



# NEWSLETTER

CENTRE for  
CRITICAL INFRASTRUCTURE  
PROTECTION

Volume 2, Issue 8

October 2003

## SANS TOP 20 INTERNET SECURITY VULNERABILITIES

The following lists, produced by the SANS Institute, are the ten most commonly exploited services in Microsoft Windows, and the ten most commonly exploited services in UNIX and Linux.

### Microsoft Vulnerabilities:

1. Internet Information Services (IIS)
2. Microsoft SQL Server
3. Windows Authentication
4. Internet Explorer (IE)
5. Windows Remote Access Services
6. Microsoft Data Access Components (MDAC)
7. Windows Scripting Host
8. Microsoft Outlook/Outlook Express
9. Windows Peer-to-Peer

- File Sharing
10. Simple Network Management Protocol (SNMP)

### UNIX / Linux Vulnerabilities:

1. Berkeley Internet Name Domain (BIND) System
2. Remote Procedure Calls (RPC)
3. Apache Web Server
4. General UNIX Authentication -Accounts with No Passwords or Weak Passwords
5. Clear Text Services, e.g. telnet
6. Sendmail
7. Simple Network Management Protocol (SNMP)
8. Secure Shell (SSH)
9. Misconfiguration of

- Enterprise Services NIS/ NFS
10. Open Secure Sockets Layer (SSL)

According to the SANS website, "The vast majority of worms and other successful cyber attacks are made possible by vulnerabilities in a small number of common operating system services. Attackers are opportunistic. They take the easiest and most convenient route and exploit the best-known flaws with the most effective and widely available attack tools. They count on organizations not fixing the problems, and they often attack

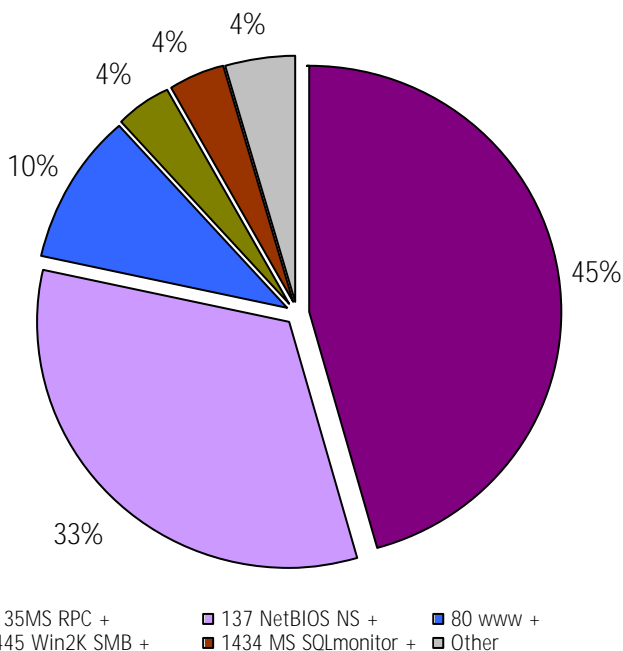
*(Continued on page 2)*

### IN THIS ISSUE:

- New Zealand Port Scanning Activity* 1
- Virus Activity* 2
- Recent Significant Alerts & Advisories* 2

## NEW ZEALAND PORT SCANNING ACTIVITY

New Zealand port scanning activity by port number from 18 September to 14 October.



Scanning for Microsoft Distributed Component Object Model (DCOM) ports accounts for over 75 percent of the port-scanning activity reported to incidents.org. Microsoft patch MS03-039 does not mitigate all known DCOM vulnerabilities. New exploit code has been released, we therefore recommend the following - use network or host-based/ personal firewalls, and block RPC network traffic (TCP ports 135, 139, 445, 593 and UDP ports 135, 137, 138, 445). More on the RPC DCOM vulnerabilities in the next CCIP newsletter.

Communication regarding this newsletter should be addressed to: [newsletter@ccip.govt.nz](mailto: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](mailto:info@ccip.govt.nz)  
Web: [www.ccip.govt.nz](http://www.ccip.govt.nz)

PO Box 12-209  
Wellington, New Zealand



## SANS TOP 20 INTERNET SECURITY VULNERABILITIES (cont.)

(Continued from page 1)

indiscriminately, scanning the Internet for any vulnerable systems. The easy

and destructive spread of worms, such as Blaster, Slammer, and Code Red, can be traced directly to

exploitation of unpatched vulnerabilities."

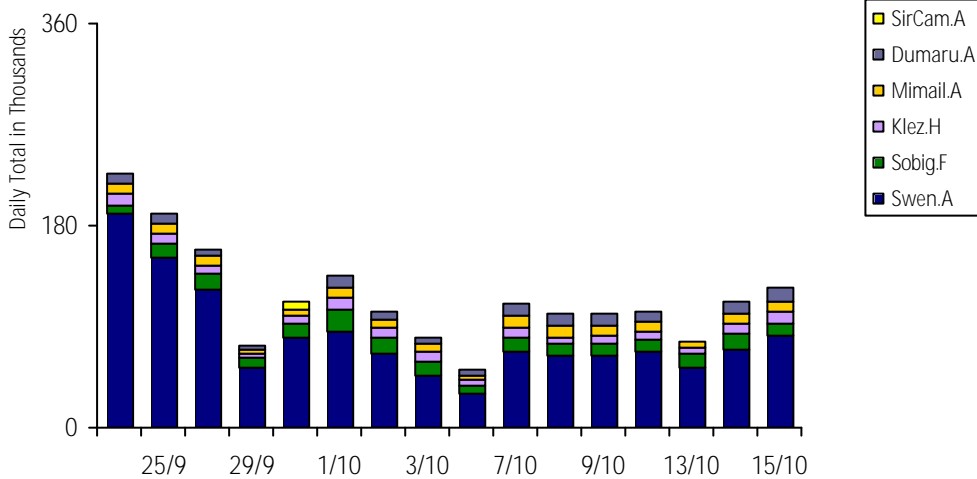
## VIRUS ACTIVITY

Swen.A features in the virus statistics for the last three weeks. It exploits a two-year old vulnerability in Internet

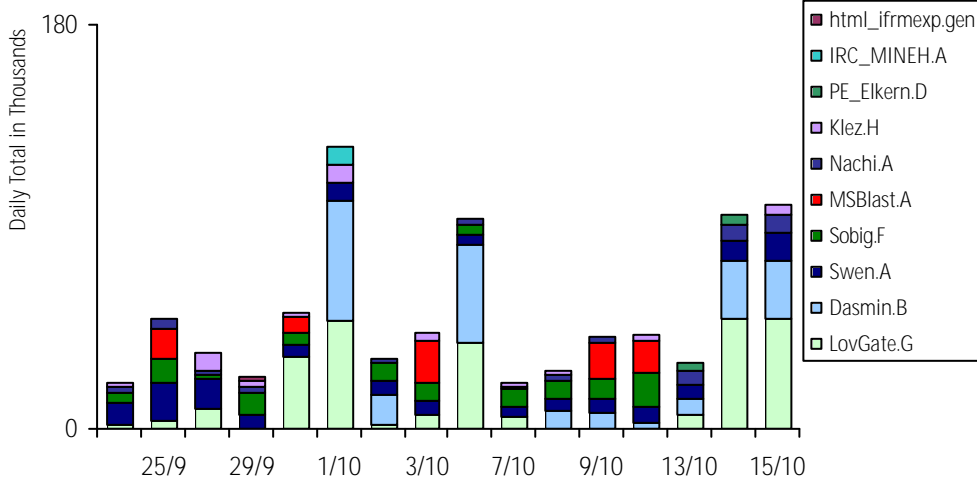
Explorer and arrives as an e-mail appearing to be a patch from Microsoft. Swen.A is being captured in significant

numbers so be aware that Microsoft does not send patches via e-mail.

Daily top 5 viruses captured worldwide by MessageLabs



Daily top 5 viruses captured worldwide by TrendMicro



## RECENT SIGNIFICANT ALERTS & ADVISORIES

Reference	Description	Date
UNIRAS	Microsoft Windows RPC DCOM Vulnerability	15/10
Microsoft	Cumulative Patch for Internet Explorer	6/10
CERT	Multiple Vulnerabilities in SSL/TLS Implementations	2/10
CERT	Exploitation of Internet Explorer Vulnerability	2/10

## 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.

