

CCIP Monthly Report for MAY

Welcome to the May 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](#)

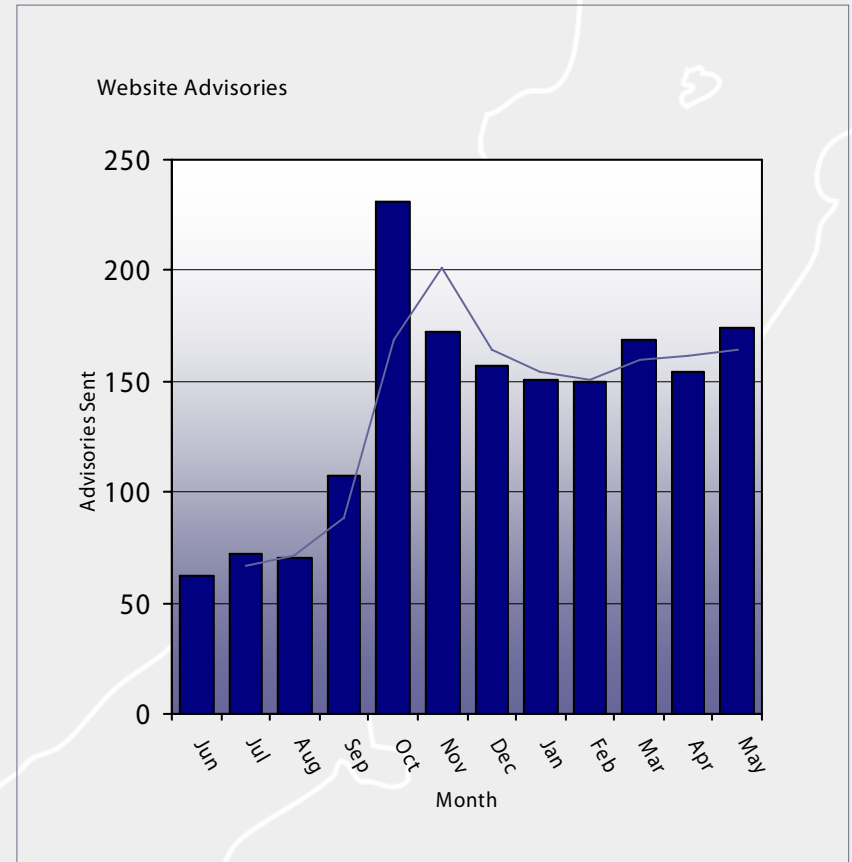
Operations Centre Activity

There were a total of 174 advisories posted by the CCIP Operations Centre during the month of May, up from last months figure of 154 advisories. The number of advisories that were deemed to be of significant importance for April was again high, standing at 15 significant advisories.

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

Alerts sent directly via the CCIP mailing lists throughout March were extremely low, with only 1 alert being sent out relating to multiple vulnerabilities in PHP.

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 May.

Date	Detail	Source
29/05/07	Java System Web Proxy Server SOCKS Module Buffer Overflows	Sun
28/05/07	Mac OS X Security Update for Multiple Vulnerabilities	Apple
21/05/07	Update for PhpWiki	Gentoo
10/05/07	Red Hat update for php	Red Hat
10/05/07	DB2 Universal Database Unspecified Code Execution Vulnerability	IBM
10/05/07	SecurityCenter Subscription Manager ActiveX Control Buffer Overflow	McAfee
10/05/07	Explorer Multiple Vulnerabilities	Internet
10/05/07	Exchange Multiple Vulnerabilities	Microsoft
09/05/07	Internet Explorer Multiple Vulnerabilities	Microsoft
09/05/07	Microsoft Exchange Multiple Vulnerabilities	Microsoft
09/05/07	Excel Three Code Execution Vulnerabilities	Microsoft
09/05/07	Office Drawing Object Code Execution Vulnerability	Microsoft
09/05/07	TAL Bar Code ActiveX Control Buffer Overflow Vulnerability	Secunia
03/05/07	Multiple Vulnerabilities	PHP
03/05/07	Java System Directory Server Denial of Service	Sun

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

- [Issue 39 ~ 16 May 2007](#)
 - Coalition of Security Leaders Announces First Secure Coding Assessment and Certification Exams for Programmers
 - CERT's Podcast Series: Security for Business Leaders
 - Animated Cursor Security Bug
 - How to Establish and Enforce a Wireless Security Policy
 - Building A Web-Based Neighbourhood Watch
 - Fraud: One of the Greatest Risks to a Company's Reputation & Viability
 - Blended Threats Considerations
 - NIST Issues Guidelines for Ensuring RFID Security
 - Google Searches Web's Dark Side

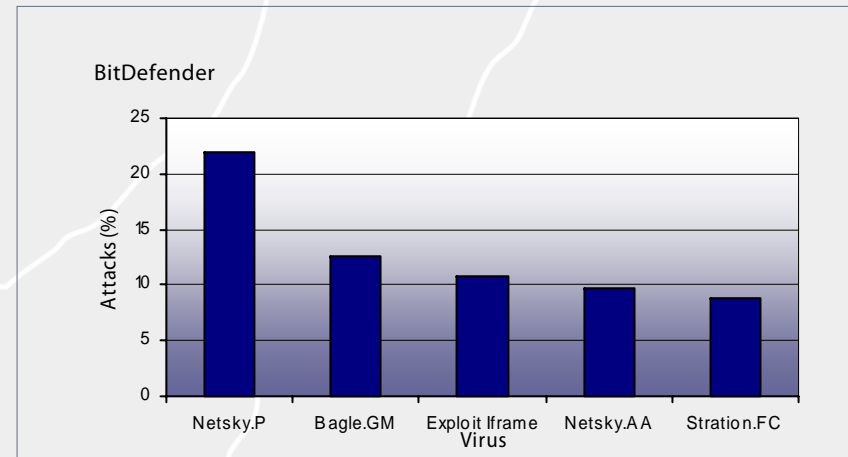
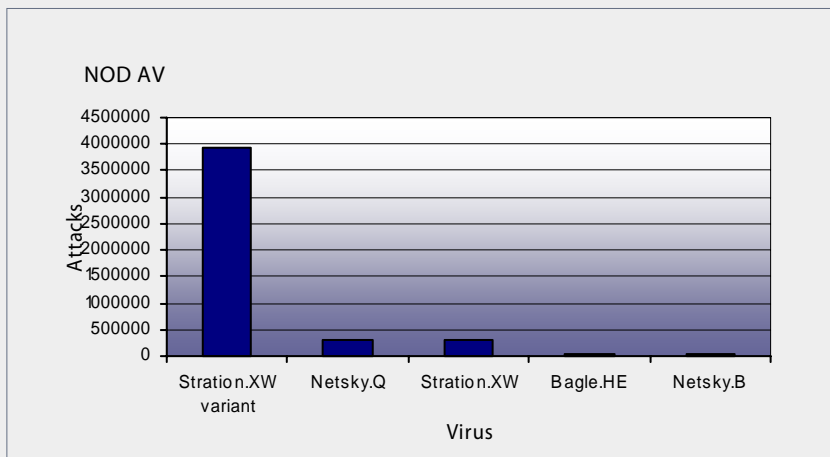
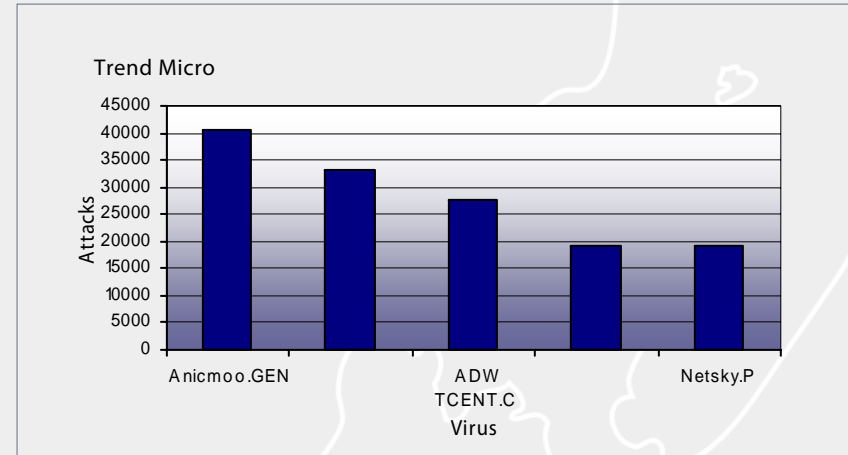
e-Bulletins are sent to members of the CCIP mailing lists. Back issues can be obtained by visiting the [Publications](#) page of the CCIP website.

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

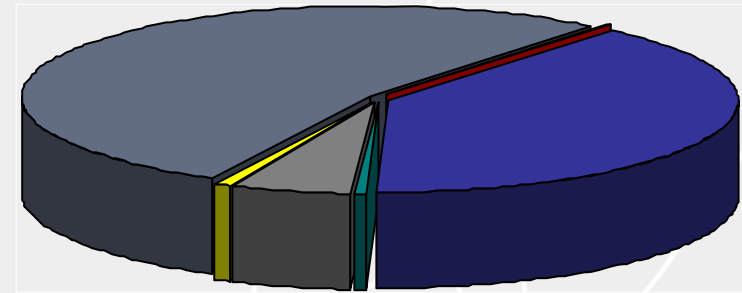
The Australasian region profile on the virus front increased slightly in May. There were a total of 95,552 viruses detected during May, slightly down on the April figure of 111,521 but the percentage of detected viruses worldwide increased slightly to 0.68%, up from the April figure of 0.60% of detected viruses worldwide.

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



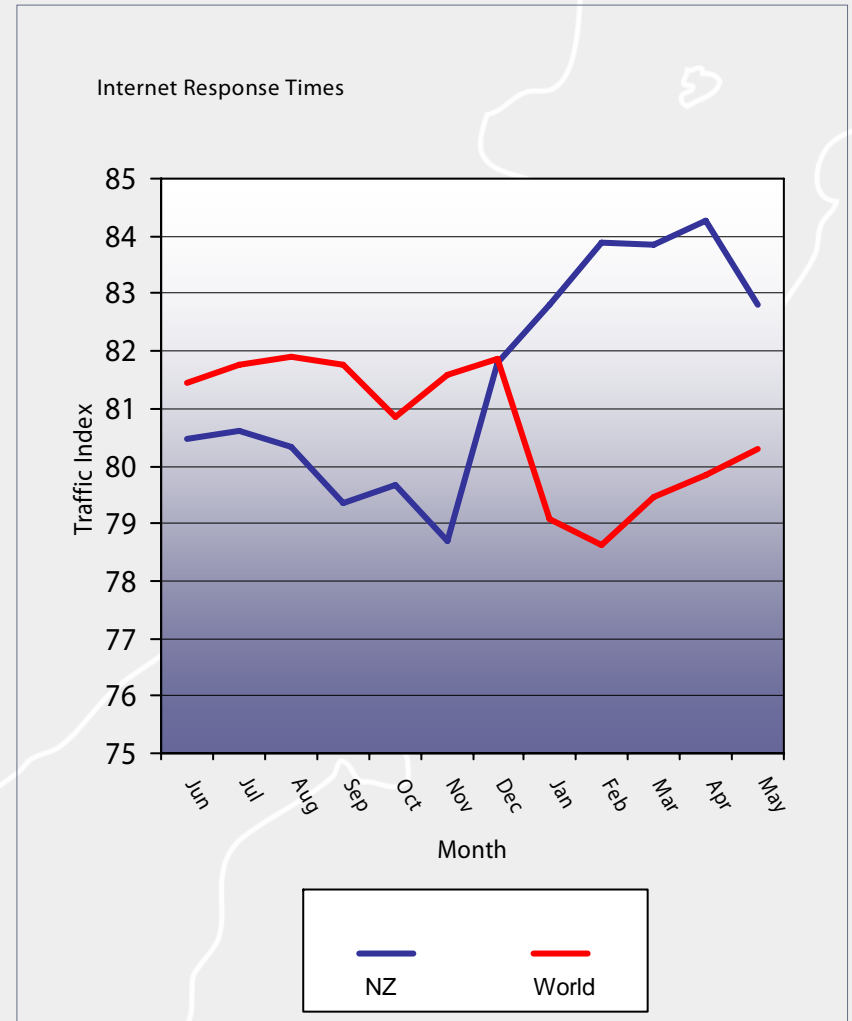
■	14,608	Unknown	0.10%
■	5,489,173	North America	38.83%
■	107,131	South America	0.76%
■	783,844	Europe	5.54%
■	95,552	Australasia	0.68%
■	7,479,670	Asia	52.91%
■	32,559	Africa	0.23%

Internet Response Times

Internet response time figures for New Zealand increased during May, driving the Traffic Index down, and bringing an end to the recent upward trend in New Zealand's Internet Response Times. The average response time was 165ms with an overall Traffic Index of 82.8. This compared to the world average Traffic Index of 80.3.

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.

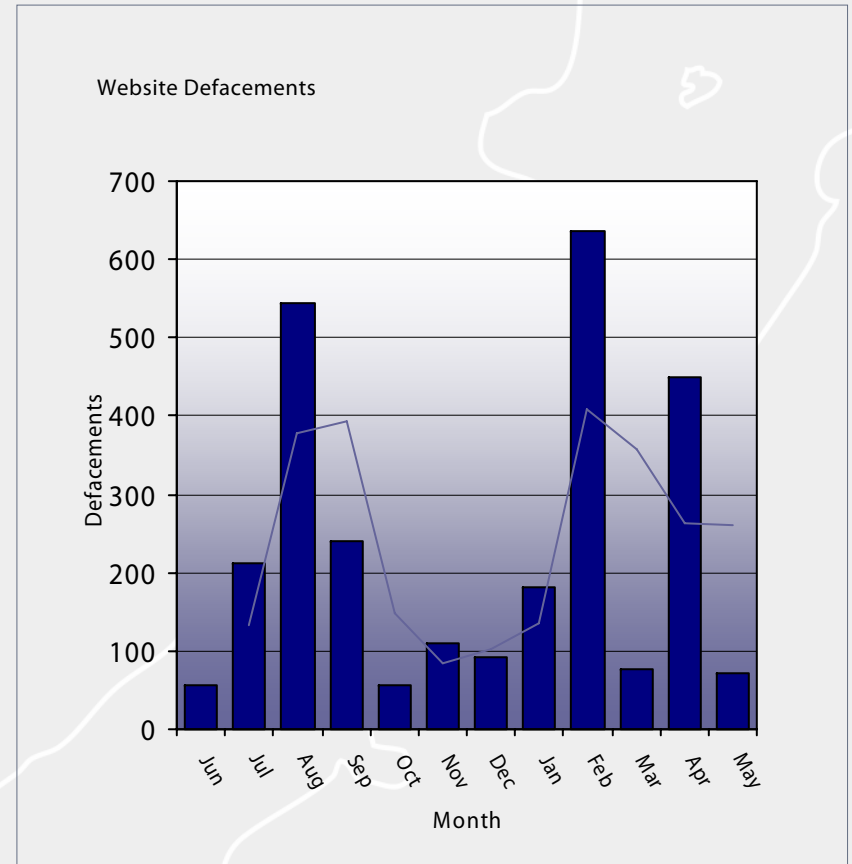


Website Defacements

The number of reported website defacements of May was 71. down from last months upsurge of 450 logged reports. The average number of New Zealand websites being defaced has grown to 227 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.