



NEWSLETTER

CENTRE for
CRITICAL INFRASTRUCTURE
PROTECTION

Volume 2, Issue 1

March 06, 2003

WELCOME BACK

Welcome back. This is the first edition of the CCIP newsletter for 2003. I am sure we have all (re)learned lessons from the recent Slammer worm outbreak. The main one is 'keep your patches up to date'; easier said than done but ultimately unavoidable.

In this edition, we have added another graph to our usual offerings. Message-Labs, a UK-based Managed Service Provider, provide a service similar to the Trend-Micro Virus Map but with a

more European focus. We collect the top five reported viruses from both of these web sites each work day and generate the graphs, which tell their own story.

The graph of port scanning activity in New Zealand, which is generated from data published by the Internet Storm Centre, has also been updated to a format similar to the virus trends graphs. Once again port 137 (NETBIOS Name Service) is the most popular target, accounting for 30% - 60% of

all targets reported over the past month.

Also included in this edition is an item on the Open Web Application Security Project and From the CCIP Files, an article outlining two recent incidents.

We welcome any feedback regarding the content of this, or any other, newsletter and also our web site (refer to the side panel for relevant contact points).

OPEN WEB APPLICATION SECURITY PROJECT (OWASP)

When organisations put up a web application, they invite the world to send them HTTP requests. Attacks crafted into these requests can pass through firewalls, filters and intrusion detection systems. Even "secure" web sites that use SSL generally just accept the requests that arrive through the encrypted and authenticated tunnel without scrutiny. This means that the web application is not protected by the security perimeter. As the number, size and complexity of web applications increase, so does the perimeter exposure. Web application security vulnerabilities are often highly exploitable and the consequence of an attack could be significant.

Summary of the top vulnerabilities in web applications:

Unvalidated parameters

If information from web requests is not validated before being used by a web application, then attackers could use these flaws to attack backend components through a web application.

Broken access control

Restrictions on what authenticated users are allowed to do may not be properly enforced. Attackers can exploit these flaws to access other users' accounts, view sensitive files, or use unauthorised functions.

Broken account and session management

Account credentials and session tokens may not be properly protected. Attackers that can compromise passwords, keys, session cookies or other tokens can defeat authentication restrictions

and assume other users' identities.

Cross-site scripting flaws

The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose an end user's session token, attack the local machine, or spoof the content to fool the user.

Buffer overflows

Web application components in some languages that do not properly validate input can be crashed, and in some cases, used to take control of the web server process. These components can include CGI, libraries, drivers, and web application - server components.

INSIDE THIS ISSUE:

<i>Recent Significant Advisory & Alert list</i>	2
<i>From the CCIP Files</i>	2
<i>Virus Activity</i>	3
<i>Mailing List</i>	3
<i>New Zealand Port Scan Activity</i>	4
<i>OWASP Cont.</i>	4
<i>Reference List</i>	4

Communication regarding this newsletter can 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

PO Box 12-209
Wellington, New Zealand

(Continued on page 4)

RECENT SIGNIFICANT ADVISORY & ALERT LIST

REFERENCE	DESCRIPTION	DATE
CERT/CC	Remote Buffer Overflow in Sendmail	4/03/03
ISS	Snort RPC Preprocessing Vulnerability	4/03/03
HP	Security Vulnerability in DNS and resolver libraries	28/02/03
HP	Security Vulnerability in XDR library	28/02/03
iDefense	TCPDUMP Denial of Service Vulnerability in ISAKMP Packet Parsing	28/02/03
Microsoft	Flaw in Windows Me Help and Support Center could enable Code Execution	27/02/03
Cisco	Multiple Product Vulnerabilities Found by PROTOS SIP Test Suite	25/02/03
FreeBSD	Brute force attack on SYN cookies	25/02/03
UNIRAS	Malicious Software Report - W32/Lovgate variant	25/02/03
CERT/CC	Multiple vulnerabilities in implementations of the Session Initiation Protocol (SIP)	24/02/03
Cisco	Cisco response to Cisco IOS OSPF exploit	24/02/03
HP	Bastille sendmail.cf problem	21/02/03
CERT/CC	Multiple Vulnerabilities in Oracle Servers	20/02/03
HP	Potential Sec. Vulnerability in rpc.ttdbserver	20/02/03
HP	Potential Security Vulnerabilities in SNMP (revision 16)	20/02/03
HP	Potential Security Vulnerability in xfs	20/02/03
Lotus	Multiple security advisories for Lotus iNotes and Lotus Domino web server	20/02/03
ORACLE	Buffer overflow in ORACLE.EXE binary of Oracle9i/Database server	19/02/03
IBM	Buffer Overflow in AIX libM.a	18/02/03
Microsoft	Cumulative Patch for Internet Explorer (revised)	14/02/03
SGI	IP denial-of-service fixes and tunings	13/02/03
redhat	Updated kernel-utils packages fix setuid vulnerability	11/02/03
redhat	Updated w3m packages fix cross-site scripting issues	11/02/03
Microsoft	Flaw in Windows WM_TIMER Message Handling Could Enable Privilege Elevation	10/02/03
Microsoft	Unchecked Buffer in Windows Redirector Could Allow Privilege Elevation	6/02/03
MIT	Multiple vulnerabilities in old releases of MIT Kerberos	3/02/03

Please refer to the CCIP website for a more complete list of alerts and advisories.

Two New Zealand organisations recently informed CCIP that their computer systems had been used for unauthorised purposes.

From the CCIP Files

FROM THE CCIP FILES

Two New Zealand organisations recently informed CCIP that their computer systems had been used for unauthorised purposes. In one case a server was compromised and unauthorised software installed, and in the other case a publicly accessible ftp server was used to host and distribute illegally copied software ("warez"). In both instances the compromise appeared to be possible due to insecure firewall configurations.

A firewall will normally be a company's first line of protection against external hackers. For it to be effective, the rules defining the types of traffic permitted through the firewall need to be managed, documented and periodically

audited. The firewall should limit the traffic to only allow authorised services, IP addresses and possibly users. There should be a configuration management process in place and the configuration and log files should be reviewed on a regular basis. In addition, as the majority of firewall models only carry out limited application level checks, it is important that the servers behind the firewall are appropriately patched and configured. The firewall logs and configuration details should be regularly backed up and stored in a safe location. The use of a separate log server could also be considered. This will make it harder for hackers to cover their tracks

as well as provide the ability to restore firewall configuration in disaster recovery situations.

Closely examining the logs will not itself prevent a hacking attack. However, it may give the administrator a "heads-up" that something is amiss, and more time to react before attacker has time to consolidate their position.

In the second incident mentioned earlier, the server was used to store and distribute "warez" for several months before the compromise was discovered. Regular checking of the access and usage logs would have revealed unusual patterns much earlier.

For guidance in this area, the

(Continued on page 3)

Seven CERT/CC advisories this year to date. Three in the last month.

Recent Significant Advisory & Alert list

FROM THE CCIP FILES CONT.

(Continued from page 2)

Minimum Standards for Internet Security in the New Zealand Government are now incorporated in the document titled "Security in the Government Sector" (available from www.security.govt.nz). The CCIP appreciates the

cooperation of both of the organisations in question. We correlate reports from various sources - including incident reports - in order to develop an understanding of current hacking attempts and tactics so we can report on trends and current issues to NZ IT users. We encourage

other NZ organisations to report IT security incidents or issues. Our incident reporting form is available from the CCIP website. Any CCIP reporting of the incident will ensure anonymity of the information sources unless otherwise explicitly agreed.

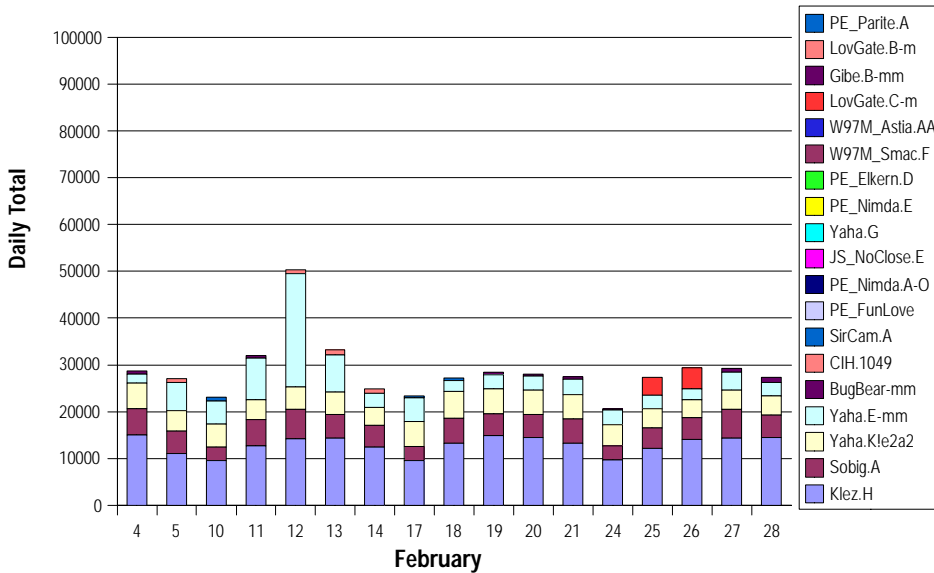
Attackers that can compromise passwords, keys, session cookies or other tokens can defeat authentication restrictions and assume other users' identities.

Open Web Application Security Project, page 1.

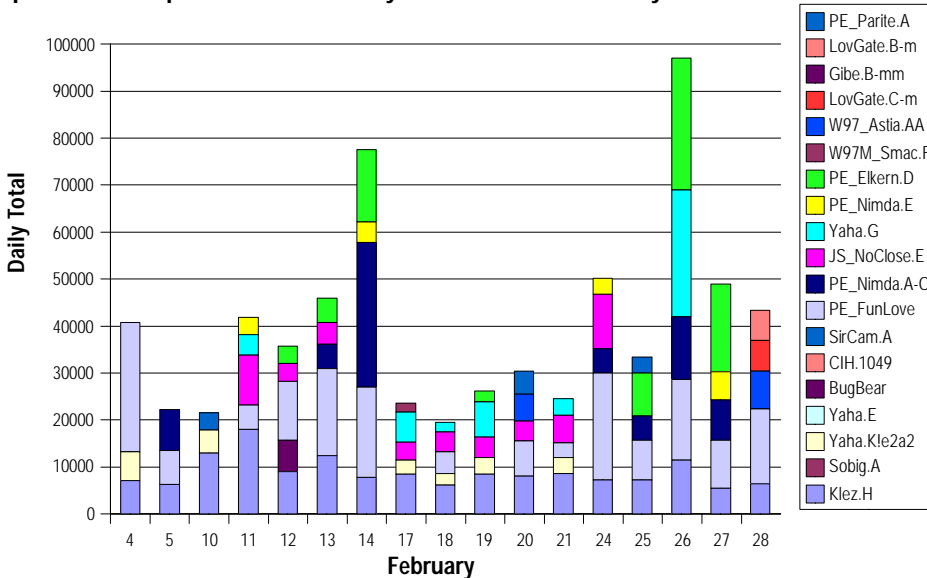
VIRUS ACTIVITY

After a busy start to the year by virus writers, Klez.H continues to be the most prolific worm surviving 11 months now, PE_FunLove is still number one in the US according to TrendMicro.

Top 5 Viruses captured Worldwide by MessageLabs in February



Top 5 Viruses captured Worldwide by TrendMicro in February



Klez.H continues to be the most prolific worm worldwide

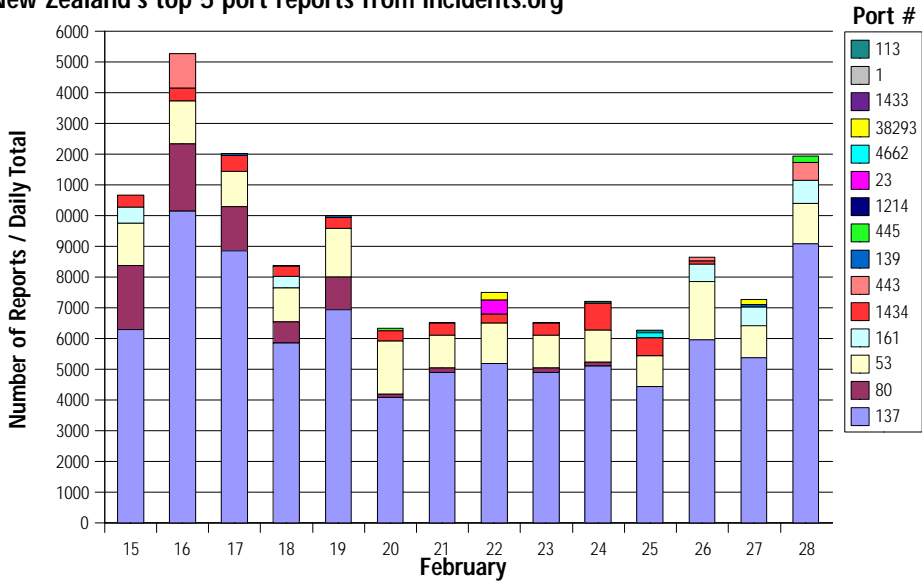
Virus Activity



NEW ZEALAND PORT SCAN ACTIVITY

Port 137 (NETBIOS Name Service) is clearly the most scanned port in New Zealand during the last half of February. The key to the right shows other TCP/UDP ports to make the top five.

New Zealand's top 5 port reports from Incidents.org



OWASP CONT.

(Continued from page 1)

Command injection flaws

Web applications pass parameters when they access external systems or the local operating system. If an attacker can embed malicious commands in these parameters, the external system may execute those commands on behalf of the web application.

Error handling problems

Error conditions that occur during normal operation are not always handled properly. If an attacker can cause errors to occur that the web application does not handle they can gain detailed system information, deny service, cause security mechanisms to fail, or crash the server.

Insecure use of cryptography

Web applications regularly use cryptographic functions to protect information and protect credentials. These functions and the code to integrate them have proven difficult to code properly, frequently resulting in weak protection.

Remote administration flaws

Many web applications allow administrations to access the site using a web interface. If these administrative functions are not very carefully protected, an attacker can gain full administration access to the site.

Web and application server misconfiguration

Having a strong server configuration standard is critical to a secure web application. There are many server configuration options that can affect security. These are often not set in the standard configuration.

The security issues listed are not new, in fact, some have been well understood for decades. Still these vulnerabilities continue to jeopardise local security.

The complete document, which details the vulnerabilities and offers best practice guidelines for mitigation, can be found at the Open Web Application Security Project website.

REFERENCES

OWASP: www.owasp.org
TrendMicro: www.trendmicro.com

MessageLabs: www.messagelabs.com
Internet Storm Centre: isc.incidents.org

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 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

PO Box 12-209
Wellington, New Zealand