



NEWSLETTER

CENTRE for
CRITICAL INFRASTRUCTURE
PROTECTION

Volume 2, Issue 9

November 2003

“PHISHING” SEASON REOPENS

Six months have passed since we published our article “eFraud on the Rise” (see page three) in which we highlighted Seven Simple Steps to Help You Avoid Being Scammed. With the recent increase in ‘phishing’ expeditions, especially those targeting bank customers in New Zealand, it is time to revisit the list. Also, an analysis of one of the latest phishing e-mails,

purportedly being sent from the ANZ Banking Group, shows an interesting variation in the HTML code formatting the message. Although there are obvious indications of impersonation in the content of the message (e.g. the bogus phone number ‘13 13 13’), a look at the HTML code also highlights another trick being used by the fraudsters. Depending on the mail client and text

editor in use, the true hyperlink may or may not be visible as white-space has been inserted before the offending HTML code. When viewing the message source, ensure that ‘word wrap’ is enabled and all will be revealed. It has been reported that over 300 customers in New Zealand have fallen victim to these latest scams in recent days.

DCOM, RPC, & MSBLAST

Microsoft announced last July that a [critical vulnerability](#) had been discovered in several versions of the Windows operating system. Four weeks later, the “MSBLAST” worm was discovered, exploiting this vulnerability. On 10 September, Microsoft announced [further vulnerabilities](#) in the same service, and with the same potential consequences.

The vulnerabilities exist in the Distributed Component Object Model (DCOM). This is a set of concepts and program interfaces that allows communication between running programs (processes) and computers, across a network. This service can have beneficial effects in various situations, e.g. when an Internet Information Services web-server needs to talk to an application server-farm running components on separate machines. DCOM uses the industry

standard Remote Procedure Call (RPC) protocol to communicate by inserting its own data into some RPC fields. DCOM does not correctly check, in all cases, that it has allocated enough memory (called a “buffer”) to store an incoming RPC message, which can lead to other memory being overwritten (known as a “buffer overflow”). Further information on buffer overflows is available at [SearchSecurity.com](#), and [LinuxJournal.com](#). These particular DCOM buffer overflows can cause the computer to stop performing useful work, or perform any other function, of an attacker’s choosing.

The vulnerability was easily exploited because recent versions of Windows have had DCOM enabled by default. Vulnerable versions of Windows include NT (4.0), 2000, XP, and Server 2003 (Windows 95, 98 and ME do not appear to be affected).

Microsoft suggest that although DCOM is enabled by default, it is not intended to operate in a “hostile” environment such as the Internet, and should be disabled in these circumstances.

The MSBLAST worm used this DCOM vulnerability to spread. The worm passes the victim computer a message designed to exploit the DCOM vulnerability. The message causes that computer to download the worm’s executable code from the attacking machine, and then run it. This executable code takes various actions, such as installing itself in the Windows registry, attempting a Denial of Service attack on the Windows-Update website, and opening a backdoor command-shell on the Transmission Control Protocol (TCP) port 4444. It also begins scanning for

(Continued on page 2)

IN THIS ISSUE:

<i>DCOM, RPC and MSBLAST</i>	1
<i>eFraud on the Rise Revisited</i>	3
<i>Virus Activity</i>	3
<i>New Zealand Port Scan Activity</i>	4
<i>New CCIP Manager Appointed</i>	4
<i>Recent Significant Alerts & Advisories</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

PO Box 12-209
Wellington, New Zealand

DCOM, RPC, & MSBLAST (cont.)

(Continued from page 1)

other computers to infect. Fortunately, the MSBLAST worm is not very efficient:

- It does not check which version of Windows it is about to attack, randomly choosing which version of the exploit to use. Some systems will crash or reboot rather than transparently being infected when sent the wrong version of the exploit. A computer connected to the internet could continually be reinfected, causing ongoing reboots.
- It unnecessarily uses an unusual protocol (Trivial File Transfer Protocol) to connect back to the attacking computer and download the executable code. This service is rarely used and should be blocked at the firewall, and is also easily noticeable in system logs.
- The MSBLAST worm uses only the first DCOM vulnerability discovered (MS-03-026). It is likely only a matter of time before a faster and more efficient worm is released which targets all of the discovered vulnerabilities.
- The worm is coded to attack a Microsoft website by overloading it with spurious requests. The target-site was simply redirecting traffic to another Microsoft site, which enabled Microsoft to take the target-site offline without any loss of functionality.

If kept properly patched, a computer will not be vulnerable to the recently

discovered DCOM flaws. Microsoft worked with the team that discovered the first vulnerability ([The Last Stage of Delirium](#)) and then the teams that discovered the later vulnerabilities (eEye Digital Security, NSFOCUS Security Team, and Xue Yong Zhi and Renaud Deraison from Tenable Network Security) to develop a patch before the vulnerability became public. The initial patch released by Microsoft for the first vulnerability has now been superseded by a later patch, which addresses the earlier and the subsequently discovered vulnerabilities in this service.

Although patching computers promptly to prevent the exploitation of flaws is sound security practice, patches should be tested before being deployed on critical systems.

For DCOM to function, certain ports must be accessible via the network. However, an open port is a potential attack avenue from the Internet. If ports are not required to be open to the Internet, then they should be blocked at the firewall. The DCOM ports include UDP ports 135, 137, 138, 445 and TCP ports 135, 139, 445, 593, as well as any other ports that are configured to use DCOM. Blocking these ports at the firewall will limit your computer's exposure.

But the infection often did not come directly from the Internet, instead coming from inside the corporate network. Laptops in some cases became infected with the MSBLAST worm outside of an organisation's network, e.g. at a worker's home.

Those laptops were then connected to the internal network, where they were able to infect other machines – bypassing the firewall completely. Each computer should be hardened against the vulnerability, to prevent one unexpected source of infection from taking down the entire network.

In the majority of cases DCOM will be enabled by default and although it can be useful in some situations, if it is not required then it should be disabled.

For further information on this topic, refer to Microsoft's "[How to Disable DCOM Support in Windows](#)".

The RPC and DCOM services can also be used over HTTP, for example to connect an Outlook 2003 client to a remote Exchange server from any World Wide Web connection. This means that it may also be necessary to disable COM Internet Services and RPC over HTTP, which listens on ports 80 and 443. Further information is available at "[How to Remove COM Internet Services \(CIS\) and RPC over HTTP Proxy Support](#)".

DCOM has had several vulnerabilities discovered and it may contain others. The MSBLAST worm used only one of these flaws to spread and cause considerable damage. Future malicious software exploiting DCOM flaws may bring even more disruption. Disabling DCOM and/or blocking the ports used by DCOM will mitigate all known vulnerabilities in this

(Continued on last page)

The vulnerability was easily exploited because recent versions of Windows have had DCOM enabled by default.

DCOM, RPC, & MSBLAST
pages 1, 2 & 4

Never follow a hyperlink supplied in an e-mail. Connect to the site by typing the URL into the browser or by using a bookmark.

eFraud on the Rise Revisited
page 3

eFRAUD ON THE RISE REVISITED

Below are the seven simple steps to help you avoid being scammed; first published in our May newsletter (v2i3).

1. Never follow a hyperlink supplied in an e-mail. Connect to the site by typing the URL into the browser or by using a bookmark.
2. Verify that the domain name is the correct one for the organisation.
3. Check the details of the website's digital certificate and ensure it has been issued by a verified Certificate Authority (CA).
4. Do not use the same password for different websites.
5. Make yourself aware of the company's on-line security policy. Never provide account details and passwords in response to unsolicited e-mail.
6. Read the e-mail request carefully - you should be suspicious if the request is written poorly or has obvious grammatical errors.
7. Visit the netsafe.org.nz website for advice on general Internet safety.

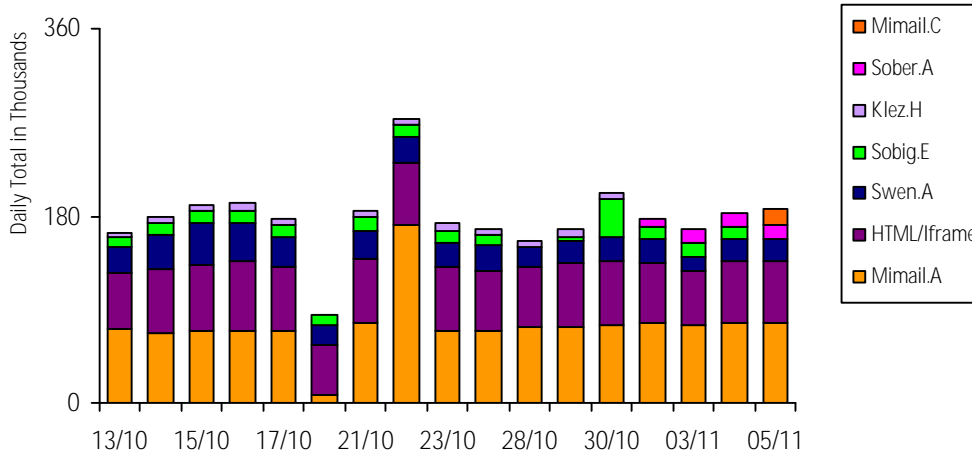
Previous newsletters are available on request.
E-mail us at: newsletters@ccip.govt.nz

This month has seen the departure of the founding CCIP manager, Jay Garden.

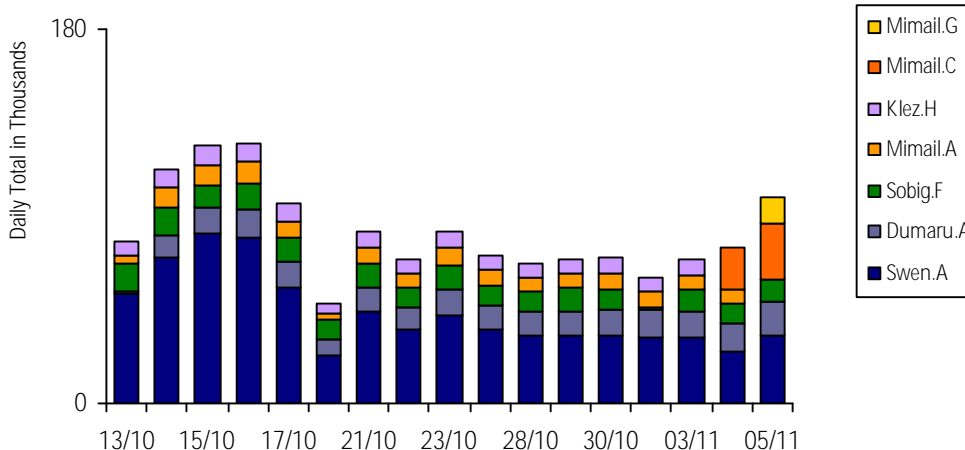
New CCIP Manager Appointed page 4

VIRUS ACTIVITY

Daily top 5 viruses captured worldwide by [RAV](#)



Daily top 5 viruses captured worldwide by [MessageLabs](#)



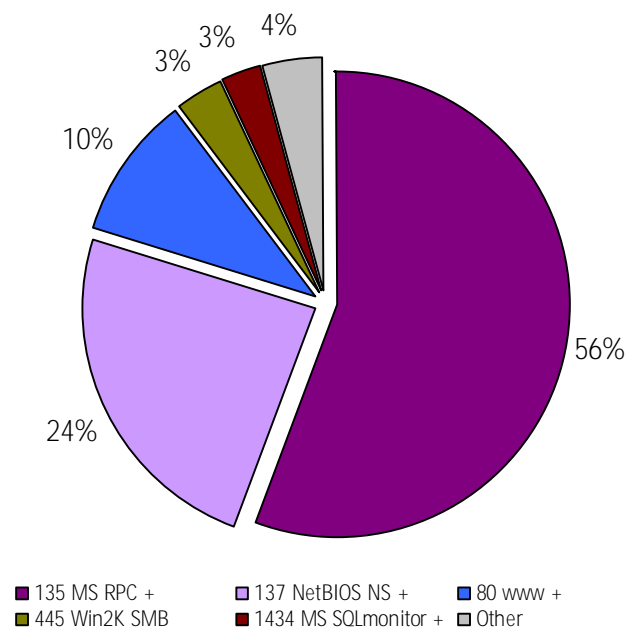
It is likely only a matter of time before a faster and more efficient worm is released which targets all of the discovered vulnerabilities.

DCOM, RPC, & MSBLAST pages 1, 2 & 4



NEW ZEALAND PORT SCAN ACTIVITY

New Zealand port scanning activity by port number from 9 October to 1 November.



Scanning for Microsoft DCOM ports still accounts for over 75 percent of the port scanning activity reported to incidents.org. Hopefully the feature article in this Newsletter gives some insight in to the vulnerability in this service and a possible reason for this scanning.

If you are interested in how the port scan activity is obtained, by the Internet Storm Center (ISC), please see their "[about page](#)" which discusses the methodology and location of the sensors.

For more information see 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.

NEW CCIP MANAGER APPOINTED

This month has seen the departure of the founding CCIP manager, Jay Garden. He has moved back to the mainland to utilise his wide array of skills in the private sector.

All at CCIP wish him well in his new venture.

Succeeding Jay is Chris Roberts, most recently manager of the GCSB INFOSEC Assessments Unit.

Chris brings considerable international consultancy experience to the role, in both the public and private sector.

DCOM, RPC, & MSBLAST (cont.)

(Continued from page 2)

service. Applying a "defense-in-depth" policy should include all three of the options mentioned above – patch necessary

services, remove or disable unnecessary services, and block all the non-essential ports from passing through the firewall. Hopefully, these will prevent

MSBLAST.2 (watch this space) from taking down your mission-critical network.

RECENT SIGNIFICANT ALERTS & ADVISORIES

Reference	Description	Date
NISCC	Vulnerability Issues in Implementations of the S/MIME Protocol	05/11/03
NISCC	Vulnerability Issues in Implementations of the X.400 Protocol	05/11/03
OpenSSL	OpenSSL Denial of Service in ASN.1 parsing	05/11/03
Microsoft	Microsoft Windows, Revised Security Bulletin Summary for Oct 03	31/10/03
Apache	HTTP Server 2.0.48 Released addresses two security vulnerabilities	31/10/03
CERT	Multiple Vulnerabilities in Microsoft Windows and Exchange	17/10/03

Please refer to the CCIP website for a more complete list of 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

PO Box 12-209
Wellington, New Zealand