



NEWSLETTER

CENTRE for
CRITICAL INFRASTRUCTURE
PROTECTION

Volume 3, Issue 6

August 2004

EDITORIAL

This month the feature article provides an update on Internet Protocol version 6 (IPv6). It suggests that those charged with the acquisition of network equipment should begin to consider equipment that is IPv6 capable and backward compatible with the existing standard, IPv4.

Also this month, Microsoft released not only the scheduled [security bulletin](#) in the middle of the month, but also followed this up with the release of the first 'out of band' bulletin which provided details of a cumulative [security update](#) for Internet Explorer. In total Microsoft

provided details of three critical, four important and one moderate update to their product range. In addition, [Service Pack 1](#) (SP1) for Office 2003 was also released. Of note, it contains significant enhancements, as well as stability and performance improvements.

And just to prove that Internet Explorer is not the only vulnerable browser on the market, AusCERT advises that working proof-of-concept code has now been published for a vulnerability in all current versions of Mozilla and Firefox. AusCERT expects this exploit code to be utilised to

facilitate identify fraud (aka "phishing") which may capture sensitive account details. Further details of this vulnerability can be found [here](#).

And as we go to press, details of multiple critical vulnerabilities in libpng are being published. Libpng is a popular reference library available for application developers to support the Portable Network Graphics (PNG) image format, an alternative to other image formats such as the Graphics Interchange Format (GIF). Further details are available on the [CCIP website](#).

INTERNET PROTOCOL VERSION 6 (IPV6)

Rapid growth in the use of the Internet (in particular, the World Wide Web) has prompted concern over the limitations of the Internet Protocol version 4 (IPv4), the data networking protocol on which the Internet is based. New users and usages of the Internet have the potential to exhaust the available IPv4 address space, although IPv4 address space will continue to be available for many years. Vinton Cerf¹ of the Internet Corporation for Assigned Names and Numbers (ICANN), estimates that two-thirds of the available IPv4 addresses have already been used².

A co-operative effort between the Regional Internet Registries (RIRs) and the various Internet Protocol version 6 (IPv6) Task Forces are working on this issue. IPv6, also known as Internet Protocol – next generation (IPng), was first mooted some years ago, to address these concerns. Recommended by the Internet

Engineering Task Force (IETF) in July 1994, it was adopted as a Proposed Standard in November 1994. In August 1998, it became a Draft Standard.

The primary motivation for IPv6 was to expand the available address space of the Internet, thereby enabling the use of billions of new devices (PDAs, cellphones, appliances, etc.), large numbers of new users and always-on technologies (xDSL, cable, Ethernet-to-the-home, fibre-to-the-home, Power Line Communications, etc.). At the same time, improvements in security, routing and network autoconfiguration were also specified.

How will it help?

The IPv4 protocol has a 32-bit address space providing for approximately 4 billion unique globally addressable network interfaces. IPv6 has a 128-bit address space that can uniquely

address about 340 sextillion (340,282,366,920,938,463,463,374,607,431,768,211,456) network interfaces.

This has been described as providing an address for every human, cellphone, mobile device, lighting, and air conditioning equipment, and even kitchen appliances. Any other device that can imaginably be connected to the Internet, will be able to have an IP address.

Transition from IPv4 to IPv6

IPv6 is designed to interoperate with IPv4 anywhere in the Internet, until IPv4 addresses are exhausted. It will also allow IPv6 and IPv4 hosts to interoperate indefinitely after that, but with reduced scope. Hosts that need only limited connectivity (such as printers) will never need to be upgraded to IPv6. These aspects were specified in order to protect investment in IPv4 architectures

Continued on page 2

CONTENTS

<i>Internet Protocol version 6 (IPv6)</i>	<i>1</i>
<i>New Zealand Portscanning Activity</i>	<i>3</i>
<i>Virus Activity</i>	<i>3</i>
<i>Who is the Mystery Shopper?</i>	<i>4</i>
<i>CCIP Watch Centre Analysts Wanted</i>	<i>4</i>

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

Prudent organisations will be looking to ensure equipment replacements, software, upgrades and new developments are IPv6 capable.

Internet Protocol Version 6

The Centre for Critical Infrastructure Protection is seeking Watch Centre Analysts to join the Head Office in Wellington.

Applications close Friday 20 August 2004.

CCIP Watch Centre Analysts Wanted, page 4.

IPv6 Continued

and equipment and to allow a phased replacement and retirement of older devices, software and systems³.

What is happening?

Four Regional Internet Registries (RIRs)⁴ provide registration services and are globally responsible for the management of Internet numbering resources, including IPv4 and IPv6 address space. The RIRs are working with the IPv6 Task Forces and the IPv6 Forum⁵ towards the deployment of IPv6.

In July 2004, ICANN announced it had added IPv6 nameserver addresses to the Internet's DNS root server system for Japan's (.jp) and Korea's (.kr) country code Top Level Domains (ccTLDs)⁶. The IPv6 records for France (.fr) are expected to be added shortly and approvals for other country codes will follow.

Conclusions

Today's Internet protocols cannot fully support the requirements for more address space, more security, more efficiency and improved communications. Business drivers such as broadband, better entertainment experiences and mobile computing are adding pressure to this need for change.

With the advent of multiple always-on devices, wireless handhelds and 3G mobile handsets, the Internet community must prepare for a sharp increase in IP address space utilisation. The global rollout of IPv6 is essential to support these needs. The rollout of IPv6 on this scale requires significant preparation, particularly in terms of training and planning.

Deployment of IPv6 is starting. With ten years of solid

development and support from major technology vendors, IPv6 is a protocol that Internet users are going to have to deal with in the near future. While early adoption of new technologies can be costly, they are already signs that costs are falling as more vendors roll out equipment and software that is IPv6 capable.

ICANN have indicated that IPv4 will run in parallel with IPv6 for up to twenty years. While not being forced to commit fully to an IPv6 rollout (yet), prudent organisations will be looking to ensure equipment replacements, software, upgrades and new developments are IPv6 capable and are fully backward compatible with IPv4.

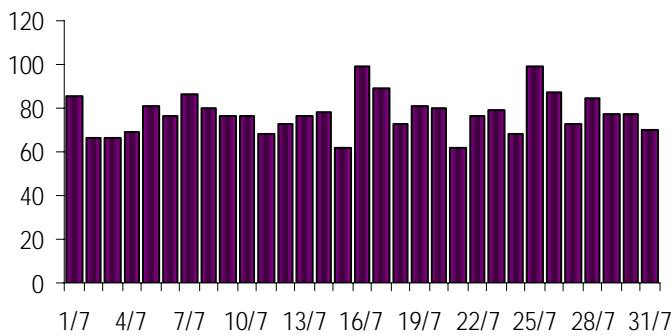
• Turn to page four for *IPv6 References*.
• Table extract below from "Introduction to IPv6", Microsoft Corporation. Published: 09/03, Updated: 03/04.

Table 1: Differences Between IPv4 and IPv6

IPv4	IPv6
Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length.
IPSec support is optional.	IPSec support is required.
No identification of packet flow for QoS handling by routers is present within the IPv4 header.	Packet flow identification for QoS handling by routers is included in the IPv6 header using the Flow Label field.
Fragmentation is done by both routers and the sending host.	Fragmentation is not done by routers, only by the sending host.
Header includes a checksum.	Header does not include a checksum.
Header includes options.	All optional data is moved to IPv6 extension headers.
Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IPv4 address to a link layer address.	ARP Request frames are replaced with multicast Neighbour Solicitation messages.
Internet Group Management Protocol (IGMP) is used to manage local subnet group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages.
ICMP Router Discovery is used to determine the IPv4 address of the best default gateway and is optional.	ICMP Router Discovery is replaced with ICMPv6 Router Solicitation and Router Advertisement messages and is required.
Broadcast addresses are used to send traffic to all nodes on a subnet.	There are no IPv6 broadcast addresses. Instead, a link-local scope all-nodes multicast address is used.
Must be configured either manually or through DHCP.	Does not require manual configuration or DHCP.
Uses host address (A) resource records in the Domain Name System (DNS) to map host names to IPv4 addresses.	Uses host address (AAAA) resource records in the Domain Name System (DNS) to map host names to IPv6 addresses.
Uses pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.	Uses pointer (PTR) resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.
Must support a 576-byte packet size (possibly fragmented).	Must support a 1280-byte packet size (without fragmentation).

NEW ZEALAND PORTSCANNING ACTIVITY

NZ Portscan activity by [ISC](#) for July.



Daily Total in Thousands

You may have noticed that in recent months we have been

unable to produce our statistics detailing portscanning activity in New Zealand. The raw data for this service was provided by the

[Internet Storm Center \(ISC\)](#). The database service provided by these cyber warriors is currently undergoing a major overhaul. As a result, the detailed port activity data is unavailable.

However, daily cumulative data for New Zealand is available and this is graphed (left). As you can see, the number of scans varies between 60,000 and 100,000 per day, with an average of around 77,500 and this positioned the country in the top thirty to forty of all reports received by ISC.

This month saw the emergence of a new breed of malware. MyDoom.M/O, a variant of the original MyDoom mass mailing worm, not only harvested e-mail addresses from the local machine, it also used a variety of world-wide web search engines to find more addresses based on the domain names of addresses found on the local hard disk.

According to [Sophos](#), the percentage chance that each search engine is used is:

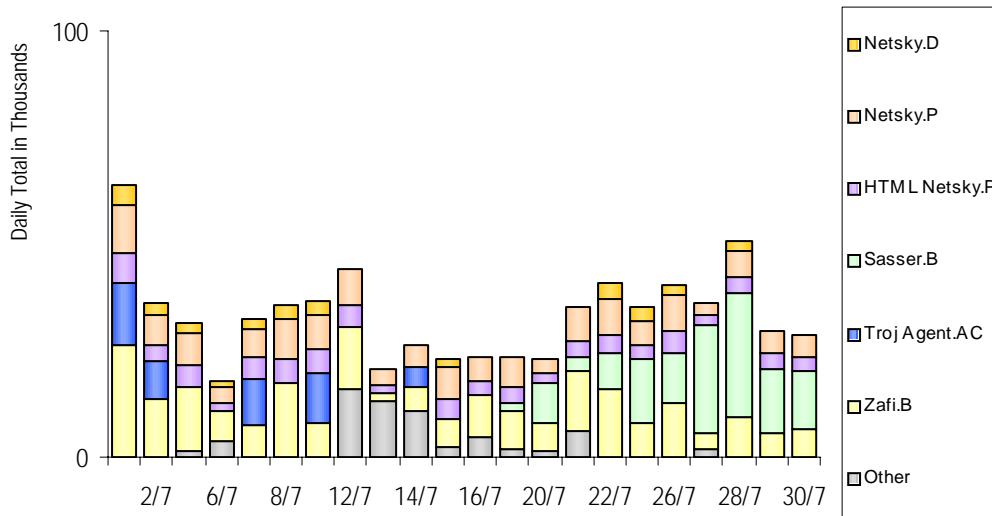
*www.google.com (45%)
search.lycos.com (22.5%)
search.yahoo.com (20%)
www.altavista.com (12.5%)*

Overall, the Zafi-B, another peer-to-peer (P2P) and mass mailing worm, dominated the statistics this month with Netsky variants taking up the minor places.

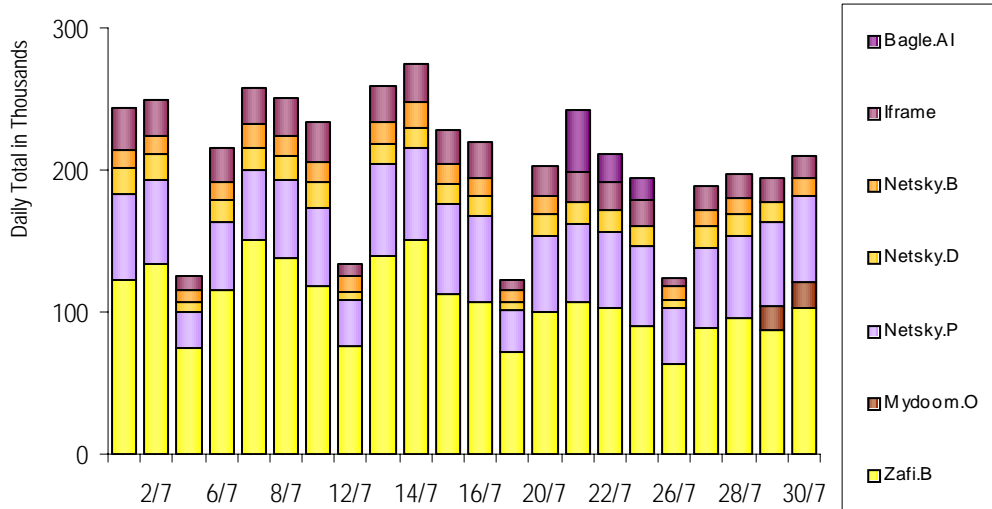
Virus Activity

VIRUS ACTIVITY

Daily Top Five: viruses captured worldwide by [TrendMicro](#) for July.



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



WHO IS THE MYSTERY SHOPPER?

With the proliferation of mobile devices, particularly those with built-in cameras and microphones, there is increasing risk to organisations and individuals. Key risks include information theft, identity theft and subsequent impersonation and fraud. It is becoming easier to capture important and valuable information without its owner being aware that the information has been copied until, in some cases, it is too late.

Many devices were developed for personal convenience and entertainment, but these devices are generally the least secure of any the devices we use to process and store information. These devices can be used to steal large quantities of corporate data, and can also be used to introduce viruses and worms into corporate networks.

[Gartner](#)¹ estimates that by 2007, it is likely that more than 60 percent of the E.U. and U.S. population aged 15 to 50 will carry or wear a wireless computing and communications device at least six hours a day. Voice access and text access will be the principal interface for services such as e-payments, e-wallets and e-cash. However, the same elements that offer such easy access to the e-world can also result in accumulation of information by marketers or criminals.

We generally do not protect this information well. [Gartner](#)² estimates that, in 2005, more than 50 percent of online transactions involving people will rely solely on passwords. The use of other or additional methods of authentication is growing, but

not at a sufficient rate to combat this threat.

We are seeing criminals take advantage of these devices and the ease with which information can be captured. One recent activity is the use of cellphone cameras to capture your image, credit card and sometimes your PIN in the supermarket, restaurant, retail stores or at the ATM. Identity theft is one of the fastest growing crimes internationally and armed with this information, the criminal can perpetrate fraud in your name, causing great personal distress and loss.

So be aware of your surroundings when using your EFTPOS or credit cards and watch for that mystery shopper talking on a cellphone!

1 & 2. <http://security1.gartner.com/>

CCIP WATCH CENTRE ANALYSTS WANTED

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

CCIP provides an exciting work environment for those interested in information network threat and protection.

Watch Centre Analysts publish IT security alerts, provide advice to critical infrastructure organisations and provide support to protect New Zealand's critical IT infrastructure from cyber attack. They do so by analysing and researching computer and communications threats, vulnerabilities, incidents

and monitoring of technological trends and developments.

You will be expected to work on a roster schedule on weekdays, with occasional night shift work. You will also be available for rostered after-hours callouts.

You will have experience in IT development and administration, extensive knowledge of computer and network systems, and a reasonable understanding of network security and risk analysis fundamentals. You will also have a degree in computing, telecommunications or a related area, or several years of relevant experience.

Please note: Applicants must be New Zealand Citizens.

For an application form and job description e-mail hr@gcsb.govt.nz or phone 04 472-6881. Application forms can be downloaded from the [GCSB website](#).

Applications close Friday 20 August 2004. Please send your CV, a copy of your academic transcript and your application form to: HR Advisor, PO Box 12-209, Wellington or fax to (04) 499-3701.

The GCSB promotes a policy of Equal Employment Opportunities.

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 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

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

Internet Protocol version 6 References:

1. Widely known as one of the "Fathers of the Internet," Cerf is the co-designer, with Robert E. Kahn, of the TCP/IP protocols and the architecture of the Internet.
2. "Net Agency Heralds Web-Addressing Advance", Reuters, July 20 2004.
3. See <http://www.ietf.org/> for related RFCs
4. The Regional Internet Registries are:
 - [Asia Pacific Network Information Centre \(APNIC\)](#)
 - [American Registry for Internet Numbers \(ARIN\)](#)
 - [Latin American and Caribbean Internet Addresses Registry \(LACNIC\)](#)
 - [NCC RIPE Network Coordination Centre \(RIPE\)](#)
5. The IPv6 Forum is a world-wide consortium of over 160 leading Internet service vendors, National Research & Education Networks and international ISPs to promote IPv6 and provide technical guidance for the deployment of IPv6.
6. "Next-Generation IPv6 Address Added to Internet's Root DNS Zone", 20/7/04, [icann.org](#).