

CCIP Monthly Report for JULY

Welcome to the July issue of the Monthly Report produced by the Centre for Critical Infrastructure Protection's 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](#)[Internet Response Times](#)[Website Defacements](#)[Contact Details & Disclaimer](#)

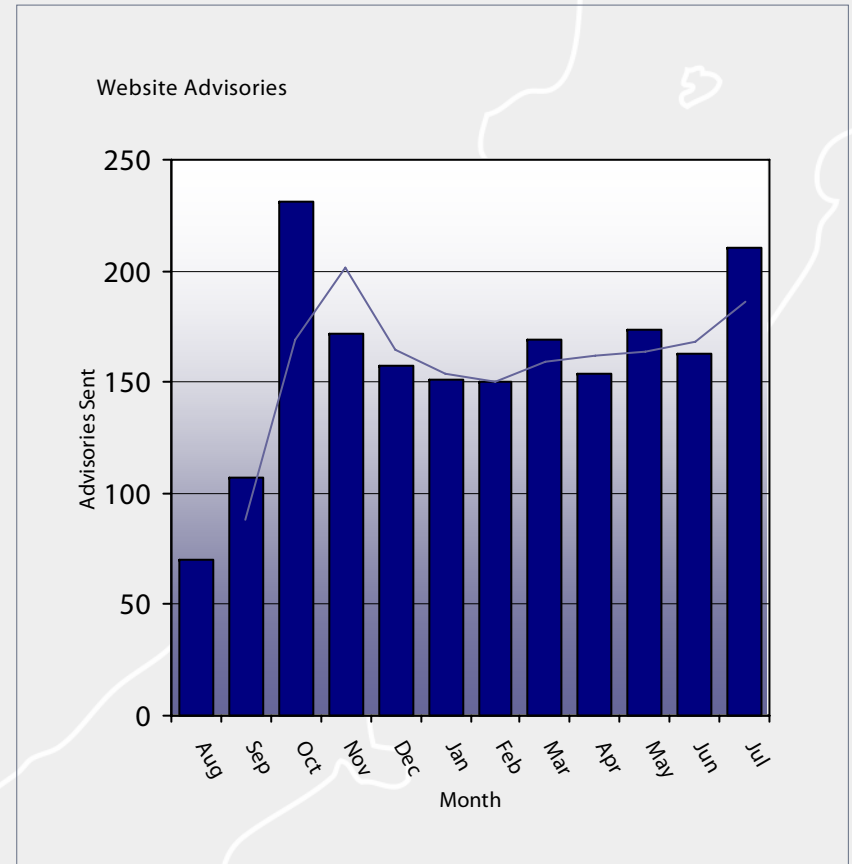
Operations Centre Activity

The month of July saw an increase in the number of advisories posted to the CCIP website, with a total of 210 vulnerabilities identified, compared to the June total of 163. The number of advisories that were deemed to be of significant importance for July also increased, standing at 32 significant advisories.

Advisories of major significance during the month included a number of planned security updates for Microsoft on the 11th July, in addition to a number of advisories from Mozilla and other software vendors..

Alerts sent directly via the CCIP mailing lists throughout July increased significantly, with 14 alerts being sent out, relating to a number of different vulnerabilities that were deemed to be of significant risk by the CCIP Operations Centre.

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

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

Date	Detail	Source
30/07/07	Widgets YDP ActiveX Control Buffer Overflow Vulnerability	Yahoo!
27/07/07	Windows URI Handling Command Execution Vulnerability	Microsoft
26/07/07	ETrust Intrusion Detection CallCode ActiveX Control InsecureMethods	CA
26/07/07	SeaMonkey Multiple Vulnerabilities	Mozilla
25/07/07	Oracle for OpenView Multiple Vulnerabilities	HP
24/07/07	Antivirus Multiple File Processing Vulnerabilities	NOD32
23/07/07	Access Gateway Multiple Vulnerabilities	Citrix
23/07/07	DirectX RLE Compressed Targa Image Processing BufferOverflow	Microsoft
19/07/07	Firefox Multiple Vulnerabilities	Mozilla
19/07/07	Products Multiple Vulnerabilities	Oracle
13/07/07	Products CAB and RAR Archive Handling Vulnerabilities	Symantec
13/07/07	QuickTime Multiple Vulnerabilities	Apple
13/07/07	Kerberos KDC Multiple Vulnerabilities	Novell
12/07/07	Flash Player Multiple Vulnerabilities	Adobe
11/07/07	Excel Multiple Code Execution Vulnerabilities	Microsoft
11/07/07	Windows Active Directory Two Vulnerabilities	Microsoft
11/07/07	.NET Framework Multiple Vulnerabilities	Microsoft
11/07/07	Office Publisher Invalid Memory Reference Vulnerability	Microsoft
11/07/07	Java JRE Web Start JNLP File Processing Buffer Overflow	Sun
11/07/07	"firefoxurl" URI Handler Registration Vulnerability	Firefox

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

- [Issue 41 ~ 9 July 2007](#)
 - Cyber Storm Warning
 - SCADA & Control Systems Procurement Project
 - The F-Secure Data Security Summary of January - June 2007
 - Finding XSS & SQLI Vulnerabilities
 - BITS Email Security Toolkit
 - Getting Real about Security Governance
 - X-Morphic Exploitation
- [Issue 42 ~ 23 July 2007](#)
 - When Spambots Attack — Each Other!
 - CIS Benchmarks
 - How to Conduct Firewall Configuration Reviews
 - Phishing under the Microscope
 - Global Security Week 2007: “Privacy in the 21st Century”
 - Employees Pose Biggest Cyber Security Risk

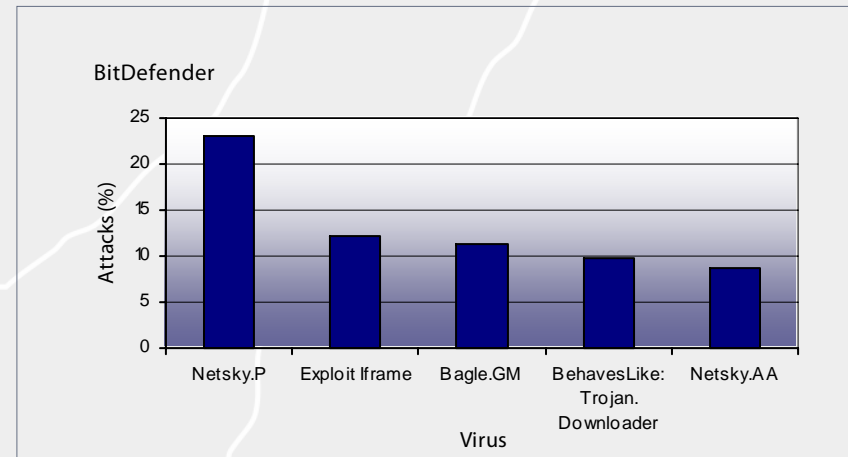
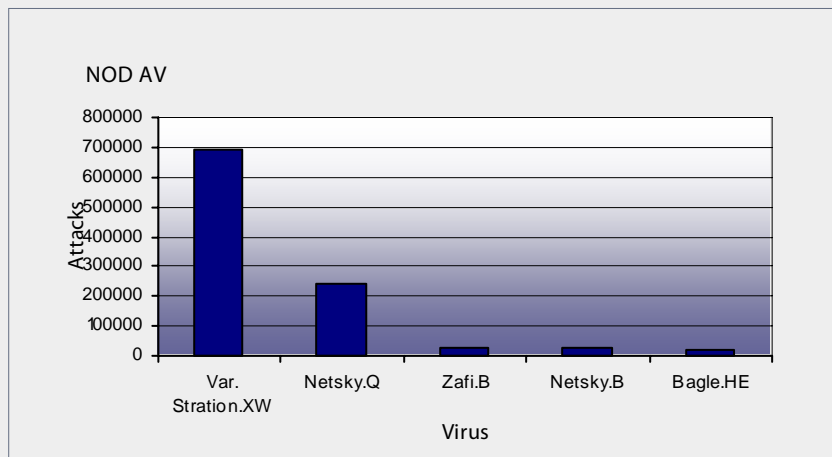
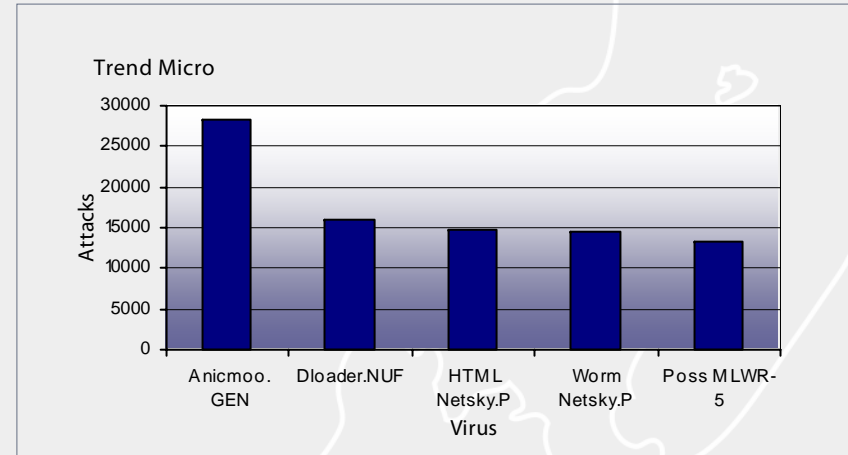
e-Bulletins are sent to members of the CCIP mailing lists. Back issues can be obtained by visiting the [Publications](#) page of the CCIP website.

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

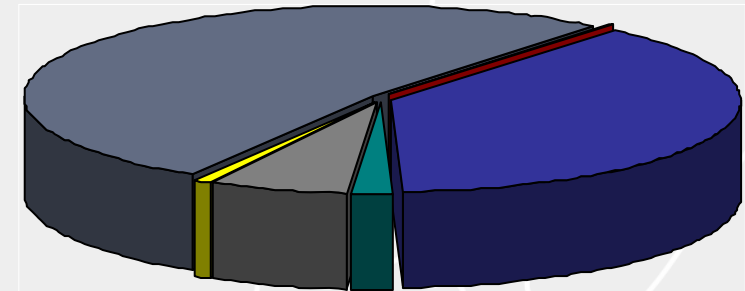
Australasia's profile experienced another upsurge on the virus front, with 0.71% of all virus detected worldwide attributed to this region by Trend Micro. Whilst the total of 74,590 viruses detected in the region, compared to the June figure of 108,183 for the region was lower, the overall percentage in July was higher, with only 0.55% of all viruses detected attributed to this region throughout June.

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.

Note:- The figures are based upon the statistics gathered by Trend Micro only and do not represent a comprehensive profile of the regional distribution of virus activity.

Regional Distribution



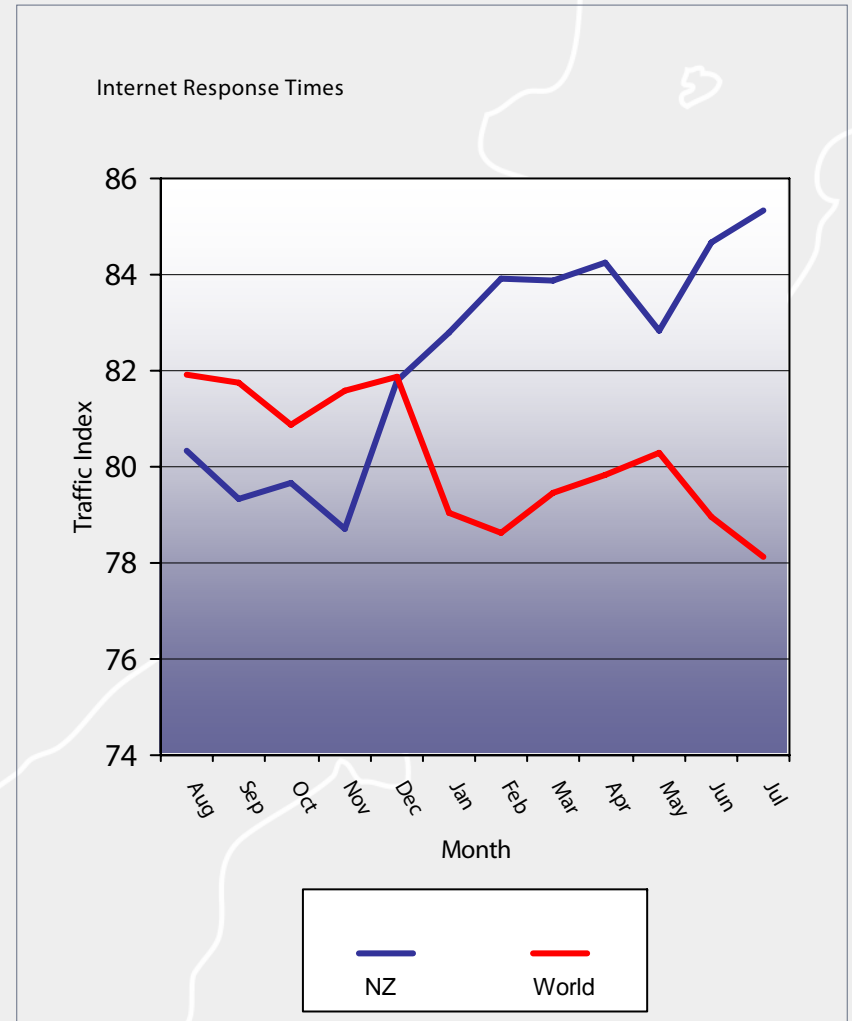
7,681	Unknown	0.07%
3,975,639	North America	37.95%
196,954	South America	1.88%
662,262	Europe	6.32%
74,590	Australasia	0.71%
5,414,820	Asia	51.68%
24,559	Africa	0.23%

Internet Response Times

Internet response time in New Zealand throughout the month of July decreased, indicating improved Internet performance. The average response time was 142ms, compared to the June figure of 148ms. This gave New Zealand an overall Traffic Index throughout July of 85.3, up from the June Traffic Index of 84.6. The world average Traffic Index stands at 78.1, down from the June figure of 78.9.

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.

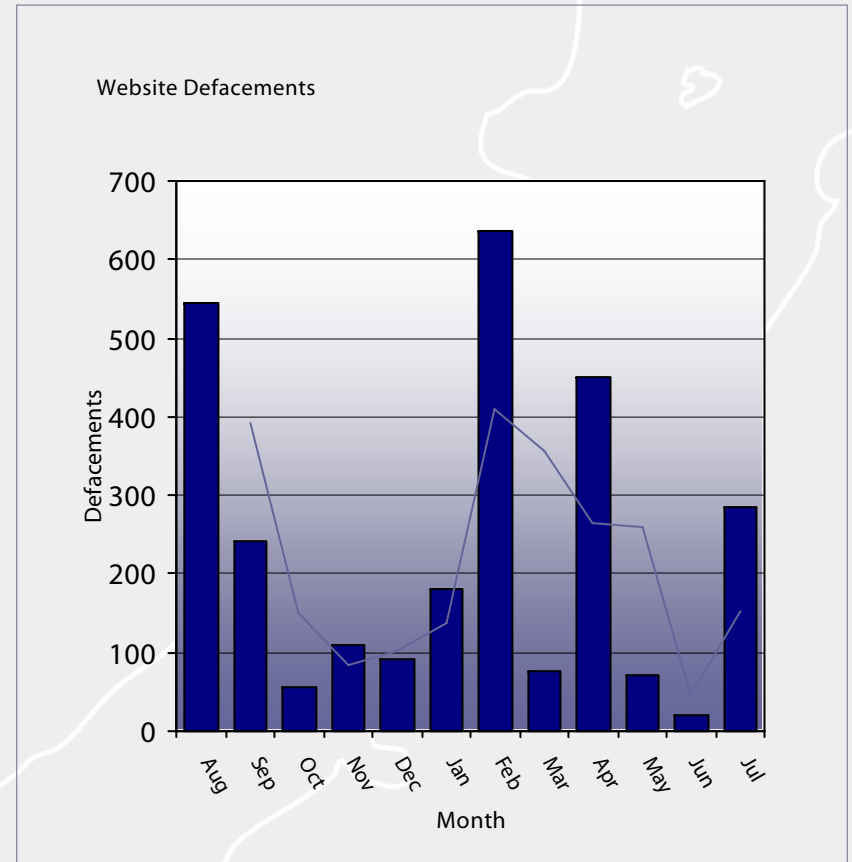


Website Defacements

Reported website defacements throughout the month of July took another big jump with a total of 286 New Zealand website being reported to Zone-H as defaced. The figure for June was 20 reported defacements. The large number for the month of July was added to by a mass defacement of a web server located in the United States on the 19th July by an attacker by the name of 'Tilkiandre'. The average number of New Zealand websites being defaced has grown to 230 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.