

# CCIP Monthly Report for AUGUST

Welcome to the August 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>

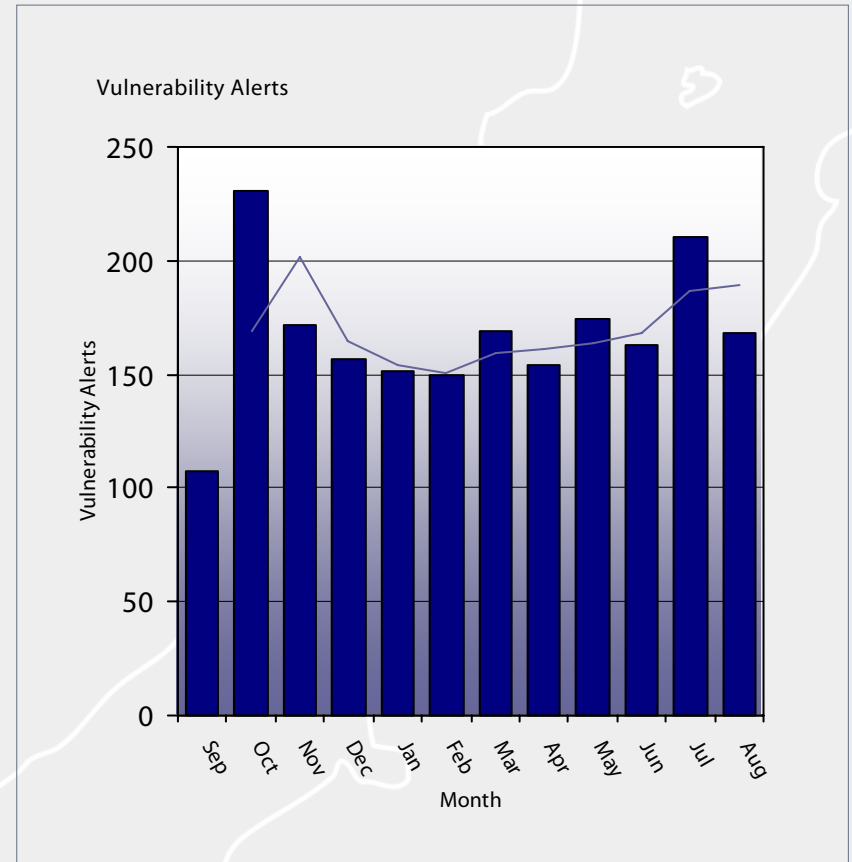
# Operations Centre Activity

August saw the number of Vulnerability Alerts posted to the CCIP website take a slight downturn on last months total, but was still around the average mark. There were a total of 168 Vulnerability Alerts posted during August, compared to the July figure of 210.

Vulnerability Alerts of major significance during the month was quite low, with only 12 being identified. The majority of these stemmed from the planned security updates for Microsoft on the 15th August.

Advisories sent directly via the CCIP mailing lists throughout August decreased significantly, with only 2 Advisories being sent out, relating to Yahoo! and MSN messenger.

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 a **Vulnerability Alert** and an **Advisory**?

**Answer :-** A **Vulnerability Alert** is a summary of a vulnerability or patch, and is released for general public information by the CCIP Operations Centre on the CCIP website.

An **Advisory** is a vulnerability that is deemed by the CCIP Operations Centre to be of significant importance and is posted directly to the CCIP subscribers via mailing lists. In addition, the advisory may be posted on the CCIP website if released for public information.

# CCIP Recent Vulnerability Alerts and Advisories

The following table shows significant Vulnerability Alerts posted by the CCIP Operations Centre during the month of August.

Date	Detail	Source
31/08/07	Messenger YVerInfo.dll ActiveX Control Buffer Overflow	<a href="#">Yahoo!</a>
29/08/07	MSN Messenger Video Conversation Buffer Overflow Vulnerability	<a href="#">Secunia</a>
16/08/07	Update for Mozilla Products	<a href="#">Gentoo</a>
15/08/07	Internet Explorer Multiple Vulnerabilities	<a href="#">Microsoft</a>
15/08/07	XML Core Services Memory Corruption Vulnerability	<a href="#">Microsoft</a>
15/08/07	Windows Vector Markup Language Buffer Overflow	<a href="#">Microsoft</a>
15/08/07	Windows OLE Automation Memory Corruption Vulnerability	<a href="#">Microsoft</a>
15/08/07	Graphics Rendering Engine Image Handling Vulnerability	<a href="#">Microsoft</a>
15/08/07	Excel rtWnDesk Record Memory Corruption Vulnerability	<a href="#">Microsoft</a>
10/08/07	Products NavComUI ActiveX Control Code Execution	<a href="#">Symantec</a>
07/08/07	System Management Homepage Apache and OpenSSL Vulnerabilities	<a href="#">HP</a>
02/08/07	IPhone Multiple Vulnerabilities	<a href="#">Apple</a>

The above list is an outline of significant Vulnerability Alerts posted by the CCIP Operations Centre during the past month, and is not a full representation of all posted Vulnerability Alerts and Advisories. These Vulnerability Alerts reference external site, CCIP cannot be held responsible for these sites content or outdated links. For a comprehensive list of Vulnerability Alerts and Advisories, Please visit the [Vulnerabilities](#) page of the CCIP Website.

# CCIP e-Bulletins

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

- [Issue 43 ~ 3 August 2007](#)
  - Patching the Holes in AJAX Security
  - You Know about XSS. How about XSRF/CSRF?
  - SCADA Honeynets
  - Malware Removal Starter Kit
- [Issue 44 ~ 17 August 2007](#)
  - Government Must Act Now to Maintain Confidence in the Internet
  - The Yin & Yang of Internet Security Research
  - The Evolution of Networks Beyond IP
  - Shared SCADA WAN: Enterprise, Surveillance & VoIP
- [Issue 45 ~ 31 August 2007](#)
  - New Zealand 2007 Daylight Saving Changes
  - Privacy Breach Guidelines
  - Know Your Enemy: Malicious Web Servers
  - When your World is Hacked

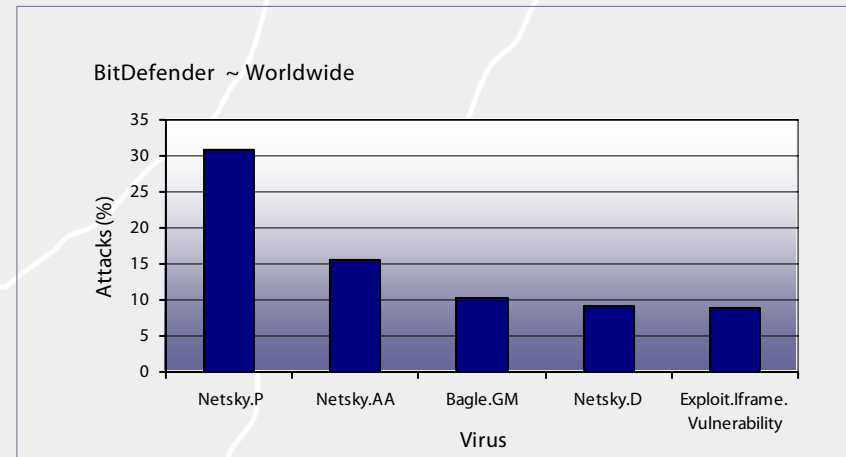
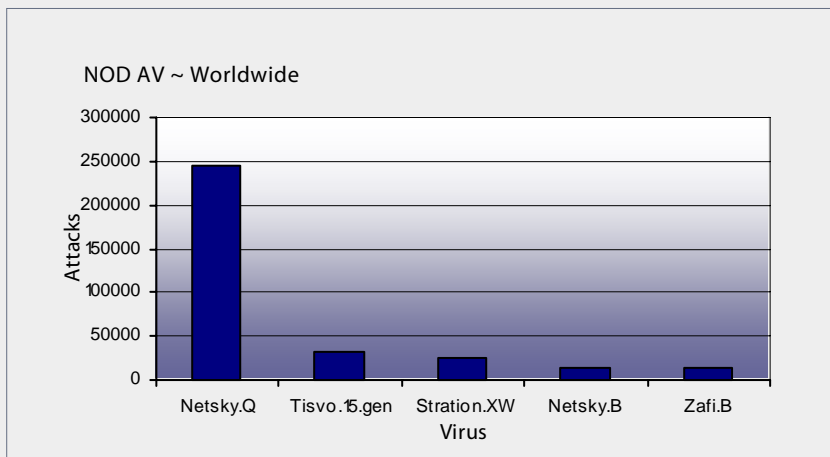
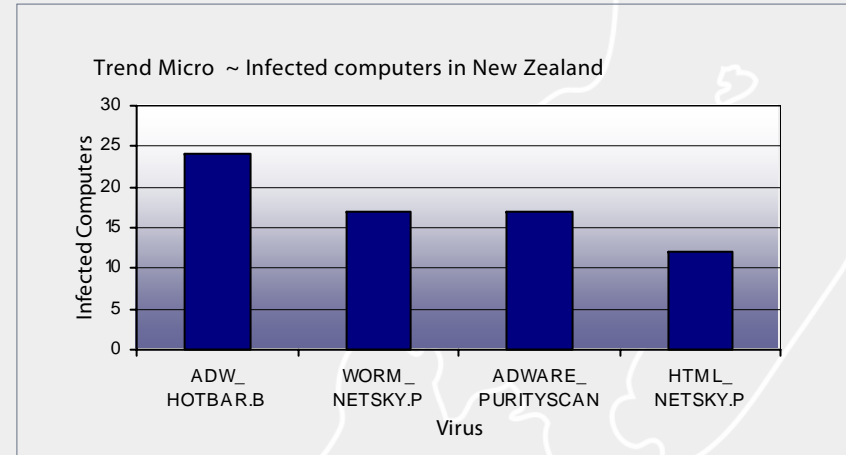
e-Bulletins are sent to members of the CCIP mailing lists. Back issues can be obtained by visiting the [Newsroom](#) page of the CCIP website.

# 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](#)



# Spam Distribution

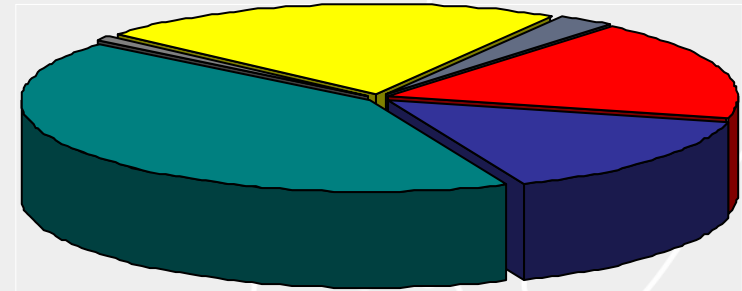
New Zealand's profile on the spam front remained relatively normal for the month of August, with 0.08% of all spam detected worldwide in the region. The Australasian region as a whole experienced 0.63% of all worldwide detected spam. There was a total of 30,186,182 detected spam messages throughout the world by TrendMicro in the month of August.

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

For more information regarding viruses, spam, 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, or spam activity.

Regional Distribution



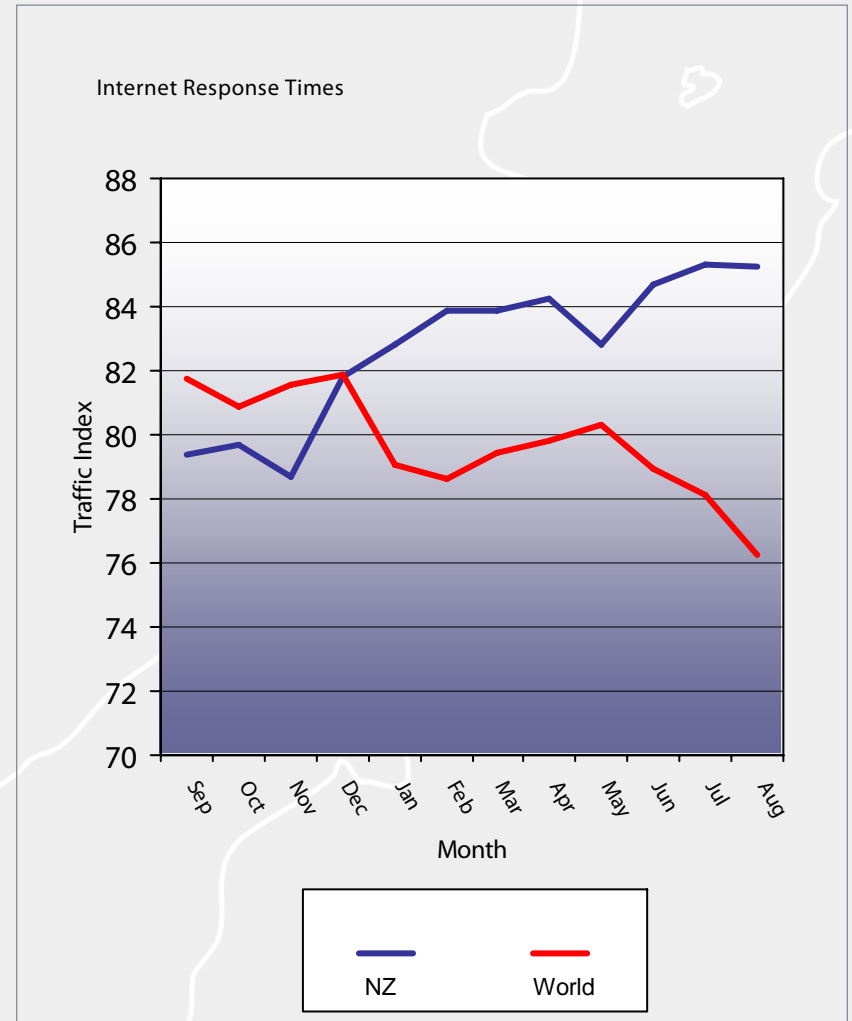
■ North America 15.6%	■ South America 12.93%
■ Europe 36.83%	■ Australasia 0.63%
■ Asia 18.95%	■ Middle East / Africa 2.5%

# Internet Response Times

The difference between Internet response times in New Zealand and the world was increased during the month of August. The average response time in August was 143ms, slightly down on the July total of 142ms. This gave New Zealand an average Traffic Index of 85.3, compared to last months of 85.3.

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.

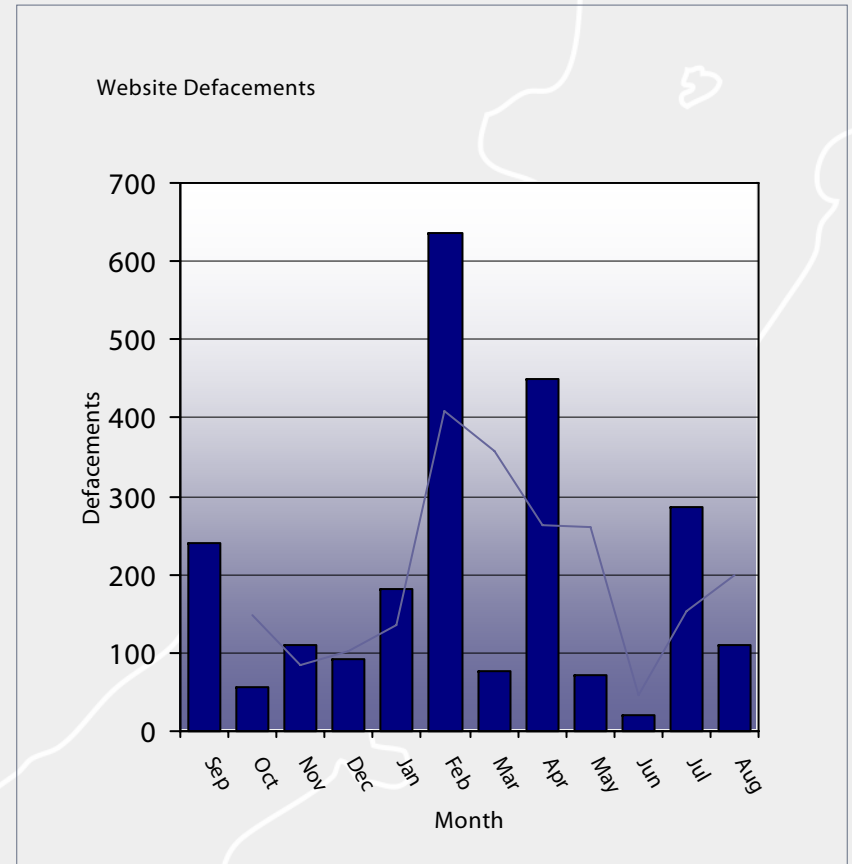


# Website Defacements

Reported website defacements throughout the month of August were down on last month. There were a total of 110 reported website defacements throughout August, and a total of 286 for July.. The average number of New Zealand websites being defaced has grown to 194.5 defacements per month for the last 12 months.

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.