

CCIP Monthly Report for SEPTEMBER

Welcome to the September issue of the Monthly Report produced by the Centre for Critical Infrastructure Protection Operations Centre. This is a new report, and is designed to provide an overview of trends in relation to virus activity, internet response times, website defacements and other relevant information for the past month. The report also aims to keep you informed about current activities related to the CCIP Operations Centre.

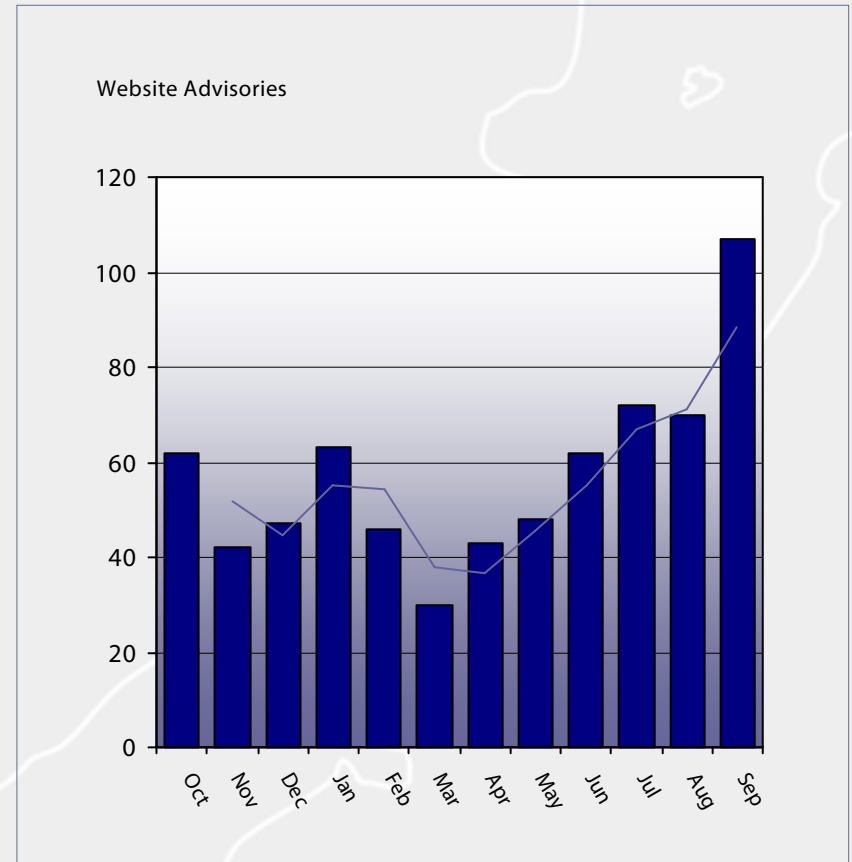
This report is currently under review by the CCIP Operations Team. Any comments regarding the content of the report, or any relevant areas you would like to see covered in future issues, are welcomed.

Operations Centre Activity

September saw an increase in the number of advisories posted on the CCIP website with 107 posted, including a high number that were deemed critical. The number of alerts being sent directly via the CCIP mailing lists also continued an upward trend with 6 during the month. Advisories of major significance during the month saw a high amount posted by Microsoft. These included a Microsoft Word 2000 Unspecified Code Execution Vulnerability, Microsoft Publisher Code Execution Vulnerabilities, Microsoft PowerPoint Unspecified Code Execution Vulnerabilities, Microsoft PowerPoint Code Execution Vulnerability and Microsoft Internet Explorer VML Code Execution Vulnerability, for which Microsoft issued an early Security Update on 27 September.

On 12 September, CCIP was informed of a malicious suite of Trojan Viruses that were being actively deployed within New Zealand. The first of five Trojans in the suite included an anti-virus software disabling functionality, allowing the rest of the suite to pass through the compromised system undetected. Additional to this, the suite attempted to infect web and mail services on the victim network to spread the redirection script, distribute malicious .exe files to servers and other PCs, act as a key logging Trojan, act as a password stealer, and exfiltrate data from the victim network. CCIP successfully had the source site closed and informed the public on mitigation of the effects of the attack.

The graph to the right represents the number of advisories posted by the CCIP Operations Centre over the last 12 months.



CCIP Recent Alerts and Advisories

Significant Advisories:

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

Date	Detail	Source
29/09/06	Microsoft PowerPoint Code Execution Vulnerability	Microsoft
29/09/06	Microsoft Internet Explorer "WebViewFolderIcon" Integer Overflow	Microsoft
27/09/06	MS06-055 - Vulnerability in Vector Markup Language Could Allow Remote Code Execution (925486)	Microsoft
25/09/06	Update for Thunderbird	HP-UX
20/09/06	Microsoft PowerPoint Unspecified Code Execution Vulnerability	Microsoft
20/09/06	Microsoft Internet Explorer VML Code Execution Vulnerability	Microsoft
18/09/06	Mozilla Products Remote Code Execution and Cross Site Scripting Vulnerabilities	Mozilla
14/09/06	QuickTime Multiple Vulnerabilities	Apple
13/09/06	Flash Player Multiple Unspecified Vulnerabilities	Adobe
13/09/06	Microsoft Publisher Code Execution Vulnerability	Microsoft
06/09/06	Microsoft Word 2000 Unspecified Code Execution Vulnerability	Microsoft

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

- [Issue 25 ~ 7 September 2006](#)
 - Spyware Infection Rates Return to Peak 2004 Levels
 - Defending Cell Phones and PDAs Against Attack
 - Microsoft Office Security, Part One
 - Study: Many Believe Data Thefts Can't be Prevented
 - Stopping Zombies, Botnets and Other Email-Borne Threats
- [Issue 26 ~ 15 September 2006](#)
 - Secure Portable IT
 - Sophos Anti-Rootkit: Overview
 - The Six Worst Security Mistakes
 - Safeguarding Your Data
 - Trusted Computing a Shield Against Worst Attacks?

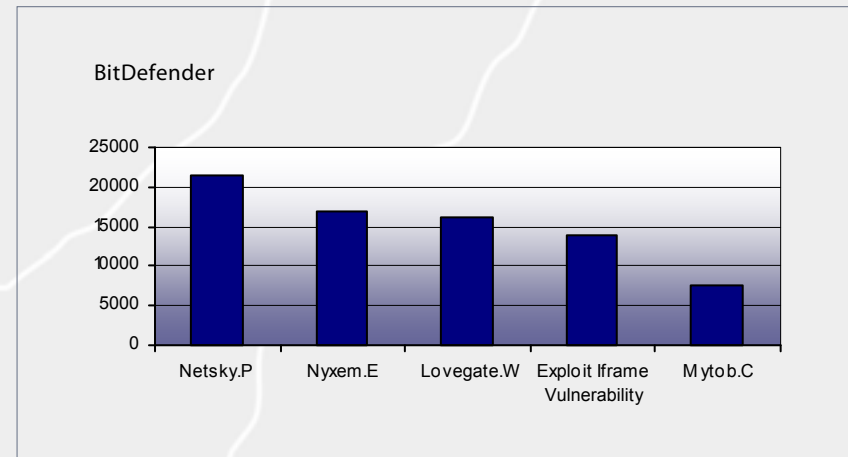
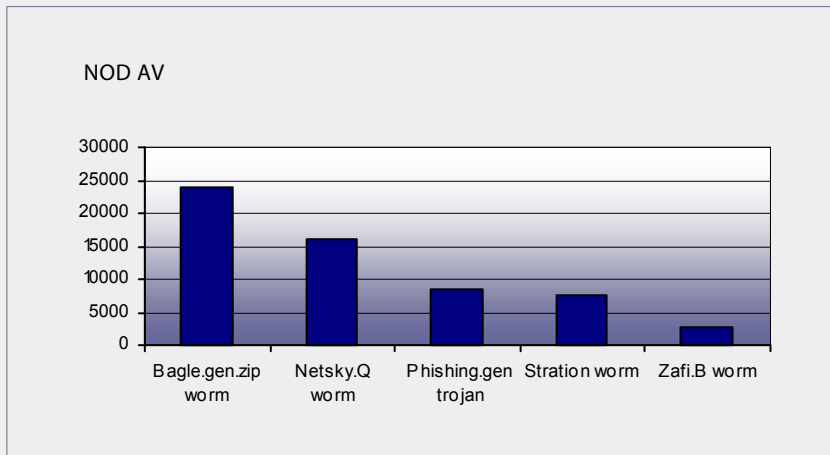
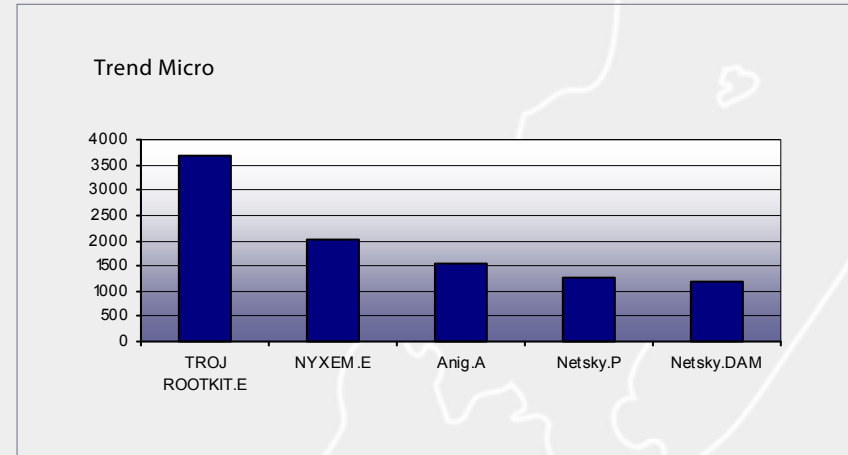
e-Bulletins are sent to members of the CCIP mailing lists. Back issues can be obtained by visiting the [Publications](#) page of the CCIP website.

Virus Activity

The graphs on this page outline the top five recorded viruses, and their daily averages over the past month as outlined by TrendMicro, BitDefender and NOD AV.

For more information regarding viruses, please refer to the following websites:

- [Trend Micro](#)
- [Bit Defender](#)
- [Virus Radar](#)

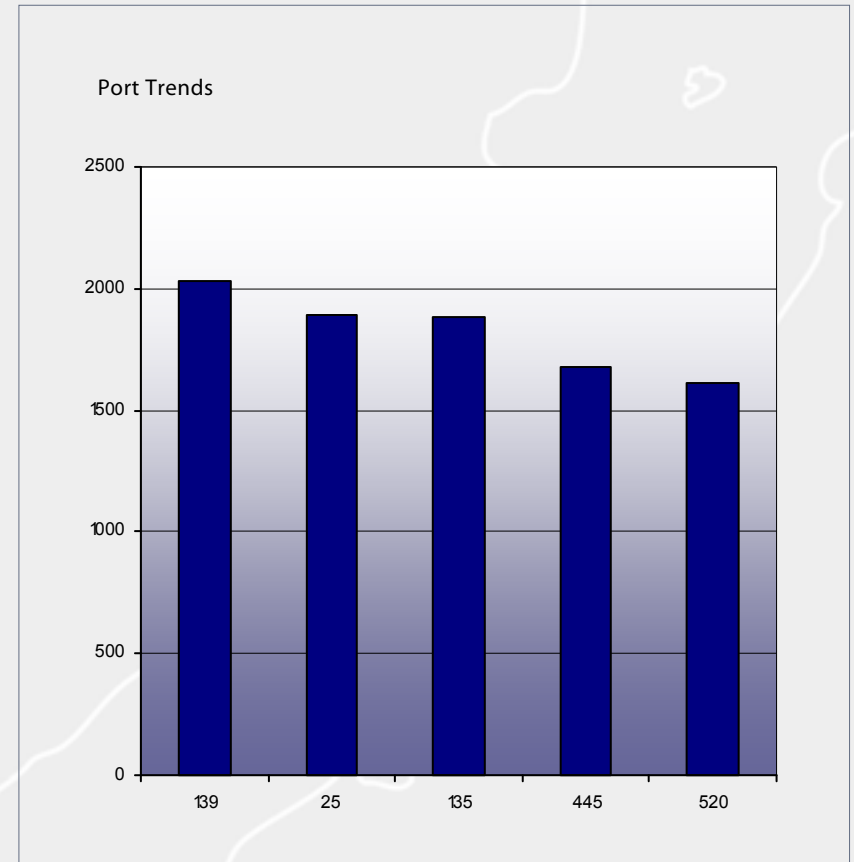


Port Scanning Activity

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 average number of daily 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.

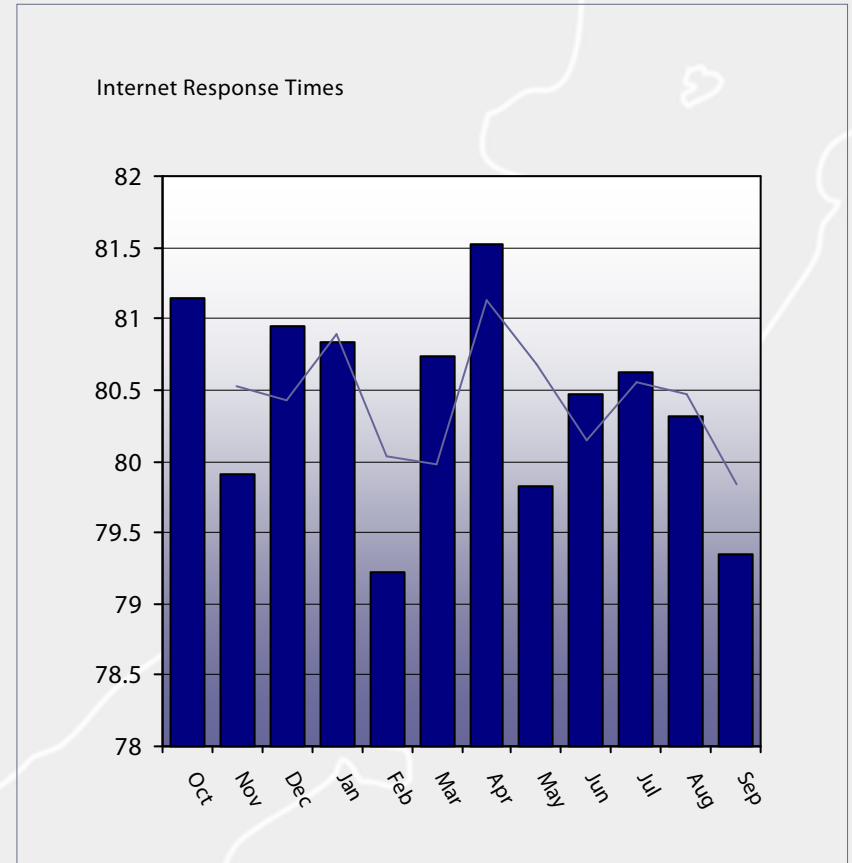


Internet Response Times

Internet Response trends for the month of September took a slight downward turn, with the New Zealand router response time remaining at a steady average of 199ms, and an overall Traffic Index average of 79.3. This is a lower than normal Traffic Index figure, indicating reduced internet performance throughout September.

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.

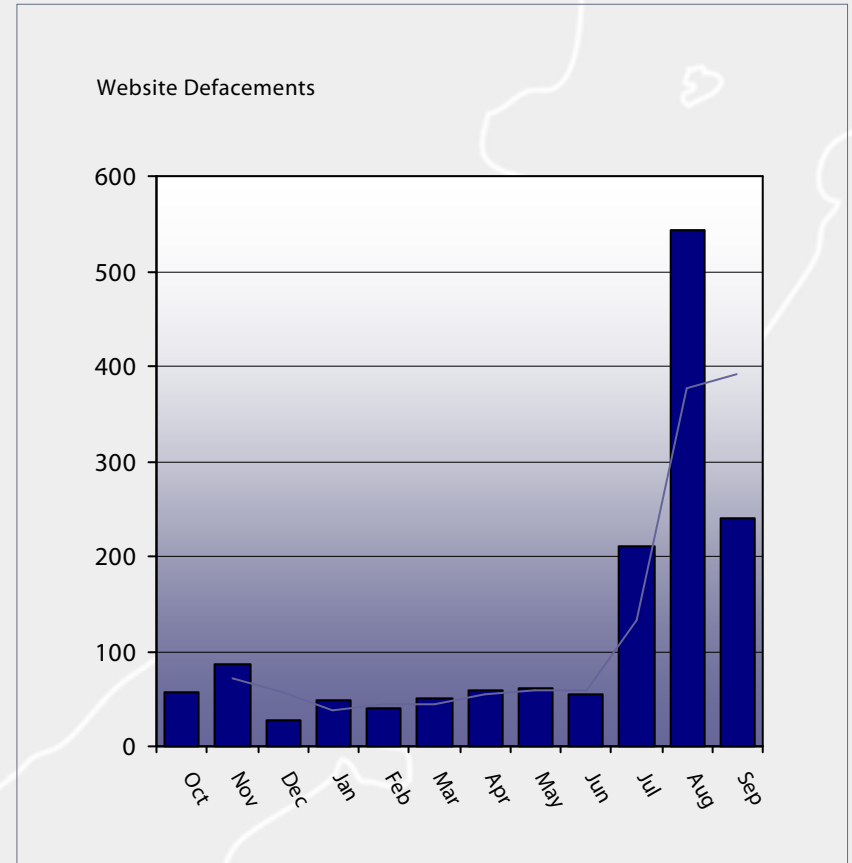


Website Defacements

Defacements of New Zealand websites for the month of September continued the recent trend of high figures, but was down on last month's record setting figures. September saw 241 reported New Zealand websites defaced compared with August's record setting 544 defacements. This month's figure is an average of 5 times the normal monthly total for reported defacements, and dragged the average number of defacements for the last 12 months up to 106 per month - well above the normal monthly average of 52 defacements.

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.