



# NEWSLETTER

CENTRE for  
CRITICAL INFRASTRUCTURE  
PROTECTION

Volume 2, Issue 4

June 2003

## REPORT from AUSCERT CONFERENCE 2003

The Australian Computer Emergency Response Team (AusCERT) held their annual conference this year on 11 to 15 May on the Gold Coast of Australia. The conference presented an ideal opportunity for some of the CCIP team to meet and exchange notes with staff from AusCERT and other international response teams.

Although the CCIP is not a dedicated CERT in the same mould as AusCERT, there are definite areas of common ground. These were discussed at the conference, and information sharing avenues were established amongst the response teams.

The high quality of the conference's speakers, and wide range of topics covered, en-

sured that attendees were up to speed with the latest developments in the world of IT security.

### The presentations included:

- Virtual Welcome from Prof. Eugene Spafford, Purdue University;
  - *Digital Signature Legislation* by Peter Guttman of Auckland University;
  - *The Role of Education and Research in Cyber Security & National Infrastructure Protection* by Prof. Bill Caelli of Queensland University of Technology; and
  - *Forensic Discovery* by Dr. Wietse Venema (of SATAN fame).
- The conference was also the launching point for three

new initiatives, which could have significant repercussions for the Australasian business community.

1. 2003 Australian Computer Crime and Security Survey;
2. Certification for Security Professionals; and
3. AusCERT National Information Technology Security Alert Scheme.

Each of which is expanded in articles below.

Thank you AusCERT for your professionalism in organising a world class conference, and keep up the good work.

### INSIDE THIS ISSUE:

*Recent Significant Alerts & Advisories* 2

*2003 Australian Computer Crime and Security Survey* 2

*AusCERT National IT Security Alert Scheme* 3

*Virus Activity* 3

*New Zealand Port Scan Activity* 4

*Certification for Security Professionals* 4

*New CCIP Director* 4

## HONEYPOTS, HONEYTOKENS & INTRUSION DETECTION

Honeypots are an evolving technology that, until recently, has been used mainly for research purposes; learning the tools, tactics and motives of the Blackhat community and sharing those lessons learnt, but is now being incorporated into Intrusion Detection Systems (IDS). The Honeynet project ([www.Honeynet.org](http://www.Honeynet.org)), defines a Honeypot as "an information system resource whose value lies in unauthorized or illicit use of that resource".

Honeytokens are an extension to the Honeypot con-

cept. A Honeytoken is a resource or piece of data that has no production value or authorized activity, if someone attempts to access or retrieve this data, they are committing an unauthorized act.

A simple example of a Honeytoken could be fake documents (with enticing names) on a file server or invalid credit card numbers in a database, with an IDS or network sniffer configured to alert when the Honeytoken appears on the network. The term Honeytoken is a new one, however the con-

cept is not. An early use of Honeytokens in computing can be seen in Cliff Stoll's 1986 book "The Cuckoo's Egg".

There has been little formal research into Honeytoken technologies and their use in Intrusion Detection until recently, but we can expect to see some interesting results as the Honeynet project focuses on the subject.

For more information, look out for Lance Spitzner's next article on the Security-Focus website ([www.securityfocus.net](http://www.securityfocus.net)).

Communication regarding this newsletter can be addressed to:

[newsletter@ccip.govt.nz](mailto:newsletter@ccip.govt.nz)



Government  
Communications  
Security Bureau

### CONTACT DETAILS

Ph: +64 4 498 7654

Fax: +64 4 498 7655

Email: [info@ccip.govt.nz](mailto:info@ccip.govt.nz)

Web: [www.ccip.govt.nz](http://www.ccip.govt.nz)

PO Box 12-209  
Wellington, New Zealand

## RECENT SIGNIFICANT ALERTS & ADVISORIES

*The Commonwealth Government has contracted AusCERT to provide a free alerts service, available to both business and private computer users.*

AusCERT National IT Security Alert Scheme, page 3

REFERENCE	DESCRIPTION	DATE
<a href="#">Red Hat</a>	Updated kernel addresses security vulnerabilities	23/06/03
<a href="#">iDEFENCE</a>	Linux-PAM getlogin() spoofing vulnerability	17/06/03
<a href="#">Ethereal</a>	Several security problems in Ethereal 0.9.12	13/06/03
<a href="#">CERT/CC</a>	Linux kernel IP stack incorrectly calculates size of an ICMP citation for ICMP error	12/06/03
<a href="#">CERT/CC</a>	Vulnerability in OpenSSH daemon (sshd)	10/06/03
<a href="#">Sun</a>	An Untrusted Applet may Access Information From a Trusted Applet	09/06/03
<a href="#">AusCERT</a>	Malicious Software Report - W32Bugbear.B	06/06/03
<a href="#">Microsoft</a>	Cumulative Patch for Internet Explorer	05/06/03
<a href="#">Sun</a>	Security vulnerability in Samba(7) versions 2.2.2 through 2.2.7 May allow remote user unauthorized privileges, on Solaris9	04/06/03
<a href="#">MAILsweeper</a>	MAILsweeper patch available for SMTP RTF Attachment Denial of Service	03/06/03

*Please refer to the CCIP website for a more complete list of alerts and advisories.*

## 2003 AUSTRALIAN COMPUTER CRIME AND SECURITY SURVEY

*Mike Spring, our Centre's "Founding Father", is taking on new endeavours in Canberra, Australia.*

New CCIP Director  
page 4

AusCERT has produced this year's Australian Computer Crime and Security Survey in partnership with the Australian Federal Police, Queensland Police, Western Australia Police and South Australia police. With over 200 responses from Australian public and private sector organisations, the survey provides the most up-to-date and authoritative analysis of computer network attack and computer misuse trends in Australia over the last 12 months.

### The key findings of the survey are:

Forty-two percent of respondent organisations experienced one or more computer attacks that harmed the confidentiality, integrity or availability of network data or systems.

Despite overall lower levels of incidents being reported, only 11% of respondents felt they were managing all computer security issues reasonably

well. Sixty-seven percent of organisations increased expenditure on network security in the last 12 months as a result of computer security incidents or concerns.

The trend shows a continuing shift towards a greater occurrence of externally, and fewer internally, sourced harmful attacks. Of those who experienced attacks that harmed data confidentiality, integrity or availability, 91% were externally, and 36% internally, sourced attacks.

Total losses for 2003 are more than double the quantified losses for 2002 (about \$12 million, compared to about \$6 million in 2002).

Financial fraud, laptop theft, and virus, worm and Trojan infections are the largest sources of computer crime losses.

Despite high use of anti-virus software and policies

for developing controls against malicious software, 80% were infected with a virus, worm or Trojan and 57% suffered financial loss as a result - more than last year

Only a minority of respondent organisations hold specialist IT security certifications, with industry vendor IT security certifications at 36% and vendor-neutral IT security certifications at 15%.

Thirty-eight percent were dissatisfied with the level of IT security qualifications, training or experience within their organisations.

The full report can be found at <http://www.ausecert.org.au/crimesurvey>

The CSI/FBI Computer Crime and Security Survey 2003, on which the AusCERT survey is based, has also been published recently and is available at <http://www.gocsi.com/press/20030528.html>

## AUSCERT NATIONAL IT SECURITY ALERT SCHEME

The Commonwealth Government has contracted AusCERT to provide a free alerts service, available to both business and private computer users. The scheme is

designed to provide greater access to information about the most critical computer network threats and vulnerabilities. AusCERT will also be providing a corresponding

reporting scheme, which will come into operation early in the second half of 2003, so computer users can provide information about suspected security incidents.

*The International Systems Security Engineering Association (ISSEA) is overseeing the implementation of a global and open certification scheme for IT and systems security professionals.*

Certification for Security Professionals, page 4

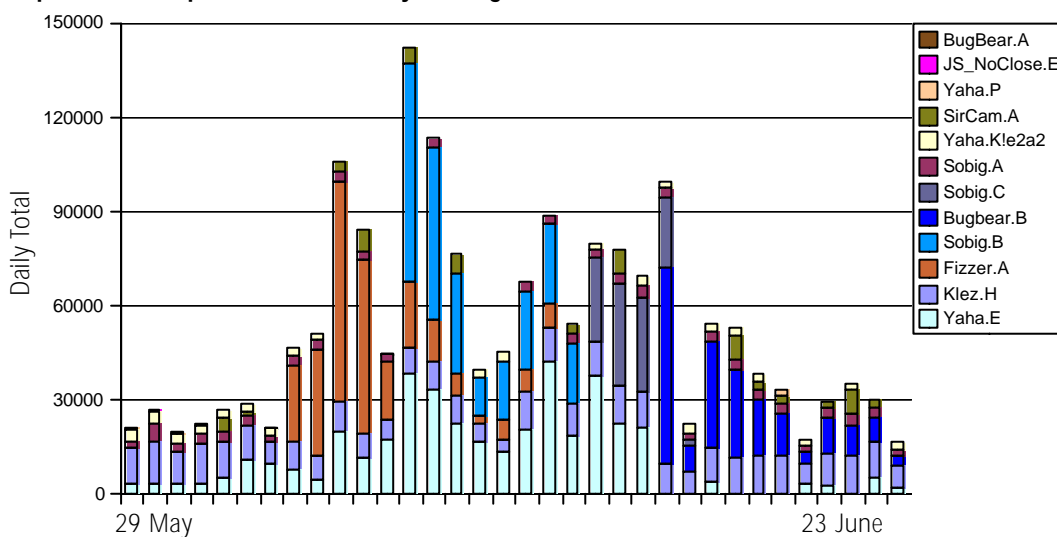
## VIRUS ACTIVITY

MessageLabs virus statistics for the past six weeks show four overlapping waves of malware; Fizzer.A, Sobig.B, Sobig.C and Bugbear.B. Bugbear.B appeared on 4 June and quickly overtook Sobig.C to become the number one virus at MessageLabs with

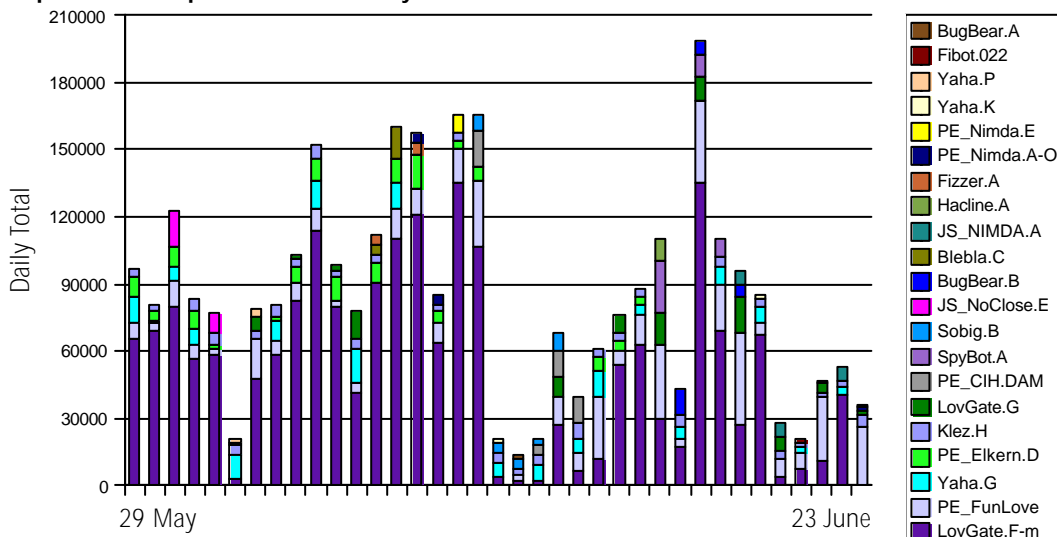
around 100,000 intercepts in the following 24 hours. Bugbear.B contains a list of domain names, including five NZ banks. AV researchers suggest that if the victim machine belongs to such a domain the worm will attempt to enable the AutoDial

feature. The infection ratio recorded by MessageLabs was driven up to around 1:60 during these waves. Klez.H still features but lately the "klez noise" is pushed to 5th at TrendMicro with LovGate.F averaging 55,000 intercepts per day.

**Top 5 viruses captured worldwide by MessageLabs**



**Top 5 viruses captured worldwide by TrendMicro**



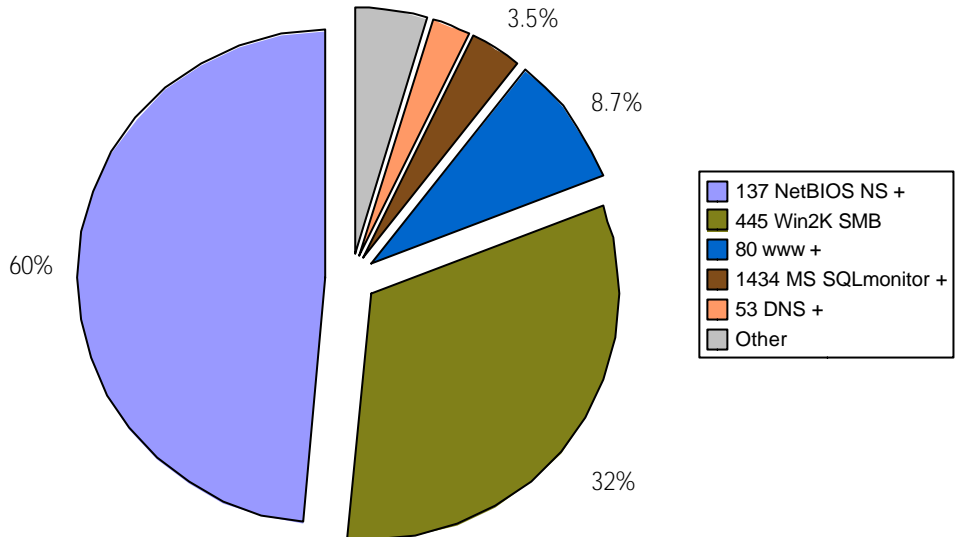
*Port 137 is again the most scanned port in New Zealand after last months aberration with 445 as number 1*

New Zealand Port Scan Activity, page 4



## NEW ZEALAND PORT SCAN ACTIVITY

New Zealand's port probe activity by port number 29 April to 16 June.



Port 137 is again the most scanned port in New Zealand after last months aberration with 445 as number 1, 445 has returned to 2nd most scanned port but spikes of

445 traffic still appear the last on 8 May 2003 with 85000 scans when the daily average is ~1800 scans. Please remember while we have listed the services reg-

istered for the ports it should be noted that other applications could be responsible for the activity. See [isc.incidents.org](http://isc.incidents.org) for more information.

## CERTIFICATION *for* SECURITY PROFESSIONALS

The International Systems Security Engineering Association (ISSEA) is overseeing the implementation of a global and open certification scheme for IT and systems security professionals. This certification scheme ad-

dresses the shortfalls of traditional IT security certifications as it is founded on essential principles of security. Initial development of the scheme is to be jointly undertaken by the University of Queensland (UQ), Electronic

Warfare Associates Australia (EWA-Australia) and the Australian Computer Emergency Response Team (AusCERT). More information on ISSPCS can be found at URL: <http://www.isspcs.org/>.

## NEW CCIP DIRECTOR

Mike Spring, our Centre's "Founding Father", is taking on new endeavours in Canberra, Australia beginning next month. Mike has been the energy core and guiding light for our work since 2001 and will be acutely missed. We wish him health and all success across the Tasman.

Mike is succeeded by Glen Singleton, who comes to us from the planning side of the GCSB. Glen is a graduate of Georgetown University's School of Foreign Service in Washington, D.C., and has worked in cryptology since 1966 both in New Zealand and North America. He

recently served over two years with the External Assessments Bureau, Department of the Prime Minister and Cabinet, as Assessments Manager. He is delighted with his new role and looks forward to meeting and working with the CIP community.

### June email alerts issued by CCIP:

- 06/06/03 W32/Bugbear.B
- 05/06/03 Cumulative Patch for IE

### DISCLAIMER

While this newsletter is accurate to the best of our knowledge, CCIP does not accept any responsibility for errors or omissions. If any of the vulnerabilities affects you, you are advised to ensure that you have the most current information available. CCIP will not be liable for any loss or damage howsoever caused, arising from or in connection with the use of information contained in this newsletter.

CCIP only issues those external alerts that we assess as serious and would affect a large number of NZ users. For notification of all discovered software vulnerabilities we recommend that you subscribe to a commercial Computer Emergency Response Team or to vendor alert lists.

Reference in this newsletter in any manner to any commercial product, process or service does not constitute or imply its endorsement or recommendation by CCIP. Views and opinions stressed herein may not be used for advertising or product endorsement purposes.

Please refer to the CCIP website for a list of recent alerts and advisories.



### CONTACT DETAILS

Ph: +64 4 498 7654  
 Fax: +64 4 498 7655

Email: [info@ccip.govt.nz](mailto:info@ccip.govt.nz)  
 Web: [www.ccip.govt.nz](http://www.ccip.govt.nz)

PO Box 12-209  
 Wellington, New Zealand