



NEWSLETTER

CENTRE for
CRITICAL INFRASTRUCTURE
PROTECTION

Volume 4, Issue 3

May 2005

LOW OR HIGHLIGHTS, TAKE YOUR PICK

With the recent spate of publicity surrounding DNS Cache poisoning, a timely report has been published by the United States National Academies. A summary of the report, "[Signposts on Cyberspace: The Domain Name System and Internet Navigation](#)", provides a good background on the history and administration of the current system and where the future may lie.

The National Infrastructure Security Co-ordination Centre (NISCC) in the United Kingdom have also published a report, "[Vulnerability Issues with IPsec Configurations](#)", which highlights

some deficiencies in the IPsec protocol when using Encapsulating Security Payload (ESP) and Authentication Header (AH). In a similar vein, NISCC also published the report "[Vulnerability Issues in ICMP Packets with TCP Payloads](#)". This report concerns the implementation of Internet Control Message Protocol (ICMP) messages that comply with a number of the Internet Engineering Task Force's (IETF's) Requests For Comments (RFCs) for ICMP. Although not critical, the existence of such vulnerabilities emphasises the need for care when configuring secure communication channels.

Last month also saw the release of a significant number of patches from database giant, [Oracle](#). This critical update includes fixes to its HTTP Server, which is based on Apache, and also resolves some SQL Injection vulnerabilities. US-CERT have published an advisory, "[TA05-117A-Oracle Products Contain Multiple Vulnerabilities](#)" documenting some of the issues.

Finally, the CCIP have issued a media statement about our Confidentiality Charter, detailing how organisations can confidently share sensitive information with the CCIP. Further details on [page two](#).

WHEN ANTI-VIRUS GOES WRONG

Incidents occurring in the last few weeks have highlighted automatic updates and their potential to cause serious problems. This time we are not talking about operating system patching but a task that most administrators automate and leave for granted - anti-virus updates. In a two-week period, two major anti-virus providers have unwittingly released updates that have caused not only the anti-virus protection to fail but also critical functions to seize.

One incident occurred in Japan where over 300,000 cases were reported. Updates for [Trend Micro's OfficeScan](#) and [VirusBuster](#) were distributed causing severely degraded performance on Windows XP Service Pack 2 Systems. In a similar incident, those running [NetIQ Integrated McAfee Anti-virus](#) in versions of MailMarshal

and WebMarshal received an update that corrupted the anti-virus. This caused filters to fail, which in turn caused email processing to be halted.

Although both situations have been remedied, incidents such as these could easily have had serious consequences if systems supporting critical infrastructure had been affected.

There are solutions that will give networks a better chance of survival. The first is fairly simple, use a distribution server for your corporate anti-virus. This gives you the control over what updates come in to your organisation. Additionally, most distribution servers will allow you to hold release of updates for a set period from when they are first available. This gives you time to deploy the update to a test environment and either allow or prevent the update. For those

who do not have the facilities of a test environment, this hold time can allow feedback from other subscribers to become known and still allow time for you to prevent deployment.

In an environment where duplication of servers is used to provide hot standbys, it is advisable to use different anti-virus vendors across the environment to limit vulnerability to any one group of servers.

These incidents are not the first and will surely not be the last, with no vendor able to offer a foolproof system. In the end it comes down to organisations being aware of potential risk, taking some responsibility for their network and implementing appropriate management systems.

CONTENTS

<i>Low or Highlights, take your pick</i>	1
<i>When Anti-Virus Goes Wrong</i>	1
<i>Voice Over IP & Voice Over Internet</i>	3
<i>SANS Top 20 Quarterly Updates</i>	3
<i>Virus Activity</i>	4
<i>Speare Phishing</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

As information is indiscriminately indexed, many organisations inadvertently make information publicly available.

Search Engine Safety

SEARCH ENGINE SAFETY

It may come as no surprise to learn that search engines are fast becoming a hacker's reconnaissance tool. Though hacking is an incorrect term for someone accessing publicly available information in a legal manner, sensitive information often appears in search engine caches, which the owner may not want to be publicly available. The intention of this article is to encourage administrators and security professionals to prevent this type of information leaking out, rather than highlighting any specific techniques that hackers may use.

Search engines

Of the many techniques available to "cyber evildoers", the most accessible is the myriad of Internet search engines. A search engine is a piece of software that enables a user to retrieve information from a database or index of information based on specific criteria, be it a word or phrase, searching within a PC, an Intranet, or on the World Wide Web.

Simply speaking, Internet search engines use robots (also known as web spiders and web crawlers) that are pieces of software that automatically traverse the web in search of new sites, update old ones, and index information into search engine databases where they can be accessed by anybody

using a Web browser. These robots are indiscriminate and seek out all information available to them whether it is a HTML or corporate Excel spreadsheet containing a company's financial position. It makes no difference!

Sensitive information disclosure

As information is indiscriminately indexed, many organisations inadvertently make information publicly available. Hackers, as part of their information reconnaissance activities, actively exploit the availability of this type of information. Information gathered through search engines may be just the starting point of a more focused attack on an organisation.

Though this type of information may be publicly available, finding it still requires more specialised types of search queries than just stringing a couple of search variables together. Though this is beyond the scope of this article, administrators and security professionals should explore this topic further.

Protecting your information

There are a few approaches to ensure your organisation does not leak information:

- A correctly configured and secure Web server. Default configurations leading to unintentional data being

leaked, such as virtual directory listings etc., should be disabled.

- A careful review of the information that can be made publicly available.
- Items that are to be kept private can either be removed from the Web server or can be hidden from the robots by the insertion of robot meta tags which will tell a robot not to index specified pages.
- Alternatively, you could use the [Robots Exclusion Protocol](#) to generate a Robots.txt document, which also tells robots what they can and cannot index.

Wise administrators will familiarise themselves with specialised search techniques to identify any problems with their own sites. If unwanted information is discovered administrators may need to the contact websites that are archiving their information and ask for it to be removed. Some websites archive old versions of websites that were created years ago. If you intend testing your own website, or somebody else's, make sure you are aware of the terms of service of the search engine you are using.

If you intend testing your own website, or somebody else's, make sure you are aware of the terms of service of the search engine you are using.

Search Engine Safety

CCIP CONFIDENTIALITY CHARTER

The New Zealand Government's Centre for Critical Infrastructure Protection (CCIP) has announced the publication of its *Confidentiality Charter* for the protection of IT information provided by its clients and partners.

Since its establishment in 2002, a key priority for the CCIP has been to ensure the confidentiality

of shared information. In the Charter it is publicly defining and explaining its approach to the protection of such information, in particular information concerning electronic attacks on critical infrastructure owners and corresponding threat mitigation and defensive measures.

A copy of the Charter is available at www.ccip.govt.nz.



VOICE OVER IP & VOICE OVER INTERNET

Is there really a difference? As with many technologies the answer can be yes and no!

Voice over Internet Protocol (VoIP) and Voice over Internet (Vol) both digitise voice signals, packetise the data and route the data to its destination. A longer explanation is that both convert voice (analogue signals) into digital form and organise the data into packets, usually conforming to the Internet Protocol (IP). Packets are then transmitted by the most convenient route to their destination and reassembled before delivery. So what is the difference?

VoIP is considered to be the commercial provision of IP telephony and much of the traffic is expected to be carried over circuits and channels provided and managed by telecommunications organisations.

Voice over Internet, by contrast, uses the Internet as its primary channel and is subject to all the

delays, variable routing and other challenges of using the Internet for voice communication.

Voice over Internet

Vol is generally a PC to PC method of communication and uses software from sites such as [Skype](#), [MyFreeLD.com](#), [Dialpad.com](#), [To-Talk Communications](#) and [Conflab.com](#).

PC to PC calling has some drawbacks. Both PC's need to be online and running the same Internet 'phone software. The quality of a call is dependent on connection speeds, routing delays, error rates and other similar factors. If the connection is slow or there are other traffic inhibitors it may be difficult to hold a conversation¹.

Some Vol software is now offering PC to normal telephone connectivity. This, however, is still subject to the difficulties outlined in PC to PC calling, due mainly to the use of the Internet.

What is VoIP?

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 networks², whether an organisation specific LAN (local area network), WAN (wide area network) or a commercially provided channel. This offers a higher degree of security and quality of service (QoS) as technical aspects of call control, call signalling and data transmission can be more carefully controlled and managed.

See last month's CCIP newsletter for a fuller discussion of VoIP.

References:

- Free Internet Phone Calls, <http://freebies.about.com/cs/faxphone/a/internetcalls.htm>, accessed 1 May 2005
- Voice over IP, Tech Papers, Protocols.com, downloaded 13 February 2005

Voice over Internet, by contrast, uses the Internet as its primary channel and is subject to all the delays, variable routing and other challenges of using the Internet for voice communication.

Voice Over IP & Voice Over Internet

SANS TOP 20 QUARTERLY UPDATES

SANS have recently released the first instalment in a new program of [quarterly updates](#) to their annual Top 20 Internet Security Vulnerabilities. It provides an additional roadmap to the new vulnerabilities that must be eliminated in any Internet-connected organisation.

The top new Microsoft vulnerabilities include:

- Windows License Logging Service Overflow (MS05-010)
- Microsoft Server Message Block (SMB) Vulnerability (MS05-011)
- Internet Explorer Vulnerabilities (MS05-014 and MS05-008)

- Microsoft HTML Help ActiveX Control Vulnerability (MS05-001)
- Microsoft DHTML Edit ActiveX Remote Code Execution (MS05-013)
- Microsoft Cursor and Icon Handling Overflow (MS05-002)
- Microsoft PNG File Processing Vulnerabilities (MS05-009)

Those still running Windows 2000 may also want to include "Vulnerability in Web View Could Allow Remote Code Execution (MS05-024)". Microsoft have also recently augmented their security offerings with a new service,

[Microsoft Security Advisories](#), which aims to provide guidance and information about security-related software changes or software updates.

Other vulnerabilities highlighted include:

- Computer Associates License Manager Buffer Overflows
- DNS Cache Poisoning Vulnerability
- Multiple Antivirus Products Buffer Overflow Vulnerabilities
- Oracle Critical Patch Update
- Multiple Media Player Buffer Overflows (iTunes, RealPlayer & Winamp)

PC to PC calling has some drawbacks. Both PC's need to be online and running the same Internet 'phone software.

Voice Over IP & Voice Over Internet

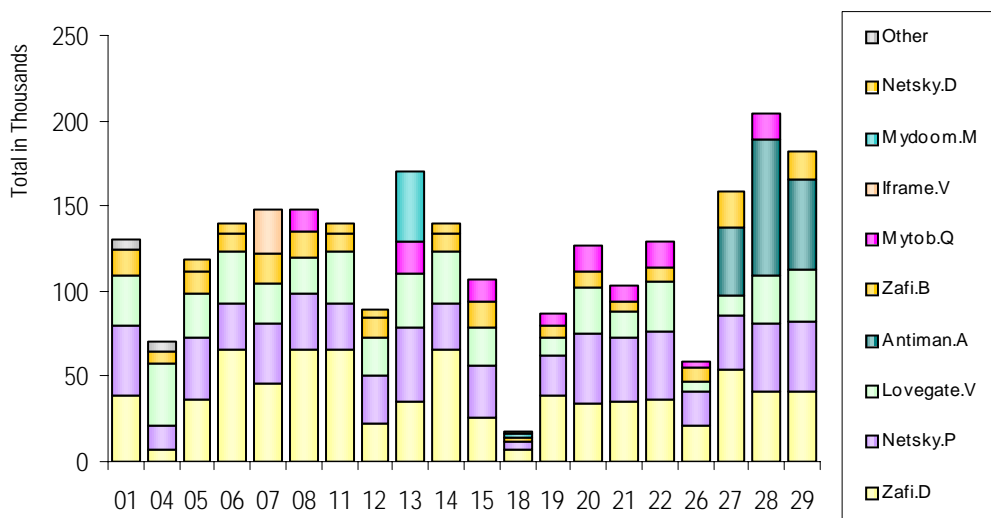
VIRUS ACTIVITY

Last month a new persistent memory-resident Trojan, [Mitglieder](#) emerged. It has consistently headed the statistics gathered from RAV AntiVirus but other vendors have reported less activity. This Trojan sets up an email relay station on the infected system and has the capability of

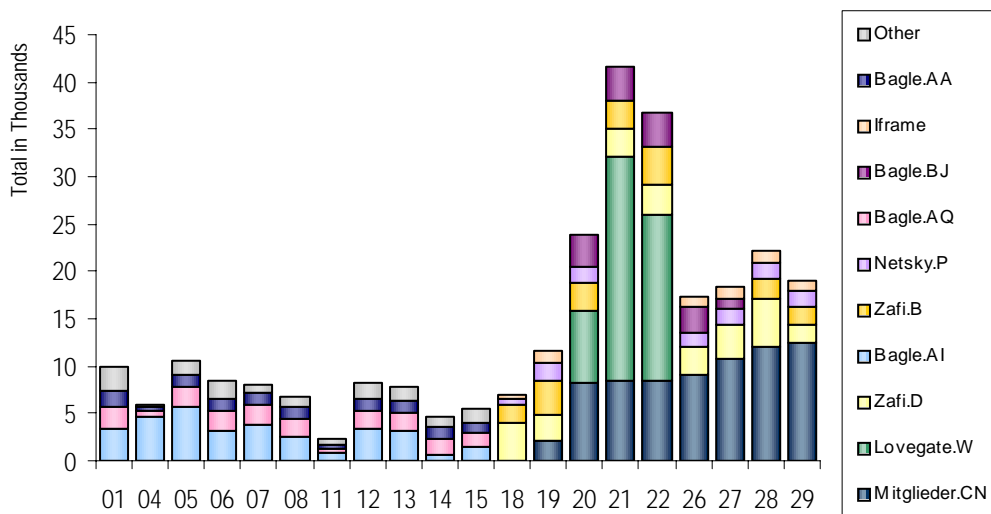
terminating processes running anti-virus applications. A new variant of the [Sober worm](#), offering free tickets to the soccer World Cup in Germany next year as bait, was also released last month with English and German versions. Volumes reported by the anti-virus vendors were variable

with Sophos reporting that it accounted for 84% of traffic early last week. Overall, numbers continue to decline which could be an indication that security vulnerabilities are being addressed by vendors and the user community, in a much more timely fashion.

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



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



SPEAR PHISHING

A recent article published by the Fairfax media group, [Spear Phishers Evade Usual Spam Defences](#), describes a new technique for capturing private information. This technique targets specific individuals in an organisation whose email

addresses have been acquired by 'standard' social engineering practices. Sender details in an email are spoofed to make it appear that it originated internally thus convincing the recipient of its legitimacy. Links to fake websites can be

embedded in such emails and that can lead to data exfiltration. Help may be around the corner, however. Reports suggest that "a number of browser developers are creating new tools designed to help users stave off phishing attacks".

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