



# NEWSLETTER

CENTRE for  
CRITICAL INFRASTRUCTURE  
PROTECTION

Volume 1, Issue 1

October 2002

## FIRST of MANY

Welcome to the first issue of the Centre for Critical Infrastructure Protection (CCIP) newsletter!

This newsletter will be published regularly and will provide subscribed members a synopsis of:

- information on recent alerts and advisories issued by various international critical infrastructure protection agencies and Computer Emergency Response Teams (CERT's)
- an analysis of recent trends on the distribution of viruses, worms, etc
- links to recent articles from the media relevant to critical infrastructure issues.

### CCIP

The CCIP is responsible for the provision of high quality

advice and support to Critical Infrastructure (CI) organisations on matters pertaining to the protection of the national critical infrastructure from information-borne threats. This will be effected primarily through the provision of three strategies:

1. Providing a 24x7 "watch & warn" service to CI organisations,
2. Analysis and investigation of cyber attacks and research into CI in general
3. To work with CI and other sectors to improve awareness and communication regarding IT security

Although much of the information being distributed is readily available from other web sources, it is our

intention to provide a single source of information security issues with a NZ focus.

A new website, <http://www.ccip.govt.nz> has been developed and the unit can also be contacted via e-mail at: [info@ccip.govt.nz](mailto:info@ccip.govt.nz).

In an ongoing effort to improve the quality of information we provide in both this news letter and our website, we welcome your feedback as we can only service our constituency successfully if our lines of communication are two-way.

Regards,

**The CCIP Team**

## ALERT & ADVISORY SUMMARY

On the following page is a list of recent Alert and Advisories posted on the CCIP website since October 1.

Some of the highlights are:

- New Virus: BUGBEAR & UDP port 137 scanning activity

- Sec. Vulnerability in Apache OpenSSL (rev.2)
- Cumulative Patch for SQL Server
- Sans / FBI Top 20 Holes
- Trojan Horse Sendmail Distribution

- Unchecked Buffer in Outlook Express S/MIME Parsing Could Enable System Compromise

A complete list can be found at <http://www.ccip.govt.nz/alerts-advisories/alerts-advisories.htm>

## MAILING LIST

Critical alerts will be emailed separately to members of the CCIP email list as and when we become aware of them.

To subscribe to the CCIP

alert emailing list, send an email entitled **Subscribe** to [alerts@ccip.govt.nz](mailto:alerts@ccip.govt.nz). To unsubscribe, send an email entitled **Unsubscribe** to: [alerts@ccip.govt.nz](mailto:alerts@ccip.govt.nz).

This service is intended for CI organisations, government departments and IT service providers in New Zealand.

### INSIDE THIS ISSUE:

Alert & Advisory List	2
Bugbear hits New Zealand	2
Virus Activity	3
Port Scan Activity	3
Remote Access Trojans	4
Useful Sources	4

Communication regarding this newsletter can be addressed to:

[newsletter@ccip.govt.nz](mailto: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](mailto:info@ccip.govt.nz)

**Web:** [www.ccip.govt.nz](http://www.ccip.govt.nz)

PO Box 12-209  
Wellington, New Zealand

**ALERT & ADVISORY LIST for OCTOBER 1-15, 2002**

Platform	Description	Date
Red Hat	Command execution vulnerability in dvips	15/10/02
Red Hat	Updated squirrelmail packages close cross-site scripting vulnerabilities	15/10/02
Debian	New heartbeat packages fix buffer overflows	15/10/02
Hewlett-Packard	Security Vulnerability in LDAP-UX Integration	15/10/02
KDE	kpf Directory traversal	15/10/02
KDE	KGhostview Arbitrary Code Execution	15/10/02
Multiple	Several ports in the FreeBSD Ports Collection are affected by security issues	11/10/02
Red Hat	Updated analog packages are available for Redhat Powertools 7.1	11/10/02
Microsoft	Unchecked Buffer in Outlook Express S/MIME Parsing Could Enable System Compromise (Q328676)	11/10/02
Hewlett-Packard	HP Tru64 UNIX /usr/sbin/routed Potential Security Vulnerability	10/10/02
Red Hat	Updated fetchmail packages fix vulnerabilities	10/10/02
Debian	Multiple Debian Advisories	10/10/02
Multiple	Trojan Horse Sendmail Distribution	09/10/02
Apache	Apache 2.0.43 Released	09/10/02
Microsoft	Internet Explorer 5.2.2 for Mac OS X	09/10/02
Apple	Stuffit Expander 7.0 to fix security flaws in version 6.5.x	09/10/02
Multiple	Plain text exploits of /bin/login login program in Telnetd	08/10/02
SuSE	mod_php4: remote privilege escalation	08/10/02
SuSE	hylafax: remote privilege escalation	08/10/02
Red Hat	Updated tcpdump packages fix buffer overflow	08/10/02
EnGarde	Multiple vulnerabilities; fetchmail, tar, glibc.	08/10/02
Debian	Source code disclosure vulnerability in tomcat4	08/10/02
Conectiva	Local vulnerabilities in Xfree86	08/10/02
SGI	rpcbind vulnerabilities	08/10/02
Red Hat	Updated packages fix PostScript and PDF security issue	08/10/02
Red Hat	Updated glibc packages fix vulnerabilities in resolver	08/10/02
Red Hat	Updated nss_ldap packages fix buffer overflow	08/10/02
Cisco	Predefined restriction tables allow calls to international operator	07/10/02
Multiple	Sans / FBI Top 20 Holes	04/10/02
Microsoft	Flaw in Services for Unix 3.0 Interix SDK Could Allow Code Execution	04/10/02
Microsoft	Cumulative Patch for SQL Server	04/10/02
Microsoft	Unchecked Buffer in Windows Help Facility Could Enable Code Execution	04/10/02
Microsoft	Unchecked Buffer in File Decompression Functions Could Lead to Code Execution	04/10/02
Multiple	Malicious Software Report - Opaserv	03/10/02
Hewlett-Packard	Security Vulnerability in VVOS tomcat 3.2.x	03/10/02
Hewlett-Packard	Sec. Vulnerability in Apache OpenSSL (rev.2)	03/10/02
Multiple	New Virus: BUGBEAR & UDP port 137 scanning activity	01/10/02

*Businesses and individuals must ensure that they have anti-virus protection and make sure they update it.*

BugBear Hits New Zealand

*It can perform various tasks, including monitoring system performance, modifying Windows registry keys, as well as modifying or deleting crucial system files.*

Remotely Anywhere, pg 4

**BUGBEAR HITS NEW ZEALAND**

The Bugbear email virus has the anti-virus software of New Zealand Internet service providers and international computer security firms working double time. The virus has generated and infected a massive number of emails, including at least three Government agencies.

Businesses and individuals must ensure that they have anti-virus protection and make sure they update it.

The virus, thought to have

entered New Zealand last Tuesday night, has led to networks crashing and printers churning out pages of unreadable script. Seven out of every 10 emails received by Ihug had been generated by the virus, but cleaned by the ISP's anti-virus software, spokesman Tim Wood said.

Xtra also reported a massive number of infected emails. The company normally receives 30,000 to 40,000 viruses a day destined for its

subscribers, but in one day last week logged almost 60,000, of which half were Bugbear.

(Asia Intelligence Wire, via NewsEdge Corporation. 08 October 02)

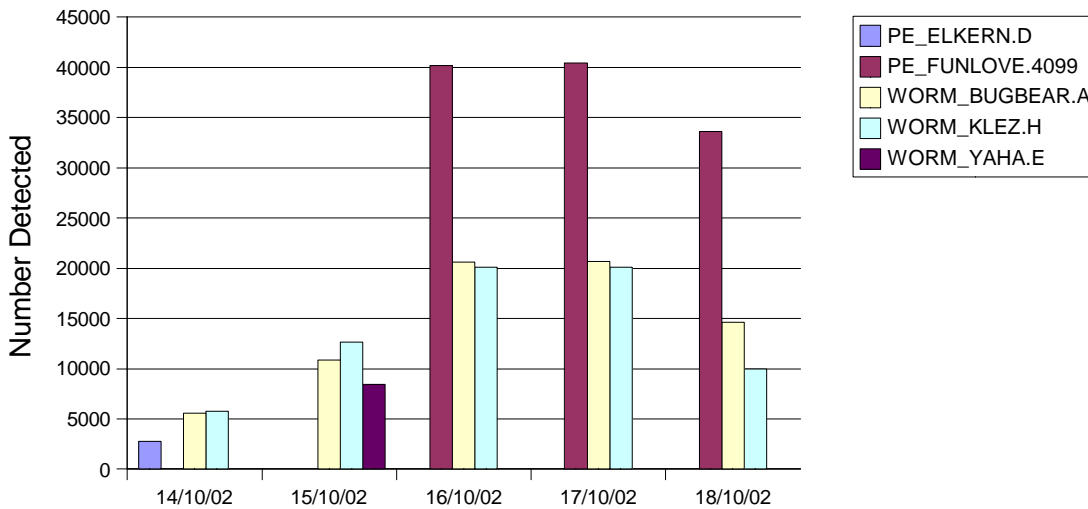
## VIRUS ACTIVITY

Klez and Bugbear continue to be the most prevalent malware affecting the New Zealand scene. However, according to TrendMicro, North America continues to be plagued by PE\_Funlove and, in Europe, Klez and PE\_ElkernD are 'top of the pops'. A graph of recent worldwide activity is attached.

*Klez and Bugbear continue to be the most prevalent malware affecting the New Zealand scene.*

Virus Activity

Worldwide Virus Trends, 13-19 October 2002, © TrendMicro Inc



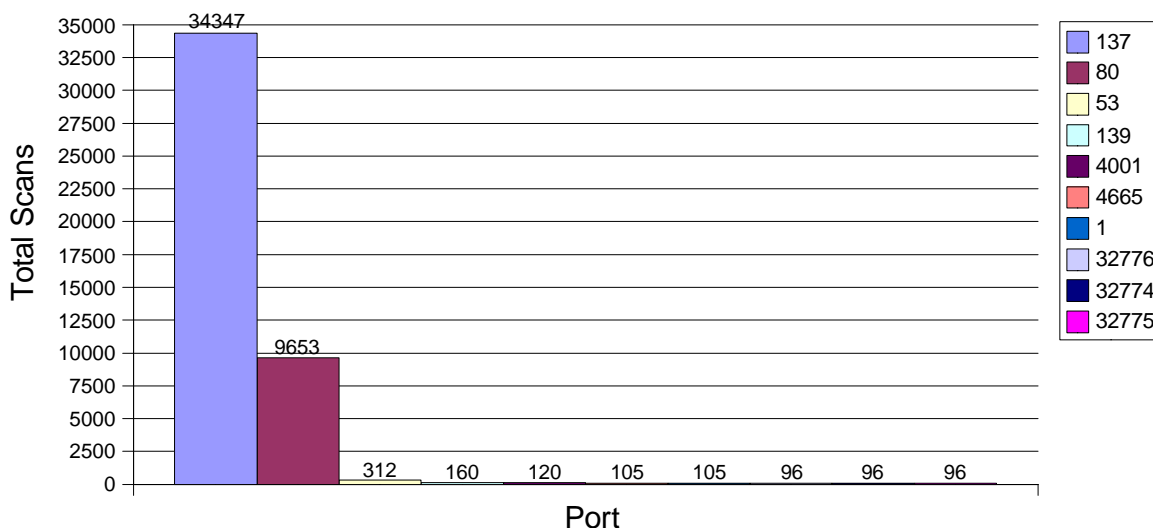
## PORT SCAN ACTIVITY

Port 137 continues to be the number one target<sup>1</sup> in New Zealand. This activity is closely associated with the widespread distribution of the Bugbear virus. Further information can be found at [http://www.cert.org/current/current\\_activity.html#W32BugBear](http://www.cert.org/current/current_activity.html#W32BugBear). (A target is defined as a 'a specific port on a distinct IP address targeted by another distinct IP address' (Internet Storm Center)). Other major targets are ports 80 (http) and 1433 (MS-SQL).

*Port 137 continues to be the number one target in New Zealand.*

Port Scan Activity

Top 10 Port Scans in New Zealand, 14-18 October 2002, © Internet Storm Centre



## REMOTE ACCESS TROJANS

Remotely Anywhere is a Windows® based remote administration tool. It is commercially available, and written by a Hungarian software manufacturer, 3am labs (<http://www.remotelyanywhere.com>). This software was recently discovered on several US government computers, prompting a high-priority search of their computer networks. It had been illegally installed, which would have required administrator access to the compromised computers.

This software is installed on a Windows computer. It sets up a world-wide web interface, allowing the computer to be controlled from the Internet. It can perform various tasks, including monitoring system performance, modifying Windows registry keys, as well as modifying or deleting crucial system files. This software was not designed as a hacking tool, and cannot perform malicious actions like crashing the computer, or keyboard logging. An ingenious attacker could still use the software to cause damage to the system or gain access to sensitive information.

There are various other remote access tools that include more malicious options. These are generally known as Remote Access Trojans (RATs). NetBus can do things like moving the mouse, swapping the mouse buttons over, and ejecting the CD tray. These actions perform no useful administrative

purpose, and are simply annoyances. BackOrifice is somewhat more covert than NetBus. BackOrifice can be silently installed over the network (in certain conditions) without the user's knowledge. It can run in the background, and then update or un-install itself remotely. It allows the client to log keystrokes and download files, and is under 2mb in size. BackOrifice has sometimes been covertly installed, and then used as an entry point to install other software, such as NetBus.

Remotely Anywhere does not include such covert options, and so it is easier to detect. For this reason many software anti-virus products do not include it in their virus definitions. There are software products that will detect it, such as PestPatrol (<http://www.pestpatrol.com>). There are also online services that will probe the ports of specified machines looking for "backdoors" e.g. Internet Security Systems (<http://www.ISS.com>). As this software has been found illegally installed on compromised machines, administrators should check their systems to make sure the software is not present.

Another RAT program is the "Global Threat Bot". This program is a modified Internet Relay Chat (IRC) client, combined with the HideWindow program, which makes it invisible to the user. It can be installed in various ways that

would be difficult for the users to notice. This program connects to an IRC channel, and awaits further instructions from the channel master. This program can only execute actions from within the IRC client, and so is predominantly used for denial of service attacks. The scripts used by this program are open source, and so have often been modified. Many different versions of this program now exist, although some have only minor changes. Different versions have different file names, and hide in different places. One common directory is the Windows Fonts directory. Most versions require the file "mir.ini" as the standard IRC client needs this file to start up. Some variants do exist where the IRC client has been modified to look for another file name. A full listing of common file names associated with this RAT can be located at <http://bots.lockdowncorp.com/list.html>. This Trojan Horse program is also common in the wild, and should be considered a significant threat to systems.

A combination of anti-virus protection, firewalls, O/S access control configuration and integrity checking will provide the best protection against RATs.

(Story collated by CCIP)

## 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 NZ 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 complete list of recent alerts and advisories.*

## REFERENCES

### SANS:

<http://www.sans.org/newlook/digests/SAC.htm>

### Internet Storm Centre:

<http://isc.incidents.org/>

### TrendMicro:

<http://wtc.trendmicro.com/wtc/>



## CONTACT DETAILS

Ph: +64 4 498 7654

Fax: +64 4 498 7655

Email: [info@ccip.govt.nz](mailto:info@ccip.govt.nz)

Web: [www.ccip.govt.nz](http://www.ccip.govt.nz)

PO Box 12-209

Wellington, New Zealand