

CCIP Monthly Report for MARCH

Welcome to the March 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	Virus Distribution
CCIP Recent Alerts & Advisories	Internet Response Times
CCIP e-Bulletins	Website Defacements
Virus Activity	Contact Details & Disclaimer

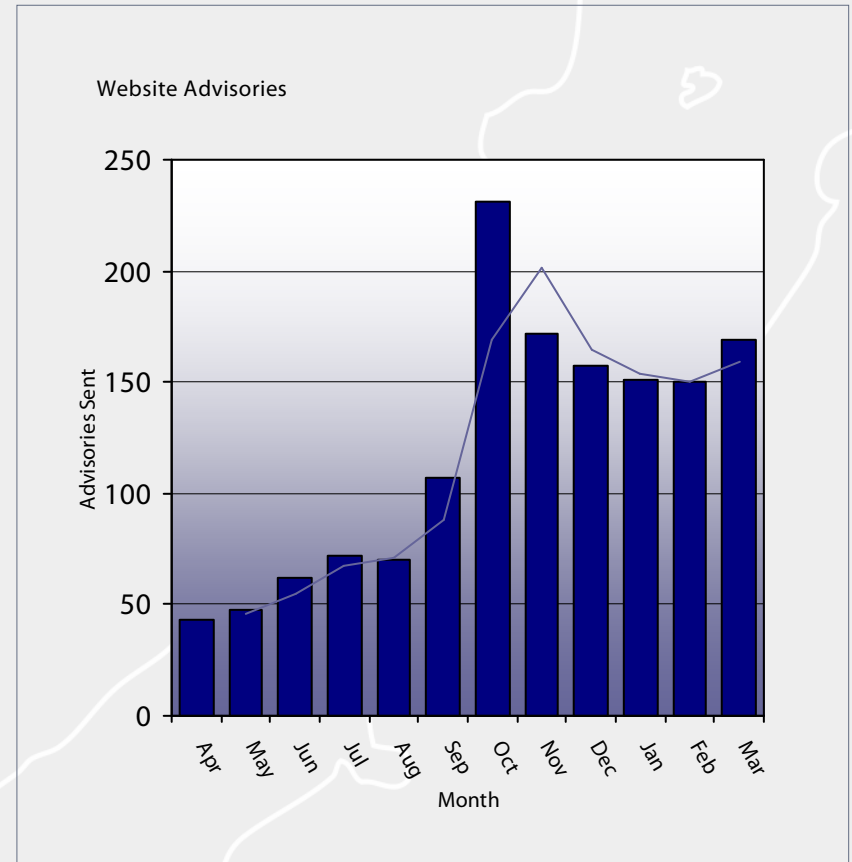
Operations Centre Activity

There were a total of 169 advisories posted by the CCIP Operations Centre during the month of March, an increase on last months total of 150. The number of advisories that were deemed to be of significant importance for March was one up on last months figure, and the highest recorded to date, standing at 22 significant advisories.

Advisories of major significance during the month included a number of updates for Mozilla products, such as Thunderbird, Firefox, and Seamonkey. Microsoft did not release any security bulletins for the month of March.

Alerts sent directly via the CCIP mailing lists throughout March were also high, with 8 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 March.

Date	Detail	Source
28/03/06	Two Vulnerabilities	StarOffice
23/03/07	update for openoffice.org	Red Hat
22/03/07	Multiple Vulnerabilities	OpenOffice.org
22/03/07	Update for php	Gentoo
21/03/07	Update for Mozilla Thunderbird and seamonkey	SUSE
20/03/07	Update for thunderbird	Gentoo
16/03/07	Solaris Adobe Acrobat Multiple Vulnerabilities	Sun
15/03/07	OS X Security Update Fixes Multiple Vulnerabilities	Mac
09/03/07	Netmail WebAdmin Long Username Buffer Overflow	Novell
08/03/07	Update for Mozilla Firefox and seamonkey	SUSE
08/03/07	Update for thunderbird	Mandriva
08/03/07	Update for thunderbird	Ubuntu
07/03/07	QuickTime Multiple Vulnerabilities	Apple
06/03/07	Multiple Vulnerabilities in mozilla and mozilla-bin	Gentoo
06/03/07	Update for mozilla-firefox and mozilla-firefox-bin	Gentoo
06/03/07	Update for thunderbird	Red Hat
06/03/07	Tomcat JK Web Server Connector Long URL Buffer Overflow	Apache
06/03/07	Command Execution and PHP "eval()" Injection	WordPress
05/03/07	Update for snort	Gentoo
05/03/07	Mail Security for SMTP Unspecified Message Handling Vulnerability	Symantec
02/03/07	Update for firefox	Fedora

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 March, CCIP released three e-Bulletins. Links to recent issues of the e-Bulletin and samples of topics included are detailed below.

- [Issue 34 ~ 2 March 2007](#)
 - Application for a New 2LD - bank.nz
 - Google Desktop Hole Closed - For Now
 - Self-Healing Networks, Myth or Reality?
 - How Does the Hacker Economy Work?
- [Issue 35 ~ 16 March 2007](#)
 - Drive-By Pharming
 - Password Malpractice: Are You Guilty?
 - Read RSS, Get Hacked
 - Improving the Intelligence of Your Gateway Security
- [Issue 36 ~ 30 March 2007](#)
 - 50 Things I Wish I'd Known Before... Becoming a CIO
 - Internet Security Threat Report
 - Malware Disrupts Half Of Global Business, Study Finds

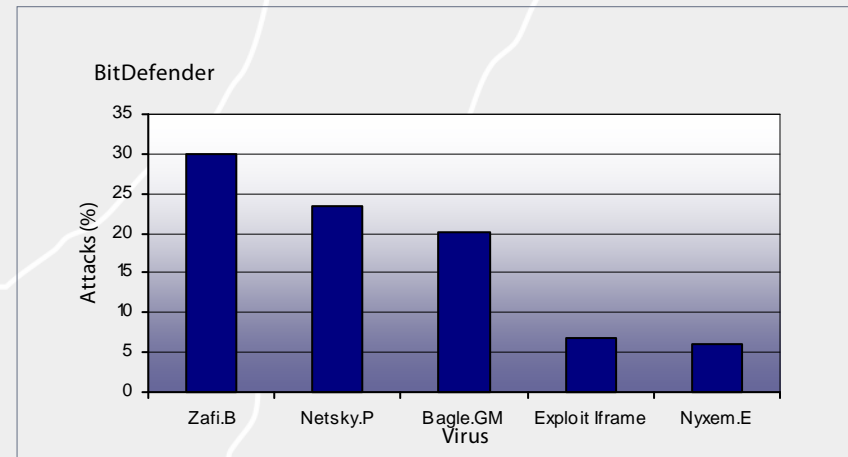
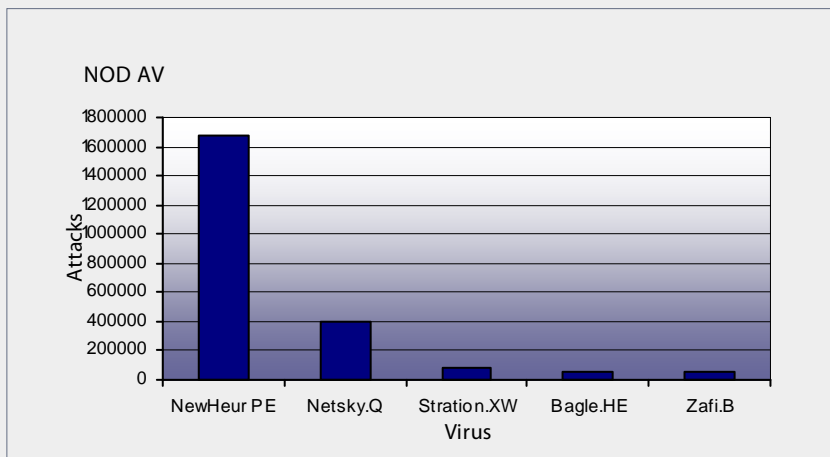
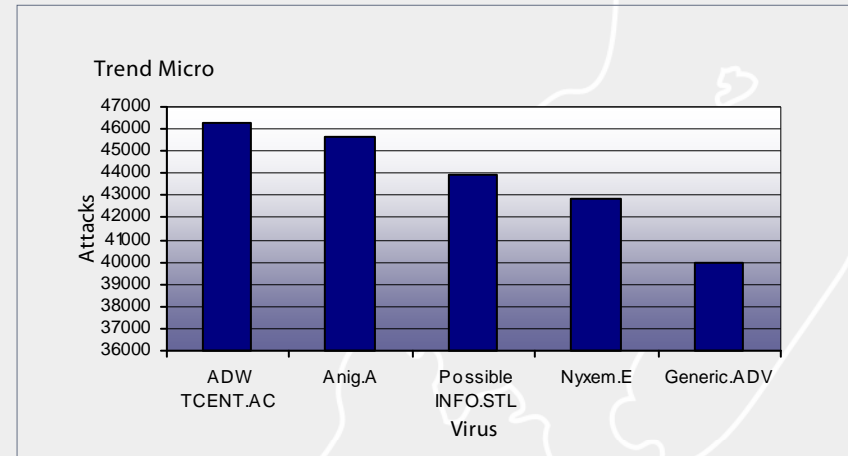
e-Bulletins are sent to members of the CCIP mailing lists. Back issues can be obtained by visiting the [Publications](#) page of the CCIP website.

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

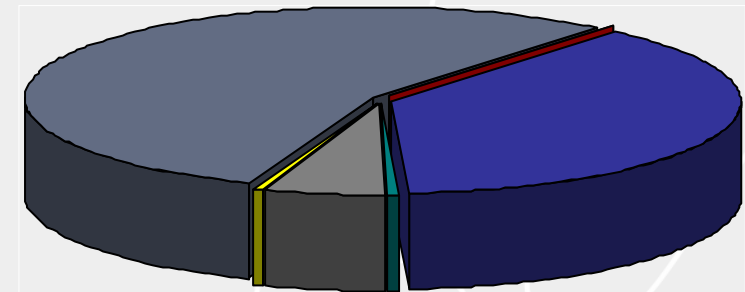
The Australasian region profile on the virus front again decreased in March, despite a higher number of detected viruses for the month. There were a total of 109,964 viruses detected in the Australasian region by Trend Micro during the month, an increase on the February figure of 108,591 detected viruses. Despite the higher number of detected viruses, the percentage of detected viruses in the region on the worldwide scale remained low at a level of 0.44%, a decrease on last months level of 0.63%. The number of viruses detected in all regions was also relatively higher than February, indicating that activity is again on the rise. The number of detects in the Asian region took another huge increase throughout March, which now stands at a level of 54.92% of all virus detections by Trend Micro.

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



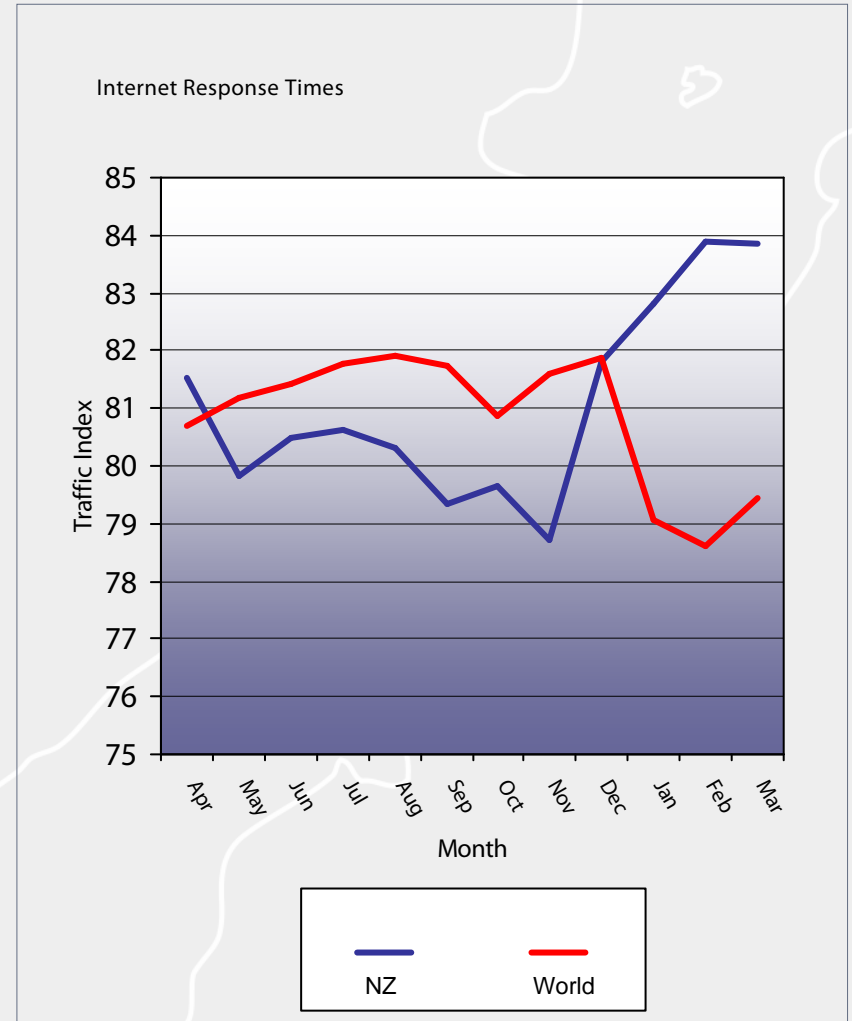
■	15,063	Unknown	0.06%
■	9,457,023	North America	37.62%
■	154,869	South America	0.62%
■	1,412,718	Europe	5.62%
■	109,964	Australasia	0.44%
■	13,804,530	Asia	54.92%
■	14,466	Africa	0.06%

Internet Response Times

Internet response times again remained high throughout the month of March following on from the positive results of the previous three months. The March response times remained relatively the same as last month. The average response time was 151ms with an overall Traffic Index of 83.9. This 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.

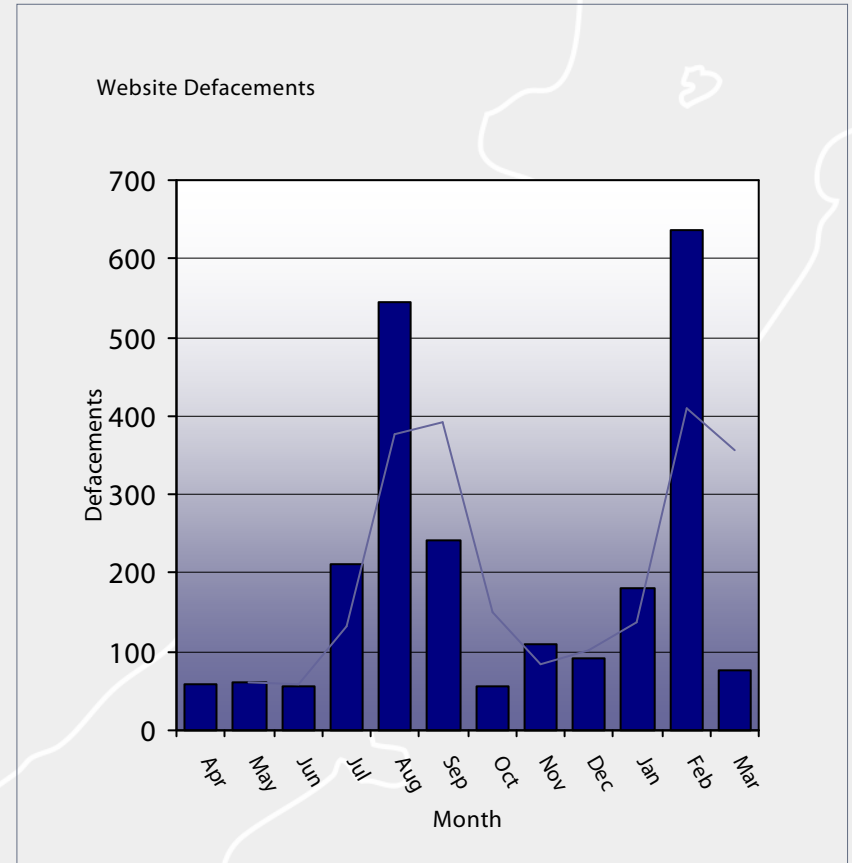


Website Defacements

Reported defacements of New Zealand websites for the month of March decreased significantly on the recent upsurge in high figures. There were a total of 77 reported defacements of New Zealand websites throughout March, down from last months record setting figure of 637 reports. As a result of the recent upsurge, the average reports of New Zealand websites being defaced has increased to 193 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.