

# CCIP Monthly Report for NOVEMBER

Welcome to the November 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](mailto: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](#)

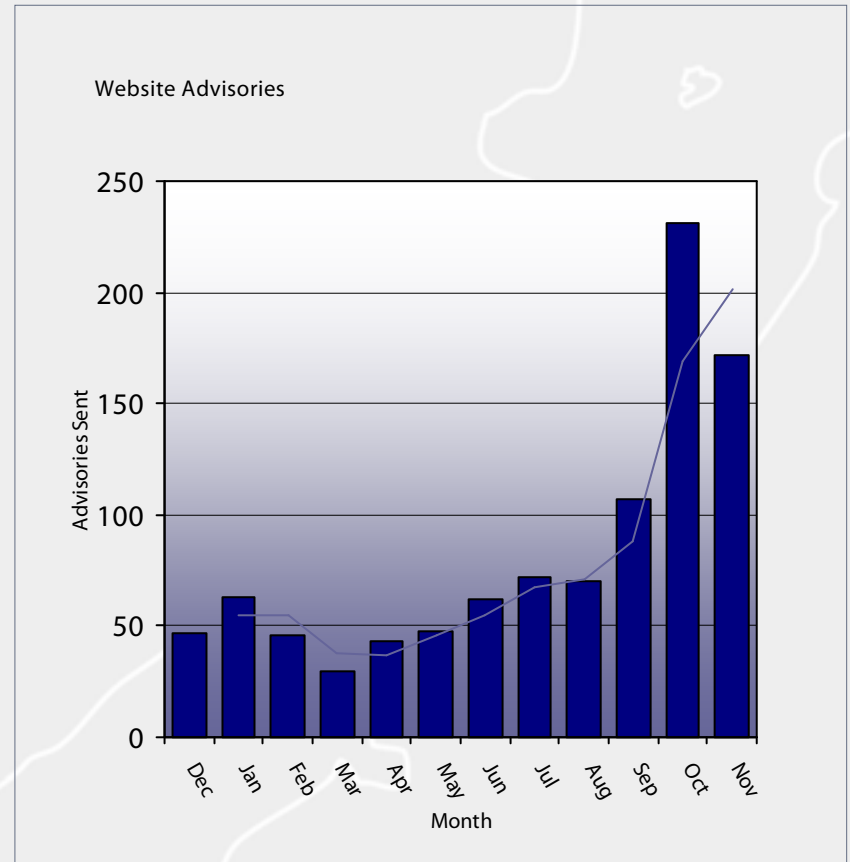
# Operations Centre Activity

The number of advisories posted to the CCIP website decreased slightly in November, but still remained comparatively high for the year. There were 172 advisories posted during the month, down from October's record setting figure of 231 advisories. The recent increase in advisories is due to additional operational activity within the CCIP. The number of advisories that were deemed critical was a record setting 18 during November.

Advisories of major significance during the month saw Microsoft again posting a number of security updates as part of the planned monthly security release. In addition to the Microsoft Security Bulletin release, other advisories of major significance included updates for both Mozilla Thunderbird and Firefox, and WinZip FileView ActiveX Control Insecure Methods.

Alerts sent directly via the CCIP mailing lists throughout November remained steady, with 2 alerts sent out, relating to the Active Exploitation of an Unpatched Remote Code Execution Vulnerability in Visual Studio 2005 and Apple Mac OS X Security Update Fixes Multiple Vulnerabilities.

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.

# CCIP Recent Alerts and Advisories

## Significant Advisories:

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

Date	Detail	Source
30/11/06	Symantec NetBackup PureDisk PHP Buffer Overflow	<a href="#">Symantec</a>
30/11/06	Mac OS X Security Update Fixes Multiple Vulnerabilities	<a href="#">Apple</a>
28/11/06	Sisfo Kampus File Inclusion and Directory Traversal	<a href="#">Secunia</a>
23/11/06	Update for mozilla-thunderbird	<a href="#">Ubuntu</a>
23/11/06	Update for firefox	<a href="#">Ubuntu</a>
20/11/06	Update for MozillaFirefox, MozillaThunderbird, and seamonkey	<a href="#">SUSE</a>
16/11/06	WinZip FileView ActiveX Control Insecure Methods	<a href="#">WinZip</a>
15/11/06	MS06-071: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution	<a href="#">Microsoft</a>
15/11/06	MS06-070: Microsoft Windows Workstation Service Buffer Overflow Vulnerability	<a href="#">Microsoft</a>
15/11/06	MS06-069: Microsoft Windows Flash Player Multiple Vulnerabilities	<a href="#">Microsoft</a>
15/11/06	MS06-068: Microsoft Windows Agent ActiveX Control Buffer Overflow	<a href="#">Microsoft</a>
15/11/06	MS06-067: Cumulative Security Update for Internet Explorer	<a href="#">Microsoft</a>
13/11/06	Cisco Products OpenSSL Vulnerabilities	<a href="#">Cisco</a>
09/11/06	Firefox and SeaMonkey Multiple Vulnerabilities	<a href="#">Mozilla</a>
07/11/06	ICQPhone.SipxPhoneManager ActiveX Control Vulnerability	<a href="#">ICQ</a>
06/11/06	Solaris NVIDIA Graphics Driver Buffer Overflow Vulnerability	<a href="#">Sun</a>
06/11/06	XMLHTTP ActiveX Control Code Execution Vulnerability	<a href="#">Microsoft</a>
02/11/06	Vulnerability in Visual Studio 2005 Could Allow Remote Code Execution	<a href="#">Microsoft</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 November, CCIP released one e-Bulletin. Links to recent issues of the e-Bulletin and samples of topics included are detailed below.

- [Issue 29 ~ 27 November 2006](#)
  - Biometrics
  - Patch Management
  - Ajax Security Dangers
  - Hacking Tor, the Anonymity Onion Routing Network
  - Security Myths
  - Strategic Considerations for an Integrated Malware Defense
  - Process Control and SCADA Security
  - Phishing Special Report: What We Can Expect For 2007
  - The Most Common Causes of IT Security

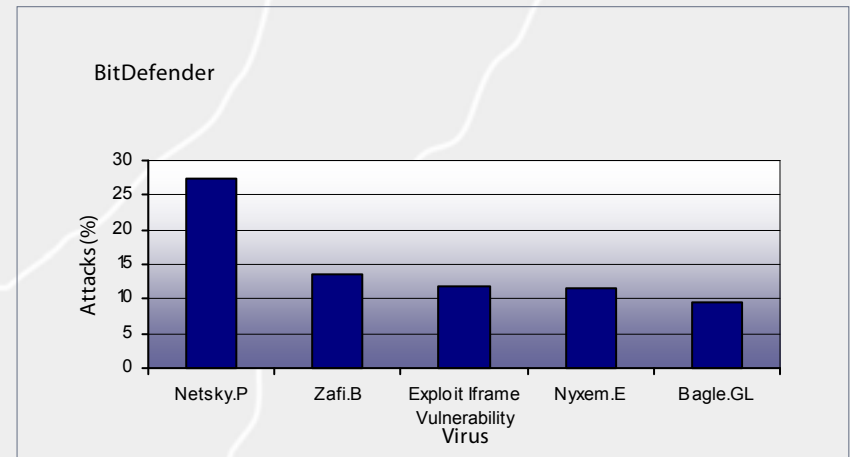
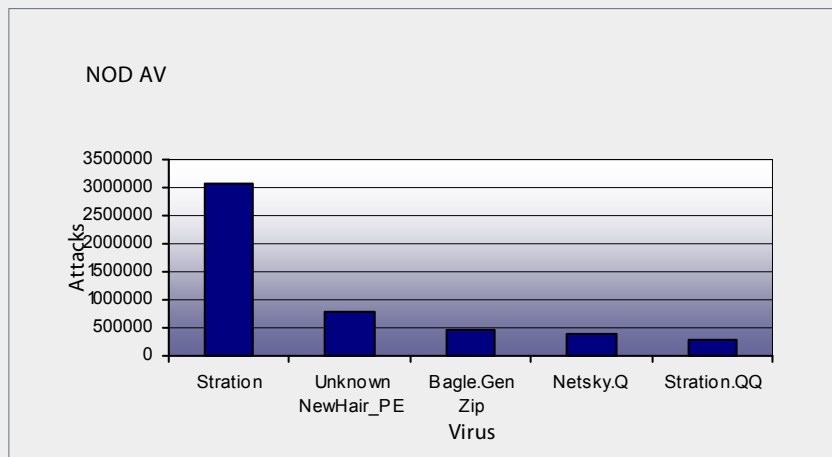
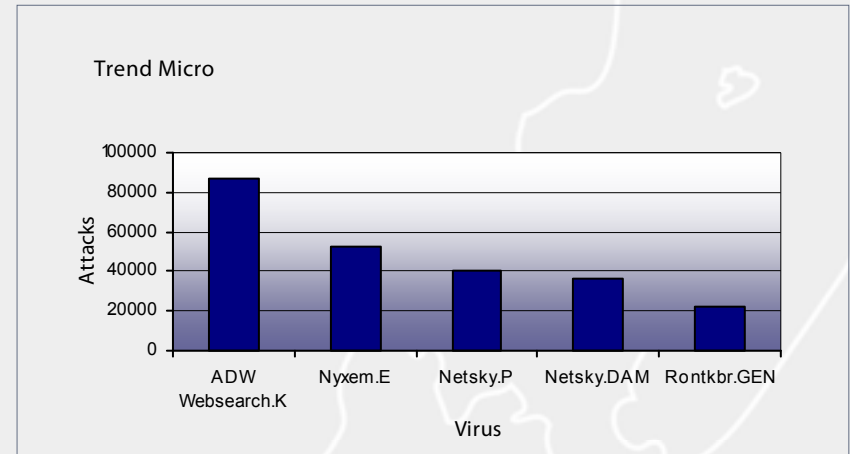
e-Bulletins are sent to members of the CCIP mailing lists. Back issues can be obtained by visiting the [Publications](#) page of the CCIP website.

# 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](#)



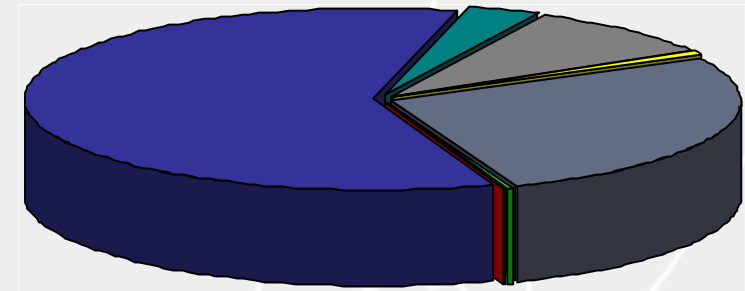
# Virus Distribution

The Australasian region maintained a relatively low profile in terms of virus distribution throughout the world for the month of November. However the number of viruses detected in the region rose to 69,316 throughout the month, up from 67,427 during October. The percentage of distribution compared to the rest of the world fell to 0.75% of all recorded virus infections.

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



6,765	Unknown	0.08%
5,419,950	North America	58.69%
307,160	South America	3.33%
827,957	Europe	8.97%
69,316	Australasia	0.75%
2,474,302	Asia	26.79%
12,915	Africa	0.14%

# Port Scanning Activity

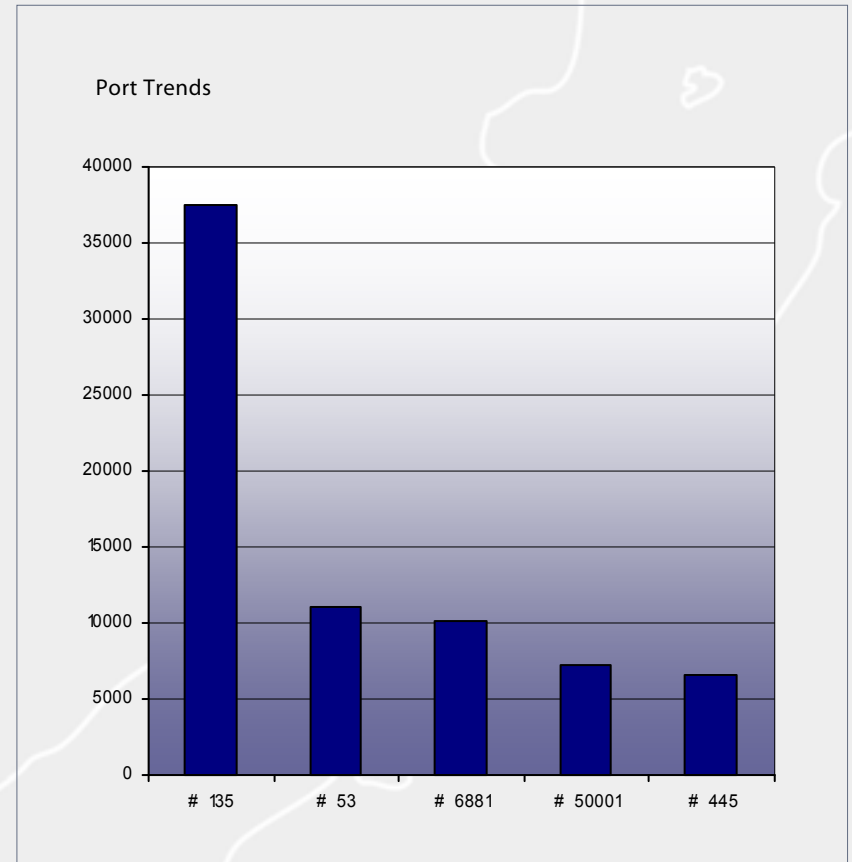
Wikipedia definition: A port scanner is a piece of software designed to search a network host for open ports. This is often used by administrators to check the security of their networks and by crackers to compromise it.

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
# 135	TCP/UDP (epmap)	37547
# 53	TCP/UDP (dns)	11042
# 6881	TCP/UDP (bittorrent)	10157
# 50001	TCP/UDP (Linux)	7296
# 445	TCP/UDP (Microsoft-ds)	6613

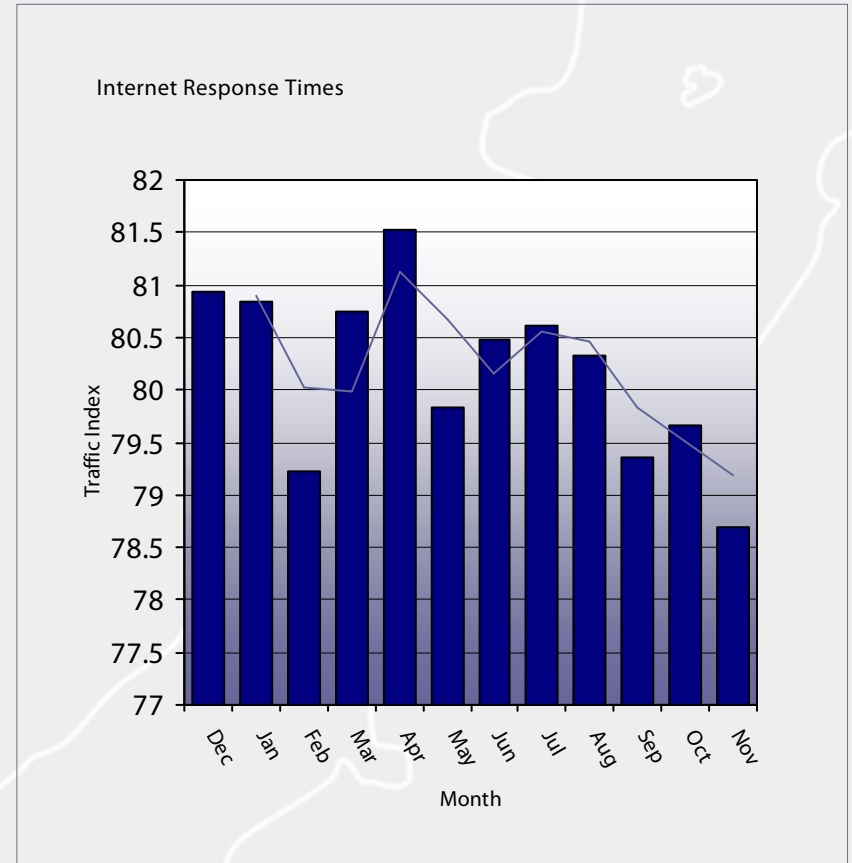


# Internet Response Times

The Internet response trends for November were the slowest recorded for the past 12 months, with the New Zealand router response time increasing to a high of 206ms, Thus reducing the overall Traffic Index average to 78.7. This is a lower than normal Traffic Index figure, indicating Internet performance throughout November was reduced. The poor response time recorded on 3rd November of 266ms was a contributing factor.

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.

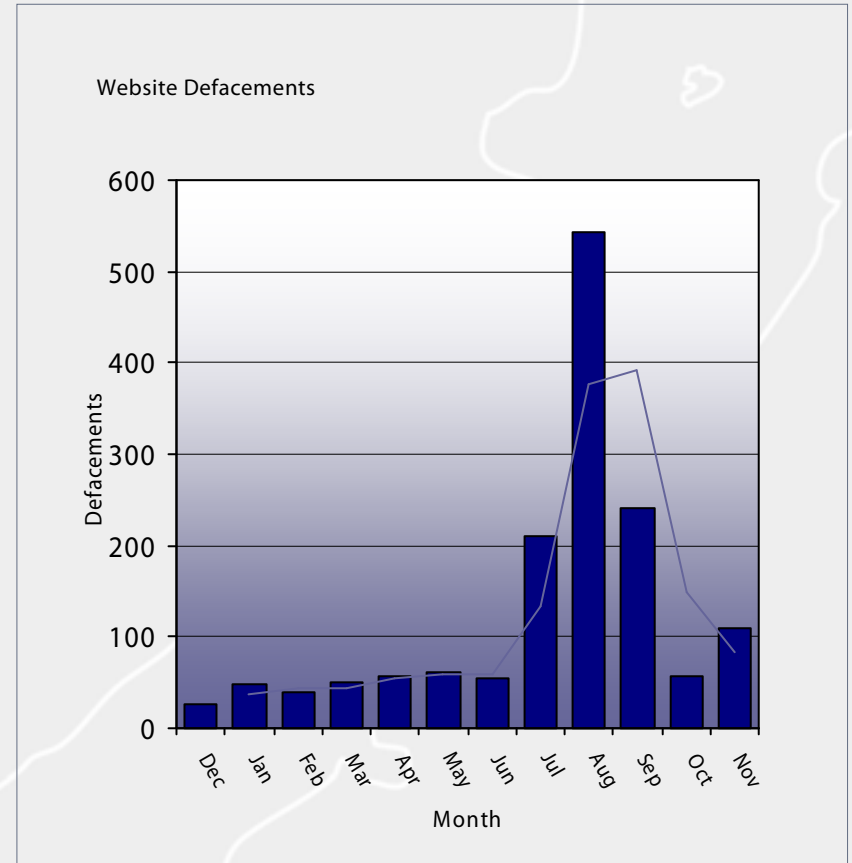


# Website Defacements

Reported defacements of New Zealand websites for the month of November almost doubled October's figure but were still relatively normal compared to the surge in activity in the period of July through September. The 110 reported defacements was up on October's number of 57, and maintained the average number of occurrences per month at 125.

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)

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)

Please include the following details in subscription emails.

First Name, Last Name, Organisation and Contact Number.

## 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.