



NEWSLETTER

CENTRE for
CRITICAL INFRASTRUCTURE
PROTECTION

Volume 2, Issue 6

September 2003

NEW MID-MONTHLY NEWSLETTER

Welcome to the first compact version of the CCIP Newsletter focusing on recent alerts and advisories as well as the usual virus and port scan statistics. It is our intention to publish the mini at mid-month to complement our existing full-length edition which will be published on the first Wednesday of each month.

We will include links to matters of interest, and we start the ball rolling with an item from SANS. Marcus Sachs, previously Cyber Program Director, Information Analysis and Infrastructure Protection, US Department of Homeland Security, has joined SANS as a researcher, author and

speaker. He has recently published a briefing for senior IT managers on the latest Microsoft RPC vulnerability, which covers the following four topics plus a selection of other relevant material:

What is MS03-039? What happens if I do nothing? What systems are affected? What can I do about it? This document is available at: <http://www.sans.org/rr/special/MS03-039.pdf>

The Australian Computer Emergency Response Team (AusCERT) are running the one-day course, Network Monitoring for System Administrators, on 5 November in Auckland (venue to be decided). This

is a companion course to Introduction to Network IDS, which was held earlier in the year. In this tutorial, participants:

1. gain an understanding of the fundamentals of inspecting networks under attack;
2. gain an understanding of the techniques required to investigate networks recently attacked in order to gather evidence of computer intrusion; and
3. take away a useful set of class notes along with other useful utilities used and mentioned during the workshop.

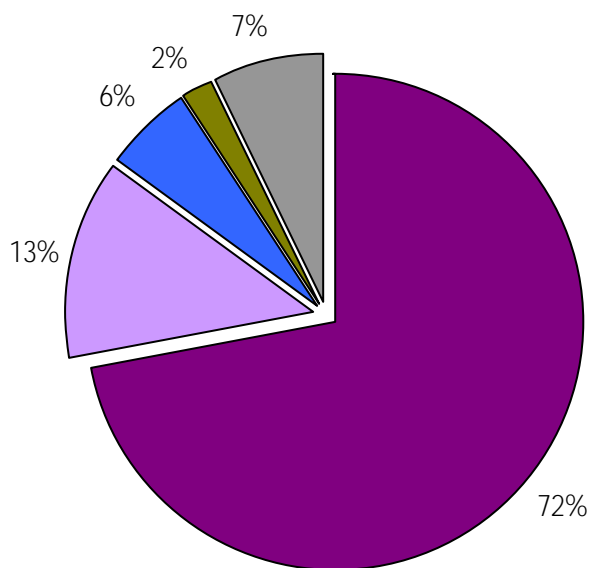
For further details go to: <http://www.auscert.org.au/render.html?it=2408>

IN THIS ISSUE:

<i>New Zealand Port Scanning Activity</i>	1
<i>Virus Activity</i>	2
<i>Recent Significant Alerts & Advisories</i>	2

NEW ZEALAND PORT SCANNING ACTIVITY

New Zealand port scanning activity by port number from 22 August to 17 September.



■ 135 MS RPC + ■ 137 NetBIOS NS + ■ 80 www + ■ 445 Win2K SMB ■ Other

Port 135 accounted for over two thirds of the port scanning carried out in New Zealand according to the [Internet Storm Center](#). This activity is mirrored globally and is related to the recent exploits of the Microsoft RPC vulnerabilities discussed in MS03-026 and MS03-039 security bulletins. Both of these bulletins have a maximum severity rating of Critical and should be patched within 48 hours of the bulletins release.

Exploit code is now available for the MS03-039 vulnerability, and given recent experience it is likely that a worm is imminent.

Communication regarding this newsletter can be addressed to:

newsletter@ccip.govt.nz



Government
Communications
Security Bureau

CONTACT DETAILS

Ph: +64 4 498 7654

Fax: +64 4 498 7655

Email: info@ccip.govt.nz

Web: www.ccip.govt.nz

PO Box 12-209

Wellington, New Zealand



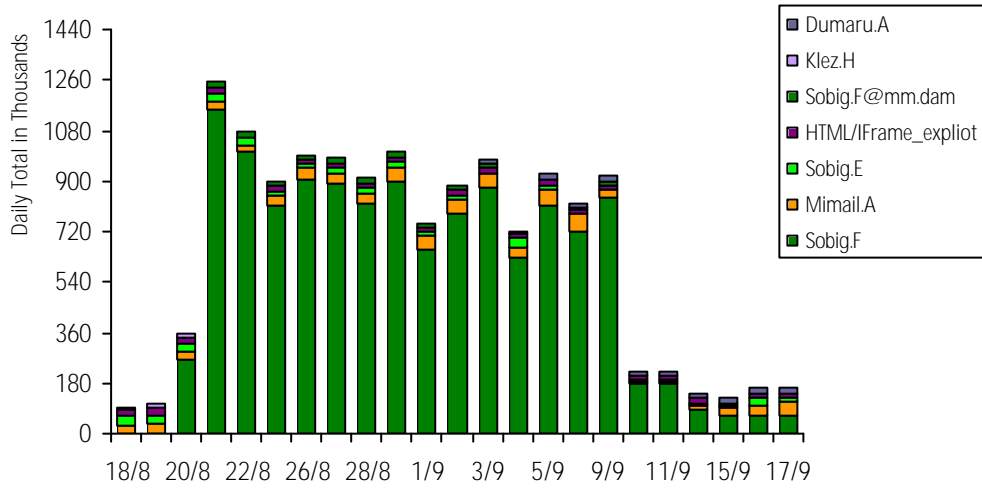
VIRUS ACTIVITY

In this edition we have chosen to include virus data from [RAV](#) (Reliable Anti-Virus). This data clearly shows the arrival of Sobig.F on 20 August and the built in shutdown of the infection routine from 10 September onwards. The voracity of the

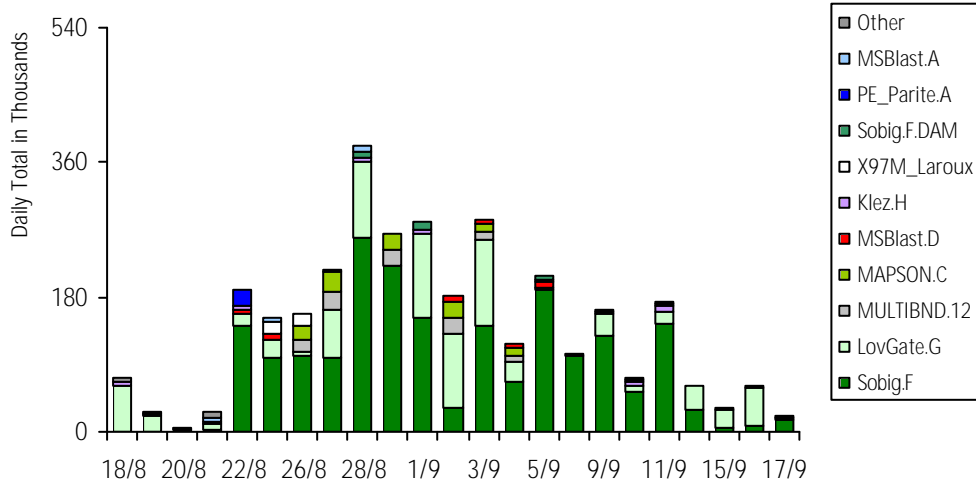
Sobig.F infections may have been exacerbated by the "blackholing" of 20 IP addresses Sobig.F intended to use for the download of code. This download step, if completed, actually terminated the infection stage of the virus. Unable to

complete this step, Sobig.F continued to spread until the programmed shutdown date, 10 September. An article discussing the evolution of Sobig variants will feature in the next CCIP newsletter.

Top 5 viruses captured worldwide by RAV



Top 5 viruses captured worldwide by TrendMicro



RECENT SIGNIFICANT ALERTS & ADVISORIES

Reference	Description	Date
CERT	Buffer Management Vulnerability in OpenSSH	17/9
Microsoft	Buffer Overrun In RPCSS Service Could Allow Code Execution	11/9
Microsoft	Cumulative Patch for Internet Explorer - Updated	9/9
Microsoft	Flaw in Visual Basic for Applications Could Allow Arbitrary Code Execution	4/9
Oracle	Buffer Overflow in XML Database of Oracle9i Server	1/9

DISCLAIMER

While this newsletter is accurate to the best of our knowledge, CCIP does not accept any responsibility for errors or omissions. If any of the vulnerabilities affects you, you are advised to ensure that you have the most current information available. 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 newsletter.

CCIP only issues those external alerts that we assess as serious and would affect a large number of NZ users. For notification of all discovered software vulnerabilities we recommend that you subscribe to a commercial Computer Emergency Response Team or to vendor alert lists.

Reference in this newsletter in any manner to any commercial product, process or service does not constitute or imply its endorsement or recommendation by CCIP. Views and opinions stressed herein may not be used for advertising or product endorsement purposes.

Please refer to the CCIP website for a list of recent alerts and advisories.

