

CCIP Monthly Report for DECEMBER

Welcome to the December 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](#)[CCIP Recent Alerts & Advisories](#)[CCIP e-Bulletins](#)[Virus Activity](#)[Virus Distribution](#)[Port Scanning Activity](#)[Internet Response Times](#)[Website Defacements](#)[Contact Details & Disclaimer](#)

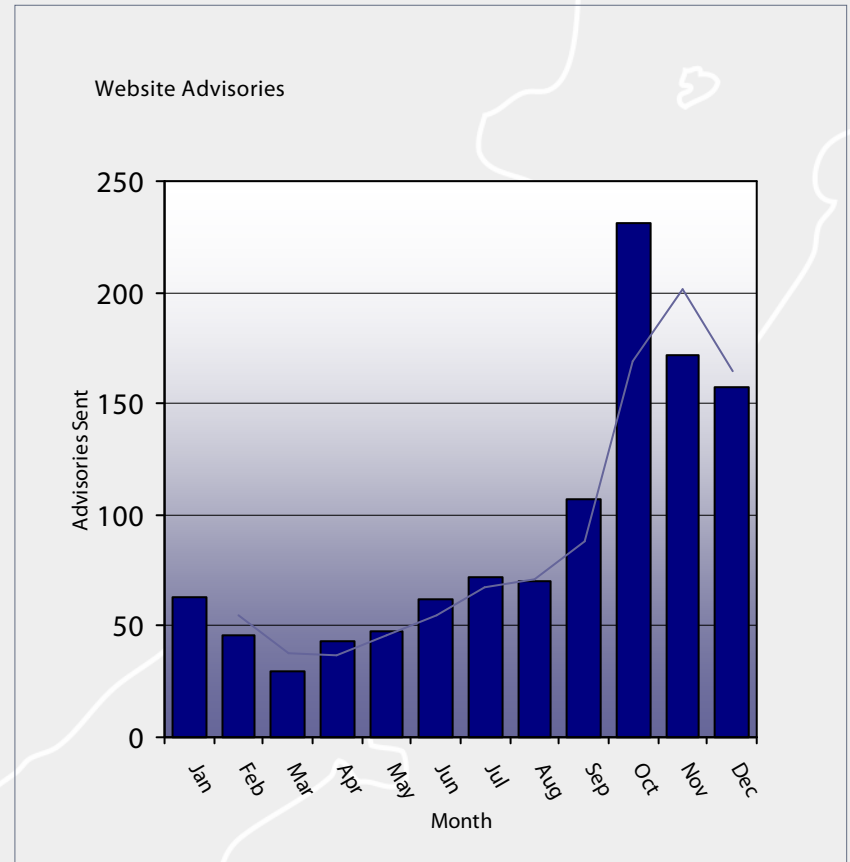
Operations Centre Activity

Advisories posted to the CCIP website during the month of December were down on last months figure of 172. There were a total of 157 advisories posted by the Operations Centre during the month. While the number of advisories posted remained quite high, the number that were deemed critical was relatively low in December, with only 10 being deemed of significant importance.

Advisories of major significance during the month included 3 Microsoft security updates relating to Internet Explorer, Windows Media, and Visual Studio 2005. Mozilla issued updates for its Firefox, Thunderbird, and Seamonkey products. There was also a buffer overflow vulnerability in Adobe Download Manager.

Alerts sent directly via the CCIP mailing lists throughout December increased slightly, with 5 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 December.

Date	Detail	Source
20/12/06	Mozilla Thunderbird Multiple Vulnerabilities	Mozilla
20/12/06	Mozilla SeaMonkey Multiple Vulnerabilities	Mozilla
20/12/06	Mozilla Firefox Multiple Vulnerabilities	Secunia
13/12/06	Microsoft Security Bulletin MS06-078 - Vulnerability in Windows Media Format Could Allow Remote Code Execution (923689)	Microsoft
13/12/06	Microsoft Security Bulletin MS06-073 - Vulnerability in Visual Studio 2005 Could Allow Remote Code Execution (925674)	Microsoft
13/12/06	Microsoft Security Bulletin MS06-072 - Cumulative Security Update for Internet Explorer (925454)	Microsoft
12/12/06	Word Unspecified Code Execution Vulnerability	Microsoft
07/12/06	Citrix ICA Client ActiveX Control Heap Overflow Vulnerability	Citrix
07/12/06	Adobe Download Manager AOM Buffer Overflow Vulnerability	Adobe
07/12/06	Microsoft Word Unspecified Memory Corruption 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 December, CCIP released two e-Bulletins. Links to recent issues of the e-Bulletin and samples of topics included are detailed below.

- [Issue 30 ~ 13 December 2006](#)
 - Zero Day Attacks & Prevention Strategies
 - Windows Vista Security Guide
 - Microsoft Security Intelligence Report
 - Security Learning Paths
 - The Vulnerability Management Lifecycle
- [Issue 31 ~ 21 December 2006](#)
 - Network Headaches to Avoid this Holiday Season
 - Computers, Networks and Theft: Part 2
 - PHP Security Under Scrutiny
 - Security a Priority Concern
 - How to Spot Insider-Attack Risks in the IT Department
 - Social Sites' Insecurity Increasingly Worrisome

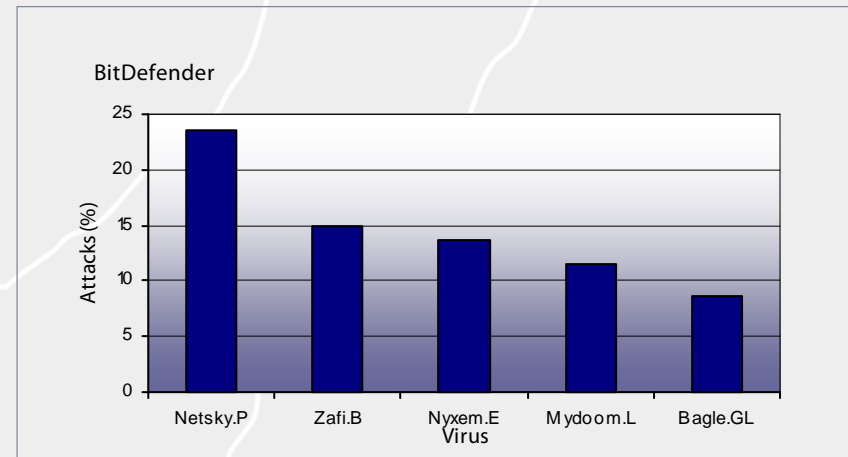
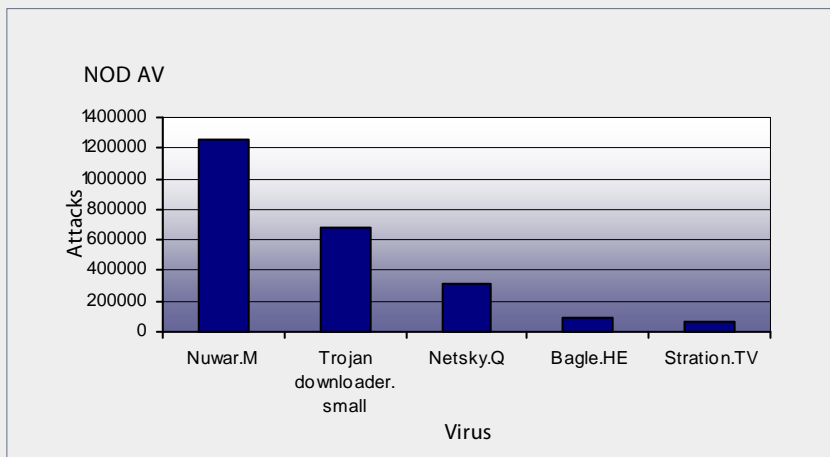
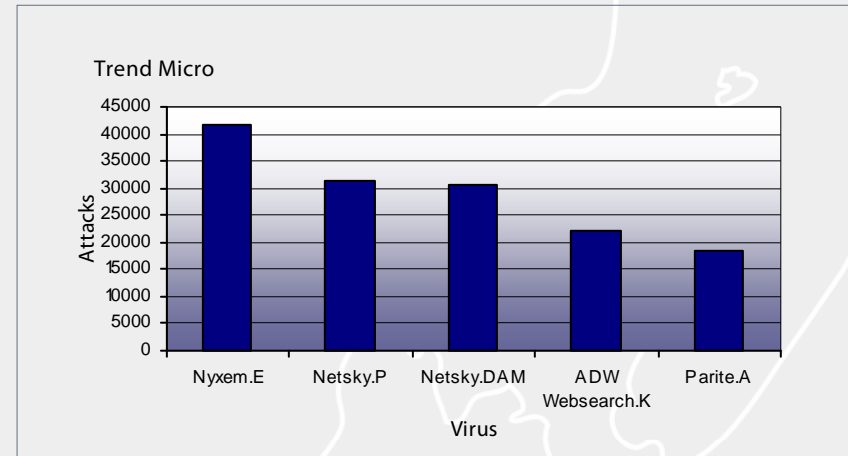
e-Bulletins are sent to members of the CCIP mailing lists. Back issues can be obtained by visiting the [Publications](#) page of the CCIP website.

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](#)



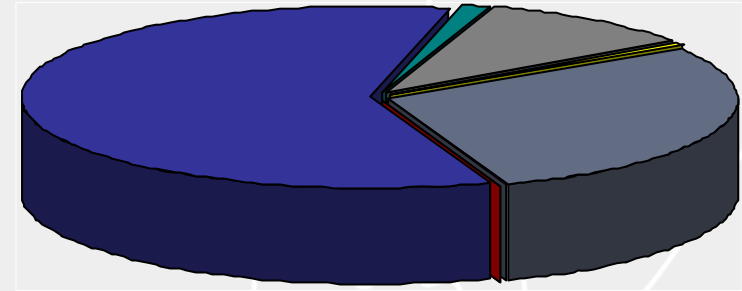
Virus Distribution

The Australasian region profile on the virus front remained relatively low for the month. There were a total of 39,672 viruses detected throughout December, almost half of last months figure which stood at 69,316, leaving the distribution in world terms at 0.59% of all detected viruses. The number of viruses detected in all regions was lower than normal throughout December, indicating that virus writers may take holidays as well.

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



■	5,107	Unknown	0.08%
■	3,912,483	North America	58.16%
■	100,100	South America	1.49%
■	678,722	Europe	10.09%
■	39,672	Australasia	0.59%
■	1,890,379	Asia	28.10%
■	8,657	Africa	0.13%

Port Scanning Activity

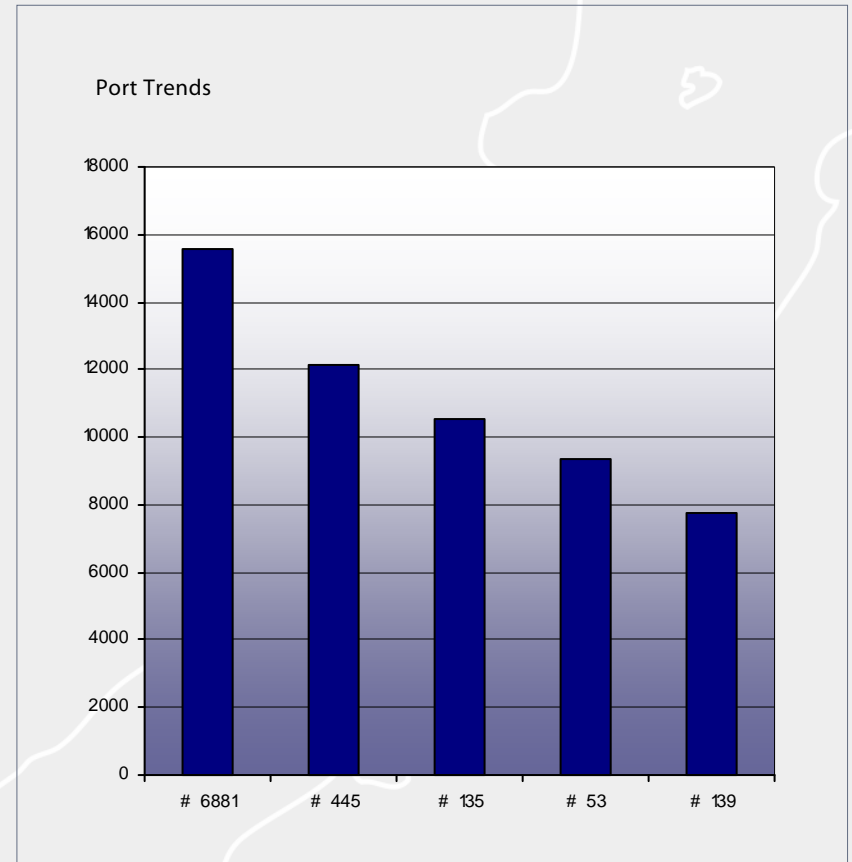
Wikipedia definition: A port scanner is a piece of software designed to search a network host for open ports. This is often used by administrators to check the security of their networks and by crackers to compromise it.

The Port Scanning Trends Graph to the right outlines the number of recorded attacks against each of the 5 highest attacked ports for the month.

For more information regarding Port Scanning, please refer to the [SANS Internet Storm Center](#) website.

Port Summary:

Port Number	Port Name	Attacks
# 6881	TCP/UDP (bittorrent)	15572
# 445	TCP/UDP (Microsoft-ds)	12153
# 135	TCP/UDP (epmap)	10522
# 53	TCP/UDP (domain)	9366
# 139	TCP/UDP (netbios-ssn)	7783

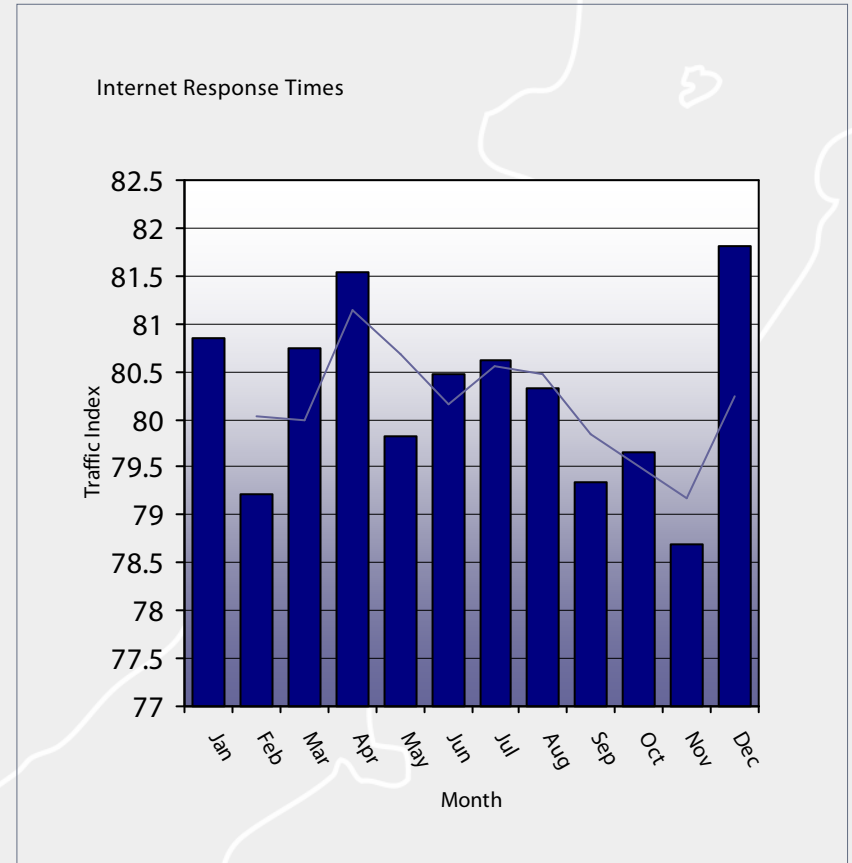


Internet Response Times

In contrast to last months extremely slow Internet response times, the figures for December were the best recorded over the past 12 months. The New Zealand router response time decreased to 177ms, a vast improvement on the November response time of 206ms. This in turn increased the overall Traffic Index average to 80.8. This is a higher than normal Traffic Index figure, indicating Internet performance throughout December was increased.

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.

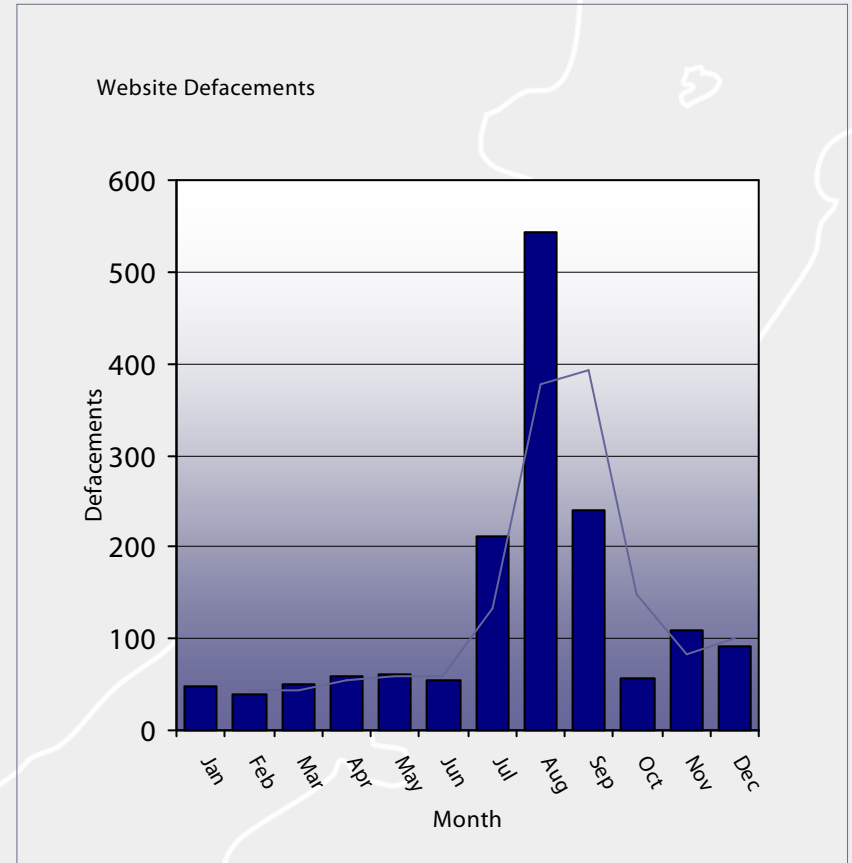


Website Defacements

Reported defacements of New Zealand websites for the month of December remained at a slightly higher, but relatively steady figure of 92 defacements. As a result of the increased numbers in the past six months, the average number of reported defacements for the year has risen to 130 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.