NOVEMBER 2006

virus BULLETIN

The International Publication on Computer Virus Prevention, Recognition and Removal

CONTENTS

ISSN 1749-7027

IN THIS ISSUE

O CANADA!

The VB conference drew to a close in Montréal last month after three packed days of presentations, panel discussions, meetings, birds of a feather sessions and lively debate, with a fair amount of eating, drinking, music and acrobatics thrown in for good measure. Helen Martin reports on VB2006.

page 9

Virus Bulletin thanks the sponsors of VB2006:

bitdefender secure your every bit
eset
ARBOR NETWORKS
McAfee Proven Security™

vbSpam supplement

This month: anti-spam news and events; and John Graham-Cumming charts the rise and rise of image spam.

'My feeling is that we are unlikely to see an open source replacement for SoftICE *any time soon.'*

Aleksander Czarnowski, Avet

SOFTICE, SECURITY AND THE FUTURE

When I first entered the infosecurity field I was of the misguided opinion that IT security problems could be solved technically through the application of great concepts and advanced code. However, I soon realized that I was (at least partly) wrong – security-related problems can't be solved with technology alone. Security issues are complex sociological problems.

As time has moved on I have shifted my concept to a higher level: I believe that IT security issues are not only sociological problems, but also economic ones.

Recently, I read a very detailed paper about one particular RPC vulnerability. The author of the paper must have put at least 50 hours of work into writing the paper – but the main facts contained in the paper could easily have been obtained within 30 minutes using a freely available debugging tool such as *SoftICE*, and an analysis of the vulnerability could have been written up within another 30 minutes.

Unfortunately however, that very tool, *SoftICE*, has officially reached the end of its life: its manufacturer, *Compuware*, announced earlier this year that it will not be developing it any further.

While open source enthusiasts (especially LAMP experts) will be quick to reassure us that an offspring project is likely to start up soon – and that we will have a free, open source replacement for *SoftICE* within a year or two – I don't believe this will be the case. Developing any kernel debugger is not an easy task, not least one that measures up to *SoftICE*'s capabilities. Keep in mind that *SoftICE* is capable of single machine debugging – a feature that has only recently been added to the *Microsoft WinDBG* debugger. Not even the newest version of *WinDBG* with the /DEBUG option enabled in boot.ini can compete with *SoftICE*.

Relatively few programmers are interested in writing debuggers – especially in comparison with the number of application programmers. That number decreases still further if we consider kernel debuggers and the length of time and level of knowledge required to accomplish such a task. Testing a kernel debugger can be a very painful and time-consuming process. My feeling is that we are unlikely to see an open source replacement for *SoftICE* any time soon.

In fact, the best debuggers for *Windows* are freeware. *OllyDBG* is a great example. While *Microsoft*'s *WinDBG* is free, it is very hard to use. The freely available *IDA Pro* also has an application-level debugger, but almost every *IDA* user I know uses it for its disassembly and code analysis capabilities, not for its debugger.

So it seems that there is no commercial place for standalone debuggers in today's market. What does this mean for security? With the demise of publicly available tools such as *SoftICE* certain areas of research will become more difficult and time-consuming, and consequently they may suffer as they will only receive attention if companies have the interest, time and/or money to dedicate to them. (It is interesting to note that, where research is concerned, the size of company has little to do with the quality and amount of research done. Companies like *Immunity Security*, *GLEG* and *Argeniss* are small companies, yet their work is usually outstanding.)

Some might say that it is a great pity that such a useful and readily available tool as *SoftICE* has been discontinued. Yet, you will find at least ten products designed for application security which incorporate debugging capabilities. These may be very specialized, but underneath they all use the same debugging API. So, although standalone application debuggers have died out, they have taken on a new life in the form of vulnerability research tools aimed at software houses.

I think this is a great example of how the economy can influence information security.

NEWS

NEWS ROUND-UP

Despite no major malware outbreaks having occurred during last month's *VB* conference (as has almost seemed a tradition in the past), October was still a busy month for the anti-malware industry.

Apple confirmed that a number of its *Video iPods* shipped in late September were found to be carrying malicious file RavMonE.exe. The company later engaged in a spat with *Microsoft* over the security (or otherwise) of *Windows* operating systems. The *Windows Vista* operating system fuelled more wars of words as *Sophos* accused *McAfee* and *Symantec* of making inadequate preparations for the forthcoming *Vista* release, while *McAfee* retorted that *Sophos* is unaffected because it is a 'single product vendor', unlike 'innovative security risk management vendor' *McAfee*.

Meanwhile, a variant of the SpamThru trojan discovered last month is believed to be the first malware known to make use of AV software to protect infected machines from rival malware. The trojan downloads and installs a pirated version of *Kaspersky*'s *KAV for Wingate* to check the infected machine for other malware before it begins a spam campaign.

A number of companies in the anti-malware market celebrated awards and accolades last month: *BusinessWeek* placed *Sophos* in 42nd position on its 'Europe's Hot Growth Companies' list; *MessageLabs* received *Frost and Sullivan*'s 'European Security Company of the Year' award for the second year running; messaging security firm *Proofpoint* was named number one 'rising star' in *Deloitte*'s 'Technology Fast 500' program; and *Fortinet* secured the number two position in *Deloitte*'s 'Technology Fast 50' program for Silicon Valley, as well as coming in at number 37 in the top 500 fastest-growing companies in North America.

October also saw the major AV companies reveal their third quarter profits. *Symantec* struggled in Q3, with disappointing sales in the European market and profits falling below expectations – the anti-virus section of the company's business was singled out as a particularly slow performer. *Microsoft*, on the other hand, posted healthy profits, beating predictions; *Trend Micro* announced record net sales for Q3, reflecting a 17% growth compared to the same period last year; and *F-Secure* reported strong third-quarter profits up 28%. *McAfee*'s Q3 results, meanwhile, gave the company reason to be cheerful at the end of a difficult month that saw the resignation of CEO George Samenuk and the sacking of president Kevin Weiss over irregularities in the company's finances. The company's third quarter results came in above target, giving profits of around $30 million. *McAfee* share prices saw a 6% surge immediately after the announcement, despite the boardroom shake-ups and the prospect of further investigations into its past financial results.

Prevalence Table – September 2006

Virus	Type	Incidents	Reports
W32/Mytob	File	4,406,652	28.47%
W32/Netsky	File	4,113,791	26.57%
W32/Bagle	File	2,402,911	15.52%
W32/MyWife	File	1,606,769	10.38%
W32/Bagz	File	832,038	5.37%
W32/Zafi	File	551,394	3.56%
W32/Mydoom	File	544,278	3.52%
W32/Lovgate	File	491,507	3.18%
W32/Parite	File	205,621	1.33%
W32/Valla	File	59,592	0.38%
W32/Funlove	File	38,241	0.25%
W32/Mabutu	File	36,322	0.23%
W32/Klez	File	30,958	0.20%
W32/Bugbear	File	23,715	0.15%
W32/Elkern	File	19,688	0.13%
W32/Agobot	File	12,243	0.08%
VBS/Redlof	Script	11,948	0.08%
W32/Virut	File	11,901	0.08%
W32/Sober	File	9,640	0.06%
W32/Lovelorn	File	9,136	0.06%
W32/Maslan	File	8,531	0.06%
W32/Kipis	File	6,259	0.04%
W32/Dumaru	File	4,874	0.03%
W32/Tenga	File	4,767	0.03%
W32/Darby	File	4,669	0.03%
W32/Traxg	File	4,601	0.03%
JS/Kak	Script	4,143	0.03%
W32/Plexus	File	2,734	0.02%
W95/Spaces	File	2,614	0.02%
W32/Sality	File	2,544	0.02%
W95/Tenrobot	File	2,055	0.01%
W32/Gurong	File	1,552	0.01%
Others[1]		12,804	0.08%
Total		15,480,492	100%

[1]The Prevalence Table includes a total of 12,804 reports across 56 further viruses. Readers are reminded that a complete listing is posted at http://www.virusbtn.com/Prevalence/.

ANALYSIS

A FORTUNE FOX HUNTER

Kaoru Hayashi
Symantec Security Response, Japan

On 25 July 2006, we received a report of a new trojan that steals targeted information from compromised computers. An interesting feature of this trojan, Infostealer.Snifula, is that it spies on *Firefox*.

JS.Ffsniff

The first threat to target *Mozilla Firefox* was JS.Ffsniff, which was discovered in March 2006. Once installed as a *Firefox* extension, JS.Ffsniff runs a sniff function every time a submit event occurs in the browser. The function then sends all the data entered in the web form to a predetermined email address. To establish a connection to an SMTP server directly, JS.Ffsniff uses the following components that are installed with *Firefox* by default:

```
@mozilla.org/network/socket-transport-service
@mozilla.org/scriptableinputstream
```

The domain of both the predetermined email address and the SMTP server used in the threat was 'example.com', which is among the domains reserved for testing purposes as specified in RFC2606 [1]. From this, we can infer that the threat was intended as a proof of concept.

SPAM

A new threat for *Firefox*, Infostealer.Snifula is downloaded and installed by another threat, Downloader.Traus. The downloader was spammed on 25 July. Just a day earlier, a variant of Backdoor.Haxdoor was spammed as well. Interestingly, the two emails were very alike – the attachment names were identical and the subject and message body were similar (see Figures 1 and 2).

Infostealer.Snifula steals information from three areas: via *Firefox*, via *Internet Explorer* and within packets.

XPCOMing

In *Firefox*, Infostealer.Snifula uses three components: XPCOM, a browser extension and the trojan itself. XPCOM, the Cross Platform Component Object Module, is a core technology of *Gecko*. It is similar to *Microsoft*'s COM technology, although there is no compatibility between COM and XPCOM.

Infostealer.Snifula installs the following files:

```
%ProgramFiles%\Mozilla Firefox\components\AppInterConn.dll
%ProgramFiles%\Mozilla Firefox\components\AppInterConn.xpt
```

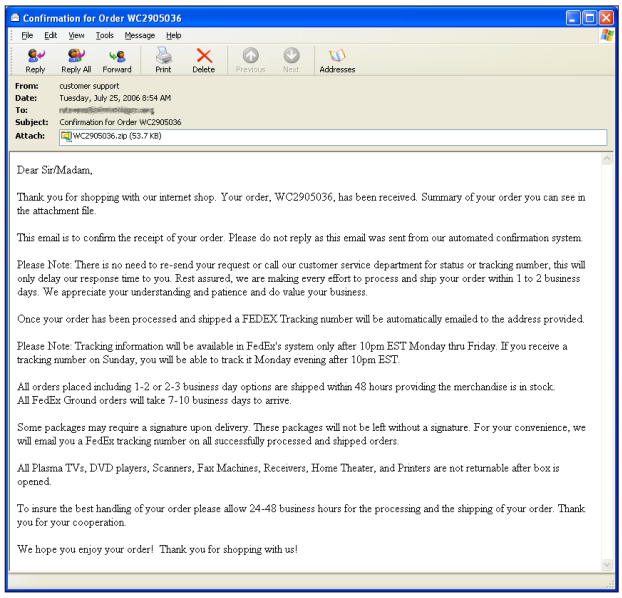


Figure 1: Spam mail with Backdoor.Haxdoor.

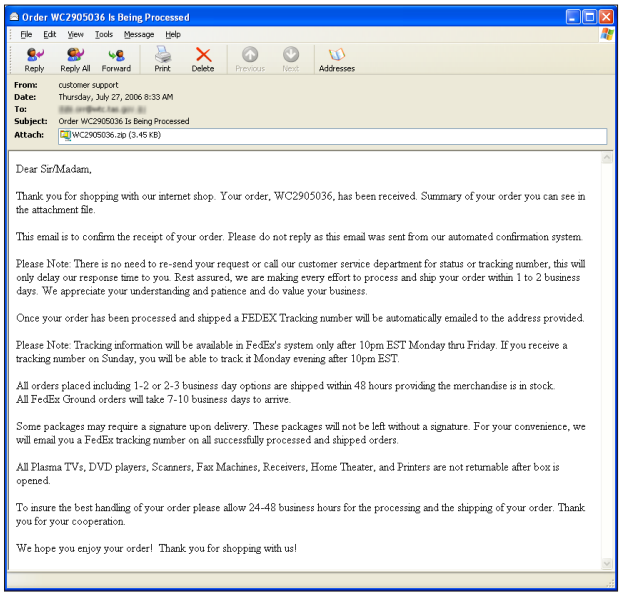


Figure 2: Spam mail with Downloader.Traus.

The DLL file is an XPCOM module that implements code. The XPT file is a typelibrary containing interface descriptions. By using the xpt_dump.exe tool from the *Gecko* SDK [2] against the XPT file, we obtain the following information:

```
Header:
  Major version:        1
  Minor version:        2
  Number of interfaces: 2
  Annotations:
```

```
    Annotation #0 is empty.
Interface Directory:
  - ::nsISupports (00000000-0000-0000-c000-000000000046):
  [Unresolved]
  - ::IAppInterConn (e116c319-c845-4abb-a1a8-123456789000):
   Parent: ::nsISupports
   Flags:
       Scriptable: TRUE
       Function: FALSE
   Methods:
       uint32 SendData(in string, in string);
   Constants:
       No Constants
```

The appInterConn.dll has a method called SendData. This method takes two parameters, the first is the WindowClass name and the second parameter is the data to send. The method sends the data to the WindowClass by using the SendMessage API with the WM_COPYDATA option.

It is the extension that calls the method. The extension masquerades as the well known *Firefox* extension 'Numbered Links'. However, no code from Numbered Links is appropriated. The extension watches mousedown and keydown events, and gathers form data and the URL when a submit or click event occurs. Then it sends that data to the WindowClass named handler_app_class by calling the SendData method.

Infostealer.Snifula itself creates handler_app_class WindowClass and waits for data. Once the data arrives, the trojan posts the data to a predetermined website in Russia.

COMing TOO

Although it is the Browser Helper Object (BHO) that is used more commonly for the purpose of stealing information, Infostealer.Snifula uses *Microsoft*'s COM technology for spying on *Internet Explorer* users. Using the ShellWindows COM object, the trojan watches instances of *Internet Explorer*, enumerates some elements in HTML, and steals the form data if the onsubmit event occurs in the browser.

The trojan mainly uses the following interfaces:

```
IShellWindows
DShellWindowsEvent
DWebBrowserEvents2
IWebBrowser2
IHTMLWindow2
IHTMLDocument2
IHTMLInputElement
IHTMLFormElement
IHTMLElement
IConnectionPointContainer
```

SNIFFING AS WELL

The trojan sniffs network packets to steal authentication information. Low-level packet capturing such as WinPcap is very powerful but it relies on another component or driver to be installed. However, simple Winsock2.0 sniffing is enough for this trojan author's purpose.

The trojan creates a socket with the SOCK_RAW parameter and sets it to promiscuous mode, receives packets and filters them against the following strings:

```
USER
PASS
220
* OK
+OK
Login
```

As a result, the trojan can obtain the username and password for most POP3, FTP and IMAP4 authentication events. FTP is a simple protocol and uses clear text for authentication. The IMAP4 and POP3 protocols support various forms of secure authentication – however, in many cases, servers and clients will fall back to clear text authentication in the event that a shared secure authentication technique is not available.

The trojan also attempts to steal username and password information for *ICQ*. It can identify FLAP packets and get the username and password from SNACK data. Although the password is encrypted with a simple XOR algorithm, the trojan can decrypt it and send it to the author of the trojan. John Canavan described the details of *ICQ* password encryption at length in his article [3].

CONCLUSION

We received a version of Infostealer.Snifula that only had the functions for stealing packets and monitoring *Internet Explorer*. According to the time stamp in the PE header, it seems the author added *Firefox* compatibility within 20 days of creating the earlier version. By adding this function to the trojan, the author can steal information from around 90% of web users [4]. Evidently, attackers continue to develop new techniques in the hunt for profit.

REFERENCES

[1] http://rfc.net/rfc2606.html.

[2] http://developer.mozilla.org/en/docs/Gecko_SDK.

[3] http://www.virusbtn.com/vba/2006/03/vb200603-imav.

[4] http://www.w3schools.com/browsers/browsers_stats.asp.

OPINION

I'M OK, YOU'RE NOT OK

David Harley
Small Blue-Green World, UK

Unfortunately I was unable to attend this year's Virus Bulletin conference, but last year's VB conference in Dublin is still fresh in my mind – in particular for the way in which it managed to mix a little media controversy in with the usual lively panel discussions.

One of the thoughts I took away with me from both panel sessions was that, irrespective of its technical advances, the anti-virus industry continues to fail to win hearts and minds. On the contrary, we are mistrusted by our customers, by the media, and especially by other sectors of the security industry. We are, apparently, incompetent, elitist, cabalist, money-grabbing, publicity-greedy, and generally ethically challenged. But we have our bad points, too.

PLASTER SAINTHOOD

In 1997, a reformed virus writer named Mike Ellison (also known as Stormbringer – who, incidentally, came across as a very nice, and intelligent bloke) addressed the Virus Bulletin conference to let the audience know why the anti-virus industry should employ him (as a channel to virus-writer thinking and initiatives).

Not surprisingly, the vendor representatives who were present came back with the usual set of responses to this sort of overture from the 'dark side':

- It would send an encouraging message to other virus writers.
- Virus writing and anti-virus development are discrete skill sets. This may not be as true now as it used to be: today's malware authors are more 'professional' – in several senses of the word – than they were in those days. Still, it's certainly true that the ability to write even a sophisticated virus is not necessarily proof of the ability to write disciplined code in collaboration with other developers, or even to analyse and write detection for someone else's malcode.
- Anti-virus developers are expected to be whiter than white. This, I guess, is still generally the case. AV teeth grind all around the world every time another malware author, whose main distinction is that he got caught, is offered a job in the security industry (though not usually within several miles of the AV industry). Certainly there is a trust issue here, although I suspect that there is also an entirely rational reluctance to allow other AV vendors the chance to reap competitive advantage by pointing the finger at those who employ black hats. I wonder whether that is why so many vendors have stated that they would not employ someone who'd gone through a controversial course at the University of Calgary which included virus creation as an academic exercise.

Thankfully, for these and other reasons, the industry does not usually employ virus writers. Pragmatically, though, I wonder if part of the problem isn't exactly that image of plaster sainthood?

Many of the people – even security people – with whom I have worked in the past have been convinced (in a jocular sort of way) that the AV industry 'writes all the viruses'. (Not to mention some of the schoolchildren I've talked to about security.) Some of them (my security colleagues, not the schoolchildren) have also pointed out that every time I left the country there was a new worm or mass mailer – and maybe that's part of the problem, too (not that I *do* write worms as I bus across the Outback, but that people *wish* I did).

THE DISAPPOINTING TRUTH

For years I've made the usual commonsense counter-arguments when people have asked me whether the AV industry writes viruses, and/or about my own virus-writing activities/prowess. For example:

- No one (outside of Hollywood) thinks that doctors go out of their way to create diseases, or that crime is a fiction dreamed up by law enforcement agencies to keep themselves in employment, or even that lavatory cleaners spend their idle moments blocking toilets. Why, then, are we regarded with especial suspicion?
- I try to explain that some researchers go to extraordinary lengths to avoid writing a new virus, even for research purposes.
- I point out that if AV developers wrote viruses, a lot of malicious code would be of a much higher standard, and that very few viruses approach the sophistication of a good commercial anti-virus suite, let alone a million and a half other legitimate applications. Surely, if all the viruses disappeared tomorrow, people who are capable of developing a state-of-the-art AV scanner would certainly be able to find coding jobs next week?
- 'No', I say, 'I've never written a virus'. 'Yes', I say, 'I *could* write one': a seriously braindead overwriter would take seconds rather than minutes. 'No,' I say, 'I won't show you one, though I might show you how one works with a bit of pseudo-code.'

You can see the disappointment in their faces, at this point, and I have some theories as to why that is.

Perhaps they want to be touched by the reflected glory of being associated with someone who plays with these dangerous, but glamorous objects.

They're curious, and want a more concrete image of what a virus looks like. Certainly I've often been asked to show people my collection, or demonstrate how viruses work, and I've even been asked to give them a sample or two to play with.

They want to be reassured that I know what I'm doing, and figure that if I know how to write viruses, I must also know everything about defending against them. (Of course, this was also a common view among hobby virus writers, in the days when I talked to some of these guys.) Clearly, it isn't altogether convincing or reassuring to say 'I could do it if I wanted, but I'm not going to.'

Some of the end-users with whom I've worked have shared this mindset, but most of them want to keep it all at a safe distance.

Do these theories take us any further towards understanding why the AV industry is so mistrusted? Some way, yes. These people have been over-exposed to the idea that the best gamekeepers are poachers, and under-exposed to the idea that not all poachers are successful poachers. Nor has it been pointed out to them sufficiently clearly that poaching and enforcing anti-poaching laws do not necessarily require identical skill sets.

But there are other reasons for this dislike. The industry is seen as elitist (and why not? AV is a difficult speciality, and that demands respect, or at least it should). 'Paternalist' is another word that is sometimes heard in reference to the AV industry – and it's true that even those of us on the fringes of the industry have been told from time to time not to bother our pretty little heads with issues that we don't understand.

However, this industry has earned its paranoia. Those who mistrust the fact that we close ranks against other sectors of the security industry perhaps do not realize that some individuals in those sectors swing between two extremes: expecting special treatment as a 'professional courtesy' (e.g. in terms of receiving samples) on the one hand, and dismissing the whole field as a minor branch of security that requires no special skills on the other.

Certainly we are secretive: we still go against the general 'full disclosure' flow, and have good reason to do so. But the fact that the research community collaborates freely among *trusted* individuals doesn't seem to have registered with the world at large: recently, the suggestion that companies still withhold samples from each other for competitive advantage resurfaced in a UK national newspaper.

YOU GET WHAT YOU PAY FOR ...

AV vendors live under a harsh spotlight. Commercial AV is seen as somehow unethical because it's paid for, whereas well-meaning, but partially ineffective and unsupported freeware is seen as laudable.

When a commercial AV product hits the false positive reef it makes headlines, but the more frequent blemishes on some non-commercial AV are rarely reported. Conversely, no freeware solution (freebie versions of commercial solutions excepted) detects everything that a commercial scanner does – but nobody seems to mind. There is a place in security for open source, but there is a tendency for some users of free software to overstate its accuracy and advantages and disregard its drawbacks.

BUT IT MIGHT BE LESS THAN YOU EXPECT

Perhaps the single most damaging perception, though, is that the industry remains wedded to the evil subscription model. Everybody 'knows' that anti-virus vendors only know about viruses, and even then only the viruses for which a signature exists.

We can keep plugging away at this half-truth by pointing out at every opportunity that AV detects many threats other than viruses, and continues to develop heuristic detection and associated technologies to astounding levels of capability.

It's more difficult to overcome the presumption behind these assertions, which is 'if they weren't so protective of their revenue stream, they would let us all use the 100% effective solution which must be out there somewhere'. Well, there are certainly conceptual and actual alternatives – though perhaps 100% is a little too much to hope for, in these days of a hopelessly diverse range of threat types – and the AV industry has embraced some of them with a certain amount of enthusiasm in the past. If the industry moved en masse to integrity checking, for instance, patches and enhancements would support that the subscription model would not disappear, as it hasn't with personal firewalls, for instance. It's likely that virus-specific detection still rules because it detects and removes malware with reasonable precision (mostly) and isn't as prone as more generic technologies to false positives. Its downfall is that it doesn't and can't detect *all* malware, especially non-replicative types.

Security isn't expected to be 100% effective – many of us may have suffered from line managers and customers who thought it should be, but it never works out like that. So why should anti-virus be perfect? Perhaps the problem isn't so much virus management, or even integrity management, but expectation management. In the end, it always is.

LETTER

HUMOUR AT SYMANTEC'S EXPENSE

I deeply regret failing to acknowledge the fantastic talent of the many employees of *Symantec* during my presentation at the *Virus Bulletin* 2006 conference last month in Montréal. I tried to be fair to *Microsoft* in criticizing some aspects of what *Microsoft* is doing and has done, while acknowledging the talented and dedicated employees working there. I had intended to publicly acknowledge the immense talent and dedication of my friends at *Symantec* (I hope they are still friends), and I failed to do so. The presentation was an evolving work up to (and into) the actual time of presentation and this oversight was unfair. I do not believe the jokes were unfair or cheap – however failing also to put a human face on *Symantec* was an inappropriate oversight.

I did criticize *Symantec* for not being as innovative as I believe it should be, and I do recognize that with talent such as Peter Ferrie, Peter Ször, Eric Chien, Mark Kennedy, Per Hellqvist, and scores of other talented researchers and developers, there is no level of innovative brilliance that could come from *Symantec* that would be beyond belief. *Symantec* has some fantastically talented people that any company – anti-virus or otherwise – would be ecstatic to have in its ranks. I suspect that if *Symantec* had key managers in the right places with half the skills, insight and wisdom of Vincent Weafer, it would be *Symantec*, and not *Microsoft*, that the rest of the industry would be scared of.

As a *Microsoft* employee for eight of the 10 *VB* conferences I have attended, I became very used to sitting through many presentations that used humour at the expense of my former employer. I was never upset by jokes at the expense of *Microsoft* where *Microsoft* had earned the derision. I believe the humour used in my presentation at the expense of *Symantec* was justified, but it was unfair to fail to acknowledge the dedication, intellect and ingenuity of the many people *Symantec* employs.

My apologies to any who may have been offended – that was never my intent. I appreciate the many times that various people in the AV industry, including *Symantec* employees, have invited me to join their tables, even at the peril of lowering the overall IQ of the group! The presentation was my personal perspective. *ESET* was not afforded editorial review of the final presentation, and only had access to a semi-final draft of the printed review for feedback prior to submission. The contents of the printed and published presentations were my own work and my responsibility.

Special thanks to Jimmy Kuo and Nick FitzGerald for the live 'command performance' of their quotes.

Randy Abrams
ESET, USA

ERRATUM

CORRECTIONS TO WINDOWS 2000 SERVER COMPARATIVE REVIEW

Following the publication of last month's *Windows 2000 Server* comparative review, some questions have arisen over several of the files from the clean test set which caused false positives from a number of vendors. After some deeper analysis, *VB* concludes that some amendments are required to the clean test set, as well as to the number of VB 100% awards given in last month's review.

The file that spoiled *BitDefender*'s chances of gaining a VB 100% award, along with those of *G DATA* and *AEC* (manufacturer of *Trustport*), has been identified as a hacker tool, detection for which was recently added to the *BitDefender* product. The file will be struck from the clean set, and since this was the single point of failure for all three of these products, all three are now awarded a VB 100%. *G DATA* also joins the elite group of products detecting 100% of samples across all the test sets in October's review. *VB* extends its apologies to all three companies.

The file labelled 'suspicious' by *Symantec* has also been identified as a hacker tool, and as such it will be removed from the clean set (since *Symantec*'s product merely labelled the file as 'suspicious', rather than claiming that it was malicious, the product was not denied a VB 100% in last month's review).

Finally, a corrupted zip which *Avira*'s *Antivir* product flagged as infected, has been identified as a file which should have been removed from the clean set a while ago. The file has been confirmed as containing code of the Fosforo virus, which after careful extraction remains a working threat. *Antivir* was the only product to detect this. The remaining clean set file alerted on by *Avira* has been confirmed to be a false positive – we are told that *Avira* developers spotted and fixed this issue in late September.

Moving on from false positives, *VB* regrets that typographical errors appeared in both the on-demand and on-access tables published for the October 2006 comparative review. In both tables the number of files missed by *Antivir* in the polymorphic and standard test sets were transposed. In both tables the numbers *should* have read '0' in the standard set and '150' in the polymorphic set. The percentages reported in the tables are correct as they stand. *VB* apologises for the confusion.

A thorough review of the *VB* clean test set will be conducted before the next comparative review, which will test products for the *Windows XP 64-Bit* platform. The results of that review will be published in next month's issue of *VB*. Vendors wishing to submit products for future reviews should contact John Hawes at john.hawes@virusbtn.com.

CONFERENCE REPORT

MONTRÉAL IN THE FALL

Helen Martin

This year the *VB* conference travelled to the second largest French-speaking city in the world – the vibrant Canadian city of Montréal. The venue for this year's event was the Fairmont Queen Elizabeth – a hotel whose claims to fame include having hosted the second of John Lennon and Yoko Ono's legendary 'bed-ins'. John and Yoko spent seven days at the Queen Elizabeth in 1969, during which they recorded the song *Give Peace a Chance* in the hotel.

There was no time for bed-ins at the *VB* conference though: continuing the trend of the last two years, VB2006 was the longest and most content-filled *Virus Bulletin* conference to date. The full three-day format seemed to be a hit with delegates, with a greater number of presentations on offer, as well as increased networking (and drinking?) time.

GETTING THE BALL ROLLING

The conference programme kicked off at 10.30am on Wednesday morning and straight after the official conference opening Mikko Hyppönen took to the stage for his keynote presentation 'Case: Virus X'. At least that was the plan. Mikko explained that he had been prepared to present an interesting case study of a several-month-long criminal investigation with which he had been involved, which had followed the movements of a for-profit botnet gang. Unfortunately, three weeks prior to the conference Mikko received a phone call from a 'friendly police officer' telling him he couldn't speak publicly about the case. Instead, Mikko pulled together a sharp and entertaining presentation on the major developments in malware over the last 20 years. While possibly not as sexy a subject as originally planned, the presentation was exceptionally well executed and got the conference off to a roaring start.

Rob Murawski followed with a presentation that was the start of what proved to be something of a theme for the conference – Rob was the first of several speakers to look at different aspects of cybercrime, his presentation concentrating in particular on how attackers steal sensitive data.

Wednesday afternoon saw the conference split into its traditional two-stream format (technical and corporate). Peter Cooper and Stefan Görling battled it out in the corporate stream over the virtues or otherwise of user education. Stefan Görling was first to speak, the crux of his argument being that, since security will always be a secondary goal for users, teaching them how to be safe online will never solve any problems. Peter Cooper's paper, meanwhile, argued that user education can be significantly more effective if the information is presented in an appropriate manner. Peter illustrated a variety of different learning styles and gave examples of how information can be presented to cater to each, thus maximising the amount of information users process and take away with them. Peter was unlucky enough to suffer from hardware failure during his presentation, when his Mac laptop unexpectedly shut down. The mishap couldn't have been more brilliantly timed however, since his very next slide (once re-booted) advised 'be memorable' – raising a round of applause and laughter from the audience and leaving many wondering whether the hardware failure had been a deliberate stunt. (We are assured that it was merely a fluke.)

The serious business of day one was rounded off at the end of the afternoon with sponsor presentations from the two platinum sponsors of the conference. *ESET*'s Andrew Lee and *BitDefender*'s Beau Roberts both presented papers looking at heuristic detection, with both sessions being well attended.

Of course, at the end of day one that only left the *other* serious business: the VB2006 drinks reception. Four of Montréal's most talented caricaturists set up their easels in the hotel's Hochelaga rooms and were soon frantically sketching the night away as delegates lined up for their turn to be depicted in amusing situations, cartoon style. Some of the results can be seen above.

IN THE MIDDLE

Day two of the conference kicked off bright and early with presentations by Jeff Williams and Roel Schouwenberg in

the corporate stream, and Jim Wu and Aleksander Czarnowski in the technical stream. Aleksander's presentation – which took an in-depth look at rootkits and anti-rootkit safeguards – was the subject of much discussion and media attention as he indicated that features of *Microsoft*'s imminent *Vista* release will likely be abused by hackers and malicious code writers within several months of its release.

Alex Shipp presented a paper on targeted trojan attacks, revealing that of the three million pieces of malware *MessageLabs* sees each day, an average of only seven will represent targeted trojan attacks. Alex illustrated the ease with which such attacks can slip under the radar with an example of one targeted trojan, identified months previously, for which just four anti-virus products included detection. Alex concluded that, while the good news is that the probability of a company being attacked successfully is extremely low, the bad news is that the potential cost of such an attack is very high indeed.

Later in the corporate stream, Guillaume Lovet's presentation – illustrating the business models of cybercriminals – raised some eyebrows in shock when he indicated that phishing attacks could be more profitable (as well as significantly less risky) than the manufacture and sale of hard drugs.

Thursday afternoon was dedicated to papers covering corporate and technical aspects of spam and phishing, amongst which birthday boy Dmitry Samosseiko and his colleague Ross Thomas provided an analysis of modern spam techniques, and Dmitri Alperovitch revealed how easy it has become to create customized phishing trojans. With do-it-yourself trojan creation kits ranging from approximately $100 to $5,500, it's a sobering thought that even the most technically inept criminal can create trojans that will go undetected by most AV engines.

In the technical track Vipul Sharma revealed how spammers' obfuscation tactics can be exploited to improve spam filtering and showed how *Proofpoint* had constructed a custom classifier for 800 commonly obfuscated words.

Thursday afternoon's programme culminated with a discussion of the work past, present and future of the Anti-Spyware Coalition. This was followed by an off-schedule birds of a feather (BoF) session organized by John Graham-Cumming on the subject of image spam – which John reports was well attended with some interesting discussions.

CIRQUE DE VB

Of course, no *VB* conference would be complete without the annual *VB* gala dinner and cabaret. Every year *VB* invites delegates to dress formally for the occasion – while equally warmly welcoming those who prefer not to, of course – and every year *VB* is delighted by the turnout of beautifully preened delegates. This time was no exception as the photographs below testify. Entertainment for the evening was provided by three jaw-dropping cirque-style acts followed by the beautiful music of the François Dufresne jazz band.

Starting the evening off was Sam Alvarez who wowed the room as he demonstrated a stunning combination of grace, strength and flexibility in his aerial tissue performance. Next up was Throw 2 Catch, a highly entertaining juggling duo whose energetic act made juggling with nine batons look easy. Finally, all eyes were on Genevieve Bessette's dizzying aerial hoop performance high above the stage. After dinner the dulcet tones of the François Dufresne jazz band provided the

perfect background for relaxed after-dinner conversation as the evening came to a close.

UNLUCKY FOR SOME ...

Day three of this year's conference fell on Friday 13th. While the *VB* conference organizers try to avoid superstition where possible, when taking into consideration the catalogue of disasters that have befallen *Virus Bulletin* conferences over the past 16 years we couldn't help but feel a little apprehensive waking up on the morning of Friday 13th. Happily, however, our fears were allayed when the final day of the conference went without a hitch.

Adam O'Donnell and Masaki Suenaga should be congratulated for braving the early morning shift on the morning after the night before. In the event, both presentations drew respectably sized audiences and the number of bleary eyes spotted was minimal.

After coffee John Morris and Eric Kedrosky showed how their forensic tool, 'the inspector', has resulted in a fivefold reduction in the number of infections seen on systems in their organization. As an aside, John revealed to the audience in the corporate stream that he uses *Linux* because he believes it currently to be less vulnerable to viruses than *Windows* – confessing that he only said so because he felt safe in the knowledge that all those with a strong 'belief' in Unix viruses were likely to be next door. Which indeed they were – listening to presentations by Patrick Knight, Jakub Kaminski and Marius van Oers on Unix malware, *Linux* threats and Macintosh OSX binary malware, respectively.

Paul Ducklin started his presentation with some audience participation. Paul asked all those with laptops in the audience to follow his directions and delete notepad.exe – then revealed that we had just witnessed the recreation of a little piece of malware history, it being 19 years to the day (Friday 13th) since the payload of the Jerusalem virus first activated. Paul's presentation itself was less historical and was based around the question:
'Can strong authentication sort out phishing and fraud?'. Thankfully Paul resisted the temptation to provide a single-slide, one-word answer to the question and instead gave a lively and informative presentation.

The highlight of the conference for many was Randy Abrams' presentation. With a title as provocative as 'Microsoft AntiVirus – extortion, expedience or the extinction of the AV industry?' it was little surprise when delegate after delegate filed in for this potential showdown from the former *Microsoft* employee. Recognising the potential for some lively discussion and controversy from this particular presentation, session chair Jan Hruska began the session by dashing off stage only to return seconds later to the tune of *Ride of the Valkyries* and wearing protective headgear. As the delighted audience snapped away with their cameras at the tomfoolery, Randy himself seemed a little concerned, saying 'It's a sobering thought to think that the last living picture of me could be with him in it!' After that it was down to the serious business of the presentation. Randy's presentation was entertaining and informative and he gave a balanced and considered opinion on what *Microsoft*'s entry into the AV market will mean for the rest of the industry. He was a little less kind to other AV giants, most notably *Symantec*, and although the majority of attendees took his comments in good humour, a letter from Randy is published in this issue (at his request) as an addendum to his presentation.

The closing panel session saw the 'Internet Strike Force' (David Perry, Righard Zwienenberg, Alex Shipp, Stacy Arruda, Jeannette Jarvis and Larry Bridwell) discuss different aspects of fighting international cybercrime. Strangely no one came forward when the panel challenged 'If anyone in the audience is a member of organized crime, please raise your hand.' As is often the case with these panel sessions, the discussion could have gone on long into the evening, but had to be cut short as the conference came to a close. No doubt it is a topic that we will return to time and again in the future.

While there has not been enough room here to mention more than a small selection of the presentations, I would like to extend my thanks to all of the VB2006 speakers (and the reserve speakers who stood on standby with their papers but were not needed this time) for the contributions they made to the conference. Some of the slides from their presentations, as well as more photographs of the event will be available soon at http://www.virusbtn.com/conference/vb2006/.

VIENNA WAITS FOR YOU

As always, the organizers of the *VB* conference appreciate the feedback delegates provide (we do read *all* of the assessment forms). It is clear from this year's feedback that the inclusion of a good deal more technically focused material is in order for next year. A call for papers for VB2007 will be issued next month, so if you think you are up to the job, start preparing your submission now!

VB2007 will be held 19–21 September 2007 in the beautiful historic city of Vienna, Austria. I look forward to seeing you there.

Photographs courtesy of: John Alexander, Jeannette Jarvis, Andrew Lee, Petr Odehnal, Martin Overton and Eddy Willems.

PRODUCT REVIEW

F-SECURE INTERNET SECURITY 2007

John Hawes

On my return from the VB2006 conference, there remained little time to source and review a product for these pages. With most products these days offering far too much functionality to be covered adequately in just a few days of testing, I opted to avoid the sprawling catch-all corporate offerings and instead to get my hands on something for the workstation, offering all its components in a single package for use on a single machine.

F-Secure has long enjoyed a high public profile, with vigorous marketing activity and a penchant for controversy. The company has strong PR, led by the charismatic Chief Research Officer Mikko Hyppönen, and a solid history in technical tests and reviews alike. With a reputation for making use of technologies licensed from other leading security developers in combination with its own efforts, the Finnish company is strong in both detection and innovation. The company's *BlackLight* anti-rootkit tool hit the market long before other vendors were able to follow suit, and the company placed considerable faith in mobile phone security some time ago (which now finally seems likely to become as important as the company has long believed it to be).

F-Secure Internet Security 2007 (*FSIS2007* from here on in) is very new, having been released in mid-October. The product replaces *F-Secure Internet Security 2006*. It offers a range of anti-virus, anti-spyware, anti-spam and firewall functionality, much of it improved over previous releases, along with various other security tools including a parental control module, which is new in this version. Also new for 2007 is 'DeepGuard', described as 'a unique proactive detection technology', designed to protect against as-yet-unknown issues.

Priced at a fairly modest 79.90 euros in the *F-Secure* online store, the product is aimed firmly at the home user market, and I expected to find chunky buttons and sliders for the ham-fisted mouse user, cuddly cartoon graphics (*F-Secure*'s association with classic Finnish cartoon characters *The Moomins* is legendary), and simplified or even locked-down controls.

WEB PRESENCE, INFORMATION AND SUPPORT

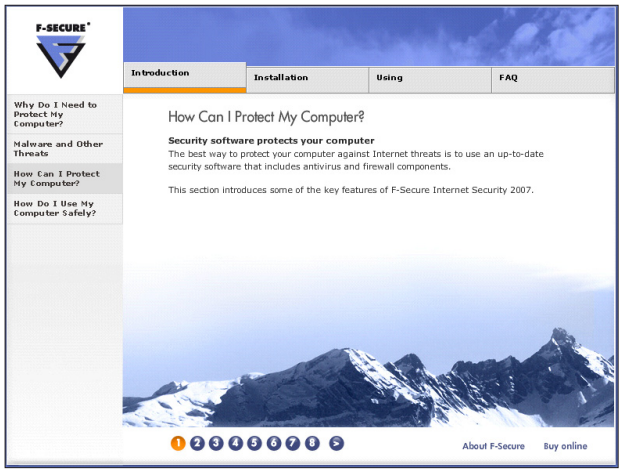
The company's flagship website, http://www.f-secure.com/, is decked out in corporate colours – a chilly pale blue and white, accompanied generally by pictures of cold-looking water, snowy mountains or frozen fields. At the time of writing the front page carried a banner promoting the new product, displaying its packaging with an even chillier polar landscape and the stark slogan 'BE SURE'.

The site features the standard malware and company news sections, areas dedicated to various different customer types and to partners, and a security centre carrying malware descriptions, guides and tools, statistics, and the lab team's blog. This blog is a miscellaneous resource blending the informative with the trivial, often within the same posting, and comes adorned with a group photo of the research team in all their glory, gathered around their long-haired leader.

Prominent throughout the site are references to the company's response time, which apparently leads the field, averaging two to four hours, with updates 'twice as often as major competitors'. The 'Radar' alert system is available to send warnings of security issues to mobile phones and other devices, and applies a rating system to malware based on how widely it spreads and other factors.

I searched elsewhere on the site for some of the company's graphical gizmos, the latest and most awe-inspiring of which were demonstrated spectacularly by Mr Hyppönen during his keynote speech at the recent *VB* conference. A Virus World Map is linked to from most pages, and displays virus outbreak data. The map depicts either all malware or one of a select list, over time periods ranging from the last hour to the whole of the current year, and covering the globe as a whole or by individual continent. Viewing the map on a larger scale is fairly uninformative, but focusing in is more revealing, and with a few quick clicks of the mouse I learned that Sweden, Finland, Denmark and Belgium were among the most virus-hit places in Europe during October, and that Vietnam had been a hotbed of malware activity that day in an otherwise quiet Asia.

Accessing the area of the site dedicated to *FSIS2007*, I found an online tutorial, illustrated with photos and artwork



appropriate to the given information. *F-Secure*'s trademark cool blue-tinged images of frozen landscapes and close-ups of water reflecting cloudless skies mingled with pictures of Swiss army knives connected to the network port of laptops and cartoons of wriggling worms and scary spiky bombs. The tutorial commences with some general information on the risks threatening computer users, and some tips on computer security and how to be safe online. This is followed by fairly detailed sections on installing and using the software, and an FAQ, spread over numerous short pages embellished with pictures.

The support area of the website carries a more substantial FAQ, supplementing the questions answered by the tutorial. The support section has a slightly different design from the main body of the site, although still sticking to the white-and-blue colour scheme, and along with the product-specific areas also has a selection of tutorials, articles, tools and tips. The 'How to contact support' page seems to try to avoid mentioning the possibility of actually getting in touch with *F-Secure*, first discussing the wide range of online facilities and other support channels available to various types of customer, before eventually conceding that a call could be made to the company itself and providing a list of contact numbers. Deciding to take a chance, I left the web behind and ploughed ahead with installing the product.

INSTALLATION AND SETUP

Without a hard copy of the product to play with, I had to content myself with running the downloaded installer file.

The installation process is simple and straightforward, with few options to bemuse the novice user. Indeed, after selecting my preferred language – from a list including a broad set of European languages as well as Japanese – the only real choice (other than whether or not to accept the licence agreement and where to place the root folder) was whether to drop the parental control functionality from the install. I allowed this module to be installed, as without web access (as is the case in the test lab) it defaults to an inactive state, and thus wouldn't prevent me from doing anything naughty while trying out the other aspects of the product.

The EULA contained all the standard disclaimers and reservations, including granting the rights to display any statistical data that may be gathered in forms such as the World Map mentioned above.

The online FAQ mentioned an ability to detect automatically and remove 'software from the largest security software vendors' as part of the installation process. I checked this out, installing the product over a selection of other security products including anti-virus from *Symantec* and *McAfee*, and *Webroot*'s *SpySweeper* anti-spyware. It detected each of them quickly and ran their uninstallers. The process was a little confusing however, as each opened their 'Are you sure you want to remove me?' and 'I need a reboot now' dialogs behind the *F-Secure* install window, which showed a progress bar chugging slowly along while it waited for me to let the uninstallation continue. Once I realized what was happening, the process completed smoothly and without further issues.

On a rather weary old machine, rather below the minimum recommended specifications, the final stage of the installation and setup process took several minutes. This time was reduced considerably on more modern hardware, but still averaged around a minute even on a fairly high-powered computer.

The install and setup is followed by a reboot to get things fully operational – the reboot mechanism grants the user 300 seconds to prepare themselves, but in my eagerness to get a look at the product I avoided waiting the full five minutes, and hurried things along.

The product's initial action on activation was to attempt to contact home, to verify my subscription and check for updates. Prevented from doing this in my sealed-off lab, it offered me the options to retry the validation, to uninstall the product, or to carry on regardless – in which case the product would deactivate after seven days.

Next up, according to the online tutorial I had so closely followed, should have been a startup wizard, offering configuration of the parental controls, and setup of the spam filtering, application control, an initial scan of the machine and some scheduled checks. Without proper validation, however, these steps were skipped, but could be accessed again later via an option available from the Start menu (with the exception of the parental control sections, the wizard for which was available from the main dialogue).

OPERATION AND DOCUMENTATION

Opening the product from the system tray (no desktop shortcut was provided), I was presented with a surprisingly small and busy GUI that was rather heavy on text. The 'Home' page informed me that updates and the parental control functions were disabled, and that validation had yet to take place, but that all other modules were operating normally.

The other modules comprised 'Virus and spy protection', scanning both file access and email, an 'Internet shield' made up of a firewall, HIPS and application control, and 'Spam control'. Small but smooth buttons down the left-hand side led to individual panes for each section, while clicking on 'Advanced' or any of the numerous 'Change' or 'Configure' links brought up a second window, again text-oriented, with a tree structure and numerous configuration options.

The home page featured a security news ticker, which unfortunately didn't work in my isolated environment. There were also links to the main *F-Secure* site, and to the support section, while buttons allowed the user to update or validate their software.

Apart from these links to external resources, most of the main GUI was purely informational. Status, and in some cases statistical data, was presented in each section, along with a link to the appropriate page of the 'Advanced' controls. The main exception to this was the 'Scan my computer' link on the 'Virus protection' tab, which opened a small menu of scanning options, including scanning a particular target, a full drive, checking for spyware or rootkits, or performing a complete scan of the system. Each of these in turn opened a further window: the scan wizard. This displayed the file currently being scanned, and details of the number of files scanned and detections, but no estimate of the progress made. There was also an option to run scans from the right-click menu in *Explorer*, which again led to the same scanning screen.

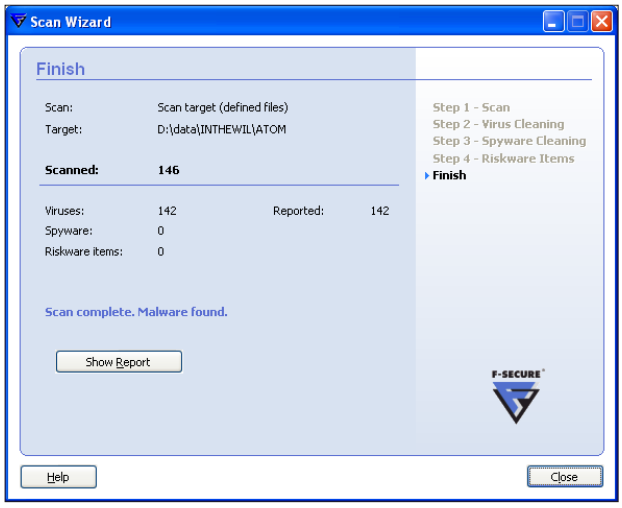
The 'Advanced' tab contained numerous sub-sections, some of them with their own layers of tabs for further control. Many of these offered information with few options, while others were loaded heavily with tweakable controls. The main on/off functionality for each section tended to be greyed out, and could only be accessed using a 'Change' link from the main GUI; this in turn opened a dedicated dialog from which one could adjust, say, the paranoia level of the virus monitoring. The net result of this multi-window system was perhaps a little confusing, and occasionally left me searching for the settings for a particular feature, but once I had gained a feel for where things were it did seem fairly sensibly laid out.

Help is generally available via a context-sensitive link, opening a large and once again rather chilly-looking window with some information on the given section. Like the interfaces, the help is fairly text-heavy, with little in the way of the friendly diagrams and step-by-step guides I had expected to see in a home-user product. There were also none of the handy links to the corresponding page of controls in the main interface, only descriptions of how to open them for yourself. As such, it was less integrated with the product than some users may find useful, seeming to be aimed more at those wishing to learn how to use the product in full rather than those looking for a quick fix to a given problem. It is, however, fairly thorough for those who have the time and inclination to wade through it all, with most of the hidden or hard-to-decipher functionality explained at some point.

MALWARE SCANNING

The first thing I spotted after the initial setup of the product was a message, displayed when hovering my mouse over the system tray icon, informing me that my virus definitions were 'very old'. When the GUI came up, I was reminded of this in bold red text across the top of the main page, this time using the words '*really* old'.

Checking on the advanced page for the updates, I saw that the virus definitions included with the shipped product dated from late May, and the spyware identities from early June. It seemed a little odd that a product shipping in October should contain such old data (perhaps the datestamps displayed were misleading), but of course for the real user this would be remedied on install, as soon as the software connected to the web for the initial validation and update. For me, however, it presented an ideal opportunity to try out the product's heuristics and the new 'DeepGuard' proactive detection.



I ran a few scans over the *VB* virus collections, and was not surprised, given *F-Secure*'s performance in most recent *VB* comparative tests, by the rigorous detection of just about everything we had (barring a few file types that were not scanned in certain modes).

What was somewhat surprising – and quite pleasantly so – was the product's detection rate when faced with some newer files. A scan over some of the more recent additions to the WildList revealed several files that were not detected, either on demand or when accessed by a simple file-opening utility. However, when the files were executed properly, several examples of the older and more numerous WildList favourites – such as W32/Bagle, W32/Mytob and W32/Mydoom, as well as more recent additions such as W32/Areses (aka Scano) – were picked up by generic detection in the virus engine.

Elsewhere, a selection of the latest malware joining the list, including W32/Banwarum and even W32/Stration (aka Warezov), were stopped by the System Control function, which picked up on some suspicious behaviours and added them (after prompting in some cases and automatically in others) to a list of blocked applications. This area of the product, hidden away as a tab on the virus scanning config page, creates a list of blocked applications, offering options to prompt before including. It presumably utilizes some features from the Windows Security Centre, as it is available only under fully patched *Windows XP*.

The only piece of malware to cause any trouble was W32/Looked (also called 'Philis' and 'Viking' by some naming systems). Of four variants hitting the WildList in July, none were picked up by straightforward scanning. When executed, with the protection setting at its default level, most were blocked by the System Control. With the setting turned up to high, all but one sample were detected as generic P2P worms. Some behaviour was permitted, including dropping some files and creating a few copies, and a couple of variants managed to sneak past the standard level of defence to the extent that files picked up as suspect could not be removed, or the explorer.exe process into which they had injected themselves crashed, on one occasion bringing the whole machine to a standstill. Nevertheless, nothing in the WildList escaped detection of some sort, with at least a warning being given that some suspicious activity was happening. With more up-to-date definitions, of course, all these problems were dealt with more accurately and efficiently.

Clean files caused no problems either, with no false positives on any scan of the standard *VB* clean sets. Running a random selection of applications, of various degrees of usefulness and taken from both the clean set and other sources, also failed to generate any unnecessary warnings from the monitoring system.

At the end of one scan of what I believed to be a clean machine, the action dialog was presented to me with two items of 'riskware' discovered. The actions offered included delete, quarantine, exclude and do nothing. The names given to the riskware items were clickable, but led only to some online threat information, (which, being in my lab, I could not access), so I was at a bit of a loss to figure out just where these files were, and what they were doing on my freshly-imaged machine.

This minor annoyance was solved simply by ignoring the actions and going straight on to the report, but it would perhaps have been useful to know the filenames and perhaps even paths of infected or supposedly dangerous objects, before deciding whether they should be removed or not. In the end I learned that the items in question were merely copies of the old *PSKill* utility from *Sysinternals*, stored in a stash of testing tools.

Another scan, running over the full collection and clean sets in full-paranoia mode, took a considerable length of time and eventually froze up scanning a clean file, requiring me to kill it using the task manager. Repeated attempts to reproduce this behaviour brought no luck, however, and I was forced to put it down to a random event. Even in the most thorough mode, with numerous infections and bad files to deal with, scanning a standard *Windows* install, with a mid-sized drive and a selection of software installed, along with a scattering of typical large media files, never took more than a few hours – a pretty decent result compared to the overnight or even full weekend required by some products.

The system overhead seemed fairly reasonable too, with no noticeable slowdown, even during some intensive activity.

OTHER FUNCTIONALITY

The product contains far more than standard anti-malware, of course. The various other components were tried out to a greater or lesser extent, as time was limited and, thanks to a recent relocation, the machines I would normally use to access the Internet were unavailable for most of the review period. Much of the following was therefore assessed in a sealed-off environment, using spoofed services where appropriate.

In the 'Internet Shield' section, the firewall is controlled by a number of rules, ready populated with a comprehensive set of known malicious probes and dangerous activities. These can be edited and added to, creating personalized rules to allow or deny specific actions and communications, and can then in turn be switched on or off as required; many of the pre-defined rules default to off. The system is perhaps a little more intuitive than many firewall control setups, although still requiring some understanding from the user.

Those with a more paranoid approach to their security may prefer the more usual 'training mode' style of firewall setup, which requires the user to grant networking powers specifically to all software attempting to connect from one's machine, giving them the opportunity to ponder the needs of their software, app by app, should they so wish. This functionality is, in *FSIS2007*, divorced from the firewall configuration section, and instead resides under 'Application Control'.

I was surprised, given its name, that the Application Control functions only over the web, offering no facility to block local use or activity of unwanted software. Such functionality is, of course, more expected in and more suited to a corporate environment, and perhaps a home user would find the title of the section quite appropriate. Selected software can be allowed or denied access to the network, and unknown apps can either be allowed, but logged, or allowed only after user interaction. The first question asked by the startup wizard is whether to allow access to all software, only logging attempts to contact the outside world, or to block everything until permission is granted, the default being the more secure block mode. This can be changed from within the Advanced GUI.

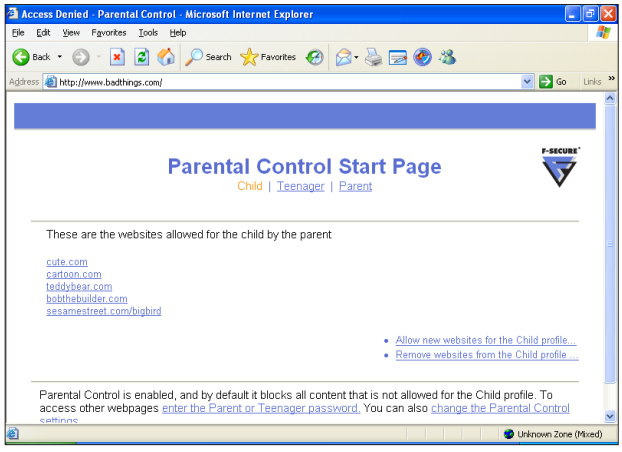
The HIPS system has little configuration available, with only on or off, and block or log only on detection of a suspected intrusion attempt. There is also a dial-up section, where connections to specified numbers can be allowed or denied.

Under 'Spam control', another fairly basic set of controls allow the user to change the spam settings from the default medium to 'relaxed' or 'aggressive', as well as to switch off RBL checking. White- and blacklists of email addresses can be set up, with an option to import *Outlook* addresses to populate the whitelist. *Outlook* is integrated automatically, while other clients require some setup of spam folders and filter rules (instructions are provided in the help pages for *Netscape* and *Mozilla*, *Opera*, and *Eudora*). Separate phishing filtering, which places known phishing scams into a separate phishing folder, is supported only under *Outlook*. The accuracy or otherwise of the spam filtering, like that of the HIPS system, sadly falls outside the scope of this review.

The 'Parental Control' feature is one of the main items that is new in this version. Once set up from a simple wizard, which involves little more than entering passwords for 'Parent' and 'Teen' users, the access control system is opened on the next attempt to browse the web. From here, settings can be decided for the 'Child' and 'Teen' users.

Younger children are granted access only to an explicitly designed list of websites, a 'walled garden' wherein they can play safely. Full sites or subsections thereof can be entered into the list, and an option is available to allow access to all sites designated child-friendly by *F-Secure*. On attempting to access a site not included on the list while the child mode is active, the browser redirects to the control page, which displays a clickable list of the permitted sites. The screen is rather stark and cold, in typical *F-Secure* style, and could perhaps do with a little warming up for the youngest audience.

For the teenager group, a slightly more complex system operates. Certain types of site are barred, presumably using a central blacklist maintained by *F-Secure* or one of its affiliates. These are grouped into categories, which can then be allowed by more permissive parents (categories are also set up for chat and webmail sites, but allowed by default). Specific sites can be allowed within these groups should the need arise, and others blocked specifically at the whim of the parent, using the same selection system as for children.



A time lock function is also available, to control when the net is available, with separate time settings for the two different groups (no time settings are available for the adult user). Once the parental password has been set, generally as part of the install, it is requested every time changes are attempted to the settings of the product. The parental controls revert to child mode on reboot or on activation of a screensaver.

Were I a parent I expect I would feel fairly happy leaving my offspring in the hands of *F-Secure*'s product, but a few things could usefully be added, I thought. A keyword-based web blocking system is common in parental controls, scanning sites for undesirable words, but these are notoriously 'dumb' and prone to error. Perhaps with more security companies joining the market, some extension of anti-spam technology could be usefully applied to the problem. Also, the blocking of undesirable software, such as games that are unsuitable for younger types, may be handy. The System Control feature creates a list of blocked apps, but seems to lack the option to add things to the list oneself, including them only once they have been flagged as suspicious by the behavioural monitors.

Away from the main set of functions, there are a few other little tools available. According to the documentation, those lucky enough to have the full CD product will find it is possible to boot straight into a scan from the CD – a handy trick which should circumvent the stealth measures used by certain particularly nasty infections.

For those having trouble with their product, the start menu folder contains a diagnostic function, which runs a set of tests and creates a file which can be forwarded to *F-Secure* tech support to aid in the analysis of problems. The file contains a swathe of logs, stowed in .tar.gz format, packed with data on the system, its makeup and settings, data on the content and layout of the *FSIS* installation, and information about numerous registry keys related to the product. It was in one of these logs that I saw the only mention of *F-Secure*'s previous name, *Data Fellows*, still lurking in a number of legacy registry settings.

CONCLUSIONS

FSIS2007 provides a pretty thorough selection of security tools designed to guard against a wide variety of threats. Its detection of viruses, trojans and spyware is highly impressive, especially when blocking unknown threats using either generic identities or behaviour patterns, and its speed, overhead and reliability cannot be faulted. The numerous other functions: filtering spam, monitoring network and local activity, and blocking unwanted web content from younger users, covers most of the security issues facing users. The only component that seemed to be missing was full local application control, giving users of the parental functions the option to keep their offspring from using certain types of software.

The user experience, for my tastes, left a little to be desired, with the GUIs possibly a little daunting for the average home user, and a little lacking in obvious fine-tuning options for the more experienced. The multi-window approach gives the product something of a disjointed feel, and adds further complexity to the task of configuring the software to one's individual preferences. Functionally, however, it was a slick and fairly comprehensive set of controls, with no important options absent or unusable. Of course, for the truly novice user, the entire interface can be ignored most of the time, with the default settings providing comprehensive protection straight out of the box.

Overall, this is a solid product that oozes reliability, giving a warm feeling of safety despite the cool themes of its design. Indeed, it could be that the interface deliberately shies away from the friendly, cuddly touches I had expected, precisely in order to foster this sense of solid, professional protection. I only wish I had more time to try out the wide range of features in a more rigorous and scientific manner; doubtless we will meet again on the *VB* comparative test bench.

Technical details

F-Secure Internet Security 2007 was tested on:

AMD K6, 400MHz, with 512MB RAM and dual 10GB hard disks, running *Microsoft Windows 2000 Professional Service Pack 4*.

Intel Pentium 4, 1.6GHz, 512MB RAM, dual 20GB hard drives, 10/100 LAN connection, running *Windows XP Professional SP2*.

AMD Athlon64, 3800+ dual core, 1GB RAM, 40GB and 200GB hard drives, 10/100 LAN connection, running *Windows XP Professional SP2* (32bit).

END NOTES & NEWS

InfoSec World 2006 Lapland takes place 21–24 November 2006 in Rovaniemi, Lapland, Finland. For more information see http://www.mistieurope.com/.

SecureGOV 2006 takes place 3–5 December 2006 in Farmington, PA, USA. The fourth annual SecureGOV strategic intelligence meeting offers senior government IT, security and privacy officers insight into the latest developments critical to maximizing the protection of information resources, wireless communications, networks and critical infrastructure. See http://www.convurge.com/.

AVAR 2006 will be held 4–5 December 2006 in Auckland, New Zealand. For full details, conference agenda and online registration see http://www.aavar.org/.

The 22nd ACSAC (Applied Computer Security Associates' Annual Computer Security Conference) takes place 11–15 December 2006 in Miami Beach, FL, USA. Alongside a technical program and a 'work in progress session' attendees may also register for a workshop on host-based security assessment and tutorials on subjects that include biometric authentication, malware, live forensics, security engineering, next-generation wireless risks, certification and accreditation, and large-scale network traffic analysis. For details see http://www.acsac.org/.

The 2nd AVIEN Virtual Conference will take place online on Wednesday 10 January 2007, from 15:00 to 17:00 GMT (starting at 8am PST, 11am EST). This year's conference topic is 'The new face of malware: stories from the battlefield'. Sign-up details will be announced in due course.

RSA Conference 2007 takes place 5–9 February 2007 in San Francisco, CA, USA. The theme for this year's conference – the influence of 15th century Renaissance man Leon Battista Alberti, the creator of the polyalphabetic cipher – will be covered in 19 conference tracks. For full details see http://www.rsaconference.com/2007/US/.

Black Hat Federal Briefings & Training 2007 take place 26 February 26 to 1 March 1 2007 in Arlington, VA, USA. Registration for the event will close on 18 February 2007. For details see http://www.blackhat.com/.

Websec 2007 will take place 26–30 March 2007 in London, UK. More information will be available in due course at http://www.mistieurope.com/.

The 16th annual EICAR conference will be held 5–8 May 2007 in Budapest, Hungary. A call for papers for the conference has been issued with a deadline of 12 January 2007 for peer-reviewed papers and 1 December 2006 for non-reviewed papers. Full details can be found at http://conference.eicar.org/2007/index.htm.

The 22nd IFIP TC-11 International Information Security Conference takes place 14–16 May 2007 in Sandton, South Africa. Papers offering research contributions focusing on security, privacy and trust are solicited. For more details see http://www.sbs.co.za/ifipsec2007/.

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

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

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

The 17th Virus Bulletin International Conference, VB2007, takes place 19–21 September 2007 in Vienna, Austria. Online registration and further details will be available soon at http://www.virusbtn.com/.

SUBSCRIPTION RATES

Subscription price for 1 year (12 issues):

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

Corporate rates include a licence for intranet publication.

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

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

vbSpam supplement

CONTENTS

NEWS & EVENTS

PHISH CHECK INTERFACE

The people behind *PhishTank*, a collaborative clearing house for data and information about phishing, have revealed a simplified developer interface for checking suspicious URLs against the *PhishTank* database. The *PhishTank* team envisage the interface being used for anything from mitigating new threats on mobile platforms to easing the development of check-only plug-ins for browsers and mail clients – and invite developers to let them know how they put it to use. Details can be found at http://www.phishtank.com/.

SENDER ID SPECIFICATION RELEASED

Microsoft has made its Sender ID Framework specification available as part of its recent Open Specification Promise, allowing developers to use the technology without paying a licence fee to *Microsoft* and without facing penalties for patent infringement.

The Sender ID system ties email addresses to IP addresses in an attempt to prevent spammers and phishers from spoofing sender details. The technology is currently used by a number of mail filter developers, including *Symantec* and *Sendmail*, as well as in *Microsoft*'s *Hotmail* service.

Sender ID has been criticized in the past because the previous *Microsoft* licence didn't allow the technology to be used with open source software. Brian Arbogast, corporate VP of the Windows Live Platform Development Group explained: 'There have been lingering questions from some members of the development community about the licensing terms from *Microsoft* and how those terms may affect their ability to implement Sender ID ... By putting Sender ID under the Open Specification Promise, our goal is to put those questions to rest and advance interoperable efforts for online safety worldwide.'

SPAMHAUS RESTS EASY

At the end of a month-long court battle, a US judge has ruled that UK anti-spam advisory organization *Spamhaus* will not have its domain suspended as a penalty for mislabelling a spammer.

Back in September, a US court found *Spamhaus* guilty of mislabelling Illinois-based company *e360 Insight* as a spammer, and ordered the British organization to pay $11.7 million in damages. *Spamhaus* merely laughed off the ruling at first, pointing out that the US court had no authority over the UK-based organization.

Determined to have their vengeance however, *e360 Insight* and its head David Linhardt then demanded, as part of an appeal, that domain management organization ICANN be ordered to suspend the spamhaus.org domain.

However, Judge Charles Kocoras issued an order late last month denying *e360 Insight*'s motion on the basis that the suspension of the spamhaus.org domain would cut off all lawful online activities of *Spamhaus*, not just those in contravention of the Illinois court's injunction.

EVENTS

The Text Retrieval Conference (TREC) 2006 will be held 14–17 November 2006 at NIST in Gaithersburg, MD, USA. For more details see http://plg.uwaterloo.ca/~gvcormac/spam/.

A workshop on countering spam will be held on 8 December 2006 as part of the ITU Telecom World 2006 event in Hong Kong. The workshop will present the activities of relevant organizations and consider the potential for future cooperative measures and partnerships for countering spam. For details see http://www.itu.int/WORLD2006/.

The Authentication Summit 2007 will be held 18–19 April 2007 in Boston, MA, USA. The two-day intensive program will focus on online authentication, identity and reputation, highlighting best practices in email, web and domain authentication. Presentation proposals are currently being reviewed, with a submission deadline of 15 December 2006. For full details see http://www.aotalliance.org/summit2007/.

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

FEATURE

THE RISE AND RISE OF IMAGE-BASED SPAM

John Graham-Cumming
Independent consultant, France

Anyone looking in their quarantined spam folder will soon notice that a lot of spam these days is being sent using images instead of text.

In a paper presented at the Virus Bulletin conference last month [1], Dmitry Samosseiko and Ross Thomas of *Sophos* reported that, on some days, 40% of the spam seen in *SophosLabs*' spam traps is image-based spam and that the amount of image-based spam has doubled since the start of 2006.

At a birds-of-a-feather meeting on image spam held during the same conference, a representative of one major anti-spam service provider reported that, some days, the amount of image-based spam peaks at 95% of all spam sent, but that 20–40% is typical.

NOTHING NEW

However, image-based spam is not new. The very first trick entered in the *Spammers' Compendium* [2] in January 2003 is 'The Big Picture', which entails sending a spam that consists merely of an embedded picture.

Samosseiko and Thomas [1] report having seen image-based spams in Russian in September 2004. The users of *SpamAssassin* have been discussing the use of optical character recognition (OCR) techniques since 2002 – indicating that image-based spam has been with us for a number of years. According to *IronPort* statistics [4] 1% of spam was image-based in June 2005. By June 2006 that figure had risen to 16%.

Within the last six months image-based spam has become a major problem for anti-spam vendors, all of whom have adapted their tactics and issued press releases touting their solutions. The spammers, meanwhile, have not remained idle and have modified the types of image-based spam they are sending in an attempt to avoid filtering.

Clearly, spammers believe that the right battleground between spam filters and spam is in image processing – and accordingly they have switched from the use of ever more complex text obfuscation (which spam filters easily see through – see for example [3]) to image obfuscation.

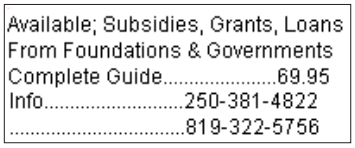


Figure 1: Late 2003 image-based spam.

THE BIG PICTURE

In 2003, when I first reported on image-based spam [2] the images used were very simple. Figure 1 shows a spam image from late 2003.

At that time images were typically loaded from remote websites using a simple HTML <img src=> tag. But the use of remote images died out as email clients (such as *Mozilla Thunderbird* and *Outlook Express 6* in *Windows XP Service Pack 2*) started blocking remote images by default, and spammers started sending their images as MIME-encoded attachments (as they still do). The image in Figure 1 was sent as an attached GIF file.

2006: THE YEAR OF IMAGE-BASED SPAM

Despite having existed for a while, there was little innovation in image-based spam until 2006. In January 2006 the trick named 'The Small Picture' was added to [2]. Within the next couple of months OCR plug-ins were announced for *SpamAssassin*.

'The Small Picture' involves embedding GIF images in the email message. Each image consists of a single letter and is positioned strategically within the text of an HTML-based email to form readable text. Figure 2 shows an example of spam using the 'Small Picture' trick.

Figure 2: 'The Small Picture'.

In Figure 2 the letter 'm' in Ambien, 'o' in Propecia, the first 'a' in Xanax, 'e' in Levitra, the first 'A' in VIAGRA and 'a' in Soma are embedded images.

CHOP GUI

Towards the middle of January 2006 the trick 'Chop GUI' was added to [2]. Here, the spammer attempted to avoid detection (and possibly OCR) by chopping a single image into multiple, randomly chosen rectangles, and then reconstructing the original image using HTML. Figure 3 shows an example of 'Chop GUI' with the boundaries between the individual images highlighted; in the real spam there were no boundaries.

Figure 3 is a rather simple example, where the spammer has simply cut a single image horizontally through the text. A much more complex example is shown in Figure 4, once again with the boundaries highlighted. Here the spammer chose random cuts in the image and used HTML to reconstruct it.

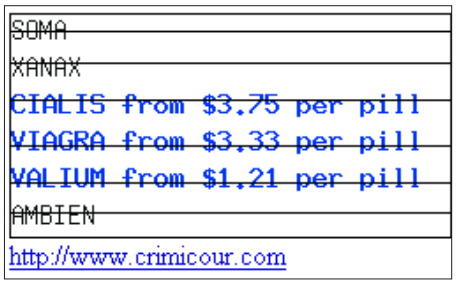


Figure 3: Simple 'Chop GUI'.

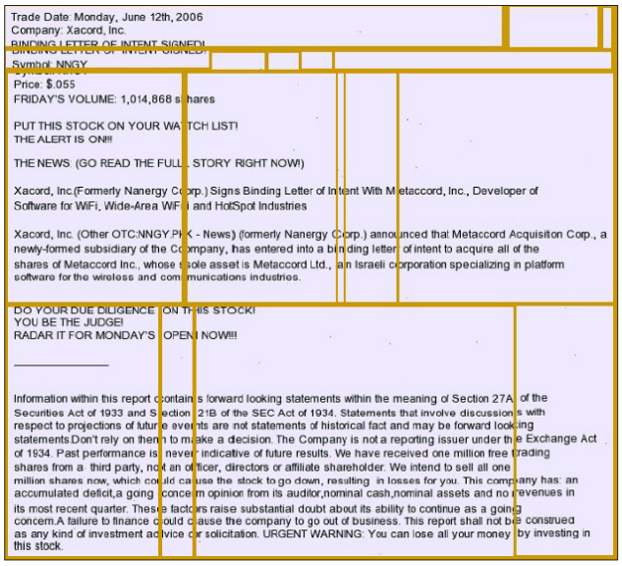


Figure 4: Complex 'Chop GUI'.

At around the same time spammers started to try to resist optical character recognition of their images by overlaying their text with random lines (as shown in Figure 5) or by introducing random stippling of the background, as shown in Figure 6 (which can also be used to change the hash value of the image at will).

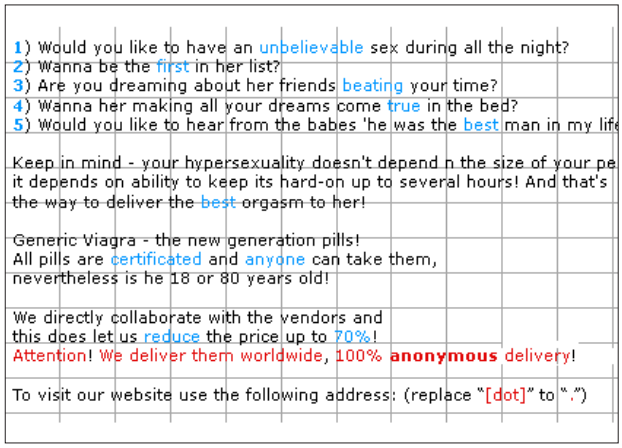


Figure 5: Random lines to avoid OCR.

Figure 6: Random pixels to avoid OCR and hashing.

More recently, spammers have tried using fonts that are almost humanly unreadable as a tactic to avoid optical character recognition. However, this tactic appears to have died out – given that the fonts are hard to read for even the human recipient (see Figure 7) one assumes that the decline of this tactic has been due to the ineffectiveness of the spams.

Notice that the spam shown in Figure 7 also includes a block of random pixels in the bottom left-hand corner. The purpose of this is to change the hash value of the image each time it is generated.

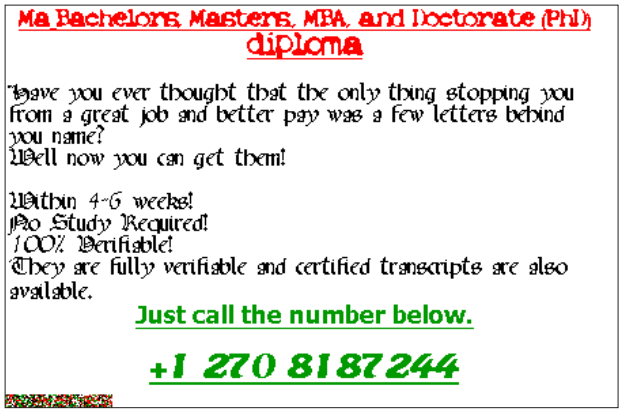


Figure 7: Using fonts that are difficult to OCR.

ANIMATED SPAM

As spam filters have become adept at filtering these images (albeit with random elements added to attempt to avoid hashing or detection), spammers have adapted to use animated GIFs. In August 2006 the first animation-based trick was added to [2]: 'Animated Noise'.

In 'Animated Noise' the spammer sends an animated GIF with a number of decoy frames that consist solely of random noise, and a single frame that contains the actual spam message. The real frame appears for a long period of time (for example, it may stay visible for ten minutes), whereas the decoy frames appear before and after the real frame and last mere milliseconds. The spammer is attempting to fool the spam filter into missing the real frame, although examination of the animation times makes the real frame easy to detect.

Figure 8 shows three decoy frames used in a real 'Animated Noise' spam.

Figure 8: Decoy frames that were displayed for 100ms before and after a real frame.

A progression of the 'Animated Noise' trick was to use the rapidly shown decoy frames to display a 'subliminal' message. As well as flashing frames with random noise added, the decoy frames contained the word 'BUY' in random positions. Figure 9 shows two frames from a 'subliminal' spam.

The frame containing the word 'BUY' (there were three such decoy frames) was flashed for 10ms on screen, the

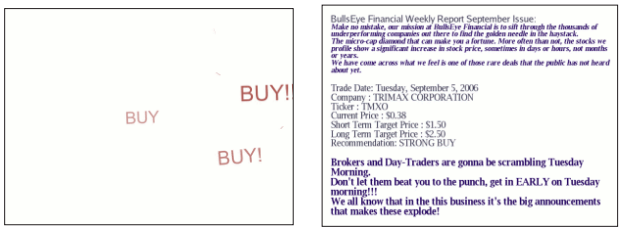


Figure 9: Subliminal spam (left frame shown for 10ms; right frame shown for 17s).

frame containing the real spam message remained visible for 17s.

Since finding the real frame is relatively easy (a spam filter need only look for the frame that is displayed for the longest time, or perhaps for the first frame that is displayed for many seconds), spammers have adapted to use both animation and GIF transparency.

Figure 10: 'Strip Mining'.

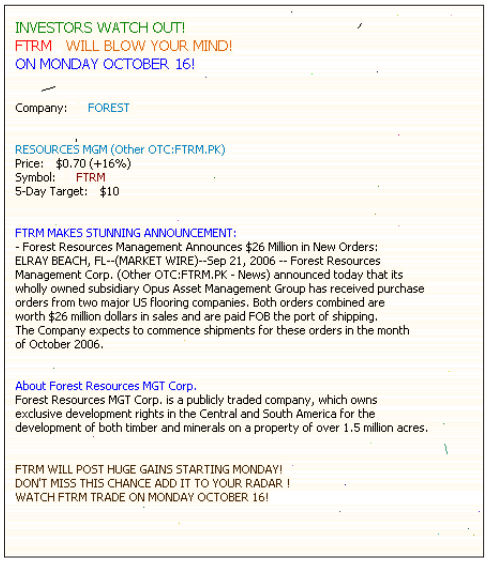
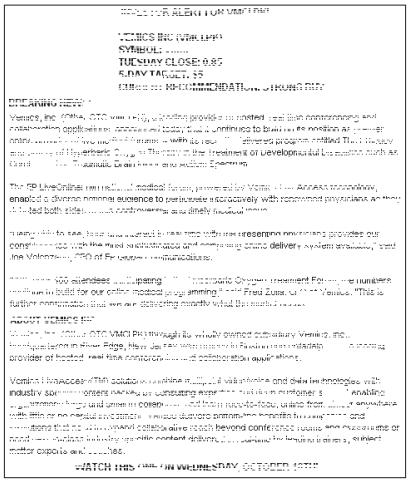


Figure 11: Final image of a 'Strip Mining' spam.



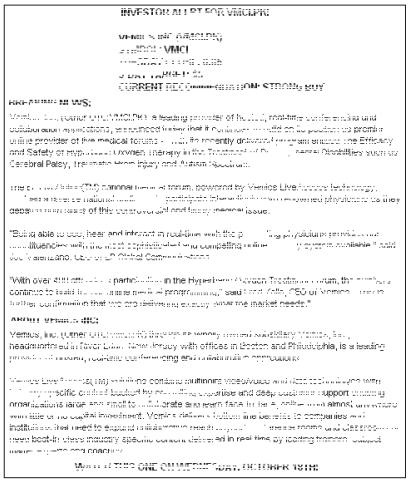


Figure 12: Random pixel stripping between two animated, transparent frames.

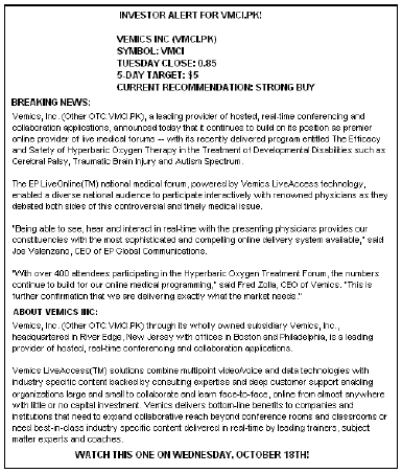


Figure 13: Result of merging the two frames using animation.

STRIP MINING

The first attempt at using animation and transparency follows the 'Chop GUI' style of splitting an image into parts (in this case strips). Each strip of the image is a single frame in the spam image on a transparent background. By animating the various strips one after another each frame shows through the transparency to the next frame, building up a complete picture. This is called the 'Strip Mining' trick in [2].

Figure 10 shows two frames from a 'Strip Mining' spam (the blank areas are transparent) and Figure 11 shows the final image after the animation has completed.

And most recently spammers have taken the animation plus transparency to a new extreme in their battle against OCR by starting from a single spam image and randomly choosing pixels from it to appear on one of two animated frames. In this way neither frame contains text that is readable (by a human or a machine), but the final merged image is readable.

Despite the cleverness of this scheme the developers of the *SpamAssassin* OCR plug-in report that the latest version of the plug-in merges and OCRs these image spams successfully.

Figure 12 shows an example of two frames from such a spam, and Figure 13 shows the merged result.

CONCLUSION

Despite the cleverness of the trickery being used by spammers, current techniques for filtering image-based spam are working. Anti-spam vendors report using a mixture of image hashing, regular expressions and examination of image meta data (such as the palette, presence of animation and compression ratio) to catch image-based spam. A great danger for spammers is that (as in the case of text-based spam) they become enamoured with the obfuscation possibilities present in image-based spams only to see their spams easily filtered just by detecting the obfuscations themselves.

Spam filter authors will need to be on the lookout for new image-based spam techniques as spammers are innovating actively to attempt to avoid detection. Recently spammers have started to switch from GIF formatted images to PNG, some spammers are corrupting their images deliberately to make decompression difficult, and others are reporting that an image is a JPEG when it is, in fact, a GIF.

Image-based spam remains fertile ground for spammers and spam filter authors.

REFERENCES

[1] Samosseiko, D.; Thomas, R. The game goes on: an analysis of modern spam techniques. Proceedings of the 16th Virus Bulletin International Conference 2006.

[2] Graham-Cumming, J. The Spammers' Compendium. http://www.jgc.org/tsc/.

[3] Sharma, V.; Lewis, S. Exploiting spammers' tactics of obfuscations for better corporate-level spam filtering. Proceedings of the 16th Virus Bulletin International Conference 2006.

[4] Image-based spam makes a comeback. http://www.dmconfidential.com/blogs/column/Web_Trends/916/.