

CCIP Monthly Report for OCTOBER

Welcome to the October 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.

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](#)

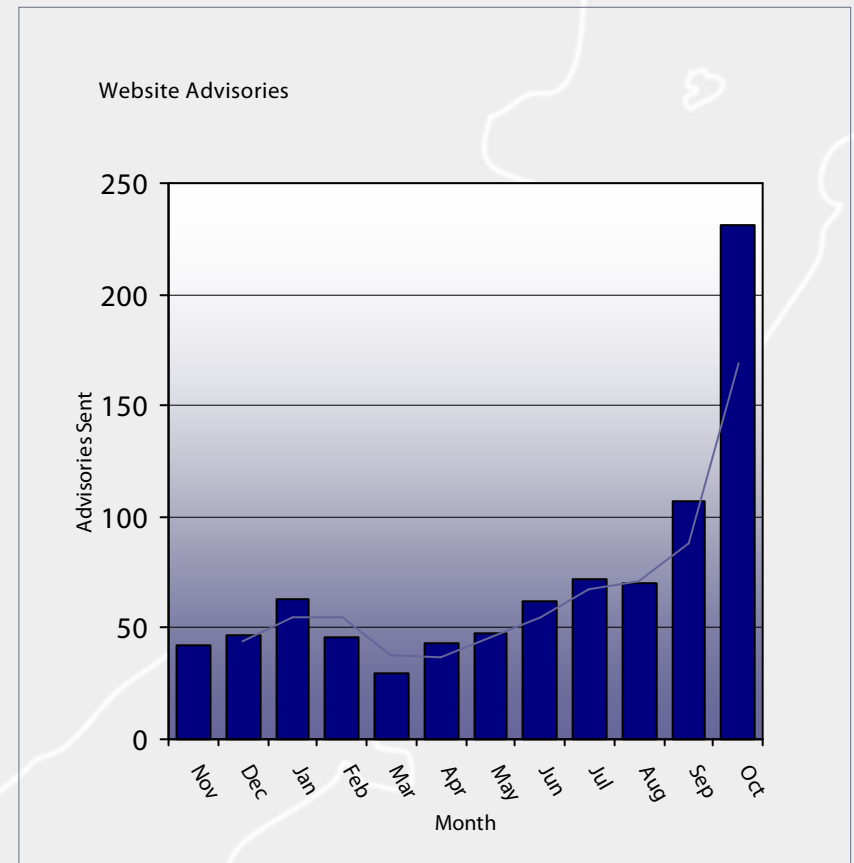
Operations Centre Activity

The number of advisories posted to the CCIP website increased significantly in October. The record setting 231 posted advisories were up from last months number which was 107. This was a result of increased operational activity within the CCIP. The number of advisories that were deemed critical also remained relatively high at 11 during October.

Advisories of major significance during the month saw a high amount posted by Microsoft as part of the planned monthly security release. In addition to the Microsoft Security Bulletin release, other advisories of major significance included multiple vulnerabilities in Oracle, an Apple MAC OS Security update, an Opera web browser URL handling buffer overflow vulnerability, and Sun Java system messaging server webmail script insertion.

Alerts sent directly via the CCIP mailing lists throughout October was low, with only 1 alert sent out on 20 October, relating to the re-release of MS06-061, Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (924191).

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 October.

Date	Detail	Source
26/10/06	Java System Messaging Server Webmail Script Insertion	Sun
20/10/06	Updated Security Bulletin MS06-061: Vulnerabilities in Microsoft XML Core Services	Microsoft
19/10/06	Oracle Products Multiple Vulnerabilities	Oracle
19/10/06	Opera Web Browser URL Handling Buffer Overflow Vulnerability	Opera
11/10/06	MS06-062: Microsoft Office Multiple Code Execution Vulnerabilities	Microsoft
11/10/06	MS06-061: Microsoft XML Core Services Information Disclosure and Code Execution	Microsoft
11/10/06	MS06-060: Microsoft Word Document Handling Command Execution Vulnerabilities	Microsoft
11/10/06	MS06-059: Microsoft Excel Document Handling Command Execution Vulnerabilities	Microsoft
11/10/06	MS06-058: Microsoft PowerPoint File Handling Command Execution Vulnerabilities	Microsoft
11/10/06	MS06-057: Microsoft Windows Explorer Could Allow Remote Execution	Microsoft
03/10/06	Mac OS X Security Update Fixes Multiple Vulnerabilities	Apple

For a comprehensive list of advisories posted by CCIP, please refer to the [Alerts and Advisories](#) page on the CCIP website.

CCIP e-Bulletins

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

- [Issue 27 ~ 10 October 2006](#)
 - Hacker Discovers Adobe PDF Back Doors
 - Cross-Site Scripting the Top Security Risk
 - Managing Windows Security Patches
 - What E-Mail Hackers Know that You Don't
 - CERT Secure Coding Standards
- [Issue 28 ~ 20 October 2006](#)
 - Security Best Practices for C++
 - Network Attacks: Analysis of Department of Justice Prosecutions
 - Web Security Trends Report - Q3/2006
 - Malware: The changing landscape
 - Internet Security Threat Report
 - Managing a Honeypot

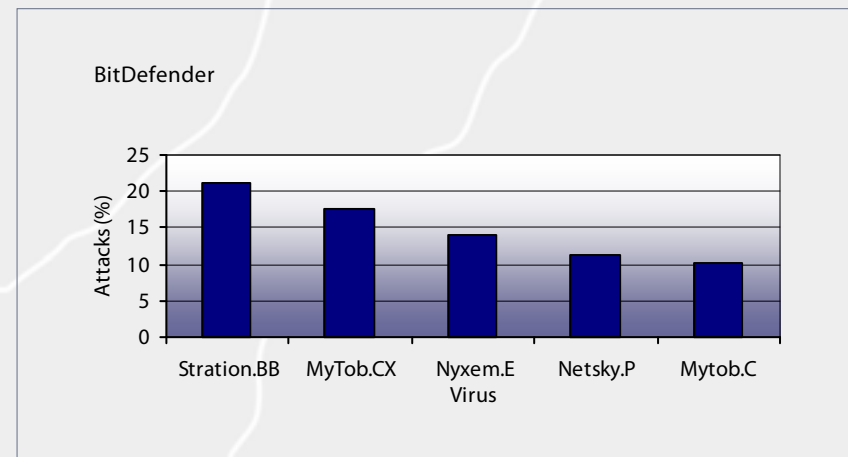
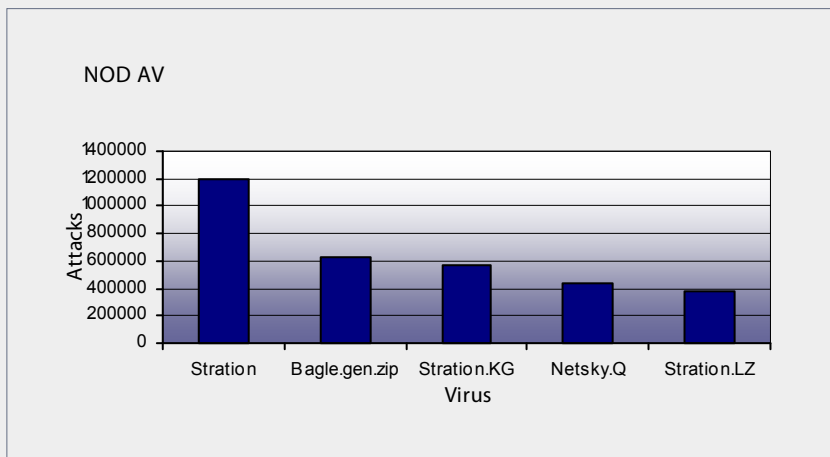
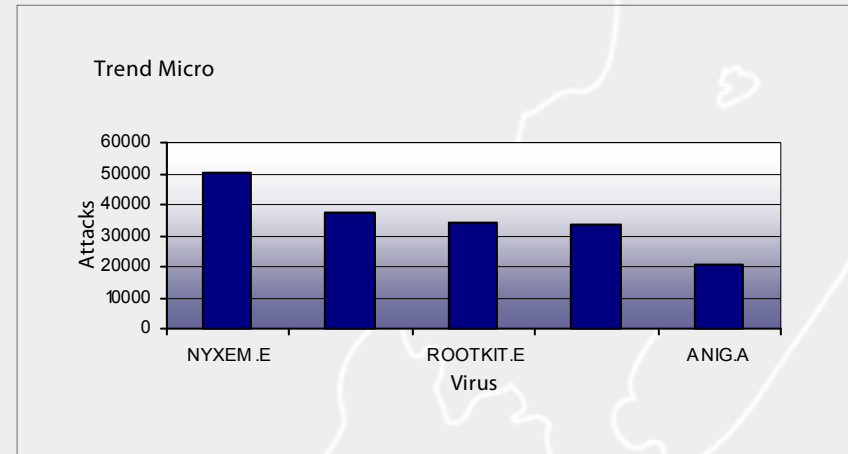
e-Bulletins are sent to members of the CCIP mailing lists. Back issues can be obtained by visiting the [Publications](#) page of the CCIP website.

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](#)



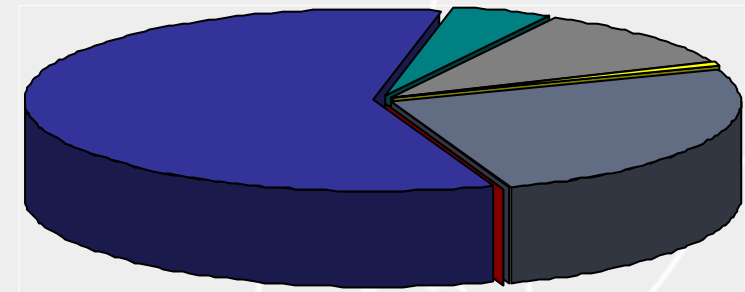
Virus Distribution

The Australasian region maintained a low profile in terms of virus distribution throughout the world. 67,427 viruses were detected in the region by TrendMicro throughout the month of October, giving a distribution of 0.82% 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%
4,733,395 North America	57.80%
401,048 South America	4.90%
843,441 Europe	10.30%
67,427 Australasia	0.82%
2,043,267 Asia	24.95%
10,857 Africa	0.13%

Port Scanning Activity

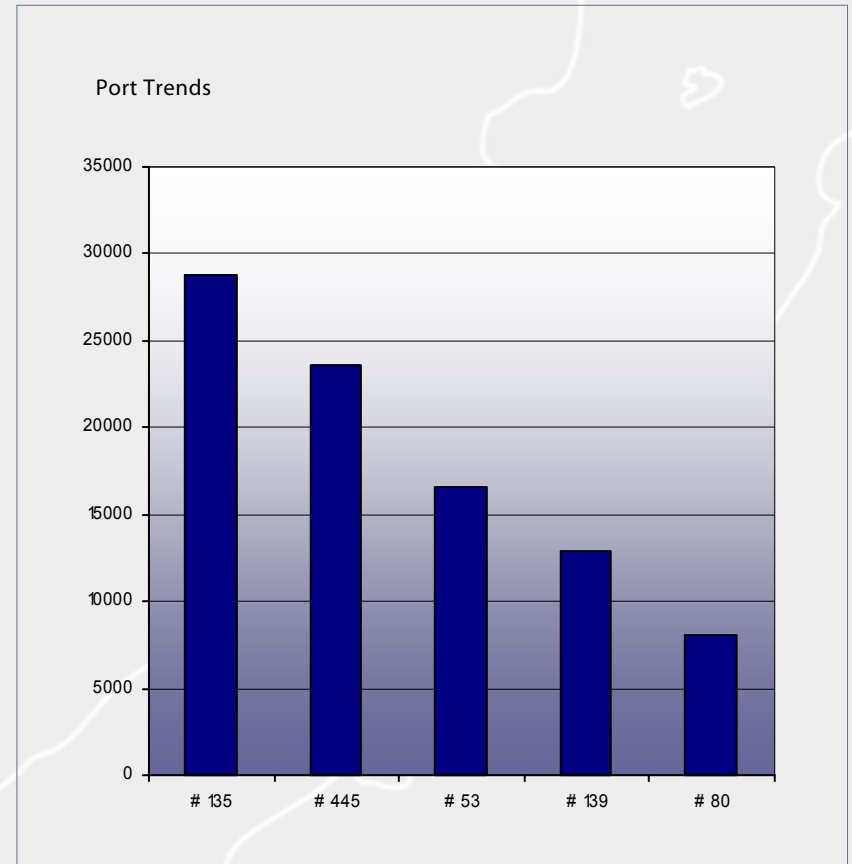
Wikipedia definition: A port scanner is a piece of software designed to search a network host for open ports. This is often used by administrators to check the security of their networks and by crackers to compromise it.

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
# 135	TCP/UDP (epmap)	28754
# 445	TCP/UDP (Microsoft-ds)	23625
# 53	TCP/UDP (domain)	16557
# 139	TCP/UDP (netbios-ssn)	12895
# 80	TCP/UDP (www)	8008

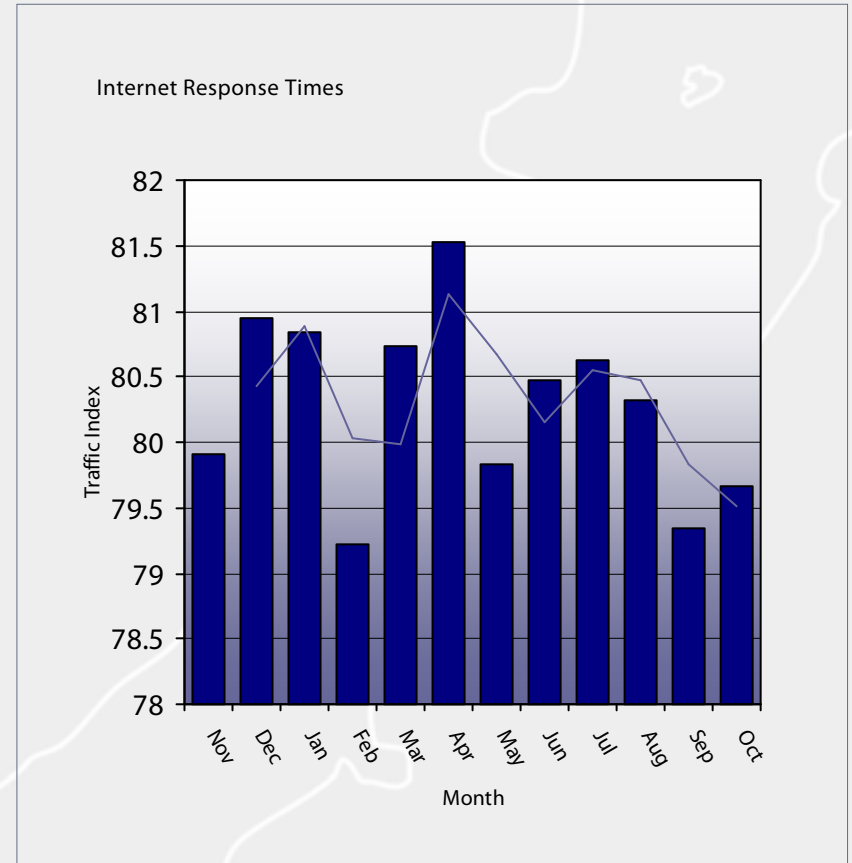


Internet Response Times

October's Internet Response trends increased slightly, with the New Zealand router response time remaining at a steady average of 198ms, and an overall Traffic Index average of 79.7. This is a slightly lower than normal Traffic Index figure, indicating Internet performance throughout October was still slightly reduced, but an improvement on last month.

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.

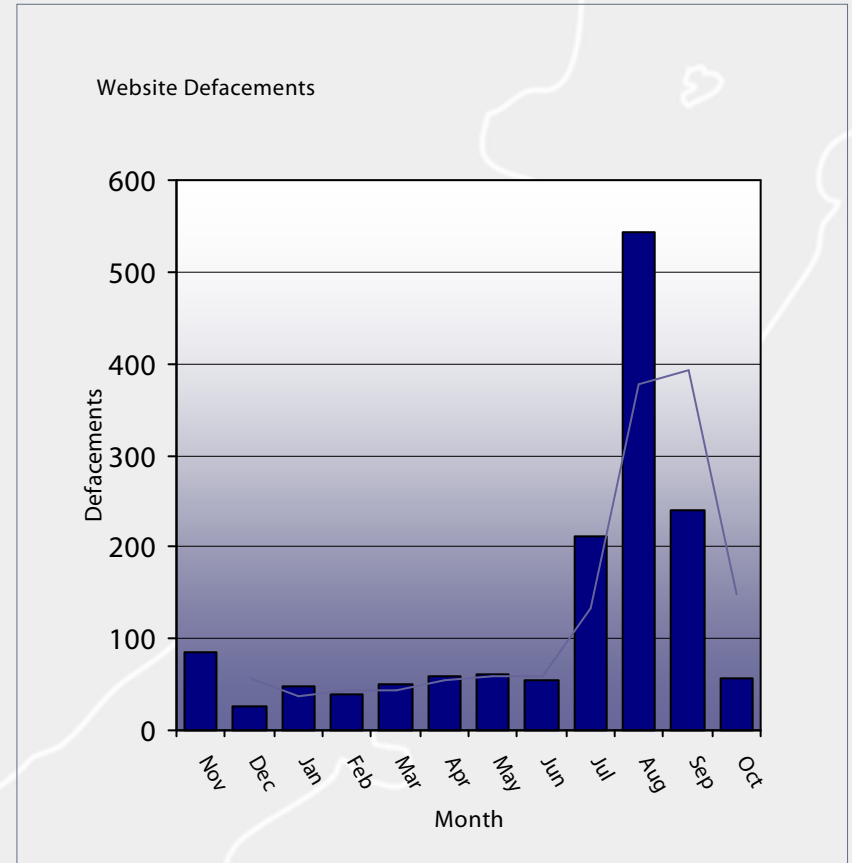


Website Defacements

Reported defacements of New Zealand websites for the month of October returned to relatively normal figures after the unusual surge in activity in the period of July through to September. The 57 reported defacements brought the average number of occurrences per month back down to 123.

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

Subscribe to the CCIP Monthly Report

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

To subscribe to Significant Alerts & Advisories, CCIP Monthly Reports, CCIP e-Bulletins and CCIP Newsletters 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.

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.