



NEWSLETTER

CENTRE for
CRITICAL INFRASTRUCTURE
PROTECTION

Volume 3, Issue 1

February 2004

A BUSY BEGINNING

It has been a busy start to 2004. The CCIP has published over 100 alerts and advisories to the [website](#). Three of these were prompted by the release of the National Infrastructure Security Co-ordination Centre (NISCC) advisory [006489/H323](#) on 13 January (see [H.323 Vulnerabilities](#) on page three).

Bagle and Mydoom are the latest viruses of note. Mydoom arrives as a .zip attachment (which passes through many e-mail gateways) and, interestingly, includes a list of excluded domains such as .mil and .gov. Bagle sends an executable file which harvests e-mail addresses and then resends itself,

usually with the subject line "test".

As usual, users should be educated to avoid opening unknown attachments, even if executable attachments are blocked at the network perimeter. The spread of these viruses also highlights the need to ensure that virus signature files are kept as up-to-date as possible.

OPERATING SYSTEM HARDENING

Typically, many Operating System (OS) installations are insecure by default. They can have services running that are not necessary for the general operation of the system. Often these services open various network ports, which provide a vector for the exploitation of vulnerabilities. Some OS's also have additional applications installed that may not be needed by an end user and which render systems vulnerable to IIS exploits, for example the Code Red and Nimda worms.

The requirements for frequent patch application are costly for many organisations. Systems administrators need to take the time to test new patches and prepare them for deployment throughout the network. This window of time for testing and rolling out patches is being diminished by the ever-decreasing time between vulnerability disclosure and exploit availability.

Advantages

OS hardening is a strategy to improve the security profile of any system, and to reduce the threat of compromise to that system. OS hardening is performed during installation and deployment of a system, and has many benefits, including:

- increased system security;
- lessened cost of on going administration;
- reduced reliance on urgent patch and hotfix applications to maintain system integrity;

- increased system uptime due to fewer patch and hotfix requirements; and
- improved system auditing ability due to simplification and increased knowledge of system components.

Disadvantages

The major disadvantage of OS hardening is that the process can take a significant amount of time (depending on the extent of hardening and the OS being hardened). In addition, the increased security of a system can reduce its ease of use or functionality. So any hardening procedure must be carefully planned in accordance with the acceptable levels of functionality and risk to a system.

Methodologies

Virtually every system can be hardened in some fashion. Most OS vendors have security

(Continued on page 2)

IN THIS ISSUE:

Operating System Hardening	1
H.323 Vulnerabilities	3
Virus Activity	3
New Zealand Port Scan Activity	4

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

OPERATING SYSTEMS HARDENING (cont.)

(Continued from page 1)

configuration or hardening recommendations for their system, and many third-party guides are available. Also, many server applications can and should be hardened before deployment (in particular web, mail and Domain Name Service (DNS) server applications, which are more likely to have direct connections to the Internet). Most modern firewalls come with a prehardened OS, which is often a minimised Unix distribution.

The methodology that is used for hardening varies depending on the extent of the hardening. Planning and documentation are essential.

There are five main steps to hardening a system:

1. Define the system's purpose

This will clarify the application requirements and which components and services will be removed or disabled.

2. Minimise system components

Remove applications and OS packages that will not be needed.

3. Minimise services

Disable all services that are not required for the day-to-day operation of the system.

4. Harden the configuration

This is the step where hardening guides and templates are most useful as they generally list the exact configuration commands, files, or registry keys used to harden the system. This step can also include setting secure password policies and

improvements to system auditing, such as log files and settings, remote logging and alerting.

5. Add additional security software

This is an optional step; however, the addition of host-based intrusion detection software (HIDS), such as Tripwire, or a host-based firewall can improve confidence in the security of a system.

Once these steps are complete, a baseline of the system should be recorded. The baseline should include the applications and OS components installed, services running, usernames and settings, and anything else the administrator thinks may be useful for future reference. This baseline should be used as a reference for regular system audits to ensure the integrity of the system is maintained. It is particularly important to review the system configuration after patch application as some patches re-enable disabled services or make changes to the configuration that may affect the security of the system.

Tools, Guides & Applications

There are many useful tools and guides for hardening systems. Some of the most popular and best-known third-party guides are published by the [National Security Agency](#) (NSA) and the [Center for Internet Security](#) (CIS).

The NSA publishes guides for Windows XP, Windows 2000, Windows NT, Solaris 8 and various applications including Microsoft SQL server and the Apache web

server. The Windows guides also come with template files. These templates can be used with the Windows Security Configuration and Analysis utility to analyse or apply security settings or, in conjunction with Group Policy, to apply settings over a number of hosts.

The CIS provides guides for Windows 2000, Windows NT, Solaris, Linux, HP-UX, Cisco IOS and Oracle Database. CIS also provides template files and separate benchmarking tools that measure compliance with the hardening recommendations.

With increasing security awareness, many application and OS vendors are now producing their own hardening guides and tools (as well as improving the default security of their products). The NSA has stated that it will not be producing its own guide for Windows Server 2003, instead linking to the Microsoft guide that contains tools and templates for securing Windows Server 2003 in a variety of configurations.

There are also tools that can be downloaded separately to harden OS's on their own, for example Bastille, which is a tool for hardening Unix & Linux OS's. It currently works with Debian, Mandrake, Red Hat, and Turbolinux Linux distributions as well as HP-UX and Mac OS X. The Titan tools perform similar operations on Solaris systems.

Some networking and security vendors are now developing host protection systems as they realise that,

(Continued on last page)

The methodology that is used for hardening varies depending on the extent of the hardening. Planning and documentation are essential.

System hardening should be part of your organisation's IT security policy, and the organisation should maintain a set of hardened builds for installing or rebuilding servers and workstations.

Operating Systems Hardening
page 4

H.323 VULNERABILITIES

Several vulnerabilities were recently discovered in the Ethernet protocol H.323. This protocol is widely used for packet-based multimedia communications such as videoconferencing and voice over IP (VoIP) across the Internet.

In 2002, Finland's Oulu University Secure Programming Group (OUSPG) examined the Simple Network Management Protocol (SNMP) for vulnerabilities.

They devised a test suite that discovered multiple vendor specific vulnerabilities in this protocol. As a result, the National Infrastructure Security Co-ordination Centre (NISCC) of the United Kingdom commissioned the OUSPG to perform similar studies on other protocols critical to the UK's information infrastructure. This list of critical protocols included the H.225 protocol, a component of H.323. The OUSPG-designed test suite

for this protocol was distributed to a range of vendors whose products utilised the H.225 and associated protocols. As a result, the vendors discovered various vulnerabilities, and on 13 January 2004 NISCC issued an [alert](#) concerning these issues.

While some vendors are unaffected, others may be vulnerable to Denial of Service attacks, or even

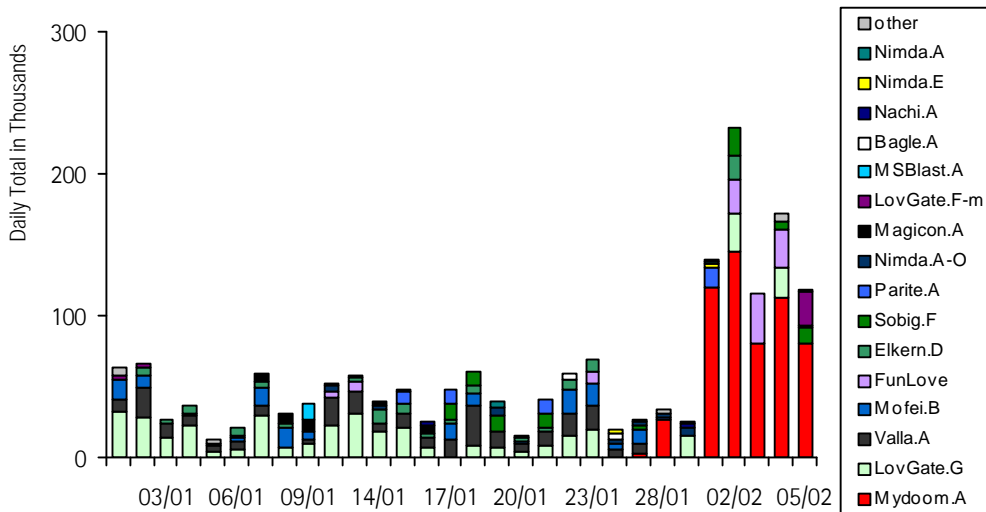
If you are using a product that is vulnerable, that product should be patched to remove the vulnerability as soon as possible.

H.323 Vulnerabilities page 4

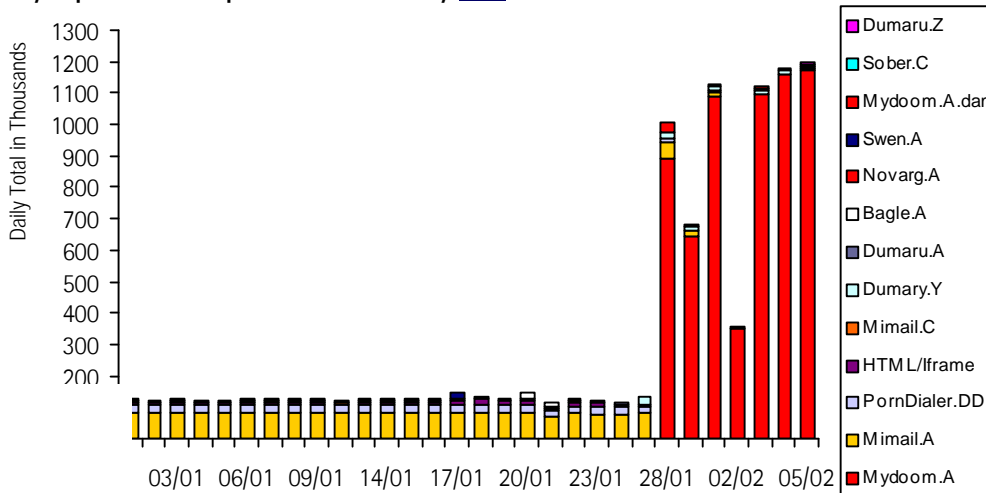
(Continued on last page)

VIRUS ACTIVITY

Daily top 5 viruses captured worldwide by [TrendMicro](#)



Daily top 5 viruses captured worldwide by [RAV](#)



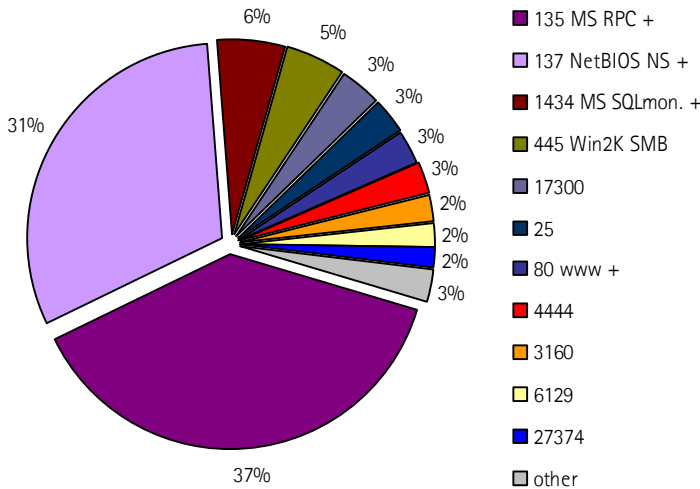
In e-mail security terms, the final week of January 2004 is unique. Never before have so many worms that demanded so much attention been released in such rapid succession. Whether or not the events of the week were planned is difficult to say as that would require a degree of co-operation on behalf of the groups behind each worm, and whether that happened will probably never be known.

[MessageLabs Intelligence Newsletter](#)



NEW ZEALAND PORT SCAN ACTIVITY

New Zealand port scanning activity by port number from 1 to 20 January.



While TCP/UDP port 135 is still the most commonly scanned port, scanning continues to decrease overall, with current levels about half of the August 2003 peak.

Another port of note is TCP 6129, registered to the `dameware_remote` administration tool. Scanning for this port has been causing some discussion on the bugtraq mail lists, due to the static source port characteristic of the scans. Incidents.org

H.323 VULNERABILITIES (cont.)

(Continued from page 3)

arbitrary code execution via buffer overflows. Many vendors (including Microsoft and Cisco) have published alerts concerning the potential exposure of their own products to the H.323 vulnerabilities. Many of these alerts are available through the CCIP website.

For information on a specific vendor's vulnerability status, refer to the NISCC alert

[page](#), which contains an up-to-date list of vendor responses and links to vendor home pages.

If you are using a product that is H.323 vulnerable, that product should be patched as soon as possible. If your organisation does not require H.323 protocols and applications for business reasons, then unnecessary ports (default ports for this protocol suite

are 1720 UDP and 1720 TCP, although these may vary from site to site) should be closed off at the network perimeter.

For other tips on securing your system, refer to our feature article on Operating System hardening.

OPERATING SYSTEM HARDENING (cont.)

(Continued from page 2)

increasingly, threats are bypassing traditional network defences such as firewalls. These types of products perform host firewalling functions and harden the system by restricting the types of behaviour that can be performed on a system.

Host based protection is becoming more important as part of an organisation's defence in depth strategy.

System hardening should be part of your organisation's IT security policy, and the organisation should maintain a set of hardened builds for installing or rebuilding servers and workstations. In addition, well-defined patch-management procedures and regular system auditing will help maintain the security of your network.

Links

- [NSA Security Recommendation Guides](#)
- [Center for Internet Security](#)
- [Microsoft Security Guidance for the Enterprise](#)

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.



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