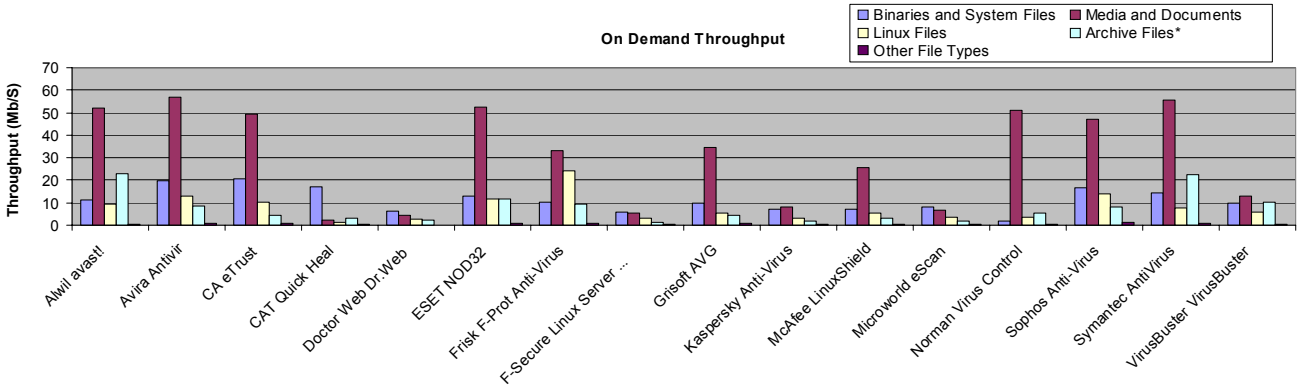
The command line was used for most testing, to ensure fairness in comparison with other products in the speed tests. However, speeds were not impressive, particularly once archive scanning was enabled on-access for the archive speed set. Viewing the logs showed that this could, in part, be due to the double scanning of all files, even once a detection is found, which would also account for the superb detection rates.

The only files the product missed were in archive types ignored by default (with some justification), and the alerts generated on two files in the clean set presented no challenge to *F-Secure*'s entitlement to a VB100 award – while one, the same *Sysinternals* pstools kit alerted on by many products, was described as a 'risktool', the other, an IRC client from *Microsoft*, was labelled, quite accurately, an IRC client.

Grisoft AVG 7.5

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Polymorphic**	75.64%
File infector	100.00%	**Worms & bots**	99.42%
DOS	97.33%	**Linux**	65.00%

AVG was another rpm-based installer, following which came a registration step with a special tool provided for applying a licence. A GUI is apparently available, although it was not included with the submission for testing. The command line proved more than adequate for my testing however, offering a nice, straightforward set of options, and the various scans were carried out



without difficulty. Scanning speeds were good, and detection was fairly decent too, with a few large sets missed in the DOS collection and a few in the polymorphic set.

Nothing was missed in the WildList set, although yet another undesirable item was spotted in the clean set, this time described as a 'Hacktool' (in fact, something designed to block advertising from an instant messaging client which has recently had some problems with serving up malware via its advertising system, which may be a bit of a hack but is also arguably a security benefit). However, this did nothing to spoil *Grisoft*'s chance of gaining another VB100 award.

Kaspersky Anti-Virus for Linux 5.5.9

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Polymorphic**	100.00%
File infector	100.00%	**Worms & bots**	100.00%
DOS	100.00%	**Linux**	100.00%

With *Kaspersky* we move away from *Dazuko* once more and into the murky world of *Samba* VFS objects, which have so far proved somewhat problematic.

The product was provided as an rpm, with an install script to run afterward for initial setup. In fact, a range of Perl scripts were provided for the configuration, including inserting appropriate entries into the *Samba* configuration file to operate the on-access side of things. Controlling the product from another browser-based GUI was apparently also possible, but as this required some third-party software to support it, it was not examined.

The command line once again proved more than adequate, with some rather off-the-wall syntax quickly mastered. On access, my fears about the use of the VFS functionality proved unfounded, with scanning as thorough and dependable as it was on demand.

Speeds were not electric – perhaps in part due to some vigorous attention to all manner of archive files – but detection was superb, with *Kaspersky* achieving the first unblemished record of the month. Not even a whisper of suspicion was raised in the clean set, with the only problem provided by a particularly large self-extractor, at which the product complained gracefully of an error while scanning. *Kaspersky*'s VB100 award is thus thoroughly deserved.

McAfee LinuxShield 1.4.0

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Polymorphic**	100.00%
File infector	100.00%	**Worms & bots**	100.00%
DOS	99.85%	**Linux**	100.00%

After my struggles with *CA*'s product, I feared a similar experience with another large, multi-faceted corporate-oriented product. This time around things were a little less troublesome.

A lengthy interrogation following the initial install demanded login details to access the obligatory web interface, and discussed web and mail filtering as well as file-based anti-malware. The web interface itself seemed fairly clear and comprehensive, but the fact that the page did not refresh proved to be confusing occasionally, leaving me clicking back and forth around the thing trying to discover if a task had completed. The updater task, achieved in my offline state by pointing a browse box at the location where the data was placed, seemed unable to spot the dat files, and in the end I resorted to dropping them in manually, which proved much more effective.

Scanning, carried out in part via the command line, involved setting up scanning tasks in the GUI, and then running them from the shell. The resulting speeds were possibly less impressive than a straightforward command-line scan might offer, but detection figures were

File access time lag	Executables and system files		Media and documents		Linux		Other file types		Archive files	
	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)
Alwil avast!	529	0.32	164	29.60	264	48.40	403	74.38	85	14.89
Avira Antivir	113	0.06	27	4.09	202	36.83	28	4.20	93	16.33
CA eTrust	248	0.14	37	5.85	280	51.27	24	3.44	90	15.83
CAT Quick Heal	109	0.06	37	5.95	1319	245.57	31	4.75	(NA)	(NA)
Doctor Web Dr.Web	325	0.19	276	50.70	752	139.59	84	14.65	283	51.91
ESET NOD32 for Linux Server	123	0.07	28	4.20	250	45.78	23	3.34	61	10.50
Frisk F-Prot Anti-Virus	257	0.15	59	10.03	177	32.04	22	3.04	137	24.58
F-Secure Linux Server Security	204	0.12	41	6.61	428	79.08	35	5.48	452	83.46
Grisoft AVG	163	0.09	45	7.47	427	78.84	30	4.69	215	39.21
Kaspersky Anti-Virus for Linux	249	0.14	157	28.45	482	89.13	32	4.91	364	67.06
McAfee LinuxShield	284	0.17	68	11.78	347	63.91	39	6.38	143	25.77
Microworld eScan AntiVirus for Linux File Servers	(NA)	(NA)	(NA)	(NA)	(NA)	(NA)	(NA)	(NA)	(NA)	(NA)
Norman Virus Control	303	0.18	96	16.88	1252	233.13	98	17.35	(NA)	(NA)
Sophos Anti-Virus for Linux	160	0.09	44	7.19	294	53.97	30	4.64	144	25.90
Symantec AntiVirus	150	0.08	31	4.85	269	49.38	23	3.28	39	6.33
VirusBuster VirusBuster Scanner for Linux	808	0.49	79	13.71	2620	489.01	220	37.62	28	4.24

very good, with the only misses in the DOS set, mostly in the new batches.

With nothing from the more 20th-century sets missed, and certainly nothing in the WildList, *McAfee*'s handful of messages warning me about items I may not want in my corporate network do nothing to jeopardise its VB100 award.

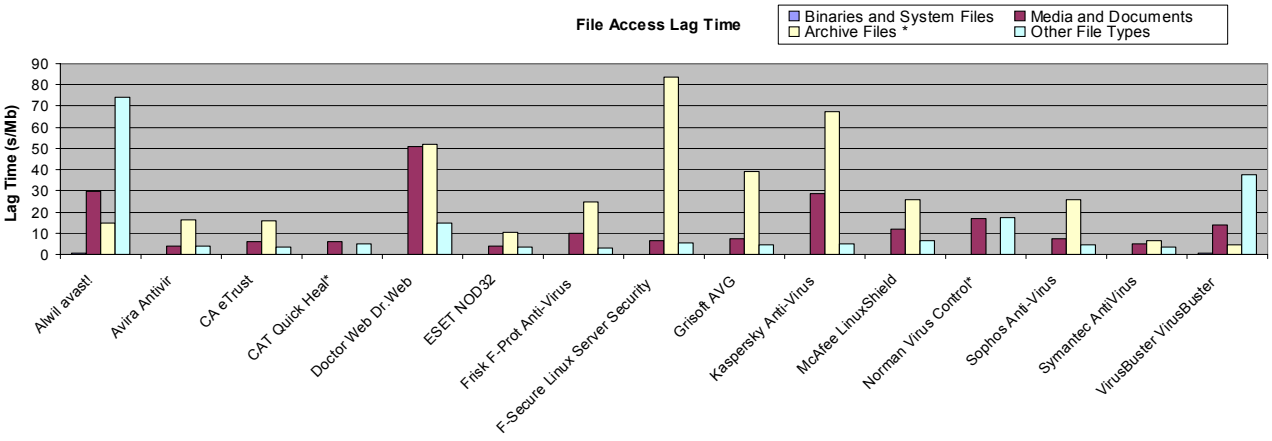
Microworld eScan AntiVirus for Linux File Servers 2.0.11

ItW	99.76%	**Macro**	100.00%
ItW (o/a)	99.76%	**Polymorphic**	100.00%
File infector	100.00%	**Worms & bots**	100.00%
DOS	100.00%	**Linux**	100.00%

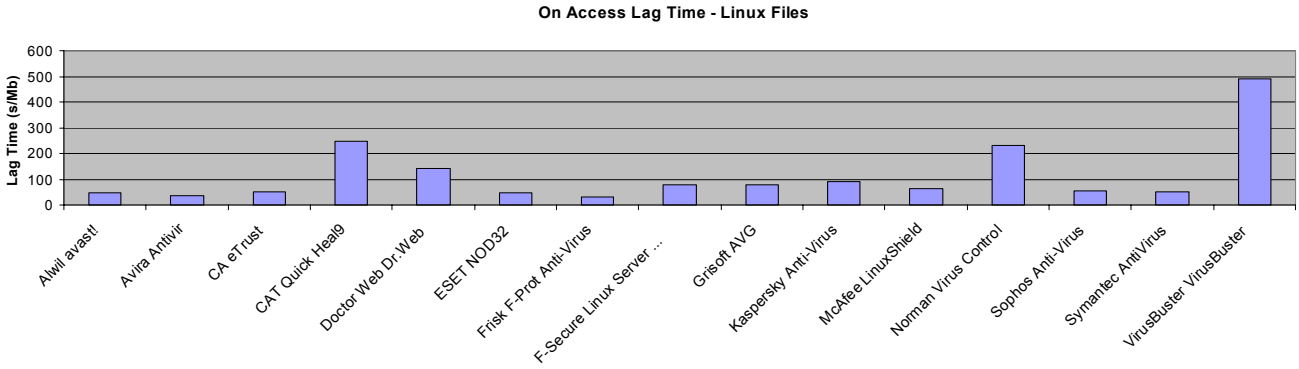
Microworld's product arrived as a swathe of rpms, along with strict instructions as to the order in which they should be installed. While most installed without problems, the web interface section got stuck several times looking for missing files; these I soon diagnosed as pointing to specific versions of items rather than the bare .so filenames, and some symlinking soon got it into a somewhat hacked state of running. An errant line regarding logging in one of the product's own config files also brought things to a halt, but I divined that commenting this out would cause no significant problem.

On-demand scans were carried out without further ado, although defaulting to disinfecting or quarantining infected files caused a moment of teeth-gnashing. Having assumed that my rather inelegant bullying of the web interface into operation would have little effect on my testing, I discovered that I did indeed require the GUI, as the documentation lacked detail on the syntax of the config files for some aspects of the product, notably the on-access scanner. This was once more a *Samba* VFS implementation, requiring several lines to be added to the *Samba* config, and once it was up and running I quickly saw that some scanning of files on access was indeed happening. Satisfied that scanning was in progress, I wandered off for refreshment, leaving it to chug slowly along through the first of the speed file sets.

Returning some time later, I was surprised to see it still going. Watching more closely, I noted frequent long periods of inactivity, with no files accessed at all. Running the scanner over the infected set was even more painful – despite having switched off the 'alert me when something is detected' option, a popup appeared in the *Windows* client for each detection, along with a warning 'ping' noise. Investigating the syslog, I found numerous complaints of a failure to



*May not be default setting.
Note: no archive scannng times available for CAT & Norman products.



quarantine files, with a message suggesting there might be a problem with access rights to the quarantine folder. However, checking the rights and expanding them proved no help here.

Looking further into the beleaguered *Linux* system, I found ever larger numbers of *Samba* daemons were being spawned, along with accompanying copies of the *eScan* daemon, presumably each time the scanning hit a snag.

With careful coaxing and splitting into chunks, I nursed the product through the collection, achieving some decent results over the full range of test sets, but unfortunately I had neither the time nor the patience to sit through the full range of speed tests. Before anyone complains that this gives an unfair advantage in terms of the chances of scoring false positives, I should say that the product had already lost its chance of a VB100 award, as both on access and on demand those pesky pstools and MIRC files were spotted and labelled clearly as viruses, which was enough to deny the product its prize.

But even had these unfortunate misnomers not been applied, the missing of two samples of W32/Bagle, introduced in the November WildList, would have been reason enough to withhold the award.

Norman Virus Control 5.70.01

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Polymorphic**	85.53%
File infector	98.97%	**Worms & bots**	100.00%
DOS	100.00%	**Linux**	100.00%

Norman's product came as another simple .tgz file, with a post-install script tucked away inside to set things up for me. After some initial tinkering, and the discovery that cleaning of files was the default, I soon had the on-demand detection and speed tests out of the way.

Unfortunately, configuration of the on-access files seemed to be via some config files in an obscure format. To continue, I required another interface, this time back to Java. Once this was in place, I was able to access a fairly simple, minimalist GUI, operating the configuration

controls only with no ability to run scans itself. It provided ample controls to get through the rest of the tests, although there was apparently no option to enable archive scanning on demand, thus upsetting my plan to include only on-access speed data in this mode. Despite this minor setback, *NVC* was generally easy to use and achieved decent levels of detection, with no false positives and spotting everything in the WildList set, thus comfortably winning a VB100 award.

Sophos Anti-Virus for Linux 5.70.1

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Polymorphic**	100.00%
File infector	97.95%	**Worms & bots**	100.00%
DOS	99.78%	**Linux**	71.67%

Sophos's *Linux* product uses its own alternative file-hooking system, released like *Dazuko* under an open-source licence. The product arrives as a .tgz file, with an installer inside, which checks the kernel version against a list of prepared builds of the driver. Apparently unsupported kernels are provided for by an on-the-fly compilation process built into the installer, but the SLES10 kernel was among those provided for in advance and installation proceeded without difficulty.

The browser-based interface proved pleasantly straightforward, simply laid out and responsive. For on-demand scanning the command line was used. Updating required implanting a large number of small identity files, which are then listed at the start of each command-line scan, and described in more detail when requesting version information, which required a considerable amount of scrolling up the screen to check the numbers, and may have added somewhat to the time taken to get each scan going.

Nevertheless, speeds were excellent, and detection impressive too, with a smattering of misses mostly due to archive scanning not being a default setting. *Sophos* also earns a shiny VB100.

Symantec AntiVirus for Linux 1.0.1.66

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Polymorphic**	100.00%
File infector	100.00%	**Worms & bots**	100.00%
DOS	99.97%	**Linux**	100.00%

Having expected *Symantec* to sit alongside its global giant rivals with a sprawling corporate-network product, I was surprised to find the product's version number so low, suggesting an immaturity which made me nervous.

Installing the product was no major issue, with a handful of rpms to run. Once this was done, I was at something of a loss as to how to get anything done, even having dug out the associated binaries tucked away under /opt. Some problems with the updater provided – which proved to be the wrong one for the platform under test – were resolved eventually, and in the process of installing and trawling the documentation for advice, I gradually picked up an idea of how things worked.

A central daemon supplies the scanning, with requests for on-demand scans passed into it through a tool which is also used to manage updating and checking up on the on-access part. Once scans are initiated, results are available only in the system log, although if the rather basic GUI (requiring Java) is running, detection reports are flashed on screen too.

The process of changing the configuration of scans, and of the on-access scanner, involves another tool which passes settings into the daemon's config database – not a simple config file but a binary file modelled on, of all things, the *Windows* registry. Indeed, at one point the manual seemed to suggest that the easiest way to set up the desired configuration would be to install a *Symantec* product on a *Windows* system, save the settings from there and export them to the *Linux* setup.

I eventually learned how to deactivate automatic disinfection, a process requiring two separate commands of over 150 characters each just for the on-access scanner, and chugged through the tests relying on the times recorded in the syslog for my on-demand speed results. In the end, very little was missed, and speeds were more than respectable, but would have been much slower had I included the time I spent puzzling over the control system. With no misses in the Wild, and no false positives, *Symantec* also earns a VB100 award.

VirusBuster VirusBuster Scanner 1.3.4/ SambaShield 1.1.3-2 for Linux

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Polymorphic**	87.64%
File infector	99.23%	**Worms & bots**	100.00%
DOS	99.32%	**Linux**	86.67%

VirusBuster's product comes in two separate modules, one for the on-demand scanner and another to provide on-access protection. The on-demand scanner was pretty basic: a bunch of files in a .tgz file, with updates simply dropped in on top of the existing files. Running from the command line brought up a warning

that the product was unlicensed, so I entered the code provided, assuming that this would be stored somewhere and not needed again. However, it turned out that the code had to be provided for every scan – I assume it could also be entered into a config file providing default scan settings.

Once this was figured out, scanning was no problem, although the logging was a little overzealous, recording everything so much as glanced at in the log file. When it came to the on-access portion, things got a little more fiddly, with several components installed to various places and some rather confusing information provided about how to set up one's *Samba* installation to redirect via another of those tricky VFS objects.

Once this was set up, a visit to my *Samba* share showed two lonely files, in English and Hungarian, informing me rather comically that my scanner was unlicensed and access to my files would be denied until this was rectified. A quick search located a config file where the code info could be entered and stored, and the expected set of folders returned to view after a restart of the *Samba* daemon. Testing proceeded at a somewhat leisurely pace, but detection was thorough and false positives pleasingly absent, allowing *VirusBuster* to add another VB100 to its tally.

CONCLUSIONS

The last time *SUSE Linux* found itself on the VB100 test bench (see *VB*, April 2002, p.16) was memorable for several reasons. It was not merely the last time one of the VB100's most consistent performers failed to make the grade, it was in fact the last *VB* comparative in which not a single award was issued. At the time, on-access scanning for *Linux* was in its infancy. In the intervening years, considerable ground has been made up, with a diverse range of systems – proprietary, open-source and integrated with aspects of the operating system – allowing products to control access to infected files. *Dazuko* in particular has proved a popular and successful option, and the many products that make use of it seem to have done so with considerable success. Other methods are less mature, and seem to have caused difficulties for some, although none so disastrous as to spoil anyone's chances of gaining the coveted award.

On the whole, the products fell into a few broad categories, in terms of both usability and implementation. Those that made use of *Dazuko* tended to be simpler, with more basic installation systems and interfaces, though some did offer full installers. Those attempting to take advantage of *Samba*'s VFS system tended to be meatier products, with more complex configuration required, while the chunky corporate products integrating their own methods of file-hooking were generally the most bewildering to operate, attempting to combine *Linux* products into a cross-platform offering, with varying degrees of success. Almost all offered some degree of automated updating, and most also had a GUI of some sort. *Linux* tends to be the domain of more technically literate administrators, who may prefer the flexibility and simplicity of command-line driven products, but the market for products designed for the less experienced user, more comfortable with an attractive graphical interface, is almost certainly the fastest growing end; it seems a pity that so many of these interfaces add more rather than less complexity to the process of configuring and administering anti-virus.

However, representatives of both the most basic and the most complex types of product managed to pass the tests and to do well in terms of speed, and there were delights and horrors at either end of the scale. It seems in many cases that usability and aptness of design are a reflection of a general company ethos, as many that have caused me trouble in their *Windows* incarnations were equally pesky under *Linux*.

As far as detection goes, after several months in which missing WildList viruses has been quite a common occurrence, it seems it is the turn of the false positive to rear its ugly head once more. Several products failed due to false alarms, while the 'suspicious' label which has long been allowed under the VB100 methodology has become ever more popular.

As more products move beyond adware and spyware into detecting legitimate and often useful software which could be put to malicious ends, a new category of 'toolware' is forming – one which may even be worthy of its own subset in our test collection. This would, of course, be rather difficult to populate and to make any useful judgements about, with such diverse opinions of what should be included. As long as it is made clear that such things are risky rather than innately malevolent, products are free to point them out as they please under the rules of the VB100. One product failed to do so, labelling such items viruses and was penalised accordingly, while several others had false positives in other areas entirely. The false positives will of course, like missed viruses, all be resolved with the vendors, for the benefit of their users, as soon as possible.

Technical details

Test environment: Tests were run on identical machines with *AMD Athlon64* 3800+ dual core processors, 1GB RAM, 40GB and 200 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy drive, all running *Novell*'s *SUSE Linux Enterprise Server 10*. Clients for the on-access test ran *Microsoft Windows 100 Professional*, Service Pack 4, on 1.6 GHz *Intel Pentium* machines with 512 MB RAM and 20 GB dual hard disks.

Virus test sets: Complete listings of the test sets used can be found at http://www.virusbtn.com/Comparatives/Linux/2007/test_sets.html.

END NOTES & NEWS

HITBSecConf2007 - Dubai takes place 2–5 April 2007 in Dubai, UAE. The conference will include presentations by respected members of both the mainstream network security arena as well as the underground or black hat community. For details see http://conference.hackinthebox.org/.

Infosecurity Europe 2007 takes place 24–26 April 2007 in London, UK. Full details of the exhibitors, seminar programme and keynote presentations, as well as online registration, can be found at http://www.infosecurity.co.uk/.

RSA Conference 2007 Japan takes place 25–26 April 2007 in Tokyo, Japan. For more details see http://www.cmptech.jp/rsaconference/.

The 16th annual EICAR conference, originally to be held 5–8 May 2007, has been cancelled. See http://conference.eicar.org/.

DallasCon VI will take place 7–12 May 2007 in Dallas, TX, USA. Programme details and online registration are available at http://www.dallascon.com/.

The 22nd IFIP TC-11 International Information Security Conference takes place 14–16 May 2007 in Sandton, South Africa. For more details see http://www.sbs.co.za/ifipsec2007/.

The 4th Information Security Expo takes place 16–18 May 2007 in Tokyo, Japan. For more details see http://www.ist-expo.jp/en/.

The 8th National Information Security Conference (NISC 8) will be held 16–18 May 2007 at the Fairmont St Andrews, Scotland. For the conference agenda and a booking form see http://www.nisc.org.uk/.

The CISO Executive Summit & Roundtable takes place 6–8 June 2007 in Nice, France. The event will focus on how today's CISO can drive and integrate security into the very core of the business. For details see http://www.mistieurope.com/.

The 19th FIRST Global Computer Security Network conference takes place 17–22 June 2007 in Seville, Spain. For full details see http://www.first.org/conference/2007/.

IT Underground Dublin will be held 20–22 June 2007 in Dublin, Ireland. IT Underground will cover a wide range of security topics ranging from hacking techniques to OS hardening, reverse engineering, forensics and legal aspects of computer security. For details see http://www.itunderground.org/.

The Information Security Asia 2007 Conference & Exhibition takes place on 10 and 11 July 2007 in Bangkok, Thailand. For details see http://www.informationsecurityasia.com/.

The International Conference on Human Aspects of Information Security & Assurance will be held 10–12 July 2007 in Plymouth, UK. The conference will focus on information security issues that relate to people. For more details see http://www.haisa.org/.

Black Hat USA 2007 Briefings & Training takes place 28 July to 2 August 2007 in Las Vegas, NV, USA. Registration is now open. All paying delegates also receive free admission to the DEFCON 15 conference, which takes place 3–5 August, also in Las Vegas. See http://www.blackhat.com/.

HITBSecConf2007 - Malaysia will be held 3–6 September 2007 in Kuala Lumpur, Malaysia. A call for papers for the conference remains open until 1 May 2007. For more details see http://conference.hackinthebox.org/.

The 17th International VB Conference, VB2007, takes place 19–21 September 2007 in Vienna, Austria. Full details and online registration can be found at http://www.virusbtn.com/conference/.

COSAC 2007, the 14th International Computer Security Forum, will take place 23–27 September 2007 in Naas, Republic of Ireland. See http://www.cosac.net/.

RSA Conference Europe 2007 takes place 22–24 October 2007 in London, UK. See http://www.rsaconference.com/2007/europe/.

SUBSCRIPTION RATES

Subscription price for 1 year (12 issues):

- Single user: $175
- Corporate (turnover < $10 million): $500
- Corporate (turnover < $100 million): $1,000
- Corporate (turnover > $100 million): $2,000
- *Bona fide* charities and educational institutions: $175
- Public libraries and government organizations: $500

Corporate rates include a licence for intranet publication.

See http://www.virusbtn.com/virusbulletin/subscriptions/ for subscription terms and conditions.

Editorial enquiries, subscription enquiries, orders and payments:
Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England
Tel: +44 (0)1235 555139 Fax: +44 (0)1235 531889
Email: editorial@virusbtn.com Web: http://www.virusbtn.com/

vb Spam supplement

CONTENTS

NEWS & EVENTS

SCAMMERS LAUNCH ANTI-TERRORIST HOTLINE

Last month saw the appearance of the latest 419 scamming trick: 'anti-terrorist certificates' sold via a fake version of the London Metropolitan Police website complete with fake anti-terrorist hotline number.

The scam referred recipients to what appeared, to all intents and purposes, to be the official website of the London Met. To the untrained eye, the genuine and fake sites were almost impossible to tell apart (see http://momusings.com/momusings/2007/03/police-website-line-up-whos-imposter.html). However, the scammers' version of the site included a fake anti-terrorist hotline number.

According to 419-tracking organization Ultrascan Advanced Global Investigations, the scam directed victims to the fake website to purchase so-called 'anti-terrorist certificates', needed to secure payments from abroad.

The fake site, which was hosted in Australia, has now been closed down by the service provider. According to a spokesperson from the Met, the case has also been reported to Australia's High Tech Crime Unit for investigation.

PHISHING ATTACKS REACH NEW HIGH

Phishing attacks and password-stealing applications both reached record levels in January 2007 according to the latest report from the Anti-Phishing Working Group (APWG).

The APWG recorded 29,930 unique phishing reports in January 2007 – an increase of nearly 5% from the previous high, which had been recorded in June 2006.

A total of 135 brands were targeted in January – not a record number, but up nearly 35% on the same time last year. Few will be surprised to learn that financial services is still the industry sector most targeted by phishers, taking the brunt (88.9%) of the attacks recorded. However, the APWG noted an increase in the number of attacks against brokerage companies and international banks and brands, as well as an increase in the number of gambling and social networking sites targeted.

The US, China and Korea hold on to the top three spots in the league table of countries hosting phishing websites, while the top three countries hosting phishing-based keyloggers and trojan downloaders this time were the US, China and France.

Despite the fact that phishing is receiving increasing amounts of media coverage (which one would think would have raised the awareness of the general public to the threat), the phishing business shows little sign of waning. The subject of educating users about phishing will be one of the many subjects discussed at this year's *VB* conference (VB2007). David Harley and Andrew Lee will ask '*Phish phodder: is user education helping or hindering?*'. VB2007 takes place 19–21 September 2007 in Vienna, Austria. The full conference programme and online registration are available at http://www.virusbtn.com/conference/vb2007/.

EVENTS

The Authentication Summit 2007 will be held 18–19 April 2007 in Boston, MA, USA. See http://www.aotalliance.org/.

The EU Spam Symposium takes place 24–25 May 2007 in Vienna, Austria. See http://www.spamsymposium.eu/.

Inbox 2007 will be held 31 May to 1 June 2007 in San Jose, CA, USA. For more details see http://www.inboxevent.com/.

The 10th general meeting of the Messaging Anti-Abuse Working Group (MAAWG) will take place 5–7 June in Dublin, Ireland (members only) and a further meeting (open to both members and non-members) will be held 3–5 October in Washington D.C., USA. See http://www.maawg.org/.

CEAS 2007, the 4th Conference on Email and Anti-Spam, takes place 2–3 August 2007 in Mountain View, CA, USA. Full details can be found at http://www.ceas.cc/.

The Text Retrieval Conference (TREC) 2007 will be held 6–9 November 2007 at NIST in Gaithersburg, MD, USA. See http://plg.uwaterloo.ca/~gvcormac/spam.

FEATURE

AN AFRICAN A-F-F-AIR…

Martin Overton
Independent Researcher, UK

I last visited the topic of 419 scams in 2003 (see *VB*, May 2003, p.15), when I described what they are, how they work, and how they have developed over the years, from the original paper-based versions sent via the post or via fax, to what we have now: the email versions that most of us see day in, day out.

Just to refresh our minds, the following is a brief introduction:

419 scams combine the threat of impersonation fraud with a variation of an advance fee fraud (AFF) scheme. A letter or email (originally from Nigeria, but we see them coming from just about any country now), offers the recipient the opportunity to share in a percentage of millions of dollars in return for helping the author – often a self-proclaimed government official, doctor, engineer, bank official, religious minister etc. – transfer the money out of the country illegally. The victim is encouraged to send information to the author of the letter, such as blank letterhead stationery, their bank name and account details and other identifying information.

The scheme revolves around convincing a willing victim (who has demonstrated a 'propensity for larceny' by responding to the invitation) to send money to the author of the letter in several instalments of increasing value. Often, the scammers elicit these instalments from the victim by describing in great detail the requirement to pay taxes, bribes to government officials, and legal fees, with the promise that all expenses will be reimbursed as soon as the funds are spirited out of the country. Of course, the millions of dollars do not exist and the victim ends up with nothing.

Should the victim stop sending money, the perpetrators have been known to use the personal information they were sent to impersonate the victim, draining bank accounts and credit card balances until the victim's assets are exhausted.

Most law-abiding citizens identify the 419 emails/letters as hoaxes/scams. However, millions of dollars are transferred annually around the world as a result of these schemes.

The scheme violates section 419 of the Nigerian criminal code, hence the label '419 fraud', although the fraud is now common the world over.

This article will focus on the changes that have been seen in the 419 scam over the last few years. Although the basic formula has (in most cases) stayed the same, the scammers have changed their approach and style – as you will see, many are now highly polished and very inventive.

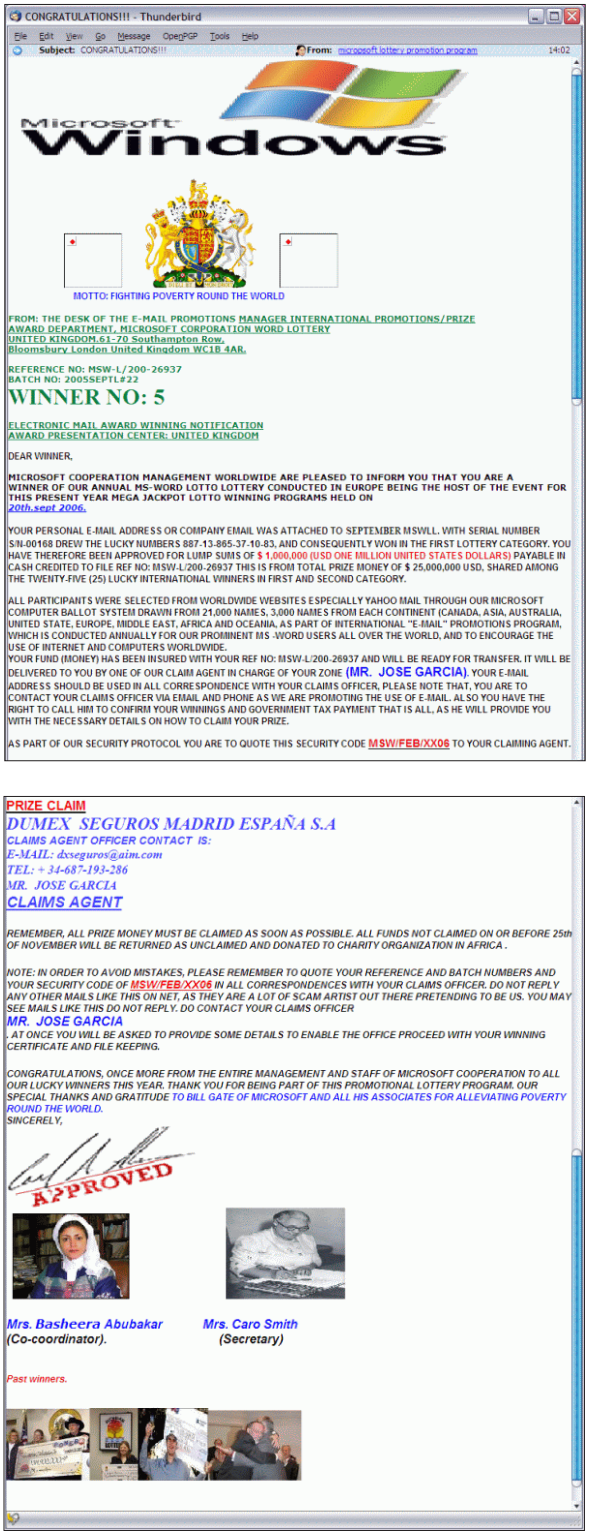


Figure 1: A typical Microsoft lottery 419 email.

LIFE IS A LOTTERY

In my last article on 419s, I mentioned that we were seeing a move towards versions of the scam that claim that you have won a lottery; one that you don't even remember entering, because you didn't.

Since then, the lottery variant of the 419 genus has flowered and borne much fruit. Some of these lottery scams are very well thought out and executed. The use of well-known company names and the names of wealthy individuals are commonplace, as is the use of HTML rendering and images such as logos and even 'borrowed' photographs of individuals who are not involved with these scams.

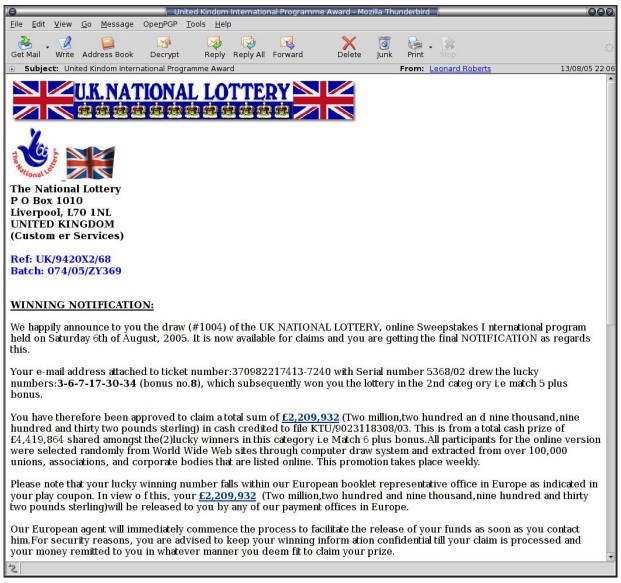
Figure 1 shows one of the many lottery variants of the 419 family. In this case, the name used to lend credence to the story is none other than *Microsoft*, and even Bill Gate[s] gets a mention. However, it is the following line in this particular variant that made me chuckle:

> 'DO NOT REPLY ANY OTHER MAILS LIKE THIS ON NET, AS THEY ARE LOT OF SCAM ARTIST OUT THERE PRETENDING TO BE US…'

Tell me about it, what a bunch of scammers!

As illustrated in Figure 2, the names and graphics of real lottery companies are often used to try to hook victims. I have seen variants of this particular trick for almost all of the major lottery companies throughout the world.

There are many other versions of lottery scams, some of which are simple ASCII text versions, while others are more polished, but they are all scams and people are still being tricked into believing they have won a non-existent prize.


United Kindom International Programme Award - Mozilla Thunderbird

File Edit View Go Message OpenPGP Tools Help

Get Mail Write Address Book Decrypt Reply Reply All Forward Delete Junk Print Stop

Subject: United Kindom International Programme Award From: Leonard Roberts 13/08/05 22:06

U.K. NATIONAL LOTTERY

The National Lottery
P O Box 1010
Liverpool, L70 1NL
UNITED KINGDOM
(Custom er Services)

Ref: UK/9420X2/68
Batch: 074/05/ZY369

WINNING NOTIFICATION:

We happily announce to you the draw (#1004) of the UK NATIONAL LOTTERY, online Sweepstakes I nternational program held on Saturday 6th of August, 2005. It is now available for claims and you are getting the final NOTIFICATION as regards this.

Your e-mail address attached to ticket number:370982217413-7240 with Serial number 5368/02 drew the lucky numbers:3-6-7-17-30-34 (bonus no.8), which subsequently won you the lottery in the 2nd categ ory i.e match 5 plus bonus.

You have therefore been approved to claim a total sum of £2,209,932 (Two million,two hundred an d nine thousand,nine hundred and thirty two pounds sterling) in cash credited to file KTU/60231183308/03. This is from a total cash prize of £4,419,864 shared amongst the(2)lucky winners in this category i.e Match 6 plus bonus. All participants for the online version were selected randomly from World Wide Web sites through computer draw system and extracted from over 100,000 unions, associations, and corporate bodies that are listed online. This promotion takes place weekly.

Please note that your lucky winning number falls within our European booklet representative office in Europe as indicated in your play coupon. In view o f this, your £2,209,932 (Two million,two hundred and nine thousand,nine hundred and thirty two pounds sterling)will be released to you by any of our payment offices in Europe.

Our European agent will immediately commence the process to facilitate the release of your funds as soon as you contact him.For security reasons, you are advised to keep your winning inform ation confidential till your claim is processed and your money remitted to you in whatever manner you deem fit to claim your prize.

Figure 2: A typical National Lottery 419 email.

EVERY CLOUD HAS A SILVER LINING

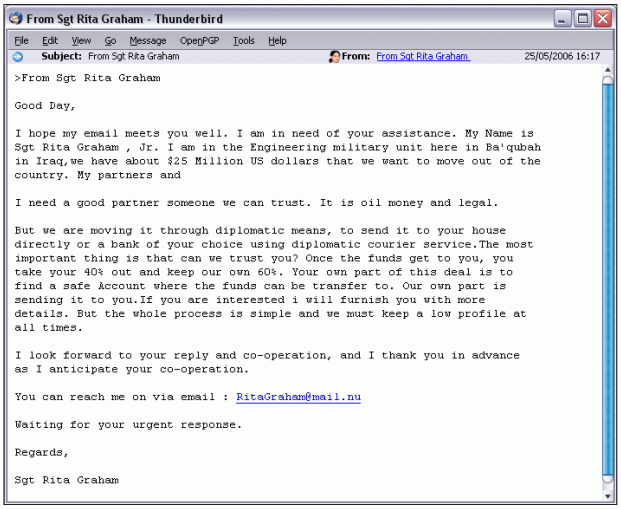
Below is a list of just some of the events/disasters that scammers have exploited to try to fleece good, honest people wanting to help the real victims of these tragic events:

- London bombings
- Asian tsunami
- Hurricane Katrina
- 9/11
- The situation in Iraq
- The situation in Iran
- The Israel and Lebanon conflict
- Air/car crashes

The 419ers are not alone in exploiting these tragic events, many phishers and malware authors also jumped on the bandwagon when the opportunity arose. The bad guys and girls just can't seem to resist using other people's misfortune to line their own pockets – in this instance at the expense of both the recipients of the scam and the victims of the relevant disaster.

SOLDIERS OF FORTUNE?

As mentioned above, I have seen a number of 419 scams that use the situation in Iraq as a basis for their stories. Those who have seen the film *Three Kings* will see the obvious similarities with the example email shown in Figure 3 (those who haven't seen the film can read a synopsis at http://imdb.com/title/tt0120188/).


From Sgt Rita Graham - Thunderbird

File Edit View Go Message OpenPGP Tools Help

Subject: From Sgt Rita Graham From: From Sgt Rita Graham 25/05/2006 16:17

>From Sgt Rita Graham

Good Day,

I hope my email meets you well. I am in need of your assistance. My Name is Sgt Rita Graham , Jr. I am in the Engineering military unit here in Ba'qubah in Iraq,we have about $25 Million US dollars that we want to move out of the country. My partners and

I need a good partner someone we can trust. It is oil money and legal.

But we are moving it through diplomatic means, to send it to your house directly or a bank of your choice using diplomatic courier service.The most important thing is that can we trust you? Once the funds get to you, you take your 40% out and keep our own 60%. Your own part of this deal is to find a safe Account where the funds can be transfer to. Our own part is sending it to you.If you are interested i will furnish you with more details. But the whole process is simple and we must keep a low profile at all times.

I look forward to your reply and co-operation, and I thank you in advance as I anticipate your co-operation.

You can reach me on via email : RitaGraham@mail.nu

Waiting for your urgent response.

Regards,

Sgt Rita Graham

Figure 3: A typical 'Three Kings' 419 email.

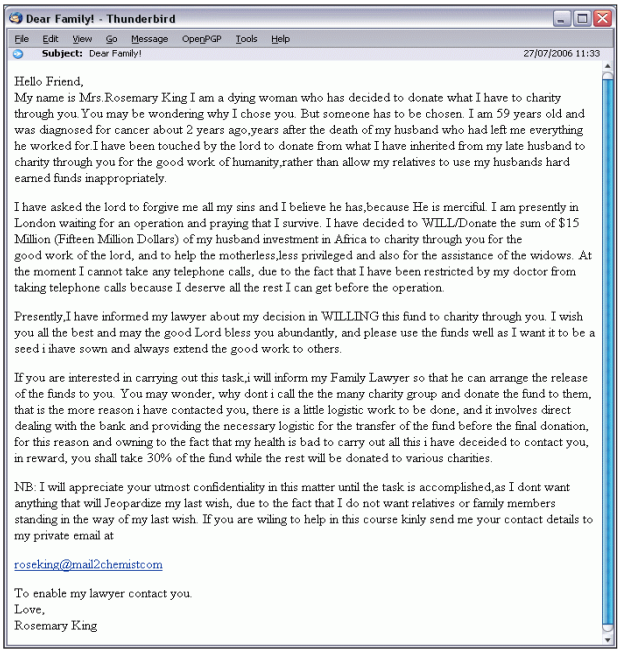
The interesting twist here is that this variant uses the name of a female sergeant rather than a male sergeant as is more commonly seen in this scam.

DYING TO HELP

Not only do I often see 419 scams using high-profile events/disasters as bait, but there are also numerous scams that attempt to draw the victim in using the subject of illness. I have seen many examples of scams using sorry tales of the following illnesses as a way to push your buttons:

- Cancer (usually of the oesophagus, liver or prostate)
- HIV or AIDS
- Stroke
- Fibroids
- Unknown incurable illness
- All or several of the above at the same time.

Usually, the person named in the email claims to be seeing the errors of their ways and experiencing a change of heart, from being selfish and self-obsessed to becoming a philanthropist as a way of paying for the mistakes they have made in their lives. In many cases they state that they need your help in order to give money to a charity or a church (as shown in Figure 4). All very touching, but still a pack of lies.


Dear Family! - Thunderbird

File Edit View Go Message OpenPGP Tools Help

Subject: Dear Family! 27/07/2006 11:33

Hello Friend,
My name is Mrs.Rosemary King I am a dying woman who has decided to donate what I have to charity through you.You may be wondering why I chose you. But someone has to be chosen. I am 59 years old and was diagnosed for cancer about 2 years ago,years after the death of my husband who had left me everything he worked for.I have been touched by the lord to donate from what I have inherited from my late husband to charity through you for the good work of humanity,rather than allow my relatives to use my husbands hard earned funds inappropriately.

I have asked the lord to forgive me all my sins and I believe he has,because He is merciful. I am presently in London waiting for an operation and praying that I survive. I have decided to WILL/Donate the sum of $15 Million (Fifteen Million Dollars) of my husband investment in Africa to charity through you for the good work of the lord, and to help the motherless,less privileged and also for the assistance of the widows. At the moment I cannot take any telephone calls, due to the fact that I have been restricted by my doctor from taking telephone calls because I deserve all the rest I can get before the operation.

Presently,I have informed my lawyer about my decision in WILLING this fund to charity through you. I wish you all the best and may the good Lord bless you abundantly, and please use the funds well as I want it to be a seed i ihave sown and always extend the good work to others.

If you are interested in carrying out this task,i will inform my Family Lawyer so that he can arrange the release of the funds to you. You may wonder, why dont i call the the many charity group and donate the fund to them, that is the more reason i have contacted you, there is a little logistic work to be done, and it involves direct dealing with the bank and providing the necessary logistic for the transfer of the fund before the final donation, for this reason and owning to the fact that my health is bad to carry out all this i have deceided to contact you, in reward, you shall take 30% of the fund while the rest will be donated to various charities.

NB: I will appreciate your utmost confidentiality in this matter until the task is accomplished,as I dont want anything that will Jeopardize my last wish, due to the fact that I do not want relatives or family members standing in the way of my last wish. If you are wiling to help in this course kinly send me your contact details to my private email at

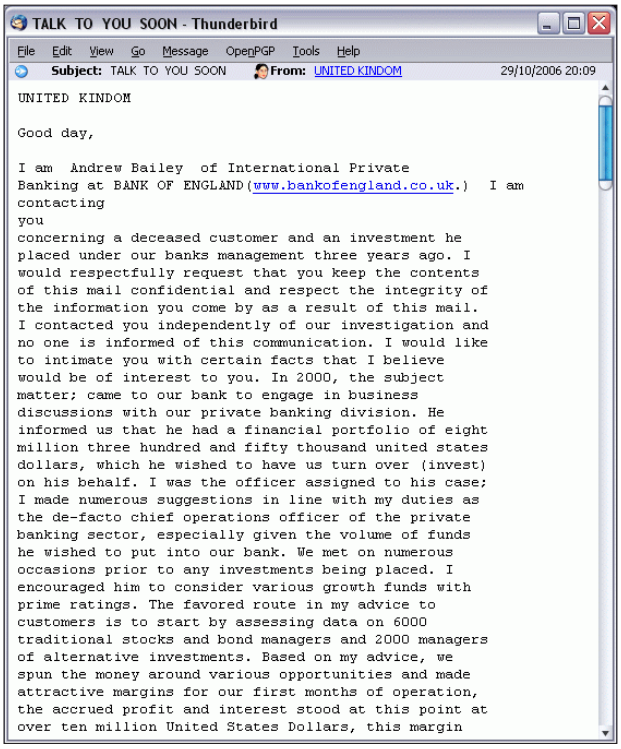
roseking@mail2chemistcom

To enable my lawyer contact you.
Love,
Rosemary King

Figure 4: A typical 'Dying to help' 419 email.

YOU CAN BANK ON ME

Banks the world over are targeted not only by phishers, but 419 scammers have also spotted the potential for drawing in victims using the name and details of well-known banks.


TALK TO YOU SOON - Thunderbird

File Edit View Go Message OpenPGP Tools Help

Subject: TALK TO YOU SOON From: UNITED KINDOM 29/10/2006 20:09

UNITED KINDOM

Good day,

I am Andrew Bailey of International Private Banking at BANK OF ENGLAND(www.bankofengland.co.uk.) I am contacting you concerning a deceased customer and an investment he placed under our banks management three years ago. I would respectfully request that you keep the contents of this mail confidential and respect the integrity of the information you come by as a result of this mail. I contacted you independently of our investigation and no one is informed of this communication. I would like to intimate you with certain facts that I believe would be of interest to you. In 2000, the subject matter; came to our bank to engage in business discussions with our private banking division. He informed us that he had a financial portfolio of eight million three hundred and fifty thousand united states dollars, which he wished to have us turn over (invest) on his behalf. I was the officer assigned to his case; I made numerous suggestions in line with my duties as the de-facto chief operations officer of the private banking sector, especially given the volume of funds he wished to put into our bank. We met on numerous occasions prior to any investments being placed. I encouraged him to consider various growth funds with prime ratings. The favored route in my advice to customers is to start by assessing data on 6000 traditional stocks and bond managers and 2000 managers of alternative investments. Based on my advice, we spun the money around various opportunities and made attractive margins for our first months of operation, the accrued profit and interest stood at this point at over ten million United States Dollars, this margin

Figure 5: A typical 'You can bank on me' 419 email.

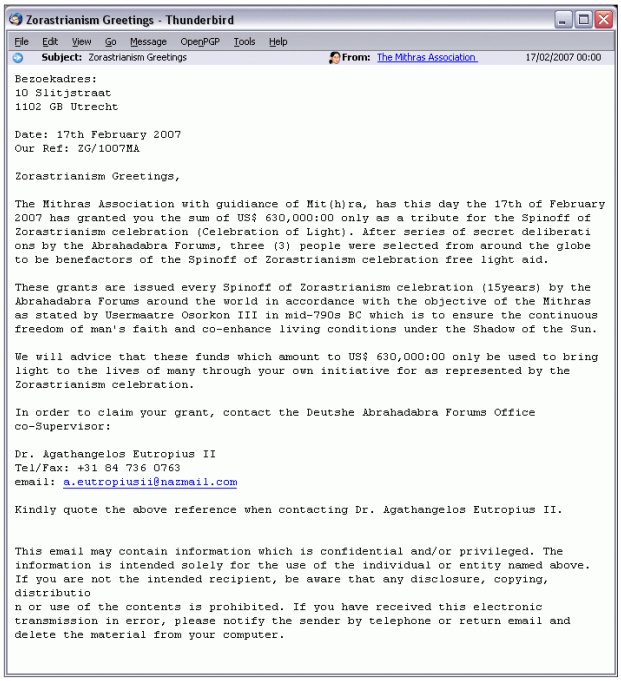
The email shown in Figure 5 claims to be from someone at the Bank of England. I have seen versions of this approach featuring all the major UK, Spanish, Swiss, Chinese, US, Canadian, French and South African banks, to name just a few – the list is almost endless. The scam usually involves an account that has become dormant, due to its (non-existent) owner having died. The victim's mission, should they accept it, is to pretend to be a relative of the account holder and claim the money; less a percentage for the banker, of course.

THE POWER OF RELIGION

The use of religion as a hook is a common way for scammers to try to convince potential victims that they have high ethical standards, because they (claim to) subscribe to a particular religion.

However, as you can see in Figure 6, sometimes they use a religion as the originator of a lottery or other scam, rather than simply saying they are a devout believer. Occasionally, they even masquerade as religious officials, such as priests or nuns.

I find it interesting that I have not yet seen a 419 scammer use Buddhism, Hinduism, Judaism, Sikhism or even Santeria in their scams. Maybe the scammers have only been exposed to Islam and Christianity.


Zorastrianism Greetings - Thunderbird

File Edit View Go Message OpenPGP Tools Help

Subject: Zorastrianism Greetings From: The Mithras Association 17/02/2007 00:00

Bezoekadres:
10 Slitjstraat
1102 GB Utrecht

Date: 17th February 2007
Our Ref: ZG/1007MA

Zorastrianism Greetings,

The Mithras Association with guidiance of Mit(h)ra, has this day the 17th of February 2007 has granted you the sum of US$ 630,000:00 only as a tribute for the Spinoff of Zorastrianism celebration (Celebration of Light). After series of secret deliberati ons by the Abrahadabra Forums, three (3) people were selected from around the globe to be benefactors of the Spinoff of Zorastrianism celebration free light aid.

These grants are issued every Spinoff of Zorastrianism celebration (15years) by the Abrahadabra Forums around the world in accordance with the objective of the Mithras as stated by Usermaatre Osorkon III in mid-790s BC which is to ensure the continuous freedom of man's faith and co-enhance living conditions under the Shadow of the Sun.

We will advice that these funds which amount to US$ 630,000:00 only be used to bring light to the lives of many through your own initiative for as represented by the Zorastrianism celebration.

In order to claim your grant, contact the Deutshe Abrahadabra Forums Office co-Supervisor:

Dr. Agathangelos Eutropius II
Tel/Fax: +31 84 736 0763
email: a.eutropiusii@nazmail.com

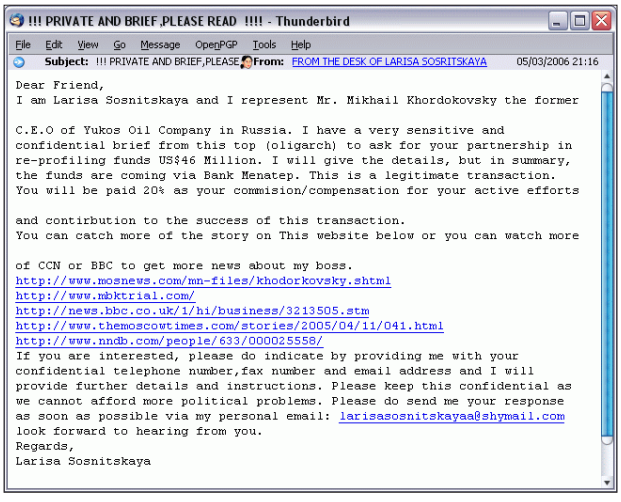
Kindly quote the above reference when contacting Dr. Agathangelos Eutropius II.

This email may contain information which is confidential and/or privileged. The information is intended solely for the use of the individual or entity named above. If you are not the intended recipient, be aware that any disclosure, copying, distributio
n or use of the contents is prohibited. If you have received this electronic transmission in error, please notify the sender by telephone or return email and delete the material from your computer.

Figure 6: A typical 'Power of religion' 419 email.

WELL OIL BE SCAMMED

419 scams based around the oil industry are nothing new; these have been around in one shape or another almost since the beginning of the scam. However, every now and then a new twist emerges which raises the scam from being 'just-another-419-oil-scam' to something special. Figure 7 shows one of the latest scams in that vein – one which J.R Ewing would be proud to call his own.


!!! PRIVATE AND BRIEF,PLEASE READ !!!! - Thunderbird

File Edit View Go Message OpenPGP Tools Help

Subject: !!! PRIVATE AND BRIEF,PLEASE From: FROM THE DESK OF LARISA SOSRITSKAYA 05/03/2006 21:16

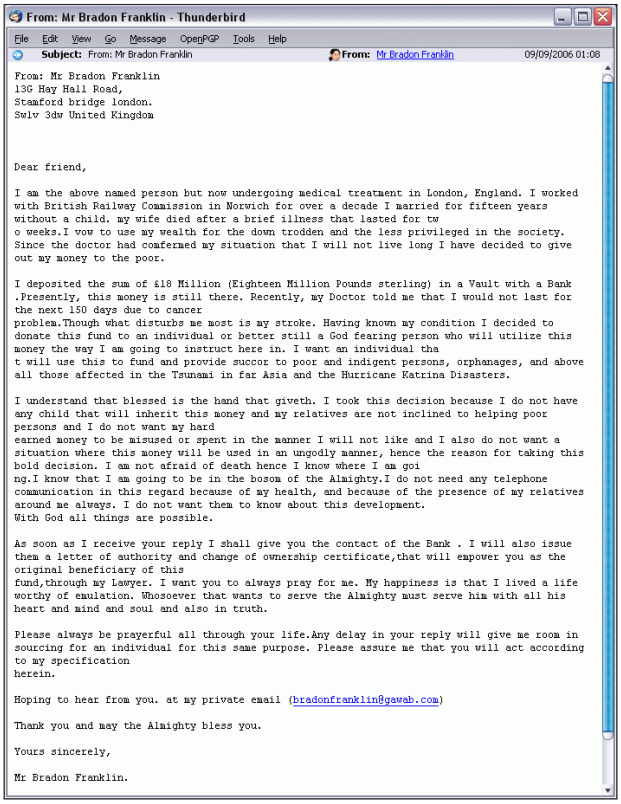
Dear Friend,
I am Larisa Sosnitskaya and I represent Mr. Mikhail Khordokovsky the former

C.E.O of Yukos Oil Company in Russia. I have a very sensitive and confidential brief from this top (oligarch) to ask for your partnership in re-profiling funds US$46 Million. I will give the details, but in summary, the funds are coming via Bank Menatep. This is a legitimate transaction. You will be paid 20% as your commision/compensation for your active efforts

and contirbution to the success of this transaction.
You can catch more of the story on This website below or you can watch more

of CCN or BBC to get more news about my boss.
http://www.mosnews.com/mn-files/khodorkovsky.shtml
http://www.mbktrial.com/
http://news.bbc.co.uk/1/hi/business/3213505.stm
http://www.themoscowtimes.com/stories/2005/04/11/041.html
http://www.nndb.com/people/633/000025558/
If you are interested, please do indicate by providing me with your confidential telephone number,fax number and email address and I will provide further details and instructions. Please keep this confidential as we cannot afford more political problems. Please do send me your response as soon as possible via my personal email: larisasosnitskayaa@shymail.com
look forward to hearing from you.
Regards,
Larisa Sosnitskaya

Figure 7: A typical 'Yukos Oil' 419 email.


From: Mr Bradon Franklin - Thunderbird

File Edit View Go Message OpenPGP Tools Help

Subject: From: Mr Bradon Franklin From: Mr Bradon Franklin 09/09/2006 01:08

From: Mr Bradon Franklin
13G Hay Hall Road,
Stamford bridge london.
Swlv 3dw United Kingdom

Dear friend,

I am the above named person but now undergoing medical treatment in London, England. I worked with British Railway Commission in Norwich for over a decade I married for fifteen years without a child. my wife died after a brief illness that lasted for tw
o weeks.I vow to use my wealth for the down trodden and the less privileged in the society. Since the doctor had comfermed my situation that I will not live long I have decided to give out my money to the poor.

I deposited the sum of £18 Million (Eighteen Million Pounds sterling) in a Vault with a Bank .Presently, this money is still there. Recently, my Doctor told me that I would not last for the next 150 days due to cancer
problem.Though what disturbs me most is my stroke. Having known my condition I decided to donate this fund to an individual or better still a God fearing person who will utilize this money the way I am going to instruct here in. I want an individual tha
t will use this to fund and provide succor to poor and indigent persons, orphanages, and above all those affected in the Tsunami in far Asia and the Hurricane Katrina Disasters.

I understand that blessed is the hand that giveth. I took this decision because I do not have any child that will inherit this money and my relatives are not inclined to helping poor persons and I do not want my hard
earned money to be misused or spent in the manner I will not like and I also do not want a situation where this money will be used in an ungodly manner, hence the reason for taking this bold decision. I am not afraid of death hence I know where I am goi
ng.I know that I am going to be in the bosom of the Almighty.I do not need any telephone communication in this regard because of my health, and because of the presence of my relatives around me always. I do not want them to know about this development.
With God all things are possible.

As soon as I receive your reply I shall give you the contact of the Bank . I will also issue them a letter of authority and change of ownership certificate,that will empower you as the original beneficiary of this
fund,through my Lawyer. I want you to always pray for me. My happiness is that I lived a life worthy of emulation. Whosoever that wants to serve the Almighty must serve him with all his heart and mind and soul and also in truth.

Please always be prayerful all through your life.Any delay in your reply will give me room in sourcing for an individual for this same purpose. Please assure me that you will act according to my specification
herein.

Hoping to hear from you. at my private email (bradonfranklin@gawab.com)

Thank you and may the Almighty bless you.

Yours sincerely,

Mr Bradon Franklin.

Figure 8: The 'British Railway' 419 email.

ON THE WRONG TRACK?

The tale that appears in the email shown in Figure 8 has to be one of the oddest I've seen yet. It claims to be from a (dying) former employee of the British Railway Commission, who wishes to use his great wealth to help the poor and needy. One has to wonder how a 'British railway worker' could amass over £18 million. Either those who work on the railway are very, very well paid (I know that they are not) or most likely the scammers believe that we, in the UK, are *all* millionaires.

POLITICIANS AND RULERS

According to the email shown in Figure 9, a certain Mr Berlusconi needs your help in moving some funds before they all get frozen by the authorities investigating him for alleged fraud. Poor man, don't you feel sorry for him?

Whether he is innocent or guilty is irrelevant, at least as far as it has to do with this request. Why? Well, guess what, the email isn't from Mr Berlusconi, or indeed anyone acting on his behalf. Don't you just love the wording '…rest assured that this transaction would be done legally…'?

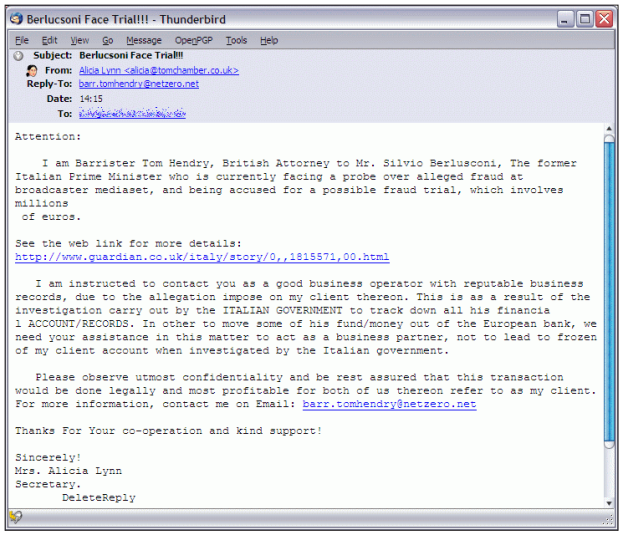


Figure 9: A typical political 419 email.

On 11 November 2004, the very day that Yasser Arafat died, I saw a new 419 using his name and claiming to be from his widow. And in March 2006, scammers used the death of none other than King Fahd of Saudi Arabia, who died on 1 August 2005 at the age of 84, as a basis for their scam.

THE SCAM THAT WARNS ABOUT SCAMS

Once in a while I see a 419 like the one shown in Figure 10, which claims to be from someone who is trying to stamp out these scams and the related corruption – of course, it is a scam in its own right.

CONCLUSIONS

Below are just some of the many rules that many 419s will trigger, indicating that they are not what they claim to be:

- Tell you to keep the deal secret, even from your family and solicitors. And mention that failure to keep it secret will void your winnings, etc.
- Claim they are representing a large company, financial or other trusted or well-known organisation or person.
- Use free web mail addresses instead of ones for the company they claim to represent.
- Include only a mobile phone number, fax number or premium rate number.
- Use common social-engineering tricks, playing on greed, illness, empathy, altruism, etc.
- Claim that the deal is perfectly legal, even when they are asking you to move stolen/trapped funds/goods they have no right to (even if they did exist).

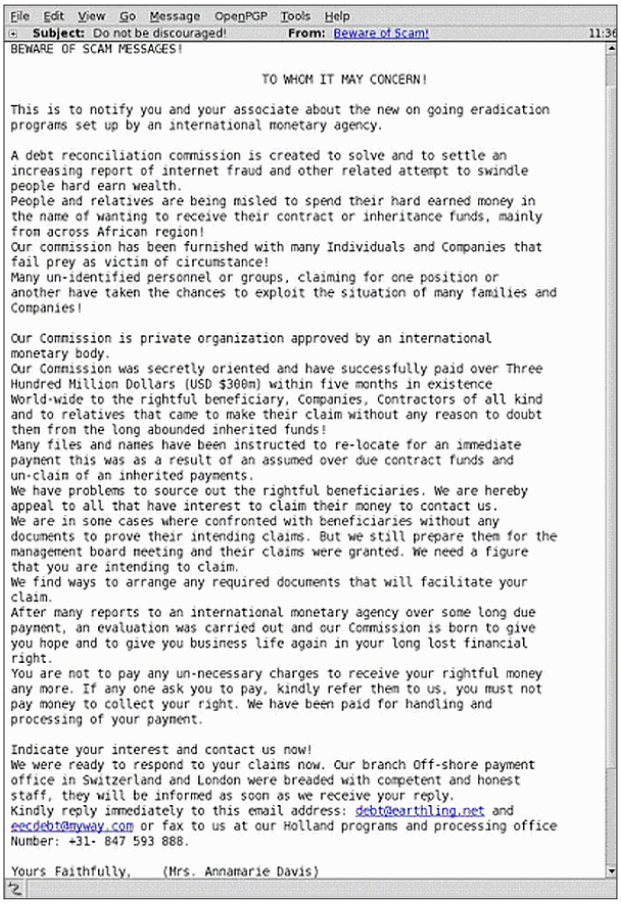


Figure 10: The 'Warning You About Scams' 419 email.

The boys and girls from Lagos – or indeed anywhere in the world now – are not shy about using current events or disasters to try and part you from your money, and they seem to be obsessed with lotteries, believing that people will fall for this ploy (unfortunately they are often right). What's more, this article only scratches the surface of the scale and inventiveness of the 419 scammers.

So, next time you are:

- Told that you have won a lottery that you didn't enter.
- Approached to help someone move trapped funds/goods.
- Asked to make a donation to a disaster fund by a person claiming to be a victim of said disaster.

Don't be fooled, even if your heart strings have been tugged and you want to help the poor unfortunate person, or the thought of all that money you have (supposedly) won has bypassed your normal healthy scepticism. If you fall for the ploy, you may find yourself with a seriously depleted bank account.