

CCIP Monthly Report for JANUARY

Welcome to the January issue of the Monthly Report produced by the Centre for Critical Infrastructure Protection 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

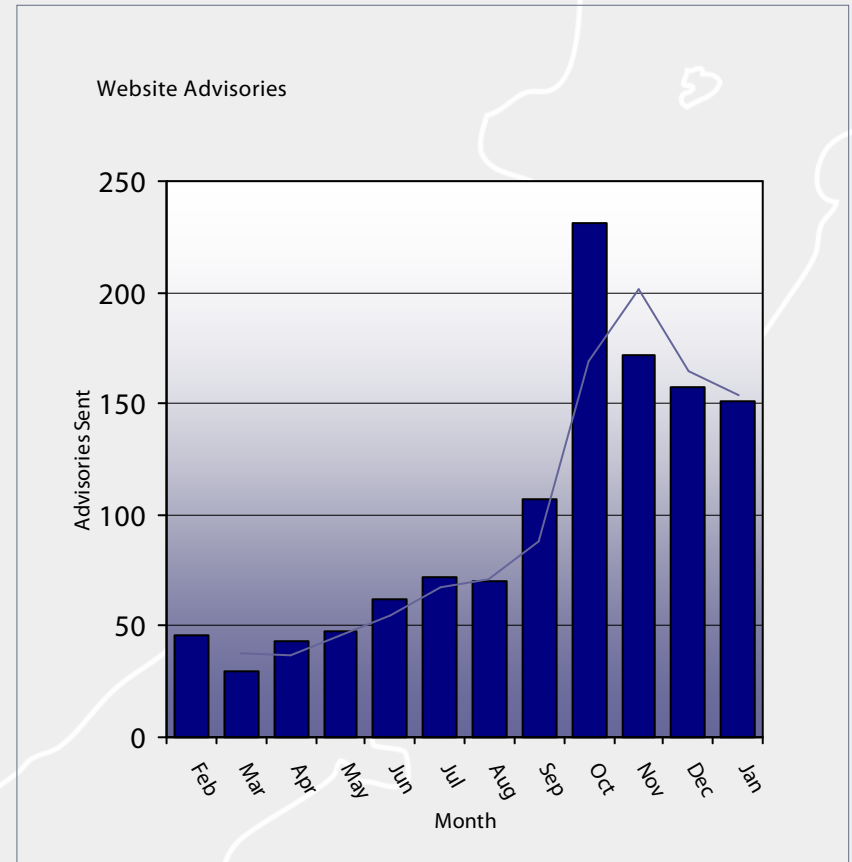
Operations Centre Activity

The CCIP Operations Centre posted 151 advisories during the month of January, slightly down on the December total of 157, but still reasonably high. The number of advisories that were deemed to be of significant importance for January was also relatively high at 13.

Advisories of major significance during the month included 3 Microsoft security updates relating to Outlook, Excel, and Vector Markup Language. Microsoft also posted a revised security bulletin relating to Microsoft Excel on 19 January. An Unspecified Code Execution Vulnerability relating to Microsoft Word was also announced on 29 January.

Alerts sent directly via the CCIP mailing lists throughout January remained steady, with 3 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

Significant Advisories:

The following table shows significant advisories posted by the CCIP Operations Centre during the month of January.

Date	Detail	Source
29/01/07	Microsoft Word Unspecified Code Execution Vulnerability	Secunia
26/01/07	Advanced Linux Environment Multiple Updates	SGI
24/01/07	Update for acroread	SUSE
24/01/07	Update for sun-jdk and sun-jre-bin	Gentoo
24/01/07	Update for acroread	Gentoo
19/01/07	Revised Security Bulletin MS07-002: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution	Microsoft
18/01/07	Products Multiple Vulnerabilities	Oracle
15/01/07	Update for mozilla-firefox	Mandriva
15/01/07	Update for mozilla-thunderbird	Mandriva
11/01/07	Reader Unspecified Heap Corruption Vulnerability	Adobe
10/01/07	Windows Vector Markup Language Buffer Overflow	Microsoft
10/12/07	Outlook Multiple Vulnerabilities	Microsoft
10/01/07	Excel Unspecified Code Execution Vulnerability	Microsoft

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

- [Issue 32 ~ 31 January 2007](#)
 - Technology Predictions 2007
 - Non-OS-Dependant Malware
 - One Hacker Kit Accounts For 71% Of December Web-Based Attacks
 - Spear Phishing – Casting a Narrow Net
 - Commonsense Guide to Prevention & Detection of Insider Threats
 - Review of Secunia's "Software Inspector" - Detects Insecure Application Version
 - Network Access Control Learning Guide
 - Identity Theft
 - Internet Threat Outlook Finds Rise in Sophisticated Attacks Against Savvy PC Users
 - IEEE 802.11n Working Group Approves Draft 2.0

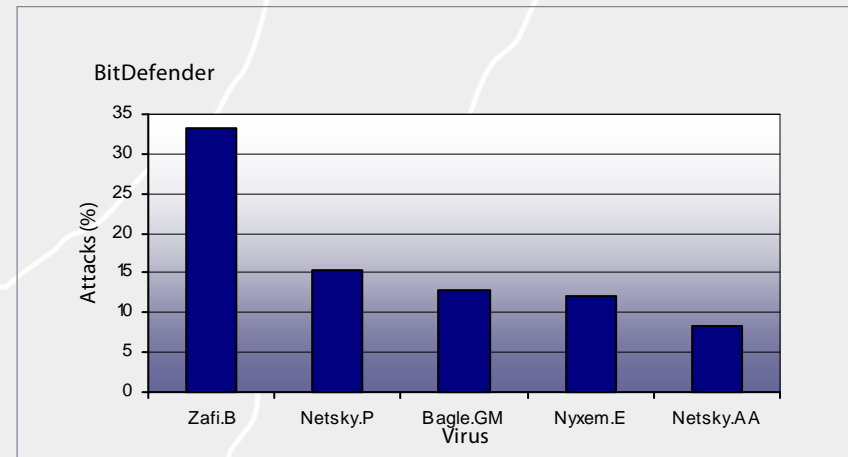
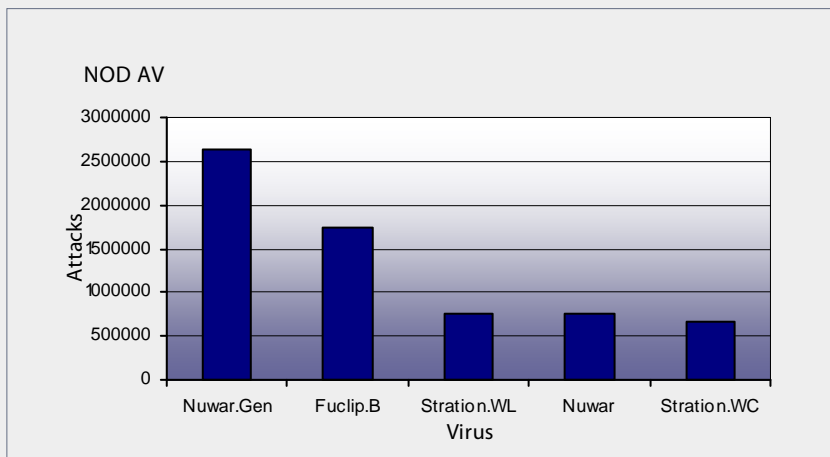
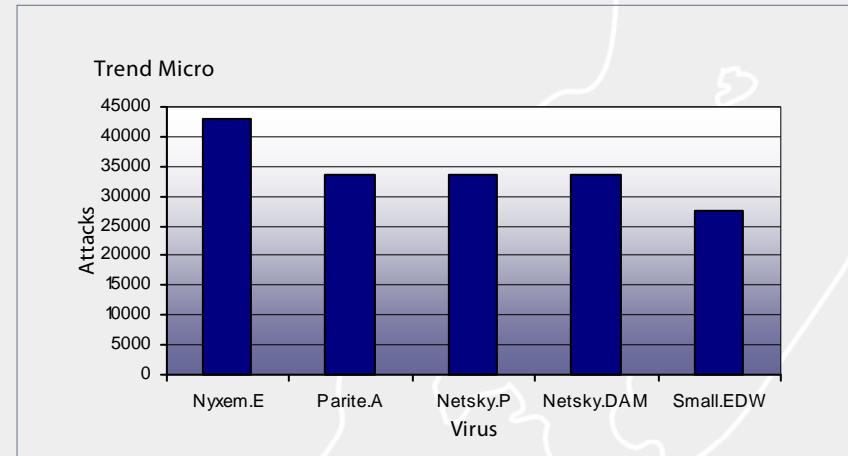
e-Bulletins are sent to members of the CCIP mailing lists. Back issues can be obtained by visiting the [Publications](#) page of the CCIP website.

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](#)



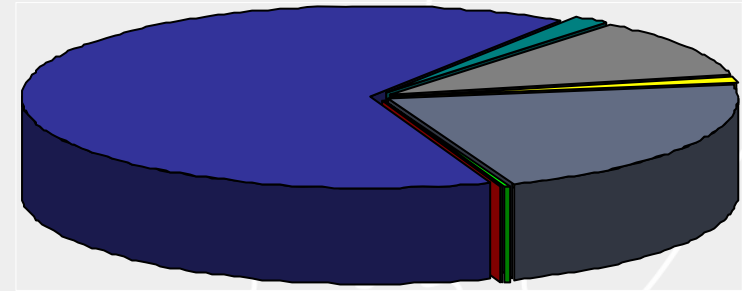
Virus Distribution

The Australasian region profile on the virus front took an increase in January with a total of 77,549 detected viruses, an increase on the 39,672 reports for last month. This in turn increased the percentage of detected viruses within the region to a level of 1.17%, doubling the December percentage of 0.59% of all detects. The number of viruses detected in all regions was also slightly higher than December, indicating that activity is again on the rise after the holiday period.

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.

Regional Distribution



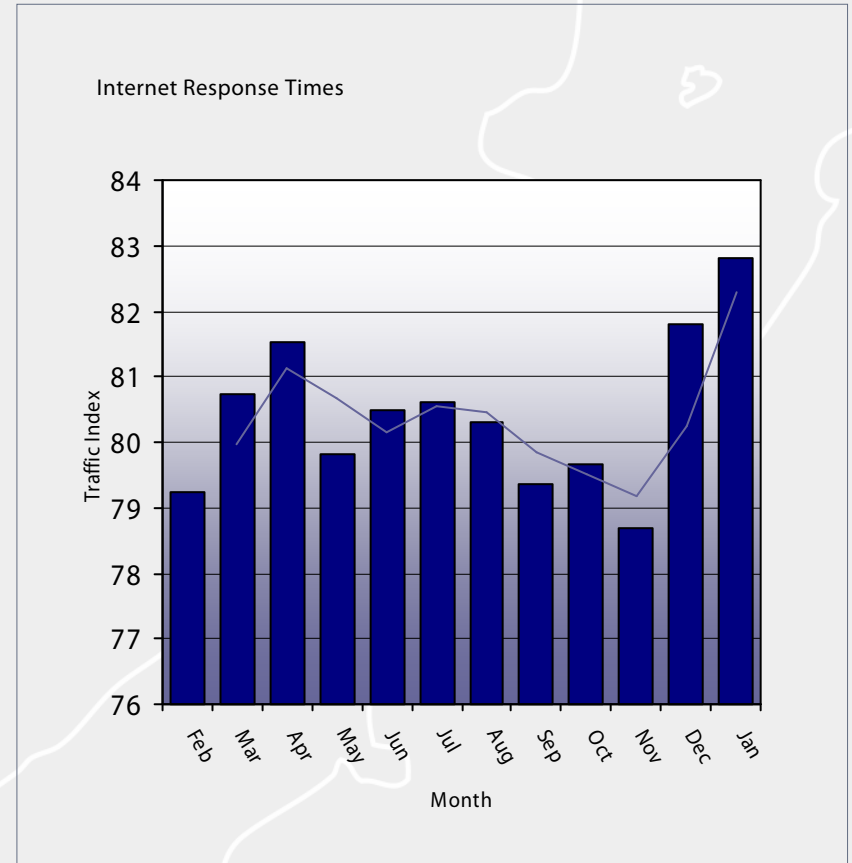
■	5,507	Unknown	0.08%
■	4,236,744	North America	63.66%
■	109,105	South America	1.64%
■	705,894	Europe	10.61%
■	77,549	Australasia	1.17%
■	1,423,093	Asia	21.38%
■	9,511	Africa	0.14%

Internet Response Times

Internet response times were again high this following a good December result. The January response times were the fastest recorded over the last 12 months. The average response time throughout January was 159ms, leaving the overall Traffic Index figure at a low of 82.8. This was an increase on last months response times of 117ms, and a Traffic Index of 80.8. This strongly indicates that New Zealand's Internet performance is trending upwards over the previous two months.

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.

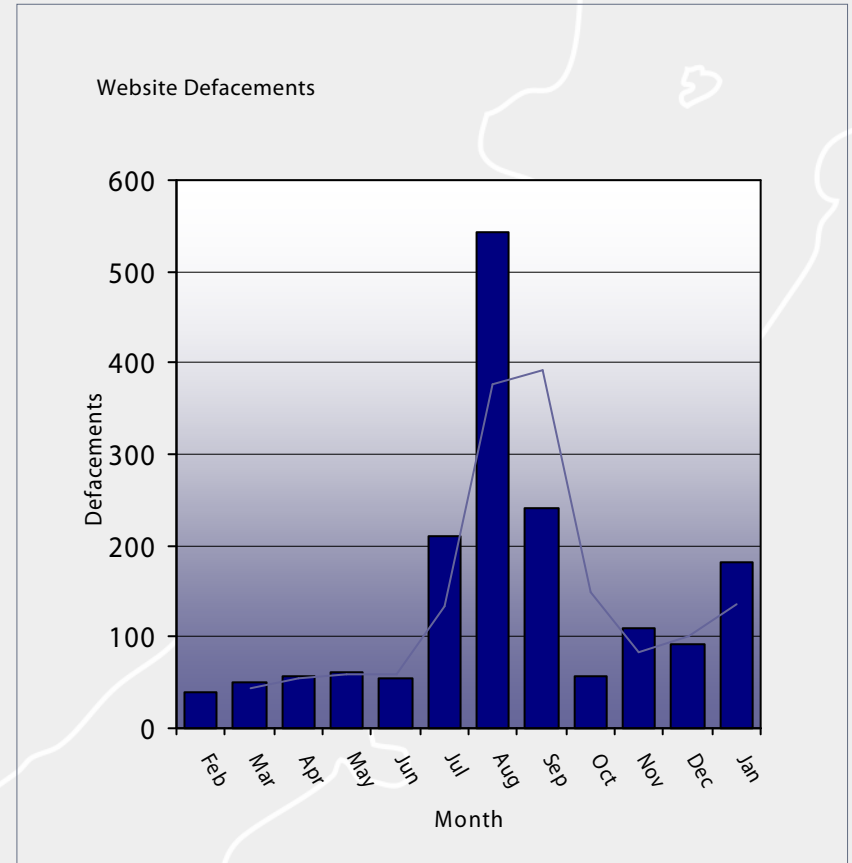


Website Defacements

Reported defacements of New Zealand websites for the month of January took another upsurge, with an increase to 181 reported defacements, almost double December's figure of 92. This has increased the average reports of New Zealand websites being defaced to 141 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.