

# CCIP Monthly Report for JUNE

Welcome to the June 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](mailto:info@ccip.govt.nz) and include "MONTHLY REPORT" in the subject line.

Regards,  
Richard Byfield  
Manager  
Centre for Critical Infrastructure Protection

## Contents

<a href="#">Operations Centre Activity</a>	<a href="#">Virus Distribution</a>
<a href="#">CCIP Recent Alerts &amp; Advisories</a>	<a href="#">Internet Response Times</a>
<a href="#">CCIP e-Bulletins</a>	<a href="#">Website Defacements</a>
<a href="#">Virus Activity</a>	<a href="#">Contact Details &amp; Disclaimer</a>

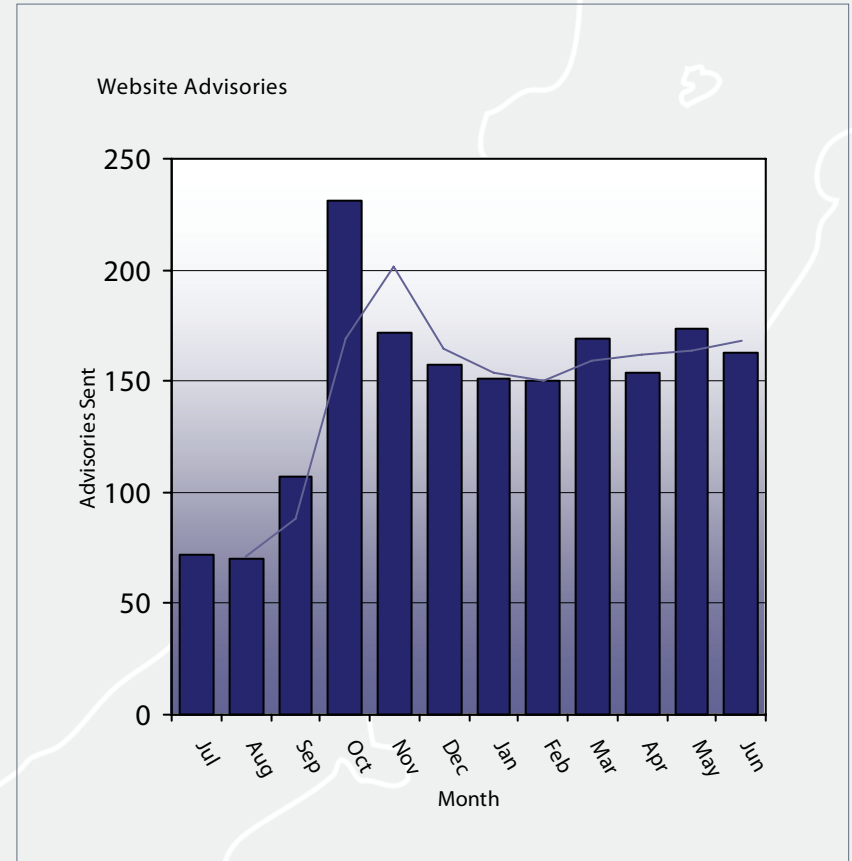
# Operations Centre Activity

Throughout June, there were a total of 163 advisories posted by the CCIP Operations Centre, slightly down from the May total of 174 posted advisories. The number of advisories that were deemed to be of significant importance for June increased, standing at 18 significant advisories.

Advisories of major significance during the month included a number of planned security updates for Microsoft, in addition to advisories from Red Hat and other software vendors..

Alerts sent directly via the CCIP mailing lists throughout June were steady, with 4 alerts being sent out, relating to Red Hat and a PHP vulnerability.

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 June.

Date	Detail	Source
14/06/07	Update for mozilla-firefox	<a href="#">Mandriva</a>
13/06/07	Multiple Vulnerabilities	<a href="#">Internet Explorer</a>
13/06/07	Windows Win32 API Code Execution Vulnerability	<a href="#">Microsoft</a>
13/06/07	Outlook Express and Windows Mail Multiple Vulnerabilities	<a href="#">Microsoft</a>
13/06/07	Secure Channel Digital Signature Parsing Vulnerability	<a href="#">Windows</a>
13/06/07	Visio Two Code Execution Vulnerabilities	<a href="#">Microsoft</a>
11/06/07	Solaris Mozilla 1.7 Vulnerability	<a href="#">Sun</a>
08/06/07	Messenger Two ActiveX Controls Buffer Overflows	<a href="#">Yahoo!</a>
07/06/07	FirePass 4100 SSL VPN "username" Command Injection	<a href="#">F5</a>
07/06/07	Anti-Virus Engine CAB Archive Processing Buffer Overflows	<a href="#">CA</a>
01/06/07	Update for mplayer	<a href="#">Gentoo</a>
01/06/07	Firefox Multiple Vulnerabilities	<a href="#">Mozilla</a>
01/06/07	SeaMonkey Multiple Vulnerabilities	<a href="#">Mozilla</a>
01/06/07	Update for firefox	<a href="#">Red Hat</a>
01/06/07	Update for thunderbird	<a href="#">Red Hat</a>
01/06/07	Update for seamonkey	<a href="#">Red Hat</a>
01/05/07	QuickTime Java Extension Two Vulnerabilities	<a href="#">Apple</a>
01/06/07	System Management Homepage PHP Multiple Vulnerabilities	<a href="#">HP</a>

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

- [Issue 40 ~ 22 June 2007](#)
  - CERT's Resiliency Engineering Research
  - OPERATION: BOT ROAST - 'Bot-herders' Charged
  - February 2007 Root Server Attacks - A Qualitative Report
  - Implementing an Effective Security Strategy
  - Security Analogies Wiki
  - Security Hacks
  - Issues in Using DNS Whois Data for Phishing Site Take Down
  - What is Social Engineering?

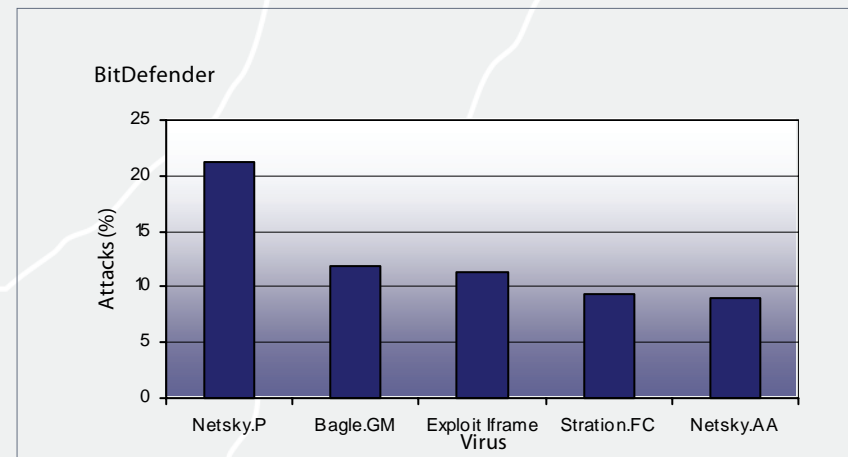
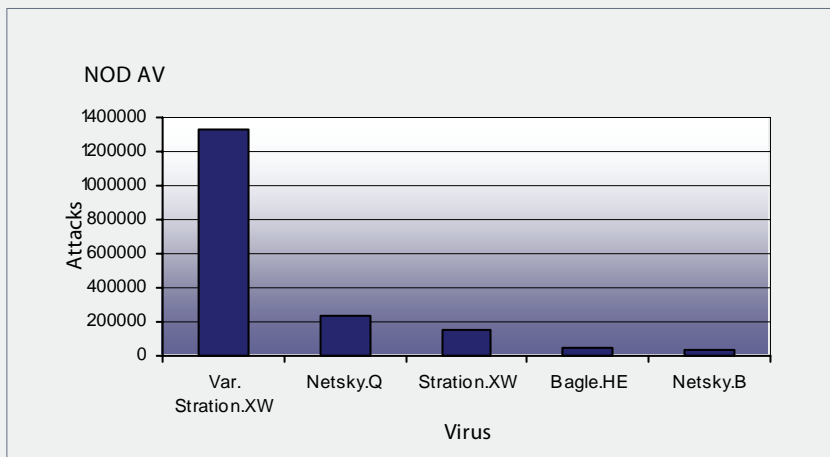
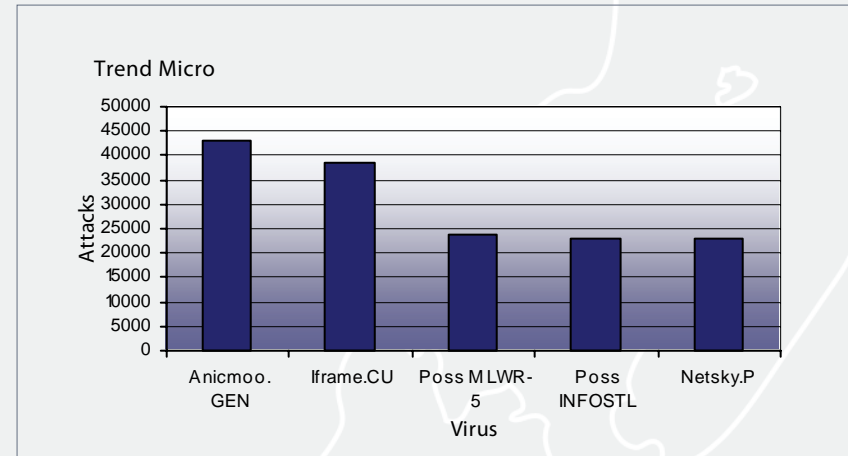
e-Bulletins are sent to members of the CCIP mailing lists. Back issues can be obtained by visiting the [Publications](#) page of the CCIP website.

# 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

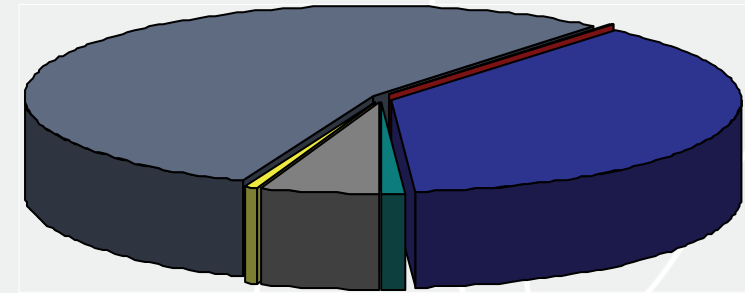
The Australasian region profile on the virus front took a downturn during June. There were a total of 108,183 viruses detected during the month, up from the May figure of 95,552 detected viruses. The percentage of detected viruses worldwide, however, decreased to 0.55% from the May percentage of 0.68% 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



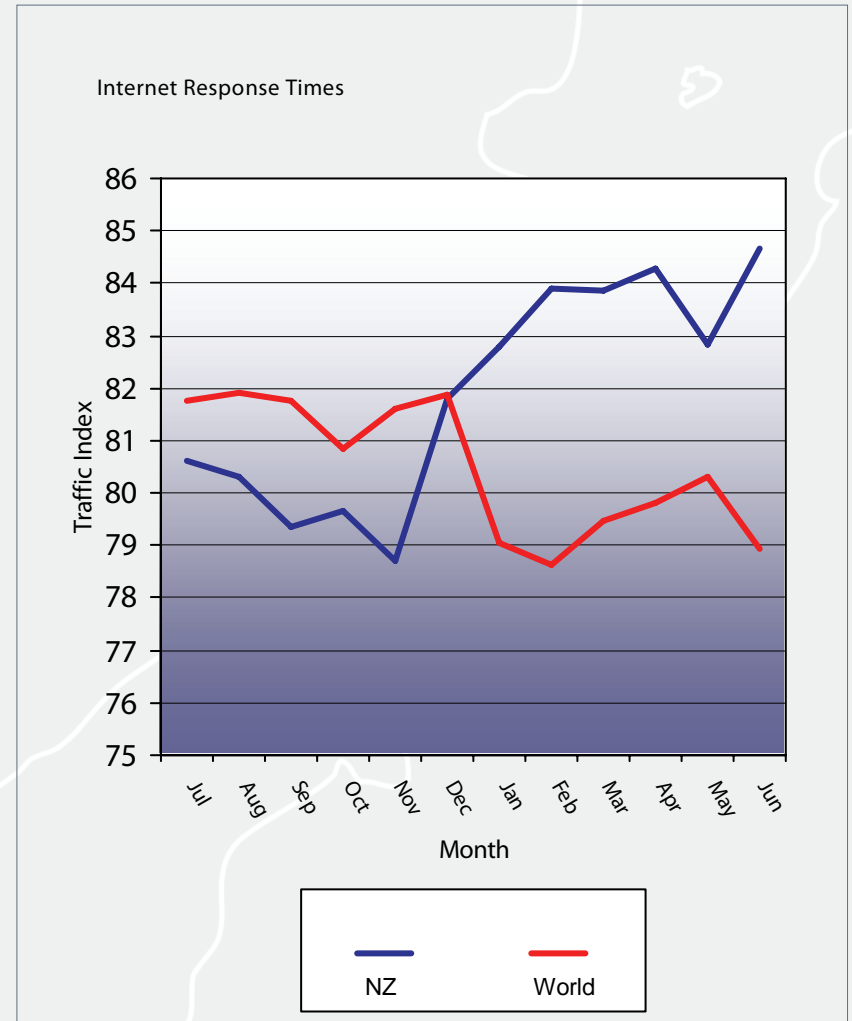
■	14,266	Unknown	0.07%
■	7,349,005	North America	37.39%
■	201,011	South America	1.02%
■	1,101,755	Europe	5.61%
■	108,183	Australasia	0.55%
■	10,617,432	Asia	54.02%
■	51,342	Africa	0.26%

# Internet Response Times

Junes Internet response time figures for New Zealand decreased, driving the Traffic Index upwards. The response time for June was 148ms, down from the May figure of 165ms. This produced a Traffic Index of 84.6, which compared to the May figure of 82.8, shows that the New Zealand profile on Internet Response times is increasing steadily. The world average Traffic Index stands at 78.9 for the month of June.

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.

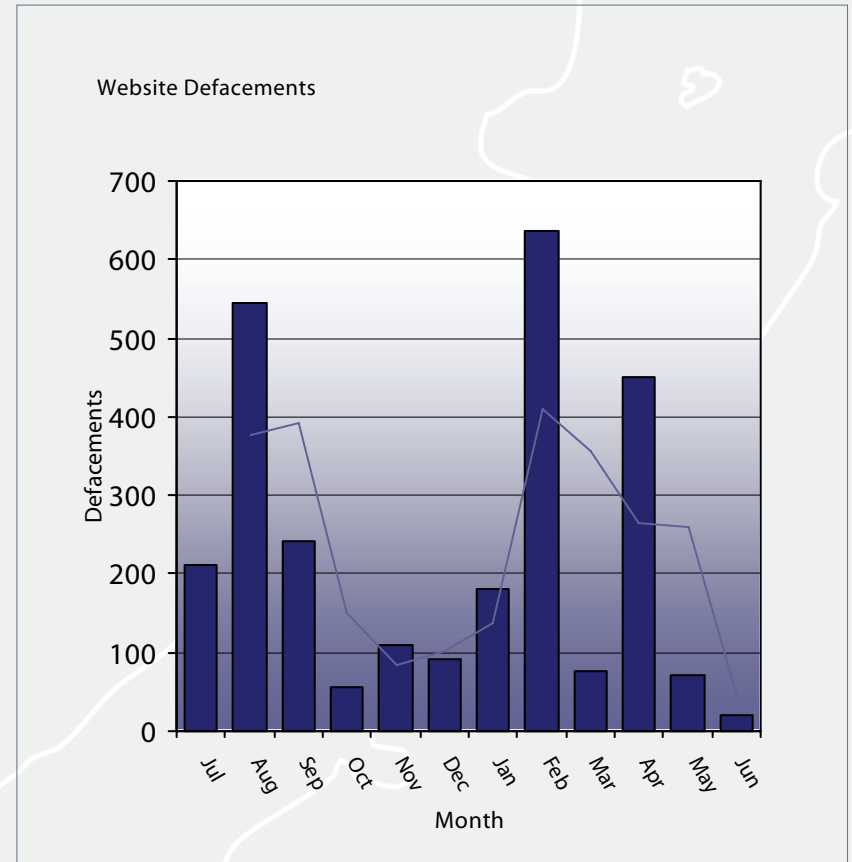


# Website Defacements

Reported website defacements throughout the month of June remained very low, with only 20 reports received. Down on the May figure of 71 reports. The average number of New Zealand websites being defaced has grown to 228 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](mailto:info@ccip.govt.nz)  
Web: [www.ccip.govt.nz](http://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](mailto: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](mailto: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.