OCTOBER 2005

virus BULLETIN

The International Publication on Computer Virus Prevention, Recognition and Removal

CONTENTS

2 **COMMENT**
Time to embrace the digital age

3 **NEWS**
AVIEN virtual conference
Symantec snaps up WholeSecurity
CME initiative sets forth

3 **VIRUS PREVALENCE TABLE**

FEATURES
4 Zo-to-business
6 Grey clouds on the horizon

11 **BOOK REVIEW**
Vers & virus

12 **COMPARATIVE REVIEW**
Windows 2003 Advanced Server

20 **END NOTES & NEWS**

IN THIS ISSUE

UNDER ATTACK

Apart from being large multinationals, what do *CNN*, *UPS*, the *New York Times*, *General Electric* and *ABC News* have in common? The answer is that they (reportedly) were all infected by Zotob. Martin Overton provides an overview of this summer's most fast-spreading network worm.
page 4

GATHERING CLOUDS

PSGuard is a 'virus and spyware remover' program which is promoted through the Win32/Nsag infectors. While questionable in terms of motive, the program itself has no malicious payload. Roel Schouwenberg considers the problems 'light grey' applications such as this pose for the AV industry.
page 6

COMPARATIVE REVIEW

27 products squeeze onto the *Windows 2003 Advanced Server* testing bench this month. Matt Ham has the details.
page 12

vbSpam supplement

This month: anti-spam news and events, we review Jonathan Zdziarski's *Ending Spam*, and Des Cahill explains the benefits of trust and accountability.

ISSN 0956-9979

virus BULLETIN COMMENT

'This new format will enable us to deliver Virus Bulletin *almost instantaneously.'*

Helen Martin
Editor, Virus Bulletin

TIME TO EMBRACE THE DIGITAL AGE

Virus Bulletin has seen a few changes over the years – editors have come and gone, the days of listing all known viruses along with descriptions and their hexadecimal search patterns are long gone (indeed the days of being able to list all known viruses within the confines of a 24-page publication are over – when *VB* was first published in July 1989 the total was a manageable 14), the design and layout of the magazine have been updated, while features such as the VB 100% award scheme and the *VB Spam Supplement* have been introduced and become part of the furniture along the way.

The next major change is that, from January 2006 *Virus Bulletin* will become a wholly electronic publication, delivered in PDF format to all subscribers.

Every month all subscribers will receive notification via email that the new issue of *Virus Bulletin* has been released, and a simple click of the mouse will take the subscriber to www.virusbtn.com where the latest issue will be available in PDF format to be read online, saved to disk or downloaded and printed. This new format will enable us to deliver *Virus Bulletin* almost instantaneously, cutting out the inevitable postal delays as well as the limits imposed by the printing schedule, thus allowing us to include the most up-to-the-minute material each month.

For those who lovingly maintain a back catalogue of hard copy *VB*s, this is without doubt the end of an era, but it also marks the start of a new chapter. *VB* will revert to the practice of producing an annual CD-ROM and in future every subscriber will receive a CD-ROM in January containing all the issues of *Virus Bulletin* published in the previous 12 months (January to December).

Alongside the new format, a new pricing and licensing structure will be introduced from January 2006 – the first time the basic price of *VB* has changed in 16 years.

Individual subscribers will see a significant cost saving, with the new subscription costing $175. Corporate customers will see a change too – from January a corporate subscription (or 'licence') will allow subscribers to post *Virus Bulletin* issues on their company intranet or otherwise circulate them internally, thus allowing all employees access to the magazine. The new pricing structure will be as follows:

- Individual subscribers (the magazine may be accessed only by the named individual): $175
- Corporate subscriber whose company's annual turnover is $0–10 million (the magazine may be circulated internally/posted on intranet): $500
- Corporate subscriber whose company's annual turnover is $10–100 million (the magazine may be circulated internally/posted on intranet): $1000
- Corporate subscriber whose company's annual turnover is $100+ million (the magazine may be circulated internally/posted on intranet): $2000
- *Bona fide* educational institutions/charities: $175
- Public libraries: $500

As previously, individual subscribers will qualify for a discount on the cost of registration for the *Virus Bulletin* conference, and corporate subscribers will be assigned a block of discounted conference registrations, the number depending on their subscription type.

While this will almost certainly qualify as the greatest change the magazine has seen so far, subscribers should rest assured that, as the adage goes, the more things change the more they remain the same: there will be no change in the nature of the magazine, its content, or its purpose. As ever, *Virus Bulletin* will remain dedicated to its quest to provide unbiased and exceptional reporting of all matters relevant to the anti-virus and anti-spam industries.

More information about the changes will be sent to subscribers over the coming months.

NEWS

AVIEN VIRTUAL CONFERENCE

The organisers of the inaugural AVIEN/AVIEWS virtual conference have issued a call for papers. The conference, which will take place on 18 January 2006 by webcast, will be based on the theme 'Battling malware – a view from the trenches'. The organisers are seeking submissions for 30-minute presentations on a range of subjects (a full list can be found at http://www.avien.org/conf2006cfp.html). Abstracts should be sent in RTF or plain text format to avien_conf@avien.net by 10 October 2005.

While the conference will be open only to members of the AVIEN/AVIEWS forums, members may sponsor non-members, who will be vetted for approval. Registration details will be circulated in the forums and on the website in due course.

SYMANTEC SNAPS UP WHOLESECURITY

Symantec has announced that it plans to purchase privately held behavioural endpoint security solutions provider *WholeSecurity Inc*.

WholeSecurity's behavioural detection technology identifies both known and unknown threats without requiring users to install or update signatures, and can be used against traditional malware threats such as viruses and worms, as well as against phishing threats. *WholeSecurity*'s customers include *eBay*, *Deutsche Bank* and *Visa*. *Symantec* plans to offer standalone products using *WholeSecurity*'s technology as well as incorporate it into its security software suites. The acquisition is expected to complete later this month.

CME INITIATIVE SETS FORTH

US-CERT will officially unveil its Common Malware Enumeration (CME) initiative this month. The scheme, which will be operated by *MITRE*, and will work very much like the current Common Vulnerabilities and Exposures (CVE) initiative, aims to reduce the public's confusion during malware incidents, enhance communication between anti-virus vendors and improve communication and information sharing between anti-virus vendors and the rest of the information security community (see *VB*, September 2005, p.14). This month sees the debut of the CME website, which will host information about threats, together with the all-important CME tag for each major threat – which it is hoped security companies will incorporate into the names they assign to the threats. The first version of the CME website will include descriptions of a couple of dozen threats, but a more comprehensive collection is planned for later in the year. Information about the initiative can be found at http://cme.mitre.org/.

Prevalence Table – August 2005

Virus	Type	Incidents	Reports
Win32/Netsky	File	16,929	47.35%
Win32/Bagle	File	6,537	18.28%
Win32/Mytob	File	3,985	11.14%
Win32/Mydoom	File	2,928	8.19%
Win32/Zafi	File	2,287	6.40%
Win32/Lovgate	File	520	1.45%
Win32/Klez	File	275	0.77%
Win32/Funlove	File	226	0.63%
Win32/Dumaru	File	218	0.61%
Win32/Bagz	File	215	0.60%
Win32/Pate	File	123	0.34%
Win32/Bugbear	File	119	0.33%
Win32/Mabutu	File	109	0.30%
Win32/MyWife	File	104	0.29%
Win32/Agobot	File	95	0.27%
Win32/Reatle	File	94	0.26%
Win32/Mimail	File	93	0.26%
Win32/Fizzer	File	90	0.25%
Win32/Swen	File	83	0.23%
Win32/Sdbot	File	82	0.23%
Win32/Valla	File	79	0.22%
Redlof	Script	72	0.20%
Win32/Mota	File	64	0.18%
Win32/Bobax	File	46	0.13%
Win32/Yaha	File	45	0.13%
Win32/Randex	File	23	0.06%
Win32/Wurmark	File	19	0.05%
Psyme	Script	18	0.05%
Win32/Hybris	File	16	0.04%
Win32/Magistr	File	16	0.04%
Win32/Maslan	File	15	0.04%
Laroux	Macro	11	0.03%
Others[1]		220	0.62%
Total		35,756	100%

[1]The Prevalence Table includes a total of 220 reports across 60 further viruses. Readers are reminded that a complete listing is posted at http://www.virusbtn.com/Prevalence/.

FEATURE 1

ZO-TO-BUSINESS

Martin Overton
Independent Researcher, UK

On Monday 15 August something started to spread quickly on the Internet, causing many companies' *Windows 2000* systems to reboot themselves without human assistance. Next, system administrators saw the unexplained slowdown of internal networks. We were once again under attack from a fast-spreading network worm.

MICROSOFT'S UNLUCKY NUMBER?

It appears that, for *Microsoft*, the number 39 is unusually unlucky – at least when it comes to security advisories. Here are three examples of 'the curse of 39' in action:

- MS02-039 – exploited by Slammer
- MS03-039 – exploited by Blaster
- MS05-039 – exploited by Zotob

Each of these worms caused a significant outbreak. In all cases, not only did they cause mass infection very rapidly, but they also had a significant impact on the networks of companies they had infected, in some cases to the point of exhausting all available bandwidth. So, let us now look at the latest 'curse-of-39' worm and see how it fared.

MS05-039 OR BUST!

On 9 August, *Microsoft* released security advisory MS05-039 [1] which revealed a vulnerability in the Plug-and-Play component of *Windows 2000*. The vulnerability was rated as critical. *Microsoft* also released a fix to patch the loophole.

Barely five days after the warning, a worm called Zotob [2] appeared that exploited the loophole. This meant that all those systems which had not been patched, or were not protected by other methods were vulnerable to a dose of digital pox.

According to *F-Secure* [3], Zotob was captured and an initial analysis was made at around 12pm (GMT) on 14 August.

The initial analysis of Zotob.A mentions that the worm may be using the 'houseofdabus' exploit code [3] and that when a system becomes infected it scans the network for other systems via port 445/tcp, at a rate of 300 threads per infected system. Each thread will attempt to connect to a random IP address, created by taking the first two octets of the current system's IP address and randomising the last two octets – e.g. if the system infected has an IP address of 10.10.10.1 then it will attempt to scan random IP addresses in the range 10.10.0.0 to 10.10.255.255.

Any system that shows the port to be open (*Windows 2000* and *XP*) is sent a copy of the exploit code, regardless of whether it has been patched, or is vulnerable.

If the system is an unpatched *Windows* 2000 system, then the exploit code should run and cause a buffer overflow unless the system is protected in other ways. If the exploit code runs successfully, this will create a shell (CMD.EXE) which listens on port 8888/tcp. The scanning (infected) computer will then try to send an FTP script to the newly listening shell on the victim computer. This script is written to the victim's hard disk as '%SYSTEM%\2pac.txt' which tells the newly exploited victim to download a copy of the worm binary from the attacker.

The attacker's FTP server runs on TCP port 33333 and exists only to act as a pickup point for the worm's binary, which is called 'haha.exe'. When run, this downloaded file creates a copy of itself in the %SYSTEM% directory (e.g. C:\WINNT\SYSTEM32 or C:\WINDOWS\SYSTEM32) as a file called 'botzor.exe'. It then creates a mutex named 'B-O-T-Z-O-R' to ensure that only one copy of itself is running on the newly infected system.

Next it adds itself to the system registry to ensure that it is loaded each time the system starts, and also adds a key which disables the shared access service. The newly infected system now connects to IRC server 'diabl0.turkcoders.net' on port 8080, effectively signing in for service as part of a botnet.

Zotob also adds a list of common anti-virus and security-related sites to the hosts file on the newly infected system. This is to try to stop the owner accessing the sites for updates or information. All entries are redirected to 127.0.0.1 (the local loopback address).

Zotob also writes other strings into the hosts file of the newly infected system, these are:

```
Bozor2005 Made By … Greetz to good friend Coder.
Based on HellBot3

MSG to avs: The first who detects this worm will be
the first killed in the next 24 hours!
```

The mention of HellBot3 is a clear indication that Zotob was based on Mytob.

Although Zotob.A can't infect *Windows XP* systems automatically, the worm code can be installed manually or by clicking on an infected file, which will then infect the system running *XP* and Zotob will start scanning for new hosts to infect and exploit. Of course, some of the later variants also spread via email, just like many of the Mytob variants do.

ARRESTED DEVELOPMENT

Several weeks after the initial outbreak of Zotob, breaking news arrived [4], stating that Moroccan authorities working

with the FBI had arrested 18-year-old Farid Essebar, a Moroccan national born in Russia who went by the screen moniker 'Diabl0'. A 21-year-old Turkish citizen named Atilla Ekici, aka 'Coder' was also arrested in Turkey.

The hacker pseudonym 'Diabl0' can be found in around 20 variants of Mytob, which may implicate Essebar as the author. It is also alleged that Mr Essebar was paid by Mr Ekici to create the Zotob worm which Mr Ekici is believed to have distributed. The article also indicates that Essebar and Ekici may have used the information they stole from infected computers to facilitate a bank card forgery scam.

Further breaking news came on 30 August [5], stating that the FBI had confirmed that Turkish law enforcement officials were investigating 16 more suspects in connection with the Zotob worm and its variants. So we may yet see more arrests in relation to Zotob.

THE AFTERMATH

At the time of writing this article, there are 14 variants of the Zotob worm (according to *Trend Micro*), as well as several other worms which use the same exploit to get them onto target systems.

It has been suggested that well over 100 large companies were hit badly by Zotob. These include *CNN*, which provided open coverage of its own massive outbreak. The *New York Times* and *ABC News* were also reported to have suffered from a widespread infection of Zotob. One report suggests that systems the U.S. Department of Homeland Security uses to screen airline passengers entering the United States may have been disabled temporarily by the worm. Other large multinationals reported to have been infected include: *UPS*, *General Electric*, *Caterpillar*, the *Canadian Imperial Bank of Commerce* and *BMO Nesbitt Burns* [6].

MITIGATION

Let us now look at ways in which we could have slowed, hobbled or stopped Zotob in the first place.

Patch me if you can!

Many organisations have patching cycles; each new patch from *Microsoft* is rated individually according to the risk to the relevant infrastructure, and is then tested to ensure that the cure is not worse than any disease that may come along to take advantage of the infection vector the patch mitigates. In most cases this cycle takes a minimum of 14 days, and may be as long as 120 days from analysis to full production deployment.

However, after Blaster, Slammer and Sasser many organisations have pulled the window in to an average of around 30 days. Some organisations now have a 7–10 day patch testing turnaround. But, as we have seen in the case of Zotob, a patch test cycle of 7–10 days is just not fast enough. We can expect other worms to arrive which won't allow any time for patching and which will become widespread as quickly as Slammer, Blaster and Zotob. So, what can be done to offset this risk? The following covers a number of the more obvious solutions that you should already have in place or be considering.

Personal firewalls, network firewalls and routers

As a rule your perimeter firewalls should not have allowed port 445/tcp (and udp) to traverse from/to your network and the Internet. Likewise, if you had set your router ACLs to block traffic destined for systems on port 445/tcp, even if you had Zotob on your network its progress would have been slowed dramatically.

If your systems had personal firewalls installed Zotob would probably have been stopped from scanning your network and infecting other vulnerable hosts. Likewise, if you had a managed personal firewall policy you could have pushed out a new policy to block port 445/tcp inbound (which would have stopped even a vulnerable uninfected system from becoming infected via the port scan) as well as outbound (which would stop an infected system from scanning your network for new victims).

IDS and IPS

As soon as details of Zotob and its spreading pattern emerged, it was a fairly simple matter to create some basic signatures/rules for Snort. These were followed quickly by binary signatures that would trigger on the worm being sent from one system to another, just after it had been exploited via PnP. This was extremely useful as it would list both the attacker's and victim's IP addresses, which would allow faster remediation, or at least removal of the infected systems from the network.

On 11 August, *Sourcefire* had written and released signatures (of high enough quality to be used in an IPS) for the exploit code used in Zotob, and the copycats. IPS signatures for the exploit used by Zotob had been available since before Zotob was first spotted, which would have minimised the likelihood that your vulnerable systems would become infected as the IPS would block the malicious traffic.

Anti-virus

I shouldn't need to say this, but you should ensure that your anti-virus is up to date and that all clients are, by default, requested to check for new updates at least once a day. Again, if you have a managed anti-virus infrastructure this can be significantly easier as you can force all connected managed clients to update themselves when an outbreak is

in progress. This will help to shrink the 'possible infection pool' and make cleanup less expensive.

There are a number of other methods which could have been used to mitigate the threat of Zotob (and most other malware), but I have run out of space to describe them.

ZOTOB'S PROGRESS

Finally, the following is a timeline charting Zotob's progress [7]:

9 August 2005: *Microsoft* releases six security patches (MS05-038–43). Four are rated as critical. Initial exploit code is written and released for two of the vulnerabilities; MS05-038 and MS05-041.

11 August 2005: Exploit code is written and released to take advantage of the vulnerability patched in MS05-039. This is the PnP (Plug and Play) vulnerability.

12 August 2005: Snort signatures are released to detect the exploits, and code for another MS05-039 exploit is released.

14 August 2005: A new worm based on Mytob code and containing exploit code as its attack vector is released, discovered by *F-Secure*, and named Zotob. The exploit code used is from the 'houseofdaubus' hacking group (exploit code from the same group was used in the Sasser worm).

15 August 2005: The source code for the widespread IRCbot family is updated to take advantage of the MS05-039 exploit. New variants of Zotob appear. Snort signatures for detecting the binary as well as the IRC traffic are written and released. Most anti-virus products can now detect Zotob.A.

17 August 2005: There are now seven variations of Zotob, one Rbot, one SDbot, one CodBot, three IRCbots and two Bozori variants using the PnP vulnerability. The Bozori and IRCbots are deleting other bots. The Bot-wars have begun!

So there you have it, Zotob in a nutshell.

REFERENCES

[1] http://www.microsoft.com/technet/security/bulletin/MS05-039.mspx.

[2] http://www.microsoft.com/security/incident/zotob.mspx.

[3] http://www.f-secure.com/weblog/archives/archive-082005.html#00000624.

[4] http://blogs.washingtonpost.com/securityfix/2005/08/arrest_of_zotob.html.

[5] http://www.computerworld.com/securitytopics/security/story/0,10801,104269,00.html?from=story_kc.

[6] http://business.timesonline.co.uk/article/0,,9075-1738986,00.html.

[7] http://singe.rucus.net/blog/archives/510-MS05-039-and-the-Zotob-summary.html.

FEATURE 2

GREY CLOUDS ON THE HORIZON

Roel Schouwenberg
Kaspersky Lab, The Netherlands

In December 2004, I received reports from the anti-spyware community about some ad/spyware which was very difficult to identify. After some research, it was clear that the first file-infecting ad/spyware had been found – by accident.

The infector, named Virus.Win32.Implinker.a, used an old, but interesting tactic. The main file consists of two components, a file-infecting dropper and an adware dll. The adware component is detected by *Kaspersky Anti-Virus* as 'not-a-virus:AdWare.Visiter', also known as Holax.

Upon execution the .dll file is dropped into %sysdir% and the infector looks for the usual RUN keys for programs executed at boot. It copies the files it finds into %temp% and adds an import which refers to the .dll component in the target file. PendingFileRenameOperations is then used to replace the files in %temp% with the original files at the next system boot.

This was quite a different way of loading a .dll file. It marked the first real blow against dedicated anti-spyware applications, whose engines are not sophisticated enough to detect or disinfect the infected files. An additional downside to only deleting the malicious .dll file is that due to the missing import library, infected files can no longer be executed.

The impact of this piece of malware was quite noticeable. Even after the first positive identification, the anti-spyware community continued to have great difficulty identifying this infection. Although it's hard to compile precise statistics, the number of reports suggest that this was a minor (adware) epidemic.

BEAVIS IS THE NAME

At the end of January 2005, Virus.Win32.Bube.a (aka Beavis) was detected. A number of variants appeared in a short space of time, but they hardly differed from each other, incorporating only minor changes such as the target URL.

Bube quickly became notorious. Just like many other pieces of malware, it was installed in the system when the user visited an infected site, with the MHTML URL Processing Vulnerability (see http://secunia.com/advisories/11067/) being used to install it on unpatched machines.

The infector appended code to explorer.exe so that *Explorer* functioned as a Trojan downloader, downloading adware and Trojans. Once all adware and Trojan programs had been installed, an infected machine would be hosting about 200 infected files.

Bube also infected the copy of explorer.exe in %sysdir%\dllcache. This made removal difficult, and as the number of infected users rose, it became clear that a number of anti-malware applications were not able to disinfect explorer.exe.

Whoever wrote Bube produced a program which:

- anti-spyware applications could not disinfect
- could not be detected as abnormal by inspecting active processes due to the use of *Explorer*, which would display as a normal process
- would not alert some firewalls to the fact that explorer.exe, a trusted process, was downloading
- was very difficult for many anti-virus products to remove.

It's a little unexpected that malware with a mutex referring to *MTV*'s *Beavis and Butthead* would be so complex. But getting rid of the infection was a simple matter of terminating the process and running an anti-virus that was capable of disinfecting explorer.exe.

WHAT'S FRAUD GOT TO DO WITH IT?

The Bube case led us to the following conclusions:

- A major epidemic caused by this vector was not only very possible, but also likely.
- The creators of this type of malware would see to it that the next target file would be even more vital for *Windows*, and consequently more difficult to remove/disinfect automatically.

Our fears were realized with the introduction of the Virus.Win32.Nsag.a infectors. These started to become highly prevalent at the beginning of June this year.

At the moment, there are four major Nsag.a infectors: Trojan-Downloader.Win32.Agent.ns was first detected in the middle of May, with Trojan.Win32.Agent.eo, Agent.ev and Agent.ff being detected shortly after. These four pieces of malware have been modified very slightly by the authors in an attempt to evade detection. This is particularly noticeable in the cases of Trojan.Win32.Agent.eo, Agent.ev and Agent.ff which have been altered numerous times.

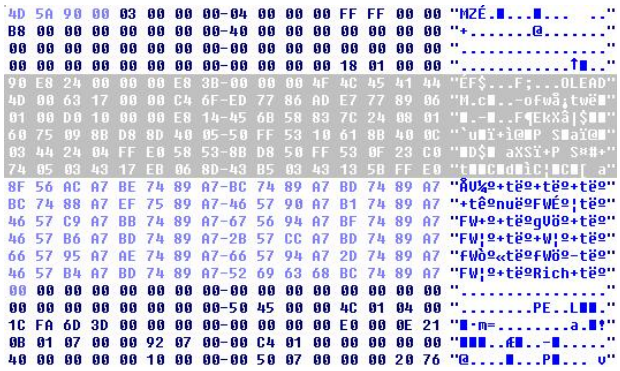
Trojan downloaders are used to install this malware in the system. These Trojan downloaders are installed either via exploits on web pages, or by other Trojan downloaders. The specific Trojan downloaders which installed the Nsag infectors also often download other Trojan programs, and something called *AntiVirus-Gold*, which describes itself as an anti-virus program.

At the end of July new infectors were found. These were similar to previous Trojans, but as some filenames differ we chose to call them Nsag.b infectors. Let's take a look at two different Trojans, one Nsag.a infector and one Nsag.b infector. They are both detected as Trojan.Win32.Agent.eo.

NSAG.A INFECTOR

When executed, the infector (normally named loader.exe) starts by dropping oleadm.dll into the system directory, this is the main Trojan component.

After dropping oleadm.dll, a file named oleadm32.dll is created, also in %sysdir%. This is a copy of the system's wininet.dll. The infector then starts to infect oleadm32.dll with Trojan code. It checks for the location of the HttpSendRequest function and then creates an entry point in the file header (and makes other corresponding changes), so that all calls to this function are transferred to oleadm32.dll, instead of wininet.dll.



The MZ header has been modified. The reference to oleadm is clear.

After infection oleadm.dll is loaded into the dropper's process. The .dll uses the mutex 'OLEADMUTEX' to ensure that only one instance of itself is running at any time.

TWO ORDERS PENDING

The dropper then makes entries to [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager] and [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager], where it uses the function 'PendingFileRenameOperations' for replacing and deleting files. This is quite a powerful function, as is shown by the fact that it is able to replace wininet.dll with another file.

The dropper also adds a line which will delete the copy of itself. After this has been done, the dropper adds '"AllowProtectedRenames"=dword:00000001' to the same keys in the registry. This value needs to be set in order to rename vital files. In operating systems such as 9x, which

don't support this function, the dropper uses good old WININIT.INI to achieve the same goals.

The infector then tries to download a file via HTTP from a website, but this file was unavailable at the time of writing.

Regardless of whether the download is successful, a file called wp.gif is created in the system directory. This is rather interesting as the .gif file is converted to a .bmp file. When the files are unpacked, there's a 95KB difference between them, but the difference in size between the compressed files is negligible.

WHAT'S PHISHING GOT TO DO WITH IT?

This image will be set as the new wallpaper. It warns that Trojan-Spy.HTML.Smitfraud.c has been detected. This is actually a *Kaspersky Anti-Virus* detection for a very popular phishing mail.

Additionally, the background colour will be changed to '1 2 172' to match the wallpaper's colour. NoDispBackgroundPage and NoDispAppeancePage values are set to 1 to try to prevent the user from changing the relevant settings back again.

The wallpaper set by Trojan.Win32.Agent.eo.

UNINSTALL

UninstIU.exe is dropped into %windir%. Although this file is detected as a Trojan, it actually reverses some of the changes made by the initial Agent.eo. It reverses only the registry changes which relate to the desktop and also deletes the 'SpyWare' entries which are created following the installation of uninstU.exe.

SPYWARE DETECTED

After uninstIU.exe is dropped, the following keys and values are added to the registry:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Internet Update]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Internet Update\{357A87ED-3E5D-437d-B334-DEB7EB4982A3}]

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{357A87ED-3E5D-437d-B334-DEB7EB4982A3}]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Internet Update]

DisplayName="Internet Update"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Internet Update]

UninstallString="uninstIU.exe"

'Internet Update' refers to the spyware that will be detected by the program oleadm.dll downloads.

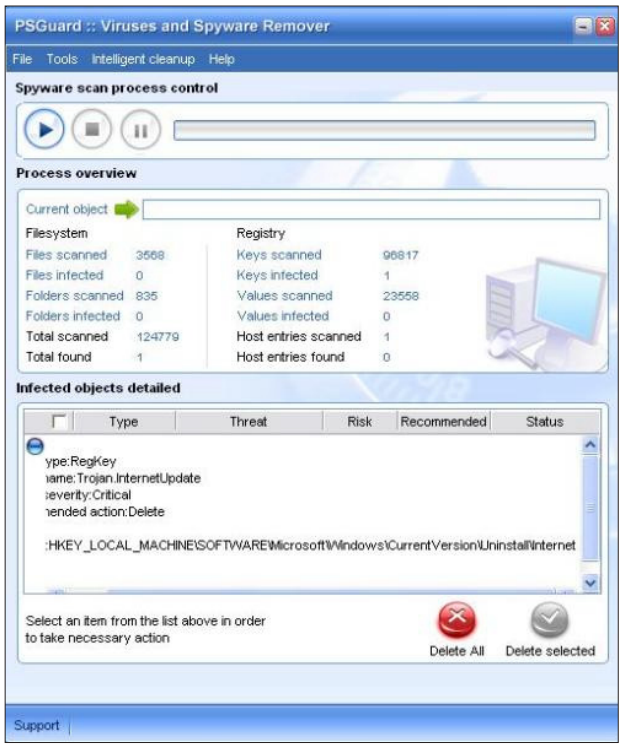
When these registry entries have been added, oleadm.dll launches a hidden instance of *Internet Explorer* which will download a 'virus and spyware remover' program called *PSGuard*. If it is not installed successfully, *Internet Explorer* will download the *PSGuard* installation file repeatedly until the process is successful.

The tempfile is created in the Windows directory and is called w[seven random characters].exe.

PSGuard will secretly install and register to start at boot. It detects the 'spyware' mentioned above as Trojan.InternetUpdate.

PAYLOAD

Oleadm.dll is designed with two goals in mind. One is spying on HTTP traffic. This is done very cleverly simply by hooking all calls to the HTTPGetRequest function. A



PSGuard detecting the registry key added by the Nsag infector.

bonus is that oleadm.dll will be loaded each time the system starts without any references to it besides those in the infected wininet.dll. This makes initial detection difficult.

The other goal is to install and promote *PSGuard*. But the biggest advantage is that wininet.dll is involved – this important *Windows* file is very hard to disinfect automatically without using PendingFileRenameOperations.

NSAG.B

Nsag.b (Agent.eo) is very similar to the Nsag.a package. Instead of oleadm.dll and oleadm32.dll, the files are called oleext.dll and oleext32.dll respectively. Apart from this, registry keys and internal filenames are the same, and the actions taken with *PSGuard* and uninstIU.exe are identical.

Instead of using a .bmp for wallpaper an .html file is used. A big red 'Warning!' blinks at the top of the screen, when the user is warned of infection. There's also a 'Click here' which leads to the *PSGuard* site.

This version of Agent.eo includes Trojan.Win32.Small.ev. Some Nsag.a infectors carry this Trojan as well. Its main payload is that it is displayed as a tray icon, claiming the system has been infected. When the icon is clicked, *Internet Explorer* will be opened to the *PSGuard* site.

Nsag.b infectors' wallpaper.

Small.ev will be registered to execute at system start.

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
intell32.exe="C:\%sysdir%\intell32.exe"

Perhaps the most interesting development in the Nsag case is that there has been no significant evolution apart from an increasingly aggressive approach, and more and more new pieces of malware which install it.

INCREASED AGGRESSION

It's interesting to note that the first Nsag infector, Trojan-Downloader.Win32.Agent.ns, was much less aggressive in its promotion of *PSGuard* than later infectors. It did not have the 'taskbar trojan', nor did it download *PSGuard* automatically.

The user was presented with a pop-up which asked if the system should be checked for viruses and spyware. If the user clicked 'yes', *PSGuard* would be downloaded, and the download process was clearly visible to the user. Additionally, in comparison with later variants, its wallpaper was not particularly eye-catching.

The wallpaper set by Trojan-Downloader.Win32.Agent.ns.

TO INFECT OR NOT TO INFECT?

One major question comes to mind when discussing Implinker, Bube and Nsag: are we talking about viruses or Trojans?

The problem, more or less, is that this type of malware can be viewed from different angles. Let's look at the infector components first. These 'special target infectors', as I've dubbed them for the time being, infect the target with code which is not able to replicate.

Perhaps this type of behaviour is comparable to what you get when you put a black sock in with your white laundry. The white laundry gets 'infected' by the black sock, but the 'infected' whites won't 'infect' other clothes.

Let's take a look at the target components.

The target components are infected by the infector with code that is not designed to replicate; it is pure Trojan code. So can we classify these infected files as Trojans? No, the term Trojan implies that the file can't be disinfected (and is 100% malicious), while the samples we're dealing with can be disinfected.

The terms 'virus' and 'Trojan' don't really seem to fit in this context, so perhaps a new type of classification is in order.

I propose the term 'poison' – this type of malware is highly selective, just as poison can be selective, attacking very specific cells and structures. Additionally, malware classified as poison doesn't necessarily have to spread further, and objects it infects can be disinfected. The term seems to fit perfectly and given the likelihood that this type

of malware will become more and more popular, the time for a new classification seems ripe.

PSGUARD: AN ANTI-MALWARE APPLICATION?

As mentioned earlier, *PSGuard* is the software which the Nsag infectors aim to promote. Between the beginning of June and the beginning of August, the people behind *PSGuard* seem to have changed direction.

Firstly, the program was upgraded from v2 to v3. The major change seems to be a completely redesigned GUI. Luckily for the people who use this software, the upgrade meant that the update functionality was no longer impaired. Version 2 always encountered a 404 when trying to update.

Unfortunately, detection rates do not seem to have improved. The software was tested on some older Sober, Kelvir and Mytob variants, but all went undetected, even though detection of Kelvir is mentioned specifically on the *PSGuard* site.

But with the latest build of this software, the authors decided to alter the program's behaviour radically in comparison to earlier versions.

Version 3.3.0.1/3.3.0.0 (engine/update respectively) is not (yet) available for direct download from the *PSGuard* site; you have to update the downloadable package. This version considers its own presence on the system to be a critical risk while previous builds do not exhibit this behaviour.

When the user tries to remove malware which has been detected on the system by *PSGuard*, the program will ask the user to pay to register. If registration (and payment) is not completed, *PSGuard* will not delete the detected objects.

A DARKER SHADE OF GREY?

AntiVirus-Gold seems to be rather more aggressive than *PSGuard*. Trojan downloaders which download this program (e.g. Trojan-Downloader.Win32.Small.bdw) also download Trojans/hoaxes which state that the computer is infected with spyware.

When the user clicks on the message displayed by the Trojan the Internet browser is opened at the *AntiVirus-Gold* website. If the user opts to scan with *AntiVirus-Gold*, he will be told that the computer is infected with spyware, even if the machine is clean.

WHATWARE?

The anti-virus world is assisted by the changes that *PSGuard* has made. Previous versions/builds did not display any significant suspicious behaviour, except for the way it was being promoted. Certainly detection rates are not on a par with those of other products and the user has to pay up before cleaning the infected machine – but couldn't the same be said about some products with established names?

Anti-Virus Gold's infection message, without any detected threats.

The fact of the matter is that more and more of these 'light grey' products are surfacing. If we look exclusively at the code of these programs they shouldn't be detected at all. But the community wants anti-virus solutions to detect these programs.

A permanent solution needs to be found as soon as possible. One option would be a maintained Rogue/Suspect Anti-Spyware list, similar to Eric L. Howes' list. If a listed program was detected, users could be directed to the list, leaving them to decide whether or not to remove it manually.

WHAT NEXT?

Given the success of the different 'poisons' so far, it's safe to say that we will see more of these infections in the future.

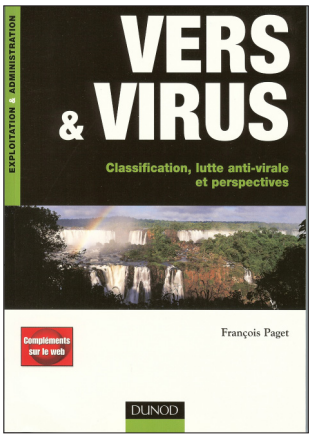
So far, such threats have revealed a number of anti-malware programs with removal problems. Detection and disinfection therefore clearly need to be improved to stand a chance of counteracting the next generation of 'poisons'. The search for vital (infectable) system files shows that new versions will undoubtedly be more difficult to remove.

Aggressive promotion of such 'light grey' software has brought unwanted attention from those in the security industry, and made the community as a whole more aware of such issues. It seems that programs like *PSGuard* and *AntiVirus-Gold* may have dug their own grave in using malware to promote their programs. It remains to be seen what other grey clouds are gathering on the horizon.

BOOK REVIEW

VERS & VIRUS

Eddy Willems
NOXS and EICAR, Belgium



Title: Vers & Virus
Author: François Paget
Language: French
Publisher: Dunod 2005
ISBN: 2 10 008311 2

There have been many useful and informative books written about viruses in English. However, during a recent visit to Paris it occurred to me that I couldn't find a single good book about viruses that was written in French.

L'AUTEUR

During the same trip I met with my friend François Paget, a well respected anti-virus expert who has been working in the anti-virus industry for around 14 years.

François is one of the founders of *McAfee*'s AVERT group (Anti Virus and Vulnerability Emergency Response Team). He is also a long-standing member of EICAR and has been a WildList reporter in France since the start of the WildList. François is the person the French media contact when they need information or a comment on a new virus outbreak or malware attack. During our meeting he revealed that he had just written a new book – in his native French – which would be released one week later. I decided to buy a copy.

QUELQUE CHOSE POUR CHACUN

The book contains over 300 pages of virus information and is divided into 10 chapters. I felt that it had something for everyone – this book will help even non-specialist readers understand the virus-related security issues they encounter in their day-to-day work and it contains valuable information for IT technicians and managers.

The opening chapter is dedicated to definitions of all virus-related matters. Although these definitions are broad, they are illustrated with many examples, and the combination of the definitions and the examples provides the reader with an excellent overall picture.

The second chapter was my favourite: the history of viruses, worms and other malware. This chapter also covers some of the history of the anti-virus industry. For example, there is a mention of the start of *Virus Bulletin* in July 1989 and even a reference to the original connection between EICAR and CARO – something not many people know about these days. The history section covers events as far as the end of 2004.

Chapter 3 gives an overview of viruses catalogued by infection method, type and functionality. The next four chapters provide a more detailed look at all the viruses described in Chapter 3. The information here is set out in a clear and not excessively technical manner, thus making the book accessible for all.

Near the end of the book is an overview of anti-virus programs. The descriptions and accompanying tables are quite comprehensive. François also gives the reader suggestions as to how to go about selecting the right protection for their company. For me, though, this part of the book seems too theoretical. Having a long career as an IT security consultant behind me, I felt that this could have been written from a more practical angle. However, a description of the impact of virus outbreaks and an estimate of the financial damage caused by some virus attacks boosts this chapter significantly.

The final chapter draws some conclusions and looks at the evolution of viruses. Again, the information is well presented and backed up with plenty of diagrams and charts. Indeed charts are well used throughout the book, and the book is very logically structured with clear figures and tables. François has also included a number of notes throughout the book, providing links to relevant Internet sites.

À MON AVIS

In my opinion François has done a very good job and I believe this book is a must-have for anybody who works with or is interested in 'viruses and worms' (the translation of the title). If you understand French, buy this book – you will not be disappointed. If you don't understand French, buy it as well – it could be the start of your new French language course!

As a Belgian I feel lucky to have been taught to speak and understand a number of different languages. I hope that eventually this book will be translated into English, as its style is refreshingly different from that of any other books on the subject and it will, inevitably, gain a wider audience in English.

I will certainly be adding *Vers & Virus* to my expanding library of security-related books. At this rate I will need to open some form of public library, as the supply of high quality anti-virus and security-related books seems to be never ending!

COMPARATIVE REVIEW

WINDOWS 2003 ADVANCED SERVER

Matt Ham

With *Windows Longhorn* now renamed *Windows Vista*, and still not expected for years, *Windows 2003 Server* remains the most recent server platform at the moment and for the foreseeable future. Having been in production for several years now, I expected the tests to progress easily on this occasion, since mature platforms tend to be less prone to problems. In the event, however, a host of problems were encountered. Some of these were due to the efficiency of the products, though rather more were the result of questionable design decisions.

TEST SETS

The products included in this month's review were required to have publication dates no later than 31 August 2005 (both for the product itself and any database updates). The test sets were aligned with the most recent WildList published at the time, which was the June 2005 edition.

As expected, the bulk of additions to the test sets were W32/Mytob variants. This worm was of note more for its vast number of variants than the overwhelming success of any particular specimen – over 100 variants were added to the test sets. The majority of additional samples within the WildList (and added to the In the Wild [ItW] test set) were worms of one sort or another.

With the addition of the horde of W32/Mytob variants to the test sets, one feature of the scanners which would be of particular interest was their ability to use efficient generic detection techniques. All in all, however, there were no great challenges in terms of detection.

As a special note, when performing throughput tests on the zipped clean sets, most products were set up so as to detect within archives in their default state. The other products were activated for archive scanning during these tests alone. The products where archives are not scanned by default are those produced by *AhnLab*, *Eset*, *McAfee*, *Sophos* and *VirusBuster*.

AhnLab V3Net 6.0 2005.08.31.10

ItW Overall	100.00%	**Macro**	98.97%
ItW Overall (o/a)	100.00%	**Standard**	90.61%
ItW File	100.00%	**Polymorphic**	46.52%

The only major problem encountered with *AhnLab*'s offering was with the logs produced during on-demand scanning. These note only the file name on a single line, rather than the full path, thus making analysis lengthy. However, this problem does not affect detection rate and is likely to be of little relevance for most users. Of much more importance are the matters of detection and false positives, both areas where *V3Net* performed sufficiently well to be awarded a VB 100%.

Alwil avast! 4.6.497

ItW Overall	100.00%	**Macro**	99.56%
ItW Overall (o/a)	100.00%	**Standard**	99.38%
ItW File	100.00%	**Polymorphic**	93.57%

With absolutely no problems or outstanding issues in its operation, *avast!* is destined for a rather uneventful write-up in this review. A VB 100% award will, one hopes, go some way towards making up for the lack of discussion concerning the product.

Authentium Command AntiVirus 4.93.0

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.72%
ItW File	100.00%	**Polymorphic**	100.00%

Again, the performance of *Command AntiVirus* produced nothing to comment on other than the full detection of viruses in the ItW set and the lack of false positives. Instead I will content myself with congratulating *Authentium* on achieving a further VB 100% for its collection.

Avira Avira for Windows Server 1

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	100.00%
ItW File	100.00%	**Polymorphic**	100.00%

Having detected all samples in all of the test sets in the last *Windows* review, *Avira* will be pleased to have repeated the performance on this occasion. The fact that false positives are counted only in the non-archived clean test sets turned out to be fortuitous for *Avira*, since one clean archive was declared to contain a sample of W32/Fosforo.

Scanning was otherwise a little slow but uneventful and a VB 100% award is thus winging its way to *Avira*'s headquarters.

CA eTrust Antivirus (InoculateIT engine) 7.1.192 23.70.24

ItW Overall	100.00%	**Macro**	99.90%
ItW Overall (o/a)	100.00%	**Standard**	99.61%
ItW File	100.00%	**Polymorphic**	99.89%

eTrust AntiVirus is provided with two scanning engines which can be exchanged at will: one can be used for on-access and the other for on-demand scanning if so desired. The *InoculateIT* engine is not activated by default, though, and is thus not eligible for a VB 100% award. It did, however, detect all samples in the wild, with no false positives.

CA eTrust Antivirus (default Vet engine) 7.1.192 11.9.9371

ItW Overall	100.00%	**Macro**	99.82%
ItW Overall (o/a)	100.00%	**Standard**	99.84%
ItW File	100.00%	**Polymorphic**	99.95%

The *Vet* engine in the *eTrust* product performed slightly better in terms of detection than its optional counterpart, while speed tests produced similar results. Customers should therefore find little to complain about over the choice of default engine. Likewise, *CA*'s developers will be unlikely to complain at receiving a VB 100% award for their efforts.

CA Vet Anti-Virus 10.67.0.0 11.9.1.0 9371

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.96%
ItW File	100.00%	**Polymorphic**	99.95%

The strangest thing to happen while testing *Vet* was the production, during the installation procedure, of a dialog which read 'Should not see me' while the machine was rebooting. That apart, detection and false positives were much the same here as when the engine was tested in its *eTrust* incarnation. A second VB 100% for a product based on *Vet*'s engine is the result.

CAT Quick Heal 2006 8.00

ItW Overall	99.97%	**Macro**	98.27%
ItW Overall (o/a)	100.00%	**Standard**	96.12%
ItW File	99.97%	**Polymorphic**	96.23%

Quick Heal has established itself in *VB*'s tests as a reliable regular which tends to produce no major problems in testing. I appreciated this more than usual on this occasion, since I managed to lose my initial results for *Quick Heal* and was forced to repeat the tests. The overall result was identical, with a VB 100% narrowly missed on both occasions. The offending file was a .EML sample of W32/Nimda.A, missed on demand.

Dr.Web Dr.Web 4.33.0.08190

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	100.00%
ItW File	100.00%	**Polymorphic**	100.00%

Dr.Web's detection rates have always been high, with a handful of misses in the last few tests being attributable to optimization of older virus detections. On this occasion the optimizations were clearly working well, since all samples were detected in all test sets. A continuing irritation is this product's on-access scanner, which although still requiring a reboot for any configuration changes, no longer announces this fact. Irritation aside, a VB 100% is well deserved by the product.

Eset NOD32 1.1207

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	100.00%
ItW File	100.00%	**Polymorphic**	100.00%

NOD32 has a strong history of detecting all infected files, with only a few minor deviations over the years. Yet again, no infected samples were missed across this month's test sets. A VB 100% award for *Eset* is the predictable result.

Fortinet FortiClient 2.0.110

ItW Overall	100.00%	**Macro**	99.39%
ItW Overall (o/a)	100.00%	**Standard**	98.84%
ItW File	100.00%	**Polymorphic**	97.04%

Fortinet's product is beginning to become a familiar subject in *VB*'s tests and its scanning results reflect this, with further improvements likely in the future. A VB 100% is awarded to *FortiClient* – which is also starting to become a regular result for the product.

On-demand tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
AhnLab V3Net	0	100.00%	0	100.00%	100.00%	47	98.97%	8834	46.52%	191	90.61%
Alwil avast!	0	100.00%	0	100.00%	100.00%	18	99.56%	113	93.57%	14	99.38%
Authentium Command	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	2	99.72%
Avira Avira	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
CA eTrust Antivirus (I)	0	100.00%	0	100.00%	100.00%	4	99.90%	1	99.89%	3	99.61%
CA eTrust Antivirus (V)	0	100.00%	0	100.00%	100.00%	12	99.82%	1	99.95%	3	99.84%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.95%	1	99.96%
CAT Quick Heal	1	99.97%	0	100.00%	99.97%	71	98.27%	317	96.23%	106	96.12%
Dr.Web Dr.Web	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Fortinet FortiClient	0	100.00%	0	100.00%	100.00%	31	99.39%	73	97.04%	38	98.84%
FRISK F-Prot Antivirus	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	2	99.72%
F-Secure Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	1	99.98%
GDATA AntiVirusKit	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Grisoft AVG	0	100.00%	0	100.00%	100.00%	0	100.00%	257	85.97%	27	98.56%
H+BEDV AntiVir	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Hauri ViRobot	0	100.00%	0	100.00%	100.00%	12	99.71%	9	99.76%	15	99.17%
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
McAfee VirusScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
MicroWorld eScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	0	100.00%	180	91.24%	8	99.62%
SOFTWIN BitDefender	0	100.00%	0	100.00%	100.00%	34	99.12%	5	99.78%	17	99.27%
Sophos Anti-Virus	1	99.84%	0	100.00%	99.84%	8	99.80%	0	100.00%	15	99.30%
Symantec SAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Trend Micro Server Protect	0	100.00%	0	100.00%	100.00%	0	100.00%	215	95.77%	6	99.39%
UNA UNA	3	99.53%	0	100.00%	99.53%	1891	55.06%	13008	24.40%	433	80.43%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	7	99.88%	171	92.29%	28	98.88%

FRISK F-Prot AntiVirus 3.16c

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.72%
ItW File	100.00%	**Polymorphic**	100.00%

Unusually, several more files were missed by *F-Prot* while scanning on access than were missed on demand. *FRISK*'s development team will no doubt be looking into this, although the problems did not occur in the ItW test sets, rather among very much older samples. Therefore, with no

false positives generated, a VB 100% makes its way to Iceland for *F-Prot*.

F-Secure Anti-Virus 5.50 11110

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.98%
ItW File	100.00%	**Polymorphic**	100.00%

F-Secure's product has had a number of uncharacteristic non-detections in some recent tests, but the product's detection rate returned to its usual high levels in this test, and with no false positives a VB 100% is the result.

GDATA AntiVirusKit 15.0.5 16.230

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	100.00%
ItW File	100.00%	**Polymorphic**	100.00%

With its combination of two engines, *AVK* has sometimes seemed slightly slow while scanning, though on this occasion speed problems were comparatively non-existent. The engine combination has also traditionally paid off with good detection rates and in this there was no change – all infected files being detected in all test sets. With no false positives, the product qualified easily for a VB 100%.

Grisoft AVG Anti-Virus 7.00 344

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	98.56%
ItW File	100.00%	**Polymorphic**	85.97%

Unfortunately *AVG* generated one false positive while scanning the clean set this month. Despite good performance in all the detection-based tests this was sufficient to prevent *Grisoft*'s product from achieving a VB 100% this time.

H+BEDV AntiVir 6.31.1.0

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	100.00%
ItW File	100.00%	**Polymorphic**	100.00%

Since *AntiVir* is all but identical to *Avira*, it came as no great surprise that the scanning results for the two products were identical – all infections were detected as such. Scanning speeds were also very similar, with differences easily attributable to those induced by background OS activity. Like its twin product, therefore, *AntiVir* gains a VB 100% award.

Hauri ViRobot 2005-08-24.00

ItW Overall	100.00%	**Macro**	99.71%
ItW Overall (o/a)	100.00%	**Standard**	99.17%
ItW File	100.00%	**Polymorphic**	99.76%

ViRobot started the testing process disappointingly, with three false positives being picked up in the clean set. The scanning of infected files was, if anything, more frustrating, since numerous files took well over a minute to be scanned. Scanning of the test set rapidly became slower during the process, with a virtual memory warning also occurring. This combination suggests that bad things are afoot. It also seemed that exclusions were totally non-functional, requiring the product to be fully uninstalled for any manipulation of infected files to occur. It was perhaps not surprising that many files were missed on access, presumably due to timeouts during scanning.

Kaspersky Anti-Virus 5.0.50.0

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	100.00%
ItW File	100.00%	**Polymorphic**	100.00%

The *Kaspersky* entry this month was a great surprise, consisting of a command line scanner rather than the usual GUI. An optional 'free' GUI was suggested to interface with this. However, the interface required a fully operational SQL database to be installed on the machine in question. While many servers will have SQL available, those which do not will require a new installation which is free neither in a financial sense nor in a manpower sense. Oddly enough the command line version seemed, by pure observation, to be slower at scanning infected files than the more usual GUI versions tested. All these oddities aside, *KAV* receives a VB 100% award.

McAfee VirusScan Enterprise 8.0.0 4400 4571

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	100.00%
ItW File	100.00%	**Polymorphic**	100.00%

The greatest surprise when testing *VirusScan* was noted during on-access scanning, where many samples of W32/Etap were not detected. It is possible that timeouts are responsible for this behaviour. W32/Etap is not a member of the ItW test set, however, so these obscure missed detections still allow *McAfee* to take home a VB 100% award for its pains.

MicroWorld eScan Win 1.27

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	100.00%
ItW File	100.00%	**Polymorphic**	100.00%

MicroWorld's *eScan* is part of a suite of, at least in some cases, rebadged products covering a variety of security functions. The anti-virus is provided by a version of *GDATA*'s *AVK*, which, as in its original form, detected all samples that passed its way. It will come as little surprise, therefore, that a VB 100% is awarded to *MicroWorld*.

Norman Virus Control 5.81

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.62%
ItW File	100.00%	**Polymorphic**	91.24%

Norman's product remains a solid workhorse, the only real complaint being that the scanning throughput is somewhat low. This is not the gravest of sins, however, and other areas of performance were sufficiently good that a VB 100% award is the result.

SOFTWIN BitDefender 2.0.172

ItW Overall	100.00%	**Macro**	99.12%
ItW Overall (o/a)	100.00%	**Standard**	99.27%
ItW File	100.00%	**Polymorphic**	99.78%

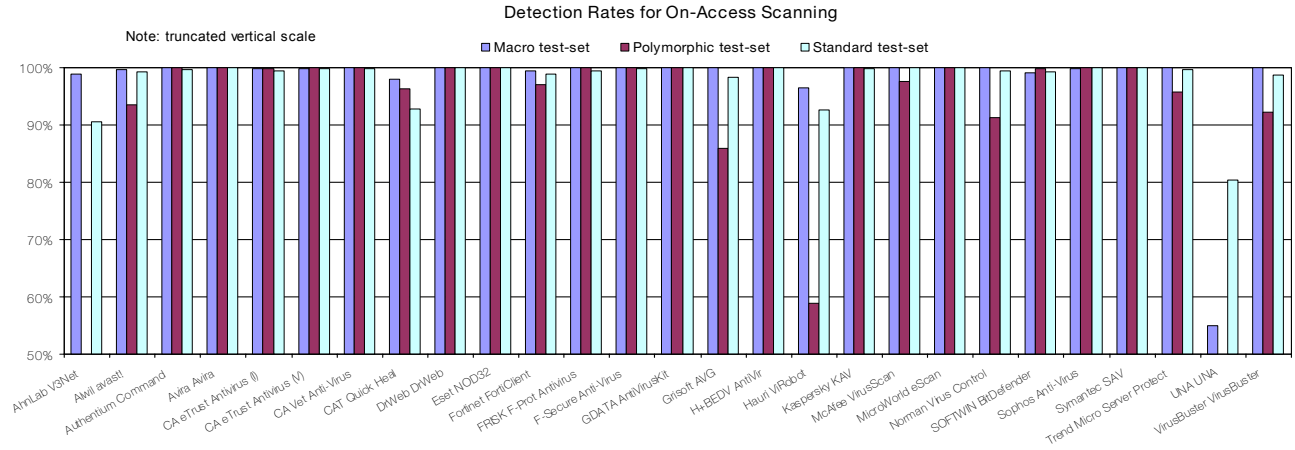
A notable change in this version of *BitDefender* is the interface, which is much more akin to MMC than a usual anti-virus GUI. This added some initial frustration to the process of scanning, though once the changes had become less unfamiliar, the frustration was substantially lessened. With novelty present in the interface, the underlying scanning capacity of the program remains similar. As a result a VB 100% award is appropriate.

Sophos Anti-Virus 5.0.5

ItW Overall	99.84%	**Macro**	99.80%
ItW Overall (o/a)	99.84%	**Standard**	99.30%
ItW File	99.84%	**Polymorphic**	100.00%

The new *Sophos* interface includes a quarantine function which has certain peculiarities. Having scanned the test sets on demand, the summary declared that there were over 20,000 items in the quarantine. A different area claimed that this total was 1,000, while inspecting the quarantine area itself showed that there were precisely zero files in that location.

There were also new occurrences during scanning. On access several files were detected on this occasion which have not been detected in any previous default scan. Unfortunately, both on access and on demand, a sample of W32/Sdbot was missed from the ItW test set, thus denying the product a VB 100% award.



On-access tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
AhnLab V3Net	0	100.00%	0	100.00%	100.00%	47	98.97%	8842	46.49%	191	90.61%
Alwil avast!	0	100.00%	0	100.00%	100.00%	18	99.56%	113	93.57%	17	99.18%
Authentium Command	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	5	99.58%
Avira Avira	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
CA eTrust Antivirus (I)	0	100.00%	0	100.00%	100.00%	4	99.90%	1	99.89%	4	99.51%
CA eTrust Antivirus (V)	0	100.00%	0	100.00%	100.00%	12	99.82%	1	99.95%	3	99.84%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	1	99.95%	3	99.84%
CAT Quick Heal	0	100.00%	0	100.00%	100.00%	82	98.04%	313	96.25%	156	92.72%
Dr.Web Dr.Web	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Fortinet FortiClient	0	100.00%	0	100.00%	100.00%	31	99.39%	73	97.04%	38	98.84%
FRISK F-Prot Antivirus	0	100.00%	0	100.00%	100.00%	0	100.00%	4	99.98%	8	99.40%
F-Secure Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	3	99.85%
GDATA AntiVirusKit	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Grisoft AVG	0	100.00%	0	100.00%	100.00%	3	99.93%	257	85.97%	30	98.41%
H+BEDV AntiVir	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Hauri ViRobot	0	100.00%	0	100.00%	100.00%	145	96.44%	5358	58.94%	112	92.61%
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	2	99.88%
McAfee VirusScan	0	100.00%	0	100.00%	100.00%	0	100.00%	29	97.67%	0	100.00%
MicroWorld eScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	0	100.00%	180	91.24%	10	99.50%
SOFTWIN BitDefender	0	100.00%	0	100.00%	100.00%	34	99.12%	5	99.78%	17	99.27%
Sophos Anti-Virus	1	99.84%	0	100.00%	99.84%	8	99.80%	0	100.00%	0	100.00%
Symantec SAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Trend Micro Server Protect	0	100.00%	0	100.00%	100.00%	0	100.00%	215	95.77%	9	99.63%
UNA UNA	3	99.53%	0	100.00%	99.53%	1891	55.06%	13008	24.40%	433	80.43%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	0	100.00%	172	92.30%	30	98.64%

Symantec AntiVirus 10.0.0.359

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	100.00%
ItW File	100.00%	**Polymorphic**	100.00%

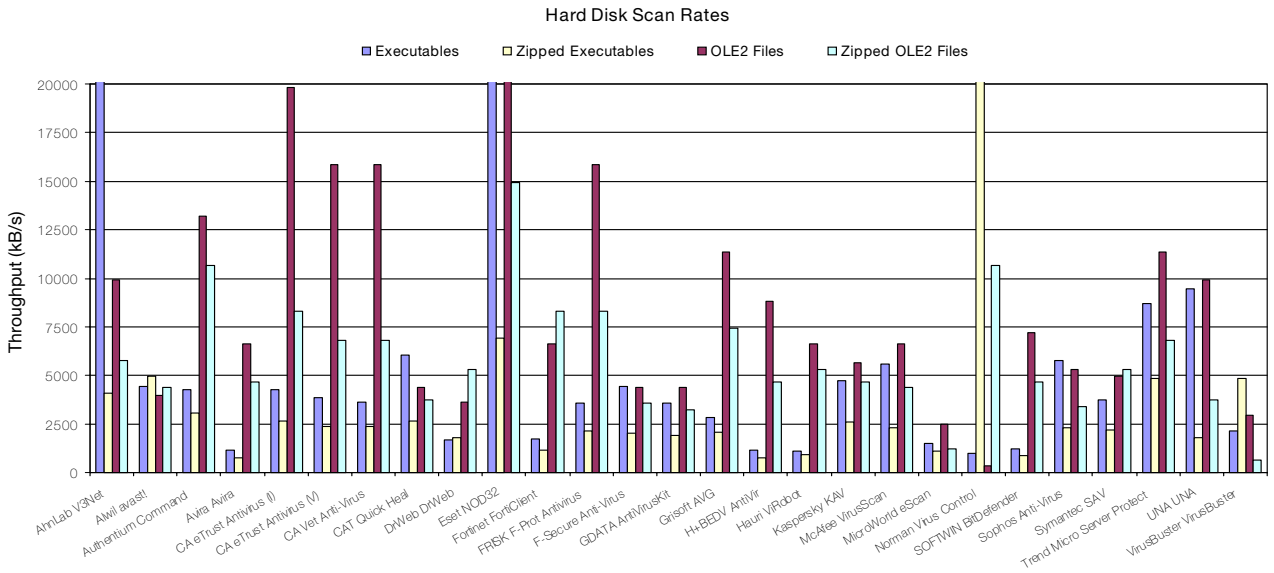
Symantec's new engine seemed to bring few major changes to the process of scanning, and indeed none whatsoever in the results of those scans. With all infected files detected, however, an improvement would be hard to obtain and a VB 100% award impossible to deny.

Hard Disk Scan Rate	Executables			OLE Files			Zipped Executables		Zipped OLE Files	
	Time (s)	Throughput (kB/s)	FPs [susp]	Time(s)	Throughput (kB/s)	FPs [susp]	Time (s)	Throughput (kB/s)	Time(s)	Throughput (kB/s)
AhnLab V3Net	26.0	21035.9		8	9916.7		39	4087.6	13	5739.0
Alwil avast!	123.0	4446.6		20	3966.7		32	4981.8	17	4388.7
Authentium Command	129.0	4239.8		6	13222.3		52	3065.7	7	10658.2
Avira Avira	465.0	1176.2		12	6611.1		221	721.3	16	4663.0
CA eTrust Antivirus (I)	128.0	4272.9		4	19833.4		60	2656.9	9	8289.7
CA eTrust Antivirus (V)	142.0	3851.6		5	15866.8		68	2344.4	11	6782.5
CA Vet Anti-Virus	150.0	3646.2		5	15866.8		68	2344.4	11	6782.5
CAT Quick Heal	90.0	6077.0		18	4407.4		60	2656.9	20	3730.4
DrWeb DrWeb	325.0	1682.9		22	3606.1		90	1771.3	14	5329.1
Eset NOD32	27.0	20256.7		3	26444.6		23	6931.2	5	14921.5
Fortinet FortiClient	315.0	1736.3		12	6611.1		140	1138.7	9	8289.7
FRISK F-Prot Antivirus	154.0	3551.5		5	15866.8		74	2154.3	9	8289.7
F-Secure Anti-Virus	124.0	4410.7		18	4407.4		78	2043.8	21	3552.7
GDATA AntiVirusKit	152.0	3598.2		18	4407.4		85	1875.5	23	3243.8
Grisoft AVG	195.0	2804.8	1	7	11333.4		77	2070.3	10	7460.7
H+BEDV AntiVir	470.0	1163.7		9	8814.9		217	734.6	16	4663.0
Hauri ViRobot	506.0	1080.9	3	12	6611.1		172	926.8	14	5329.1
Kaspersky KAV	116.0	4714.9		14	5666.7		62	2571.2	16	4663.0
McAfee VirusScan	98.0	5580.9		12	6611.1		70	2277.4	17	4388.7
MicroWorld eScan	366.0	1494.4		32	2479.2		148	1077.1	62	1203.3
Norman Virus Control	545.0	1003.5		222	357.4		6	26569.4	7	10658.2
SOFTWIN BitDefender	460.0	1189.0		11	7212.2		189	843.5	16	4663.0
Sophos Anti-Virus	95.0	5757.2		15	5288.9		70	2277.4	22	3391.2
Symantec SAV	147.0	3720.6		16	4958.4		72	2214.1	14	5329.1
Trend Micro Server Protect	63.0	8681.5		7	11333.4		33	4830.8	11	6782.5
UNA UNA	58.0	9429.9		8	9916.7		88	1811.6	20	3730.4
VirusBuster VirusBuster	257.0	2128.1	2	27	2938.3		33	4830.8	120	621.7

Trend Micro Server Protect 5.58.0.1060 7.510-1002 2.811.00

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.39%
ItW File	100.00%	**Polymorphic**	95.77%

As has been the case with *Trend*'s server products for some time, *Server Protect* needed to be within a domain for installation. My main complaint, however, was with the log file, which seemed to be truncated to the point of uselessness. This was bypassed by setting the scanner to delete infected objects, rather than relying on parsed logs for detection calculations. *Server Protect* missed no ItW files and produced no false positives, therefore receives a VB 100%.



UNA UNA PRO 1.83 269

ItW Overall	99.53%	**Macro**	55.06%
ItW Overall (o/a)	99.53%	**Standard**	80.43%
ItW File	99.53%	**Polymorphic**	24.40%

The user interface of this product has changed slightly since the last time it was reviewed, offering an easier and more pleasant experience on this front. There was also an improvement in detection rates, although misses of ItW samples were still present, thus denying *UNA* a VB 100%.

VirusBuster VirusBuster 2005 5.0.175

ItW Overall	100.00%	**Macro**	99.88%
ItW Overall (o/a)	100.00%	**Standard**	98.88%
ItW File	100.00%	**Polymorphic**	92.29%

Unfortunately for *VirusBuster*, two false positives were noted in the clean test set and a VB 100% award was denied for this reason. *VirusBuster* is unusual in that it can use MMC as an interface for control. Control through MMC, however, seems not to allow the choice of areas to scan. A standard GUI is also available, with control here being irritatingly long-winded, but allowing the selection of scan areas.

CONCLUSION

For such a stable and standard platform it was something of a surprise that so many problems showed themselves during testing. The usual caveat applies: that our test scenarios tend to throw more infected files at the scanners than might be expected in the real world. In the case of a server-based scanner, however, the loads produced by our tests might very well be reproduced in the case of a major outbreak, and under such circumstances some of the products tested here would be worthless. Scanning files at a rate of less than one per minute is far too slow and a server crippled by the load of scanning infected objects will prove more of a frustration than a useful tool.

Apart from the cries of woe brought about by these technical problems, design decisions also took their toll on my sanity. In a disturbingly high percentage of the products, the interface has been substantially changed for the worse over the last year. The most common irritation was the length of time required to set up a scan, for example, of a single directory. However much the design gurus may suggest otherwise, it is counterproductive to spend several minutes producing a detailed scan setup for an object, which will never be used again. Certainly complex feature tweaking should be a possibility, but making it a necessity is fundamentally user-unfriendly.

Technical details

Test environment: Identical 1.6 GHz Intel Pentium machines with 512 MB RAM, 20 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy drive running *Windows Server 2003 Web Edition V5.2* Build 3790.

Virus test sets: Complete listings of the test sets used are at http://www.virusbtn.com/Comparatives/Win2K/2005/test_sets.html.

A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.

END NOTES & NEWS

The SophosLabs Malware Analysis Workshop will be held 4 October 2005. The course is aimed at IT security professionals who are responsible for implementing and maintaining IT security solutions, or who are involved in computer security research. For details see http://www.sophos.com/.

The 15th Virus Bulletin International Conference, VB2005, will take place 5–7 October 2005 in Dublin, Ireland. The programme for the three-day conference can be found on the *VB* website. For more information or to register online see http://www.virusbtn.com/.

Black Hat Japan (Briefings only) will be held 17–18 October 2005. See http://www.blackhat.com/.

RSA Europe 2005 will be held 17–19 October 2005 in Vienna, Austria. More information, including track sessions and speaker details are available from http://www.rsaconference.com/.

The 12th ACM Conference on Computer and Communications Security takes place 7–11 November 2005 in Alexandria, VA, USA. For full details including a list of accepted papers and online registration, see http://www.acm.org/sigs/sigsac/ccs.html.

The CSI 32nd Annual Computer Security Conference and Exhibition takes place 14–16 November 2005 in Washington, D.C. Topics covered include: awareness training and education, risk and audit, compliance and governance, critical issues, attacks and countermeasures, forensics, identity and access management, and working with developers. For full details see http://www.gocsi.com/.

WORM 2005 (the 3rd Workshop on Rapid Malcode) will take place 11 November 2005 in Fairfax, VA, USA. The workshop will provide a forum to bring together ideas, understanding and experiences bearing on the worm problem from a wide range of communities, including academia, industry and the government. For more details see http://www1.cs.columbia.edu/~angelos/worm05/.

The eighth Association of Anti-Virus Asia Researchers International Conference (AVAR 2005), takes place in Tianjin, China 17–18 November 2005. The theme of this year's conference will be 'Wired to Wireless, Hacker to Cybercriminal'. For details email avar2005@antivirus-china.org.cn or see http://aavar.org/.

Infosecurity USA will be held 6–8 December 2005 in New York, NY, USA. The conference will take place 6–8 December, with the accompanying exhibition running from 7–8 December. The full conference programme will be announced this month. For details see http://www.infosecurityevent.com/.

The inaugural AVIEN/AVIEWS conference will take place from 1100am to 4pm Eastern Standard Time on 18 January 2006 by webcast. The organisers are currently seeking submissions for the conference (see p.3). Details of how to register will be released and circulated on the AVIEN and AVIEWS forums in due course.

RSA Conference 2006 will be held 13–17 February 2006 in San Jose, CA, USA. An early bird reduced registration rate is available for those who register before 18 November 2005. For more details see http://2006.rsaconference.com/us/.

The 15th EICAR conference will take place from 29 April to 2 May 2006 in Hamburg, Germany. Authors are invited to submit full papers, abstracts and posters for the conference. The deadlines for submissions are as follows: non-academic papers (abstracts) 25 November 2005; academic papers (in full) 13 January 2006; poster presentations 24 February 2006. For more details, including the full call for papers, see http://conference.eicar.org/2006/.

The Seventh National Information Security Conference (NISC 7) will take place from 17–19 May 2006 at St. Andrews Bay Golf Resort & Spa, Scotland. Enquiries may be directed to tina.deighton@sapphire.net or via http://www.nisc.org.uk/ .

The Fourth International Workshop on Security In Information Systems, WOSIS-2006, will be held 23–24 May 2006 in Paphos, Cyprus in conjunction with the Eighth International Conference on Enterprise Information Systems ICEIS 2006. The workshop will present new developments, lessons learned from real world cases, and would provide the exchange of ideas and discussion on specific areas. For details see http://www.iceis.org/.

SUBSCRIPTION RATES

Subscription price for 1 year (12 issues) including first-class/airmail delivery: £195 (US$358)

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

S1 **NEWS & EVENTS**

S2 **BOOK REVIEW**
Ending Spam

S3 **FEATURE**
Trust and accountability

NEWS & EVENTS

IRISH SPAM CONVICTION

Ireland's first anti-spam conviction was made last month against a company whose marketing methods relied heavily on social engineering.

4's A Fortune Limited, a company which runs an online casino game, was convicted of sending unsolicited marketing messages to mobile phones. The method used to 'send' the messages was to make calls using an autodialler which would hang up after two rings, thus leaving the 'missed call' message on the recipient phone's screen. If the owner of the phone then dialled the number recorded in the missed calls list (to find out who had been trying to get in touch with them), they would hear a recorded message encouraging them to call a premium rate number and play the company's online casino game.

A total of 165,000 calls were made to customers of the mobile service provider *O2*, however the conviction was made on the basis of just five complaints, and as a result the company was fined a total of only €1,500 – €300 for each of the five complaints.

Although a spokesman for the Data Protection Commissioner's office said he felt the fine was appropriate in this case (since it was a first offence and the company cooperated at a fairly early stage), Ireland's Department of Communications is reported to be considering larger fines as well as prison sentences for those found to be in violation of the country's anti-spam regulations.

SPAM 'HOTLINE' FOR GERMAN USERS

German email users can now report spam directly to the Federation of German Consumer Organisations (*vzbv*), a non-governmental umbrella agency for 38 German consumer associations. Unsolicited emails can be forwarded directly to the organisation, where they will be reviewed in an attempt to determine their origin and, where appropriate, legal action will be initiated against the senders/their clients.

The agency hopes that its move to prosecute spammers will have a deterrent effect on other would-be spammers. The hotline is intended only for consumer use – corporate users can report spam to Germany's unfair competition watchdog.

CZECH SPAMMERS RECEIVE FINES

The Czech Office for Personal Data Protection (UOOU) has imposed its first fines for spamming offences.

Since the office first started to handle the issue of spamming 12 months ago, the UOOU has registered 656 complaints about spam. A spokeswoman for the office said that they had not anticipated the magnitude of the problem at the outset. The office has now issued four fines, the largest of which was for 160,000 Czech crowns (approx. £3,680). Complaints can be submitted to the UOOU at http://www.uoou.cz/spam.php3.

A GLOBAL VIEW

Maintainers of cartographic collections may be interested in a new map created by *Mailinator*, a company that provides disposable email addresses for use in web registrations. *Mailinator* has used the IP address data it collects from the one million spam messages it receives per day, together with *Google* maps, to come up with a live spam map showing exactly where the spam is coming from (or where the proxies are located). See http://mailinator.com/.

EVENTS

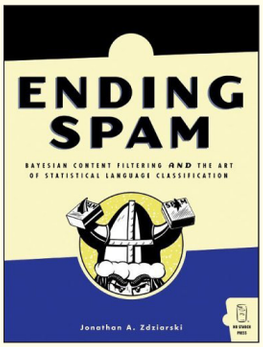
TREC 2005, the Text Retrieval Conference, takes place 15–18 November 2005 at NIST in Gaithersburg, MD, USA. For more details see http://trec.nist.gov/.

The third Conference on Email and Anti-Spam, CEAS 2006, will be held in July 2006 in Silicon Valley, USA. Interested parties should subscribe to a low-volume mailing list for details of the event; see http://www.ceas.cc/mailinglist.htm.

BOOK REVIEW

ENDING SPAM

John Graham-Cumming
The POPFile Project



Title: Ending Spam
Author: Jonathan A. Zdziarski
Publisher: No Starch Press
ISBN: 1593270526

Ever since Paul Graham posted his renowned 'A Plan for Spam' web page, the web has been the publishing medium of choice for the hackers behind the annual Spam Conference at MIT.

Jonathan Zdziarski has done an adequate job of summarizing this collective web wisdom in his book *Ending Spam*. The book covers all the major thoughts of the open source Bayesian spam-filtering community, but is marred by the author's strong biases and missing explanations. Despite those problems the book is accessible to any reader with a computer science background and is essential reading for anyone wanting to understand Bayesian spam filtering.

The book opens with a redundant chapter recounting the history of spam from 1978 through 2005 and is followed by the oddly titled Chapter 2, 'Historical approaches to fighting spam', which describes an almost random collection of old and new spam fighting techniques, yet omits others. Techniques such as greylisting and fuzzy hashes (e.g. DCC) are not mentioned. The omission of fuzzy hashing is odd because the chapter includes a discussion of 'collaborative filtering'.

Chapter 3 provides an overview of a statistical filter's building blocks and introduces terminology that the author has popularized through his *dspam* project. There are two big disappointments here: first, there is no explanation of Bayes Theorem (just a couple of paragraphs that give a general description), and second, the section on 'understanding accuracy' promotes the use of a single 'accuracy' percentage as a way of comparing spam filters. It's a pity that the author provides no discussion of false positives and false negatives, nor does he point out that users care much more about false positives than false negatives and that a single percentage accuracy figure can disguise a false positive problem.

It is also in Chapter 3 that the author's open source axe to grind becomes obvious with the bizarre claim that 'Most manufacturers are a bit concerned with the idea of deploying a box that learns on its own. Their customers will no longer need annual contracts for nightly updates [of rule sets] or as many software upgrades, which certainly puts them in a precarious financial position'. That's probably news to the folks at *Proofpoint* (amongst others).

Chapter 4 describes in detail the operation of a statistical spam filter with a clearly worked example. In addition, the chapter explains the various mathematical techniques used in a number of filters (starting with Paul Graham's original proposal and going through to the Inverse Chi-square test proposed by Gary Robinson).

Chapter 5 points out that messages need to be decoded into a readable form for a statistical filter to work. It brushes very lightly over quoted-printable and base 64 encoding without describing how they work, and talks about some HTML encodings used by spammers to disguise messages. There's also a small, odd section entitled 'Message actualization' that reads like an implementation detail of *dspam*.

Chapter 6 talks about message tokenization with an interesting discussion of what constitutes a word and how, for example, words in the subject line of an email are treated differently from the same words appearing in the body. The inadequate section on 'internationalization' reveals the author's anglophone-centric world view with the statement: 'The issue of foreign languages will eventually require a solution' – I suggest ignoring this bit.

Chapter 7 describes the tricks that spammers use to attempt to subvert spam filters. There's an excellent discussion of why these tricks don't work and the author busts through a few myths about statistical spam filtering with clear explanations and examples of actual spammer tricks.

Chapters 8 and 9 could have been omitted. Chapter 8 describes a number of database solutions and their relative merits with respect to spam filtering; chapter 9 outlines some of the issues that a spam filter author faces when their filter is used in a large organization.

The chapters in Part III are the most lucid in the book. They draw heavily on the author's previous writing and cover spam filter testing (Chapter 10), tokenization methods other than 'split the message into words' (Chapter 11), removing useless features from a message to improve accuracy (Chapter 13) and some examples of how Bayesian spam filters can collaborate (Chapter 14). Chapter 12 provides an interesting look at a non-Bayesian spam filtering technique using Hidden Markov models.

An appendix highlights five spam fighters: *POPFile* (for which I was interviewed), *SpamProbe*, *TarProxy*, *dspam* and *CRM114*.

Overall this is a book worth buying. If you want to know how Bayesian spam filters work then open the book at Chapter 3; if you already know how they work then jump straight to Chapter 10.

FEATURE

TRUST AND ACCOUNTABILITY

Des Cahill
Habeas, USA

The email ecosystem – which includes not only email vendors, but also any company that utilizes email to conduct its business – is under attack from spammers, phishers, hackers, spoofers and other criminals. The response thus far from the email industry (those vendors that provide the infrastructure for email) has been to concentrate on blocking the bad stuff. A reasonable approach initially, but one that has caused two big problems:

1. Filtering out the bad stuff often results in legitimate email being filtered out mistakenly. Some studies have shown that as much as 20 per cent of opt-in mail does not reach recipients' inboxes. It is a real headache for a bank when it can't send an email to its customer containing the words 'mortgage', 'free checking' or 'new low rate' for fear of being blocked by email filters.
2. Receivers pay a heavy price to block the bad stuff. Content filter-based anti-spam measures can be applied only once a receiver takes delivery of the message. So if, as some studies suggest, 70–80 per cent of email volume is spam, that's a lot of disk space, server CPU cycles, network bandwidth and anti-spam software licences that must be paid for by receivers.

To address these two issues, sender authentication has risen in prominence recently as the next phase in the evolving fight against spammers. Sender authentication operates much like an email passport. It allows the receiver of an email message (such as an ISP) to verify quickly that a given email really has originated from the sender's domain. Unfortunately, just as in the real world, it turns out that the bad guys can get passports, too.

Indeed, spammers have been enthusiastic in their adoption of sender authentication. While authentication does allow receivers of email to hold the spammer's domain accountable for bad behaviour – and to block them or otherwise interdict their tactics – we also know that spammers are likely to abandon one domain quickly and jump to another new one because a new domain can be acquired rapidly and inexpensively.

Does this mean that authentication is unnecessary or ill-advised? No, establishing accountability for a legitimate company's 'email sending identity' is important, irrespective of spammer behaviour. Certainly, spammers will adapt and try new tactics to subvert authentication (they always do), but using authentication to establish the identity of legitimate senders prevents spammers from hijacking a company's identity while forcing new costs and barriers on them.

Habeas encourages its customers, as part of its best practices standards, to adopt the path-based Sender-ID/SPF authentication standard immediately, and to begin planning for future adoption of DKIM, a robust, PKI-based authentication standard that is currently in the final stages of definition.

These standards are tools that enable legitimate senders to improve their email reputation and delivery performance in three critical ways:

1. Help protect your email domain and brand from being damaged by spammers, phishers and hackers sending out illicit email which purports to be from you.
2. Identify your company as a credible member of the email community by establishing your ownership and accountability for your sent email.
3. Avoid negative treatment from email receivers who are starting to view the lack of ability to authenticate an email as a reason to view the email as possibly spam.

CAN AUTHENTICATION OFFER A REMEDY TO SPAM?

Yes authentication can help, but it is clear that it is not a panacea to cure all forms of spam. Adopting authentication is the first step an email sender can take to establish itself as a member of the email community that can be held accountable for its actions. By adopting authentication, a company indicates that it is willing to tie its domain (its online identity) to its email practices – and resulting email performance (e.g. delivery rates, complaints, blacklisting, etc.).

Adopting authentication can result in more favourable treatment for email by some receivers, while some email providers, such as *Hotmail*, are now treating non-authenticated mail less favourably (i.e. it will indicate within the *Hotmail* user interface to consumers that the domain of the sender could not be authenticated). It is likely that other ISPs will begin to adopt similar approaches.

There is also an additional benefit to a company that adopts email authentication across all its domains: it makes it easy

for others to identify email which purports to be from that company, but is in fact email from a spammer, phisher or hacker.

Authentication allows a company to protect its brand and reputation from the actions of others who are pretending to be sending mail from that company – something that, technically, is trivial to do. If the *Acme Widget* company, a reputable vendor of widgets and responsible sender of email, uses an email authentication technology such as Sender-ID or SPF to identify all of the outbound emails from acmewidget.com, then receivers of email can easily identify any mail purporting to be from acmewidget.com but which in fact was sent by a spammer in China or a zombie PC in Baltimore.

AUTHENTICATION: NECESSARY BUT INSUFFICIENT

So authentication tells us who sent the mail. That's good, but it's not enough. For example, let's say your ISP gets an email from xyz.com, a company that uses authentication: your ISP knows the email has actually come from xyz.com. So the email should be put in your inbox – right?

Well, maybe. Your ISP still needs to understand if xyz.com is a reputable mailer or a nasty spammer in order to determine whether to deliver it to you. And if there is no information available on xyz.com's reputation as a mailer, then your ISP needs to put your message from xyz.com through the expensive and inaccurate spam-filtering process, analysing every word of the message for potential signs of spam. Clearly, authentication alone doesn't determine what is legitimate mail or what is spam. It just helps you know that what appears to be the sending domain is indeed the sending domain.

Authentication needs to work hand-in-hand with another new technology that is the 'next big thing' within the fabric of email. It's a rapidly emerging area the industry is calling 'email certification and reputation services'. The idea is to develop an email infrastructure for identifying and rating the trustworthiness of mailers.

If my ISP knows that xyz.com has a reputation as a legitimate mailer, from whom recipients generally want to receive emails, then my ISP can deliver the email straight to my inbox. The combination of authentication and reputation services is a much more efficient way to address the spam problem: rather than focusing on trying to stop the 80 per cent of mail that is spam, let's instead work on solutions to identify the 20 per cent of mail that people actually want.

Sender certification and reputation standards tell receivers whether the sender is known by the industry to be a reputable sender – that is, a trustworthy bearer of a valid email passport.

Email reputation services that certify senders as trustworthy (such as *Habeas* and *BondedSender*) work with legitimate senders to audit, improve, certify and monitor their email practices. Once a sender 'checks out' as a good citizen, *Habeas*, for example, adds the sender to its DNS whitelist of certified senders (known as the *Habeas SafeList*) that is used by ISPs including *Hotmail*, *Roadrunner*, *NetZero* and *Prodigy* to identify and deliver legitimate email from trustworthy senders. The sender now has a positive email reputation and is extremely motivated to ensure this reputation is maintained.

CERTIFIED EMAIL ENABLES BETTER EMAIL-HANDLING DECISIONS

Certified email unlocks some additional benefits. Receivers, such as ISPs and enterprises, can use reputation services such as DNS-based blacklists and whitelists to make better mail-handling decisions. An ISP using the *Habeas SafeList* now knows not only that the email came from xyz.com, but also that xyz.com conforms to a rigorous email best practices certification program and ongoing compliance monitoring.

For example, an ISP could decide to deliver 'transactional' email such as an airline ticket confirmation to the addressee immediately, while holding a high-volume email marketing campaign email for later in the day when there is less load on the system. This makes much more sense than blocking indiscriminately or throttling (inbound email delivery rate limiting) email from specific senders.

Better still, ISPs can make these email-handling decisions at the edge of their network – before the email is run through the expensive gauntlet of content filtering. If an email was sent by a sender with a poor reputation, it can be dropped right there. Conversely, if the sender checks out as a *bona fide* email citizen, it can be delivered without delay. Either way, the email doesn't need to be subjected to expensive and inaccurate content filtering. And this means a reduction in false-positives.

The war on spam can still be won. But the next phase in the war requires us to turn the tables on spammers. Authentication enables receivers and senders to shake hands and exchange business cards. The combination of certification and reputation enables receivers – and, ultimately, consumers – to know with whom they're really doing business.

Suddenly, because trust and accountable email practices are now the key determinants of delivery, the door can be shut on spammers, phishers and other criminals prowling the Internet.