



NEWSLETTER

CENTRE for
CRITICAL INFRASTRUCTURE
PROTECTION

Volume 4, Issue 1

February 2005

WELCOME BACK

Unlike past years, the start of 2005 has been a relatively quiet period. Whilst there has been no significant release of particularly virulent malware, variants of Netsky, Bagle and Zafi are still doing the rounds. However, what has not changed is the number of significant advisory notices that have been published on our website. In addition to the usual smattering of *NIX security advisories published in the past month, there have also been a number of advisories published relating to other software vendors, including:

- IBM;
- Apple;
- Cisco;
- Juniper;
- Sun;
- Mozilla; and
- Oracle.

In this edition of the newsletter there is a bit of a Microsoft focus

as we take a look at their new Anti-Spyware solution. Also released last month, is their new Malicious Software Removal Tool, which should be another useful aid to keep handy especially if it will help lessen the spread of botnets. And let us not forget the proposed anti-virus software which is imminent.

We also have a look at the recently published Windows Server Product Roadmap and a very brief outline of Windows Server Release 2, which contains the usual batch of bug fixes, performance improvements and, last but not least, security enhancements.

Well worth a read is a report published late last year by the State Services Commission's E-government Unit, titled 'Trust and Security on the Internet'. Although it "assesses the threats that relate to e-government",

there is plenty of material which is common to all web-related activity that could equally apply to the non-government organisations. The report is available from the [SSC](#) website.

As mentioned in previous years, any feedback and/or contributions, relevant to the nation's critical information infrastructure, would be most welcome, particularly relating to electronic attacks, for example:

- intrusions;
- malware attacks; and
- trojans, etc.

And remember, KEEP THOSE SYSTEMS PATCHED and implement a robust 'defence-in-depth' infrastructure to protect your information.

US SCIP METHODOLOGY

The US Department of Homeland Security (DHS) operates SAFECOM, "the umbrella program within the Federal Government that co-ordinates local, state, federal and tribal public safety agencies and to improve public safety through more effective, efficient, interoperable wireless communication."¹

Under this program, DHS has recently released the guidelines document, "Statewide Communication Interoperability Planning (SCIP) Methodology". Published in November 2004, these guidelines are now available from the [SAFECOM](#) website.

The SCIP process is modelled after the strategic planning process used by the Commonwealth of Virginia and is designed to develop a strategic plan to overcome:

- Legacy equipment issues;
- Limited funding;
- Limited and fragmented planning;
- Cultural issues; and
- Inadequate radio spectrum (channels or frequencies)

A key objective was the implementation of reliable, real-time interoperable wireless communications for first responders, emergency services,

and law enforcement and public safety officials. More on the Virginia project can be found at the [Interoperability in Virginia](#) website.

References:

- 1 Statewide Communication Interoperability Planning Methodology, Department of Homeland Security, November 2004

CONTENTS

<i>Welcome Back</i>	1
<i>US SCIP Methodology</i>	1
<i>Microsoft's Anti-Spyware Solution</i>	2
<i>Windows Server Product Roadmap</i>	3
<i>Virus Activity</i>	4
<i>Recent Significant Alerts & Advisories</i>	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

Mail: P.O. Box 12-209
Wellington
New Zealand

Microsoft AntiSpyware (currently in Beta) ranked number one in a recent comparison of 20 anti-spyware tools.

Microsoft's Anti-Spyware Solution

Microsoft stresses that the Malicious Software Removal Tool is a post-infection removal utility only and should be used in conjunction with antivirus software.

Microsoft's Anti-Spyware Solution

MICROSOFT'S ANTI-SPYWARE SOLUTION

In December 2004, Microsoft joined the anti-spyware campaign when they acquired GIANT Company Software Incorporated, a United States based provider of anti-spyware and Internet security products. Based on GIANT's technology, Microsoft is developing the Windows AntiSpyware protection, detection and removal tool.

Microsoft AntiSpyware (currently in Beta) ranked number one in a recent [comparison of 20 anti-spyware tools](#), making 100 out of 134 (75%) critical detectionsⁱ. Since 25% of critical detections were missed, still further improvements are needed to detect and eradicate all instances of spyware. It only takes one spyware program to compromise the privacy of a system, monitor and steal information and deliver it to third parties.

The tool offers more than 50 ways to mitigate spyware installation onto users' computers. It accomplishes this by monitoring and blocking a number of unsolicited processes including:

- unauthorised connections to the Internet;
- automatic downloads of Internet Explorer add-ons;
- potentially unwanted programs starting when the user's PC is turned on; and

- changes to critical password, Internet, and system settings, security permissions, and applications.

If an unknown program is detected, the tool will prompt the user either to allow or deny the program to continue running. More information regarding Microsoft's strategy for mitigating spyware and other potentially unwanted software can be found [here](#)ⁱⁱ.

A free Beta version of this tool was released this month and is available for download from the Windows AntiSpyware [webpage](#)ⁱⁱⁱ.

In addition, users of the Windows AntiSpyware tool will be able to join [SpyNet](#)^{iv}, an online community where users can submit reports of potential spyware. These reports are used to classify and develop spyware detection signatures for distribution to all AntiSpyware users through the Windows AntiSpyware AutoUpdater.

Microsoft has also recently released The Malicious Software Removal Tool. This utility is designed to aid in the removal of malicious software, rated with a Microsoft severity rating of "Moderate" or higher. It can be run either online from Microsoft's

Malicious Software Removal Tool [webpage](#)^v or downloaded and run locally. The tool will be updated each month on "Patch Tuesday" (the second Tuesday of every month) and will be available via the Windows Update and Automatic Updates services (currently Windows XP only) and from the Windows Update website. Each update is cumulative, adding new malicious software detection/removal capabilities to the tool with each release. Microsoft stresses that the Malicious Software Removal Tool is a post-infection removal tool only and should be used in conjunction with antivirus software^{vi}.

The acquisition and development of these security tools from Microsoft is a step forward for Windows users, with improvements expected over time. Anti-spyware tools should be regarded as just one layer of your system's security posture. Firewalls, antivirus software, and up-to-date update security patches must also be maintained.

NB: These tools support computers running Windows 2000, Windows XP and Windows Server 2003 only. The Windows AntiSpyware tool is still in Beta and may have unresolved issues.

Microsoft's Anti-Spyware Solution References:

- "The Spyware Warrior Guide to Anti-Spyware Testing." Howes, Eric L. 2004. <http://spywarewarrior.com/asw-test-guide.htm>
- Spyware solutions: Technology and leadership. Microsoft's strategy for addressing spyware and other potentially unwanted software. December 17, 2004. <http://www.microsoft.com/athome/security/spyware/strategy.mspix>
- Microsoft Windows AntiSpyware <http://www.microsoft.com/athome/security/spyware/software/default.mspix>
- SpyNet™ Spyware Research Center <http://www.spynet.com>
- Malicious Software Removal Tool <http://www.microsoft.com/security/malwareremove/default.mspix>
- The Microsoft Windows Malicious Software Removal Tool helps remove specific, prevalent malicious software from computers that are running Windows Server 2003, Windows XP, or Windows 2000. January 11, 2005. <http://support.microsoft.com/?id=890830>

WINDOWS SERVER PRODUCT ROADMAP

Following Windows Server 2003 SP1 featured in last month's newsletter, is Windows Server 2003 Release 2 (R2). Due out in the latter half of 2005, R2 is described as the second version of windows 2003. The two-CD pack will incorporate Windows Server 2003 and service pack 1, and will also include:

- bug fixes;
- security enhancements; and
- performance improvements.

The second CD will contain additional optional feature packs such as Windows Rights Management Services.

The server will be available in the following three options:

1. Branch - to assist in management of branch offices;
2. Active Directory Federation Services - for use with e-commerce, which includes better web interoperability; or
3. Storage Management - focusing on simpler management of SANs and storage resource management.

Those customers currently using Windows Server 2003 with

Enterprise or Software Upgrade Assurance will receive R2 free of charge, with existing CALs transferable to R2. The release will also mean the end of shipping of the original 2003.

The table below has been published by Microsoft to reflect the key deliverables on the Windows Server roadmap.

For more information, see the [Windows Server Product Roadmap](#) webpage.

Windows Server 2003 Release 2 (R2). Due out in the later half of 2005, R2 is described as the second version of windows 2003.

Windows Server Product Roadmap

Windows Server Roadmap Deliverables

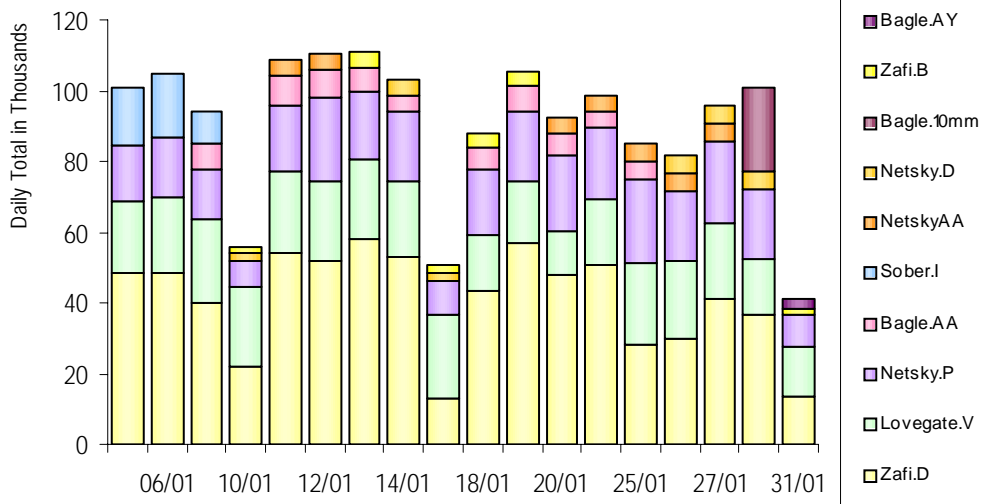
2005 (first half)	
Windows Server 2003 SP1	<ul style="list-style-type: none"> • Reliability improvements to address top customer issues • Security enhancements • Performance increased by up to 10 percent for key workloads
Windows Server 2003 for 64-Bit Extended Systems release	<ul style="list-style-type: none"> • Evolutionary path to 64-bit technology with greater price-performance. • Single code-base providing AMD Opteron and Intel Xeon EM64T support
2005 (second half)	
Windows Server 2003 "R2" Update	<ul style="list-style-type: none"> • Streamlined and secure information access for remote workers, trusted partners, and branch office users • Available to servers covered by Software Assurance (SA) at the time of release
Windows Server "Longhorn" Beta 1	<ul style="list-style-type: none"> • First available version of the next Windows Server major release, to be distributed to early adopter customers
2006	
Windows Server "Longhorn" Beta 2	<ul style="list-style-type: none"> • Code refresh of the next Windows Server major release, to be distributed to early adopter customers
Windows Server 2003 SP2	<ul style="list-style-type: none"> • Improvements to address top customer issues
2007	
Windows Server "Longhorn"	<ul style="list-style-type: none"> • Next-generation Web services application platform, including integrated management of IIS, ASP.NET, and the set of new .NET technologies that form the communications infrastructure code-named "Indigo" • Manageability from the ground up, such as role-based deployment that reduces maintenance and attack surface • New hardware and standards support, such as dynamic partitioning for Windows "mainframes" and support for PCI Express

The release of R2 will mean the end of shipping the original 2003. Existing CALs will be transferable to R2.

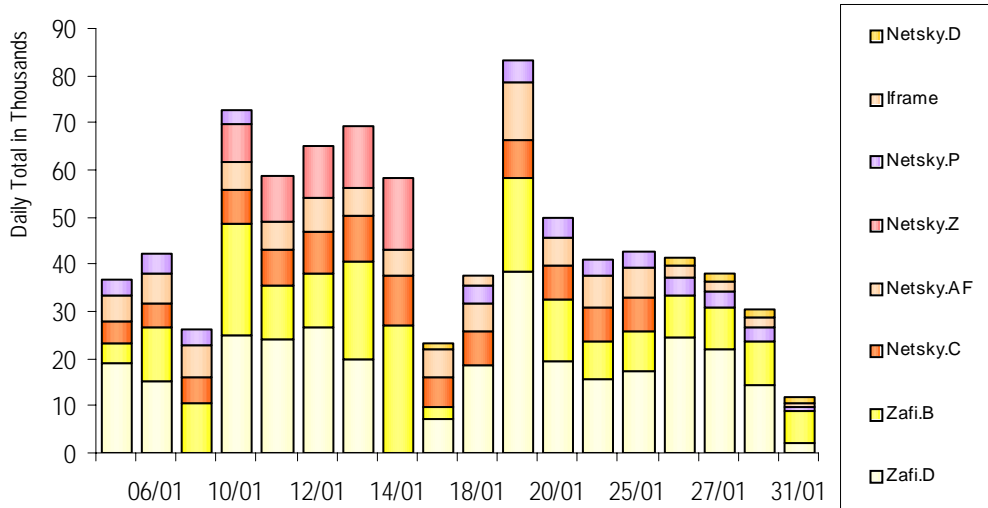
Windows Server Product Roadmap

VIRUS ACTIVITY

Daily Top Five: viruses captured worldwide by [BitDefender](#) for January.



Daily Top Five: viruses captured worldwide by [RAV](#) for January.



RECENT SIGNIFICANT ALERTS & ADVISORIES

REFERENCE	DESCRIPTION	DATE
Apple	Mac OS X Security Update Fixes Multiple Vulnerabilities	27/01
Cisco	Crafted Packet Causes Reload on Cisco Routers	27/01
Cisco	Multiple Crafted IPv6 Packets Cause Reload	27/01
Juniper	Juniper Denial of Service Vulnerability	27/01
UNIRAS	Vulnerability Issues with the BIND 9 Software	27/01
UNIRAS	Vulnerability Issues with the BIND 8 Software	27/01
Sun	Security Vulnerability in Solaris 8 DHCP Administration Utilities	25/01
iDEFENSE	Multiple Vendor xpdf PDF Viewer Buffer Overflow Vulnerability	25/01
Cisco	Vulnerability in Cisco IOS Embedded Call	21/01
RealPlayer	RealPlayer Vulnerabilities	21/01

Please refer to the [CCIP website](#) for a complete list of alerts & advisories.

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 New Zealand 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 expressed 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

Mail: P.O. Box 12-209
Wellington
New Zealand