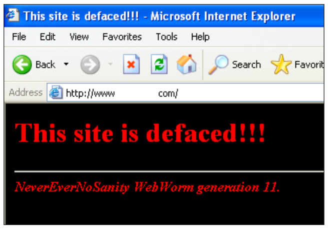
MARCH 2005

virus BULLETIN

The International Publication on Computer Virus Prevention, Recognition and Removal

CONTENTS

IN THIS ISSUE



This site is defaced!!!

NeverEverNoSanity WebWorm generation 11.

RATTLING THE PERLY GATES

Perl/Santy is, essentially, a small piece of Perl code that spreads to vulnerable web servers located using the *Google* search engine. Frédéric Perriot describes Santy's unusual replication strategy and explains why this worm exemplifies the need for the 'defence in depth' approach.

page 4

HOME SWEET HOME

Randy Abrams looks at how the security support needs and behaviours of home users have changed over the years, and describes how *Microsoft* is adapting to maximise customer support now that consumers' first port of call is their ISP.

page 6

vbSpam supplement

This month: anti-spam news & events; review of *Fighting Spam for Dummies*; MIT Spam Conference report; ASRG summary.

ISSN 0956-9979

‘The number of phishing attacks, and the associated costs, are increasing.’

David Emm
Kaspersky Labs, UK

PLENTY OF PHISH IN THE SEA

In the last 12 months or so we have seen a growing commercialisation of malware, with malicious code written (and ‘leased’ to the criminal underground) for the specific purpose of making money illegally. The increase in phishing scams is one part of this phenomenon.

The financial losses resulting from phishing scams are no easier to quantify than those resulting from viruses, worms and Trojans. Search online and you will find estimates ranging from $400 million to $2.4 billion. However, one fact is clear: the number of phishing attacks, and the associated costs, are increasing. According to the Anti-Phishing Working Group, between July 2004 and December 2004, there was a 38 per cent average monthly growth rate in the number of new, unique phishing email messages; and a 24 per cent average monthly growth rate in the number of unique fraudulent websites.

In a typical phishing scam, the phishers create a fake website which looks as similar as possible to that of a target financial institution or other organisation. Then they send out emails that purport to be from the target organisation, using genuine logos, good business style and even the names of senior management. They spoof the header of the email to make it look even more legitimate. Typically the email states that the organisation has changed its IT structure, and customers are required to re-enter their user data. The email lures the recipient into clicking on a link that directs them straight to the spoofed website where they are asked to enter their personal information, providing the phishers with access to the victim’s bank details, credit card, or on-line shopping account.

In any single scam, only a small proportion of recipients will be customers of the spoofed organization, and only a small proportion of these will ‘take the bait’. However, as with spam, such large volumes of messages are sent that even a low response rate harvests enough data to make the scam worthwhile.

Some phishers also place exploits for *Internet Explorer* (*IE*) vulnerabilities on their sites. When the victim views the fake site, the exploit uploads a Trojan to the victim’s computer. As a result, not only is the user’s banking information harvested, but their machine becomes part of a zombie network that can be used for other malicious activities – such as DDoS attacks designed to extort money from victim organizations, for use as a spamming platform, or to spread other malware.

Some phishers now make use of vulnerabilities to make their scams less obvious. An *IE* vulnerability documented by *Microsoft* in late 2003 (for which a patch is now available) allows phishers to create fake websites that not only have the look and feel of a legitimate site, but which also display the URL of a genuine site. When the user clicks on the link in the phisher’s email, the web browser displays content from the fake website, but the URL in the browser window is that of the genuine bank.

In November 2004, phishers found a way to bypass the need for the victim user to click on a bogus link. Script instructions embedded within an HTML email edit the hosts file on the victim’s machine and, as a result, the next time the user directs their browser to their bank’s website, it is automatically redirected to a fraudulent site, where any input can be captured. The user has no reason to think that there is anything different about the way in which they have accessed their bank’s website.

Since phishing scams continue to grow, it is becoming ever more important that we urge users to exercise caution, to minimise the risk of getting ‘hooked’ by the phishers.

- Don’t divulge passwords, PINs, etc.
- Don’t fill out forms contained in emails.
- Don’t click on links in emails.
- If using *IE*, use the lock symbol in the status bar to confirm the site being accessed.
- Check bank accounts regularly and report anything suspicious.

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

MICROSOFT ONE STEP CLOSER TO AV

The news that set industry analysts chattering (and doom-sayers prophesying) last month was *Microsoft*'s acquisition of email-scanning software provider *Sybari Software Inc*. Reaction to the news has been mixed – the feeling of many is that, rather than attempting to enter the AV market itself, *Microsoft* should concentrate its efforts on securing its current products. Analysts predict that the biggest AV vendors, *Symantec*, *McAfee* and *Trend Micro*, will feel the pressure from *Microsoft*'s entry into the market (indeed share prices of *McAfee* and *Symantec* saw a dip immediately following the announcement) and that smaller security firms will face a struggle to remain in the market.

What makes the acquisition intriguing is that *Sybari*'s product (*Antigen*) does not have its own scanning engine – instead it allows customers to use virus engines from multiple vendors (which currently include *AhnLab*, *Authentium*, *CA*, *Kaspersky*, *Norman*, *Sophos* and *VirusBuster*). *Symantec* representatives have been quick to identify this as a weakness, saying 'The acquisition does not provide *Microsoft* with the security and AV response infrastructure necessary to support the virus protection needs of enterprise customers.' Perhaps in their haste, however, they overlooked the fact that *Microsoft* has had the Romanian *GeCAD* AV technology on the backburner since mid-2003 and has said that it plans to add this to the options that run on *Antigen*. Gene Hodges, president of *McAfee Inc.,* is confident that his company's reputation will keep customers loyal, saying, 'We've stopped millions of viruses this year, and *Microsoft* hasn't stopped one. So let's fight.' Interesting times lie ahead.

ERRATA: FEBRUARY 2005 WINDOWS NT COMPARATIVE REVIEW

Virus Bulletin regrets that the *Windows NT Workstation* comparative review published in the February 2005 issue of *VB* (see *VB*, February 2005, p.12) contained two errors.

First, *AhnLab V3 VirusBlock* was noted as having missed a single file in the In the Wild (ItW) test set. However, the apparent miss proved to have been caused by an error in the parsing of the product's log files. *V3 VirusBlock* is thus owed a VB 100% award.

Secondly, *F-Secure Anti-Virus 5.43* was noted as having missed several files in the ItW test set. However, subsequent investigation indicated that the product's update process had not completed before the test. After further testing, allowing longer delays after updating, all ItW files were detected. *F-Secure Anti-Virus* is thus entitled to a VB 100%.

Virus Bulletin apologises for the errors and points readers to http://www.virusbtn.com/vb100/about/ for an up-to-date summary of the results of recent comparative reviews.

Prevalence Table – January 2005

Virus	Type	Incidents	Reports
Win32/Netsky	File	64,413	61.48%
Win32/Bagle	File	21,980	20.98%
Win32/Sober	File	10,949	10.45%
Win32/Bagz	File	1,010	0.96%
Win32/Zafi	File	846	0.81%
Win32/Mydoom	File	772	0.74%
Win32/Dumaru	File	755	0.72%
Win32/Mabutu	File	552	0.53%
Win32/Funlove	File	434	0.41%
Win32/Klez	File	412	0.39%
Win32/Sobig	File	412	0.39%
Win32/Lovgate	File	363	0.35%
Win32/Valla	File	312	0.30%
Win32/Bugbear	File	203	0.19%
Win32/Mimail	File	129	0.12%
Win32/Swen	File	106	0.10%
Win32/Mywife	File	100	0.10%
Redlof	Script	90	0.09%
Win32/Pate	File	90	0.09%
Win32/Fizzer	File	84	0.08%
Win32/Yaha	File	77	0.07%
Win32/Mota	File	70	0.07%
Win32/Hybris	File	50	0.05%
Mumu	Script	47	0.04%
Win95/Tenrobot	File	43	0.04%
Win32/Mylife	File	40	0.04%
Win95/Spaces	File	39	0.04%
Win32/Nachi	File	36	0.03%
Win32/Kriz	File	34	0.03%
Win32/Buchon	File	27	0.03%
Win32/BadTrans	File	22	0.02%
Win32/Magistr	File	22	0.02%
Others[1]		244	0.23%
Total		**104,763**	**100%**

[1] The Prevalence Table includes a total of 244 reports across 56 further viruses. Readers are reminded that a complete listing is posted at http://www.virusbtn.com/Prevalence/.

VIRUS ANALYSIS

BLACK PERL

Frédéric Perriot
Symantec Security Response, USA

Besides a heap of email worms and a big pile of buffer overflow bots, 2004 also brought a few original viruses. Perl/Santy.A, which appeared in December 2004, is one such virus. Santy replicates to web servers running the bulletin board framework phpBB. It does so by exploiting a script injection vulnerability in phpBB, which is present in versions of the software prior to version 2.0.11.

Santy is, essentially, a small piece of Perl code that spreads to vulnerable web servers that it locates using the *Google* search engine. Even though the vulnerability it exploits resides in PHP code, Santy is written in Perl. The PHP language would have seemed like a natural choice, but instead the worm author chose to use as little PHP as possible: only small snippets of PHP code are injected to upload the worm and invoke a Perl interpreter. Santy's replication strategy sets it apart from usual worms. Let us see how.

CHAIRMAN OF THE BOARD

phpBB is a very popular open-source bulletin board software package. Discussion forums of all kinds – including security-related ones – use phpBB (just type 'powered by phpBB' in your favourite search engine, and millions of hits will come up).

At the end of November 2004, a vulnerability in phpBB was announced, affecting the 'highlight' functionality of the 'viewtopic.php' page. Shortly thereafter, a proof-of-concept exploit surfaced that demonstrated the severity of the vulnerability. This prompted the phpBB authors to fix the bug in a new version of their software (version 2.0.11).

About a month later, on 21 December 2004, Santy systematically exploited the 'viewtopic' vulnerability in order to spread. Thanks to the worm's website defacement payload (which will be described later), it was possible to evaluate the number of infected websites by querying some search engines. Between a few thousand and a few tens of thousands of sites were affected. (Search engines report defaced web pages, rather than individual websites, hence the rather wide range of this estimate.)

DO AS I SAY

The 'viewtopic' vulnerability exploited by Santy results from a lack of user input validation. By submitting a specially crafted 'highlight' request to the 'viewtopic.php' page of a vulnerable phpBB server, a user can cause arbitrary PHP code to execute in the context of the 'viewtopic.php' script.

The script injection occurs in a tortuous line of PHP code, involving two nested calls to the preg_replace() function, responsible for string substitutions. Somewhere in there, unsanitized user data is evaluated as part of a dynamically generated script snippet. Ironically, the faulty line is even commented in the phpBB source as having been 'shamelessly "borrowed"' from a coding manual.

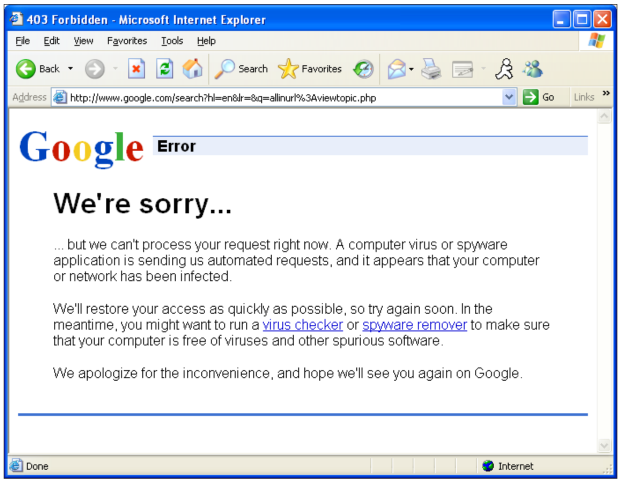
The exploit string arrives as part of an HTTP request for the 'viewtopic.php' page. It employs double URL-encoding to achieve script injection, in a manner reminiscent of Nimda's attack on web servers (but, unlike Nimda, the peculiar encoding is not for the purpose of directory traversal here).

OGLING YOUR WEB SITE

Rather than scanning the IP address space for target web servers, Santy uses the *Google* search engine as a 'metaserver' (that is, a directory of servers).

The worm uses an advanced search feature of *Google* to look for pages whose URLs contain the string 'viewtopic.php', along with a topic identifier. The topic identifier, a random number between 0 and 29999, introduces some variability in the search requests and thus reduces the likelihood of multiple copies of the worm hitting the same targets repeatedly.

The metaserver approach to locating potential targets has been used by a few email worms to collect recipient addresses (for instance W32/Toal.A@mm queried ICQ white pages for email addresses) and frequently to determine mail servers (by querying MX records from the



http://www.google.com/search?hl=en&lr=&q=allinurl%3Aviewtopic.php

Error

We're sorry...

... but we can't process your request right now. A computer virus or spyware application is sending us automated requests, and it appears that your computer or network has been infected.

We'll restore your access as quickly as possible, so try again soon. In the meantime, you might want to run a virus checker or spyware remover to make sure that your computer is free of viruses and other spurious software.

We apologize for the inconvenience, and hope we'll see you again on Google.

Figure 1: The result of a Santy query on Google today.

DNS), but exploit-based worms have generally shied away from it, preferring random IP scanning.

Even if the metaserver introduces a single point of failure for a worm (as demonstrated by *Google* when it blocked Santy's queries; see Figure 1 for the result of a Santy query today), it is also much more efficient than random scanning at finding potential victims on the vast Internet.

In the case of Santy, the target search is also a form of fingerprinting that selects websites that are very likely to run phpBB. It is reasonable to expect the metaserver technique to be reused by malware in the future, as well as hybrid techniques employing a combination of metaservers and scanning.

BEST THING SINCE SLICED BREAD

Once Santy gets the results of its search request, it parses the HTML pages returned by *Google* to extract the URLs of potentially vulnerable sites. Against each URL, the first attack is attempted through an HTTP request to 'viewtopic.php'. If successful, the attack causes the server to return a special marker to the worm, and to create a transfer file called 'm1ho2of' on the remote host. If the marker comes back from the server, the worm proceeds to upload and run itself there.

Interestingly, Santy does not upload itself to the server in one go. Instead, it splits its code into segments of 20 characters, and sends each one in turn. Each segment is uploaded via the 'viewtopic' vulnerability, through the injection and execution of a snippet of PHP code that opens and writes to the transfer file.

Therefore, servers are exploited not once but multiple times – hundreds of times in fact. Each attack causes a segment of the worm to be appended to the transfer file. Finally, the last attack causes the 'viewtopic.php' page to invoke the Perl interpreter and run the transfer file containing the worm code, thereby closing the infection cycle.

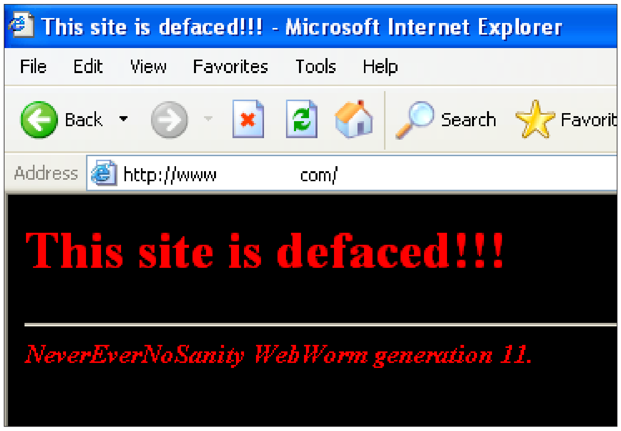
The slicing of the worm into 20-character segments is probably not gratuitous. Transferring the worm in one go would have resulted in a long GET request about 50 kilobytes long – enough to raise suspicion among IDSs and filtering devices. On the other hand, a succession of small GET requests is a common network traffic pattern, and therefore more likely to bypass network defences successfully.

However, the slicing of the worm into small segments also has an unexpectedly adverse effect on Santy's propagation: it causes corruptions during replication. In the real world, unsynchronized accesses to the transfer file by several web server instances (usually Apache instances) result in a number of worm segments being dropped. Occasionally the transfer file contains an invalid Perl script, which does not even pass compilation.

ELEPHANT WORM

Santy's payload consists of defacing the websites it infects. Upon startup, the worm gathers a list of 'root' directories. These include the '/' (slash) directory, the list of drives from 'A:' to 'Z:' (targeting *Windows* platforms), and the home directories of all users, gathered from the password file (for Unix-like platforms).

Then, Santy visits all subdirectories of these roots, looking for files whose names contain '.htm', '.php', '.asp', '.shtm', '.jsp' or '.phtm'. It replaces all such files with a copy of the defacement page (see an example in Figure 2 below).



This site is defaced!!!

NeverEverNoSanity WebWorm generation 11.

Figure 2: Example of a Santy defacement page.

The generation counter on the page reflects a variable which is updated by the worm each time it starts. This variable is sufficiently faithful to plot a graph of the worm instances by

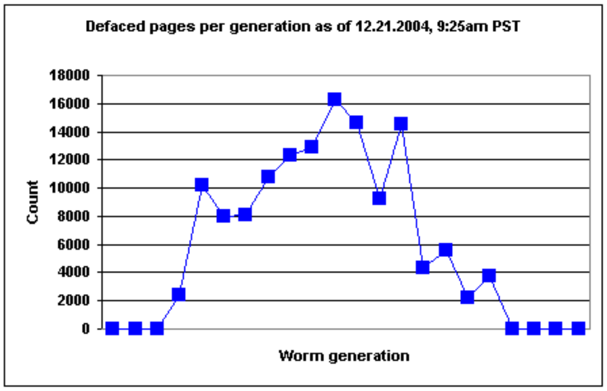


Figure 3: Number of defaced pages produced per generation – the result of a search query carried out on 21 December 2004 at 9:25am.

generation. A search query carried out on 21 December 2004 at 9:25am PST, gives the distribution shown in Figure 3. Note that the payload routine is triggered only on generation 4 and later, which explains the absence of defaced pages with a generation counter of 1, 2 or 3 (or 0, for hackers at heart).

As for platform dependency, the worm works on *Windows* as well as Unix-derived systems. Although, at first glance, it may seem that the worm uses Unix-like features (such as the getpwent() and fork() Perl keywords), it is careful to enclose them within eval{ } blocks, so as to catch exceptions that may result from non-implemented features on the current platform.

Santy also features a self-deletion trick that has a Unix flavour to it (the idea was originally used by the 1988 Internet worm), but which really works on *Windows* too: when it runs, Santy loads its own source code from its program file (for replication purposes), then deletes the file from underneath the running script.

This is an effective concealment method, and probably explains why most samples of Santy received by AV researchers from the field were, in fact, corrupted. Fortunately, reconstruction of the worm code from web server log files is possible.

DEFENCE IN DEPTH

Santy exemplifies the need for the 'defence in depth' approach. Riding HTTP, it is allowed through the firewall by design. Unlike a CodeRed, however, it will not be stopped by a buffer overflow protection, because it uses a higher-level method of turning data into code: the omnipotent 'eval' keyword of modern dynamic languages like PHP and Perl.

Proper use of the data-tainting feature built into the server-side language, and the use of a tight RSBAC (Rule Set Based Access Control) setup to limit the actions allowed to the web server, offer the extra protection layers to mitigate this kind of threat.

Perl/Santy.A

Aliases:	PHP/Santy.worm, Worm.PhpBB.Santy.A, Net-Worm.Perl.Santy.a.
Type:	phpBB worm replicating through a server-side script injection vulnerability.
Payload:	Defaces web pages.

FEATURE 1

PROTECTING THE HOME USER

Randy Abrams
Microsoft, USA

Remember when 'tech support' meant RTFM (Read The Fine Manual)? Remember when the manual weighed more than the media the software came on, and people did read it, and even understood it?

In the early days of the PC, users had to learn how to use a command line and either resolved problems themselves or knew someone who had been down the same road shortly before them and had already encountered (and resolved) the problem.

For the most part, users did not have to worry about security back then, as their PCs were not connected to the Internet. Of course there were some exceptions, but they were few and far between. Of those users whose computers were connected to the Internet, few worried about security and few understood security – witness the pervasiveness of the UNIX-based Morris Internet worm in 1988. For PC users viruses were relatively rare and if virus-related support was needed, they called their anti-virus company.

THE UNCONNECTED HOME USER

When *Microsoft* released *Windows 3.1*, the personal computer was made significantly easier to use and a new breed of user was introduced: the technically unsophisticated home user.

At the time, home users had relatively few security concerns and only a handful of them used anti-virus software. As far as most users were concerned, a firewall was the metal shield in the car between the engine compartment and the passenger compartment.

This was the beginning of an age of users who did not understand the difference between an operating system and a word processing program. Still, somehow the small number of users who did run anti-virus software knew that they needed to contact their anti-virus vendor for support when there was a virus problem. However, anti-virus companies soon began to notice that users didn't understand what a virus was, or what it could and could not do, and as a result these users also called their anti-virus vendor's support line when they encountered a problem with autoexec.bat, config.sys, or a mis-configured application.

Anti-virus tech support calls required support capabilities that went far beyond anti-virus software. Many anti-virus companies attempted to help the users with their problems, even though it was not their anti-virus software that was the issue. The anti-virus companies understood that if the problem wasn't resolved when the user called, the customer would not be happy. Making the customer happy (by solving their non AV-related problems) was generally better for business.

THE CONNECTED HOME USER AND THE OEM SUPPORT MODEL

When *Windows 95* was released, the computing industry witnessed a major transformation of the consumer support model. OEM licensing agreements mandated that PC manufacturers who bundled *Windows 95* would also support their users for operating system issues.

Those users who built their own PCs or who bought retail copies of *Windows 95* still came to *Microsoft* for support, but if the user bought a *Dell*, *HP*, or an *IBM* computer, they were routed to the OEM reseller for support. With *Windows 95*, a breed of technically-naïve computer users began connecting to the Internet and the prevalence of computer viruses increased.

Now the OEMs found that they were in the position of needing to provide not only operating system support but also, in many cases, anti-virus support.

There have been a multitude of stories about OEM tech support personnel blaming any problem they couldn't resolve on a virus. Anti-virus companies began to find they were blamed for their product not catching the 'driver conflict virus' or the 'heavily fragmented file system virus', or any other number of configuration error 'viruses'. Clearly the OEMs needed to be able to provide their technical support staff with quality anti-virus training – but the availability of such training was, and even today remains, fairly scarce.

THE CONNECTED HOME USER TODAY

With the advent of widespread broadband connectivity the support model was about to undergo another drastic change. The collective technical skills of connected users are significantly lower now than in the pre-GUI days. Many users do not understand that *Office* is not *Windows* and that *Windows* is not the Internet.

The burden of support has shifted to the Internet Service Provider (ISP). If a virus causes the PC to reboot, it is the staff of the ISP who find themselves answering a support call with the customer claiming that the Internet is broken. Some users have even asked their ISP how it is that the worm was able to crawl up the cable and get into their computer! If there is a problem with *Outlook Express* retrieving email then 'the Internet is broken' and it must be an ISP issue. ISPs are fielding an ever-growing support burden for virus issues.

This change in whom customers look to for support necessitates a realization of the new dynamics and a strategy to maximize customer support within the framework of the ISP model is required. Some anti-virus companies have realized that the ISP is a new sales vector, but are any adapting to the support environment?

When Blaster evolved from germ to widespread infection, *Microsoft* experienced a tremendous spike in call volume. The day after Blaster was discovered in the wild, *Microsoft Product Support Services* received more calls than had ever been received in a single month. ISPs encountered similar call volumes.

At the time, there was no channel for an ISP to move ahead in *Microsoft*'s call queue, even though each call from a major ISP would have resulted in support for hundreds of thousands of users. *Microsoft* had mitigation strategies, but its relationships with the ISPs had not been developed and there was no effective means to get the information to the people who could help most effectively.

This was the genesis of *Microsoft*'s Global Infrastructure Alliance for Internet Safety (GIAIS) Program (see http://www.microsoft.com/serviceproviders/giais/). GIAIS is an alliance of large ISPs who provide Internet connectivity for the vast majority of *Windows* users throughout the world. The GIAIS vision is 'All member companies working in partnership for the protection of our mutual customers.'

DOES GIAIS WORK?

The Sasser worm had the potential for a Blaster-class impact, but this was not to be. Clear communication channels had already been established and used effectively. Prior to the release of Sasser, ISPs had been provided with an analysis of Microsoft Security Bulletin MS04-011 with specific focus on anticipated exploit approaches and corresponding mitigation techniques.

While Sasser still became a significant problem, GIAIS collaboration helped to reduce the worm's impact dramatically. Support call volumes were lowered significantly and ISPs were prepared to assist in mitigation and remediation efforts.

Security, of course, includes keeping up to date with patches and virus signatures and upgrading to more secure systems when possible. *Windows XP Service Pack 2* (*SP2*) represented the first major paradigm shift of the age-old adage 'functionality before security'. The changes in *SP2* were such that, had *Microsoft* simply released *SP2* as if it were just another service pack, ISPs would have been forced to tell their customers that it would not be supported and advise customers not to install it.

Microsoft worked extensively with the GIAIS partners around the release of *SP2* and GIAIS members were engaged early in the *SP2* beta process. Feedback was solicited and extensive training materials were provided in order to enable the ISP call centres to assist their customers with the upgrade. Consumer information concerning *SP2* was syndicated, further assisting ISPs in consumer education.

When *Windows 2000* was released, the message from many ISPs was that the operating system was not currently supported by the ISPs. Thanks to the effectiveness of the GIAIS program, many ISPs sent communications to their customers actively encouraging the upgrade – and they continue to do so today. ISPs were also able to prepare their customers so that consumers would not be prevented from connecting to their ISPs.

Mitigation of worms and the adoption of service packs are not the only protection strategies. Other issues affecting ISPs include spyware, phishing, botnets, child pornography and consumer security education. *Microsoft* and GIAIS member companies are collaborating to address all of these issues.

GIAIS members participate actively in the *Microsoft Windows AntiSpyware* beta program and their feedback represents a significant portion of the online home user community. By providing the ISPs with the opportunity to learn about the program prior to the release of the production code, the ISPs are in a better position to address their customers' support needs.

GIAIS partners have been working with government agencies and industry groups around the world on programs such as Sender ID and child protection initiatives. In the United States, *Microsoft* recently launched an education program in some public schools to educate students and their parents on how to use the Internet more safely. This program was developed and launched through the *Microsoft Consumer Security Mobilization Initiative*. US-based GIAIS members participated in this outreach program as well. (To find out more about the work done by the Consumer Security Mobilization Initiative, please visit http://www.microsoft.com/athome/security/default.mspx.)

To help address spam issues, some GIAIS ISPs have begun blocking Port 25 on home user accounts. The overwhelming majority of home users do not use Port 25 and do not notice when it is blocked, yet these ISPs have reported substantial decreases in spam originating from their users. GIAIS members also continue to participate in a variety of other projects designed to bring the spam problem under control, both within GIAIS and through other organizations.

WHAT DOES THIS MEAN TO THE ANTI-VIRUS INDUSTRY?

Microsoft continues to work on educational materials specifically to address the needs of the home user. The technical information provided through *TechNet*, security programs and premier partnerships is not particularly suited for typical home user consumption. The same is true for the technical descriptions of viruses that most anti-virus companies provide on their websites.

Anti-virus companies have long shared the same problem of how to get important information about threats and viruses in front of the consumer. *Microsoft* is working to address this problem by providing consumer-friendly guidance to customers at http://www.microsoft.com/security and http://www.microsoft.com/protect. An example of educational content aimed at the consumer market is a video about spyware that can be viewed at http://www.microsoft.com/athome/security/spyware/video1.mspx. This video targets the consumer audience and explains the important information at an appropriate level.

Microsoft has come to realize that the most significant relationship with the home user is shifting progressively from traditional contact points to the ISP. The ISP has an ongoing, daily relationship with the customer. In order to get security information to the home user the *Microsoft* GIAIS team is working to help syndicate the important content for hosting by the GIAIS partner ISPs.

There is an old saying that you can lead a horse to water, but you can't make him drink. If the horse is thirsty he'll drink, but who leads him to the water?

In today's consumer support model, the ISPs are the ones holding the reins. In many, if not most cases, the browser home page for the home user belongs to their ISP. If the horse is to be led, then talk to the person holding the reins. Similarly, if a uniform level of support is to be provided to customers, realize that in a large number of cases the customer's ISP is providing the support. This means that relevant support information needs to be made available to the ISPs.

Through a variety of programs, such as the Virus Information Alliance, OEM channels and other security partner organizations, *Microsoft* will work to facilitate communications across the various industry segments to protect the home user better, but at the end of the day, the ISP is in the best position to ensure that our mutual home consumers see the information they need to enjoy their online experience more safely.

FEATURE 2

VIRUS OUTBREAK PROTECTION: NETWORK-BASED DETECTION

Oren Drori
Commtouch Software, Israel

Timely response is the major challenge facing email security solutions. Today's malware is distributed more rapidly than ever before, with major outbreaks reaching their peak within a few hours. Unfortunately, while the response time of security software has improved over the years, there remains a dangerous window of vulnerability that can last hours or even days. Identifying new viruses, locking down signatures with 100 per cent certainty, and producing a vaccine is a lengthy process, leaving users unprotected while outbreaks are peaking.

This article suggests an alternative approach – pre-emptive mass outbreak detection – which represents a powerful complement to existing virus outbreak protection methods.

THE ACHILLES HEEL OF THE AV INDUSTRY

Despite heavy anti-virus investments, viruses and other types of malware are still the number one security problem facing computer systems. Reports suggest that malware damage exceeds $55 billion annually.

The reason why malware attacks succeed is not that they are immune to vaccines. They succeed because they are fast and efficient enough to cause damage before users are vaccinated. Yet, despite the crucial importance of timing in the battle against malware, response time has not improved significantly for a number of years.

In recent years, the computing world has come to function as a global network – resulting in exponentially faster infection rates.

One of today's most significant drivers of virus production is spam. For spammers, viruses serve as an effective means of penetrating defences. This gives the AV industry a good deal to worry about, since it means that there is now a strong financial motivation to making viruses.

'INNOCENT UNTIL PROVEN GUILTY'

The key factor determining the response time to new threats is the period between the outbreak's distribution and the moment protection is available on the desktop. Traditional anti-virus approaches are designed, first and foremost, to prevent 'false accusations': AV updates are released only after a bulletproof signature has been established. Even in the case of minor mutations, this process stretches over hours. However, in the more severe case of a new virus type (the scenario with the highest probability of causing excessive damage) identification and vaccine creation can easily exceed 24 hours – a wide window of vulnerability.

Delays can happen for a number of reasons: lag time between distribution and first sample; lag time between first sample and signature; lag time between signature and production-level vaccination; and customer update schedule. Even if customers are updated several times per hour, several hours are lost before the first sample is identified and the first signature is created.

MyDoom is now considered the largest malware outbreak of 2004, and perhaps the one that created the most damage in the industry. The time of its release is unknown, but the peak occurred 6.5 hours after *MessageLab*'s first detection of the worm. Yet the first Beta signature, which came from *McAfee*, was released eight hours after detection – meaning that even the best-protected users were vulnerable during and after the peak. In fact, the first sample and general public protection were available 17 hours after first detection.

SIGNATURE-LESS TECHNOLOGY

As noted, anti-virus technology traditionally takes the 'innocent until proven guilty' approach. This means that messages are blocked only once they have been determined conclusively to be infected; until that happens, infected messages circulate freely.

Clearly, enormous end-user benefits are riding on the ability of the AV industry to minimize the vulnerability window, to provide what is called zero-hour or zero-day protection.

One highly promising new approach to zero-hour protection is real-time massive outbreak detection. This approach shifts the centre of gravity away from individual messages and towards the network itself. It is based on automated data collection and analysis, rather than manual intervention; and

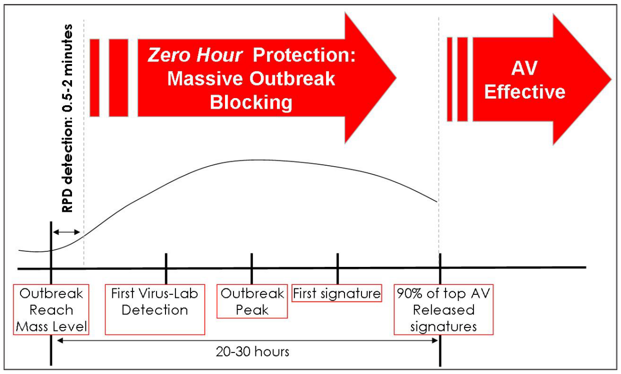

RPD detection: 0.5-2 minutes
Zero Hour Protection: Massive Outbreak Blocking
AV Effective
Outbreak Reach Mass Level
First Virus-Lab Detection
Outbreak Peak
First signature
90% of top AV Released signatures
20-30 hours

Figure 1: Outbreak detection plays preemptive protection role.

it risks delaying 'innocent' messages, rather than leaving users unprotected from emerging, unidentified threats.

Massive outbreak detection has already demonstrated detection rates of well over 95 per cent, coupled with extremely low false-positive rates. When used as an anti-spam tool – both by *Commtouch* and by big ISPs such as *Yahoo!* – it has years of immunity to the evolving obfuscation attempts of spammers.

MASSIVE OUTBREAK DETECTION

Though implementation is far from simple, the technological concept behind massive outbreak detection is easy to understand. Very large amounts of real email traffic are analysed centrally, to identify recurrent distribution patterns. By identifying their mass-distribution patterns, it is possible to detect new email outbreaks within minutes, or even seconds, of their introduction into the Internet. Subsequently, each incoming message is compared, in real time, to an active outbreak database. Any message identified with a mass outbreak is blocked.

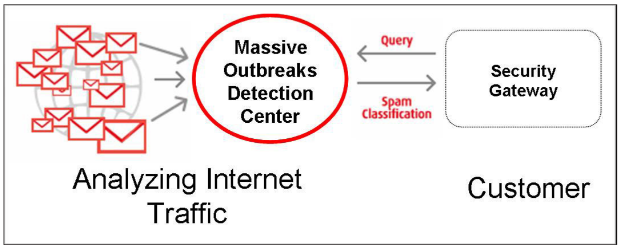

Massive Outbreaks Detection Center
Query
Spam Classification
Security Gateway
Analyzing Internet Traffic
Customer

Figure 2: Commtouch's Recurrent Pattern Detection.

As mentioned, massive outbreak detection is far simpler in theory than in implementation. The first challenge in operating such a solution is obtaining real-time access to a live email stream. This stream must not only be of significant volume (millions or even tens of millions of messages), but it must also be a representative sample (geographic areas, etc.). Secondly, identification of recurrent patterns must be carried out automatically and with high efficiency.

Finally, this information must be communicated to the end user in real time, since using periodic updates would mean undermining the method's zero-hour capabilities. At the same time, communication with the end user must be highly efficient; clearly, an entire database of mass-outbreak indicators cannot be replicated for each end user.

IMPLEMENTATION CONSIDERATIONS

Massive outbreak detection is a complement to existing anti-virus solutions, not a replacement. Its value can be summarized in two categories:

1. Early detection. Emerging outbreaks are identified ahead of time, and reported to the anti-virus labs. The lab can then determine if the outbreak is indeed a new virus, and respond accordingly.
2. Zero-hour prevention. Used as an additional layer in an anti-virus solution, massive outbreak detection provides valuable zero-hour protection. It buys precious time for anti-virus providers by blocking or detaining 'suspect' messages while the labs complete their analysis.

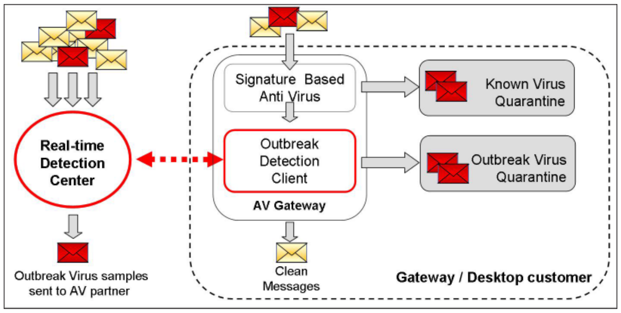

Signature Based Anti Virus
Known Virus Quarantine
Real-time Detection Center
Outbreak Detection Client
Outbreak Virus Quarantine
AV Gateway
Outbreak Virus samples sent to AV partner
Clean Messages
Gateway / Desktop customer

Figure 3: Mass outbreak detection complementing a traditional anti-virus solution.

BUYING PRECIOUS TIME FOR AV VENDORS

Today's malware can spread at phenomenal speed, and the more networked our world becomes, the faster the infection rates are likely to become. Traditional anti-virus solutions experience difficulties in matching these infection rates, resulting in a window of vulnerability of strategic importance.

By identifying new outbreaks instantly and reporting them to the anti-virus labs, the massive outbreak detection technique can dramatically shorten the time to first sample. Needless to say, such time savings are critical.

By blocking instantly or at least detaining emails which are of mass-distribution nature, massive outbreak detection can prevent over 95 per cent of viruses from entering the user's inbox. This protection is available long before traditional AV signatures are produced.

This type of filter is nearly impossible to circumvent. It is effective against any type of threat that is mass distributed over the Internet – indeed massive outbreak detection is a mature technology, which has already been used widely to provide spam protection.

Massive outbreak detection is a signature-less network-based approach to email security, which provides a powerful ally to an anti-virus engine.

INSIGHT

NEW KID ON THE BLOCK

Helen Martin

Having made its *Virus Bulletin* debut in the February 2004 comparative review (see *VB*, February 2004 p.12), *UNA*, from the *Ukrainian Antivirus Center*, is a relative newcomer to the AV scene. Over the 13 months since its first appearance in *VB*, the product's performance has shown some progress, although there remains plenty of room for improvement.

Recently, *VB* met with the founders of the company and discovered a small, enthusiastic and highly-driven team determined to get their product into shape and fit for market in Europe and, ultimately, the rest of the world.

THE UKRAINIAN ANTIVIRUS CENTER

UNA's history goes back to the early 1990s, when Oleg Braginsky (now executive director of the *Ukrainian Antivirus Center*) developed an anti-virus program called *BravO*. Later, in November 1997, Dmitro Zagorodniy (now president of the company), Oleg Sych (now head of the anti-virus lab) and Eliash Golovatsky (now head of systems integration) began development of a product named *VirusDetector*. Eventually, in March 2001, elements of *BravO* and *VirusDetector* were brought together to form the product that is now known as *Ukrainian National Antivirus*, or *UNA*.

The *Ukrainian Antivirus Center* is a relatively small company and a youngster in the AV market, employing some 70 full-time workers, with around the same number again of remote workers. However, the company is still growing – a fact evidenced by the doubling of staff numbers over the course of the last year.

The *Ukrainian Antivirus Center* employs highly-skilled specialists who, according to the company's founders, are driven by their enthusiasm for the subject matter. Alongside the full-time specialists, the company also engages the talents of local technology students in their final years of higher education. The students are tasked with less specialised mechanical work and some of them go on to work for the company after they have completed their studies.

DOMESTIC BLISS

Until now the *Ukrainian Antivirus Center* has concentrated on the domestic market within the Ukraine – indeed, it enjoys approximately 60 per cent of the domestic market share and has amassed a collection of certificates, testing victories and glowing testimonials in its home country.

The majority of the company's customers are based in the state sector, with government bodies accounting for 63 per cent of its customer base (while corporate users comprise 22 per cent, home users and educational institutions just 8 per cent and 7 per cent respectively).

While Ukrainian home and corporate users generally tend to use fairly contemporary technology (*Windows 9x* and, more commonly, *Windows 2000/XP*), in the state sector there is widespread use of the older i386 technologies and it is still common in some establishments to find systems running MS-DOS.

This means that, in addition to working on emerging threats for modern platforms and applications, the company needs to provide support for older systems. And, being such a youngster in the AV market, *UNA* finds itself having to run to catch up with the bigger boys – still needing to add detection and removal capabilities for older viruses. *UNA*'s founders have a positive outlook, however, pointing out that they have the advantage of being able to learn from the mistakes other companies have already made. And they are quick to point out that the need to 'catch up' on the older viruses and platforms has not prevented them from creating solutions for the latest operating systems and applications – including protection for mobile devices.

Use of the Internet in the Ukraine is still expensive, but has seen rapid growth recently, rising from approximately 900,000 users in 2002 to almost 4 million in October 2004 (according to *SputnikMedia*). This accounts for approximately 8.4 per cent of the population (compare this with the UK where, according to www.internet.world.stats.com, 58.5 per cent of the population are online, and the USA, where 68.8 per cent of the population use the Internet). Mindful of the high cost of Internet connectivity, every effort is made to keep *UNA*'s anti-virus updates as small as possible to minimise download time. Signature updates are issued weekly (unless there is a virus outbreak, when updates are issued daily), with program updates once a month.

The company's current product range consists of anti-virus for the desktop (both enterprise and home user), anti-virus for fileservers, anti-virus for mail servers and local network protection. Alongside its AV solutions the company also provides firewall software, security test software, customer training and certification for anti-virus safety, penetration tests of local networks and data recovery services.

DOMESTIC HURDLES

According to analysts at the *Ukrainian Antivirus Center*, the most significant malware-related damage suffered in the Ukraine last year was caused by Trojans. In particular, many Ukrainian and Russian Internet users fell victim to

Backdoor/Ubriel.B in the summer of 2004 – while the rest of Europe remained oblivious to the same threat. Conversely, while Sober.I was nearing the top of the virus prevalence charts in the rest of Europe in November/December 2004, Ukrainian users remained unaffected. Malware-related losses suffered by Ukrainian companies in 2004 were estimated by *Ukrainian Antivirus Center* analysts to have reached 'hundreds of millions of hryvnas' (currently, US$1 = 5.51 hryvnas).

Virus writing has recently become illegal in the Ukraine – new legislation having been passed at the end of 2004 – but a significant problem that remains untackled in the Ukraine is software piracy. Use of unlicensed software is commonplace, with pirated software freely and easily available. As a result, *UNA* finds itself having to compete with anti-virus software from the big international AV players. Despite the widespread nature of the problem, however, software developers receive little support from the state in rectifying the situation.

GETTING PERSONAL

The *Ukrainian Antivirus Center* is driven by a spirited and industrious team, whose collective ambition is to see *UNA* distributed worldwide. *VB* asked the Ukrainian-born founders of the company about their backgrounds and their early virus experiences.

Dmitro Zagorodniy, President, Ukrainian Antivirus Center

President of the company Dmitro Zagorodniy studied in the microelectronics and technology faculty of the Taganrog State University of Radioengineering, graduating in 1994.

It was while he was studying that Dmitro first began to research computer viruses: 'At university in 1992 we researched the action of self-replicating programs on computer systems and the network.' Initially, however, Dmitro's passion was not for the prevention and cure of viruses *per se*, but rather for the protection of information. He says, 'When the scale of virus propagation became too great, I decided to study both theoretical and practical means of information protection.' And it was while he was at university that he had his first experience of a virus outbreak: 'Several computers in the department were infected – these machines contained strategically important and confidential information, so I needed to find out how to disinfect them.'

Oleg Braginsky, Executive Director, Ukrainian Antivirus Center

Executive Director Oleg Braginsky graduated with a red diploma from Kiev Polytechnic Institute's (KPI) Department of Information Theory and Computer Technology in 1996 (in the Ukraine a red diploma is awarded for academic excellence, while 'standard' candidates earn a blue diploma). He then moved on to the International Scientific Technical University, where he graduated with another red diploma, this time from the juridical department. Finally, he completed his studies in 2001 with a dissertation on artificial intelligence, gaining docent status in 2002.

One of Oleg's first encounters with a virus was in the winter of 1990 when a virus infected his only 5 1/4" floppy disk – upon which was stored all of his coursework. He says, 'I had two choices: to leave the course and join the army or to try to restore the file. I spent three nights working in the university to try to restore the file [and eventually succeeded]. When it turned out that the same virus had struck tens of computers in Kiev, I was able to disinfect them – I became a computer guru and was even awarded by the government for the best student scientific research development.'

Surprisingly, Oleg does not rate this as his first serious virus incident. That, he says, occurred in 1995 when the computer network of the admissions board of KPI was struck by the OneHalf virus (whose payload was to encrypt two cylinders of the hard disk every time the system was rebooted). 'I found the virus immediately,' he said, 'it took me three days to decrypt the data – after that they paid me a three-month salary and presented me with a brand new computer.'

Oleg Braginsky gained his first work experience early in life while still at school: 'In 1986, thanks to my father [a military man], I became involved in the creation of the program model of the navigation system for military aircraft.' Later, Oleg worked as an offshore programmer in the Ukrainian/Canadian corporation of international business collaboration, programmed transputers and wrote parallel algorithms on the assembler for the *Motorola* digital signal processor DSP-96001. More recently he has worked for *Siemens* and for *Alfa Bank*. Oleg says that his interest in anti-virus programming began when he saw *Aidstest*, the anti-virus program designed in the late 1980s by Dmitry Lozinsky and produced by *DialogueScience* in Moscow. He says, 'The product's speed of operation and virus database impressed me so much that I decided I wanted to compete.'

Oleg Sych, Head of Antivirus Lab, Ukrainian Antivirus Center

Oleg Sych, Head of the Antivirus Lab, began studying automation and control at Kiev Polytechnic Institute in 1996, but transferred within a year to the Engineering Technological Institute of Zhitomir, where he completed his studies in 2001.

Oleg says, 'I was introduced to computer viruses for the first time in 1994. At that time, virus writers in the former Soviet Union tended not to include destructive payloads in their creations, and it was interesting to study viruses, analyse new technologies and ways of controlling them. Later, however, the Russian-language virus writers became embittered and I finally understood that viruses are a very serious evil.' Oleg's first serious virus experience came in 1996: 'During my studies I had to contend with a local virus epidemic, and it was then that I acquired my first experience of anti-virus program development. Later, when other viruses were discovered on the local network they were analysed and the modules of detection/disinfection added to the program, which served as the prototype of the first version of *VirusDetector*.' Oleg Sych began his professional career with *Ukrainian Antivirus Center* itself.

ALL FOR UNA, AND UNA FOR ALL

The *Ukrainian Antivirus Center* is a family business – the wives of the three founders also have strategic roles in the company. While Oleg Sych claims he is too young to have children, and that he and his wife are too dedicated to their work to keep pets, Oleg Braginsky and his wife have an eight-year-old daughter who entertains the family's dog and cat. Dmitro Zagorodniy has a son aged nine and a Persian cat, *UNA*, whose name is evidence that the business is never far from the family's minds.

Ask any of the company's founders what they wish for and the answer is unanimous: the vision of the *UNA* management team is to have an office on every continent. As the first step towards realising that ambition the *Ukrainian Antivirus Center* is working diligently to prepare the product for introduction to the European market in the near future.

The Ukrainian Antivirus Center can be found online at http://www.unasoft.com/index_e.html.

PRODUCT REVIEW 1

VIRUSBUSTER 2005 PROFESSIONAL

Matt Ham

The name *VirusBuster* will be familiar to readers of *Virus Bulletin*, the company's product having featured in *VB*'s comparative and standalone product reviews since 2000.

VirusBuster is based in Hungary, although it has embraced internationalisation of both its product and its marketing. Currently, English, Hungarian and German languages are supported and the *VirusBuster* product line represents almost the entirety of *VirusBuster*'s business. With trends in the AV industry having swung from dedicated anti-virus to suite-based security, back, and forth again, it remains to be seen whether the company will stick with its relatively pure focus in the future.

The *VirusBuster 2005* range is so new that the product line as a whole is still considered to be in the final stages of beta – although the version of the product tested, *VirusBuster 2005 Professional*, is complete and ready for market.

As with all 'new' product lines, the first question I have is whether it is merely the user interface that is new, or whether there has been any deep underlying change to the application mechanics. On first inspection of this product, both seemed to be the case: the interface has certainly changed since the last version of *VirusBuster*, as has the virus database format – which is likely to signify a change in the underlying detection technology.

With changes in all aspects of the program, I was rather spoiled for choice as to what to test first. The test platforms used were *Windows XP Professional* with and without *Service Pack 2*, and unless stated otherwise the results here were produced on *Windows XP SP2*. The *Windows NT* platform used in the last comparative review (see *VB*, February 2005 p.12) was also tested tentatively, but setup failed due to *NT* lacking some of the more up-to-date resources required by the program.

WEB PRESENCE AND DOCUMENTATION

The English-language *VirusBuster* web presence is located at http://www.virusbuster.hu/en/. The contents of the site are much as expected: news, views, virus data and product downloads. However, the website does make it tricky to find the new products. Any readers intent upon performing their own tests will find the downloads for the *2005* versions concealed within the Support area of the website.

For a product so new, the electronic documentation provided was impressive. Three main PDFs were supplied, covering the *VirusBuster Professional* product, the server product and details of *Microsoft Management Console* snap-in functionality for the product. Of these the *Professional* version documentation was inspected the most thoroughly and appeared to be a direct copy of the printed manual for the product.

The documentation covered all of the areas that were encountered during testing, with copious illustrations provided to aid comprehension. However, thanks to the rather more user-friendly GUI that is now in place, extensive reference to the manual was not required.

INSTALLATION AND UPDATE

VirusBuster 2005 Professional was packaged as a self-extracting compressed executable of some 14 MB, which showed a slight lack of polish in that it requested a destination for temporary interim files. The interim state of unpacking (before actual installation but after initial decompression) upped the size of the package to 16 MB. Oddly, the server-based product weighed in at only 12 MB packed and 14 MB unpacked – smaller than the (presumably) less complex general user edition. This discrepancy in file size might be explained by the fact that the administration suite in the server product is currently incomplete. This is also the reason why the single-user version was chosen for review.

Upon execution of the package, the familiar *InstallShield* interface is launched. Despite there being MSI files within the package, the installation progresses entirely with this *InstallShield* look and feel.

First in the installation process is the obligatory end user licence agreement (EULA). Following the EULA is a warning that installation should not be performed on a computer upon which other anti-virus software is already present. However, this precaution should not be necessary when running on *Windows XP*, where anti-virus applications should be able to coexist happily. To test this, *VirusBuster* was installed alongside anti-virus applications from other vendors and there were no ill effects. With *Service Pack 2* installed, the operating system was also able to accept *VirusBuster* for on-access scanning while using a firewall registered by another anti-virus product.

The next step is to select an installation location. This is followed by the *InstallShield* Typical/Compact/Custom page, where the type of installation can be selected. In a custom installation the various components may be selected individually. This is of note mainly because the dialog displays what it considers these components to be. The three main components are the on-access, on-demand and content filtering functions. These can be disabled if the user wishes. 'Optional' components listed are the Updater, Central Alert, Mailer and Administration Panel.

My feeling is that the Updater should not be listed as 'optional'. Theoretically there are circumstances under which updating could be disabled, but these are sufficiently rare that I would rate them outweighed by the possibility of a misguided user deciding to disable this 'optional' component. With all components selected, installation requires 25 MB.

Next, the user is required to specify the SMTP settings – although, where no SMTP server is available the dialog may be left blank without further problems. Similarly, the settings for Central Alerts may be left blank if required. Otherwise this is the area in which a central mail address may be specified to receive all messages generated by *VirusBuster*, selected messages (virus detection, critical error, configuration change and security issues), or no messages at all.

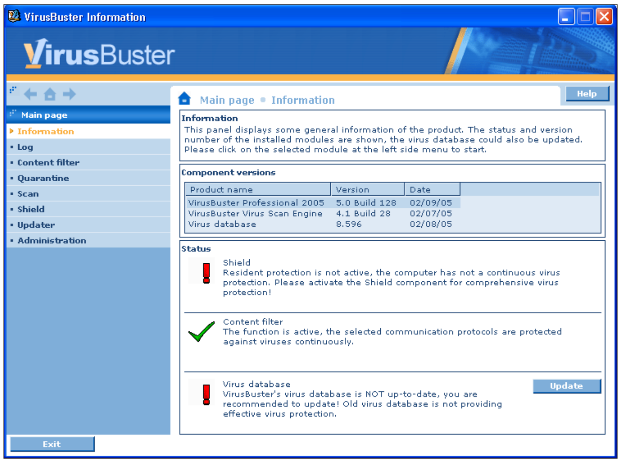
The Update settings page follows. By default, the updater runs daily for virus database detection and weekly for program updates. The latter may be somewhat slow if the program requires an update to detect a new threat type. Similarly, daily scanning for virus database updates may be ample under normal circumstances, but will be unpleasant if an emergency update is published. What is, perhaps, more worrying is the fact that updates may be disabled very easily here. My preference would be for this option to be hidden away in a place discernable only by a user who actively sought it out.

Update locations are selected next, the default being *VirusBuster*'s servers. Updates may also be downloaded from a local repository directory or CD, or from FTP or HTTP sites designated by the user.

Somewhat later than expected, the registration page is the next to appear, although it is possible to ignore the registration page and use the application for a 30-day trial period. As the final part of installation the opportunity is given to place a shortcut to *VirusBuster* on the desktop. A summary of the selected options is then presented, and installation completes. No reboot is required.

At this stage a notification popup appears to the effect that the on-access component is active. This is likely to be followed closely by a notification that the databases are antiquated and in need of updates.

As yet, updates are not available as standalone downloads in the version 8.* format required by *VirusBuster 2005* (current releases of *VirusBuster* use updates designated by version numbers beginning with 7). The inbuilt updater must therefore be used. This seems to perform the update in two stages.



Information
This panel displays some general information of the product. The status and version number of the installed modules are shown, the virus database could also be updated. Please click on the selected module at the left side menu to start.

Component versions

Product name	Version	Date
VirusBuster Professional 2005	5.0 Build 128	02/09/05
VirusBuster Virus Scan Engine	4.1 Build 28	02/07/05
Virus database	8.596	02/08/05

Status

Shield
Resident protection is not active, the computer has not a continuous virus protection. Please activate the Shield component for comprehensive virus protection!

Content filter
The function is active, the selected communication protocols are protected against viruses continuously.

Virus database
VirusBuster's virus database is NOT up-to-date, you are recommended to update! Old virus database is not providing effective virus protection.

First, a small file is downloaded which provides information about what should be downloaded, then the main download proceeds. Several user actions are required during the process in default mode. The feedback provided here was a little limited. The progress of the download of the main update data, measuring 3 MB, seemed to be stuck on 1 per cent for a long time, then suddenly leapt to 100 per cent just as I was beginning to suspect a problem had arisen. However, I suspect that subsequent updates would be somewhat smaller and faster.

FEATURES

The previous versions of *VirusBuster* offered a large number of options through an interface which tended to cause confusion for anyone without a long familiarity with its quirks.

The interface has been totally overhauled – giving it, among other important changes, a rather more modern look and feel. Of particular note is the fact that the interface is available in two versions. The standard interface is available by default, while many pages may be expanded by selecting an advanced version of the same functionality.

The start point of the interface, the Information view, bears a passing resemblance to the *Microsoft* security interface, consisting of a status display for three components: Shield (the on-access function), Content Filter and the Virus Database. The status of each of these is represented graphically by a red exclamation mark or a green tick.

In addition to this main Information view, there are also views for Log, Content Filter, Quarantine, Scan, Shield, Updater and Administration. Each of these may have several sub views associated with it, organised in a tree structure with navigation icons provided. This organisational approach both offers a large amount of control, and is significantly less confusing than the previous *VirusBuster* interface.

The Scan view was inspected next. Initially there are three scan areas available: all hard drives, all removable media and network drives. If a more finely-tuned scan is required it must be created anew. Initially the interface for this feature seems very limited, since it really only offers more of the same in terms of possible scan targets. However, selection of the advanced view provides a more traditional tree browser. The dual aspect continues with the areas concerning which scan methods should be used, how the scan should be instigated and what actions should be taken when detection occurs. The advanced settings are discussed below.

Somewhat unusually, *VirusBuster* uses an extension list to determine which objects should be scanned. This can be tweaked in a user-friendly fashion, since such categories as Script Files, Program Files and Jet Engine files may all be selected or deselected from scanning as groups rather than fiddling with individual file types. Individual extensions may also be included or excluded as desired. Scanning of memory and scanning of compressed files are activated by default but may be disabled.

There is also an option here to change the scan method and heuristic sensitivity. In this area the in-program help proved to be useful and informative. The exact definitions of such terms as 'full scan' and 'quick scan' are often a mystery but they are well explained here – for example, a 'quick scan' ignores detection of viruses which require extensive calculations in their detection, such as *Excel* formula viruses. Upon detection of a virus the usual range of activities may be set.

Another unusual default option is that of how the scan will be commenced. The default is that any scan will be scheduled, rather than the more common option of starting a session manually. With options for scanning depending upon day, time, system start and the like, there are no major surprises here.

The Shield view, relating to the on-access scanner, is not significantly different from the on-demand settings described above. Exclusion of areas from scanning on-access is supported.

Scanning is also provided for other modes of information exchange, which are covered by the Content Filter view. The scan options here, as far as sensitivity and actions are concerned, are identical to those available on access and on demand. The three channels where scanning is supported here are mail (covering POP3, IMAP and SMTP), HTTP and FTP. This was tested in passing with large file transfers via HTTP and did not seem to have an immediately noticeable effect upon transfer speed.

In the Quarantine view there are two features of note: first, the Quarantine area can be set to be rescanned after the engine or definitions have been updated – in case the quarantined samples can now be identified more accurately or perhaps disinfected where previously this was not possible. There is an option to put files that have been disinfected back where they came from. However, this might prove awkward if the file has been replaced with one that has newer or different content and, in such a case, the newly disinfected file will be deposited in the temporary directory.

The second Quarantine function of note is that it interacts with the Mail module. Files may be sent directly to *VirusBuster*, in a somewhat packaged form, for examination in their labs.

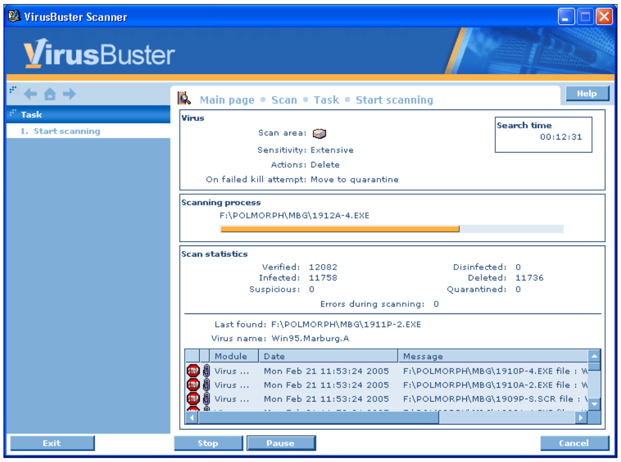
The Log view offers filters but is not really a subject of great interest. The final view is that of Administrator. Again, this is supplied via an optional module and offers password protection of various scan settings. The potential issues with users turning off updates and the like could at least be mitigated with this functionality.

A great deal of the functionality offered above is also offered by the tray icon which appears after installation. The main application may be launched from here, though the exact view opened is dependent upon which area has been selected through the tray icon. This is a very fast and convenient way of making adjustments to, for example, the scanning parameters.

Although there were slight issues with the responsiveness of the icon if it was used overzealously in very short periods of time, this is unlikely to be an issue for anyone other than those performing product testing. One other slightly irritating point was that the icon does not have a significantly different appearance if on-access scanning is disabled. This is offset to a great degree on *Windows XP SP2* by the appearance of a large red warning shield icon. Under other operating system versions, *VirusBuster* itself pops up a warning message, making the issue much less vexing than might otherwise be the case. These warning popups also occur in cases where the virus database is outdated.

SCANNING TESTS

Since the *VirusBuster 2005* program will be tested in forthcoming comparative reviews, the scanning tests carried out here were not particularly rigorous. Testing was performed with default settings for detection – that is setting sensitivity to Extensive, scanning files by extension and with heuristics enabled at the normal level of sensitivity. Since detailed results were not required, the option to delete all files flagged as infected was selected.



Virus

Scan area:
Sensitivity: Extensive
Actions: Delete
On failed kill attempt: Move to quarantine

Search time
00:12:31

Scanning process
F:\POLMORPH\MBG\1912A-4.EXE

Scan statistics

Verified: 12082	Disinfected: 0
Infected: 11758	Deleted: 11736
Suspicious: 0	Quarantined: 0

Errors during scanning: 0

Last found: F:\POLMORPH\MBG\1911P-2.EXE
Virus name: Win95.Marburg.A

Module	Date	Message
Virus ...	Mon Feb 21 11:53:24 2005	F:\POLMORPH\MBG\1910P-4.EXE file : W
Virus ...	Mon Feb 21 11:53:24 2005	F:\POLMORPH\MBG\1910A-2.EXE file : W
Virus ...	Mon Feb 21 11:53:24 2005	F:\POLMORPH\MBG\1909P-S.SCR file : \

During scanning it was noticeable that a large number of files were scanned before any were noted as infected, and there was also a delay before these were flagged as deleted. The former issue was due to objects being counted as scanned when active processes were under scrutiny, these being scanned by default though not listed as targets in the scan. The latter delay was lessened when throughput was slower, as with the polymorphic set, this clearly being an issue with screen updates of data.

It was noticeable that even with the deletion option selected, files which would be considered to contain infected objects were not deleted – most notably *PowerPoint* infections. With these files taken into consideration, detection was very similar to that seen with the older versions of *VirusBuster*. Additional rigour in the scanning, brought about by setting heuristics to Strong and scan to Full, did not add more than a handful of detections, although scanning was noticeably slower.

CONCLUSIONS

The new version of *VirusBuster* certainly shows improvements over the old, at least in terms of its interface. From a tester's point of view the product is certainly easier to operate. Let us hope that the product's scanning rates are as pleasant to behold.

Technical details

Test environment: Identical 1.6 GHz Intel Pentium machines with 512 MB RAM, 20 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy drive running *Windows XP Professional*. Athlon XP1600+ machine with 1 GB RAM, 80 MB hard disk, DVD/CD-ROM and ADSL internet connection running *Windows XP Professional Service Pack 2*.

Developer: *VirusBuster* 1518 Budapest, PF 54, Hungary; tel +36 1382 7000; fax +36 1382 7007; email mail@virusbuster.hu; web http://www.virusbuster.hu/en/.

PRODUCT REVIEW 2

RESOLUTION ANTIVIRUS

Matt Ham

Resolution Antivirus is new to the *Virus Bulletin* testing regime. Unlike many newcomers it has a large number of features which, although not novel, are implemented in somewhat non-standard ways. The company behind the product, *Secure Resolutions*, specialises in remote administration.

One of the first questions which springs to mind when I encounter a new product is 'Where does the detection functionality come from?' Very few products are brand new in this area and, like the majority, *Resolution Antivirus* falls into the category of rebadged products. In this case the underlying detection is provided by *Panda Antivirus*.

Panda is a sufficiently established company that I would not expect *Resolution Antivirus* to make any serious errors in its basic technology – leaving implementation as the primary point of interest.

INSTALLATION

The first sign that this was not to be a standard review came when details were supplied for a trial administrator account. Initially, standalone installation of *Resolution Antivirus* in an isolated environment (my usual first port of call when undertaking a product review) seemed impossible. However, I soon discovered that standalone installation of the product is possible, but it is considered such a minor feature that the options for it are not immediately obvious. Installation via a web client is the preferred method, and this is reflected in the web page hierarchy.

Local and remote installation are both supported from within this interface. Local installation was selected first, and it was here that the first problems were encountered. The primary test machine ran *Windows XP SP2*. With SP2 installed, the local *Internet Explorer* security settings are slightly more restrictive than with an unpatched version of the operating system. In addition, anti-pop-up functionality is built into *Internet Explorer* as part of the SP2 package. Unfortunately, installation of *Resolution Antivirus* relies on an applet which runs within a spawned pop-up window, thus the process failed without much warning. In addition, Windows Scripting Host must be installed and fully operational for full product functionality – a requirement which will be unpopular with many administrators despite being the default on most *Windows* installations.

To be fair, the need for these settings to be adjusted is noted on the installation web page, and I was aware of why installation was failing even without warning dialogs. However, security products that require the relaxation of security settings before they can be installed are one of my pet hates.

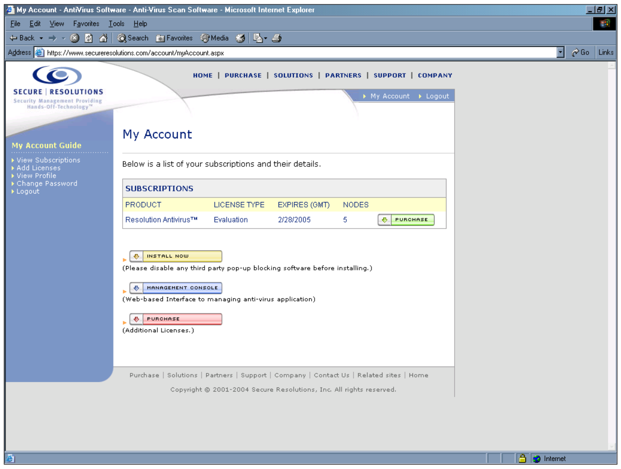
Once the necessary security adjustments have been made, the installation process is a simple and automated affair, with no decisions required for installation settings. The lack of decision-making at this stage is due to an emphasis on central administration – installations follow the parameters set up through the web interface.

Pre-configuration is managed through the 'Policies and Groups' portion of the web interface. Here, policy settings can be configured and saved for use in local, standalone and remote installation. (The options available are noted later.)

Standalone installation is carried out through the 'Installation tokens' portion of the site. An installation token is an executable which can be used for standalone installation. The installation is preconfigured as one of the available policies and contains the latest available virus definition files. Tokens created during testing were just over 11MB in size, with the file names derived from the policy selected during creation.

Remote installation is also supported, with the download of the product being triggered remotely on the target machine. This may be triggered via dissemination of a URL token (which requires a web connection), but an alternative – which, presumably, will be preferable for organisations with restricted access to the Internet – is to use the executable installation token. This can be located on a network share local to the target machine, meaning that the installation process can be executed via a simple login script.

Matters are a little worrying, however, when it comes to updates to virus definition files. It appears that the only method of performing updates without a net connection is by a full reinstallation of a freshly prepared executable token. This could certainly prove to be an issue.


My Account - AntiVirus Software - Anti-Virus Scan Software - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://www.secureresolutions.com/account/myAccount.aspx
Go Links
SECURE | RESOLUTIONS
Security Management Providing Hands-Off-Technology™
HOME | PURCHASE | SOLUTIONS | PARTNERS | SUPPORT | COMPANY
My Account Logout
My Account Guide
View Subscriptions
Add Licenses
View Profile
Change Password
Logout
Purchase | Solutions | Partners | Support | Company | Contact Us | Related sites | Home
Internet

My Account

Below is a list of your subscriptions and their details.

SUBSCRIPTIONS

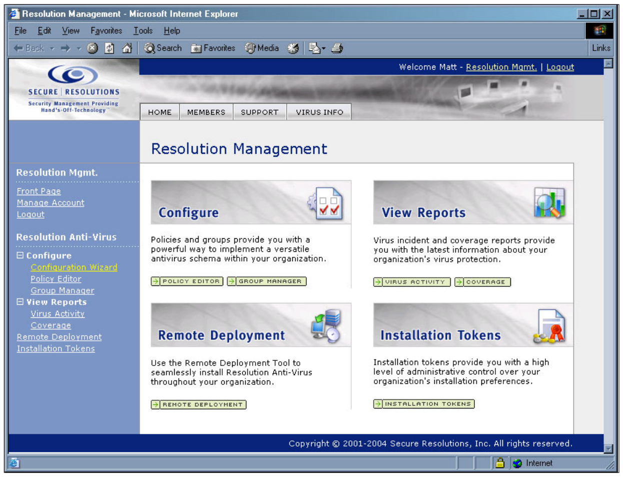
PRODUCT	LICENSE TYPE	EXPIRES (GMT)	NODES	
Resolution Antivirus™	Evaluation	2/28/2005	5	PURCHASE

INSTALL NOW
(Please disable any third party pop-up blocking software before installing.)

MANAGEMENT CONSOLE
(Web-based Interface to managing anti-virus application)

PURCHASE
(Additional Licenses.)

Copyright © 2001-2004 Secure Resolutions, Inc. All rights reserved.



Resolution Management

Configure

Policies and groups provide you with a powerful way to implement a versatile antivirus schema within your organization.

View Reports

Virus incident and coverage reports provide you with the latest information about your organization's virus protection.

Remote Deployment

Use the Remote Deployment Tool to seamlessly install Resolution Anti-Virus throughout your organization.

Installation Tokens

Installation tokens provide you with a high level of administrative control over your organization's installation preferences.

Copyright © 2001-2004 Secure Resolutions, Inc. All rights reserved.

WEB SUPPORT AND DOCUMENTATION

Secure Resolutions's web presence is located at http://www.secureresolutions.com/. As is common with developers using a third party engine in their solutions, the public area of the website consists, by and large, of a mixture of advertising and information that is more concerned with product descriptions than technical details of viruses. The website does include a reasonably complete FAQ for *Resolution Antivirus* – indeed this was sufficient to answer my general queries on almost all facets of the program.

The private area of the website is where the majority of the interest lies. Once logged in, there are four main headings within the web interface: 'Policies and groups', 'Virus incident and coverage reports', 'Remote Deployment Tool' and 'Installation tokens'. There is also the aforementioned option for local installation, which requires an active Internet connection.

'Virus incident and coverage reports' offers information as to the current status of machines administered through the web interface and any infections discovered on them. Information is stored on individual machines as XML files – one each for machine status and infected objects. The XML can easily be inspected, and indeed could be edited by mischievous users. While inspecting these files it was noted that SP2 did not seem to be detected as an installed service pack. Presumably this problem will be addressed in a future release, when one would also hope that the installation process will work on SP2 without the need for tweaking.

The virus incident report pages are well constructed for the production of graphs charting viral infections. Statistics may be viewed on a per machine or per group basis, with the starting point set at a view of one month, with daily statistics making up the graphs. Granularity is highly configurable, however, with a time scale of minutes being obtainable if desired. This is visually very appealing, though from an administrative viewpoint it is more likely that results will need to be collated into a machine-readable format. Happily this is possible, with options to export to XML or CSV.

Documentation concerning operation of the software was limited to that supplied as web pages in addition to the help available within the installed application. The in-program help is clear and easy to navigate, though this is not surprising given the relatively small amount of information that will be needed by an end user. The information supplied for the administrator is not particularly verbose in nature either. This can lead to confusion when first faced with the applications, though the learning process is not exactly tricky.

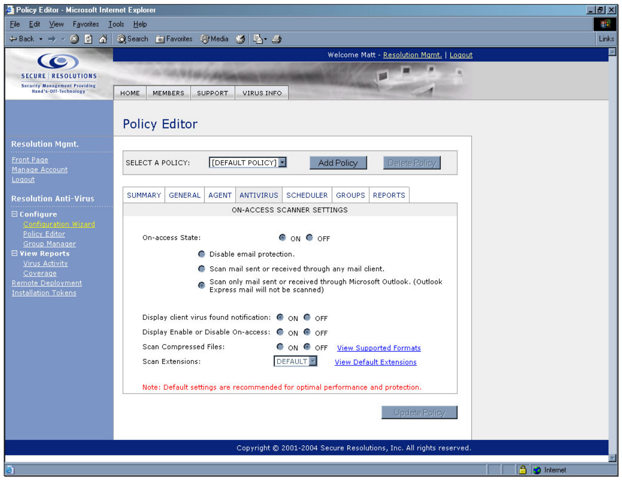
OPERATION

To a default user, the appearance of the product is minimal to say the least. A tray icon is present, which acts as a reminder that there is software installed, but updates are not visible. Similarly, on-access scanning is obvious only if a detection occurs. When detection occurs the default action is for the item to be disinfected, without the user being consulted. An informational dialog box does appear in the case of detection, offering a link to virus information. This links directly to the *Panda* virus information database.

From an administrator's point of view, matters of control are substantially different – though not, perhaps, to the extent that might be expected. *Secure Resolutions*'s doctrine of remote administration is very much in effect here, with the functionality for administration available only through the website interface.

The 'Policy Editor' passably simulates a tabbed dialog through its layout, the default view being a summary of the configuration selections made in other areas. These other areas are 'General', 'Agent', 'Antivirus', 'Scheduler', 'Groups' and 'Reports'. 'General' is less than inspiring, giving the name of the policy and only one real option, which is as to whether the version of software to be installed should be the live version, the early version or the beta version. This allows for differentiation between machines where greater protection is considered to outweigh potential issues with less tested updates.

In the 'Agent' area selections are made as to how and when updates should be detected and applied. By default the agent will attempt to find updates at boot and at one-hour intervals thereafter. For the mightily paranoid this polling can be set as frequently as once a minute, though I suspect that the network traffic caused by this on larger installations might be prohibitive. An improvement here might be to institute some randomness in the first update after the boot.



Policy Editor

SELECT A POLICY: [DEFAULT POLICY]

ON-ACCESS SCANNER SETTINGS

On-access State: ● ON ○ OFF

○ Disable email protection.
○ Scan mail sent or received through any mail client.
● Scan only mail sent or received through Microsoft Outlook. (Outlook Express mail will not be scanned)

Display client virus found notification: ● ON ○ OFF
Display Enable or Disable On-access: ○ ON ● OFF
Scan Compressed Files: ○ ON ● OFF
Scan Extensions: DEFAULT

Note: Default settings are recommended for optimal performance and protection.

Copyright © 2001-2004 Secure Resolutions, Inc. All rights reserved.

Currently, in an office where all machines are booted at 9am there will be much network activity every hour, with little during the intervening times. This could be mitigated by introducing less predictability in the update polls.

The ‘Groups’ area is simply a summary of which groups are selected to use the policy currently under inspection. ‘Scheduler’, as might be expected, offers the opportunity to allocate scheduled tasks to a policy.

Likewise, the ‘Reports creation’ settings allow determination of where and when the reports should be collated for a whole group. As with the update polls, the report generation can be set only to specified times with no randomness within a group. This means that spurts of report files will be generated en masse due to all machines in a group being synchronised.

In addition to the web-based report option it is also possible to set machines to report to an email address in either CSV or XML format. This should allow the creation of parsing scripts so as to provide results that can be transferred automatically to, for example, an administrative database.

The ‘Antivirus’ area will, no doubt, be that of most interest to many readers. This is the area in which more control might have been expected. Admittedly, mail scanning is configurable as per normal – with all mail, no mail or only mail passing through *Outlook* being selectable for scanning. By default, the Client is informed when a virus is discovered, though an alternative to this is silent operation. Similarly, the default of mandatory on-access protection may be set so that users can disable this feature.

By default, compressed files are not scanned – the reason being the usual desire to lessen overheads, though the administrator may opt for more paranoia here. Another area where more paranoia can be applied is the addition of more extensions to the default scanned list. It is unusual, these days, to see the use of an extension list, rather than all files being scanned, though this may also improve throughput for the on-access scanner. Finally, folders may be added to an exclusion list here.

Given that the user has no control over the parameters for on-demand scans other than location, I expected there to be provision for control over such matters as heuristics here. More importantly, I would also have expected some control over the action taken upon detection of viruses. As it stands, all viruses will automatically be disinfected – a situation which may not be to an administrator’s, or user’s, liking.

CONCLUSIONS

The recurrent theme throughout this review has been the way in which central administration is assumed rather than simply being supported. With this assumption come several features which may be positive or negative depending on the administrator’s preferences. The level of scanning control is, by general standards, fairly basic. This simplifies the task of an administrator as far as ease of policy creation and mitigation of user enquiries are concerned. On the other hand, some administrators might find the lack of fine tuning in certain areas to be somewhat restrictive.

Likewise, the heavy emphasis on web access in order to perform administrative tasks might be seen as a blessing or curse, depending on the network structures within individual organisations, especially where updates are concerned.

Overall, *Resolution Antivirus* is an example of a niche product, which will have loyal adherents as well as folk who prefer to head elsewhere. Although not yet represented greatly in reviews, this variety of anti-virus solution is likely to expand as more vendors see engine licensing as a good stream of revenue, while licensees see niche marketing as a way to compete against the same vendors.

If anything, the knowledge that *Microsoft* is increasingly likely to become a threat to their core business, may mean that, in the future, the large vendors see more specialist products as being desirable. When faced with a behemoth in competition it can be useful to have features which make your product stand out.

Technical details

Test environment: Identical 1.6 GHz Intel Pentium machines with 512 MB RAM, 20 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy drive running *Windows XP Professional*. Athlon XP 1600+ machine with 1 GB RAM, 60 GB hard disk, DVD/CD-ROM and ADSL Internet connection.

Developer: *Secure Resolutions, Inc.*, 1959 South Power Road, Suite 103, #430, Mesa, AZ 85206, USA; telephone +1 (480) 807 3930; fax +1 (480) 830 7178; email sales@secureresolutions.com; website http://www.secureresolutions.com/.

END NOTES & NEWS

The E-crime and Computer Evidence conference ECCE 2005 takes place in Monaco from 29–30 March 2005. ECCE 2005 will consider aspects of digital evidence in all types of criminal activity, including timelines, methods of evidence deposition, use of computers for court presentation, system vulnerabilities, crime prevention etc. For more details see http://www.ecce-conference.com/.

Black Hat Europe takes place in Amsterdam, The Netherlands, from 29 March to 1 April 2005. Black Hat Europe Training runs from 29 to 30 March, with the Black Hat Europe Briefings following, from 31 March until 1 April.

Black Hat Asia takes place 5–8 April 2005 in Singapore. The Briefings take place 5–6 April, with the training on 7–8 April. For details and registration see http://www.blackhat.com/.

The first Information Security Practice and Experience Conference (ISPEC 2005) will be held 11–14 April 2005 in Singapore. ISPEC is intended to bring together researchers and practitioners to provide a confluence of new information security technologies, their applications and their integration with IT systems in various vertical sectors. For more information see http://ispec2005.i2r.a-star.edu.sg/.

Infosecurity Europe 2005 takes place 26–28 April 2005 in London, UK. There will be more than 250 exhibitors and the organisers expect over 10,000 visitors. See http://www.infosec.co.uk/.

The 14th EICAR conference will take place from 30 April to 3 May 2005 in Saint Julians, Malta. See http://conference.eicar.org/.

The sixth National Information Security Conference (NISC 6) will be held 18–20 May 2005 at the St Andrews Bay Golf Resort and Spa, Scotland. For more information see http://www.nisc.org.uk/.

The third International Workshop on Security in Information Systems, WOSIS-2005, will be held 24–25 May 2005 in Miami, USA. For full details see http://www.iceis.org/.

AusCERT 2005 takes place 22–26 May 2005 in Gold Coast, Australia. Programme details and online registration are available at http://conference.auscert.org.au/.

The 3rd annual BCS IT Security Conference takes place on 7 June 2005 in Birmingham, UK. The conference focuses on identity theft, hacking, cyber-terrorism, network forensics, secure web services, encryption and related topics. See http://www.bcsinfosec.com/.

NetSec 2005 will be held 13–15 June 2005 in Scottsdale AZ, USA. The program covers a broad array of topics, including awareness, privacy, policies, wireless security, VPNs, remote access, Internet security and more. See http://www.gocsi.com/events/netsec.jhtml.

A SRUTI 2005 workshop entitled 'Steps to Reducing Unwanted Traffic on the Internet' takes place 7–8 July 2005 in Cambridge, MA, USA. The Usenix-sponsored workshop aims to bring academic and industrial research communities together with those who face the problems at the operational level. For more information see http://www.research.att.com/~bala/sruti/.

Black Hat USA takes place 23–28 July 2005 in Las Vegas, NV, USA. The deadline for submitting paper proposals is 1 May 2005; registration for the event opens 1 April 2005. For details see http://www.blackhat.com/.

The 14th USENIX Security Symposium will be held 1–5 August 2005 in Baltimore, MD, USA. For more information see http://www.usenix.org/.

The Network Security Conference takes place 19–21 September 2005 in Las Vegas, NV, USA. The conference is designed to meet the education and training needs of the seasoned IS professional as well as the newcomer. For details see http://www.isaca.org/.

The 15th Virus Bulletin International Conference, VB2005, will take place 5–7 October 2005 in Dublin, Ireland. The call for papers closes on **10 March 2005**. For conference registration, sponsorship and exhibition information and details of how to submit a paper see http://www.virusbtn.com/.

RSA Europe 2005 will be held 17–19 October 2005 in Vienna, Austria. For more details see http://www.rsaconference.com/.

ADVISORY BOARD

SUBSCRIPTION RATES

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

Editorial enquiries, subscription enquiries, orders and payments:

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

Tel: +44 (0)1235 555139 Fax: +44 (0)1235 531889
Email: editorial@virusbtn.com Web: http://www.virusbtn.com/

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.

vb Spam supplement

CONTENTS

NEWS & EVENTS

IM SPAMMER ARRESTED

An 18-year-old New Yorker was arrested last month and charged with sending more than one million spam messages to customers of online instant messaging site *MySpace.com*.

Anthony Greco created thousands of user accounts on *MySpace.com* and used them to send more than 1.5 million unsolicited messages to members of the website (the site's regulations allow a maximum of 500 messages per day to be sent from each user account). After launching the spam attack, Greco contacted the owners of *MySpace.com* to claim responsibility and to request that he be given exclusive rights to send commercial email to users of the site. When his request was ignored, however, Greco attempted to blackmail the company, threatening to share his spamming techniques with others: 'I have no choice but to just sell off my coding to other people and allow them to pick up the projects,' he wrote.

Upon receiving the threats, *MySpace.com* executives contacted the Los Angeles Police Department and arranged a meeting with Greco, telling him they needed to meet with him in person in order to sign a contract. However, when Greco arrived at Los Angeles airport for the meeting, he was arrested and charged with violating the Can-Spam Act, threatening to cause damage to *MySpace.com* computers and attempting extortion. If convicted of all three offences, Greco faces a maximum sentence of 18 years in federal prison.

DOUBLE-PRONGED ATTACK SLAMS SPAM

Software giant *Microsoft* and pharmaceutical giant *Pfizer* have joined forces in an effort to crack down on drug-related spam. The corporations have filed 17 parallel lawsuits against two 'international pharmacy spam rings' accused of selling illegal versions of *Pfizer*'s erectile dysfunction drug *Viagra*.

Pfizer has filed civil actions against the operators of two websites, CanadianPharmacy and E-Pharmacy Direct, that it accuses of selling illegal drugs that have not been approved by US drug regulators. Meanwhile, *Microsoft* has filed civil actions against the spammers promoting the same websites. In addition, *Pfizer* has filed ten further domain name actions against sites using its *Viagra* trademark in an unauthorized manner and *Microsoft* has filed three suits against spammers advertising other online pharmacies.

Brad Smith, *Microsoft*'s Senior Vice President and General Counsel, described the double-pronged attack by the two corporations as a wake-up call to those who abuse the Internet for illegal purposes. He said, 'Leading businesses are teaming up, pooling resources and sharing investigative information to stop this illegal activity at the source.'

EVENTS

The Anti-Phishing Working Group (APWG) General Meeting takes place on 19 April 2005 in London, UK. For details see http://www.antiphishing.org/events.html

CEAS 2005, the Second Conference on Email and Anti-Spam, will be held 21–22 July 2005 at Stanford University, CA, USA. The conference committee is currently seeking submissions for papers, with a submission deadline of 15 March 2005. A call for workshop proposals will follow the call for papers. For more information see http://www.ceas.cc/.

INBOX IT is planned for early June 2005 in the San Francisco Bay area, CA, USA. The event will focus on all aspects of email. More information will be available in due course from http://www.inboxevents.com/.

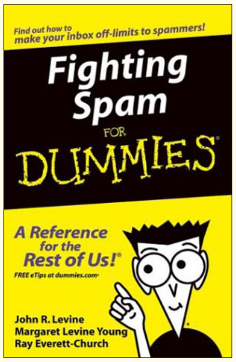
TREC 2005, the Text Retrieval Conference, will be held 15–18 November 2005 at NIST in Gaithersburg, MD, USA. The conference includes a new track on spam, the goal of which is to provide a standard evaluation of current and proposed spam filtering approaches. For more information see http://trec.nist.gov/.

BOOK REVIEW

DUMMIES' GUIDE TO SPAM

Paul Baccas
SophosLabs, UK

Title: Fighting Spam for Dummies
Authors: John E. Levine, Margaret Levine Young, Ray Everett-Church
Publisher: Wiley
ISBN: 0-7645-5965-6



The bright yellow and black cover design and the cartoon character of Wiley's '*For Dummies*' series have frequently been the subject of pastiche and pillory, and I have to admit that the prospect of reviewing this offering filled me with a little trepidation. Luckily, however, I was to be pleasantly surprised.

Between them, the three authors of *Fighting Spam for Dummies* have written several books; as a consequence the book's style, within the confines of the series, is concise and witty.

The only complaint I have with the style of the book is the number of references made in the text (as opposed to appendices) to other books in the series. In fact, there are no appendices in this small, 200-page A5-sized, book. I feel that the inclusion of appendices – containing references, a bibliography and a 'further reading' section – would have added significantly to the value of the book.

The book is divided into four parts: 'The World of Spam', 'Filtering Spam Out of Your Inbox', 'Spam-Filtering Programs and Services' and the ubiquitous 'The Part of Tens' (a section common across the '*For Dummies*' series of books, which provides a number of quick reference ten-item lists).

Part one, 'The World of Spam', provides an introduction to spam, covering historic, economic, comedic, legal and political aspects of unsolicited commercial email as well as the tinned meat product. There is also a tutorial, in what could be called 'Email and the Internet, 101', that details how to find out who has been spamming you, plus a basic description of how spammers work – for example, how they harvest email addresses and how they send spam. This section is lightweight, but there is sufficient detail to whet the reader's appetite and the detail is up to date.

Part two, 'Filtering Spam Out of Your Inbox', looks at how to filter email using your email client. This section covers all of the most popular home user email clients and web mail clients: *Outlook Express* and *Outlook*, *Netscape* and *Mozilla Mail*, *Eudora*, *AOL* and *AOL Communicator*, *Hotmail*, *MSN* and *Yahoo! Mail*. This section is highly informative, explaining why email filtering is a good practice and how to do it. The book also advises on which software versions you should be using and how to configure them – for example how to create whitelists and blacklists, how to configure in-built spam controls and generally how to make the client more secure.

Part three, 'Spam-Filtering Programs and Services', deals with spam solutions that are separate from the email client – covering several open-source, free and cheap home-user solutions, ISP-level spam solutions and a general overview of server-side spam blocking. This section goes heavily into the detail of the setup and configuration of *POPFile* (accounting for almost 10 per cent of the book).

The description of ISP-level solutions details only a small subset of those available and there are some glaring omissions. The server-side chapters explain DNSBL (domain name service blacklisting/blocking) and DNSWL (domain name service whitelisting) and describe a number of free, commercial and third-party solutions.

Part four is the amusing, informative and thought-provoking 'The Part of Tens'. There are just two lists of ten in this book, the first dealing with standard email scams and the second with Internet security. A couple of paragraphs of information is devoted to each entry in each of the lists.

The list of ten spam scams includes: 419, 'make lots of money', 'free holiday', paypal/bank phishing, credit, 'lose weight', prescriptions, male enhancement and pornography.

The list of Internet security items includes: pop-up blockers, firewalls, anti-virus software, adware/spyware and other diverse topics.

While I would hesitate to recommend this book as a good read for any of the technical readers of *Virus Bulletin* or email administrators, I would certainly recommend that they buy it. There are a number of reasons for this seemingly contradictory advice.

The content of the book is not sufficiently complete to teach readers everything there is to know about spam – the level of knowledge about email and Internet that comes from being online for a decade cannot easily be taught. For large organisations the details included in the book are not sufficient to be of assistance in making informed decisions about how to tackle spam or what solutions to implement.

On the other hand, however, this book is perfect for those people who ask: 'How do I get rid of spam on my home machine?', or 'So, what do you do again?'. This is an informative, fun and easy-to-read book which does not patronise the reader and will not confuse.

CONFERENCE REPORT

SPAM CONFERENCE 2005

John Graham-Cumming
The POPFile Project, USA

21 January 2005 saw the third of Paul Graham's Spam Conferences at MIT, with a total of 15 talks ranging from a report about the French Government's work to combat spam, through the schadenfreude of the Jeremy Jaynes trial to technical talks with some clever, new ideas.

If you couldn't attend the Spam Conference, you still have a chance to catch the presentations in the free web cast at http://www.spamconference.org/webcast2005.html. Since the order of presentations differs slightly from what actually happened on the day, here's a handy guide to the talks and the point at which they appear in the webcast (the number in parentheses):

SESSION 1	
Bill Yerazunis	Unified Model of Spam Filtration (0.17)
Eugene Koontz	Bayesian Phishing Classification (18.37)
Jonathan Zdziarski	Bayesian Noise Reduction (39.02)
Jonathan Oliver	Lexicographical Distancing (58.05)
SESSION 2	
Richard Segal *et al.*	Classifier Aggregation (0.20)
Jim Fenton	Message vs. User Authentication (19.50)
Rui Dai *et al.*	Regulation (39.50)
Oscar Boykin	Personal Email Network Structure (1:00.15)
SESSION 3	
Brian McWilliams	Spam Kings (0.15)
John Graham-Cumming	People and Spam (19.45)
Constance Bommelaer	French Government and Spam (39.05)
Matthew Prince	Project Honeypot (1:00.15)
Jon Praed	Jeremy Jaynes Spam Trial (1:19.40)
SESSION 4	
Gordon Cormack	Standardized Filter Evaluation (0.20)
Dave Mazieres	Mail Avenger (25.20)

If you are into spam filter hacking then stop and listen to four interesting talks: Jonathan Zdziarski, Richard Segal, Jonathan Oliver and Gordon Cormack. Jonathan Zdziarski finally explained clearly how his Bayesian Noise Reduction worked. Although the technique is ad hoc and does not have a great deal of theoretical basis, it seems to work and this talk is worth 20 minutes of your time. Richard Segal from *IBM* talked about how to merge the results of more than one classifier to get the best of each technique's results. He showed that by combining multiple classifiers with an appropriate function he got better results than any single classifier alone (see also *VB* February 2005, pS2).

Jonathan Oliver talked about the billions of different ways to spell 'V1@GRA' and how to use the classic 'edit distance' to identify similar words and to identify spammy words like viagra, improving his spam filter's accuracy without adversely affecting the false positive rate. Gordon Cormack has been working for some time on standardized testing of spam filter effectiveness. He spoke about his framework for testing a filter and gave some preliminary results. Hopefully, this effort will bear fruit in some non-vendor data about spam filter effectiveness.

If you are of a legal bent then Jon Praed's discussion of the Jeremy Jaynes trial will take you inside the courtroom itself. The talk gave an idea of how the evidence nailed this prolific spammer as well as some fun facts along the way. Praed displayed a receipt that showed that Jaynes made $100,000 in one month: $400,000 in credit card charges for his business, minus $300,000 in chargebacks – presumably from disgruntled customers. A telling moment for writers of spam filters was Jaynes's hand-written 'to do' list, retrieved from his trash, which contained the line 'Figure out filters'.

Two brave souls from the French Government came out to a frigid Boston and presented a report, in English, on how the French Government is fighting spam on behalf of its citizens. An interesting note was that, although French law makes 'opt in' the standard for email marketing, no one has yet been prosecuted in France. Nevertheless, French law sounds a lot stricter than CAN SPAM.

Oscar Boykin talked about how social networks (i.e. the people you know and the people they know) can be used to identify spam by figuring out who is likely to send you email legitimately. Eugene Koontz showed that Naive Bayesian spam filters work equally well at identifying phishing fraud emails and made the important point that many people mistake phishes for real emails and when they appear in a 'spam' folder they report them as false positives!

Matthew Prince gave an excellent presentation on his Project Honeypot, which is already yielding fascinating data on the connection between the harvesting of email addresses from websites and the actual spam those addresses receive. CAN SPAM makes email address harvesting illegal, and through a cleverly disguised contract on the honeypot website Prince has built a strong legal case for canning spammers who harvest addresses. He even uses their own techniques against them by obfuscating the contract that their bots 'sign', using spam trickery derived from *The Spammers' Compendium* (http://www.jgc.org/tsc/).

Finally, if lots of percentages are your cup of tea, listen in for my talk on people and spam, where I presented the results of a huge survey of end users. The vendor-neutral survey revealed that 77 per cent of email is spam, that 98.5 per cent receive spam and that 1 per cent of recipients have actually bought something spam-advertised. 84 per cent said that if they didn't have a spam filter they would have major problems using email, would stop or would consider stopping using email completely. A depressing 76 per cent of people believe that spam will never go away.

SUMMARY

ASRG SUMMARY: FEBRUARY 2005

Helen Martin

In another rather quiet month for the ASRG, postings centred around the subject of spammer proxies using legitimate mail relays. George Ou started the topic off by posting a link to an article on the *Spamhaus* website. The article (http://www.spamhaus.org/news.lasso?article=156) reported that 'spamware' released by proxy spammers has improved its blacklist avoidance ability by using the legitimate outbound SMTP servers of the infected victim and that, as a result, an increasing amount of spam is coming from legitimate mail gateways. George asked whether anyone had any more detailed information on spamware and how it functions.

James Lick responded with some details, saying that spamware looks at the hostname of the proxy (e.g. adsl-63-29.someisp.com), then looks up the MX for 'someisp.com' and sends through that. He highlighted some drawbacks to this approach, such as the fact that the domain of the ISP's clients and the domain of their email infrastructure could differ – and that an ISP which blocked its client systems from sending out through the incoming MX could defeat the system. James also pointed out that the 'spamware' mentioned in the *Spamhaus* article refers to *Send-Safe*, the spamming software available over the *MCI* UUNET network at http://send-safe.com/ (and whose content obfuscation techniques were detailed in the January issue of *Virus Bulletin* – see *VB*, January 2005, p.S2).

James said 'The big change with this development [in spamming methods] is that now the ISPs have an incentive to take responsibility for the spam traversing their networks, because the load directly impacts upon their ability to provide a service. If the ISPs in turn implement SMTP-AUTH, then they further give their users an incentive not to get their systems owned. That may not seem like much, but given an incentive, I believe they will have to take steps to protect themselves. Ultimately those that don't will find it difficult to send email because their reputation will suffer.' James directed readers to his blog for a more detailed account of his thoughts on the subject at http://www.livejournal.com/users/jlick/10243.html.

Jonathan Morton said that, rather than examining in detail how spamming software works, he would rather spend his time working on a solution. He said, 'I'm just not that interested in ferreting around in the bowels of malware for that information and would rather let others find it and post it somewhere useful, like ASRG.' Jonathan said that, since we know that spammers adapt very quickly once they see that a feature is necessary to their operation, he is working on a solution to which spammers would not be able to adapt. He invited list members to point out any 'chinks in the armour' of his scheme which involves using hashcash alongside cryptographic signatures. The first messages in an email exchange would contain hashcash tokens – sufficiently computationally expensive to prevent spammers from flooding inboxes. During this first exchange, cryptographic signature keys would also be exchanged and subsequently used for computationally cheap conversation. George Ou, James Lick and others were quick to identify what they saw as the 'chinks' in Jonathan's scheme however, as they questioned the effectiveness of hashcash. Tony Finch posted a link to a paper by Richard Clayton and Ben Laurie which used real numbers from a medium-sized ISP to show that hashcash cannot be made to work. The paper is at http://www.cl.cam.ac.uk/~rnc1/.

Preceding his query with the admission that he is not a *Windows* man, Jon Kyme wondered whether the following would be easy to retrieve from the *Windows* system registry: HKEY_CURRENT_USER/Software/Microsoft/Internet Mail and News/Mail: DefaultSMTPServer. Larry Seltzer responded that this is not a standard value in *Windows* and, indeed, that *Outlook*, *Outlook Express* and other mail clients change the location of their server values from version to version, making the task of identifying server credentials non-trivial – but not insurmountable.

Daniel Feenberg pointed out that port 25 on 'mail' or 'smtp' is a valid SMTP relay which does not require authentication for the majority of ISPs and that the *Windows* resolver will fill in the domain part of the relay host name. He said, 'I have seen no claims that any spamware *at the moment* goes any further than this, although as time goes by it will do whatever is necessary,' adding, 'I do hope that ISPs don't get the idea that the way to fight this is to obscure the MTA name.'

George Ou felt that, while enforcement of SSL for SMTP/POP3 is a very good thing for security in general, we must assume that 'zombieware' will, at some point, be able to acquire the user's full SMTP server name and full username/password credentials. He felt that SenderID and SPF will be a good starting point to enforce some accountability that will enable accurate blacklisting of individual email accounts on ISPs that enforce SMTP-AUTH. However, Seth Breidbart argued that the chances of a small domain receiving enough spam from any individual zombie would be pretty small – meaning that blacklisting individual accounts would require either a huge public list or a major recipient domain, and the rest would have to blacklist the entirety of any ISP that does not cut off its zombies.

The full debate can be followed in the ASRG archives at http://www1.ietf.org/mail-archive/web/asrg/current/.