



NEWSLETTER

CENTRE for
CRITICAL INFRASTRUCTURE
PROTECTION

Volume 3, Issue 5

June 2004

JUNE EVENTS

There were two large events in the Critical Infrastructure (CI) arena this month. On 6 June the UK National Air Traffic Services (NATS) grounded all aircraft, due to errors detected during testing for a future upgrade of the Flight Data Processing (FDP) system. They decided to restart the FDP, which resulted in disrupted services.

On 15 June there was a large-scale Denial of Service (DoS)

attack on the Internet Domain Name Service (DNS). Akamai Technologies Inc., a distributed computing provider, released a statement regarding this event. The DNS impact was limited to approximately 4 percent of the Akamai customer base. Among those affected were: Google; Microsoft; Yahoo; and Apple. Whether Akamai or these customers were the targets of the DoS attack has yet to be resolved.

With increasing numbers of website defacements in New Zealand, we have included in this newsletter the website defacement activity for 2004, replacing the New Zealand port probe activity data which will be back next month.

An article discussing the phenomenon of electromagnetic pulse (EMP) is the feature for this newsletter.

ELECTROMAGNETIC PULSE

EMP, the weapon of Electrical Mass Disruption.

When we think of protecting Critical Infrastructure (CI) from cyber-borne threats, several vectors come to mind. For example, malware including viruses and Trojans; Denial of Service (DoS) and data integrity attacks; and hacking and website defacements. This year alone we have seen 301ⁱ viruses, 314ⁱⁱ New Zealand websites defaced and numerous large distributed DoS attacks. Electromagnetic Pulse or EMP is another threat to the electronic components of CI. While less publicised, it could be the Achille's heel of a modern technological society.

Physicist Arthur H. Compton proposed the theory behind EMP in 1925. Compton's studies into the EMP phenomenon, the Compton effectⁱⁱⁱ, and its use in elucidating atomic structure, earned him the Nobel Prize in 1927. Enrico Fermi, another Nobel laureate (1938), tried to calculate the possible electromagnetic fields produced from nuclear explosions.

Nuclear detonations produce gamma rays. These interact with the surrounding air molecules to produce electrons, which travel outward at a faster rate than the remaining heavier, positively charged ions. This separation of charges produces a strong electric field^{iv} that can spread for hundreds of miles and disrupt communications and power networks.

While nuclear generated EMP may not be accessible to most terrorist groups, there is a much less complex option: a Flux Compression Generator (FCG). An FCG is a remarkably simple weapon. It consists of an explosives-packed tube placed inside a slightly larger, energised copper coil. The explosive charge and the coil's magnetic field create a moving short-circuit. "The propagating short causes compression of the magnetic field while reducing inductance of the coil. The result is that FCGs will produce a ramping current pulse, which breaks before the final disintegration of the device. Published results suggest ramp

times of tens of hundreds of microseconds and peak currents of tens of millions of Amps^v."

This inexpensive device is a threat to modern societies increasingly reliant on electronic infrastructure systems.

The semiconductor devices in these systems, and especially commercial off-the-shelf components, are susceptible to excessive electric currents and voltages. When a semiconductor device absorbs EMP energy, it displaces the produced heat relatively slowly when compared to the time scale of the EMP. The semiconductor can quickly heat up to temperatures near the melting point of the material. Soon after, the device will short and fail.

A piece of electronic equipment may survive the initial very-high frequency pulse. It may continue to operate, but with ongoing intermittent faults, or possibly succumb to late-time EMP effects that occur in the 15 minutes after

CONTENTS

<i>Electromagnetic Pulse</i>	1
<i>Recent Significant Alerts & Advisories</i>	2
<i>Virus Activity</i>	3
<i>Website Defacements</i>	4
<i>CCIP Watch Centre Analysts Wanted</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

Continued on page 2

While cyber attacks are usually less effective and less disruptive than physical attacks, their advantage is that they are cheaper and easier to carry out^{vi}. A combination of the two, a blended attack, is in probability the biggest threat.

Electromagnetic Pulse

Military organisations have been protecting their critical systems from EMP for years. Now, however, given the current world security situation, other elements of government and the private operators of CI need to consider investing in EMP protection.

Electromagnetic Pulse

ELECTROMAGNETIC PULSE Continued

an EMP detonation. During this 15-minute period, the EMP that surged through electrical systems creates localised magnetic fields. When these fields collapse they cause electrical surges to travel through the power and telecommunication infrastructure.

This means that malicious actors would not have to be close to the targets they wish to destroy. Attacks on otherwise protected sites, such as telephone switching centres and electronic funds-transfer exchanges, could occur through their electrical and telecommunication connections.

An EMP attack highlights the connection between the cyber and physical world. The physical and cyber aspects of CI cannot be separated. With the connectivity of Supervisory Control and Data Acquisition (SCADA) systems to physical assets, a major cyber event can have physical ramifications and *vice versa*^{vi}.

While cyber attacks are usually less effective and less disruptive than physical attacks, their advantage is that they are cheaper and easier to carry out^{vii}. A combination of the two, a blended attack, is in probability the biggest threat. An EMP or

cyber attack that cripples emergency response, transport or telecommunications along with a physical attack will "force multiply" the disruption and damage. This asymmetric approach to attacks gives a small group the opportunity to attack a larger opponent.

The distributed nature of CI and its diversity and redundancy can enable restoration of services quickly after an attack or failure. A successful EMP attack and the associated destruction of electronic systems, however, could see this restoration stratagem fail.

There are two general methods to protect critical systems against EMP: metallic shielding and tailored hardening.

Metallic shielding is the most effective protection. This involves containing the equipment in an electrically conductive enclosure, termed a Faraday cage, which prevents the electromagnetic field reaching the equipment. However, such equipment must communicate, and be powered from, the outside world. This can provide entry points by which electrical transients may enter the enclosure and effect damage. While optical fibres can avoid this risk, electrical power feeds remain

susceptible. (Wireless card antennas in laptops make them especially vulnerable.)

The alternative method is tailored hardening, which involves redesigning the most vulnerable elements to withstand much higher currents.

Military organisations have been protecting their critical systems from EMP for years. Now, however, given the current world security situation, other elements of government and the private operators of CI need to consider investing in EMP protection.

The CCIP would appreciate receiving your views or other information on the EMP threat in New Zealand.

EMP References:

- ⁱ [Sophos](#)
- ⁱⁱ [Zone-h](#)
- ⁱⁱⁱ [Encyclopedia Britannica](#)
- ^{iv} EISENBERG, Adam H. [The Electromagnetic Pulse](#)
- ^v KOPP, C. Defence Analyst, Monash University.
- ^{vi} GREENE, Brenton. Deputy Director US National Communications System.
- ^{vii} LEWIS, James. Assessing the Risk of Cyber Terrorism, Cyber War & other Cyber Threats.

RECENT SIGNIFICANT ALERTS & ADVISORIES

REFERENCE	DESCRIPTION	DATE
US-CERT	Multiple Vulnerabilities in ISC DHCP 3	23/06
iDefence	GNU Radius SNMP Invalid OID Denial of Service Vulnerability	26/06
CIAC	Microsoft Windows 2000 Advanced Server Security Bypass	16/06
US-CERT	Cross-Domain Redirect Vulnerability in Internet Explorer	16/06
CCIP	Malicious Software Advisory - Zafi.B	15/06
Real	RealPlayer & RealOne Update to Address Security Vulnerabilities	14/06
Cisco	Cisco CatOS Telnet, HTTP & SSH Vulnerability	10/06
Apple	Security Update 2004-06-07	09/06

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

VIRUS ACTIVITY

Over the past week the first smart phone virus, the "Cabir" worm, has emerged. Cabir arrives as a "security update" and upon execution by the user, scans for other smart phones via its Bluetooth connection. Although Cabir is not malicious, its scanning does run down battery power. While the Cabir worm is a first for smart phones, viruses have been detected on mobile phones before. A worm named "Timofonica", which sent unwanted text messages, appeared in the Spanish cell phone network in June 2000.

Netsky variants have continued to dominate virus activity since

the last newsletter, with around 30 different variants detected since mid-February. Netsky.P, the most prevalent of these variants, is nearly 30 percent more invasive than the nearest variant, Netsky.D. The suspected Netsky and Sasser virus-author is facing prosecution, with possible thanks to Microsoft's virus-author bounty, the multimillion dollar reward program which encourages people to identify computer virus writers.

On 15 June, CCIP issued an advisory regarding the Zafi.B virus. According to TrendMicro, one in 33 computers in

New Zealand and Australia were infected. This was the highest infection rate worldwide. E-mail delivery in New Zealand slowed during its peak on 17 to 18 June because of the large number of infected e-mails being filtered by ISPs.

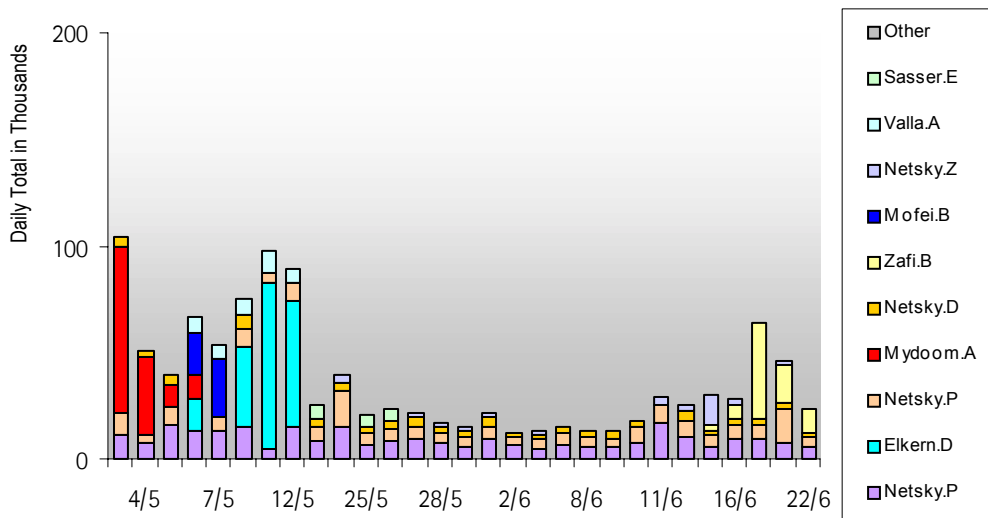
Virus Activity Reference:

As well as cell phone circuitry, a smart phone has the ability to execute programs. These programs may be useful for applications such as MP3 players, but they are also useful for malicious code.

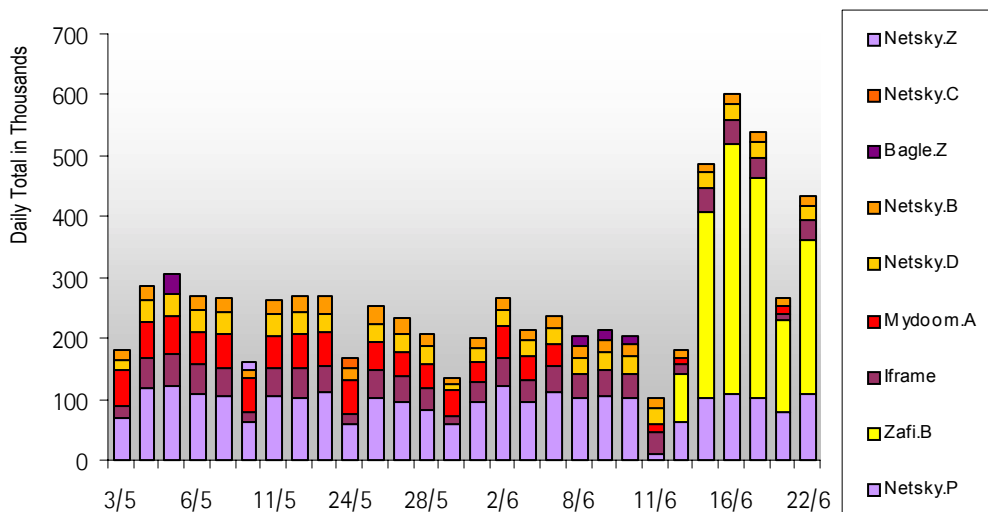
According to TrendMicro, one in 33 computers in New Zealand and Australia were infected. This was the highest infection rate worldwide.

Virus Activity

Daily Top Five: viruses captured worldwide by TrendMicro from 4 May to 22 June.



Daily Top Five: viruses captured worldwide by RAV from 3 May to 22 June.



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

Applications close Friday 2 July 2004.

CCIP Watch Centre Analysts Wanted, page 4.

NEW ZEALAND WEBSITE DEFACEMENTS

The number of New Zealand website defacements has risen to a six-monthly high of 91 for the month of June. An initial high of 73 defacements in January trended downward to a low of 9 in April and has risen sharply since.

The graph (right) shows the number of New Zealand website defacements for 2004 to date.

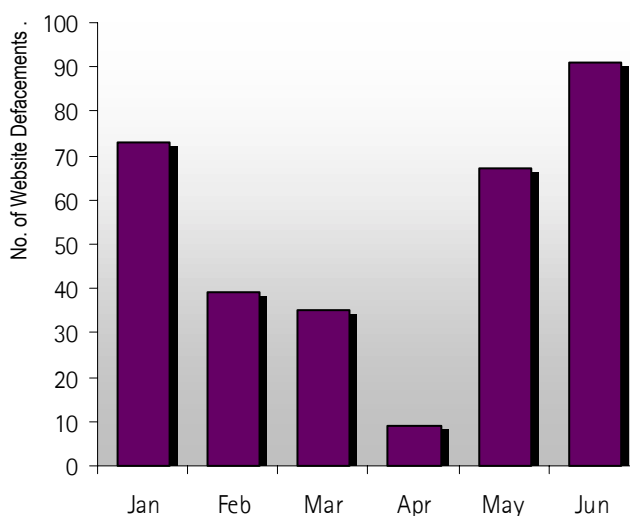
Guidance for Security Websites

The Open Web Application Security Project (OWASP) Guide to Building Secure Web Applications has become a key source for many web security professionals.

[The Guide](#) is a comprehensive manual for designing, developing and deploying secure web applications. Its contents include:

- security guidelines;
- architecture;
- authentication;

Website Defacements 2004 (as sourced from [zone-h](#))



- session management;
- access control;
- event logging;
- data validation;
- common problems;
- privacy issues; and
- cryptography.

The US National Institute of Standards & Technology (NIST), also has useful guidance on

securing websites. See NIST Special Publication 800-44, Guidelines on Securing Public Web Servers, September 2002

The current top ten web application vulnerabilities according to OWASP can be found [here](#).

CCIP WATCH CENTRE ANALYSTS WANTED

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

CCIP provides an exciting work environment for those interested in information networks and threats to those networks.

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

You will be expected to work of a roster schedule covering

7am to 7pm 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, knowledge of computer operating systems and network management 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.

You will be self-motivated with excellent interpersonal, analytical and written communication skills and have the ability to work well under pressure.

Please note: Applicants must be New Zealand citizens.

For an application form and job description:

phone: (04) 472 6881;
e-mail: hr@gcsb.govt.nz; or
download: [GCSB website](#).

Applications close Friday 2 July 2004. Please send your CV, a copy of your academic transcripts 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 Opportunity.

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