

# network SECURITY

ISSN 1353-4858 March 2009

www.networksecuritynewsletter.com

## Featured this month:

### Google hacking 101

**G**oogle provides penetration testers and hackers alike with a surprisingly powerful tool. It relentlessly indexes error messages, files in unprotected directories, log files and a plethora of other information useful to anyone wanting to probe the security weaknesses of a site.

But specially crafted searches – the technique of Google hacking – will find all sites with known vulnerabili-

ties, making Google a virtual directory of attackable sites. A weakness in your site will attract hackers who might otherwise never have heard of you. It's like advertising your weak points. Steve Mansfield-Devine examines the basic techniques of Google hacking – the so-called Google dorks – as well as simple countermeasures.

*Go to Page 4...*

### Security audits in mixed environments

**S**ecurity audits are now part of the regulatory landscape for many organisations, and it becomes particularly important when dealing with third party providers such as outsourcers. Service contracts must be complemented by documentation clearly explaining the nature of such audits, and the expectations from them. Under such agreements, individuals within the customer and the outsourcing provider must understand the role is that they play in supporting such security audits.

Making reference to best practices and international standards, Dario Forte examines the assignment and control procedures for outsourcer authorisation profiles, assessing their potential impact on data confidentiality, integrity and availability and on service levels, identifying potential weaknesses in control measures and the corresponding corrective actions that should be taken.

*Go to Page 17...*

### BBC botnet investigation causes controversy

**T**he UK's BBC has been criticised by security vendors after paying cyber criminals for use of a botnet. During an investigation by technology programme BBC Click, reporters used licence payer money to buy control of infected computers from Ukrainian crooks.

The transaction, which happened in February, gave the reporter control of over 21 000 computers, which were then used to prove that the botnet was being controlled.

"I could have used them to spread spam and phishing emails to thousands

of other computers," said the reporter, Spencer Kelly, in a written article accompanying a televised documentary about the investigation. "I did not, of course. That would have been illegal."

However, Kelly conducted a 'low-power demo' that involved sending out spam mail using a 'slow' setting. "Even with our botnet set to 'slow', we managed to send out over 10 000 emails in a few hours," he added.

Some commentators believe that remotely controlling computers in this

## Contents

### News

- BBC botnet investigation causes controversy 1
- Anti-phishing organisation launches common reporting standard 2
- McAfee: Beware the spam of March 20
- 'Monroe doctrine' needed for cyberspace 20

### Features

#### Google hacking 101

Google provides penetration testers and hackers alike with a surprisingly powerful tool for discovering sites with poor security – and then attacking them. Steve Mansfield-Devine takes a look at how this powerful search engine can help people worm their way into your organisation. 4

#### Here's looking at you Kido

Some call it Conficker. Some call it Downadup. Everyone calls it a darn nuisance. Kaspersky's Vitaly Kamluk calls it Kido, and explains how this network worm works its dark magic. 6

#### In-session phishing and knowing your enemy

Just when you thought that people were getting wise to phishing, scammers have devised a technique that makes the process even more convincing - even to those who should know better. Ori, Eisen, founder of 41st Parameter, investigates. 8

#### Is your system pwned?

Pwning is probably the most feared slang-phrase in the security world. Gaining complete control of a piece of equipment gives a hacker unprecedented access to your network and files. Aditya K. Sood explains. 11

#### Creating risk management strategies for IT security

To properly secure your systems, you must understand the risks facing them. These will vary, depending on the type of organisation you're in, and the type of resources on the network. Steve Southern, director of Amethyst Risk Management, provides some pointers. 13

#### Security audits in mixed environments

Dario Forte explores how security audits work in the context of relationships with third party business partners. 17

### Regulars

- News in brief 3
- Calendar 20

#### Photocopying

Single photocopies of single articles may be made for personal use as allowed by national copyright laws. Permission of the publisher and payment of a fee is required for all other photocopying, including multiple or systematic copying, copying for advertising or promotional purposes, resale, and all forms of document delivery. Special rates are available for educational institutions that wish to make photocopies for non-profit educational classroom use.

**Editorial Office:**

Elsevier Ltd, The Boulevard, Langford Lane  
Kidlington, Oxford OX5 1GB, United Kingdom

**Programme Editor:** Steve Barrett

Tel: +44 (0)1865 843239

Fax: +44 (0)1865 853933

Email: s.barrett@elsevier.com

Web: www.networksecuritynewsletter.com

**Editor:** Danny Bradbury

Email: danny@itjournalist.com

**Senior Editor:** Sarah Gordon**International Editorial Advisory Board:**

Dario Forte, Edward Amoroso, AT&T Bell Laboratories;  
Fred Cohen, Fred Cohen & Associates; Jon David, The  
Fortress; Bill Hancock, Exodus Communications; Ken Lindup,  
Consultant at Cylink; Dennis Longley, Queensland University  
of Technology; Tim Myers, Novell; Tom Mulhall; Padget  
Petterson, Martin Marietta; Eugene Schultz, Hightower;  
Eugene Spafford, Purdue University; Winn Schwartau, InterPact

**Production Editor:**

Lin Lucas

**Subscription Information**

An annual subscription to Network Security includes 12  
printed issues and online access for up to 5 users.

**Prices:**

€1052 for all European countries and Iran

US\$1177 for all countries except Europe and Japan

¥139 600 for Japan

(Prices valid until 31 December 2009)

To subscribe send payment to the address above.

Tel: +44 (0)1865 843687/Fax: +44 (0)1865 834971

Email: commsales@elsevier.com,

or via www.networksecuritynewsletter.com

Subscriptions run for 12 months, from the date payment is  
received. Periodicals postage is paid at Rahway, NJ 07065,  
USA. Postmaster send all USA address corrections to: Network  
Security, 365 Blair Road, Avenel, NJ 07001, USA

Permissions may be sought directly from Elsevier Global Rights  
Department, PO Box 800, Oxford OX5 1DX, UK; phone: +44 1865  
843830, fax: +44 1865 853333, email: permissions@elsevier.com. You  
may also contact Global Rights directly through Elsevier's home page  
(www.elsevier.com), selecting first 'Support & contact', then 'Copyright  
& permission'. In the USA, users may clear permissions and make  
payments through the Copyright Clearance Center, Inc., 222 Rosewood  
Drive, Danvers, MA 01923, USA; phone: +1 978 750 8400, fax: +1 978  
750 4744, and in the UK through the Copyright Licensing Agency Rapid  
Clearance Service (CLARCS), 90 Tottenham Court Road, London W1P  
0LP, UK; tel: +44 (0)20 7631 5555; fax: +44 (0)20 7631 5500. Other  
countries may have a local reprographic rights agency for payments.

**Derivative Works**

Subscribers may reproduce tables of contents or prepare lists of arti-  
cles including abstracts for internal circulation within their institutions.  
Permission of the Publisher is required for resale or distribution outside  
the institution. Permission of the Publisher is required for all other  
derivative works, including compilations and translations.

**Electronic Storage or Usage**

Permission of the Publisher is required to store or use electronically  
any material contained in this journal, including any article or part of  
an article. Except as outlined above, no part of this publication may  
be reproduced, stored in a retrieval system or transmitted in any form  
or by any means, electronic, mechanical, photocopying, recording or  
otherwise, without prior written permission of the Publisher. Address  
permissions requests to: Elsevier Science Global Rights Department, at  
the mail, fax and email addresses noted above.

**Notice**

No responsibility is assumed by the Publisher for any injury and/or dam-  
age to persons or property as a matter of products liability, negligence  
or otherwise, or from any use or operation of any methods, products,  
instructions or ideas contained in the material herein. Because of  
rapid advances in the medical sciences, in particular, independent  
verification of diagnoses and drug dosages should be made. Although  
all advertising material is expected to conform to ethical (medical)  
standards, inclusion in this publication does not constitute a guarantee  
or endorsement of the quality or value of such product or of the claims  
made of it by its manufacturer.

02158

Printed by Mayfield Press (Oxford) Limited

way, even for test purposes, contravenes the Computer Misuse Act. Graham Cluley, senior technology consultant at antivirus company Sophos, was particularly scathing about the investigation.

"Sending spam from someone else's computer obviously gobbles up bandwidth and will use up system resources. Even if the BBC felt the impact would be minimal -- it doesn't make it right," he said. He also criticised a measure taken by the programme to warn the botnet victims whose computers it was controlling. The company had changed their desktop wallpaper to display a message from the programme.

"This is clearly an unauthorised modification of computer data, and is -- to my mind -- a breach of the Computer Misuse Act," Cluley warned. He was joined by other security vendors who were equally critical.

Struan Robertson, a technology lawyer with legal firm Pinsent Masons, agreed that unauthorised access had occurred, but said that the Corporation would be unlikely to face any punishment. "The maximum penalty for this offence is two years imprisonment. But it is very unlikely that any prosecution will follow because the BBC's actions probably caused no harm," he said. "On the contrary, it probably did prompt many people to improve their security."

Jacques Erasmus of Prevx, the anti-malware security company that worked with the BBC on the investigation, was defiant about the measures taken. "I get the feeling that the only people who really are objecting are security vendors," he retorted. "Doing things in the lab is all good and well, but for the real public, it doesn't have the same effect, in my eyes."

On its Twitter account, BBC Click said "We would not put out a show like this one without having taken legal advice."

## Anti-phishing organisation launches common reporting standard

The non-profit Anti-Phishing Working Group (APWG) has unveiled a common cyber-crime reporting format that it hopes will make it easier for private organisations and law enforcers to share informa-

tion. The protocol, based on an existing security incident reporting format, will be used to support a hosted collaboration system hosted by the Group.

The format is called the Extension to IODEF-Document Class for Reporting Phishing, Fraud, and Other Non-Network Layer Reports. It builds on the Incident Object Data Exchange Format created by the IETF, which was designed to let computer security incident response teams (CSIRTS) exchange information on security incidents.

APWG chair David Jevans said that the system could be used to identify trends across organisations that may otherwise have gone unnoticed.

"You might not notice something if you're just one bank, but if ten banks share this information then you will start to see these patterns," he said.

The reporting format will form the basis for the expanded APWG online reporting system, which Jevans says has been four years in the making, and which will be unveiled at the third Counter eCrimes Operation Summit (CeCOS) in Barcelona in May.

The APWG already operates a phishing URL repository that enables partners to share information at a single point. The expanded system will harbor information such as source IP addresses for malicious attacks, sites that are recruiting money mules, and domains that are being registered for malicious purposes. The system will also make it easier and quicker to persuade registrars to de-register domain names that are being used for malicious purposes, Jevans added.

The APWG is also working on a cyber crime reporting tool under its e-Crime Reporting and Incident Sharing Project (e-Crisp X) that will enable companies to convert proprietary cyber crime incident information into its new format.

While the APWG prepares its cybercrime reporting resource, Arbor networks has launched a new version of its ATLAS Internet monitoring system. The Active Threat Level and Analysis System takes data from over a hundred ISPs and uses it to analyse internet threats. New features include expanded Fingerprint Sharing Alliance participation, real-time

*Continued on page 20...*

## In brief

### Mac hacked

Independent security researcher Dino Dai Zovi demonstrated a memory-based attack on the Mac operating system at the SOURCE Boston security conference this month. OS X lacks proper memory corruption defence features, he said. He demonstrated an attack on the heap memory, which he said is executable. Attackers can execute 12 bytes of arbitrary code, which is enough to launch a malicious payload, he announced.

### Government search system launched

Simplex is targeting the public sector with a system that lets government departments search multiple disparate data sources.

### Wardialing gets VoIP makeover

Warvox 1.0 is a VoIP-based automated wardialing tool that lets researchers profile up to 1,000 lines per hour. It analyses call audio to look for modems, voicemail systems, and faxes. <http://warvox.org>

### White listing makes a comeback

Comodo has shipped an endpoint security management tool that uses 'default deny' protection. The system uses white listing technology that only allows certain files to be executed.

### Security vendors step up to training challenge

Microsoft has launched 2CENTRE, an initiative to try and standardise cyber security training among academic institutions in Europe. The initiative, which it is hoping the European Commission will support, enables both private sector and law enforcement representatives to learn anti-cyber crime techniques. McAfee is doing its own bit, granting \$55 000 to be Council of Europe to try and combat cyber crime with better training.

### Safe mode malware found

McAfee Avert Labs warns that malware has been found loading in Windows safe mode, making it extra difficult to remove. It works by adding itself under specific registry keys within the operating system.

### Trickier Conficker emerges

The Conficker worm continues to develop. Another strain of the malware has been found that generates 50 000 potential call-home domains every day. The original version generated just 250 per day. The worm chooses 500 of them for a daily rendezvous in a bid to make it stealthier than its predecessor. The development appears to have happened in response to the efforts of the Conficker Cabal, a collection of vendors including Microsoft, which has been registering domains in a bid to stop the command and control process.

### IBM launches endpoint security system

IBM ISS has launched Proventia Endpoint Secure Control (ESC). The system, which includes an IPS, firewall and network access control, device control, data encryption and security patch man-

agement, lets administrators deploy their own third party security tools and manage them from a central point. It shares data with IBM Tivoli's systems management software.

### Sunbelt launches PC cleaner

Sunbelt Software has launched a free command line utility designed to clean up malware infected systems. VIPRE PC Rescue makes it easy to wipe infections from a nearly inoperable computer thanks to its command line status, said the company. <http://bit.ly/13MmH5>

### Egress offers hosted rights management system

Egress Software has released Egress Switch, a hosted rights management that 'wraps' files sent from one person to another, and enables use policies to be set for them.

### New tokenless auth tool hits market

SecurEnvoy is offering version 5.0 of its SecurAccess tokenless authentication product. It lets users log in via a passcode sent to their mobile phone. This latest version includes multi-platform LDAP support, meaning existing databases of users, such as employee information already in corporate systems, can be used with no integration needed. Also included in the update is an SMS phone option.

### Geo-located malware attack surfaces

Sophos warns that scammers are using web sites customised to a victim's location in a malware delivery scam. Emails with purported links to a Reuters story about a dirty bomb explosion take victims to a web page with a fake news story. The story is tailored to the visitor's country and city. While they read the story, their browser is compromised by a drive-by attack.

### Password cracker updated

L0pht has announced a new version of its L0phtCrack password cracking software. <http://bit.ly/wBVP1>

### Firefox most flaw-ridden browser last year

According to a 2008 vulnerability report from Secunia, Firefox was the browser with the most security flaws in 2008. The open source browser had 115 bugs, compared to 32 in Safari, 31 in Internet Explorer, and 30 in Opera. That said, the Mozilla Foundation was faster than Microsoft when it came to patching the flaws.

### InDorse offers rights management suite

InDorse Technologies has launched a rights management system designed to discover and semi-automatically tag data with usage policies. Protect, the third product in its core suite, sits in front of the file server and applies the rules to anyone wanting to access files. It also embeds the security rules in the header of any file copied to a client machine.

### Tiscali web site vulnerable?

In what seems to be increasingly like shooting

fish in a barrel, a Romanian hacker site claims to have discovered an SQL injection vulnerability on Tiscali.co.uk's site. The same group also revealed a similar flaw on Kaspersky's site earlier in the year, and on BitDefender's Portuguese reseller's site. <http://bit.ly/Jrt8>

### SQL injections widespread in 2008

Tiscali and Kaspersky are the tip of the iceberg, according to Breach Security's Web Hacking Incidents Database (WHID) 2008 Annual Report. The document says that half a million web sites were hit by SQL injection attacks last year. 19% of these attacks were designed to steal personal information, while 16% of them planted malware on the sites to infect visitors' machines. <http://bit.ly/yTWC>

### Microsoft releases patch set

Microsoft released its monthly patch collection, including a critical kernel flaw that could allow for remote execution. Users viewing a maliciously crafted EMF or WMF image file could be hit, said its security bulletin. The flaw affects Windows Vista, including Service Pack 1, and also affects the core server profile for Windows Server 2008. However, the company failed to patch a zero-day Excel flaw that it had discovered late last month.

### Japanese software attacked

The Japanese Ichitaro word processor has been targeted by malware. A maliciously crafted file infects a machine with a generic dropper Trojan, says McAfee's Avert Labs.

### Data Breach Watch

750 **Twitter** accounts were hijacked to pump out spam tweets.

The **New York Police Department's Pension Fund** revealed that the personal records of 80 000 former and current workers had been stolen from a disaster recovery facility by an employee. The unencrypted media were found at his house, and he was arrested.

A janitor at the **East Tennessee Technology Park** in Oak Ridge, TN pleaded guilty to trying to sell information on producing highly enriched uranium to an undercover FBI agent.

Australian domain registrar **Bottle Domains** says that in 2007, an employee at a competing registrar took advantage of a software licensing agreement between the two companies to breach its system. An arrest has been made. While the company doesn't believe that any service has been compromised, it is advising users to update their passwords.

The **City of Muskogee** recently admitted that personal information on 4,500 utility customers had been accidentally put into the public domain. A Zip disk with the customers' details, which had been created in 2000, was handed in by a member of the public.

# Google hacking 101

Steve Mansfield-Devine

**If you're looking for weak security points in a website, forget NMAP, Nessus and all those tools of the pen-tester's trade. Your first stop should be something much more basic: Google.**



Steve Mansfield-Devine

The search engine's relentless spidering of sites is remarkably adept at discovering weaknesses, all of which are meticulously indexed. This creates a valuable resource for security specialists and hackers alike through the use of specially crafted search queries – the technique of Google hacking.

Before we look at the basics of Google hacking, it's worth considering how this technique turns the usual image of hacking on its head. By and large, hacking consists of a miscreant targeting a specific site, beavering away to discover its weak spots. And Google hacking is indeed useful as a way of footprinting and probing a specific site.

***"Go through the code and remove everything that identifies the software, including any HTML comments or meta tags"***

But the real danger it poses is bringing your site to a hacker's attention. A Google hacking query can turn up a list of all sites that suffer from the vulnerability the query is designed to reveal. If your site has this vulnerability, then Google will bring hackers directly to it. It is an automated way of broadcasting your weaknesses. Hackers will not only be drawn to it, but will arrive knowing in advance what vulnerabilities they will find.

So, for those charged with the security of a website, ensuring that your site is not among those turned up in a search query is very important.

## Google dorks

These search techniques were first made famous, and were documented by,

Johnny Long, owner of the 'Johnny I Hack Stuff' website which is now dead but still currently hosts the Google Hacking Database (GHDB).<sup>1</sup> He's also author of a two-volume book on Google hacking.<sup>2</sup>

The GHDB has been little updated since 2006 but still carries the most complete list of so-called 'Google Dorks' – the search terms used to discover vulnerabilities. These make extensive use of Google's special search operators – terms that refine or modify the search and the reason why Google is so effective at this task. For example, searching with:

```
allintext: admin user password restricted list
```

This means that Google will return searches only where the pages contain all of those words in the text. Similarly, the site: operator restricts the search to a specific site or domain – handy for testing your own website.

The GoogleGuide.com site has a useful quick reference sheet for these operators.<sup>3</sup>

For our purposes, the most important categories of Google dorks are: discovering vulnerable software, finding files and directories that shouldn't be visible, and exploiting error messages or system failures.

## Vulnerable software

Google hacking provides a number of basic footprinting methods to profile a website – server software, operating system and so on. But much of that information is more easily found through sites such as Netcraft.com. Where Google dorks really come into their own

is when the software you're running is known to have vulnerabilities.

Software often uses easily identifiable filenames that will turn up in URLs. For example, one Google dork from 2004 targeted the Comersus APS-based ecommerce package which had an XSS flaw in the file `comersus_message.asp`. This could be exploited with a specially crafted URL. To find sites running this package all a hacker had to do was type the following into Google:

```
inurl:comersus_message.asp
```

Software identifies itself in other ways, too. There's often a credit along the lines of 'Powered by...'. Worse, some packages even include the version number. The second that version is known to contain a flaw, hackers worldwide will scour the web for vulnerable sites.

These credit lines are typically part of default installations and many publicly available templates or themes. It's generally fairly easy to remove them, especially if you develop your own theme. Go through the code and remove everything that identifies the software, including any HTML comments or meta tags. But remember to check each time you upgrade the software that these lines haven't been reintroduced.

Software credits also find their way into `<title>` tags sometimes. And even when they don't say 'powered by...', the page title is often enough to identify your site – using Google's `intitle:` operator – as running on a vulnerable version of the software because the text is so specific to that page. There is little you can do about that other than ensure that your software is always up to date.

## Open directories

There is nothing a hacker loves more than an unprotected directory. If web server software receives a request that contains a directory name, rather than a specific file, it will look for a default 'index' file – called 'index.html' or any one of a number of other standard files depending on the server configuration. If it doesn't find one, it will helpfully present a list of files and sub-directories in that directory, with each filename clickable.

Web servers use standard terms in the page or title when they do this, so such open directories are easily found. Here's one way to find .txt, doc and .pdf files on the site www.example.com. The first section uses the negation modifier ('-') with the inurl: operator to tell the search to ignore .html, .htm and .php files:

```
-inurl:(htm|html|php) intitle:"index of"
+"last modified" +"parent directory"
+description +size +(txt|doc|pdf)
```

That will find examples across the web. Add "site:www.example.com" to search a specific site.

It's surprising how often such directories contain text files with configuration, even password, information. (Beware, however, if you experiment with this: the results generated by Google dorks aimed at password files often lead to honey traps.) Even if the directory contains only harmless files – images, for example – the fact that your site has an unprotected directory will draw hackers to it, who will have assumed that your security is shoddy. That's not good.

It helps an attacker map the topography of your system. Some of those sub-directories, for example, might contain files that you don't want people to know about (although keeping such files in a publicly accessible part of the directory tree is a bad idea to start with).

Google won't necessarily find such directories if they are not referenced anywhere in your website, but that hardly counts as protection.

This problem is very easily fixed. Always have an index file in every directory. A simple index.html or index.htm (depending on server settings) will do it.

It doesn't even have to contain anything – so long as the server has something to grab and serve up, it won't provide a directory listing. A sensible solution, though, is to have index.html contain a very basic web page, perhaps with a link to your home page.

## Sensitive scripts

Some of the files left publicly available are there by mistake. Bizarrely, others are deliberate. Webmasters often allow scripts to output logs. For instance, the following gives interesting information about a specific piece of bulletin board software (just click through any messages that pop up):

```
inurl:CrazyWWWBoard.cgi
intext:"detailed debugging information"
```

If you have administration software that reports on, perhaps, network performance, ask yourself if those reports need to be available online. If so, make the pages that contain the output of any scripts password-protected directory.

## Error messages

Hackers really hit paydirt when your site goes wrong. Error messages often contain useful data for the hacker. Not long ago, the *Register* reported on a website that displayed a huge amount of PHP information due to an error. Google, of course, duly indexed this. It's not unknown for some site developers to enable a debugging mode that displays the output of the phpinfo() function if there's a problem. That function prints out a vast amount of information useful to a hacker. To see some sites with this issue, try:

```
intitle:phpinfo "PHP Version"
```

Various kinds of software display standard (and thus searchable) messages when they hit a problem. For example, try searching with:

```
"mysql error with query"
```

These error messages may include database, table and field names – inval-

able for SQL injection attacks – and even user names. PHP, ASP and other scripting systems may produce errors that reveal directory structures, names of otherwise obscure script files and other useful detail.

## "The results generated by Google dorks aimed at password files often lead to honey traps"

Even if the admin has since fixed the problem, so that the error message is no longer displayed, the fact that you've found this site with a search means that the problem page, including the error message, is still in Google's cache. So, on the Google results page, you simply opt for the 'Cached' link.

Certain Google dorks will find default pages that might suggest a poorly installed or maintained site. Some of these will reveal interesting information, for example:

```
intitle:"Apache Status" "Apache Server Status for"
```

This can reveal data about virtual hosts, directory structure and files.

It's therefore wise to turn off error reporting for live sites – in the database, scripting language, CMS and any other software you're using. And to make sure that you have completed configuration for all installed software.

## Security through obscurity

What Google dorks teach us is that there is no security through obscurity on the web – simply because there is no obscurity. You might think that you're the only one that knows where the login page is for your CMS, or that a certain file is not linked from anywhere else and will not, therefore, be found by Google. But it's a mistake to rely on this.

Even when a Google dork doesn't reveal specific information, it can tell a hacker where to start looking. For example, there are dorks that reveal the login pages for administrators – pages that

may not be linked ordinarily from the public side of the site:

`inurl:/admin/login.asp`

## Tools

This is just a taste of what Google dorks can achieve. Helpfully, there are tools available to automate Google hacking. One of them is produced by Google itself: GoogleHacks.<sup>4</sup> It's somewhat basic, but script kiddies will love it.

The Cult of the Dead Cow group – notorious for the Back Orifice trojan – has released a Windows-only tool, Goolag.<sup>5</sup> This is more sophisticated. It comes with a database of Google Dorks, supplied in XML

format, so it's easily readable and amendable. You can also specify your own searches.

By automating groups of Google Dorks, Goolag is a useful first step in penetration testing of your own sites. But there's no real substitute for working through the Google Dorks yourself, given that you will have some idea of where weaknesses may lie.

## Countermeasures

We've already outlined some of the measures you can take to protect yourself. The best approach is to Google hack your own site, identify all those flaws that can be picked up by Google and fix them. Skilled hackers may still be able to use some of these tricks to survey your

site if they have already targeted it. But at least you won't be advertising your problems.

## References

1. J. Long: Google hacking database, accessed March 2009 <<http://johnny.ihackstuff.com/ghdb.php>>
2. E. Skoudis and A. van Eijkelenborg: Google hacking for penetration testers, Syngress, 2005.
3. N. Blachman: Google guide advanced operator reference, GoogleGuide.com, accessed March 2009 <[www.googleguide.com/print/adv\\_op\\_ref.pdf](http://www.googleguide.com/print/adv_op_ref.pdf)>
4. GoogleHacks, Google, 2008 <<http://code.google.com/p/googlehacks/>>
5. Goolag, Cult of the Dead Cow (cDc Communications), 2008 <[www.goolag.org/download.html](http://www.goolag.org/download.html)>

# Here's looking at you Kido

Vitaly Kamluk, senior security researcher at Kaspersky Lab

**Now notorious for reaching worldwide epidemic proportions, the Kido family (otherwise known as Conficker or Downadup) is a polymorphic network worm that spreads mainly by exploiting a critical vulnerability in the Microsoft Windows operating system. Not only has Kido led to the biggest epidemic for several years, but it implements a wide array of tricks designed to make it difficult to analyse and hard to remove from infected systems, making it one of the most dangerous current pieces of crimeware.**

The worm was first identified in November 2008. Like earlier well-known network worms, such as Sasser, Kido exploits a vulnerability for which Microsoft has already released a patch; this was the MS08-067 patch (also known as KB958644), released in October 2008.<sup>1</sup> On Tuesday 13 January 2009, Kaspersky raised the alert level for the Kido family to 'moderate', acknowledging the scale of the risk presented by the worm. The worm spread very quickly, in part due to the failure of many to install the Microsoft patch on to their machines and is easily able to infect a few hundred computers in a matter of minutes. Kaspersky Lab estimates that more than 10 million machines worldwide are infected with Kido.

To date the countries that have suffered the most at the hands of Kido have been those in which pirated versions of

Windows are quite common, such as China, Brazil and Russia. It is of course harder and indeed wholly inappropriate for pirated versions of Windows to be updated and patched. Also, some organisations simply do not use automatic updates for different reasons. For example it is my understanding that military organisations need time to verify all the code from third parties, even trusted ones like Microsoft.

Although there have been a few incidents where individuals have been affected by Kido, infections have predominantly been targeted at corporate IT networks including local councils, hospitals, small and large businesses and schools. One government department was reported by the BBC to have been struggling with an outbreak for two weeks at the beginning of this year.

## How Kido works

Kaspersky Lab has detected multiple variants of the Kido worm (NetWorm.Win32.Kido). It infects using the vulnerability identified and fixed by Microsoft in its MS08-067 patch (Vulnerability in Server Service Could Allow Remote Code Execution) and spreads via local networks and removable storage media, such as USB flash drives.

Once installed, the worm disables system restore, blocks access to security websites and tries to download additional files to infected machines. The worm generates 250 pseudo-random domain names each day and registers these names. Its control-and-command centre is taken from one of these, rather than using a specific, fixed IP address.

Kido spreads in three different ways:

- Using remote automatic infections with MS08-067, Net-Worm.Win32.Kido is able to infect several hundred computers within a couple of minutes.
- By making attempts to guess the remote password for Windows users accounts, then copying the malicious executable and scheduling it for running.

- Infecting removable storage media such as USB flash drives when plugged in to a USB port.

However, it is highly unlikely that the initial cause of the Kido outbreak can be attributed to one of these methods, as this type of propagation would not make it possible to reach the epidemic proportions that have been so widely reported in so many different countries. It would have been restricted to a 'local' problem of perhaps two or a maximum of three countries.

We suspect that the initial infection was accomplished by using another botnet. By spreading in this way Kido just amplified the infection and highly increased the number of infected machines. Let us now look more closely at the propagation behaviour of one of the most prolific variants of the Kido family.

## Net-Worm.Win32.Kido.bt

Net-Worm.Win32.Kido.bt is a worm variant (it is a PE DLL file of between 155k and 165k in size, packed using UPX) that spreads via local networks and removable storage media. During installation this worm copies its executable file to the Windows system directory. It then creates a registry key ([HKLM\SYSTEM\CurrentControlSet\Services\netsvcs]) to ensure it will be run each time Windows is launched on the victim's machine, as well as modifying the registry key value.

When infecting a machine, this particular worm launches an HTTP server on a random TCP port, which is then used to load the worm's executable file to other machines. The worm obtains the IP addresses of machines sitting on the same network as the victim machine and attacks them via a buffer overrun vulnerability in the Server service. The worm sends a specially crafted RPC (remote procedure call) request to remote machines, which causes a buffer overrun, which in turn launches code that downloads the worm file and launches and installs it on the new victim's machine.

In order to exploit the vulnerability described above, the worm attempts to connect to the Administrator account on the remote machine. The worm then uses a series of passwords to brute force the account.

```
C:\tools\kido>KidoKiller.exe -h
Net-Worm.Win32.Kido removing tool, Kaspersky Lab 2009
USAGE:
C:\tools\kido\KidoKiller.exe [-y] [-s] [-v] [-n] [-r] [-p <string>]
[--] [--version] [-h]

Where:
-y, --autofinish
    End program without pressing any key.
-s, --silent
    Runs program in silent mode
-v, --verbose
    Output every scanning object
-n, --network
    Scan remote drives
```

Figure 1: KidoKiller in action.

[Download KidoKiller from: <http://support.kaspersky.com/faq/?qid=208279973>]

## Spreading via removable storage media

The worm copies its executable and places a file in the root of each disc, this protects the worm, ensuring that the executable will run each time the user innocently opens the infected disc using Windows Explorer.

When launching, the worm injects its code into the address space of one of the svchost.exe system processes and it is this code that is responsible for the malicious payload of the worm. Once in place on the machine Kido disables Windows updates by blocking access to update sites, as well as access to many anti-virus, firewall, and other security software updates servers.

## Hard to find, even harder to remove

While Kido can be pigeon-holed as an 'old school' network worm, its success has drawn much media attention and it is a distinct possibility that we may be about to witness a resurgence of such malware attacks. Ask any of the organisations that have been grappling with Kido infections over the last month and they will tell you that despite its status as a piece of 'traditional' crimeware it can be very painful to get rid of, as it uses some highly sophisticated techniques to make it difficult to analyse, detect and remove from infected machines.

The worm uses a smart AUTORUN.INF file. When the file is viewed using an application such as Notepad, or another similar text editor, there is very little that is readable and it looks like

nonsense. This is a deliberate ploy as it is designed to conceal the method of infection. In fact, it is Unicode text, and Windows is able to process it correctly. The worm removes the nonsense and processes the command:

```
icon=%syStEmrOot%\sySTEM32\
shell32.dllshellExECUte=RuNdLL32.
EXE .ARECYCLER\5-3-42-2819952290-
8240758988-879315005-3665\jwgkvsvq.
vmx,ahaezdrn
```

RUNDLL32 (used in the command above) is used to load DLL files and Kido is (as I mentioned earlier) such a file. It has a VMX extension that is designed to provide further confusion. However RUNDLL32 doesn't care about such an extension and loads a DLL regardless. The syntax used is also designed to make anti-virus researchers, or the automated tools they use, assume that 'ahaezdrn' (specified at the end of the command string) is an exported function from the Kido DLL file. However, it exports no functions at all. This too is designed to confuse. In fact, RUNDLL32 loads the DLL and only after that does it look for the 'ahaezdrn' function. During the initialisation of DllMain, Kido infects the system and kills the hosting process of RUNDLL32 so as to prevent the popup error message you would normally see if you fail to specify a function correctly.

Kido tries to prevent analysis of its code by only executing with a secret keyword; this keyword is 'ahaezdrn'.

If the worm is loaded from the SYSTEM32 directory, it does not infect

the system but simply injects code into Explorer, unloads the DLL it was loaded from and locks this DLL from within the svchost system process. So no malicious DLL is loaded, but the svchost process protects the malicious DLL on the hard drive from being read or removed. On the one hand, this is a stealth measure, preventing the worm's activity from being revealed on the infected system. On the other hand, it makes removal more difficult.

Kido employs a further stealth technique. It propagates only 90% of the time; in 10% of cases, it remains silent.

The worm's executable is protected using an obfuscated cryptor, to make analysis of the code more difficult.

The worm spreads across the local network using its own HTTP server, to mimic normal activity of the machine. As a result, the worm is less likely to be noticed. In addition, it remains invisible to many firewalls.

When the Kido DLL is loaded, it is not possible to use the MS08-067 vulnerability to infect the machine again. This ensures that the worm owns the compromised machine by preventing infection from any other malicious program.

The worm does not use a specific address for its command-and-control server. Instead, every day there are 250 new domains from which it finds the command-and-control server. As a result, if one command-and-control server is closed, the attacker is able

to register new domains. Of course, there are countless domains available.

Kido uses a number of other tricks that make it difficult for virus researchers to capture the worm and analyse it. It also mimics the icon and title of an infected USB flash drive, to avoid arousing suspicion and to ensure it is loaded automatically.

## Prevention is better than cure

As in any area of IT, a security policy that is proactive will always be more effective than responding reactively to an infection. The following precautions will help to keep networks as safe as possible from a Kido attack:

- Ensure all users have the latest security updates for their computers, particularly <[www.microsoft.com/technet/security/Bulletin/MS08-067.msp](http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp)>.
- Ensure each computer has anti-virus installed and that it is up-to-date.
- Turn off Autorun for all removable drives.
- Make it an item of security policy that USB drives should not be used unless they are verified to be clean.

## Building a Kido botnet

There has been some concern voiced in the security industry regarding the

potential for machines infected with the Kido worm to be used as a part of botnet. Indeed the possibility of a union of network worms and botnets becoming normal practice is a worrying prospect. In order to prevent such a big internet disaster, experts from many companies have united on a non-commercial basis to join efforts in order to prevent this from happening.

Kaspersky Lab is participating in this project by helping different organisations to locate, check and block domains generated by Kido. It is a vitally important step to make sure no one controls a Kido botnet. After that the infected computers have to be divided and isolated/cured locally and this work is currently ongoing.

Similar to the network worm Sasser, as well as other viruses including Blaster, MyDoom and Sobig, a substantial bounty of \$250 000 has been offered by Microsoft for information that leads to the capture and conviction of the worm author/s.

Finally, if you are a victim of Kido, our free KidoKiller tool ([kidokiller.exe](http://kidokiller.exe)) can be used to clean infected machines.

## Reference

1. Microsoft Security Bulletin MS08-067, Microsoft, October 23 2008. <[www.microsoft.com/technet/security/Bulletin/MS08-067.msp](http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp)>

# In-session phishing and knowing your enemy

Ori Eisen, founder and chief innovation officer, 41st Parameter

**The proliferation of underground forums for trading stolen personal information is fuelling the automation of identity theft and the creation and distribution of crimeware. This commercialisation of fraud is driven by well-organised, powerful fraud rings, which have emerged to capitalise on the opportunity and thrive in the anonymity the online world provides.**

User credentials are extremely valuable, but not for the obvious reason. The underground market for stolen personal information reveals two diverging

strategies. One seeks to provide high-quality information for a premium price, while the other offers stolen personal information at little or no cost

as a 'freebie' incentive to license their crimeware

## The new threat environment

The last 12 months have witnessed a significant increase in ring-originated fraud. Today, fraud managers estimate ring activity accounts for over 50% of instances in certain types of fraud. The trend is further echoed by a number of high-visibility

reports, which have documented the rapid maturation of an underground economy dealing in stolen personal information.

The primary drivers behind this underground economy are in line with the two diverging strategies. These are the proliferation of clandestine forums for trading in stolen personal information, and the emergence of a community of developers, employed by organised fraud rings, specialising in crimeware.

***“The creation of an efficient marketplace for stolen personal information has enabled crime rings to specialise in specific phases of the fraud process and to monetise their activities even before any transaction takes place”***

Unlike earlier generations of crimeware, which were developed by individuals and circulated within limited networks, the new software is developed and financed by powerful and strategically motivated rings, designed for international distribution, and made available in an easy-to-deploy, SaaS (software-as-a-service) basis.

The creation of an efficient marketplace for stolen personal information has enabled crime rings to specialise in specific phases of the fraud process and to monetise their activities even before any transaction takes place. Their ability to successfully phish quality credentials allows them the confidence to offer them as valid usernames and passwords – or they will provide new credentials at no extra cost.

## In-session phishing

A recent tactic being perpetrated by these fraud rings called, ‘in-session phishing’, has emerged as one of the chief threats to breach secured online assets. These attacks use vulnerabilities in the Javascript engine found in most of the leading browsers, including Internet Explorer, Firefox and even Google’s Chrome.

Using a host website injected with malware, this parasite monitors for visitors with open online banking sessions or similar type protected asset sites, such

as brokerage or retirement planning sites. Using the Javascript vulnerability, the parasite can identify from which bank the victim has a session currently open by searching for specific sites pre-programmed into the malware’s own code. There are no limits to the volumes of URLs a website hosting the parasite can test from the victim’s machine. The malware asks: “Is my victim logged onto X bank’s website?”, and their browser replies either yes or no.

Once any site from the list is confirmed to be ‘in session’, a pop-up claiming to be from the bank issues a warning. Most warnings appear as time out messages, stating: “For security purposes your banking session has been terminated. To continue your session please re-enter your username and password here” – which is a link supplied by the fraudster.

Once a victim complies, clicks the link and enters his/her credentials, the damage has been done, the attack was successful and the game is over – right?

In most cases it is devastating for a victim whose credentials have been breached. In a matter of minutes, fraud rings quickly begin selling off this information or pillaging through the victim’s account. Since many financial institutions rely on simple cookies or tags to discern one device entering user credentials from another, and then count on fairly common – and sometimes easily answered, out of wallet – questions to validate a new device attempting access, this would be true.

***“KYE seeks to identify the common pattern behind multiple online activities, and assemble a full picture of the fraudster’s activities across multiple accounts”***

Robust device ID technology could enable financial institutions to render credential breaches using in-session or any other type of phishing attacks useless to the fraudster. A powerful device ID, along with credentials, enables financial institutions to render user IDs and passwords in the wrong hands powerless to do harm. Doing so not only eliminates

the fraud losses but also avoids countless customer support calls for victims and the risk of serious damage to the brand of the institutions allowing their customers to feel the impact of these attacks.

## Know your enemy

The new threat environment, including the tactic described above, demands a new strategic approach to fraud management. The term ‘know your enemy’ (KYE) describes fraud management that departs from traditional approaches by focusing on the fraudster rather than the transaction.

Traditionally, fraud management has sought to profile the behaviour of true account holders and determine the reasonableness of an observed transaction for that customer. In contrast, KYE seeks to identify the common pattern behind multiple online activities, and assemble a full picture of the fraudster’s activities across multiple accounts, regardless of the credentials presented.

This approach provides unique benefits, including:

- High efficacy in situations where no prior customer history is available (e.g. new account opening).
- Early detection of account take over, and fraud staging activities (before any transactions have taken place).
- Rapid containment of scripted attacks using the first confirmed fraud to link to all others from the same ring.
- A complement to behaviour-based fraud management systems. As fraudsters improve their account surveillance techniques, their fraudulent transactions are more likely to align with the true account holder’s behavioural profile

The key lies in understanding what a suspicious or fraudulent attempt looks like upon log-in, versus a real customer’s session. For example, if you know that a legitimate customer almost always uses a device configured for local London time and the language for the device used is English, you would not provide unchallenged access to this account from a machine showing China as its country of

origin and having a default language set to Mandarin.

Further strengthening against future attacks, placing the device fingerprints gleaned from all known previous fraudulent attempts into a negative list effectively blocks the devices with a history of fraud from ever gaining access to another user account.

The benefits of adopting a ring-centric approach and the power of KYE techniques are well illustrated by a recent investigation by the fraud-management team of a large financial institution. The investigation was initiated when the team was presented with a counterfeit cheque. Using KYE tactics, the team found counterfeit cheques from 45 other accounts. Noting all of the accounts had large balances, the team suspected that the fraudsters conducted some earlier account surveillance before selecting these particular accounts.

Leveraging their KYE capabilities, the team uncovered more than 1500 additional accounts whose credentials had been compromised. Using KYE techniques to link the ring's activities, the team was able to reconstruct the attack despite frequent changes of IP addresses and deletion of cookies and other tags.

In mentioning fraudsters changing tags to avoid detection, a short discussion on the limitation of tags for detecting returning fraudsters is in order. While customers do not actively attempt to obscure their identity, fraudsters take serious measures to stay anonymous. They will either avoid being tagged, by turning off cookies, or uninstalling Flash, or use a virtual machine that will be rolled back after the session to erase any potential tags placed on it.

## Lessons from early adopters

A significant body of knowledge has been

accumulated from early adopter fraud teams in their operational use of KYE approaches. These fraud management teams, including several top US retail banks and card issuers, deployed KYE tactics to monitor a broad range of online activities including, applications for credit cards, opening of new deposit accounts, maintenance activities and payments.

Without exception, the teams reported significant finds within the first 30 days of implementation. Depending on the area being monitored, loss prevention lifts ranged from \$500 000 per month to \$1.5 million per month per area.

## Account openings

Early adopters of the KYE strategy have detected a significant increase in fraudulent new account openings. KYE techniques have proven particularly useful in detecting rings who apply under multiple identities. One fraud unit has seen an increase of over 300% in the number of fraudulent account opening attempts.

By adding covert controls, which enable the fraud investigators to link online logins to their common originating ring, fraud teams report better visibility into early-stage account take-over activities. This has led to better understanding of the fraudsters' modus operandi.

***"By adding covert controls, which enable the fraud investigators to link online logins to their common originating ring, fraud teams report better visibility into early-stage account take-over activities"***

One bank, for example, was able to reconstruct scams involving fraudulent account openings, account take-over activities and fraudulent enrolment in electronic payment services.

There are also cases where the same fraud origins are attacking multiple financial institutions.

## Increased automation

Forums which distribute stolen personal information as a freebie to drive crime-ware sales will likely focus on lowering the cost of obtaining stolen information through new techniques like in-session phishing. Fraud teams should expect to see increased automation and scripted attacks coming from these rings, and should implement rapid containment procedures to avoid being overwhelmed.

Since the capture of data is always the most costly component of any data application, there exists an ongoing effort to extract more value from data assets. Expect the same to happen with stolen personal information. New crime-ware and scams are being developed with more diverse exploitation and shorter payoff times between account compromise and the ensuing fraud attack. These trends are likely to complicate fraud operations, encouraging better KYE processes and intelligence sharing.

The accumulation of large datasets of victim information is likely to prompt data mining and more targeted victim datasets. These will likely be paired with customised crimeware designed for particular population segments. Scams addressing treasury services units, or crimeware designed for browsers used in specific geographies, are early examples of this trend.

## Connecting online and offline

Fraud managers in the retail banking space report significant success in connecting online activity to offline fraud. Although the link between online cheque viewing and offline cheque fraud was always suspected, after implement-



## A SUBSCRIPTION INCLUDES:

- 12 printed issues
- Online access for 5 users
- A four-year archive of back issues
- Free delivery

[www.networksecuritynewsletter.com](http://www.networksecuritynewsletter.com)

ing a KYE approach, one fraud team produced multiple examples of 'smoking guns', linking the specific online session in which the cheque image was viewed to the counterfeit cheque.

## Link analysis

Link analysis is another instance where lessons can be learned. This is where fraud management teams reported significant lift from the ability to extend the impact of each confirmed case of fraud by linking it to other activities from the same ring. Regardless of how the initial fraud case was identified (perhaps spotted by a fraud detection system or following a customer complaint), the unit was able to find additional fraud simply by tracking them back to the same ring.

## The security trinity – three critical questions

Three primary questions must be addressed by the risk manager when a user attempts to log in, view and potentially transact online. First, should the site allow the user to log in to the account (authentication)? Second, should the site monitor if one device is accessing multiple user accounts even without transacting (account surveillance)? Finally, should the site allow the transaction(s) to execute and money to leave the account (transaction risk monitoring)?

The first question lends itself to a real-time check. The user is either authenticated with a simple yes or no answer. The second question relates to transaction authorisation and should not be answered in real-time or during the session but it can, and should be determined post-session. This question should be answered probabilistically, and if necessary, prompt human intervention for final verification.

The third question reveals if a perpetrator is lurking and waiting to see when accounts have high balances, or alternatively, if they are gleaning sensitive customer information from online document images to commit offline fraud such as cheque counterfeit or siphoning accounts. For that reason it is critical to mask sensitive customer and account data in addition to quickly detecting and containing such attacks.

Viewed collectively, all of these developments should prompt fraud management teams to re-evaluate their operations. 41st Parameter recommends that teams avoid over-reliance on single indicators of fraud (such as IP address) or behavioural transaction monitoring, and implement command-and-control processes which can respond to automated attacks, without overwhelming the team or demanding excessive manual reviews.

## Multi-layered approach

A multi-layered approach to data security is by far the most effective

strategy to combat fraud. If a company cannot maintain the integrity of the data that it has demanded from its customers, regardless of what channel it collects it from, then it is failing to meet a requisite level of corporate responsibility.

Fraudsters commonly take the easiest route to the information they need, and by adding more new layers to the system at regular intervals, organisations can combat fraud in a similar way to changing the rules of the existing network – making life far more difficult for anyone trying to infiltrate the system.

## About the author

*Prior to founding 41st Parameter, Ori Eisen served as the worldwide fraud director for American Express focusing on internet, mail order/telephone order and counterfeit fraud. During his tenure with American Express, Mr Eisen championed the project to enhance the American Express authorisation request to include internet specific parameters.*

*Prior to American Express, Mr Eisen was the director of fraud prevention for VeriSign/Network Solutions. By developing new and innovative technologies, he reduced fraud losses by over 85% in just three months.*

*Mr Eisen holds a Bachelor of Science degree in business administration from Montclair State University.*

# Is your system pwned?

Aditya K Sood, founder, SecNiche Security, and independent security researcher

**What is the relationship between humans, technology, and fraud? They are all linked together in a triangle. Most monetary transactions today are carried out using digital technologies, most frauds are monetary, and all frauds are perpetrated by people. As fraud prevention experts, we try to break the triangle – to ensure that people don't interact with technology to create fraudulent situations.**

## Elements of system pwning

The 'pwning' (a hacker term for owning or controlling) of computer systems does not depend on a single factor. An attack exploits not only information about the

system itself, but information about the environment in which the system operates. Accessing such information often requires interaction with people, meaning that social engineering plays a decisive role.

The truly adept attacker will be well-versed in a variety of techniques

to obtain this information, including shoulder surfing and dumpster diving. They will usually use different techniques in conjunction with each other to get the information that they need by exploiting human weaknesses.



Aditya K Sood

To pwn a system, an attacker works to discover the appropriate target, and will then build up an understanding of the relative impact of other subsystems on it. There are number of factors that constitute the attack occurring on the system. The system is comprised of the root software, and the applications running on it. There is always an interface between the two, and that interface is always prone to exploitation. The system-level vulnerabilities are different from the vulnerabilities that persist in the application. The bug exploited in the context of the system-level software results in full compromise at the root level. So, we need to think about the technology at both levels, keeping in mind the attack pattern that the attackers follow to pwn the machine.

## System-level exploits

System-level exploits have multiple variants. Attackers could use a straightforward denial of service, system compromise, or the subversion of systems using a rootkit. It adheres to the pattern of exploitation on which functionality depends, and is manipulated in to complete the malicious operations. It depends a lot on the psychology of hackers to choose the type of technology they want to exploit.

In many cases, attackers like to do service degradation by launching denial of service attacks with larger bots on companies' infrastructure. The technology has shifted its step towards more advanced techniques like rootkits, and virtualisation. Once the system is compromised, attackers like to install rootkits. They are highly advanced stealth malware that performs a lot of functions on victims' computers, from keylogging to system file infection.

The efficiency of rootkits lies in their ability to hide processes. A user will not be able to detect the rootkit process, as it is hidden and cannot even be traced through task manager. Rootkits are applicable to both Windows and Unix/Linux platforms, making them useful for attackers on a large scale.

Backdoors and rootkits are different sides of a same coin. For banking systems, capturing keystrokes from

victims' machine is the target. Usually we have seen that once the rookit captures the keystrokes, they are self-sustained enough to mail that file directly from the victim's computer to the attacker's machine, or to a third party target controlled by the attacker. The client side software used to connect to a server for performing these operations are also used to infect user systems by downloading malicious files or executing commands through linked files.

Privilege escalation is also one of the important exploitation vectors once a system with low-level privileges is compromised. The attacker exploits the process space or system calls to escalate privileges for executing administrative actions. In a system compromise, this involves gaining control at the kernel level.

## Remote payloads

With existing vulnerabilities, it is sometimes possible to crash the critical processes in the system by sending the payload remotely. Mainly this is an approach followed by the attackers to disrupt the normal functioning of organisations during production hours.

For example, an organisation may need large scale database servers running Oracle as their backend. Due to the cost issue of upgrading to newer versions of the Oracle database, the same older version remains in use. The Oracle works on the Transport Network Substrate, which is a technology used in centralised Oracle environments to provide client-level access to the Oracle database. The attackers shut down this service remotely due to presence of a vulnerability in older versions of Oracle 9. It is an outcome of both vulnerability and misconfiguration, and the impact is high, as the business is hampered due to downtime in production hours.

The main goal of such attacks is to completely marginalise the network and gain root authority over the system. It impacts the system more than indirect frauds and crimes by breaking the system itself. These types of attacks are summed up as system pwning. It can result not only in downtime

on production servers, but can also adversely impact the business by giving the attacker control over the fundamentals of your computing infrastructure. If the attackers are really notorious and believe in complete devastation of systems, then the attack can end with the blue screen of death, or root-level segmentation fault. The low-level crash happens as a result of the rogue action performed in the kernel address space attacking kernel drivers or system calls. Again the thinking process plays a part because the motive of an attacker is to dismantle the system completely.

## Tactically exploiting applications

With the advent of new anti-exploitation techniques, system-level compromises are getting lower. The trend of exploitation and frauds has moved towards the applications running on them, and also to the highest level of the stack – the user – who can be exploited using social engineering and human error.

Let's take banking fraud as an example. The bank will have a back-end database that stores a plethora of information regarding customer records. Banking web sites are typically based on a three-tier structure. The user interface provides a simple means for customers to execute a transaction online. With many banking web sites vulnerable to SQL injections, it's theoretically possible to inject parameters to help attackers understand the application and control the back-end system. They could create false users in the system that could access the web site directly. They don't need to deface the web site. Instead, they need to just trigger actions in a stealthy way.

## Banking on security

Let's consider the ATM of the same bank from a social engineering perspective. Usually, the ATM has a dump bin attached. When a customer completes a transaction, the account slip is dumped into the bin. This can carry grave implications. Account slips can carry a lot of information that is useful for hackers to enhance the level of fraud. This data can

be folded into a wider set of information compiled by the attacker using the different techniques at their disposal, which can eventually be used as the basis for fraudulent activity.

Another means of committing electronic fraud is traffic redirection. Traffic can be redirected from a legitimate web site to an attacker-controlled site with the same look and feel as the original site. The user unwittingly provides their credentials to the fake site. Chinese hackers performed this type of attack a couple of years ago, purchasing domains containing the same name as the target bank and replicating the target bank's markup. They would then place online advertisements that attracted users to the fake website.

The biggest threat to commercial web sites is cross-site scripting (XSS) and cross-site request forgery (CSRF). If a person is in an active session on a commercial web site, an attacker can send a

malicious link inside an email. The link serves an HTTP request to the back end, and the money is transferred from one account to another. The most dangerous part is that the user does not know what is happening. This is very common in phishing emails and identity spoofing attacks. Instead of eradicating all the vulnerabilities, our strategy should be to create efficient filters to stop these spams coming into our mail boxes.

Computer frauds and crimes are intrinsic components of a modern security matrix that is so complex that it is difficult to traverse in one flow. Technology alone cannot protect us from exploitation, but must be part of a broader working strategy for security.

### About the author

*Aditya K. Sood (aka OknOck) is an independent security researcher and founder of SecNiche Security, and has been working*

*in the IT security field for six years. He writes regularly for the Hakin9 group and Elsevier journals. His research has been featured in Usenix; login magazine. His work has been quoted on sites including Zdnet, and Infosecnews, and internet-news etc portals He holds a BE and MS in Cyber Law and Information Security from the Indian Institute of Information Technology (IIIT-A). He had already spoken at conferences like EuSecWest, XCON, Xkungfoo, OWASP, CERT-IN etc.*

*His other projects include Mlabs, CERA and TrioSec. He has written number of security papers released at packetstorm security, Linux security, infosecwriters, Xssed portal etc. He has also given number of advisories to forefront companies.*

*At present he is working as an IT Advisor in KPMG IT Advisory Services. [www.secniche.org](http://www.secniche.org) <http://zeroknock.blogspot.com>*

# Creating risk management strategies for IT security

Steve Southern, director, Amethyst Risk Management

**Creating risk management strategies for IT security has different connotations for different people. It depends, for example, on whether you're in the public or private sectors, and which part of those sectors you operate within, such as financial, retail, and production.**

To properly address this subject we need to outline what risk management means, and decide upon how we define IT security. Does the latter relate solely to IT systems? Are we concerned with the information processed and stored by these systems, or is it a combination of both? It is also necessary to compare and contrast the approach to risk management within the public and private sectors, as there are key differences, not only in approach but also in the methodologies used for assessing risk and implementing strategies. As we can illustrate, these differences are a consequence of external factors and

goals; conversely we can also highlight aspects that are common to both.

## What is risk management and what do we understand by IT security?

The concept of risk management is now fairly universally understood, having been in widespread use for a number of years. It is applied in all aspects of business, including planning and project risk management, health and safety, and finance. It is also a very common term amongst those concerned with IT security.

A generic definition of risk management is the assessment and mitigation of potential issues that are a threat to a business, whatever their source or origin. IT security may not be the best term or concept when considering risk management strategies, as it can be misinterpreted to be concerned only with the security of the systems, excluding the data they store and process.

In both the public and private sectors, a more widely recognised term approach is information security or information assurance. By inference, securing the information also entails protecting and assessing the risks to the IT infrastructure that supports, processes and stores that information. Information assurance relates to the confidentiality, integrity and availability of the information, the IT system, and the service it provides. Information assurance, or IA, is therefore the term used in place of IT security in the remainder of the article.

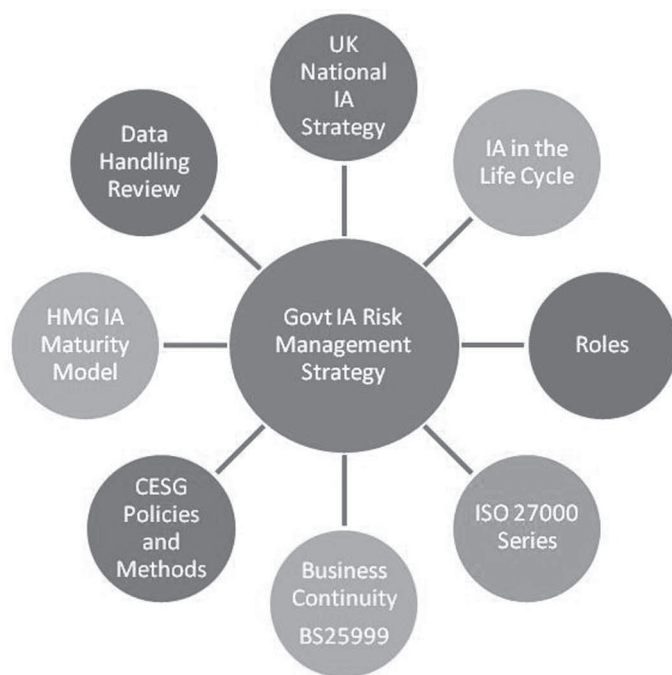


Figure 1: IA in the public sector.

## Risk management strategies for IA in the public sector

The perception of and appetite for risk within the public sector is the subject of widespread debate, consultation and change. Most recently for example, the report by Sir David Omand considers implications of the National Security Strategy for the UK Intelligence Community.<sup>1</sup>

***"IT security may not be the best term or concept when considering risk management strategies, as it can be misinterpreted to be concerned only with the security of the systems"***

At the heart of this debate is the need to balance conflicting and legitimate concerns from fundamentally different perspectives. On the one hand, we have the need to gather and analyse information as a normal function of Government, and on the other, to properly protect that information in order to maintain public confidence and support. At the simplest level, risk is a product of threat and vulnerability, and threats to public sector assets

and services are also changing more rapidly. Against this backdrop, risk management strategies are nevertheless very clearly defined within the public sector, and apply not only to central Government departments such as the Home Office, Ministry of Defence, and Foreign & Commonwealth office, but also to private sector companies that provide services to those departments. While the approach might be very prescriptive and, at times, quite mechanistic and even bureaucratic, it is clearly defined and does enable a common set of standards and criteria to be implemented. Risk management for IA can be viewed as a cyclical process, and Figure 1 can be used to assess how it is implemented within the public sector.

The overall approach by the Government to risk management within information assurance is driven by the National Information Assurance Strategy.<sup>2</sup> This aims to meet the transformational government agenda of better public services through use of IT, protection of those systems and information, and to enhance the economic well being of the public and businesses.

The strategy identifies three strategic outcomes. Firstly, the Government is better able to deliver public services

through the appropriate use of ICT. Second, the UK's national security is strengthened by protecting information and information systems at risk of compromise. Finally, the UK's economic and social well being is enhanced as government, businesses and citizens realise the full benefits of ICT.

## Implementation

The implementation of information assurance within IT development projects is clearly outlined in Government policies from the national technical authority for information assurance, the Communications Electronics Security Group (CESG). Its Information Security Standard Number 2 (IS2) clearly defines when risk assessments (including penetration tests), should be undertaken, the policies and mechanisms for risk assessment, the implementation of protective measures, (such as authentication processes, firewalls and anti-virus software), and the boundaries of responsibility. These include senior information risk owner (SIRO), senior risk owner (SRO), and information asset owner (IAO). The bottom line is that a system cannot go live unless the risks have been assessed and managed to a level commensurate with Government guidelines.

The Accreditor, a role that is not widely found outside Government, determines whether the level of risk is acceptable for each system. Where there are risks outside acceptable limits, then the risk acceptance decision is elevated to the department's SIRO.

The Government also embraces various national and international standards in its approach to risk management within information assurance, primarily the ISO 27000 series, and BS 25999. This may have been driven by the increased outsourcing of services and support to the private sector, where such standards are increasingly being adopted. By linking to these standards the Government has made it easier for the private sector to meet the Government's risk management requirements.

The risk to IT systems and information within the public sector is determined by specific methodologies. The mitigation of those risks is also largely determined through the use of Government-approved products, and although individual departments may have their own risk management methodologies and risk appetites, these are still within, and derived from, the policies produced by CESG.

***“Once the risk level is determined, countermeasures can be identified, if required, to reduce it to a level acceptable to the accreditator”***

Creating a risk management strategy is therefore quite a clearly defined process. A risk assessment and initial risk treatment are determined using the CESG Information Security Standard Number 1 (IS1). This details how the risks to the system are determined by identifying the threat sources such as foreign intelligence services, hostile media, or organised crime, their ‘agents’ e.g. bystanders, bribed users, or hackers, and the critical assets, typically including servers, networks, user communities and data.

Once the risk level is determined, using a series of algorithms for motivation and capability, countermeasures can be identified, if required, to reduce it to a level acceptable to the accreditator. Again, many of these ‘baseline’ countermeasures are pre-determined depending upon the protective marking and type of data being processed by the system. This is known as risk treatment.

The IS1 standard also clearly outlines the level of assurance that must be provided by procedural, physical and, most importantly, technological countermeasures. It includes assurance that can be derived from ISO 27001 certification. However, additional measures are often required and CESG has evaluated and certified a number of products, at the request of and investment by the product vendor. These are:

- CESG Assured Products (CAPS), which predominantly relate to



Figure 2: A private sector approach.

- encryption, data erasure and access controls.
- Operating systems and a sundry of other utilities that are assessed according to a set of Common Criteria (CC) which identifies a level of assurance and security functionality.
- The CESG Claims Tested Mark (CCTM), appropriate for products that will typically be deployed in local government or similar environments.
- The mitigation of the identified risks is generally achieved by use of CAPS, CC and/or CCTM products/systems.

So there is much policy and guidance regarding the application of risk management strategies to information assurance within the public sector, and some of the methodologies are quite prescriptive. The maturity of the risk management process within a project or department can also be assessed as part of an on-going risk management process. This is achieved via the CESG Information Assurance Maturity Model.<sup>3</sup> This has five levels of maturity, (level one being the lowest and five the optimum). They are used to assess a system or department against five criteria: leadership and governance, training,

education and awareness, information risk management; through-life IA, and assured information sharing and compliance.

More recently, there has been a major focus on the protection of personal data, which now forms a crucial part of any risk management strategy. This arose due to the highly publicised data losses by HMRC and the MOD and the subsequent inquiries and reports, most notably the Data Handling Review, often referred to as the Hannigan report. The effects have included a requirement for all departments to review their data handling processes, greater use of encryption on all media, and the need for a forensic readiness policy to aid any investigation into security breaches or data loss.

## Risk management strategies for IA in the private sector

It is true to observe that the means to create risk management strategies in the private sector is not nearly so clearly defined or prescriptive. There are a number of reasons for this, including the difficulty in agreeing mutually

acceptable methodologies and goals for different businesses, and also the wide variety of external IT compliance requirements such as Sarbanes-Oxley and the Payment Card Industry (PCI) Data Security Standard that affects financial institutions such as American Express and Visa.

A single strategy or methodology, where so many variables exist, is not achievable. However, a high level strategy can be applied, using risk management of information assurance as the central focus along similar lines to that applied in the public sector. Figure 2 illustrates the initial approach that Amethyst uses in the private sector to ensure that all of the main elements are assessed, and to gauge what is, or is not, applicable.

There are strands common to both public and private sectors, especially in the reliance upon national and international standards. Both sectors must also address legislative compliance in areas such as data protection and freedom of information, but for the private sector there are a plethora of additional IT compliance requirements that may or may not apply.

Best practices, such as ITIL for IT Service Management, are useful for addressing and minimising risks by having good practices, but the identification of which legal requirements are applicable is a potential minefield. This makes deciding upon a risk assessment, treatment and an overarching management process more complex than within government.

***“There are strands common to both public and private sectors, especially in the reliance upon national and international standards”***

Compliance is a major challenge in the private sector, requiring specialist resource. Some legislation can be quite obscure, such as the Senate Bill 1386 from California. At first sight, this would not appear to affect UK or European companies. However, the Bill is related to personal data about California residents, and if a company

holds any data on one of its employees that is resident in California, then it applies. This may be an extreme example but it does illustrate how complex the issue of applicable legislation can be. This has a knock on effect to risk management, as it is necessary to identify what is applicable or important at the beginning of the process.

However, all is not doom and gloom, as a clear risk management strategy can be applied, and it does not matter to any great extent which methodology is used. The principles are the same: confirmation of the business aim, identification of assets, establishing of threats, vulnerabilities and risks. The appropriate risk treatment can then be defined.

Once these have been determined, using any one of a number of risk analysis tools that are available, (provided that it assesses the likelihood and impact to determine a risk level), the results can be reviewed. Using ISO 27001 as the basis for a risk management policy makes sense, as it has a set framework that is internationally recognised, and against which formal certification is an option. Specific technical countermeasures such as whether to have two or three anti-virus software programmes, the type of firewall to deploy, and whether items such as an IDS are required will be based on the risk analysis, legal and regulatory requirements, and ultimately the risk appetite of the company.

## Conclusions

Within the public sector, policies and methodologies for risk assessment, treatment and management are very mature. Although they may appear somewhat prescriptive, there are advantages in having one approach across the whole sector. For example, it enables the interconnection of systems to be better assessed from a risk perspective.

However, within the private sector things are not anywhere near as clear-cut. Standards such as ISO 27001 and BS 25999 enable businesses to produce risk management policies

and business continuity plans, but the actual risk assessment and treatment are not centred on a single common policy or methodology.

It is down to individual organisations and businesses to decide upon which risk assessment method they wish to use before determining their risk management strategy. This is further complicated, or even dictated, by other compliance requirements such as the Data Protection Act and Sarbanes-Oxley legislation.

***“It is down to individual businesses to decide which risk assessment method they wish to use”***

Risk management strategies will remain an interesting conundrum in both sectors. The government approach will be driven to some extent by ‘security incidents’ and the perceived threats to the data and systems; while the private sector’s approach will largely be dictated by the business area and the applicable legislation and compliance requirements. These are likely to become more and more pertinent as CEOs and companies are held more and more accountable for their business’s approach to risk and, in particular, the information they hold and use.

It would appear that there is no single risk management strategy that can be used for information assurance, or IT security.

## References

1. The National Security Strategy: Implications for the UK Intelligence Community, Institute for Public Policy Research February 2009.
2. A National Information Assurance Strategy, Central Sponsor for Information Assurance, June 2007. <[www.cabinetoffice.gov.uk/csia/national\\_ia\\_strategy.aspx](http://www.cabinetoffice.gov.uk/csia/national_ia_strategy.aspx)>
3. Information Assurance Maturity Model and Assessment Framework, CESG, February 2009. <[www.cesg.gov.uk/products\\_services/iacs/iamm/media/iamm-assessment-framework\\_v2.pdf](http://www.cesg.gov.uk/products_services/iacs/iamm/media/iamm-assessment-framework_v2.pdf)>

# Security audits in mixed environments

Dario Forte, CFE, CISM, CEO and founder, DFLabs Italy

Laws in various countries require multi-level audits, especially for information systems managed wholly or partially via service contract with outsourcers. The documentation describing the logical security controls and methodology for protecting data integrity in the context of such services comprises a series of annexes to the service contracts, as well as a security manual which is usually necessary for setting forth policies and procedures. Both company and outsourcer personnel must be assigned authorisation profiles that are appropriate to their roles in the provision of service.

Making reference to best practices and international standards, this article examines the assignment and control procedures for outsourcer authorisation profiles, assessing their potential impact on data confidentiality, integrity and availability and on service levels, identifying potential weaknesses in control measures and the corresponding corrective actions that should be taken.

## Scope of work

Reference is made to the following management phases during this audit:

- Security governance.
- Configuration management.
- Incident and anomaly management.
- Data management.
- Operations management.

Accordingly, analysis focuses mainly on the following aspects:

- Alignment of information systems with legal requisites.
- The existence and dissemination of security policies.
- Adequacy of the process for issuing and managing authorisation credentials.
- System and application access control.
- Network access control.
- Existence and adequacy of access monitoring systems.
- Protection actions implemented by the outsourcer regarding its clients.

## Risks analysed

We then move on to analyse organisational and operational risks as classified on the basis of the model adopted in the auditing standards.

Organisational risks derive from:

- Inadequacy of information resources.
- The organisational model implemented by the outsourcer to manage the service.

Operational risks relate to:

- System malfunctions or anomalies.
- Potentials for insider or outsider fraud.
- Inadequacy of customer, product or business practices management.

## Audit methodology

Audits involve document review, system testing and interviews with company personnel involved in information storage, processing or transmission. Outsourcer personnel are also consulted regarding certain specific themes.

***“Both company and outsourcer personnel must be assigned authorisation profiles that are appropriate to their roles in the provision of service”***

More specifically, the audit comprises several components. It requires a critical analysis of security manuals (where present)



Dario Forte

regarding management of operational relations between client and outsourcer, and management of the security of data processing environments by the outsourcer. These contents (guidelines, rules, policies, procedures, etc.) are generally organised as collected documentation or manuals.

Interviews with company personnel are also necessary as a means of gaining information and insight regarding specific operational aspects of security management.

Finally, the audit requires the development and administration of tests of technical and procedural aspects. These tests are selected on the basis of the results of the above two steps. In a financial environment, for example, the tests cover all three operating environments (mainframe, midrange and desktop). Their general objective includes the verification of the methods used to implement the logical security measures described in the manuals (where such exist).

## Assessment of internal control systems

Relations with outsourcers involved in the operation of information systems and information system support infrastructure are generally formalised in a specific and detailed contract between the client and the outsourcer. They specify that all actions necessary for the proper operation and maintenance of the client's information processing resources are to be carried out by the outsourcer's own technical personnel.

The information processing resources included in this type of service generally comprise:

- Mainframes.
- Midrange processors (UNIX servers and Microsoft Windows servers).
- Desktop devices (user workstations with Microsoft Windows or other client OS).
- Devices and infrastructure for managing connections and interaction between information processing resources.

The services provided by the outsourcer generally involve one or more of the following:

- System management to ensure the proper function of information processing resources and operation and maintenance of associated system software and utilities.
- Database system management to ensure the proper performance of software associated with database use.
- Operations management to ensure that data processing in the various environments is carried out correctly. This service also generally includes providing responses to queries from operators.
- Network management to ensure the proper operation of geographical network data transmission systems for client inter-branch communications. This generally involves physical placement of processing equipment at outsourcer facilities.

Given the complexity and critical nature of the activities and operations that may be delegated to the outsourcer, the contract generally spells out (in addition to service and payment terms) the principles and practices for physical and logical security to which the outsourcer must adhere in providing services.

These requisites apply to the various information processing environments used by the client and establish the terms of a reciprocal and binding commitment for managing the physical and logical security of these environments, including the drafting and updating of appropriate security manuals.

## Logical security audit of outsourcer access to client systems

Given the high level of technical skills generally possessed by outsourcer personnel assigned to operational tasks, it is particularly important that their access to data archives and systems be limited exclusively to the activities and operations strictly necessary for the tasks specifically assigned to each of them.

It is also very important to keep in mind that the delegation of management of data processing systems to the outsourcer in no way relieves the client of the responsibility for monitoring and verifying the operations carried out on its behalf by the outsourcer. This is an extremely important factor for obvious reasons, and in many cases it is also required by law.

Specifically, the objectives of the audit process entail the assessment of:

- The appropriateness and coherence of the assignment, modification and control of outsourcer personnel access profiles to client systems in terms of tasks and roles.
- The completeness and coherence of guidelines contained in security manuals for the three environments (mainframe, midrange, desktop).
- The effectiveness of system monitoring operations.

To achieve these objectives and perform the audit using internationally accepted methodologies, the activities are carried out in reference to and compliance with the basic principles and best practices in information security, setting forth a list of objectives for control and verification:

- Access control requirements.
- User access management.
- User responsibilities.
- Network access control.
- Operating system access control.
- Application access control.
- System access and use monitoring.

Particular attention is paid to verifying midrange server configurations and observations are made on the basis of three principles. The first is minimisation, also

known as 'least privilege', which entails minimising information exposure, allowing only that access which is indispensable.

***“Each security measure must ensure the ability to monitor and trace security events, both as a means of prevention and during post-mortem investigations after a security incident has occurred”***

The second, defence in depth, involves setting security measures at a level that is directly proportional to the degree of criticalness of the resources that are being protected;

The final measure is vigilance and control. Each security measure must ensure the ability to monitor and trace security events, both as a means of prevention and during post-mortem investigations after a security incident has occurred.

Some of the subtasks in the audit process are described and discussed below, on the basis of the different objectives for control and verification.

## Access control requirements

All decisions and orientations regarding security must be made formally explicit within the company, especially in cases where the operation of information processing systems is entrusted to an outsourcer.

In this case, in addition to the necessary and opportune contractual safeguards, it is important that the terms of system access and use by third parties be regulated in formalised and mutually agreed procedures and practices, to maintain control over who is authorised and what actions they may perform.

In relations between client and outsourcer, the formal and explicit rules on security management for creating system access profiles appropriate to the operational needs of the individual users should, as a rule, be contained in security manuals. The absence of such manuals constitutes a critical point.

In the author's personal experience with examining security management rules, the required actions and operations for the

assignment, modification or cancellation of user accounts in all environments are substantially adequate. There are, however, exceptions. These situations must be assessed with extreme care, in that the failure to observe basic rules may also create compliance issues.

Another activity regards the assessment of the criticality of system software in the mainframe environment, which often leads to the formalisation of specific control activities to be carried out by the client's various internal security personnel. However, in the author's experience, these specific control activities are more oriented toward the verification of system availability than to the detection of security violations.

In the midrange environment, areas for improvement are generally found. For example, there is often no process for formalising internal security practices and procedures in the administration of access credentials. There is no internal company analogue to what is done in the security manuals to formalise procedures with the outsourcer.

Similarly, monitoring and control activities performed by the client and by the outsourcer in the various information processing environments are not always fully defined and formalised. This opens the door to potential problems in the event of a security incident.

## User access management

Formal procedures should be provided for the management of user access to systems in order to control the allocation of access privileges. These procedures should cover the entire lifecycle of each user's access profile, from its initial assignment to the cancellation or de-registration should the user no longer be justified in accessing the system.

In many contexts, the control of access privileges is even more crucial. This is especially true regarding the management of access privileges for outsourcer personnel, who may have profiles as system administrators. Such user profiles, allowing extensive access for system maintenance and management, may end up allowing, although not explicitly authorised, much greater direct access

to company information than that envisioned for a 'standard' user.

Granted the fact that the roles listed in the manuals that the author has had the opportunity to examine are coherent in terms of the activities entrusted to the outsourcer, there is very often an initial difficulty in identifying the corresponding roles on the client side. This may complicate the security governance process.

***"There also ways to check and review the upkeep of system access authorisations, which entail requesting a list of accounts that have not been used for over 90 days in either the mainframe or the midrange environment"***

Another part of the audit process is a thorough and critical reading of the procedures described in the manuals for the management of user accounts. There are tests that can be performed in the mainframe and midrange environments to verify whether the procedures regarding access requests and authorisations are actually applied in practice. There also ways to check and review the upkeep of system access authorisations, which entail requesting a list of accounts that have not been used for over 90 days in either the mainframe or the midrange environment.

## User responsibilities

This aspect, which deals in particular with the methods for creating and managing passwords and their safe custody by users, requires user awareness and collaboration, as well as respect for any privacy laws in force.

Ideally the outsourcer should be invested with the role of subject responsible for the custody, processing and transmission of personal data. This obliges the outsourcer to comply with laws in force in a given country and share with the client the legal responsibility for proper custody, processing and transmission of the personal data of third parties. The outsourcer must also comply with the security requirements described in the same laws. This is especially important in light of the fact that users involved

in password management generally have advanced skills in information technology and great familiarity in the use of access devices, and in many cases, also enjoy system administrator access privileges.

The portions of the manuals regarding the rules for composing passwords and how often they should be changed usually exhibit notable weaknesses. While the rules are generally in line with legal requirements, there are some exceptions regarding the passwords of administrators of midrange UNIX systems. A certain lag is noted here with respect to Windows administrators, due to the lack of an automatic periodic password changing system paired with the use of cryptography for storing them.

## Conclusions

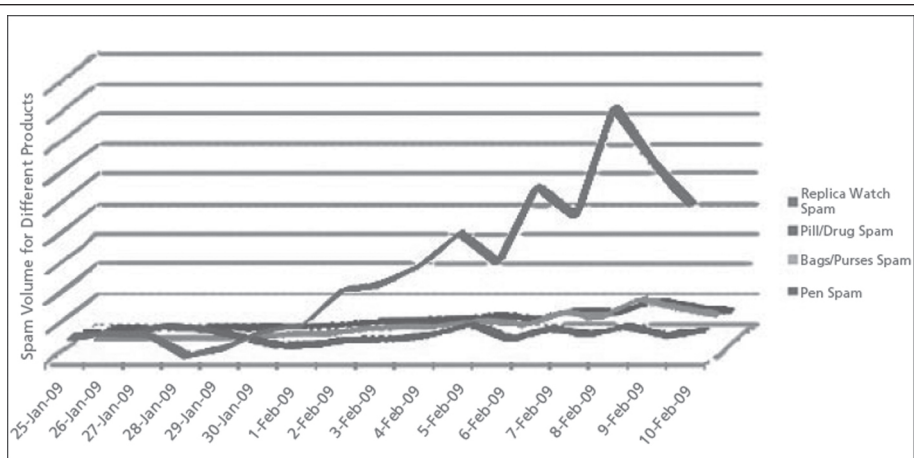
In this article we have discussed some initial thoughts regarding verification of security configurations in the delicate relationship between client and outsourcer. The playing field here is by no means simple. In addition to the likelihood of there being technical issues, it is also essential to keep track of contract and policy issues.

In the author's experience, the outcomes of audit processes such as those described in this article are anything but trivial, in terms of both governance and compliance and, more than anything, at the level of contractual relations and business management.

## About the author

*Dario Forte, CFE, CISM, former police detective and founder of DFLabs has worked in information security since 1992. He has been involved in numerous international conferences on information warfare, including the RSA Conference, Digital Forensic Research Workshops, the Computer Security Institute, the US Department of Defense Cybercrime Conference, and the US Department of Homeland Security (New York Electronic Crimes Task Force). He was also the keynote speaker at the Black Hat conference in Las Vegas. He provides security consulting, incident response and forensics services to several government agencies and private companies.*

*[www.dflabs.com](http://www.dflabs.com)*



Spam volume by product in the run-up to Valentine's Day. Source: McAfee March 2009 Spam Report.

...continued from page 2

'coarse' Internet traffic levels, protocols, and applications, and a topologically diverse global view of Internet routing system security, stability and intelligence, says the firm.

## McAfee: Beware the spam of March

McAfee has predicted a 'tsunami' of spam this month, based on a combination of empirical evidence from past years, and recent takedown activity in the spam industry.

In its March 2009 spam report, it notes that spam volumes go through a traditional up-tick between February and March each year. In 2006, it rose 20%. 2007 saw a 40% increase, while 2008 saw it jump by half month-on-month. "This year the impact on your e-mail infrastructure might be even worse, as the current volumes are lower than usual because of the McColo shut down; yet the volume is quickly catching up," said the report.

Other trends noted included an increasing tendency to partition botnets, which the company said goes beyond the goal of producing more local language spam. It posits that the partitioning behaviour is designed to protect botnets from suffering a single point of failure, while also probing the limits of spam researchers, and vetting their email lists.

"Blacklist systems that rely on honeypots and addresses to gather data may be

weakened, as may systems that require a certain threshold or signature distribution to trigger," it warned.

The report also noted that replica watch spam took the number one spot in the run up to Valentine's Day this year. It spiked considerably compared to medication spam, which declined likely.

## 'Monroe doctrine' needed for cyberspace

As the Obama administration's review of federal cybersecurity continues, Congressional witnesses have called for an electronic version of the Monroe doctrine to tighten up defences in cyberspace.

At a hearing by the Subcommittee on Emerging Threats, Cyber Security, and Science and Technology, Oracle CSO Mary Ann Davidson called for a tougher stance on cyberspace, akin to the US presidential doctrine of the early 1800s. It considered any act of interference with its territory as an act of aggression.

"The advantages of invoking a Monroe-like doctrine in cyberspace would be to put the world on notice that the US has cyber 'turf,'" Davidson said. "We will defend our turf. We need to do both. Now."

The hearings came shortly after Rod Beckstrom resigned as the head of the Department of Homeland Security's secretive National Cyber Security Centre.

## EVENTS CALENDAR

### 26 March 2009 CSO Executive Seminar Series on Data Loss Prevention

Location: Chicago, Illinois, USA  
Website: <<http://public.cxo.com/conferences/index.html?conferenceID=34>>

### 31 March 2009 Eurosec

Location: Nuremburg, Germany  
Website: <http://dcs.ics.forth.gr/eurosec09/>

### 31 March–3 April 2009 Web 2.0 Expo

Location: San Francisco, California, USA  
Website: <[www.web2expo.com/webexsf2009/public/schedule/presentations/235](http://www.web2expo.com/webexsf2009/public/schedule/presentations/235)>

### 20–22 April 2009 Security 2009

Location: Atlanta, Georgia, USA  
Website: <http://net.educause.edu/sec09>

### 20–24 April 2009 RSA Conference

Location: San Francisco, California, USA  
Website: <<https://365.rsaconference.com/index.jspa>>

### 25–26 April 2009 2009 International Conference on Network Security, Wireless Communications and Trusted Computing

Location: Wuhan, China  
Website: [www.ieee-cs.com/nswtct/index.htm](http://www.ieee-cs.com/nswtct/index.htm)

### 28–30 April 2009 InfoSecurity Europe

Location: London, UK  
Website: <[www.infosec.co.uk/page.cfm/Link=18/t=m/trackLogID=4281840\\_8BCB7F6E4D](http://www.infosec.co.uk/page.cfm/Link=18/t=m/trackLogID=4281840_8BCB7F6E4D)>

### 29 April–1 May 2009 Compliance & Risk Management Summit

Location: Chicago, Illinois, USA  
Website: <[www.gartner.com/it/page.jsp?id=676310](http://www.gartner.com/it/page.jsp?id=676310)>