



NEWSLETTER

CENTRE for
CRITICAL INFRASTRUCTURE
PROTECTION

Volume 2, Issue 5

August 2003

HACKING NOW ADDRESSED IN CRIMES ACT

This month Parliament signed off on the Crimes Amendment Act (No 6), which comes into force on the 1st of October. Four new offences, relating to the misuse of computers and computer systems, will be created with penalties of up to ten years for serious offences. Under certain conditions, exemptions exist for the New Zealand Security Intelligence Service and the Government Communications Security Bureau, our parent organisation. A brief overview in relation to crimes involving computers is included in this issue.

The past few weeks have

seen yet another hectic time in cyberspace. It started, at the beginning of July, with the 'Defacement Challenge', which promised to have a major impact on insecure websites. In the end, the hacker community assailed the competition scorekeepers Zone-H, the only defacement register on the web, which forced their web administrators to disable the defacement recording facility for a number of days.

There was also a batch of significant Microsoft vulnerabilities published and more patches were released which should keep system administrators busy for a while.

However Microsoft were not

alone as a major purveyor of susceptible software. Cisco also released details of a major IOS software vulnerability, for which an exploit was published within a few days of it being published.

We at CCIP added over 80 advisories to the our website and sent out one CCIP Advisory and three External Advisory redistributions, all relating to the Microsoft and Cisco vulnerabilities.

In general, virus trends have remained relatively static, although very recently the Blaster worm and Sobig.F have made their presence felt. Port probe activity in New Zealand has also been relatively quiet.

INSIDE THIS ISSUE:

Recent Significant Alerts & Advisories 2

More Microsoft Vulnerabilities Published 2

Cisco Denial of Service Vulnerability 3

Virus Activity 3

New Zealand Port Scan Activity 4

July E-mail Alerts Issued by CCIP 4

CRIMES AMENDMENT ACT 2003

Introduction

The Crimes Amendment Act 2003 will come into force on 1 October 2003.

The Act will create four new offences relating to the misuse of computers and computer systems. These offences are:

1. Accessing a computer system for a dishonest purpose (section 249)
2. Damaging or interfering with a computer system (section 250)
3. Making, selling, or distributing or possessing software for committing crime (section 251)

4. Accessing a computer system without authorisation (section 252)

The expressions "access" and "computer system" are defined in section 248.

Penalties

The first two offences carry a range of penalties depending on the degree of seriousness of the offence, with a maximum of seven and 10 years imprisonment respectively, while the remainder carry a maximum penalty of two years imprisonment.

Offences

The section 249 offence involves accessing a computer system directly or indirectly

either to obtain a benefit for oneself or to cause loss to another person, or with intent to do so. The essential element of the offence in either case is dishonesty, or deception (which is separately defined in section 240(2)).

The section 250 offence involves intentional or reckless destruction, damage or alteration of a computer system. At its most serious, if this is done by a person who knows or ought to know that danger to life is likely to result, the section provides a maximum penalty of 10 years imprisonment. Where, without au-

(Continued on page 4)

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

RECENT SIGNIFICANT ALERTS & ADVISORIES

Microsoft	Unchecked Buffer in DirectX Could Enable System Compromise	21/08/2003
UNIRAS	Malicious software report W.32/Sobig.F-mm	20/08/2003
AusCERT	Malicious software activity WORM_MSBLAST.D (W32/Welchia, W32/Nachi)	19/08/2003
CERT/CC	GNU Project FTP Server Compromise	14/08/2003
CCIP	Microsoft RPC/DCOM Worm	12/08/2003
CERT/CC	W32/Blaster worm update	12/08/2003
CERT/CC	Malicious software activity W32/Mimail	04/08/2003
Apache	Apache HTTP Server 1.3.28 Released	22/07/2003
CERT/CC	Exploit available for the Cisco IOS Interface Blocked Vulnerabilities	19/07/2003
Cisco	Cisco IOS Interface Blocked by IPv4 Packet	17/07/2003
Microsoft	Buffer Overrun In RPC Interface Could Allow Code Execution	17/07/2003
Microsoft	Unchecked Buffer in Windows Shell Could Enable System Compromise	17/07/2003
CERT/CC	Buffer Overflow in Microsoft Windows HTML Conversion Library	16/07/2003
Apache	Apache 2.0.47 released to fix three security issues	10/07/2003
CCIP	Website Defacement Challenge - 6 July 2003	04/07/2003

Please refer to the [CCIP website](#) for a more complete list of alerts and advisories.

CCIP recommends that all systems are patched tested and audited on a regular basis.

Virus Activity
page 3

MORE MICROSOFT VULNERABILITIES PUBLISHED

July was a busy month for Microsoft, with many vulnerabilities published regarding their products. Details of ten of these advisories were published on our website in the last two weeks of the month.

By far the most critical vulnerability was the "[Buffer Overrun In RPC Interface Could Allow Code Execution](#)". A number of exploits are available for this vulnerability, which has been the subject of analysis not only by the AV vendors, but also organisations such as [AusCERT](#), [UNIRAS](#), [CERT/CC](#) and the [US Department of Homeland Security](#). Microsoft had a patch for this vulnerability available on 16 July.

The other two critical advisories issued by Microsoft, "[Unchecked Buffer in DirectX Could Enable System Compromise](#)" and "[Buffer Overrun In HTML Converter Could Al-](#)

[low Code Execution](#)" also have patches available for all affected software platforms.

Microsoft also released details of two new user rights, "[Impersonate a client after authentication](#)" and "[Create global objects](#)", which help to provide security in Windows 2000. In the case of the former, this is done by helping to allow authorised servers to impersonate clients that connect to it through methods such as remote procedure calls (RPC) or named pipes. In the case of the latter, allowing user accounts to create global objects in a Terminal Services session, which previously had only been assigned to members of the Administrators group, the System account, and Services that are started by the Service Control Manager.

Earlier this month, Microsoft

released the following advisories:

Microsoft Security Bulletin MS03-032: [Cumulative Patch for Internet Explorer](#) - this 'critical' advisory describes two new vulnerabilities, the most serious of which could enable an attacker to run arbitrary code on a user's system if the user either browsed to a hostile website or opened a specially crafted HTML-based e-mail message.

Microsoft Security Bulletin MS03-033: [Unchecked Buffer in MDAC Function Could Enable System Compromise](#) - this advisory supersedes MS02-040.

Given recent history, it will probably only be a matter of weeks before exploits are released to take advantage of the vulnerabilities described in these bulletins.

Given recent history, it will probably only be a matter of weeks before exploits are released to take advantage of the vulnerabilities described in these bulletins.

More Microsoft Vulnerabilities
Published

CISCO DENIAL OF SERVICE VULNERABILITY

On the 17th of July, CCIP issued an alert regarding a vulnerability that affected a large number of Cisco routers and switches. This vulnerability could be exploited by an attacker sending specially crafted packets directly to the device, resulting in a Denial of Service condition.

By default Cisco routers are configured to process IPv4 packets. In this instance, sending a number of crafted packets utilising IPv4 protocol types of 53 (SWIPE), 55 (IP Mobility), 77 (Sun ND) or 103 (Protocol Independent Multicast) to the device had the potential to cause the input queue on the device's

interface to become full. With a full input queue, the device would be unable to process packets on that interface, possibly requiring it to be manually rebooted to clear the queue and restore normal service. [Cisco](#) have provided a solution to correct this vulnerability.

The more significant in practice of these two offences is likely to be section 252, which in effect makes computer "hacking" a criminal offence.

Crimes Amendment Act
page 1 & 4

VIRUS ACTIVITY

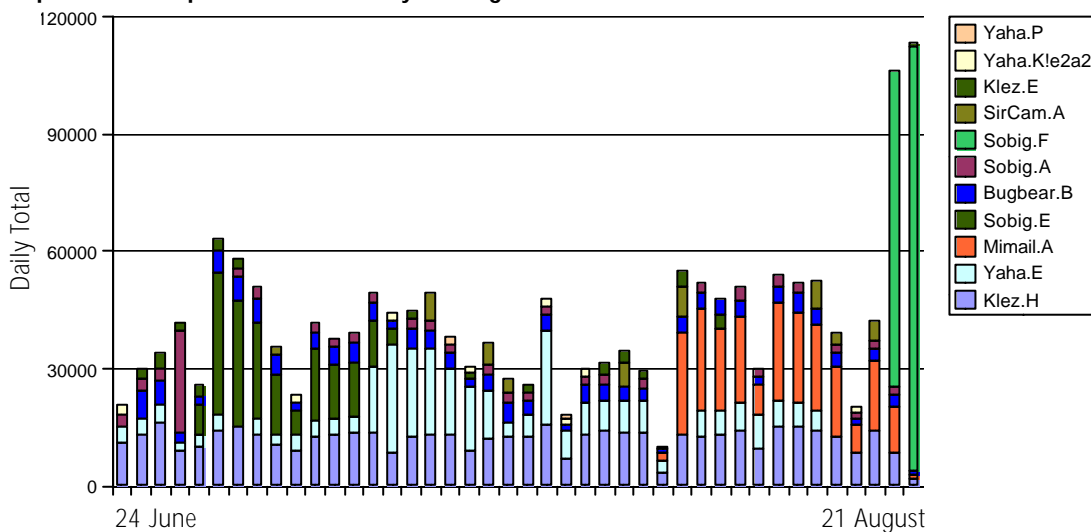
Sobig.F is the fastest growing e-mail borne virus ever according to MessageLabs. Lovgate variants are still regular

triggers for the TrendMicro detectors.

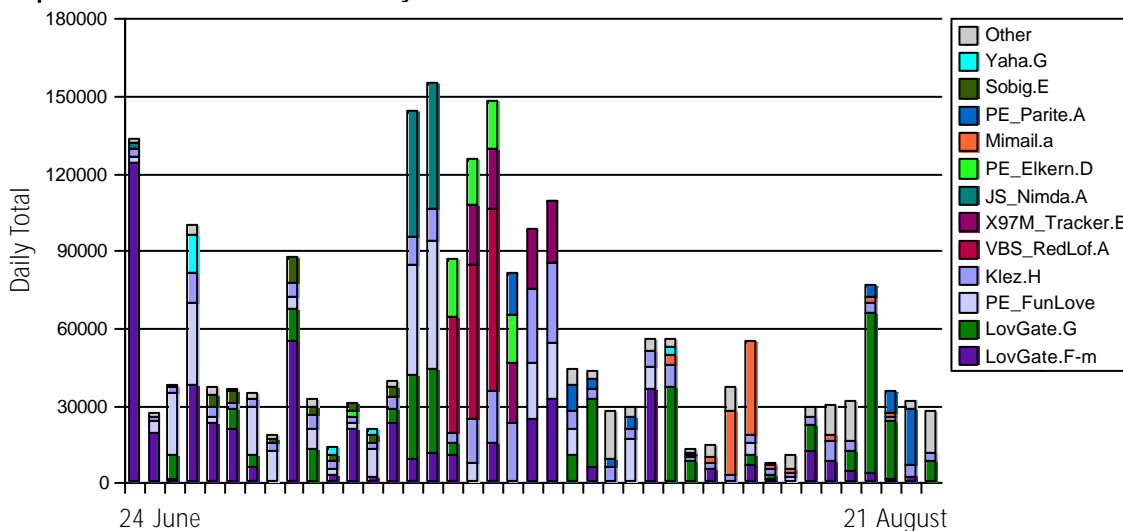
CCIP recommends that all

systems are patched tested and audited on a regular basis.

Top 5 viruses captured worldwide by MessageLabs



Top 5 viruses detected worldwide by TrendMicro



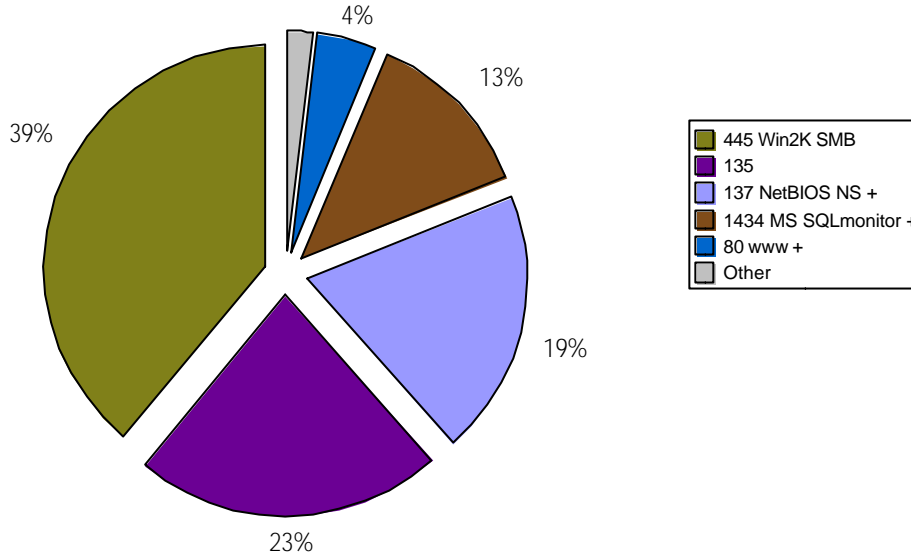
Port 445 probes continue to be detected in bursts, three single day bursts making up 40% of scan traffic in the time period shown.

New Zealand Port Scan
Activity, page 4



NEW ZEALAND PORT SCAN ACTIVITY

New Zealand's port probe activity by port number 24 June - 21 August.



Port 80 probes have been relegated to 5th with the onslaught of port 135 scans from 11 August due to the worm MSBlast.A, which exploits the Microsoft

RPC/DCOM vulnerability. The scans on port 1434 make up 13% of the total for the two months. This was mainly isolated to 15 August. Port 445 probes con-

tinue to be detected in bursts, three single day bursts making up 40% of total New Zealand port scan traffic in the time period shown. See isc.incidents.org.

CRIMES AMENDMENT ACT CONT.

(Continued from page 1)

thorisation, a person damages, deletes, modifies or otherwise interferes with or impairs any data or software, or causes a computer system to either fail or deny service to any authorised users, the maximum penalty is seven years imprisonment.

The section 251 and section 252 offences are essentially self-explanatory.

The key element of the section 251 "sale, supply or distribution" offence is that the person must either know that a crime is to be committed, or must promote the software in question as being useful for the commis-

sion of a crime knowing or being reckless as to whether it will be used for such a purpose. In the case of the "possession" offence, the key element is intention to commit a crime.

The more significant in practice of these two offences is likely to be section 252, which in effect makes computer "hacking" a criminal offence. The offence is simple unauthorised access, whether direct or indirect, to a computer system, knowing or being reckless as whether one is authorised to access that computer system.

Qualified Exemptions

Sections 253 and 254 con-

tain qualified exemptions in respect of the section 252 offence for the New Zealand Security Intelligence Service and the Government Communications Security Bureau respectively where those organisations are acting under the authority of (in the case of the NZSIS) an interception warrant or (in the case of the GCSB) a computer access authorisation issued under section 19 of the GCSB Act 2003.

Important Note

The above is a general summary only of the new provisions and should not be interpreted as, or acted upon in substitution for, professional legal advice.

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

JULY E-MAIL ALERTS ISSUED BY CCIP:

04/07/03 Website Defacement Challenge	17/07/03 Cisco IOS Interface Blocked by IPV4 Packet
17/07/03 Buffer Overrun in Microsoft RPC	19/07/03 Exploit Available for the Cisco IOS