



NEWSLETTER

CENTRE for
CRITICAL INFRASTRUCTURE
PROTECTION

Volume 1, Issue 2

November 15, 2002

SINCE THE LAST ISSUE ...

On October 21, a significant distributed denial of service (DDoS) attack was conducted against a number of root Domain Name Servers (DNS), followed by another attack against several Generic Top Level Domain (GTLN) name servers. These servers essentially translate web site names that are readable by humans into numerical Internet Protocol (IP) addresses that computers can interpret.

Although it is likely that these attacks intended to disrupt the Internet, they were unsuccessful, with users failing to notice any interruption to regular Internet service. The

source of the attack has not been identified but Robert Mueller, the FBI Director, is quoted as saying " the attacks likely emanated from computers in the United States and South Korea". Further information is available in the NISCC monthly report: www.niscc.gov.uk/Monthly/latest_monthly.pdf (page 2).

This attack has led to considerable comment and a plethora of commentators have voiced an opinion. One of the more interesting was from Ed Skoudis, Vice President of security strategy at Predictive Systems, who said when dis-

cussing other Internet choke points, " the system of core routers which act as Internet air traffic controllers is considerably more fragile than the domain name system and the next wave of attacks could take on these systems. Most of the Internet's traffic must pass through one of several core routers, and if they were somehow crippled simultaneously, the Net would grind to a halt. If you can't route packets, then that's it, you're done". Let's hope this prediction does not come to pass!

INSIDE THIS ISSUE:

<i>Alert & Advisory List</i>	2
<i>October Virus Statistics</i>	2
<i>Virus Activity</i>	3
<i>Port Scan Activity</i>	3
<i>New Thinking on Virus Propagation</i>	4
<i>Mailing List</i>	4

EXTREME HACKING COURSE

Ernst & Young will be running their 4-day eXtreme Hacking course in Wellington on the 2nd to the 6th of December. It is the first time

this course has been run in New Zealand. Details are available online at www.ey.com/nz/extremehacking

or contact Chris Gatford on: (04) 499 4888 or email chris.gatford@nz.eyi.com.

Communication regarding this newsletter can be addressed to:

newsletter@ccip.govt.nz

ALERT & ADVISORY SUMMARY

A number of significant alerts and advisories have been issued recently including:

- Three Cert/CC advisories, one relating to vulnerabilities in BIND, a Buffer Overflow in Kerberos Administration Daemon and another

relating to a denial-of-service vulnerability in multiple vendor Sun RPC-based libc implementations.

- A NISCC advisory relating to a potential crafted packets vulnerability in firewalls
- Microsoft released a num-

ber of fixes including a cumulative patch for IIS and a fix for an unchecked buffer overflow in the Point-to-Point Tunnelling Protocol (PPTP)

- A number of fixes to various Apache implementations have also been released.



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



ALERT & ADVISORY LIST for NOVEMBER 1-12

Few questions are simultaneously so baffling and so significant as: "What is the structure of the Internet?"

New Thinking on Virus Propagation, page 4

REFERENCE	DESCRIPTION	DATE
ISS	Multiple Remote Vulnerabilities in BIND 4 and BIND 8.	12/11/02
Debian	Multiple Debian Advisories	11/11/02
NetBSD	Unexpected TCP session establishment by malicious remote input	11/11/02
CERT	Multiple Sun RPC-based libc implementations fails to provide time-out mechanism when reading data from TCP connections	09/11/02
Red Hat	Updated kerberos packages available	09/11/02
Red Hat	Updated glibc packages fix vulnerabilities in resolver	09/11/02
SGI	Multiple SGI Advisories	08/11/02
Hewlett-Packard	Security Vulnerability in rpc.ttdbserver (rev.4)	07/11/02
iDEFENSE	Denial of Service Vulnerability in Xeneo Web Server	07/11/02
iDEFENSE	Pablo FTP Server DoS Vulnerability	07/11/02
Microsoft	Incorrect MIME Header Can Cause IE to Execute E-mail Attachment	07/11/02
OpenBSD	Multiple OpenBSD Advisories	07/11/02
Debian	New Apache-SSL packages fix several vulnerabilities	06/11/02
Hewlett-Packard	HP TruCluster Server Interconnect Potential Security Vulnerability	06/11/02
NetBSD	IPFilter FTP proxy vulnerability	06/11/02
Debian	New Apache packages fix several vulnerabilities	05/11/02
Cisco	Multiple Cisco ONS15454 and Cisco ONS15327 Vulnerabilities	04/11/02
Debian	log2mail -- buffer overflow	04/11/02
Debian	heimdal -- buffer overflow	04/11/02
Hewlett-Packard	Security Vulnerability in Apache	04/11/02
SCO	OpenLinux: chfn (util-linux) temp file race vulnerability	04/11/02
SCO	OpenLinux: pam_ldap format string vulnerability	04/11/02
SuSE	syslog-ng : remote command execution	04/11/02
SuSE	Vulnerabilities in lprng and html2ps	04/11/02
Microsoft	Windows 2000 Default Permissions Could Allow Trojan Horse Program	01/11/02
Microsoft	Unchecked Buffer in PPTP Implementation	01/11/02
Microsoft	Cumulative Patch for Internet Information Service	01/11/02
UNIRAS	Firewall packet filtering bypass vulnerability - multiple OS's	01/11/02

Most of the vulnerabilities reported so far in 2002 affect Microsoft platforms.

October Virus Statistics

OCTOBER VIRUS STATISTICS

A review of the October statistics produced by Sophos, MessageLabs, Kaspersky and Central Command has highlighted some interesting variations in their top five reports. W32/Bugbear-A is number one in three of the four reports, with Sophos indicating that it accounts for a massive 77.6% of all reports for the month. W32/Klez-H is number one at

Central Command and number two with Sophos and MessageLabs. W32/Yaha-E is Number two with Kaspersky. Other viruses still doing the rounds are W32/Yaha-E , W32/EIKern-C

These figures tie in generally with the trend analysis performed on the numbers from TrendMicro on page 3 of the newsletter and also reinforce

the conclusions in the recent news release from mi2g (<http://mi2g.com/cgi/mi2g/press/110702.php>) that most of the vulnerabilities reported so far in 2002 affect Microsoft platforms.

SOPHOS		MESSAGELABS		KASPERSKY		CENTRAL COMMAND	
Virus	%	Virus	%	Virus	%	Virus	%
W32/Bugbear-A	77.60%	W32/Bugbear-A	45.33%	W32/Bugbear-A	44.90%	W32/Klez-H	23.40%
W32/Klez-H	6.20%	W32/Klez-H	30.65%	W32/Yaha-E	21.60%	W32/Bugbear-A	20.90%
W32/Opaserv-A	2.50%	W32/Yaha-E	13.72%	W32/Klez-H	14.00%	W32/Yaha-E	11.50%
W32/Yaha-E	1.10%	W32/SirCam.A	2.07%	Macro.Word97.Thus	3.10%	W32/EIKern-C	8.20%
W32/Badtrans-B	0.80%	W32/Klez-E	0.40%	I_Worm.Hybris	1.10%	W32/SirCam.A	6.00%

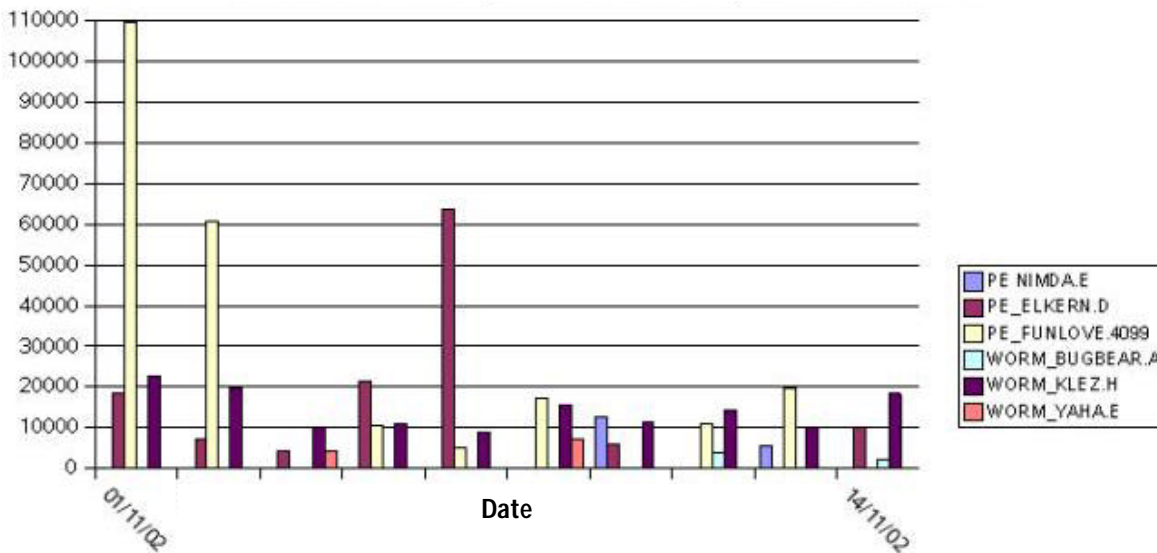
VIRUS ACTIVITY

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.

Worldwide Virus Trends, 1 - 14 November, 2002, © TrendMicro Inc

Virus Activity



PORT SCAN ACTIVITY

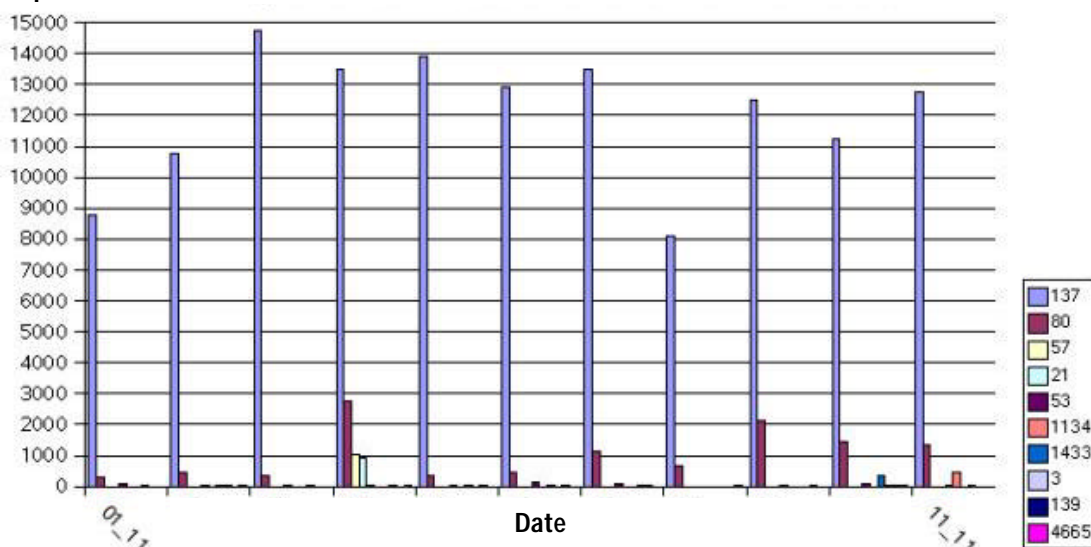
Port 137 continues to be the number one target¹ in New Zealand. This activity is closely associated with the widespread distribution of the Bugbear virus. Further information can be found at http://www.cert.org/current/current_activity.html#W32BugBear. Other major targets are ports 80 (http) and 1433 (MS-SQL).

¹A target is defined as a specific port on a distinct IP address targeted by another distinct IP address (Internet Storm Center).

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

Port Scan Activity

Top 10 Port Scans in New Zealand, 1 - 11 November, 2002, © Internet Storm Centre



NEW THINKING ON VIRUS PROPAGATION

To understand how viruses spread we need to appreciate the structure of the Internet. This is a baffling and significant concept. Baffling because it has grown without any planning or central organisation. Significant because knowing how the routing computers that are the Net's physical embodiment are interconnected is vital if it is to be used properly.

Until 1999, the standard way of modeling the Internet was to use randomly generated graphs, in which routers were represented by points and the links between them by lines. But it turns out that such random graphs are a poor approximation because they miss two important features. The first that links in the Net are "preferentially attached": a router that has many links to it is likely to attract more links; one that does not, will not. The second is that the Internet has more clusters of

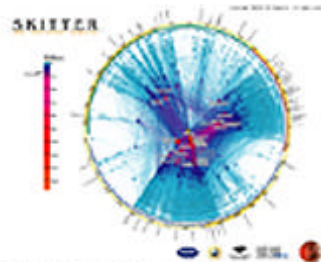
connected point than random graphs do. These two properties give the Internet a topology that is scale-free in other words, small bits when suitably magnified resemble the whole.

Dr Albert-Laslo Barabasi and his colleagues at the University of Notre Dame, in Indiana, treat the Net as though it were a natural phenomenon and noticed that the World Wide Web was scale-free in 1999, this has several implications. On the one hand, scale-free topology is resistant to random failures - one reason the Internet, despite the lack of artifice in its design, has proved so reliable. On the other hand, because there are disproportionately many hubs (well connected routers), the Net is susceptible to deliberate attacks on those hubs.

Already understanding the Net's scale free structure has led to new results. For example, it has long been

thought that the best way to curb the spread of a computer virus was to change the software of the machines on the net so that they were less easily "infected". Studies using random graphs had shown that changing software on more and more machines has a cumulative effect. That's not true in a scale-free setting. There, most software changes make no difference to the rate at which a virus spreads (although they obviously protect the machines in question). However treating the relatively small number of hubs in a scale-free system can stamp out viruses completely.

Paraphrased from 'What Does the Internet Look Like?' The Economist, 05/10/02.



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

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.

MAILING LIST

Critical alerts will be emailed 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. To unsubscribe, send an email entitled 'Unsubscribe' to the same address.

REFERENCES

Central Command:
www.centralcommand.com

Kaspersky:
www.kaspersky.com

MessageLabs:
www.messagelabs.com

Sophos:
www.sophos.com

Internet Storm Centre:
<http://isc.incidents.org/>

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

The Economist article:
http://www.economist.com/displayStory.cfm?Story_ID=S%27%29H%20%2AQA%3F%22%23%40%212%0A

Paper from Zoltan Dezso & Albert-Laszlo Barabasi:
<http://www.nd.edu/~zdezso/trans.pdf>

The skitter graph:
http://www.caida.org/analysis/topology/as_core_network/AS_Network.xml



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