



# NEWSLETTER

CENTRE for  
CRITICAL INFRASTRUCTURE  
PROTECTION

Volume 3, Issue 3

April 2004

## CRIME, COMMON SENSE & OPPORTUNITY

Police have laid New Zealand's first charges under the new Crimes Amendment (No 6) Act 2003. The act, created specifically for computer-related offences, imposes stiff penalties. The accused faces two charges for alleged damages to a U.S. company's website and computer systems. The maximum sentences being

seven and two years imprisonment respectively.

The [Internet Security Alliance](#) (ISA) has released a report "[Common Sense Guide to Cyber Security for Small Businesses](#)". This best practices guide is well worth perusal and adding to your information security library.

The Centre for Critical Infrastructure Protection (CCIP) has openings for watch centre analysts.

Please refer to page [four](#) of this newsletter for further details. The closing date for these positions is Thursday, 8 April 2004.

### INSIDE THIS ISSUE:

Virus Activity	3
Port Scan Activity	4
NISCC Technical Notes	4
CCIP Staff Vacancies	4

## PATCH MANAGEMENT

Information systems everywhere face attack. The software hosting and supporting an information system is the component most commonly targeted. Why is that? Well, information systems, as the name suggests, comprise information and a system. The system being an amalgamation of technology: hardware and software; processes: policies and configuration management; and of course people. All of which are vulnerable to attack. Hardware attacks require access to the equipment. Processes are vulnerable to security incidents due to misconfigurations. And the human component is subject to social engineering or "phishing scam" type attacks.

But it is the second part of the technology component, the software, that is the basis of this article.

Software is just that, "soft", and to fix problems inherent

in the software requires patching, a software update, or a configuration change.

Patching software, while essential to maintain the security and integrity of a system, has a cost. According to CCIP statistics there has been a 56 percent increase in the number of vendor bulletins so far this year. A recent [Yankee Group survey](#) estimated the cost to be US\$189 per patch, per computer, for companies with fewer than 5000 employees. Your organisation can work out the cost of adding a patch by using this [template](#).

It would seem that patching is here to stay and in fact the patching requirement is increasing. So the application of patches needs to become smarter. We are at a point where patching everything and then testing for adverse affects is not economical, and may not even be possible. And while the volume of advisories (and therefore patches) is

increasing, the testing window is decreasing. For example, in 2001 Nimda appeared 125 days after the vulnerability was disclosed; then in 2002 Slapper followed 45 days behind the vulnerability disclosure; and more recently Blaster was 26 days after vulnerability disclosure.

Once a vulnerability is disclosed some decisions need to be made. Are you at risk? If so, can the risk be eliminated by turning off the vulnerable service? Can the risk be mitigated by blocking the threat vector? Or can the vulnerability be remediated with a patch? As mentioned above, and possibly calculated by you or your organisation, applying a patch has associated costs. This cost is both a direct financial cost, a cost in time, and a cost associated with the possibility of the patch failing and harming the system. However, not applying a patch also has an associated cost, the cost of a

(Continued on page 2)



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

## PATCH MANAGEMENT (cont.)

(Continued from page 1)

compromise.

Looking at the patching risk analysis, two options are available:

1. Patch and test to prevent incidents;
2. Don't patch and recover from incidents.

The process of making these complex patching decisions is called Patch Management. If the decision is to patch, when is the ideal time to do so? Rush to remediate with a patch of unknown quality, and face failure because of a defective patch, or wait and risk a compromise? Beattie et al. studied this issue in their paper titled [Timing the Application of Security Patches for Optimal Uptime](#). They presented the notion that an optimal time to patch on production systems is between 10 to 30 days of the patch's release. This allows enough time to gain confidence in the patch while still closing the disclosed vulnerability, hopefully before an exploit becomes available.

The patch management process has a number of steps:

1. Identify new patches.
2. Assess applicability to your environment.
3. Test patches for need and interoperability.
4. Apply patches to all appropriate systems.
5. Review patch progress and validation.

These steps can be, and are, incorporated into automated patch management solutions, of which there are a large number on the market, for example:

The process of making these complex patching decisions is called Patch Management.

The use of an automated patching solution effectively lowers the cost of patch application and may allow more time to test.

- [BigFix](#): BigFix's Patch Manager 3.1 provides agent-based patch management for Windows (95 through 2003), Linux and UNIX platforms, including Red Hat and SUSE Linux, and Solaris, Mac OS X, HP-UX and AIX.
- [Citadel](#): Citadel's Hercules 2.2 has achieved Common Criteria Evaluation Assurance Level (EAL) 3 certification. It links to several third-party vulnerability assessment scanners and uses detailed "remediation signatures" to resolve both patches and configuration weaknesses, such as unsecured accounts and unused services on Windows (NT through XP/2003), Solaris and Red Hat Linux.
- [Configuresoft](#): Configuresoft's Security Update Manager works with its Enterprise Configuration Manager (ECM) to identify specific patching requirements for Windows (NT through 2003) and deploy them.
- [Ecora](#): Ecora's Patch Manager 3.1 provides patch management capabilities for Solaris and Microsoft products.
- [GFI](#): GFI's LANguard Network Security Scanner combines network scanning with patch management by identifying configuration errors and patching Windows (NT through 2003) and applications.
- [Novadigm](#), Novadigm's Radia Patch Manager provides agent-based patch management for Windows platforms, Unix and Linux.
- [Patchlink](#), Patchlink's Update 6.0 supports various platforms and applications, including Windows, Novell NetWare, AIX, Solaris, Linux and Macintosh.
- [Shavlik Technologies](#): Shavlik's HFNetChkPro 4.1 enhances Microsoft's free Microsoft Baseline Security Analyzer (which Shavlik developed) with both GUI and command-line capability. Shavlik's recent acquisition of Gibraltar Software adds agent-based patching capability for Windows, as well as support for Red Hat Linux and Solaris.
- [St. Bernard Software](#): St. Bernard's UpdateExpert 6.1 uses either agent or agentless capabilities to patch systems for Windows (NT through 2003), Office, SQL Server, IE and IIS.

There are also the dedicated Microsoft options: Windows Update, Office Update, Microsoft Baseline Security Advisor (MSBA), Systems Management Server (SMS) and Software Update Service (SUS - which is undergoing a metamorphosis to Windows Update Service or WUS). A comparison of the Microsoft solutions is available [here](#). Most of this list was compiled by Pete Lindstrom in his recent Information Security

(Continued on page 3)

## PATCH MANAGEMENT (cont.)

(Continued from page 2)  
 magazine article ["Patch in Time"](#).

The use of an automated patching solution effectively lowers the cost of patch application and may allow more time to test. The cost of recovering from a defective patch still exists. In this situation organisations will have to rely on their ability to recover, using a system restore or by

uninstalling the offending patch.

If your organisation is considering a patch management solution, a comparison of various solutions is available [here](#).

A useful mailing list is available to those interested in patch management and can be found at [PatchManagement.org](#). The list receives, on average,

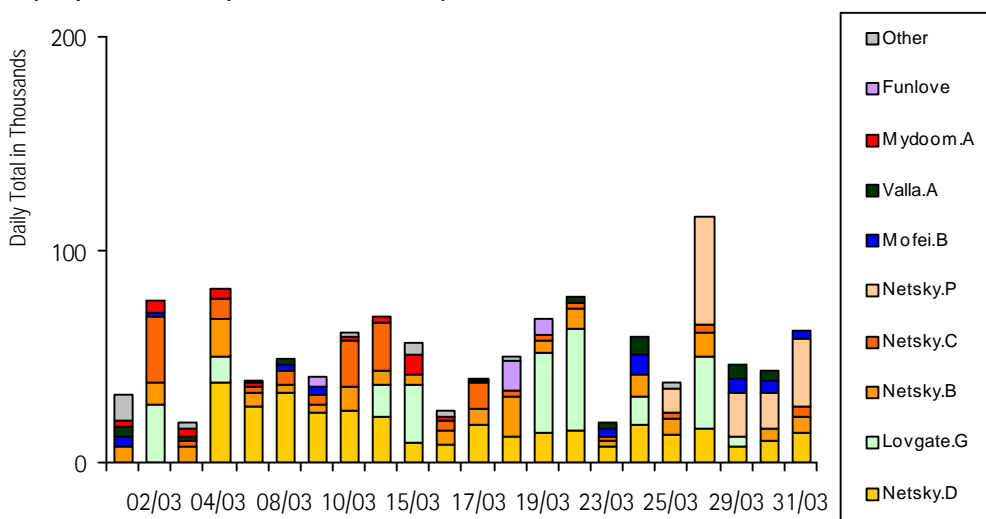
around 10 postings per day.

The following is a quote from the website: "The industry's first mailing list dedicated to the discussion of patch management. Whether it's a Linux operating system patch or a Microsoft application hotfix, this is the place to find more information about it."

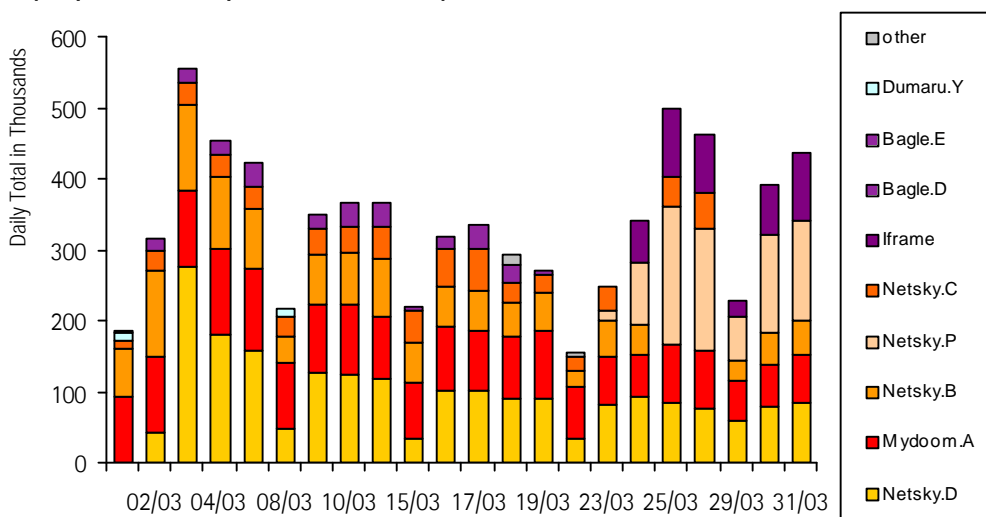
If your organisation is considering a patch management solution, a comparison of various solutions is available [here](#).

## VIRUS ACTIVITY

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



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



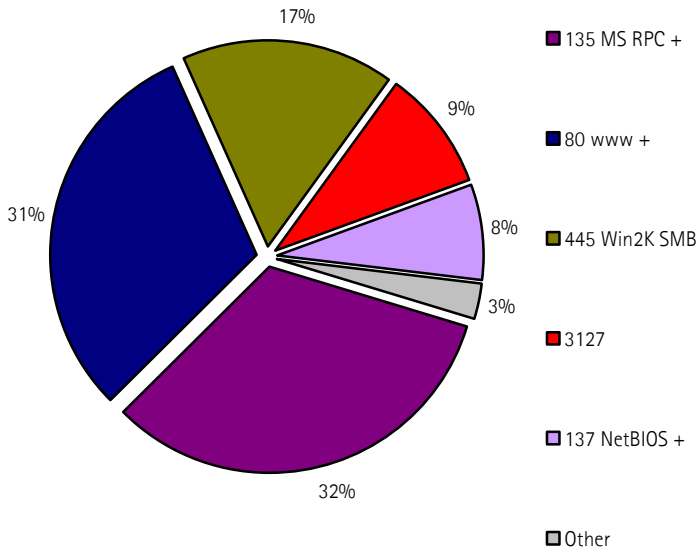
"The industry's first mailing list dedicated to the discussion of patch management. Whether it's a Linux operating system patch or a Microsoft application hotfix, this is the place to find more information about it."

[PatchManagement.org](#)



## NEW ZEALAND PORT SCAN ACTIVITY

New Zealand port scanning activity by port number for March.



Scanning for TCP/UDP ports 135,137 and 445 continue to appear in the daily top five scanned ports. Scanning for the Mydoom backdoor also continues this month with TCP port 3127 accounting for around 10 percent of New Zealand port scanning activity.

For more information see [Incidents.org](http://Incidents.org).

On the virus front, Netsky variants (of which there has been 17 in the last month and a half) dominates the virus graphs for March.

## NISCC TECHNICAL NOTES

The National Infrastructure Security Co-ordination Centre (NISCC) in the UK has published several 'technical notes' covering topics concerning:

- Increased use of Trojan Horse Programmes;
- Spam Mitigation Techniques;
- Guidance on Handling Files with Possible Malicious Content; and
- Organisational Vulnerability Management Process

Further technical notes concerning best practice guidelines for the Border Gateway Protocol (BGP) is also in the pipeline.

Documents can be downloaded from the [NISCC website](http://NISCC website).

## CCIP STAFF VACANCIES

The Government Communications Security Bureau (GCSB) is seeking Watch Centre Analysts to join the CCIP at Head Office in Wellington.

CCIP Watch Centre Analysts research computer and communications threats, vulnerabilities and incidents, and provide timely advice to critical infrastructure organisations.

They also:

- have an understanding of information security fundamentals,

particularly network security and risk analysis.

- have a tertiary qualification in computing, communications, or an allied technical field. Or have work experience in IT security, computer systems management, development, or telecommunications.
- have excellent analytical and written communication skills and the ability to work well under pressure.

If you are interested, you must hold New Zealand citizenship and be at least 21 years of age.

A [job description](#) and [application form](#) are available online. Alternatively,

Call: 04 472 6881  
 Fax: 04 499 3701  
 E-mail: [hr@gcsb.govt.nz](mailto:hr@gcsb.govt.nz)

Applications close on Thursday 8 April 2004.

## 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](mailto:info@ccip.govt.nz)  
 Web: [www.ccip.govt.nz](http://www.ccip.govt.nz)

PO Box 12-209  
 Wellington, New Zealand