

CCIP Monthly Report for FEBRUARY

Welcome to the February 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

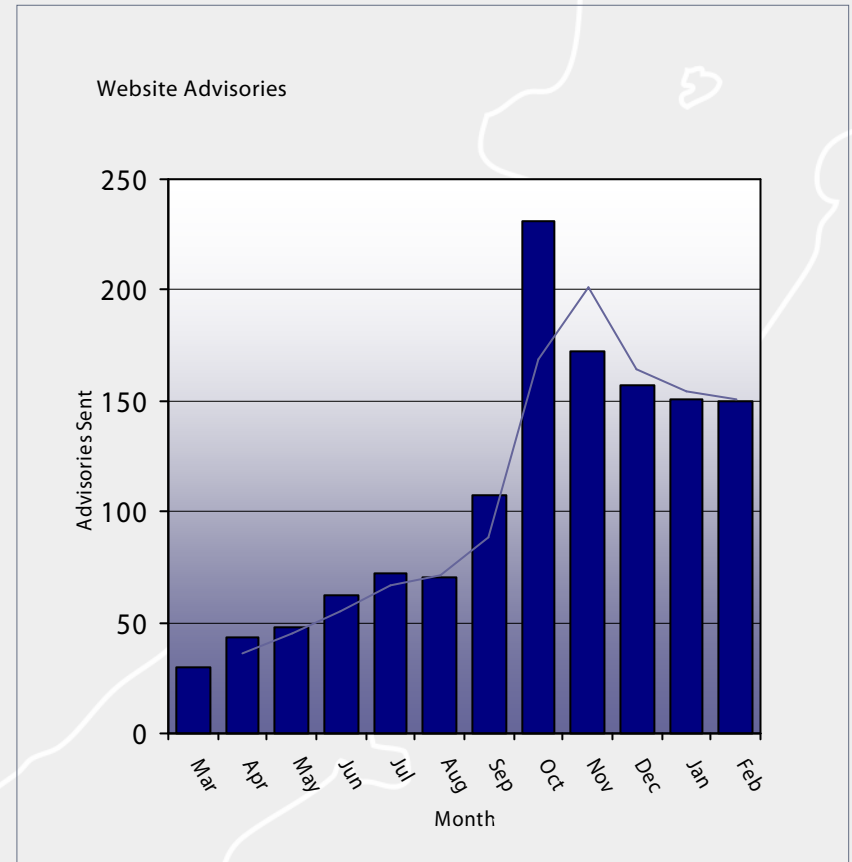
Operations Centre Activity

During the month of February, the CCIP Operations Centre posted 150 advisories, one less than the January total of 151 advisories. The number of advisories that were deemed to be of significant importance for February was the highest recorded to date, standing at 21 significant advisories.

Advisories of major significance during the month included a number of Microsoft security updates relating to Office, Word, and Internet Explorer. Microsoft also had a number of other critical advisories during February. Mozilla also featured highly with a large number of advisories being posted relating to Mozilla products throughout the month.

Alerts sent directly via the CCIP mailing lists throughout February was also the highest ever recorded, with 10 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 February.

Date	Detail	Source
28/02/06	Netscape Multiple Vulnerabilities	Secunia
27/02/07	Update for firefox	Red Hat
26/02/07	Mozilla Thunderbird Multiple Vulnerabilities	Secunia
26/02/07	Mozilla SeaMonkey Multiple Vulnerabilities	Secunia
26/02/07	Mozilla Firefox Multiple Vulnerabilities	Secunia
22/02/07	Threat Protection System DCE/RPC Preprocessor Buffer Overflow	Nortel
22/02/07	Update for koffice	Red Hat
21/02/07	Intrusion Sensor DCE/RPC Preprocessor Buffer Overflow	Sourcefire
21/02/07	DCE/RPC Preprocessor Buffer Overflow	Snort
19/02/07	OfficeScan Client Unspecified ActiveX Buffer Overflow	Trend Micro
17/02/07	Mac OS X Security Update Fixes Multiple Vulnerabilities	Apple
16/02/07	Word Unspecified Memory Corruption Vulnerability	Microsoft
14/02/07	MS07-016: Cumulative Security Update for Internet Explorer	Microsoft
14/02/07	MS07-015: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution	Microsoft
14/02/07	MS07-014: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution	Microsoft
14/02/07	MS07-010: Vulnerability in Microsoft Malware Protection Engine Could Allow Remote Code Execution	Microsoft
14/02/07	MS07-009: Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution	Microsoft
14/02/07	MS07-008: Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution	Microsoft
14/02/07	Solaris Mozilla 1.7 Vulnerabilities	Sun
07/02/07	Office Unspecified String Handling Vulnerability	Microsoft
07/02/07	Update for mozilla-firefox	Debian

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

- [Issue 33 ~ 16 February 2007](#)
 - The Psychology of Security
 - Fundamental Computer Investigation Guide for Windows
 - PHP Security from the Inside
 - Guide to Computer Security Log Management
 - Trends in Malware Threats
 - Organized malware factories threaten Internet users
 - IPv4 Countdown Policy Proposal
 - Hardening Microsoft Windows – STIGS, Baselines, and Compliance

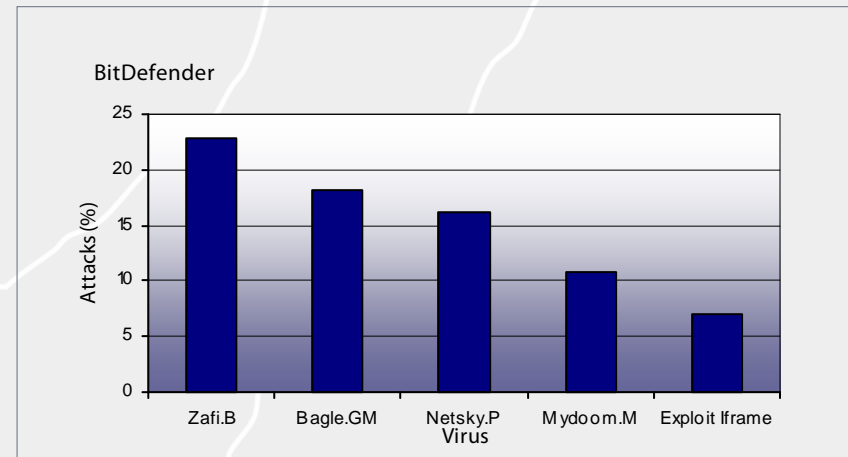
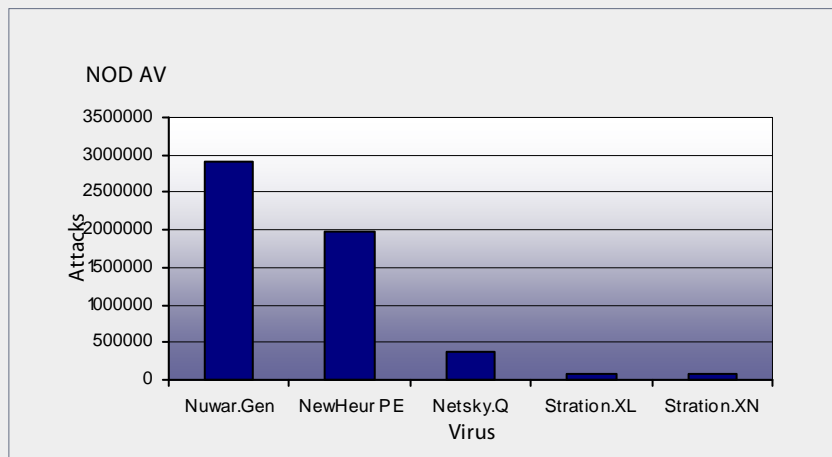
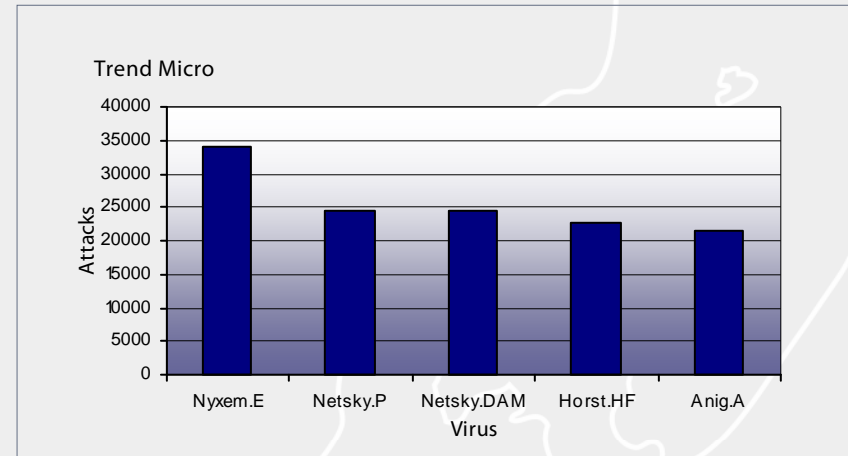
e-Bulletins are sent to members of the CCIP mailing lists. Back issues can be obtained by visiting the [Publications](#) page of the CCIP website.

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

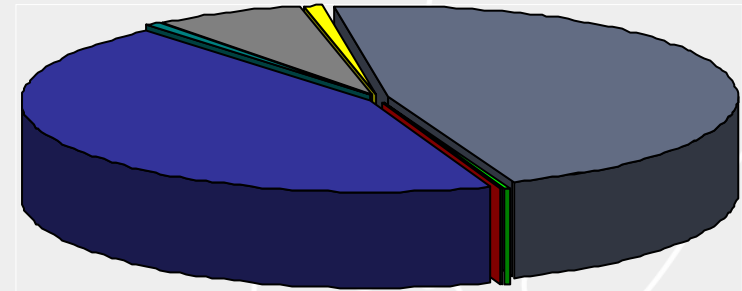
The Australasian region profile on the virus front decreased in February, despite a higher number of detected viruses for the month. There were a total of 108,591 viruses detected in the Australasian region by Trend Micro during the month, an increase on the January figure of 77,549 detected viruses. 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 0.63%, a decrease on last months level of 1.17%. The number of viruses detected in all regions was also relatively higher than January, indicating that activity is again on the rise. The number of detects in the Asian region took a huge increase throughout February, which now stands at a level of 46.47% 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



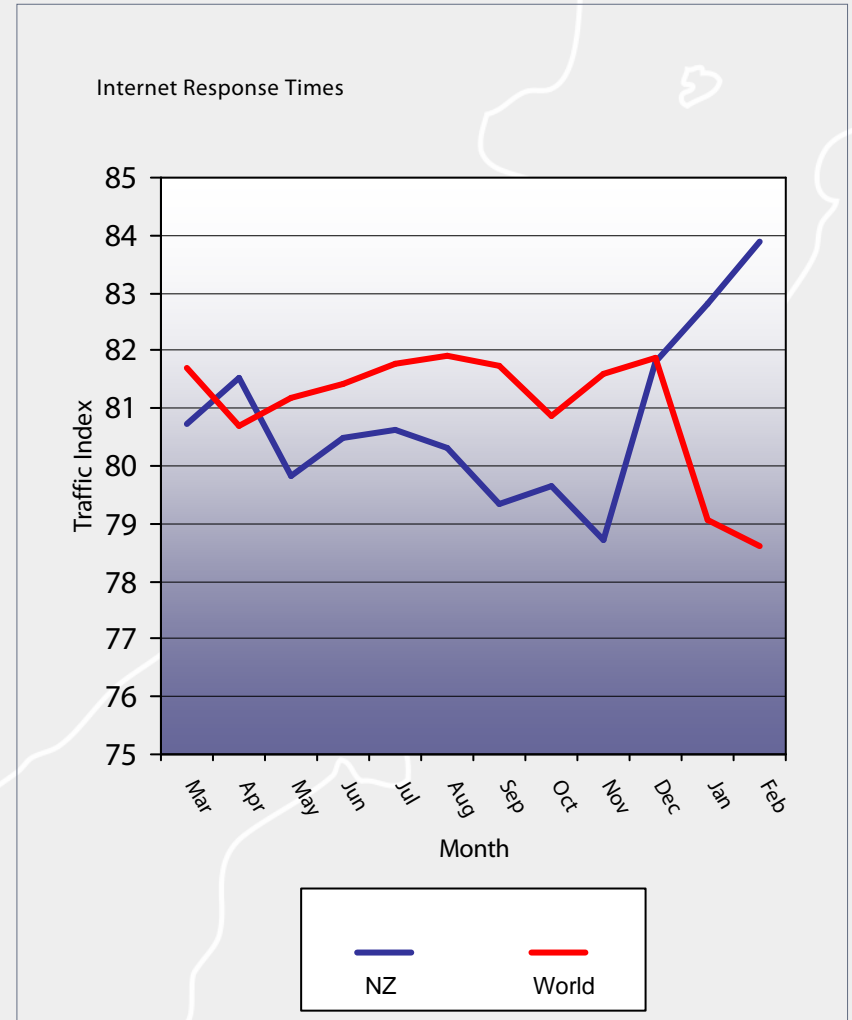
■	10,161	Unknown	0.06%
■	7,529,988	North America	43.97%
■	142,735	South America	0.83%
■	1,205,541	Europe	7.04%
■	108,591	Australasia	0.63%
■	7,959,054	Asia	46.47%
■	26,405	Africa	0.15%

Internet Response Times

Internet response times remained high throughout February following on from the positive results of the previous two months. The February response times improved on last months record and were the fastest recorded over the last 12 months. The average response time was 158ms with an overall Traffic Index of 83.9. This was an increase on last months response times of 159ms, and a Traffic Index of 82.8. This strongly indicates that 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.

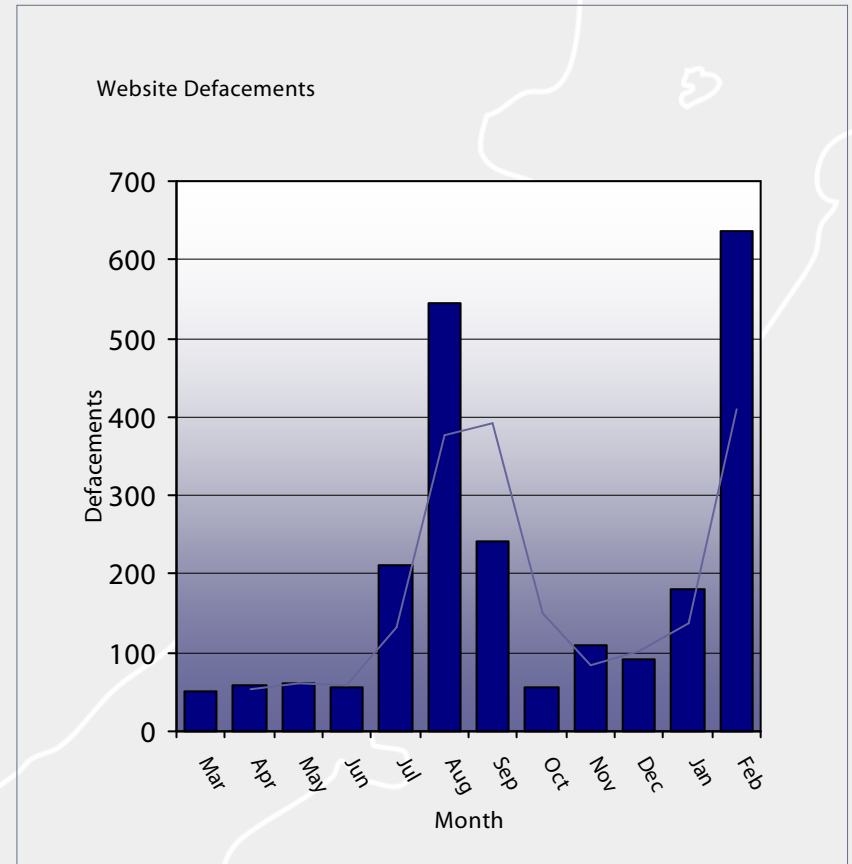


Website Defacements

Reported defacements of New Zealand websites for the month of February again took another huge upsurge, with an extremely high increase to 637 reported defacements, over three times the average number of monthly reports. As a result of this huge increase the average reports of New Zealand websites being defaced has increased to 191 defacements per month. The huge increase is due to an attack on 11 February of an overseas server, which hosted a large number of New Zealand based websites by an attacker known as "iskorpitx", a total of 604 New Zealand sites were defaced.

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.