



NEWSLETTER

CENTRE for
CRITICAL INFRASTRUCTURE
PROTECTION

Volume 2, Issue 12

December 2003

SEASON'S GREETINGS

In this final edition of the CCIP Newsletter for this year, we review port-scanning activity in New Zealand, as well as worldwide malware statistics for the past twelve months.

On the port-scanning front, port 137 (scanning for unprotected Windows networking shares) has appeared consistently throughout the year but now appears to be tapering off slightly. From March to August, port 445 (more Microsoft networking vulnerabilities) added significantly to the numbers, contributing up to 50 percent of the targets scanned. In August we saw the first major appearance of port 135, used for the propagation of the Blaster and Nachi worms. There were two major peaks during the year, the first in

April when Windows vulnerability scanning was at its most active and the second in August when the Blaster worm began propagating. Interestingly, the January statistics for New Zealand, as reported by the [Internet Storm Center](#), do not follow the international trend for the SQL Slammer worm, which peaked at over [16 million reports](#) not long after its release. The worm used UDP port 1434 to propagate. This could suggest that Kiwis are more responsible when it comes to maintaining patch levels, as the patch for the targeted vulnerability had been available for six months prior to the outbreak.

This fortnight the virus graphs are different from previous newsletters. We have compiled the daily top five viruses into monthly totals for the year since

February.

The individually recognised viruses in these graphs achieved more than 0.005% of the year's total. The remaining 48 viruses for TrendMicro and 13 viruses for MessageLabs data did not make this threshold and have been combined and represented as the "Other" category.

In both these data sets September was the worst month for total virus numbers. This is also substantiated by RAV, another anti-virus vendor whose data we monitor daily. Sobig.F was largely responsible for the huge number of infections detected in September. It remained the most prevalent virus until September 10, the date it was programmed to stop spreading. During September Sobig.F accounted for approximately

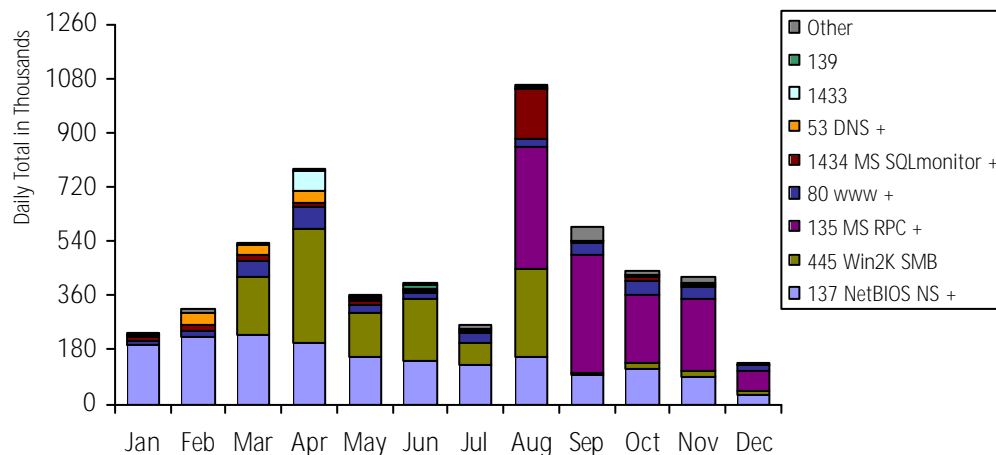
(Continued on page 2)

IN THIS ISSUE:

<i>Season's Greetings</i>	1
<i>& Happy New Year</i>	2
<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 for the year 2003.



Communication regarding this newsletter should be addressed to: newsletter@ccip.govt.nz



Government
Communications
Security Bureau

CONTACT DETAILS

Ph: +64 4 498 7654
Fax: +64 4 498 7655

E-mail: info@ccip.govt.nz
Web: www.ccip.govt.nz

PO Box 12-209
Wellington, New Zealand



& HAPPY NEW YEAR (cont. from Season's Greetings.)

(Continued from page 1)

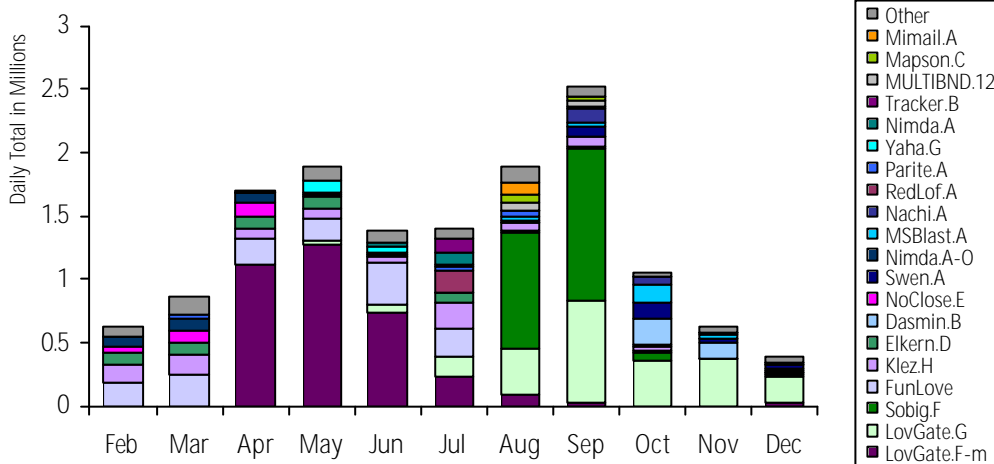
2.5 million detected infections, and in fact around half of all viral incidents detected by MessageLabs for the year were due to Sobig.F. A

couple of other viruses were detected over one million times in a calendar month; Sobig.F (August and September), Swen.A (October), and Lovgate.F (April and May). Klez.H is the

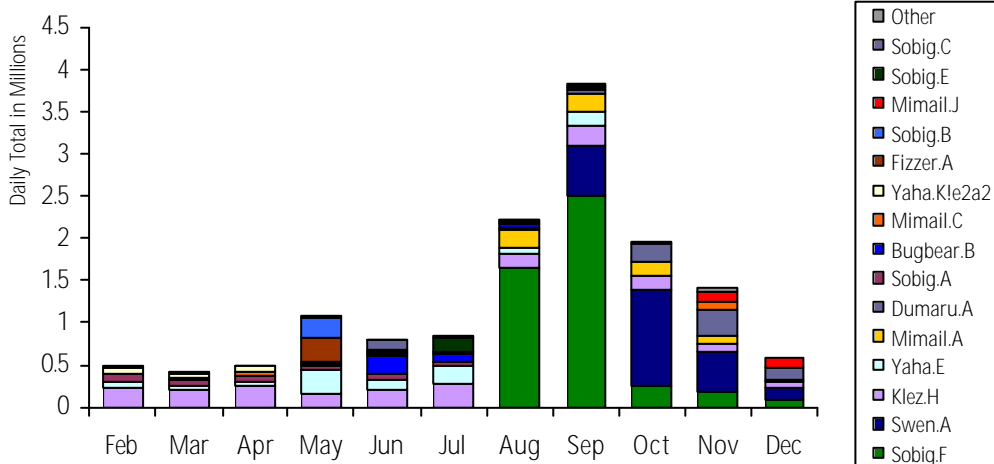
only virus we recorded in the daily top 5 for each month in both data sets. Funlove was persistent for the year in the TrendMicro data only.

VIRUS ACTIVITY

Daily top five viruses captured worldwide by TrendMicro for the year 2003



Daily top 5 viruses captured worldwide by MessageLabs for the year 2003



RECENT SIGNIFICANT ALERTS & ADVISORIES

Reference	Description	Date
Computer Associates	Vulnerability in Unicenter Remote Control and ControlIT	16/12
Cisco	PIX firewall vulnerabilities	16/12
ISC	BIND 8.4.3 has been retired, due to non security related bug	12/12
NGSSoftware	Sybase - Adaptive Server Anywhere Network Server Version 9.0.0 has multiple vulnerabilities	12/12
Cisco	Updated Cisco security notice for Blaster worm	11/12

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.

