



NEWSLETTER

CENTRE for
CRITICAL INFRASTRUCTURE
PROTECTION

Volume 2, Issue 3

May 02, 2003

THE MONTH IN REVIEW

The virus and port statistics compiled this month show a couple of interesting trends.

Messagelabs shows KLEZ.H consistently retaining its number one spot in their Top

Five, while TrendMicro's figures show the LOVEGATE.F worm as the most prolific by a considerable margin with around 350,000 on the 24th of April.

According to the Internet Storm Centre, port 445 is the top target for port scans, while Kasperky Labs are attributing some of this activity to a new blended worm/trojan called RANDON.

INSIDE THIS ISSUE:

Recent Significant Alerts & Advisories 2

Sendmail Vulnerabilities 2

Are You the Weakest Link? 3

Virus Activity 3

New Zealand Port Scan Activity 4

Fluffi Bunni 4

Mailing List 4

Reference List 4

eFRAUD ON THE RISE

Internet scams in Australia and the United States of America have begun targeting users of online banking, electronic trading and electronic payment schemes.

The scammers usually send a large number of unsolicited emails out to potential victims. These emails purport to be from an electronic trading company or bank. The scammers hope that some of the people receiving the email will have an account with the company from whom the email is supposed to have come from, and will believe and act upon the request being made. The emails, which are often poorly written, generally urge users to update their login details (usernames and passwords) and provide an HTML (Hyper text mark-up language) hyperlink to do so.

The Internet address the e-mail refers user to may appear similar to the correct URL (Universal Resource Locator, the Internet address) for the particular site being targeted in the scam. The similar URL address method was popular late last year, and targeted eBay, AOL and PayPal among others.

The recent scams targeting Australian banking institutions are a bit more subtle - the hyperlink in the email appears correct but the actual URL links to a mimic site operated by the attacker(s). The mimic site will have the same layout and function as the target's real site. The mimic sites sometimes use digital certificates to make victims feel "comfortable" with the security of the website.

7 simple steps to help you avoid being scammed:

1. Never follow a hyperlink supplied in an e-mail. Connect to the site by typing the URL into the browser or by using a bookmark.
2. Verify that the domain name is the correct one for the organisation.
3. Check the details of the website's digital certificate and ensure it has been issued by a verified Certificate Authority (CA).
4. Do not use the same password for different websites.
5. Make yourself aware of the company's online security policy. Never provide account details and passwords in response to unsolicited email.
6. Read the email request carefully - you should be suspicious if the request is written poorly or has obvious grammatical errors.
7. Visit the netsafe.org.nz website for advice on general Internet safety.

Useful eFraud Links:

www.ccip.govt.nz/security-tips/security-tips.htm
www.netsafe.org.nz
www.news.com.au/common/story_page/0,4057,6284482%255E15306,00.html
www.stuff.co.nz/stuff/0,2106,2380878a13,00.html
www.anz.com/nz/inetbank/security.asp
www.asbbank.co.nz/about-fastnet/about_classic/classic_body.stm
www.bnz.co.nz/Internet_Banking/1.1184.10-147,FF.html
www.kiwibank.co.nz/terms/generaltc.pdf
www.nbnz.co.nz/online/onlinebanking/faq/securitypassword.asp
www.westpac.co.nz/olcontent/olcontent.nsf/Content/Online+Banking+is+easy

Communication regarding this newsletter can be addressed to:

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
Web: www.ccip.govt.nz

PO Box 12-209
Wellington, New Zealand

Polish researcher Michael Zalewski recently discovered another vulnerability in Sendmail. This bug can allow denial-of-service attacks on vulnerable Sendmail machines, and could possibly allow root compromises.

Sendmail Vulnerabilities

RECENT SIGNIFICANT ALERTS & ADVISORIES

REFERENCE	DESCRIPTION	DATE
Microsoft	Cumulative Patch for BizTalk Server	01/05/03
Microsoft	Cumulative Patch for Internet Explorer	24/04/03
Microsoft	Cumulative Patch for Outlook Express	24/04/03
Microsoft	Unchecked Buffer In Windows Component Could Cause Server Compromise (revised - NT4 patch available)	24/04/03
redhat	Updated tcpdump packages fix various vulnerabilities in RH 7.1, 7.2, 7.3, and 8.0	24/04/03
Microsoft	Buffer Overrun in Windows Kernel Message Handling could Lead to Elevated Privileges - MSR Important	17/04/03
ORACLE	Potential security vulnerability in Oracle E-Business suite - Report Review Agent (RRA) / File Server(FNDFS).	15/04/03
NetSafe	online banking and electronic payment sites targeted in fraudulent activity	14/04/03
SETI@home	Security issue in SETI@home client	14/04/03
iDefense	Denial of Service in Apache HTTP Server 2.x	11/04/03
Microsoft	Flaw in Microsoft VM Could Enable System Compromise	10/04/03
Microsoft	Flaw In Winsock Proxy Service And ISA Firewall Service Can Cause Denial Of Service	10/04/03
Microsoft	Patch Available for 'Indexing Services Cross Site Scripting' Vulnerability	10/04/03
samba.org	Security bugfix for Samba	08/04/03
Apache	The Apache Software Foundation Announcement Apache 2.0.45 Released	03/04/03
CERT/CC	CERT Advisory CA-2003-12 Buffer Overflow in Sendmail	30/03/03

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

SENDMAIL VULNERABILITIES

Several months ago the Internet Security Systems (ISS) discovered a buffer overflow in Sendmail's address handling routines. This buffer overflow could allow an attacker to gain increased privileges on the system, to the same level as the Sendmail program (usually root). The exploit could be performed remotely. As the buffer overflow was based on the address line, it was content and not connection based. A message could be passed through several different systems, including firewalls, and compromise a vulnerable machine on the protected side. ISS released information on this vulnerability to Sendmail, Inc. who worked with vendors to release patched version of their software.

However, Polish researcher Michael Zalewski recently discovered another vulnerability in Sendmail. This bug

can allow denial-of-service attacks on vulnerable Sendmail machines, and could possibly allow root compromises. Like the earlier bug, this vulnerability exists in the Sendmail address handling routines. This recent bug is distinct from the earlier bug, although both occur during Sendmail's handling of a crafted email address. The earlier vulnerability occurred in the crackaddr(char* addr) function within the headers.c file. This latest vulnerability exists in the pre_scan() function within the parseaddr.c file. The bug exists due to a conversion between character and integer types being performed incorrectly in some circumstances. Due to the nature of the bug, only platforms with 'char' variable types 'signed' as default are currently known to be vulnerable. Little endian (Intel) systems are also thought to be easier to exploit.

Sendmail has produced patches for versions 8.9, 8.10, 8.11, and 8.12. However, the vulnerability also exists in earlier versions of the code; therefore, site administrators using an earlier version are encouraged to upgrade to 8.12.9.

There is no known workaround for this vulnerability. Until a patch can be applied, you may wish to set the RunAsUser option to reduce the impact of this vulnerability. As a good general practice, the CERT/CC recommends limiting the privileges of an application or service whenever possible.

Exploit code for the recently disclosed sendmail vulnerability had already been posted on the Internet at www.computerworld.com/securitytopics/security/holes/story/0,10801,79021,00.html

(Continued on page 3)

Fluffi Bunni is one of the most mysterious figures in the hacking community.

Fluffi Bunni
page 4

SENDMAIL VULNERABILITIES CONT.

(Continued from page 2)

Useful Sendmail Links:

www.cert.org/advisories/CA-2003-07.html
www.cert.org/advisories/CA-2003-12.html

2003-12.html
www.sendmail.org
www.sendmail.com/security/

CCIP has compiled a list of

vendor URLs for these vulnerabilities. To receive a copy of this list, send a request to info@ccip.govt.nz.

The recent scams targeting Australian banking institutions are a bit more subtle - the hyperlink in the email appears correct but the actual URL links to a mimic site operated by the attacker(s).

eFraud on the Rise
page 1

ARE YOU THE WEAKEST LINK?

In a recent survey by the organisers of an information security exhibition in London, it was revealed that a whopping 90 per cent of those who took part in the

survey readily gave up their computer password in exchange for a cheap pen, seemingly without a thought for the possible consequences of putting their of-

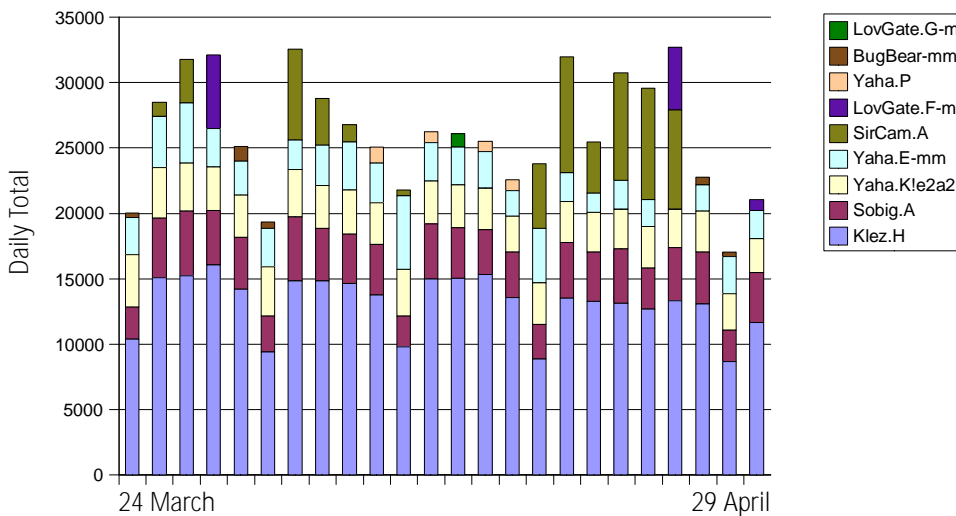
fice computer system at risk.

For further information:

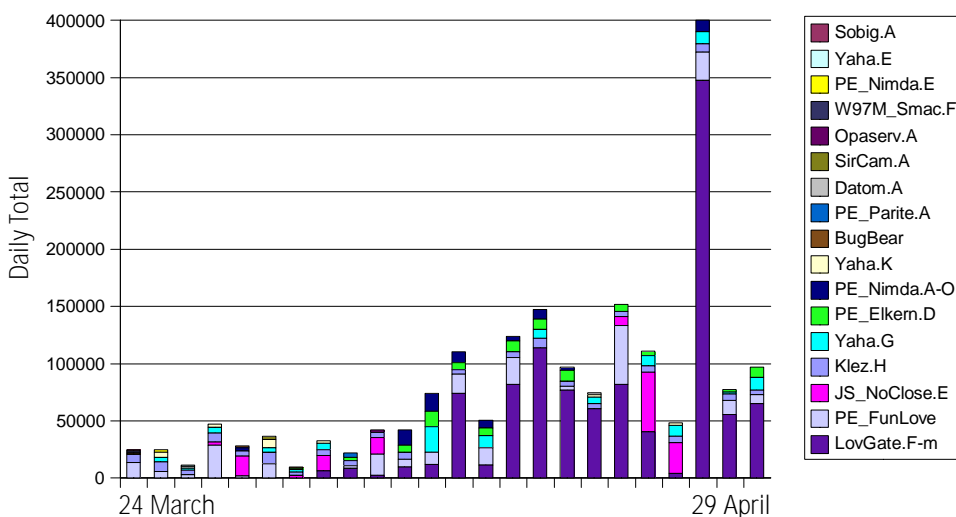
www.infosec.co.uk/page.cfm/Action=Press/PressID=255/T=m

VIRUS ACTIVITY

Top 5 viruses captured worldwide by MessageLabs



Top 5 viruses captured worldwide by TrendMicro



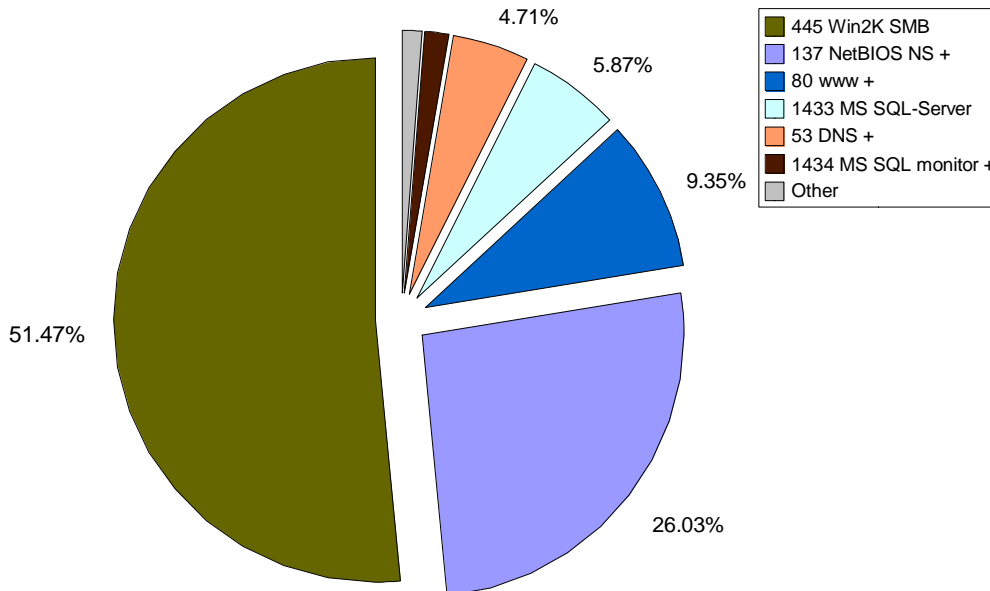
SQL Slammer worm scans port 1434, and Qaz trojan scans port 137.

New Zealand Port Scan Activity
page 4



NEW ZEALAND PORT SCAN ACTIVITY

New Zealand's port probe activity by port number 21 March to 29 April from incidents.org



While we have listed the services registered for the ports it should be noted that other applications may be responsible for the activity eg. SQL Slammer worm scans port 1434, and Qaz trojan scans port 137. The '+' sign indicates other applications/services are associated with the port. See isc.incidents.org for more information.

FLUFFI BUNNI

Scotland Yard have arrested a 24 year old man Lynn Htun, believed to be the hacker "Fluffi Bunni". The arrest took place at a security professionals trade show - InfoSecurity Europe 2003, in London. Htun has been arrested on outstanding forgery charges.

Fluffi Bunni is one of the most mysterious figures in the hacking community. He selects specific targets, and his hacks are very effective, breaking into computers of leading internet security organisations and defacing web pages and placing an image of a pink rabbit sitting

at a keyboard. (Reuters)

For the full article refer to:
www.reuters.com/newsArticle.jhtml?storyid=PLANI42IRKCJICRB&EZFSEYtype=internetNews&storyID=2661643

MAILING LIST

Critical alerts will be emailed to members of the CCIP email list as and when we become aware of them. To subscribe, send your contact details by email with the

subject line: 'Subscribe' to alerts@ccip.govt.nz. To unsubscribe, send an email with the subject line: 'Unsubscribe' to the same address.

This service is intended for CI organisations, government departments and IT service providers in New Zealand.

REFERENCES

MessageLabs: www.messagelabs.com
 Internet Storm Centre: isc.incidents.org
 TrendMicro: www.trendmicro.com

InfoSecurity Europe 2003: www.infosec.co.uk
 AusCERT: www.auscert.org.au/render.html?it=2909
 Kaspersky Labs: www.kaspersky.com

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
 Web: www.ccip.govt.nz

PO Box 12-209
 Wellington, New Zealand