



NEWSLETTER

CENTRE for
CRITICAL INFRASTRUCTURE
PROTECTION

Volume 4, Issue 2

April 2005

HOW SECURE IS SECURE?

Since the publication of our last newsletter there have been a number of significant events with at least one begging the question 'how secure is your Internet banking link?' Last month WestpacTrust New Zealand took the unusual step of disconnecting approximately 1400 Internet banking customers as a result of some users having installed a piece of 'Internet acceleration' software called MarketScore from ComScore, an online marketing company. This software effectively intercepts all encrypted and non-encrypted web traffic, stores the information in their databases for market research purposes and then reconnects the session to the original target website. If you are an AusCERT member, you have access to an excellent paper on this SSL [man-in-the-middle technique](#).

Alternatively, a Google search for 'MarketScore' will produce a number of excellent references, especially among the United States university community, particularly with regards to the detection and removal of the software.

On the patch front, Microsoft issued eight critical advisories in February but none in March. However two patches ([MS05-02](#) and [MS05-015](#)) were released last month to fix flaws in, among other things, Windows 98 & ME. There was also a reissue of [KB887742](#) that fixed a problem on Windows XP, which could stop responding if certain firewall and antivirus programs were installed. On the positive side, Bill Gates announced the impending release of Internet Explorer 7 at last month's [RSA Conference](#) and last week there was the official

launch of [Microsoft Windows Server 2003 Service Pack 1 \(32 bit\)](#).

Apple also released a new security update, [2005-003](#), which included updates to AFP Server, Mailman, Safari, Samba and Squirrelmail. New versions of [Mozilla, Firefox and Thunderbird](#) were also released to fix a highly critical vulnerability when processing GIF images.

In this edition of the newsletter, we take a look at Voice over Internet Protocol (VoIP) technology and explain some of the current technologies and relevant standards. In an upcoming issue we shall look into some of the security issues pertinent to a VoIP rollout. We also provide an analysis of website defacements in the .nz domain, as reported to Zone-H.org and pose the question 'how secure is your web server?'

VOICE OVER IP

Voice over Internet Protocol, also known as Internet Telephony and IP Telephony, is the ability to make voice telephone calls, send faxes and video-conference over IP based data networks¹, whether an organisation specific LAN (local area network), WAN (wide area network) or the Internet itself. User devices may be discrete devices, sometimes known as "hard phones" or software based "soft phones". Such devices include VoIP phones, PCs and other desktop or mobile VoIP devices such as laptop computers.

life with many manufacturers discontinuing product lines in favour of IP (Internet Protocol) telephony enabled replacements². The chances are, however, your data network is amongst the estimated 85% of networks in use today that are not ready to support IP telephony without modification³. With an industry-wide move to voice and data convergence, VoIP is likely to feature prominently in organisation's IT strategic planning and investments over the next 5 to 10 years.

Many of the analogue PBX (Private Branch Exchange) and PABX (Private Automated Branch Exchange) installations are nearing the end of their economic

In a VoIP network an IP address is the primary means of identification, although an endpoint may also be allocated a phone number. A call control

database records and manages endpoint identifiers and mappings. It will also record transactions for billing, audit, operational and security management.

In addition to integrating telephony and facsimile requirements, ubiquitous video conferencing, electronic whiteboarding, multimedia and multiservice applications will become feasible. VoIP can deliver numerous features including advanced call routing, computer integration, unified messaging, integrated information services, toll call bypass and encryption⁴. For example, the ability to

Continued on page 2

CONTENTS

<i>How Secure is Secure?</i>	1
<i>Voice Over IP</i>	1
<i>How Secure is Your Web Server?</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
Email: info@ccip.govt.nz
Web: www.ccip.govt.nz
Mail: P.O. Box 12-209
Wellington
New Zealand

Over 120 leading computer, telecommunication and technology organisations have indicated their intent to support and implement H.323 in their products and services.

Voice Over IP

IP is designed to work in a world where packet delivery cannot be guaranteed.

Voice Over IP

VOIP cont.

integrate service centre calls (help desk) with web services and shared screens is expected to provide faster call resolution times. Other examples include voice messages delivered to multiple mailboxes over the Internet, voice-annotated documents and "follow-me" features where a person is always contactable at a single telephone number or extension number, irrespective of physical location.

Various media gateways are used in VoIP, primarily to create VoIP packets from analogue voice signals using coders/decoders (CODECs). Other features such as compression, echo cancellation, silence suppression and traffic management are often incorporated into gateway functionality. Media gateways can fulfil a number of functions⁵:

- **Trunk gateways** that form the interface between a telephone and VoIP network, typically managing multiple digital circuits;
- **Residential gateways** that provide an analogue interface to a VoIP network. Examples include cable modems, xDSL devices and broadband wireless devices;
- **Access media gateways** provide an analogue or digital PBX interface to a VoIP network. Examples include small-scale (enterprise) VoIP gateways;
- **Business media gateways**

that provide digital PBX interface or an integrated soft PBX interface to a VoIP network; and

- **Network access servers** that connect a modem to a telephone circuit and provide data access to the Internet.

The International Telecommunication Union (ITU) and the Internet Engineering Task Force (IETF) are the two major international organisations recommending standards for VoIP. The ITU recommends H.323 and the IETF recommends the Session Initiation Protocol (SIP). While there is some overlap of functionality there are differences in approach and terminology. In addition, some vendors are providing proprietary, product dependent implementations. Both protocols can be extended to manage new capabilities. The argument has been advanced that H.323 is more stable because of its maturity but SIP provides better support for some functionality and is easier to implement⁶. Over 120 leading computer, telecommunication and technology organisations have indicated their intent to support and implement H.323 in their products and services. This wide-ranging support establishes H.323 as the *de facto* standard for audio and video conferencing over the Internet. Fortunately the ITU and the IETF are now co-operating in developing standards in this area.

The IP network connects the, often distributed, elements of a

VoIP network. As VoIP traffic is sensitive to delay, Quality of Service must be maintained. The IP network prioritises VoIP traffic through Class of Service (CoS) identifiers to ensure VoIP traffic is not affected by other network traffic.

IP is designed to work in a world where packet delivery cannot be guaranteed. Packet loss may occur where network congestion forces queue buffer overflows and network devices discard packets. Error correction and packet retransmission requests are designed to manage data errors and non-delivered packets in a data world. Again this can add delay. CODECs manage lost packets by substituting "white noise" or replaying the last successfully received packet. This may also occur when an "out of order" packet is received. This substitution is usually undetectable until a 1% packet loss threshold. Packet losses greater than 10% are generally not tolerable.

Today's networks are expected to provide a high reliability service and in order to do so there must be fault tolerance both in hardware and software. Fault tolerance is a function of the design, systems architecture, interoperability and quality of the system devices and software. Many existing networks will continue to handle data adequately but may require significant re-engineering and investment to provide the QoS and robustness expected in a VoIP network.

See the [CCIP website](#) for a full copy of this report.

VoIP References:

- ¹ Voice over IP, Tech Papers, Protocols.com, downloaded 13 February 2005
- ² Avoiding the Pitfalls of VoIP, Integrated Research White Paper, 2004
- ³ Ibid
- ⁴ Voice over IP 101 - Understanding VoIP Networks, Juniper Networks White Paper, August 2004, from www.juniper.net
- ⁵ Ibid
- ⁶ Consumer VoIP Markets: Early Forays into an Emerging Market, Mark Main, The Journal of The Communications Network Volume 2 Part 4, October-December 2003, pp2-11

HOW SECURE IS YOUR WEB SERVER?

In this article we have undertaken an analysis of website defacements for 2004, as reported to [Zone-H](#). It should be noted that the analysis is restricted to the .nz domain, so does not account for New Zealand websites hosted in other domains.

Of the 552 total defacements reported for 2004, 405 of these websites were victims of 49 separate mass defacements. A number of these mass defacements included websites which were not in the .nz domain but could be resolved to ownership by New Zealand entities. This latter group is not included in any statistics referenced in this report.

If we take a look at these defacements by operating system we see that Linux variants, usually running Apache web software, account for 64% of all defacements with Windows variants a distant second with 24%. These numbers track closely to worldwide statistics published by Zone-H which are 60.6% for Linux and 27.4% for Windows (as at 16 March 2005).

Homepage defacements accounted for 481 of the total defacements. The remaining defacements are usually pages inserted into a website by

hackers and a sampling of these defacements show that the inserted page has not been detected and removed by the website owner.

There were also 57 re-defacements registered last year, nearly 10% of the total – some website administrators don't learn!

So how does one protect a website against the hacking community, you may ask.

To quote from [NISCC Technical Note 06/03](#), "the security of a website is determined by the security of the following:

- The security of the web server;
- Remote web server administration;
- The security of the operating system of the web server computer;
- The security of the local area network of the web server computer;
- The security of "backend" applications supporting the web server; and
- The security of the

authoritative domain name server for the web server network".

Fortunately, there are a number of authoritative resources available to assist both policy makers and technologists. The CERT Coordination Centre (CERT/CC), based in Carnegie Mellon University, Pittsburgh, provide an excellent summary of countermeasures to "[Protect your web server against common attacks](#)" on their website.

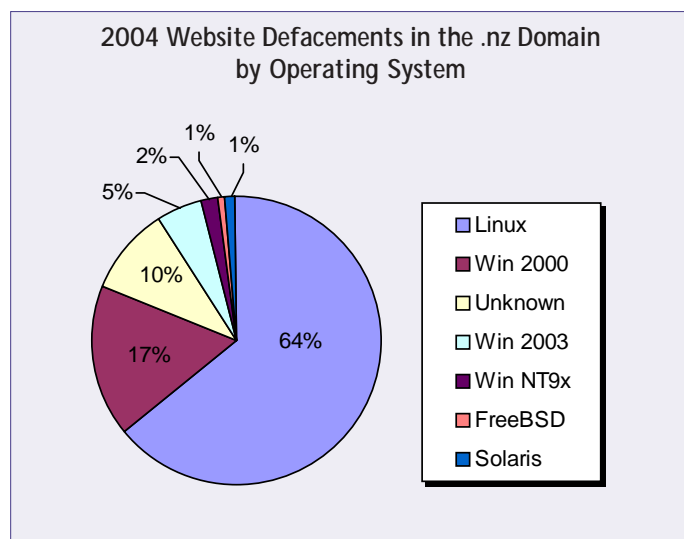
A more complete resource is the US-based, National Institute of Standards and Technology (NIST) Special Publication SP800-44, [Guidelines on Securing Public Web Servers](#). A recent publication from the National Infrastructure Security Co-ordination Centre (NISCC) in the UK, [Mitigating the risk of Malicious Software](#), provides advice "designed to inform organisations about the countermeasures that they can employ in order to help mitigate the threat posed to their information systems by malicious software (malware)". This report also contains links to a number of other useful resources, including their publication, NISCC Technical Note 06/03 - [Guidance on Securing Websites](#). This document stresses that most successful attacks on websites are made possible by misconfiguration of the web server and failure to install security patches.

If you don't want your website to appear on Zone-H, implementing the recommendations proposed in these four documents should go a long way to protect your website from the defacement brigade.

Information Source: [Zone-H](#)

Of the 552 total defacements reported for 2004, 405 of these websites were victims of 49 separate mass defacements.

How Secure is your Web Server

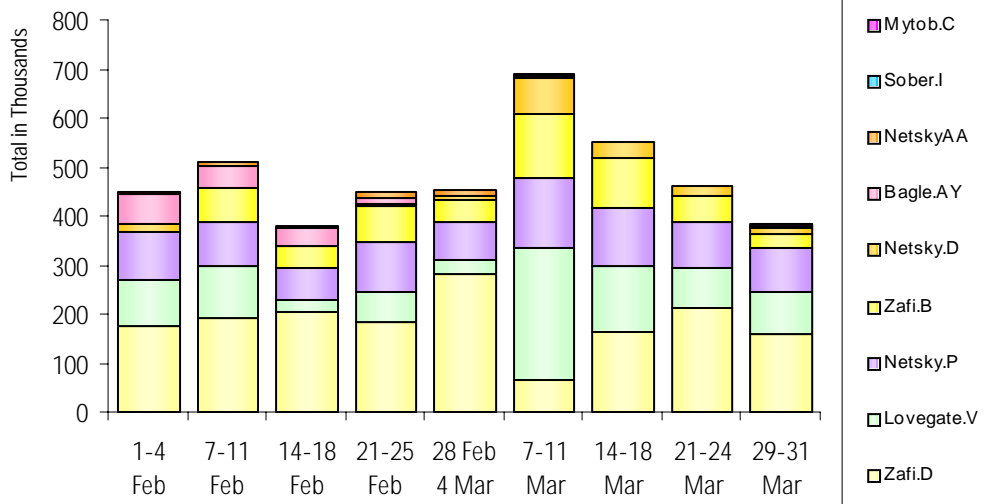


Homepage defacements accounted for 481 of the total defacements.

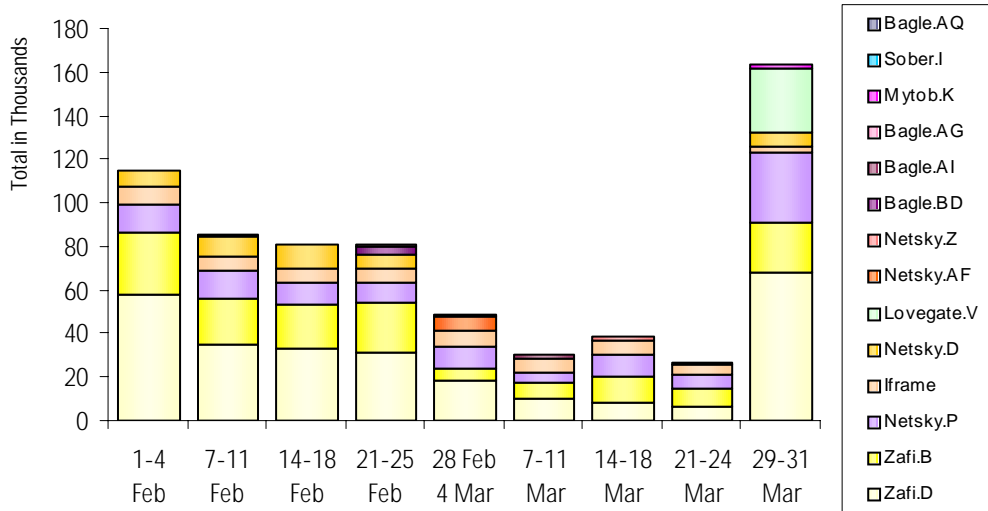
How Secure is your Web Server

VIRUS ACTIVITY

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



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



RECENT SIGNIFICANT ALERTS & ADVISORIES

REFERENCE	DESCRIPTION	DATE
Microsoft	Windows Server 2003 Service Pack 1 (SPS1)	01/04
AusCERT	High level of exploitation of AWStats, phpBB and other web bulletin board software	31/03
MIT	MIT Kerberos 5 versions 1.4 and prior	31/03
Mozilla	GIF heap overflow parsing Netscape extension 2	24/03
Apple	Security update 2005-003	22/03
Cisco	ACNS Denial of Service and default admin password vulnerabilities	25/03
Apple	Apple Mac OS X update for Java	24/03
Hewlett-Packard	HP Web-enabled Management Software Remote Buffer Overflow	17/02
AusCERT/Redhat	Redhat Enterprise Linux -- Multiple updates fix security issues	17/02

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

Email: info@ccip.govt.nz

Web: www.ccip.govt.nz

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