

CCIP Monthly Report for APRIL

Welcome to the April issue of the Monthly Report produced by the Centre for Critical Infrastructure Protection's Operations Centre. This report is designed to provide an overview of trends in relation to virus activity and distribution, Internet response times, website defacements and other relevant information for the past month. The report also aims to keep you informed of current activities related to the CCIP Operations Centre.

Please note that back issues of the monthly report are now published on the Internet and can be accessed by visiting the [Publications](#) page of the CCIP website.

Any comments regarding the content of the report, or any relevant areas you would like to see covered in future issues, are welcomed. Please send comments to info@ccip.govt.nz and include "MONTHLY REPORT" in the subject line.

Regards,
Richard Byfield
Manager
Centre for Critical Infrastructure Protection

Contents

[Operations Centre Activity](#)[CCIP Recent Alerts & Advisories](#)[CCIP e-Bulletins](#)[Virus Activity](#)[Virus Distribution](#)[Internet Response Times](#)[Website Defacements](#)[Contact Details & Disclaimer](#)

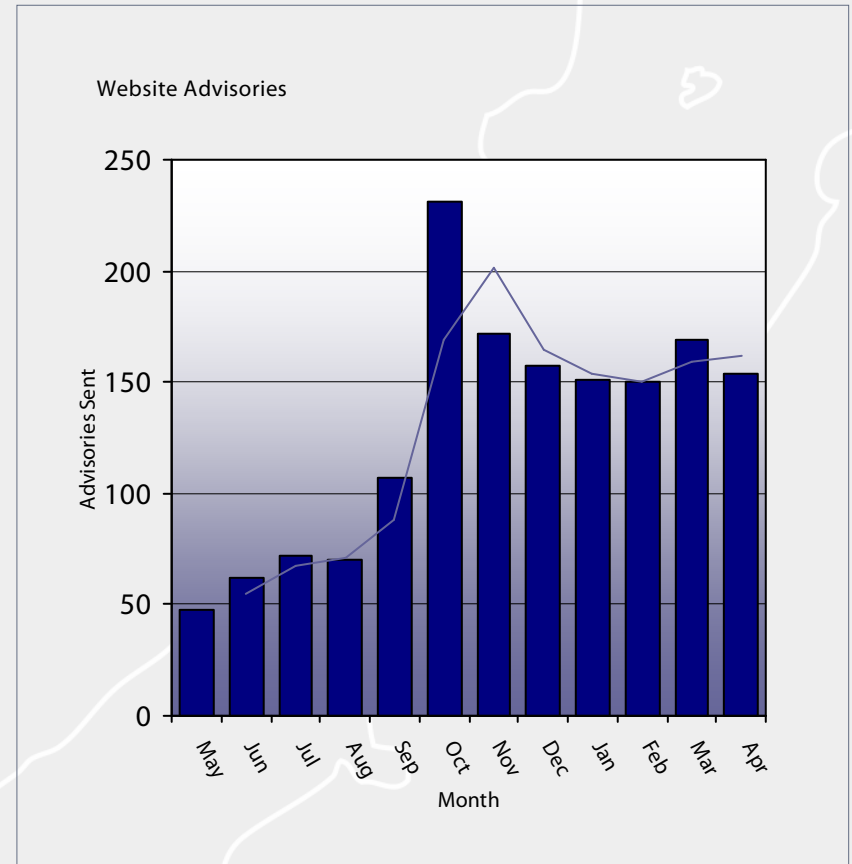
Operations Centre Activity

April saw a total of 154 advisories posted by the CCIP Operations Centre, slightly down on last months total which stood at 169. The number of advisories that were deemed to be of significant importance for April was again high, standing at 21 significant advisories.

Advisories of major significance during the month included a number of planned security updates for Microsoft, along with various other vendors.

Alerts sent directly via the CCIP mailing lists throughout March were the highest recorded to date, with 18 alerts being sent out.

The graph to the right represents the number of advisories posted by the CCIP Operations Centre over the last 12 months.



Question :- What is the difference between an **Advisory** and **Alert**?

Answer :- An **Advisory** is a summary of a vulnerability or patch, and is posted by the CCIP Operations team on the CCIP website.

An **Alert** is an advisory that the CCIP Operations team has deemed to be of significant importance and is posted directly to subscribers via the mailing list in addition to being posted on the CCIP website.

CCIP Recent Alerts and Advisories

The following table shows significant advisories posted by the CCIP Operations Centre during the month of April.

Date	Detail	Source
30/04/07	Update for java-1.4.2-ibm	Sun
26/04/07	QuickTime Java Handling Unspecified Code Execution	Red Hat
23/04/07	VPN Router Security	Apple
20/04/07	Updates for Multiple Vulnerabilities	Nortel
20/04/07	Solaris Mozilla 1.7 Vulnerabilities	Sun
19/04/07	Multiple Vulnerabilities	Oracle
18/04/07	New Rinbot Variant Attempting to Exploit Microsoft Windows DNS RPC Vulnerability	US-CERT
18/04/07	Firefox Wizz RSS News Reader Extension Cross-Context Scripting	Mozilla
18/04/07	Update for openoffice and openoffice-bin	Gentoo
16/04/07	Windows DNS Service Buffer Overflow Vulnerability	Microsoft
11/04/07	MS07-018: Content Management Server Two Vulnerabilities	Microsoft
11/04/07	MS07-020: Agent URL Parsing Memory Corruption Vulnerability	Microsoft
11/04/07	MS07-019: Windows XP UPnP Memory Corruption Vulnerability	Microsoft
10/04/07	IBM OpenSSH for AIX Two Vulnerabilities	Secunia
10/04/07	Firefox Firebug Extension "console.log()" Cross-ContextScripting	Mozilla
10/04/07	Products Multiple Vulnerabilities	Kaspersky
05/04/07	Multiple Vulnerabilities	Netscape
05/04/07	Messenger AudioConf ActiveX Control Buffer Overflow	Yahoo!
04/04/07	MS07-017 - Vulnerability in GDI Could Allow Remote Code Execution (925902)	Microsoft
03/04/07	Solaris Mozilla 1.7 Vulnerability	Sun
02/04/07	Windows Animated Cursor Handling Vulnerability	Microsoft

The above list is an outline of significant advisories posted by the CCIP Operations Centre during the past month, and is not a full representation of all posted advisories.

For a comprehensive list of Alerts and Advisories, Please visit the [Alerts and Advisories](#) page of the CCIP Website.

CCIP e-Bulletins

During the month of April, CCIP released two e-Bulletins. Links to recent issues of the e-Bulletin and samples of topics included are detailed below.

- [Issue 37 ~ 13 April 2007](#)
 - Attack of the Bots
 - Old-Timers Top Malware Chart but Web-Based Threats Pose Greater Problems
 - Schneier says Full Disclosure of Vulns a 'Damned Good Idea'
 - The Current State of PHP Security (w/ MOPB full review)
 - Free AntiRootkit Software
 - The Security Risks of Google Notebook
- [Issue 38 ~ 27 April 2007](#)
 - Internet Security Threat Report
 - Image Spam: Getting the Picture?
 - Notes on Vista Forensics
 - The Future of Security
 - First Workshop on Hot Topics in Understanding Botnets (HotBots '07)
 - Profile of a Fraudster Survey 2007

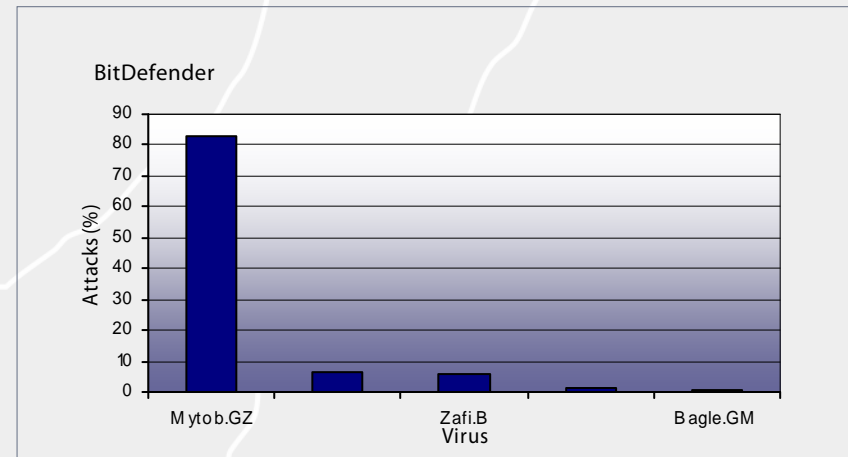
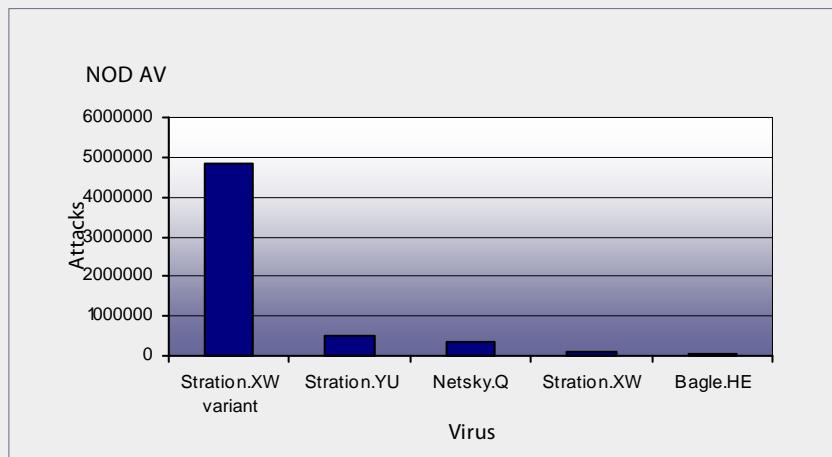
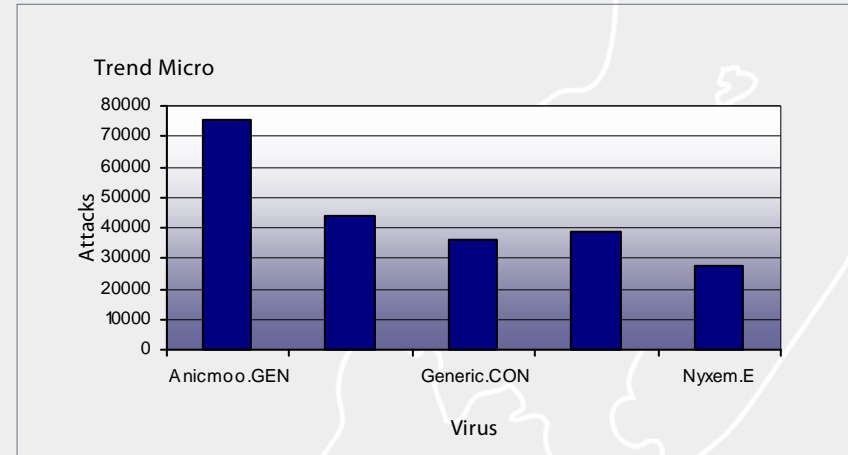
e-Bulletins are sent to members of the CCIP mailing lists. Back issues can be obtained by visiting the [Publications](#) page of the CCIP website.

Virus Activity

The graphs on this page outline the top five recorded viruses, and their recorded attacks over the past month as outlined by TrendMicro, BitDefender and NOD AV.

For more information regarding viruses, including how and in what format they are recorded please refer to the following websites:

- [Trend Micro](#)
- [Bit Defender](#)
- [NOD AV](#)



Virus Distribution

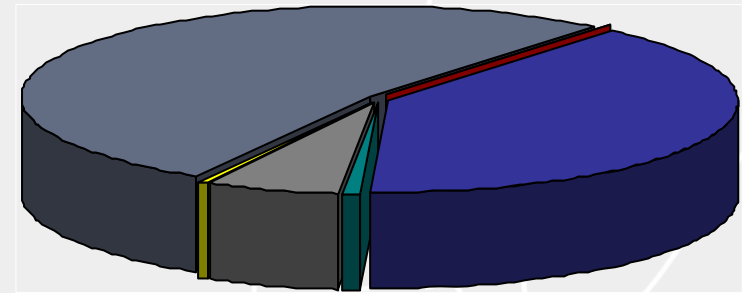
The Australasian region profile on the virus front increased slightly in April. There were a total of 111,521 viruses detected in the Australasian region by Trend Micro during the month, an increase on the March total of 109,964 detected viruses. The percentage of detected viruses in the region on the worldwide scale remained low at a level of 0.60%, an increase on last months level of 0.44%. The number of viruses detected in all regions was relatively lower than March, indicating that activity is steady.

The graph to the right outlines the regional distribution of recorded viruses for the past month as outlined by TrendMicro.

For more information regarding viruses, and regional distributions, please refer to the [Trend Micro](#) website.

Note:- The figures are based upon the statistics gathered by Trend Micro only and do not represent a comprehensive profile of the regional distribution of virus activity.

Regional Distribution



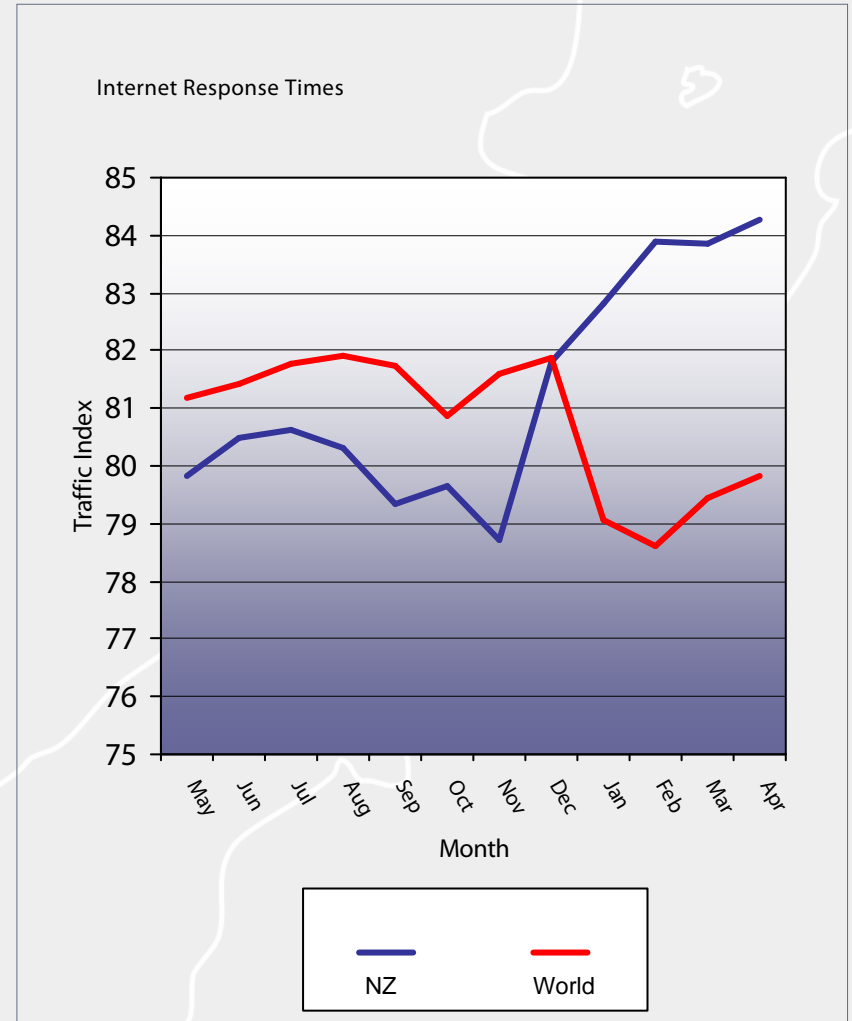
■	11,525	Unknown	0.06%
■	7,261,535	North America	39.22%
■	176,935	South America	0.96%
■	1,086,362	Europe	5.87%
■	111,521	Australasia	0.60%
■	9,672,036	Asia	52.24%
■	14,956	Africa	0.08%

Internet Response Times

Internet response times increased again in April, following on from a recent history of positive results. The average response time was 150ms with an overall Traffic Index of 84.2. This compared to the world average Traffic Index of 79.8 and reinforces the statistics that show New Zealand's Internet performance has continued to trend upwards since November 2006.

The graph to the right represents the response time of a New Zealand monitored router (b2.sxb.tsnz.net - 203.98.39.129) as a traffic index. The higher the index, the lower the response time, and therefore representing better performance and reliability of the connection.

For more information regarding Internet Response Times, Please refer to the [Internet Traffic Report](#) website.

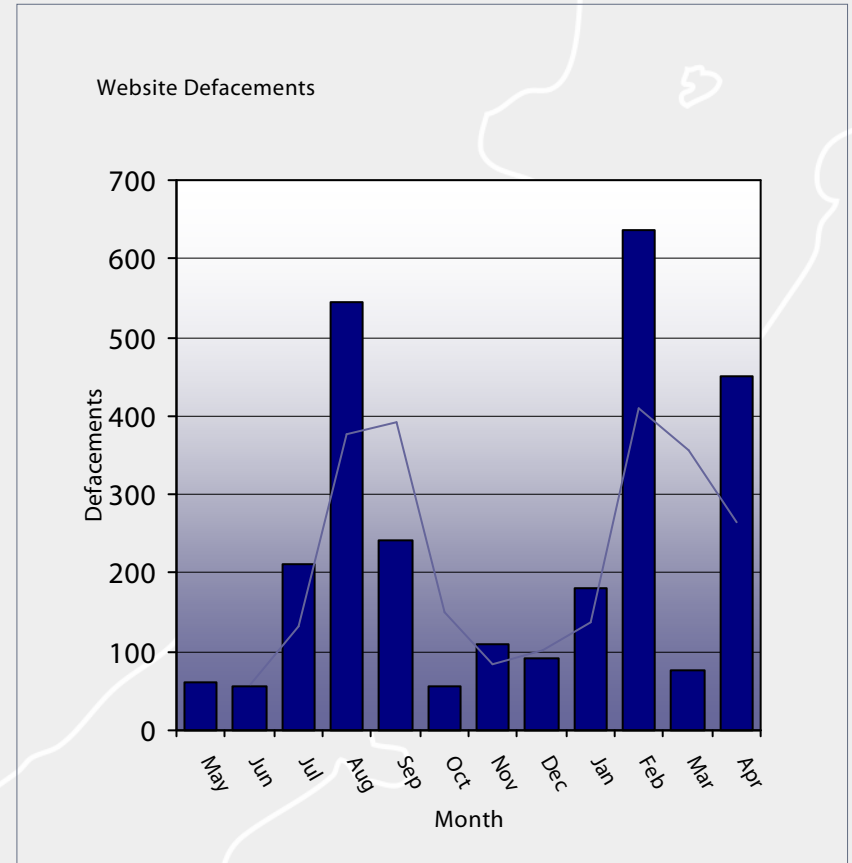


Website Defacements

April again saw a high number of reported website defacements. There were 450 reports logged, after last months low number which stood at 77 reports. As a result of the recent upsurge, the average reports of New Zealand websites being defaced has grown to 226 defacements per month.

The graph to the right indicates the number of reported website defacements against New Zealand sites recorded by the CCIP Operations Centre during the past 12 months.

For more information regarding website defacements, please refer to the [Zone-H](#) website.



Contact Details & Disclaimer

Centre for Critical Infrastructure Protection (CCIP)

PO Box 12209
Thorndon
Wellington 6144

Phone: +64 4 498-7654
Fax: +64 4 498-7655
Email: info@ccip.govt.nz
Web: www.ccip.govt.nz

Subscribe/Unsubscribe to the CCIP Monthly Report

To subscribe to Significant Alerts & Advisories, CCIP Monthly Reports, CCIP e-Bulletins and other correspondence send a blank email with 'Subscribe' in the subject line to publications@ccip.govt.nz

Please include the following details in subscription emails.

First Name, Last Name, Organisation and Contact Number.

To unsubscribe from CCIP publications send a blank email with 'Unsubscribe' in the subject line to publications@ccip.govt.nz

Disclaimer

CCIP does not accept any responsibility for errors or omissions. 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 report. Reference in the report in any manner to any commercial product, process or service does not constitute or imply its endorsement or recommendation by CCIP. Views and opinions expressed in this report may not be used for advertising or product endorsement purposes.