FEBRUARY 2004

virus BULLETIN

The International Publication on Computer Virus Prevention, Recognition and Removal

CONTENTS

ISSN 0956-9979

IN THIS ISSUE

A NEW TREND IN VIRUS WRITING?

Following in the footsteps of W32/Bugbear.A, W32/Mimail.I and .J took the concern of identity theft to another level, producing a plausible-looking popup and web page and asking questions that are favoured security checks of many banks. Stuart Taylor asks: is there a criminal element entering virus writing?

page 11

TESTING TIMES

It's not just a product's ability to detect malware that is of vital importance to the user, but the speed with which the developer produces an update in outbreak situations. Andreas Marx puts AV response times to the test.

page 4

COMPARATIVE REVIEW

Matt Ham lines up the AV products for *Windows NT*.

page 12

Feb 2004 VIRUS BULLETIN 100% www.virusbtn.com

vb Spam supplement

This month: Anti-spam news and events, *Habeas* delivering the goods, ASRG summary.

'Until now, most business use of instant messaging has been of the "stealth" variety.'

Joe Licari
Sybari Software, USA

ARE YOUR NETWORKS SECURE?

In December 2003, I attended the Emerging Technology Showcase held in Scottsdale, Arizona. The event was designed to help companies define new business initiatives and select emerging technologies that help them adapt to their markets more effectively and profitably. At the conference I was prepared to present my views on emerging technologies. I was also prepared for a timely break from the burgeoning New York winter. However, I wasn't prepared for the high level of interest and buzz surrounding instant messaging and presence-awareness in the enterprise.

Seemingly overnight, there had been a change in attitude towards real-time collaboration and instant messaging (IM) applications – which are now being viewed as critical and effective communication vehicles for the enterprise. CIOs and their IT groups are evaluating and planning for the deployment of managed real-time collaboration applications in 2004.

Until now, most business use of IM has been of the 'stealth' variety – employees using public network (consumer) IM clients on an informal basis without the approval or knowledge of their IT departments. So why the recent business interest in IM? Instant messaging provides an easy way to communicate with colleagues who are not located in the same office, who may be travelling on business or may be working from home. Managers from any location can respond to instant messages with quick decisions. Presence-awareness allows each user to see the online status and availability of other colleagues on the system. Furthermore, IM frees users from the comparatively slow alternative of email, which may be bogged down by spam, delays and restrictions.

In spite of these benefits, many organizations have previously rejected the use of IM due to compliance requirements or justifiable concerns about security and policy breaches that might result from its unmanaged deployment. Other organizations simply allowed rogue IM clients to be used without any additional security, monitoring or IT management. Clearly, these are not permanent solutions.

Network administrators now have to contend with a new network access point for viruses and malicious code. Those in charge of protecting the corporate infrastructure need to have a clear understanding of the security risks presented by real-time communications. As an initial step, administrators are urged to perform a corporate audit to determine which IM services may already be running on clients within their organizations. Time and resources must be allocated to standardize on an enterprise solution that meets user demand while instituting appropriate security and policy management.

As with email in the late 1990s, administrators may choose to ignore the imminent virus vector and simply rely on perimeter AV protection at the desktop. But, of course, when virus attacks eventually discredited this strategy, organizations and AV vendors alike quickly demanded solutions for gateway and messaging servers. As a result, today's IT professionals require server-side solutions to protect against new malicious threats in their instant messaging environments. The provision of anti-virus and content filtering protection on real-time collaboration servers is the most efficient way to scan all IM traffic for viruses, worms, IM Trojans and other malicious code. It is also the ideal location to filter and block messages and attachments containing objectionable content.

My break from New York's winter weather conditions was all too fleeting. In contrast, the acceptance and growth of instant messaging and real-time collaboration in enterprise organizations appears to be long-lasting. By applying the prudent and diligent implementation of server-based security solutions, we can ensure that this will be a safe and productive medium resulting in greater communication and efficiency in our organizations.

Editor: Helen Martin
Technical Consultant: Matt Ham
Technical Editor: Morton Swimmer
Consulting Editors:
Nick FitzGerald, *Independent consultant, NZ*
Ian Whalley, *IBM Research, USA*
Richard Ford, *Florida Institute of Technology, USA*
Edward Wilding, *Data Genetics, UK*

NEWS

VB2004: CALL FOR PAPERS

Virus Bulletin is seeking submissions from those wishing to present at VB2004, the Fourteenth Virus Bulletin International Conference, which will take place 29 September to 1 October 2004 at the Fairmont Chicago, Illinois, USA. Abstracts of approximately 200 words must reach the Editor of *Virus Bulletin* (editor@virusbtn.com) no later than **31 March 2004**. For further details see http://www.virusbtn.com/.

DIVINE INTERVENTION

We all know how quickly time flies when we're having fun, or when there's a deadline looming, but a recent news report on the Asian news website *Channel NewsAsia* (http://www.channelnewsasia.com/) had us rushing to double-check our calendars to make sure we hadn't fast-forwarded to April 1st.

The site reports that, last month, a number of Japanese IT businesses and computer vendors gathered, along with their computers, at the Kansa Myojin shrine in downtown Toyko to partake in Shinto purification rituals and receive blessings to protect against computer viruses and hackers. According to *Channel NewsAsia*, many people in Japan feel that anti-virus software and security measures alone are simply not enough to protect against the increasing number of electronic threats, hence they are turning to more ancient traditions to ward off these modern evils.

We were relieved to learn that the spiritual rituals are being used to supplement anti-virus and other security solutions, rather than as an alternative. As figures quoted by the Japanese National Police Agency suggest that the nation's computer network currently sees a monthly average of 35,000 'cyber attacks', we look forward to reading reports of the resultant decline in incidents. Who knows, there may be a whole new *VB* conference stream for spiritual anti-virus protection methods next year …

WAITING, REFLECTING AND REMOVING

While young Romanian virus author Dan Dumitru Ciobanu awaited trial by a Romanian court last month for releasing a variant of W32/Blaster that reportedly infected just 27 machines, *Microsoft* was reflecting on the success of its removal tool for the original variant. The tool, the first of its kind to be provided by *Microsoft*, was released five months after the initial appearance of the worm, and was downloaded 1.4 million times (mainly automatically through Windows Update) during the first few hours of its availability.

Prevalence Table – December 2003

Virus	Type	Incidents	Reports
Win32/Opaserv	File	5376	29.40%
Win32/Mimail	File	3606	19.72%
Win32/Dumaru	File	2940	16.08%
Win32/Swen	File	1616	8.84%
Win32/Dupator	File	764	4.18%
Win32/Bugbear	File	709	3.88%
Win32/Klez	File	541	2.96%
Win32/Yaha	File	476	2.60%
Win32/Sober	File	475	2.60%
Win32/Gibe	File	397	2.17%
Win32/Sobig	File	382	2.09%
Win32/Frethem	File	181	0.99%
Win32/SirCam	File	114	0.62%
Win95/Spaces	File	83	0.45%
Win32/Deborm	File	59	0.32%
Win32/Nachi	File	54	0.30%
Win32/Spybot	File	46	0.25%
Win32/Magistr	File	44	0.24%
Win32/Fizzer	File	33	0.18%
Win32/Lovsan	File	33	0.18%
Win32/Torvil	File	33	0.18%
Win32/Pate	File	24	0.13%
WelcomB	Boot	21	0.11%
Win32/Gaobot	File	21	0.11%
Win32/Kriz	File	21	0.11%
Win95/Lorez	File	20	0.11%
Win32/Holar	File	17	0.09%
Win32/Parite	File	17	0.09%
Win32/Valla	File	17	0.09%
Win32/Funlove	File	15	0.08%
Redlof	Script	12	0.07%
Win32/Randex	File	12	0.07%
Others		137	0.75%
Total		18,286	100%

[1]The Prevalence Table includes a total of 137 reports across 53 further viruses. Readers are reminded that a complete listing is posted at http://www.virusbtn.com/Prevalence/.

FEATURE

OUTBREAK RESPONSE TIMES: PUTTING AV TO THE TEST

Andreas Marx
AV-Test.org, Germany

Most comparative reviews of anti-virus programs focus on the products' worm and virus detection rates. But an important aspect of anti-virus products is often overlooked: it is not merely 'malware detection' that is offered by the developer, but rather a service that promises to keep your PC virus-free. This service includes responding quickly in case of local or global malware outbreaks.

In May 2003 we set out to measure the reaction times of anti-virus companies in the case of new malware outbreaks. The results for the Win32/Fizzer.A (http://www.pcwelt.de/news/viren_bugs/31094/) and Win32/Bugbear.B (http://www.pcwelt.de/news/viren_bugs/31671/) outbreaks were reported in German computing magazine *PC-Welt*.

THE FIRST ATTEMPTS

At first, we waited until we heard about a new malware outbreak, then installed all AV products in our lab as quickly as possible and checked for product updates and detection of the malware. However, this process proved to be both rather hectic for the lab staff and fairly inaccurate.

Next we tried using *VMware GSX Server*, which allows a number of virtual PCs to be run at once (providing there is sufficient processor power and especially RAM). We were able to install all GUI anti-virus products on these virtual PCs (all running *Windows 98 SE* due to RAM limitations), but this system did not work very well. After 24 hours, the consoles of one or two products would usually have crashed, so we would have to restart the virtual PCs. Furthermore, it was not always easy to grab the downloaded and installed updates, and the *Windows* patch management did not work as it should. Of course, it was not only the host PC that needed to be updated with all available (security) patches, but the virtual PCs had to be updated, too, and restarted.

THE SOLUTION: SCRIPTS WITH WGET

Finally, we decided only to check for updates, download them and store them in an archive. We did not want to install and test them automatically, nor did we want to use the GUI or command-line products; we wanted to rely only on our own scripts.

The first prototype of a shell script running on *Debian Linux* with a CVS version of wget was ready at the end of October 2003. At this time, we implemented automatic checking of the updates of only about ten anti-virus products, but we encountered several problems straight away.

The script checks every five minutes for changes in the anti-virus update and program files on FTP and HTTP servers. As an example, the updates for *H+BEDV AntiVir* are always stored at http://www.antivir.de/dateien/antivir/fuse/fuse.zip. Using wget, we simply check the length of the file, its date and time stamp every five minutes. As soon as the file has changed we download the update, write information about the update to a log file and store a copy of this file in our archive. Unfortunately, fewer than half of the products are updated so simply.

Today, most products have incremental updates, but for testing purposes it is much easier to use the full definition files. This also makes the update download process much simpler, because there is no need to use complex scripts or additional programs to recreate the full definition files, only a simple wget.

Another issue is that some companies, for example *Symantec*, publish 'intelligent EXE updater files' almost daily (which are easy to monitor, because they are stored on a public FTP server), but updates for LiveUpdate (which is built into every *Symantec* tool) are published only once or twice a week. Therefore, we had to implement additional checks to make sure that we monitored the presence of new LiveUpdates as well.

TROUBLE MAKERS

Some companies, such as *Symantec* and *Computer Associates* use more than one FTP server to store update files. We found that these servers were not always synchronised, so it was possible that we would see different updates ('old' and 'new' ones) when connecting to different IP addresses. Unfortunately, work-arounds for this issue could lead to greater problems, so we were forced to live with these discrepancies (and sort them out later).

Sometimes we found that the date/time stamp of files had changed (for whatever reason) on the server, but the file itself remained the same length. This was particularly common with the regular definition files from *CA* and the beta definition files from *Panda* and *Symantec*. When this situation arose, we downloaded the file and made a check using 'cmp' (which is similar to file compare ('fc') on *Windows*-based systems) to determine whether the file had been changed (an MD5sum for both files would be an alternative way to check for differences in the files). If the files were different, the 'new' file was processed like a standard update, but if they were identical it was ignored.

A special situation was caused by *McAfee*'s beta definition files called DailyDats which are refreshed usually every hour and available as a ZIP file. The standard definitions like scan.dat are stored inside this file. Several times a day the time stamp of the files inside the ZIP will change, but the definitions remain unchanged – a result of the fact that they are freshly uploaded, even if the files themselves are unmodified. We did not want to store such files in our archives, therefore we implemented a quick check: if the size of the ZIP file was unchanged and only the time field of the included files had altered, we would ignore the update.

In the case of *Ikarus* or *Sophos* it was difficult to use wget to download all updates, due to the fact that the names of the files we needed to download were displayed inside an HTML file only and changed often. In this case, we used 'curl', combined with 'sed', which is a little more complex, but it worked well.

Not all servers have the same bandwidth. Some are quite slow, others are very fast. After observing that the script sometimes hung on servers for quite some time, we implemented a 'quick skip' in case a server was unreachable. Ten seconds did not work very well and 20 seconds was usually too long; we found that 15 seconds worked best as a time-out value.

Currently the system runs on a Pentium IV 2.4 GHz PC with 256 MB memory and 500 GB HDD space. This should be enough to store at least all the updates released over the course of one year – currently we are collecting about 500 to 750 MB updates every day. We do not have a backup system, but we are using two DSL lines from different providers.

COOPERATION WITH AV COMPANIES

We invited all the anti-virus companies we knew of to participate in this project (which is free of charge). We needed a login to password-protected websites with the virus definitions or program updates (which would not be shared with third parties, of course). Additionally, we needed licence keys or registrations for the programs so we could test them.

At the time of writing we check the updates of 20 anti-virus companies with 21 different engines and four beta definition files. Additionally, we check for updates of A2 (an anti-Trojan scanner developed by Andreas Haak) and *RAV* (*Reliable AV*), but since the *RAV* product is no longer sold we will no longer publish test results for this tool.

The invitation emails sent to several other anti-virus companies, including *Ahnlab* (*V3*), *Cybersoft* (*VFind*), *Eset* (*Nod32*), *Hauri* (*ViRobot*) and *Proland* (*Protector Plus*), went unanswered, but we hope to be able to welcome these companies to the list of participants in the near future.

MEASURED OUTBREAK: SOBER.C

Shortly before Christmas the Win32/Sober.C worm was discovered in Germany. Like Win32/Sober.A its distribution was mainly limited to German-speaking countries, where it was widespread – possibly due to the fact that it applies very good social engineering tricks and it uses the German language (http://www.pcwelt.de/news/viren_bugs/36527/). However, after this worm was discovered (at around 03:00 h CET on 20 December 2003), it rose quickly in the statistics of several email security providers. For example, in the *MessageLabs* virus statistics (http://www.messagelabs.com/viruseye/threats/) it jumped to the sixth position very quickly and (at the time of writing) remains high in the chart with more than 4000 copies stopped every day. The *Frisk AVES* homepage (http://aves.f-prot.com/) showed it at the number one position for several days – with about 2 per cent of all scanned mails infected by Sober.C.

We felt that this local outbreak was significant enough to test the response times of all anti-virus companies that were on our watch list (see Table 1). This time, *BitDefender*, *Kaspersky*, *F-Prot* and *F-Secure* were first to release updates, but there is no guarantee that they will win the race next time.

It came as a surprise that big companies like *CA* or the German company *G Data* (which relies on the *Kaspersky* and *BitDefender* engines) seemed to have missed this outbreak completely and provided signatures at a time when

Table 1. Response times of AV companies (CET) to the outbreak of W32/Sober.C (worm discovered 2003-12-20 at 03:00 h).

BitDefender	2003-12-20 at 13:20 h
Kaspersky	2003-12-20 at 14:45 h
F-Prot (Frisk)	2003-12-20 at 15:25 h
F-Secure	2003-12-20 at 15:45 h
Norman	2003-12-20 at 18:25 h
eSafe (Aladdin)	2003-12-20 at 18:35 h
Trend Micro	2003-12-20 at 19:50 h
AVG (Grisoft)	2003-12-20 at 20:15 h
AntiVir (H+BEDV)	2003-12-20 at 22:20 h
Symantec	2003-12-21 at 04:05 h
Avast! (Alwil)	2003-12-21 at 09:55 h
Sophos	2003-12-21 at 14:35 h
Panda AV	2003-12-21 at 17:05 h
McAfee/NAI	2003-12-22 at 04:10 h
Ikarus	2003-12-22 at 10:35 h
eTrust (CA)	2003-12-22 at 17:50 h
AVK (G Data)	2003-12-23 at 23:50 h

it was already much too late to prevent the spread of the worm. The *G Data* case is especially interesting: standard customers receive updates only once a week, but after a few discussions they change the update interval to twice a week.

It should be noted that we tested only the virus definitions which were available to all customers – we did not include beta definitions which had to be applied manually. For example, *McAfee* had DailyDats available which included a detection routine for Sober.C as well as extra.dats which were available by request only.

For us, the test process for the updates was very simple: we installed the anti-virus products and tested them against the updates we had saved in our archive. To make sure that the worm had not been detected generically or heuristically, we tested the products' detection using older definitions as well as using the most current updates. However, none of the products we tested was able to catch this worm without updates.

UPDATE RELEASE CYCLES

The archived updates we have collected could be used for a number of other tests. For example they could be used to measure the actual release cycle of updates. Many companies claim that they update their signatures daily or every few hours, but after sorting out all the definitions released over a three-month period, and after duplicate updates had been removed, the reality looked a little different (see Table 2).

It is good to know that most anti-virus companies update their scanners more or less on a daily basis. They act like real security service providers, protecting against new threats proactively. Regardless of whether a malware threat has the ability to spread widely, it will be stopped by an updated product, so the chances of the virus spreading are lowered significantly. Using current pattern-based anti-virus technology, this is the only opportunity we have to stop malware – especially mass-mailer worms – quickly. It is true that providing more regular updates will result in higher costs for testing and QA, but that is what today's market expects and wants – and it is what the customers are paying for.

As an addendum to Table 2, it should be noted that *Network Associates* (*McAfee*) plans to release daily DAT updates starting early in the second quarter of 2004. Let's hope that other companies follow suit soon, because update releases only once or twice a week are simply too infrequent today.

We also have access to beta virus definitions from four anti-virus companies and these are often updated at least every few hours (see Table 3). However, according to the anti-virus companies these updates are usually only 'minimally tested' and could cause false positives or non-detections for existing viruses, so these patterns should be used only in emergencies.

Table 2. Standard regular update release intervals

Product	Number of updates per week
AntiVir (H+BEDV)	5 to 6
Avast! (Alwil)	2
AVG (Grisoft)	2
BitDefender	3 to 4
Command	2
Dr.Web	6
eSafe (Aladdin)	5
eTrust (CA)	4 to 5
F-Prot (Frisk)	4 to 5
F-Secure	6 to 7
Ikarus	4
Kaspersky	about 20
McAfee/NAI	1
Norman	2
Panda	7
Quickheal	4
Sophos	4 to 5
Symantec	1 to 2
Trend Micro	2 to 3
VirusBuster	4 to 5

Table 3. Beta update release intervals

Product	Number of updates per day
McAfee/NAI	5 to 12
Panda	40 to 50
Symantec	14 to 18
Trend Micro	6 to 7

It should be noted that there might be no correlation between the update frequency of (beta) definitions and outbreak response times. For example, *Panda* released 40 to 50 beta updates a day, yet it took more than 38 hours for an update with Sober.C detection routines to be made available. Let's hope that we will see more of a correlation in the future.

CONCLUSION

We hope to start a new interest in 'real-world' anti-virus tests. As well as testing outbreak response times, this project enables us to test the heuristics of products using retrospective test methodologies, count the number of updates released and we are even able to test the quality of these updates without any time pressure, because they are collected automatically. At a later stage we hope to make all the information available on a webpage which will be updated at regular (five-minute) intervals so that anyone can check the current update status of their anti-virus products.

TUTORIAL

MISSION IMPOSSIBLE: THE MESSENGER AND OTHERS

Aleksander Czarnowski
AVET Information and Network Security, Poland

The last couple of 'Mission: impossible'-style assignments (see *VB*, August 2002 p.10, September 2002 p.8 and May 2003 p.10) were quite successful, but in the life of every agent there comes a time when he should apply himself to a true challenge – something that really does seem impossible by design.

As before, our main objective is to secure an *IIS 5.0* server running on *Windows 2000 Service Pack 4* (the latest at the time of writing). *IIS 6.0* seems to be a little less of a challenge, as its fundamental design in terms of security has been changed for the better (for a quick introduction take a look at [1] and [2]).

STARTING WITH A SIMPLE TASK …

We will start with a Messenger service assignment. Take a look at *Microsoft Security Bulletin* MS03-043 [3]. According to the description of the vulnerability it is possible to execute code remotely by exploiting a buffer overflow in this service. This raises an important question which forms the basis of the first part of our mission: is there any way of minimising risk other than applying the appropriate hotfix?

The answer is yes – we can simply stop the service and later disable it. In environments where the highest security level is required we can do one more thing: delete the service. One tool that enables us to carry out this action is sc.exe [4] (this is installed by default in *Windows XP*, and is available for *Windows 2000* from *Resource Kit*).

By issuing the following command:

```
sc [server name] delete [service name]
```

we can delete the selected service. However, before issuing this command, bear in mind that sc does not provide the option to 'undelete', so you will be forced to edit the registry manually should you need to reverse the action. Think at least twice before deleting any service – even one that seems, to all intents and purposes, redundant. Keep in mind that some applications rely on other services.

Luckily for us, the Messenger service is not usually required in DMZ network environments and has very limited use so we can at least stop it and disable it so that it won't be started after every reboot of the system. (If you are new to managing services under *Windows*, here is a tip: after stopping some services you do not need to reboot the system in order for the changes to take effect – however, if you stop some other services the system might reboot automatically.)

So, after patching, stopping and disabling the service we have completed the first part of the assignment.

THE WORKSTATION CASE

Our next target is highlighted by *Microsoft Security Bulletin* MS03-049 [5], which describes a remotely exploitable buffer overflow in the Workstation service. Again, our objective is to secure the server from this attack vector. But before we start clicking on the Services MMC snap-in in order to stop and disable the Workstation Service, let's have a look at its Dependencies tab in the Workstation Properties window, as shown in Figure 1.

As you can see, the Workstation service is not dependent upon any other service, but there is a list of services that depend on it. You may also have noted that the target of the first part of our mission – the Messenger service – depends on the Workstation service. So, by stopping the Workstation service we will also stop the operation of the Messenger service (see Figure 2). While in hardened environments like DMZ networks you usually do not need Alerter, Computer Browser and DFS, in the case of domains you will be using Net Logon. This is one of the reasons why many documents on securing *Windows* advise against installing critical servers as domain controllers and advise against joining any

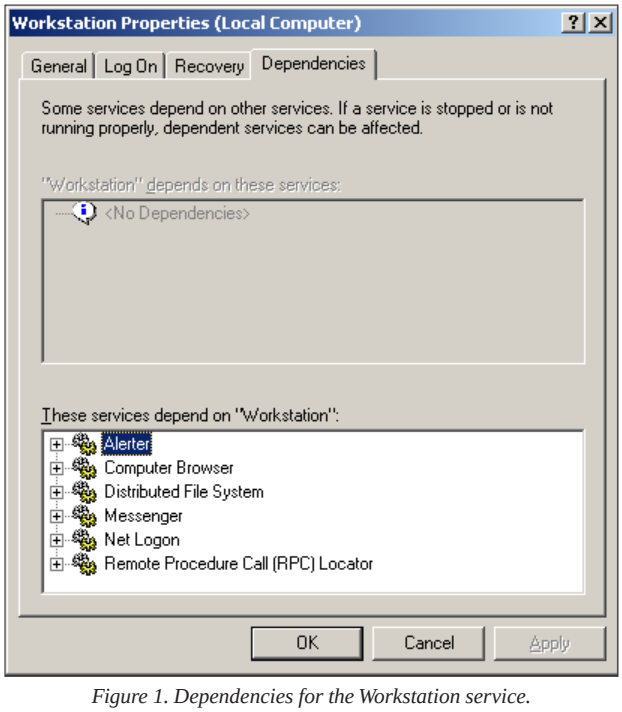


Figure 1. Dependencies for the Workstation service.

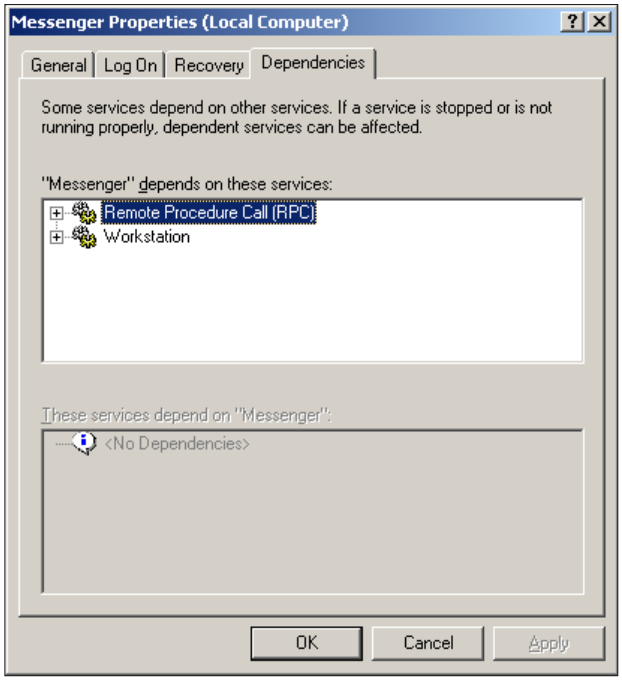


Figure 2. Dependencies for the Messenger service.

domain. You will also break the *Microsoft Baseline Security Analyzer* (MBSA).

We begin this part of our assignment with stopping the service and checking whether all the critical applications are working. If you occasionally run applications that require the Workstation service, then instead of disabling it you can change its startup type to manual.

THE IIS CATCH

We could disable the Workstation service, but we are running *IIS*, and as stated in [6], this service is required by *Internet Information Services*. The same applies to the Server service which, in many other cases, can be disabled as well.

Fortunately, the Messenger service has nothing to do with running *IIS* so it really can be disabled.

THE RPC

Now we came to the hardest part of our assignment. Proceed to security bulletins MS03-039 [7] and MS03-026 [8] (start by reading the last one first to gain a better understanding of the problem). As you see, some services can be a source of several attack vectors for different vulnerabilities – this is also the case with the MDAC component which we will discuss later.

The problem with Remote Procedure Call (RPC) is that this is a critical service for *Windows*. First, many other important services rely on it – as shown in Figure 3. Secondly, if you disable the RPC service your system might reboot or crash (some exploits for the RPC DCom vulnerability are known to crash the RPC service and, as a result, perform a remote reboot on the non-English language version of *XP* instead of penetrating the system). In the worst case, disabling the RPC service will prevent the system from booting.

From a security perspective it is also important to note that the RPC service is running within the SYSTEM account. This is why penetrating the system with a vulnerable RPC service is so trivial – it can be considered a direct hit as no additional actions are needed to control the compromised host.

So we cannot disable or stop the RPC service. How will we deal with this part of the mission?

Start by applying the hotfix from MS03-039 [7] immediately if you have not done so already. Next, review your network architecture and screen your *Windows* RPC traffic. This should be done both by implementing firewalls at the appropriate network points (do not use the *Windows 2000* TCP/IP filtering feature – use IPSec instead) and by allowing only IPSec communication between *Windows* hosts if possible.

As a side note, there is also a Remote Procedure Call (RPC) Locator service, which can be disabled in some

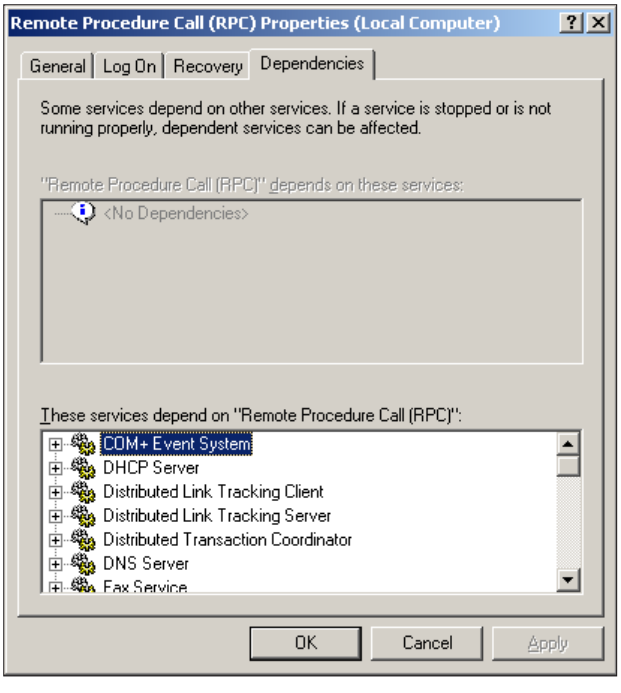


Figure 3. Dependencies for the RPC service.

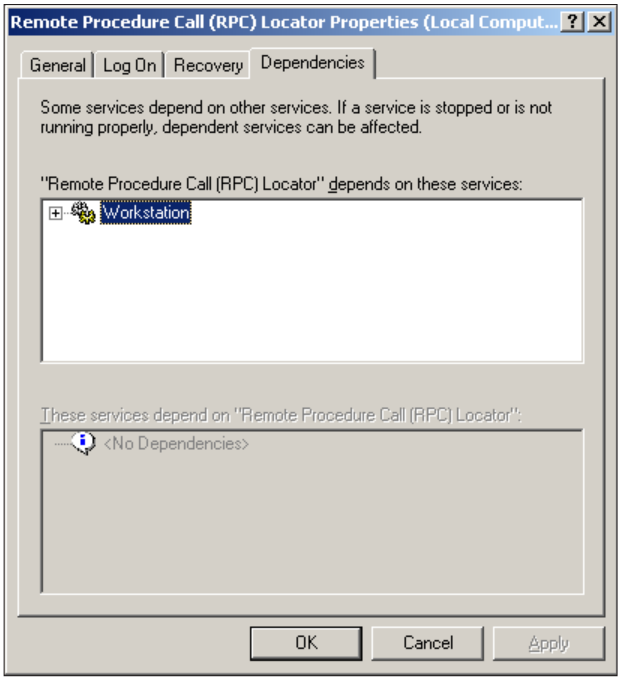


Figure 4. Dependencies for the RPC Locator service.

configurations. As shown in Figure 4, this depends on the Workstation service to work.

MDAC – A GOOD START IN 2004

The final part of our assignment is concerned with *Microsoft Security Bulletin* MS04-003 [9]. While MDAC is not a service there are some similarities from a security point of view that should be highlighted.

Just like all the services described above, the MDAC component is installed by default in *Windows 2000*, so it should be considered as a potential attack vector.

Furthermore, the vulnerability described in MS04-003 is not the first to have been discovered in this component, although it is rarely mentioned in documents describing tips for securing *Windows*. Nevertheless, this does pose some risk (the true level of risk is determined by a number of factors including how the particular host is situated in the network, and what critical business functions are performed by this system and MDAC).

If you read MS04-003 carefully you will find some real bonus information. First, there is a nice workaround based on implementing packet filtering with IPSec polices.

By issuing the following command:

```
ipsecpol -w REG -p “Block UDP 1434 Filter” -r “Block
Inbound UDP 1434 Rule” -f *=0:1434:UDP -n BLOCK -x
```

we can block traffic to UDP port 1434. The same method can be used to filter out other offending traffic, for example regarding different vulnerabilities in the service. (There is an important tool called netdiag that allows us to check for the existance of previously assigned IPSec policy [netdiag /test:ipsec] – read more about it in [10].) Note that in order to use IPSec you also need to start the IPSec Policy Agent service, which in turn can pose some risk.

Despite the trick with using IPSec polices there is an interesting article [11] which describes how to determine the version of MDAC component installed. There is another bonus to this article: the *Component Checker 2.0* tool (see Figure 5). This very valuable tool allows you to verify which version of MDAC is installed and to perform a close inspection of MDAC files.

MDAC HACKS?

Initially I planned to end the mission here and proceed to some final thoughts. But I felt that discussion of another problem related to security management and MDAC would make an interesting addition.

Some time ago, someone at *Microsoft* decided to add the Remote Registry service to *Windows*. The idea is pretty neat – using a simple Win32 API (that is also used for accessing the local registry), one can access and modify the registry on a remote host.

This might seem like a great idea, assuming that we can secure both the service and the registry appropriately and efficiently. Unfortunately it might not be that simple. A large number of patch management solutions (and MBSA, for example) rely on this service to check the status of the installed service packs and hotfixes on remote hosts. So you might need to run the Remote Registry service if you are using tools such as the commercial version of *GFI Network Security Scanner*.

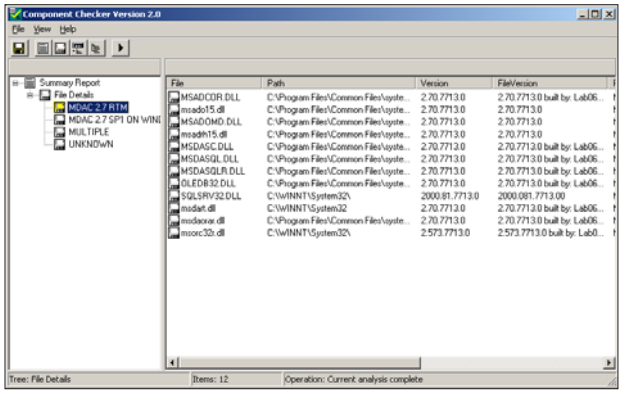


Figure 5. Component Checker 2.0 in action.

Security bulletin MS04-003 [9] and Microsoft Knowledge Base article 301202 [11] tell us the location in the registry of the MS04-003 hotfix information and the MDAC version number respectively.

As MDAC is installed by default on most current installations of *Windows* systems, a lot of administrators and security officers would like to have a tool which would allow them to check for the MDAC version and hotfix installation.

Such a dedicated tool would be far handier for quick MDAC audits than a full-blown security or vulnerability scanner like *Nessus* (with a little tweaking of *Nessus* nasl scripts you can run them as standalone by using the nasl -t command). I will not discuss further use of *Nessus* scanning *Windows* systems from *Linux* or *BSD* systems as it is something not acceptable to *Windows* purists (of which I am not one).

On the other hand one would suspect that we can employ Win32 API for accessing the registry. If you have ever used RegOpenKeyEx() and RegQueryValueEx() functions then you will feel at home. To access the registry on a remote host, you need to call the RegConnectRegistry function, passing the host name, registry hive, and a pointer where the handle for the open registry will be stored.

If you have ever written code for accessing the local registry then you don't need anything more. Just pass the handle value from RegConnectRegistry to RegOpenKeyEx (remember to close the handle with RegCloseKey) and you can read the registry on the remote computer. Sounds simple? At *AVET INS* we got the first version of this tool up and running about 10 minutes after getting the MS04-003 bulletin. So where is the catch?

First, RegConnectRegistry() always fails on *Windows XP Home Edition* (while MDAC is also installed on those systems). Secondly, if the *Windows XP Professional* or *Windows 2003 Server* is joined to the workgroup, the 'Force network logons using local accounts to authenticate as Guest' policy is enabled by default – which also causes the function to fail. So, if you wish to access the registry remotely using RegConnectRegistry() you might need to review and modify your policy first.

Also, you should be inside the domain you are scanning. You need to remember those obstacles when accessing your MDAC-enabled hosts with remote scanners.

THE LESSONS LEARNED

Services are a crucial part of the *Windows* security model. As stated in [4], in order to master *Windows* security one needs to master services security. Under *Windows 2000* many services run in the context of the SYSTEM account and in some cases this cannot be changed. Meanwhile, some services (like SQL Server) can be run with lower privileges.

In *Windows XP* and newer versions, two new accounts for services have been introduced: LocalService and NetworkService. Use of those accounts to create a separate and dedicated account (with minimal required privileges) for every available service is not an option since the number of services ranges from 50 to more than 100, depending on the installation.

The main aim of this article was to point out that *IIS* servers can be penetrated by exploiting vulnerabilities that are not directly connected with the *IIS* code base. So, when securing your *IIS* servers remember the system platform and secure it first.

Now you have a 'licence to kill [services]' – don't forget to add a double 0 before your nickname!

BIBLIOGRAPHY

[1] *IIS* architecture overview: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/iissdk/iis/iisarchitectureoverview.asp.

[2] *IIS* modes of operation: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/iissdk/iis/newsystemarchitecture.asp.

[3] MS03-043: http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-043.asp.

[4] *Securing Microsoft Services* by Mark Burnett: http://www.securityfocus.com/infocus/1581/.

[5] MS03-049: http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-049.asp.

[6] *Microsoft Knowledge Base* article 189271 – List of services needed to run a secure IIS computer: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q189271.

[7] MS03-039: http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-039.asp.

[8] MS03-026: http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-026.asp.

[9] MS04-003: http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS04-003.asp.

[10] *Microsoft Knowledge Base* article 813878 – How to block specific network protocols and ports by using IPSec: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q813878.

[11] *Microsoft Knowledge Base* article 301202 – How to check for MDAC version: http://support.microsoft.com/default.aspx?kbid=301202 .

OPINION

MISGUIDED OR MALEVOLENT? NEW TRENDS IN VIRUS WRITING

Stuart Taylor
Sophos Plc, UK

Recently there have been several reports circulating reviewing the virus scene. Most of these have been looking back at the trends seen in 2003: what types of viruses have been prevalent, when they were prevalent and what platforms have been most affected – no prizes for guessing that *Windows* has taken the brunt of attacks.

One question that keeps coming back to me is 'Who writes viruses?'. There have been many caricatures of virus writers, some accurate and some not. Are they young or old? Are they 'nerds' or professionals? Are they script kiddies or serious writers of metamorphic creations? Are they all men or are there females writing these things? In truth, I suspect that all of the above are true to some extent. However, I think that we may be experiencing a new trend in virus writing.

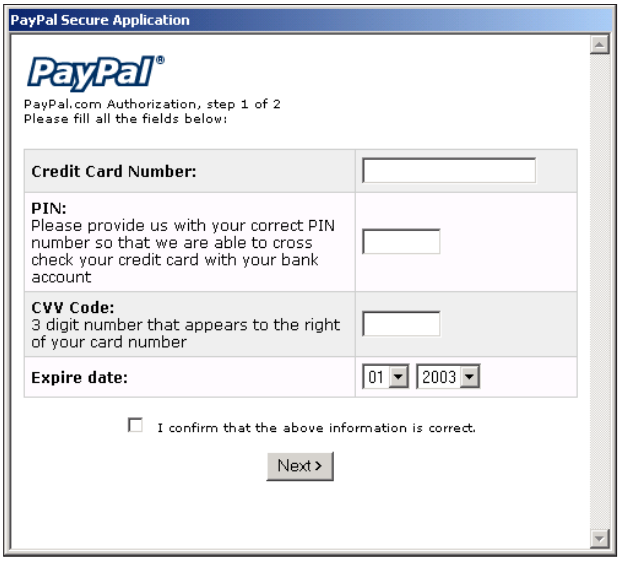
THEFT OF CREDIT CARD DETAILS

In September 2002, a virus writer unleashed the worm W32/Bugbear.A on the world. I recall that *Sophos* released an IDE promptly and we thought nothing more of it. Two days later, however, the media latched onto the idea that the worm could steal credit card details and our support department was flooded with requests for information from users who were worried they might have given away vital information. This was probably the first worm to hit the mainstream media with the concern of theft of credit card information.

In November 2003, I spoke at a two-day conference in the UK on Cyber Fraud. On both days of the conference I awoke to the news from *Sophos* that the company's virus lab in Sydney had alerted overnight on a new worm that threatened to steal credit card details directly.

The first worm was W32/Mimail.I. This worm attempted to steal credit card details by putting up a fake *PayPal* pop-up which requested credit card information from the recipient, stating that the recipient's *PayPal* account had expired. *PayPal* is a well-known method of performing a secure transaction on the Internet – this social engineering had been well thought through. A clever trick of W32/Mimail.I was to ask for the CVV (card verification value) code from the back of the credit card.

Clearly some people would have been surprised by the appearance of a pop-up requesting this information and would have exercised caution. The following day the variant W32/Mimail.J attempted to overcome this obstacle by creating a dummy web page on the local disk and bringing up the user's web browser to view the page, thus giving the recipient the impression of having been taken to a legitimate website.



W32/Mimail.I produced a fake PayPal pop-up requesting credit card information – even asking for the CVV code from the back of the credit card. Note the misspelling of 'Expiry date'.

W32/Mimail.J had one more trick up its sleeve, requesting the user's mother's maiden name – a favoured security check of most banks. However, at this point the virus writer asked for one piece of information too many – it asked for the user's Social Security number. This information is very country-specific. The USA and Australia, for instance, both use the term 'Social Security number', but other countries use different expressions, such as 'National Insurance number' in the UK.

WHO ARE THE WRITERS?

So, who is writing these worms and viruses? Is it still the person who claims to want to expose the flaws in *Microsoft*'s products, or the person who does it just because they can, or the person who wants to convey a political message? Whilst such people are clearly still in the business of writing viruses there is a definite hint that the criminal element of society may be becoming involved with the express purpose of perpetrating fraud.

In his article in last month's Virus Bulletin (see *VB* January 2004, p.14), Jamz Yaneza concluded that virus writers were moving away from destructive payloads, presumably to allow their creations to spread further before being detected.

I agree with this – we have seen very few worms recently that have been destructive.

Recently we had the mass mailing of Troj/Antikl-Dam. The actual functionality of the attached code is still a mystery as the attachment was harmless, having been truncated to leave no code inside.

The Trojan was seeded via an email containing the following text:

```
Dear customer,
The security of your personal and account information
is extremely important to us. By practicing good
security habits, you can help us ensure that your
private information is protected. Please install our
special software, that will remove all the keyloggers
and backdoors from your computer.
And will help us to prevent credit card fraud in
future.
Thank you.

Best regards,

<name>
```

The <name> in this case was the name of a banking institution, and the emails were sent with a selection of return addresses of various banks, one of which was the Bank of England.

According to news reports on the day, the Bank of England received in excess of 100,000 reports, mainly from out-of-office agents as the Trojan was spammed during the Christmas break when most businesses were closed. The sheer number of messages implied that a spam list had been used, consisting of email addresses of easily double the number of out-of-office replies. Add to this the fact that other banks were targeted as well, and the number of original emails must have been vast. It is possible that this was intended to be a denial of service attack, but it looks more like a well-organised attempt to obtain credit card details fraudulently.

A CRIMINAL ELEMENT

What does all this tell us, and what should we be doing about it? In his 2003 annual review (see http://www.sophos.com/), Graham Cluley said he believed that virus writers had learnt that money could be made from writing viruses. My question is 'Are they doing it themselves or is there truly a criminal element entering virus writing?'

It is far too early to draw any conclusions but we will monitor the trend over the next year. Anti-virus companies have always worked with law enforcement bodies to try to track down those responsible for propagating viruses, but we are always bound by customer confidentiality. Maybe we are all going to have to work much harder and more openly if we are to prevent this trend from growing.

COMPARATIVE REVIEW

WINDOWS NT 4.0

Matt Ham

With the number of *Windows* platforms that are officially supported by *Microsoft* on the decrease, it is sometimes a knotty problem deciding which platforms should be included in *Virus Bulletin* comparative testing. DOS testing is now a thing of the past, and *Windows Me* looks very much as if it too has reached the graveyard of antiquated operating systems. Personally, I had expected to see *Windows 98* being administered the last rites this year – however, it seems that *Windows NT* will officially be killed off first. This raises the question as to why *VB* has decided to test AV products on *Windows NT*, when *Windows 98* is apparently a more thriving platform.

The answer is twofold. First, the schedules for testing are planned well in advance, and the demise of *NT* as a *Microsoft*-supported system was not made clear until after the schedule had been set. The second, and more significant reason, is the fact that the decision by *Microsoft* to remove support from an OS is not necessarily an indication of that OS becoming extinct in the wild. From a marketing point of view, *NT* users are likely to upgrade to *XP* if *NT* is no longer supported. *NT* was always much stronger among corporates than in the home-user environment and, in a large company, expense is not always as significant a consideration as continuity and the ability to make long term plans. On balance, although doomed to lack of support in the near future, *NT* is still a rather more relevant platform for business users.

TEST SETS

The test sets used in this review were the first to be aligned to the real-time WildList and as such were expected to provide rather more of a challenge for the products than the test sets used in past reviews. Unfortunately, both the *VB2003* conference and the Christmas period conspired to cause delays in the updating of the real-time WildList and, on the date when the test set was finalised, the 'real-time' WildList was updated only as far as late October 2003. In future reviews the test set will be derived from the real-time WildList two days prior to the test deadline, with the hope that it will pose greater challenges for the products under test.

AhnLab V3VirusBlock

ItW Overall	100.00%	**Macro**	98.08%
ItW Overall (o/a)	100.00%	**Standard**	85.57%
ItW File	100.00%	**Polymorphic**	43.19%

Over the year since its debut in the *VB* comparative review line-up, the detection rates of *V3* in its various incarnations have improved in all test sets. Admittedly this improvement is only by a few percentage points in each category, but with the most significant improvement in the ItW set, *V3VirusBlock* gains a VB 100% award.

Alwil Avast! 4.1.319

ItW Overall	100.00%	**Macro**	99.56%
ItW Overall (o/a)	N/A	**Standard**	99.10%
ItW File	100.00	**Polymorphic**	93.54%

Changes to *Alwil*'s on-access scanner caused problems during the last review of the product (see *VB*, November 2003, p.13) and it proved troublesome again this time. With the configuration options available it is impossible to activate on-access scanning for many file types unless the files are executed. Clearly, this is infeasible when dealing with tens of thousands (or even merely dozens) of samples in a test environment. Therefore, the on-access file capabilities of *Avast!* were untestable. Where on-demand scanning was concerned the results were good – unfortunately without on-access results the product does not qualify for a VB 100% award.

Authentium Command AntiVirus 4.90.2

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.91%
ItW File	100.00%	**Polymorphic**	99.91%

A familiar product from a new company, *Command AntiVirus* performed much the same as it ever has, earning a VB 100% award in the process. Casting back to the results of the February 2003 comparative review (see *VB*, February 2003, p.16), this product (along with many others) missed the polymorphics W32/Tuareg.B, W32/Zmist.D and W32/Etap.A. Of these previously problematic viruses only a single Zmist sample was missed this time. This is a good sign that progress is being made in the more complex areas of virus detection technology.

CA eTrust Antivirus 7.0.142

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

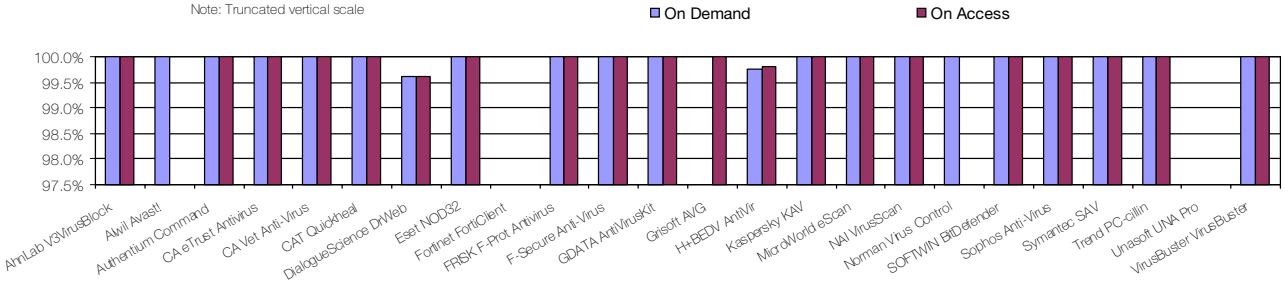
The samples missed by *eTrust Antivirus* on this occasion were very much the same as those missed last year, and with no misses in the ItW test set, another VB 100% is on its way to *Computer Associates*. Still disappointing, however, is the new log file functionality, which renders production of parseable result files an impossibility. In a very low-tech workaround the software was set up to log missed samples (which were few in number), and the results were stored in a screen shot for later reference.

CA Vet Anti-Virus Protection 10.59.2.1

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.90%
ItW File	100.00%	**Polymorphic**	99.87%

Vet's results were sufficient to warrant a further VB 100% award for *CA*. Although there is little perceptible change in *Vet*'s detection performance since this time last year, there has been a notable slowing of scanning speed over that period.

In the Wild File Detection Rates



CAT Quickheal X Gen 7.00

ItW Overall	100.00%	**Macro**	97.49%
ItW Overall (o/a)	100.00%	**Standard**	83.33%
ItW File	100.00%	**Polymorphic**	95.12%

In the last *NT* comparative, *CAT*'s detection was skewed very much in favour of ItW viruses, with a distinctly second-rate level of detection in other areas. This skew seems to have been ironed out over the course of the year, although the one remaining weak area is the polymorphic set, especially where on-access scanning is concerned. However, the detection rate of ItW files has improved, rendering *Quickheal* eligible for another VB 100% award.

DialogueScience Dr.Web 4.30a

ItW Overall	99.60%	**Macro**	100.00%
ItW Overall (o/a)	99.60%	**Standard**	100.00%
ItW File	99.59%	**Polymorphic**	100.00%

Dr.Web continues to surprise with the number of suspicious files it notes. Not because the number is excessively large but because the number of such files seems to vary from virtually zero to the mid-teens. A more disturbing surprise was that the product missed BAT/Mumu.A in the ItW test set. This missed detection was checked several times, both on access and on demand, and proved to be reproducible. *Dr.Web* is thus denied a VB 100% award on this occasion.

Eset NOD32 1.595

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

This month sees another addition to *Eset*'s growing collection of VB 100% awards. With 100 per cent detection in all categories and no false positives, *NOD32* fails to pull any surprises out of the bag.

Fortinet FortiClient 1.0.048

ItW Overall	95.55%	**Macro**	43.10%
ItW Overall (o/a)	95.39%	**Standard**	27.40%
ItW File	99.10%	**Polymorphic**	23.44%

Fortinet's *FortiClient* is not designed primarily as an AV product, although this functionality is prominent in its GUI. Unfortunately, the degree to which it detects viruses is not very impressive. Admittedly, the product's detection rates for ItW viruses are close to acceptable, and this, presumably, is the area in which the developers have decided to concentrate their efforts. Among polymorphic and standard viruses, the detection rate is so poor it is barely worth mentioning. In addition to poor detection rates the product announced an exception when scanning the clean OLE file test set. To its credit, though, this was cleanly trapped and dealt with, without a blue screen being triggered.

FRISK F-Prot Antivirus 3.14 b

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.74%
ItW File	100.00%	**Polymorphic**	99.91%

It is generally the case that rebadged products detect either identically to, or slightly less well than their parent products. Since *FRISK* supplies the engine for *Command AV* – already the recipient of a VB 100% – this should be a good omen for *F-Prot*. Indeed this proved to be the case, since *F-Prot* achieved full detection in the wild and leaves the test with a new VB 100%.

F-Secure Anti-Virus Client Security 5.52

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

Like *Command AV*, *F-Secure* also uses the *FRISK* engine, along with that of *Kaspersky* – and it would be quite an embarrassment were this product to fail to earn a VB 100% where the others succeeded. Happily, the *F-Secure* product met all the requirements for a VB 100% award.

GDATA AntiVirusKit 14.0.2

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

A chimera of the *SOFTWIN* and *Kaspersky* engines, *AVK*'s scanning results are no cause for concern for either company, since all files in every test set were detected without problem. A momentary panic on the clean test sets was

On-access tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
AhnLab V3VirusBlock	0	100.00%	0	100.00%	100.00%	82	98.08%	9139	43.19%	313	85.57%
Alwil Avast!	N/A	-	0	100.00%	-	N/A	-	N/A	-	N/A	-
Authentium Command	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.91%	4	99.76%
CA eTrust Antivirus	0	100.00%	0	100.00%	100.00%	4	99.90%	1	99.89%	2	99.88%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.87%	4	99.78%
CAT Quickheal	0	100.00%	0	100.00%	100.00%	107	97.45%	1086	92.85%	647	61.99%
DialogueScience Dr.Web	1	99.59%	0	100.00%	99.60%	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	9	98.94%	9	0.00%	95.39%	2328	43.10%	12524	23.44%	1226	27.40%
FRISK F-Prot Antivirus	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.91%	3	99.79%
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%	23	99.44%	757	83.64%	30	98.50%
H+BEDV AntiVir	1	99.79%	0	100.00%	99.80%	56	99.26%	1004	84.94%	52	97.91%
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	2	99.88%
MicroWorld eScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
NAI VirusScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	3	99.79%
Norman Virus Control	N/A	-	0	100.00%	-	N/A	-	N/A	-	N/A	-
SOFTWIN BitDefender	0	100.00%	0	100.00%	100.00%	13	99.69%	11	97.46%	60	97.79%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	8	99.80%	1	99.95%	14	99.49%
Symantec SAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Trend PC-cillin	0	100.00%	0	100.00%	100.00%	0	100.00%	215	95.77%	8	99.82%
Unasoft UNA Pro	157	76.03%	9	0.00%	73.30%	3048	26.88%	14446	11.67%	904	57.30%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	0	100.00%	101	91.78%	8	99.82%

averted since the single false positive was a warning rather than a full blown erroneous detection, thus leaving *AVK* with a VB 100% award and its component engine developers with high hopes.

Grisoft AVG Anti-Virus 7.0

ItW Overall	N/A	**Macro**	N/A
ItW Overall (o/a)	100.00%	**Standard**	N/A

ItW File	N/A	**Polymorphic**	N/A

AVG has undergone a major version change recently, bringing with it numerous changes in the look and feel of the product. The majority of these changes are positive in nature, having made the product more intuitive. There is, however, an area in which the changes have been less desirable. Currently it is only possible to automatically disinfect or log files detected as being infected. Where disinfection is impossible – for example in the case of all worms – the files will remain on the machine and at this point they must be removed manually, one by one. This, when combined with no provision for exportable logs of any great size, was sufficient to make on-demand detection testing (and consequently the chance to earn a VB 100% award) impossible. A VB 100% would have been ruled out in any case due to several false positives.

H+BEDV AntiVir 6.22.00.09

ItW Overall	99.77%	**Macro**	99.53%
ItW Overall (o/a)	99.80%	**Standard**	98.03%
ItW File	99.76%	**Polymorphic**	84.94%

Not having taken part in last year's review, *AntiVir* can also be considered as something of a newcomer, though it has been tested in the distant past and as part of the *Linux* review process. Detection rates for the product were good overall, only polymorphics showing signs of weakness. Unfortunately, however, there were several misses in the ItW test set. These were the DLL portion of VBS/Redlof.A and the extensionless samples of O97M/Tristate.C. Since the latter was detected on access this was clearly an issue of extensions.

Kaspersky Anti-Virus 4.5.0.94

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

After disabling its soul-wrenching sound effects *KAV* is always a pleasant product to deal with. Since the last review even the most pesky of the remaining polymorphics have been rendered detectable by the *KAV* engine, leaving only the zipped samples of W32/Heidi.A as undetected on access. Since this is a result of not scanning ZIP archives on access (which is entirely understandable), detection rates can be considered all but perfect. With no false positives, *KAV* has gained a VB 100%.

MicroWorld eScanWin 1.3

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

Consisting of a rebadge of the *GDATA* product, it might be expected that the results obtained by *eScan* would be similar to those of its parent product. Happily for *MicroWorld* this did indeed prove to be the case. The outcome of this review is a far cry from that of a year ago, when *eScan* suffered from a bizarre loss of detection and demonstrates that any teething troubles are now well behind the product. Little more remains, therefore, other than to pass a VB 100% in *eScan*'s direction.

NAI VirusScan Enterprise 7.1.0 4.3.20 4113

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.79%
ItW File	100.00%	**Polymorphic**	100.00%

Causing confusion with ever-mutating name, *NAI*'s product makes up for this foible by maintaining a consistent interface over all of its incarnations. This is not the only area where consistency has been achieved, with the detection rate also remaining uniformly high. Since false positives have never been a problem for *NAI* during my experience of testing, this results in a VB 100% for *Network Associates*.

Norman Virus Control 5.7

ItW Overall	100.00%	**Macro**	99.95%
ItW Overall (o/a)	N/A	**Standard**	99.89%
ItW File	100.00%	**Polymorphic**	91.72%

The *Norman* team seems to be somewhat cursed with strange bugs when it comes to *VB* testing. This time the problem lay in the on-access portion of the tests. When running the on-access scanner over the infected test sets, the number of files detected was at variance each time with the previous occasion.

Having run the tests some ten times without any form of pattern having emerged, on-access testing was abandoned. Unfortunately this means that a VB 100% award is beyond the reach of the product on this occasion, despite all other results being good.

On-demand tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
AhnLab V3VirusBlock	0	100.00%	0	100.00%	100.00%	82	98.08%	9139	43.19%	313	85.57%
Alwil Avast!	0	100.00%	0	100.00%	100.00%	18	99.56%	124	93.54%	23	99.10%
Authentium Command	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.91%	1	99.91%
CA eTrust Antivirus	0	100.00%	0	100.00%	100.00%	4	99.90%	1	99.89%	0	100.00%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.87%	2	99.90%
CAT Quickheal	0	100.00%	0	100.00%	100.00%	103	97.49%	1044	95.12%	310	83.33%
DialogueScience DrWeb	1	99.59%	0	100.00%	99.60%	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	9	99.10%	9	0.00%	95.55%	2328	43.10%	12524	23.44%	1226	27.40%
FRISK F-Prot Antivirus	0	100.00%	0	100.00%	100.00%	0	100.00%	2	99.91%	5	99.74%
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	N/A	-	0	100.00%	-	N/A	-	N/A	-	N/A	-
H+BEDV AntiVir	2	99.76%	0	100.00%	99.77%	31	99.53%	1004	84.94%	50	98.03%
Kaspersky KAV	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%
NAI VirusScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	3	99.79%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	2	99.95%	174	91.72%	3	99.89%
SOFTWIN BitDefender	0	100.00%	0	100.00%	100.00%	13	99.69%	10	97.51%	60	97.79%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	8	99.80%	1	99.95%	14	99.49%
Symantec SAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Trend PC-cillin	0	100.00%	0	100.00%	100.00%	0	100.00%	215	95.77%	8	99.82%
Unasoft UNA Pro	126	80.03%	4	55.56%	79.15%	1783	57.92%	14379	12.85%	773	64.31%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	0	100.00%	101	91.78%	8	99.82%

SOFTWIN BitDefender Standard 7.2

ItW Overall 100.00% **Macro** 99.69%
ItW Overall (o/a) 100.00% **Standard** 97.79%

ItW File 100.00% **Polymorphic** 97.51%

Having already appeared in this test as a part of both *AVK* and *eScan*, *BitDefender* now arrives for testing on its own.

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 V3VirusBlock	143	3824.7		26	3051.3		175	911.0	49	1522.6
Alwil Avast!	268	2040.8		31	2559.2		96	1660.6	36	2072.4
Authentium Command	253	2161.8		19	4175.5		85	1875.5	13	5739.0
CA eTrust Antivirus	293	1866.7		18	4407.4		107	1489.9	22	3391.2
CA Vet Anti-Virus	237	2307.7		20	3966.7		98	1626.7	27	2763.2
CAT Quickheal	149	3670.7		24	3305.6		102	1562.9	31	2406.7
DialogueScience Dr.Web	297	1841.5	[12]	31	2559.2		100	1594.2	19	3926.7
Eset NOD32	204	2681.0		21	3777.8		46	3465.6	8	9325.9
Fortinet FortiClient	258	2119.9		N/A	-		62	2571.2	20	3730.4
FRISK F-Prot Antivirus	238	2298.0		19	4175.5		106	1503.9	15	4973.8
F-Secure Anti-Virus	304	1799.1		36	2203.7		118	1351.0	30	2486.9
GDATA AntiVirusKit	824	663.8	[1]	40	1983.3		373	427.4	43	1735.1
Grisoft AVG	320	1709.2	4 [2]	24	3305.6		156	1021.9	36	2072.4
H+BEDV AntiVir	286	1912.4		19	4175.5		111	1436.2	23	3243.8
Kaspersky KAV	290	1886.0		32	2479.2		118	1351.0	27	2763.2
MicroWorld eScan	389	1406.0		38	2087.7		161	990.2	35	2131.6
NAI VirusScan	213	2567.8		26	3051.3		98	1626.7	17	4388.7
Norman Virus Control	445	1229.1		25	3173.4		216	738.0	22	3391.2
SOFTWIN BitDefender	770	710.3	[1]	21	3777.8		315	506.1	22	3391.2
Sophos Anti-Virus	182	3005.1		24	3305.6		88	1811.6	20	3730.4
Symantec SAV	299	1829.2		34	2333.3		114	1398.4	32	2331.5
Trend PC-cillin	197	2776.3		14	5666.7		71	2245.3	16	4663.0
Unasoft UNA Pro	252	2170.4	6 [8]	32	2479.2	[2]	207	770.1	39	1913.0
VirusBuster VirusBuster	313	1747.4		26	3051.3		162	984.1	29	2572.7

Despite having a scattering of misses across the test sets, none of these were in the ItW set, thus *BitDefender* earns a VB 100% award. The last year has seen small increases in detection rates overall for *SOFTWIN*, though there were only small numbers of misses to start with.

Sophos Anti-Virus 3.77

ItW Overall	100.00%	**Macro**	99.80%
ItW Overall (o/a)	100.00%	**Standard**	99.49%
ItW File	100.00%	**Polymorphic**	99.95%

Sophos continues to improve its detection rates in the polymorphic test sets, with only a single miss in that area. The remaining misses all fell into the category of samples deliberately chosen not to be detected on performance grounds, so the developers will no doubt be happy with their work on the underlying engine. With its usual lack of false positives the *Sophos* product is well deserving of a VB 100% award.

Symantec SAV 8.1.0.825

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 product detected all files in all test sets, leaving little room for discussion. What's more, the product managed exactly the same feat this time last year. As a result a VB 100% is awarded to *Symantec*.

Trend PC-cillin 10.04-1114

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.82%
ItW File	100.00%	**Polymorphic**	95.77%

With historical trends in mind, *PC-cillin* is another product whose performance has changed very little in the last year. Virtually identical results on the two occasions are slightly less impressive where misses are concerned, although the ItW and macro test sets showed perfect detection. Despite the lack of improvement during the year, *PC-cillin* is due a VB 100% award.

Unasoft UNA Pro 1.82

ItW Overall	79.15%	**Macro**	57.92%
ItW Overall (o/a)	73.30%	**Standard**	64.31%
ItW File	80.03%	**Polymorphic**	12.85%

Hailing from the Ukraine, this was another new product on offer this month – and was possibly the most disappointing product I have yet reviewed in terms of detection rate. The missed files were scattered without any distinguishable pattern throughout all the test sets, dispelling the view that perhaps detection had been concentrated in any one key area. To compound these woes, the product detected a considerable number of viruses where they did not exist.

Needless to say a VB 100% for *UNA* looks a far off prospect. However, *UNA* did excel in one area: the security measures designed to prevent unauthorised use of the program. This is a four-layer process, involving a key file, a personal serial number, an approved name and an allocated password. With this level of security it seems unlikely that any unauthorised users will be operating *UNA* – which can only be a good thing as far as protecting the world from viruses is concerned.

VirusBuster VirusBuster 4.5-12

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	99.82%
ItW File	100.00%	**Polymorphic**	91.78%

Back to more normal rates of detection, *VirusBuster* continues to whittle away at the few samples which it misses. This slow progress starts from a point at which improvement is hard, since detection rates are already very good. As a result of this detection quality *VirusBuster* is due another VB 100% award.

CONCLUSION

As can be seen from the results of this test, newcomers can have quite a harsh time as far as detection results are concerned, though old-timers do also suffer the odd indignity. Many of the reasons for this are external factors relating to the product's niche. For example, a product from the Far East will not necessarily aim to detect the same set of samples as a product from South America. Similarly, some products may focus on macro viruses or worms by dint of their perceived market. In many ways, the ItW test set is the most valid way of judging a new product, since detection rates in other test sets depend so much on the product's origin. Of course, we would expect to see improvements in detection rates in subsequent submissions, as has historically been the case, but for the products in this review only time will tell.

Technical details:

Test environment: Three 1.6 GHz Intel Pentium 4 workstations with 512 MB RAM, 20 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy, all running *Windows NT 4 Workstation Service Pack 6*.

Virus test sets: Complete listings of the test sets used can be found at http://www.virusbtn.com/Comparatives/WinNT/2004/test_sets.html.

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

END NOTES & NEWS

The 13th Annual RSA Conference takes place in San Francisco from 23–27 February 2004. The conference will cover technology trends and best practices in identity theft, hacking, cyber-terrorism, biometrics, network forensics, perimeter defence, secure web services, encryption and related topics. For more information see http://www.rsaconference.com/.

The NHTCU's Second e-Crime Congress will take place on 24 and 25 February 2004 at the Victoria Park Plaza Hotel, London. Supported by the Home Office for the second year, the congress provides an opportunity for government, law enforcement and business to develop effective partnerships to address the threat of hi-tech crime. The e-Crime Congress aims to bring together 400 senior delegates from the public and private sectors. The theme of the congress is 'Designing Out Hi-Tech Crime', an examination of pre-emptive action. A series of interactive workshops will be held over the course of the two days, with the common goal of 'designing out' hi-tech crime. For more information including registration details, see http://www.e-crimecongress.org/.

The Open University will host a one-day anti-virus conference entitled 'Combating Vandalism in Cyberspace' on 4 March 2004 in Milton Keynes, UK. The conference aims to raise awareness among end users of viruses, spam and hoaxes. Registration costs £150 for corporate attendees and £100 for those from educational institutions. For full details see http://tscp.open.ac.uk/.

The 7th Annual Websec Conference takes place 9–11 March 2004 in London, UK. The three-day, three-stream conference aims to update security professionals on strategic management issues and the latest technical developments in securing e-business infrastructure and web applications. Optional workshops will be held on 8 and 12 March. See http://www.mistieurope.com/.

InterNetSecurity Trade Fair will be held 15–18 March 2004 in St Petersburg, Russian Federation. For details see http://www.iegexpo.com/.

InfoSec World Conference and Expo 2004 takes place 22–24 March 2004 in Orlando, FL, USA. For details of the exhibition and a series of optional workshops see http://www.misti.com/.

Infosecurity Europe 2004 will be held from 27–29 April 2004 in the Grand Hall Olympia, London, UK. For all show details and registration enquiries see http://www.infosec.co.uk/.

The 3rd Annual DallasCon Wireless Security Conference takes place 1–2 May 2004, in Dallas, TX, USA. The conference will feature two tracks: one track dedicated to the latest trends and threats in wireless security and a second track focusing on general information security. For details see http://www.dallascon.com/.

The EICAR Conference 2004 will be held in Luxembourg City, from 1–4 May 2004. EICAR 2004 will feature only one stream, which will give in-depth coverage of issues including malware, critical infrastructure protection, legal and operational issues, and identity management and social issues. More information is available from http://www.eicar.org/.

RSA Japan takes place 31 May to 1 June 2004 at the Akasaka Prince Hotel, Tokyo. For details see http://www.rsaconference.com/.

NetSec will take place 14–16 June 2004 in San Francisco, CA, USA. The conference programme covers a broad array of topics, from the management issues of awareness, privacy and policy to more technical issues like wireless security, VPNs and Internet security. For full details see http://www.gocsi.com.

The 14th Virus Bulletin International Conference and Exhibition, VB2004, takes place 29 September to 1 October 2004 at the Fairmont Chicago, IL, USA. *Virus Bulletin* is currently seeking submissions from those wishing to present at the conference. For more information about the conference, including the full call for papers, and details of sponsorship and exhibition opportunities, see http://www.virusbtn.com/.

The 31st Annual Computer Security Conference and Expo will take place from 8–10 November 2004 at the Marriott Wardman Park in Washington, D.C., USA. More details will be available in due course from http://www.gocsi.com/.

ADVISORY BOARD

Pavel Baudis, *Alwil Software, Czech Republic*
Ray Glath, *Tavisco Ltd, USA*
Sarah Gordon, *Symantec Corporation, USA*
Shimon Gruper, *Aladdin Knowledge Systems Ltd, Israel*
Dmitry Gryaznov, *Network Associates, USA*
Joe Hartmann, *Trend Micro, USA*
Dr Jan Hruska, *Sophos Plc, UK*
Jakub Kaminski, *Computer Associates, Australia*
Eugene Kaspersky, *Kaspersky Lab, Russia*
Jimmy Kuo, *Network Associates, USA*
Costin Raiu, *Kaspersky Lab, Russia*
PéterSzör, *Symantec Corporation, USA*
Roger Thompson, *PestPatrol, USA*
Joseph Wells, *Fortinet, USA*

SUBSCRIPTION RATES

Subscription price for 1 year (12 issues) including first-class/airmail delivery: £195 (US$310)

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 www.virusbtn.com

No responsibility is assumed by the Publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein.

This publication has been registered with the Copyright Clearance Centre Ltd. Consent is given for copying of articles for personal or internal use, or for personal use of specific clients. The consent is given on the condition that the copier pays through the Centre the per-copy fee stated below.

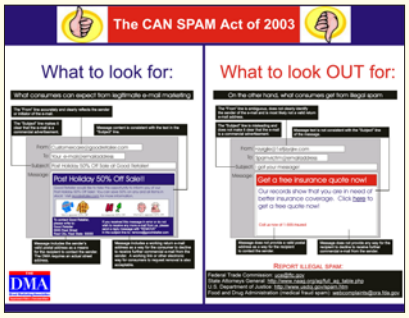
VIRUS BULLETIN © 2004 Virus Bulletin Ltd,The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England. Tel: +44 (0)1235 555139. /2004/$0.00+2.50. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

vb Spam supplement

CONTENTS

NEWS & EVENTS

EMAIL COACHING FOR MARKETERS



The Direct Marketing Association (DMA) has released a quick-glance reference guide for marketers entitled 'The CAN SPAM Act of 2003: What to Look For, What to Look OUT For'. The single-page guide provides graphical illustrations to contrast between a legitimate marketing email that complies with the law ('What to look for') and an illegal spam email that does not ('What to look OUT for'). [*Unfortunately, to the eyes of one who receives an overwhelming volume of spam on a daily basis (and who doesn't?), both examples look equally offensive - Ed.*] In addition, the DMA is running a series of briefings this month to bring its members up to speed on how to comply with the new federal anti-spam legislation and on 'how to proceed into an uncertain future'. See http://www.the-dma.org/.

SPAMMERS BROUGHT TO JUSTICE

The new year saw a flurry of reports of spammers being brought to justice, with prosecutions being made in Denmark, the USA and India.

A Danish businessman was convicted last month of having sent more than 10,000 unsolicited emails. In Denmark the practice of sending unsolicited emails has been illegal since June 2000 under the Marketing Practices Act. Danish authorities issued the man with a 400,000 Dkr fine (approximately £37,000) – a record fine for this kind of offence in Denmark.

In the US, meanwhile, a middle-aged Ohio woman who found herself in hot water after she spammed an off-duty FBI computer crime expert, was sentenced to 46 months in prison. Helen Carr, aged 55, was operating a 'phishing' scam – both Carr and her accomplice pleaded guilty to a conspiracy charge, having used spam as a means to elicit credit card details from hundreds of unwitting recipients.

Finally, in India, despite there being no laws governing the use of email, a New Delhi judge has ordered *McCoy Infosystems Private Ltd* to stop sending unsolicited bulk email to any user of the state-owned ISP *VSN Limited* (*VSNL*). The prosecutors built their case around the claim that, by sending large amounts of unsolicited email to *VSNL*'s users, the spamming company was 'trespassing' on *VSNL*'s property and breaching the privacy of *VSNL* and its subscribers.

AN END TO 419 SPAM?

Fed up of the stigma that 419 email scammers bring to Nigeria's reputation and keen to build investor confidence in the country, Nigeria's minister of finance Ngozi Okonjo-Iweala is leading a campaign against email fraud.

In late January the Federal Government of Nigeria approved a proposed amendment bill for changes to the infamous 419 Advance Fee Fraud Act. The amendments require all telephone and cyber café commercial operators to register with the Nigerian Communication Commission. Operators who fail to comply with the new requirements will be liable to imprisonment or a substantial fine, while any workers in financial institutions or bureaux de change found to be aiding in the contravention of the law will be liable to both a prison term and a ban from their respective operating point.

Other plans in the minister's campaign against email fraud include training the country's police force in combating cybercrime and the launch of a global advertising campaign to warn potential victims. Unfortunately, as pointed out by Martin Overton in his *VB* article 'Out of Africa' (see *VB*, May 2003, p.15), the 419 scam has 'travelled' in recent

years – with versions now coming from Dubai, South Africa, Sierra Leone, Zimbabwe, Angola, Taiwan, Togo, Germany and Iraq to name just a few – so no matter how tough Nigeria gets with scammers, it looks like the 419 scam and its derivatives are here to stay.

CONGRESSIONAL ATTACK ON INBOXES

While congratulating themselves for (supposedly) stemming the flow of spam with the passage of the CAN-SPAM anti-spam legislation, US Congressional representatives have at the same time been purchasing email lists with the intent to carry out bulk mailing of unsolicited mail.

According to *PCWorld* (http://www.pcworld.com/), more than 30 members of Congress have purchased lists of constituents' email addresses from e-marketing consulting firm *Rightclick Strategies*. Meanwhile, more than 20 members are customers of *@dvocacy* whose *Connected Constituency* program promises to deliver a 'cost-effective way to let you reach tens of thousands of your constituents instantly' using *ConstituentMail* – which 'makes it easy for your message to spread virally across the Internet'.

Of course, members of Congress may be mindful of the new laws concerning mass emailing, but a loophole for political mail allows members to send messages freely to constituents who have subscribed to their email lists – and to build these lists, the so-called 'franking privilege' allows Congress members to send bulk unsolicited email messages to their constituents. While these are not commercial emails, the fact remains that for many recipients they will represent nothing more than an addition to the groaning volume of unwanted email in their inboxes.

As far as spam is concerned here, it seems to be a case of what one hand taketh away, the other hand giveth …

EVENTS

An exhibition running until 7 February 2004 at a New York art gallery depicts how an archaeologist 450 million years in the future might present current culture, based only on relics of spam. See http://www.thetanknyc.com/.

The NIST/CSD Spam Technology Workshop takes place on 17 February 2004 at NIST Gaithersburg Campus, USA. For full details see http://csrc.nist.gov/spam/.

101TechStrategies will hold an Anti-Spam Summit from 17–19 March 2004 in San Francisco, USA. For details see http://www.101techstrategies.com/.

The First Conference on Email and Anti-Spam (CEAS) will be held 30 July to 1 August 2004 in Mountain View, CA, USA. Further details can be found at http://www.ceas.cc/.

SPOTLIGHT

DELIVERING THE GOODS

Helen Martin

Habeas is a young company making the headlines with its unique spin on combating the problem of unsolicited email – the company uses copyright and trademark law as a powerful tool against spammers.

Rather than blocking spam, the *Habeas* approach is to authenticate legitimate email. The authentication takes the form of a number of lines in the email x-header, which contain both a copyright-protected haiku and a trademark. Consequently, any misuse of the header content constitutes both breach of copyright and trademark violation.

POETRY IN MOTION

The company was founded about a year and a half ago when company chairman Dan Kohn came up with the idea after playing around with the settings of *SpamAssassin*. He noticed that the more he tightened down the filters to remove spam from his inbox, the more legitimate messages were being misclassified as spam and filtered out. Fascinated by the problem of how to reduce or eliminate false positives, he came up with his idea for certifying legitimate email.

The set of x-headers, which is known as the Habeas Warrant Mark (HWM), is protected by copyright law because it contains a haiku (a Japanese form of poetry) – unlike names, titles and slogans, poetry is protected by copyright law. The warrant mark is further protected by trademark law because the headers also contain a trademark:

```
X-Habeas-SWE-1: winter into spring
X-Habeas-SWE-2: brightly anticipated
X-Habeas-SWE-3: like Habeas SWE (tm)
X-Habeas-SWE-4: Copyright 2002 Habeas (tm)
X-Habeas-SWE-5: Sender Warranted Email (SWE)(tm). The
                sender of this
X-Habeas-SWE-6: email in exchange for a license for
                this Habeas
X-Habeas-SWE-7: warrant mark warrants that this is a
                Habeas Compliant
X-Habeas-SWE-8: Message (HCM) and not spam. Please
                report use of this
X-Habeas-SWE-9: mark in spam to
                <http://www.habeas.com/report/>.
```

The headers may be licensed by companies whose emailing practices comply with a set of 'best practice' requirements: they must offer a functional unsubscribe facility on all emails they send to customers; they must have a removal policy for repeated email bounces and a bounce rate of no more than five per cent for any mailing list they use; and they must have obtained verified permission from the

recipients to receive their emails. Should any licensee fail to comply with these conditions, the licence will be revoked and the licensee will be liable to *Habeas* for damages.

PILLARS OF SUPPORT

The company is supported by an advisory board consisting of luminaries from the anti-spam, Internet service and legal fields. According to CEO Des Cahill, the advisory board plays a vital role, being called upon frequently to advise about email usage, Internet standards, developments in the industry and so on. He says: 'There's a huge *esprit de corps* in the community where everyone takes a common view of the spam problem as an inherently evil thing. *Habeas* is seen as having the right kind of focus on trying to stop spam and get legitimate email delivered – and that translates into a lot of support for the company.'

Indeed, the level of support the company enjoys within the anti-spam community is an integral part of the company model. *Habeas* claims to monitor the Internet 24/7 for reports of misuse of its warrant mark. This is achieved by the systematic deployment of spam traps and scripts run by hundreds of individuals in the mail abuse/anti-spam community. Any suspect mail that is trapped and that includes the *Habeas* x-headers is passed on to the company for further investigation. In addition, any user can report the suspected misuse of the warrant mark directly to *Habeas* – the headers themselves include the relevant contact information.

LAYING DOWN THE LAW

Once a breach is discovered, the IP address from which the messages have been sent is placed on a blacklist – the Habeas Infringers List – which can be cross-referenced by spam filters. Recent versions of *SpamAssassin*, for example, will query the list automatically upon receipt of an email containing the *Habeas* x-headers.

The company can then get down to the serious business of tracing the perpetrator in order to pursue legal action.

Tracking down offenders is not often an easy task – particularly when, as is often the case, spam is being sent from servers based offshore. However, the vast majority of spam messages tend to promote products or services sold within the United States. According to Des Cahill, 'a very effective technique [for tracing the spammers] is to "follow the money" – so, if you are getting spam from servers in Malaysia promoting Viagra that can be purchased from a mail order company in the United States, you go after the guys in the US, and that leads you down a trail to the responsible individual.'

In its relatively short history the company has filed lawsuits against a number of entities whose emailing practices were in breach of the terms of use of the Habeas Warrant Mark. In August 2003 the company claimed victory in the first of these cases. The defendant was banned from sending any type of unsolicited commercial or promotional messages, regardless of whether the messages contain the *Habeas* mark.

As well as the Habeas Infringers List, the company also maintains a whitelist – a DNS-based IP address listing of *Habeas* licensees. This list is made available to ISPs and anti-spam companies to aid in the deliverability of licensees' mail.

FUTURE OUTLOOK

In January 2004, *Habeas* came under persistent attack from an (at the time of writing) unidentified spammer misusing the Habeas Warrant Mark. This instance is of particular note because the spam seemed to be coming from a distributed set of zombie machines on broadband connections – the likely result of a virus infection.

While unable to comment on the specific methods being used to 'agressively pursue' this offender(s), Des Cahill does feel confident that the company will be able to bring the responsible parties to justice. In the meantime, *Habeas* has begun the process of systematically adding the IP addresses of the hundreds of compromised PCs to the Habeas Infringers List.

As we are seeing an ever-increasing number of malware threats that seem likely to have been written for the purpose of spamming – for example W32/Sobig (see *VB*, October 2003 p.5), W32/Mimail (see *VB*, September 2003 p.4) and W32/Bagle – Cahill believes that the anti-spam and anti-virus communities will need to work closely together in the future in order to forestall or at least monitor these kinds of attack.

For Cahill, the outcome of the first stage in the war on spam is clear: it's a stalemate. 'There are the technical solutions – peer-to-peer voting, Bayesian filtering, rules-based filtering, blacklisting – and there are various legislations and there is still an incredible volume of spam, and it's growing – we're in an arms race right now.'

He feels that the next phase of the battle is about taking the kind of approach that *Habeas* takes: 'Up until now the anti-spam industry has been concentrating on identifying and blocking out the bad mail. Now, I think it's about flipping the problem on its head and saying "how do I set up a system and an infrastructure for identifying legitimate mailers?" I think it's inevitable that such an infrastructure needs to be developed more formally – that's why I'm at *Habeas* and why we're having so much fun.'

SUMMARY

ASRG SUMMARY: JANUARY 2004

Pete Sergeant

The postings to ASRG over the last month have posed a few interesting legal questions and brought to light some interesting statistics.

Hector Santos expressed concern that the US CAN-SPAM Act will give spammers legal recourse to sue or harass ISPs/anti-spam companies who block spam that complies with this law. However, Philip Miller said he thought this would not be the case, since CAN-SPAM defines only what senders *cannot* legally do. Hector disagreed, saying that the Act does not attempt to change any current policy or status quo, and that it was a 'long-standing practice held by ECPA [Electronic Communications Privacy Act] precedence' that once you accept a message, it must be delivered.

Denny Figuerres suggested that, by permitting some content to be 'published', but not permitting other similar content to be 'published', one is effectively engaging in the role of 'Editor/Publisher', which can cause legal problems – ISPs having encountered similar problems with censoring some Usenet groups. John Levine indicated that, in fact, US law 'provides broad immunity from liability due to good faith efforts to filter offensive material'.

Clearly, 'mathew' was feeling a little cynical when he said that he thought 'any kind of "ADV" flag belongs in the header defined for the purpose, so it won't collide with existing use of the subject line no matter how inevitably poorly client developers implement filtering.' He provided a real-world example of a mailing-list tag that he thought might be problematic ('[sec-adv] Security advisory'). Jon Kyme pointed out that the Act requires clear labelling of the email as such – either all MUAs (Mail User Agents) would have to adapt to read the new headers, or the marker would have to remain in the subject line itself.

Hector Santos, who himself develops SMTP server software thinks that, in the future, customers looking for an SMTP server will ask one basic question: 'Is your system CAN-SPAM ready?' Yakov Shafranovich happened to be in touch with a provider of email 'hosting' services, who claimed to be 'CAN-SPAM-friendly'– a telling transcript can be found at http://article.gmane.org/gmane.ietf.asrg/7698.

Eric Dean reported that he had accidentally been sent the entire year-to-date spam history of a company with which he does business. After sanitizing to protect the innocent, Eric posted the statistics to the list. Interested parties can check out the data here: https://www1.ietf.org/mail-archive/working-groups/asrg/current/msg08868.html. More statistics came from B. Johannessen, who posted a link to the results of his recent spam analysis: http://db.org/spam/.

John Levine wondered whether one of the reasons spam is more prevalent over SMTP than NNTP is because of the possibility of a Usenet Death Penalty (UDP) – a listing on an all-pervasive email real-time blackhole list – or whether it was simply because there is such an abundance of email users that spammers don't bother trying to get their messages onto Usenet.

Gordon Peterson had an interesting idea for reducing some of the collateral damage caused by spam. His idea was to impose a size limit and content restriction (nothing but plain text) on all unsolicited emails – in order to send large files and HTML, you must be in your recipient's whitelist. This would render a number of spammers' tricks (large sections of unrelated text, embedded images, etc.) useless, while friends would still be able to send each other cute little HTML postcards, or whatever floats their boats. This idea was reflected, to some extent, by Denny Figuerres, who suggested that a subset of HTML be defined for use in email, and that MUAs should support only that, dropping support for embedded images and scripting in email.

John Fenley had read some work on stylometric classification, and suggested the use of Support Vector Machines (SVM) in anti-spam. Art Pollard pointed out that, compared to Bayesian filtering, SVMs take a lot longer to train, and need some serious horsepower.

Finally, Yakov announced the formation and reformation of a number of subgroups:

- The *Abuse Reporting Standards Subgroup* will investigate standards for email and network abuse reports. It will coordinate with similar efforts in the IETF.
- The *Best Current Practices Subgroup* will research and document best practices for spam management.
- The *Filtering Standards Subgroup* will investigate standards for filtering for automatic updates and sharing of filtering information, and better interaction between filters, MTAs and MUAs.
- The *Inventory of Problems Subgroup* will research and list problems in the current email architecture relevant to spam.
- The *Message Verification Subgroup* will research solutions for verifying and authenticating email messages and header information.
- The *SMTP Session Verification (SMTP-VERIFY) Subgroup* will research approaches for authenticating and verifying the SMTP session.

More information about these can be found at the new ASRG website: http://asrg.sp.am/.