



NEWSLETTER

CENTRE for
CRITICAL INFRASTRUCTURE
PROTECTION

Volume 2, Issue 10

November 2003

SIX VULNERABILITIES AND A TROJAN

The latest monthly Microsoft security bulletin contained three critical advisories relating to the Windows operating system. Within days of the bulletin being published, code to exploit one of the vulnerabilities was released. The advisories detailed:

- [a buffer overrun in the Workstation service](#);
- [a buffer overrun and a 'denial of service' vulnerability in FrontPage Server Extensions](#); and
- [a cumulative security patch for Internet Explorer](#).

The [CERT](#) Coordination Centre and [Internet Security Systems](#) (ISS) describe the Workstation buffer overrun as easy to exploit and well suited to use by self-spreading Internet worms. The published exploit code targets this vulnerability. Patches are available from Microsoft's website.

Also published this month were three vulnerability advisories from the [National Infrastructure Security Co-ordination Centre](#) (NISCC) in the UK. These advisories relate to ongoing issues, with ASN.1 based protocols, that were discovered during research by the [Oulu University Secure Programming Group](#)

(OUSPG). The protocols involved are:

- OpenSSL2
- S/MIME (Secure/MIME)
- X.400

Reference should be made to specific vendors for up-to-date status and patch information.

Finally, NISCC has published an analysis of the Autoproxy trojan. Autoproxy exploits the Java ByteCode Verifier vulnerability discussed in Microsoft Bulletin [MS03-11](#), and also the Object Tag vulnerability detailed in [MS03-40](#).

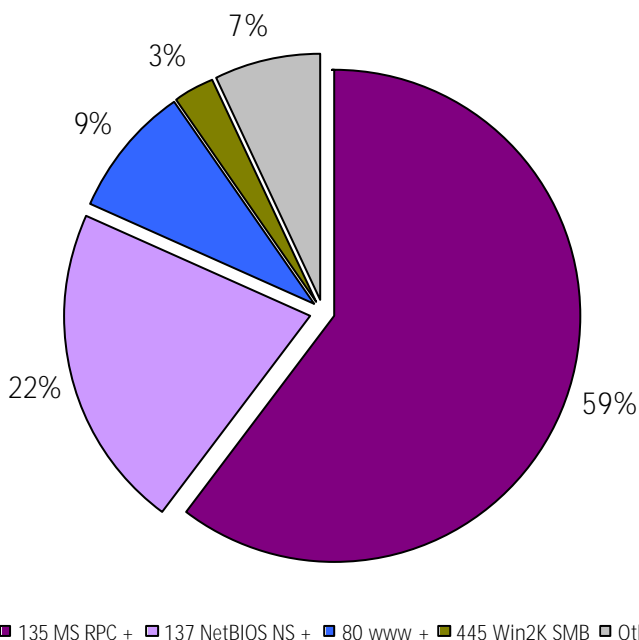
(Continued on page 2)

IN THIS ISSUE:

<i>Six Vulnerabilities and a Trojan</i>	1
<i>New Zealand Port</i>	1
<i>Six Vulnerabilities & a Trojan Cont.</i>	2
<i>Virus Activity</i>	2
<i>Recent Significant Alerts & Advisories</i>	2

NEW ZEALAND PORT SCANNING ACTIVITY

New Zealand port scanning activity by port number from 31 October to 17 November.



Scanning for Microsoft DCOM ports (135 and 137) continues to account for the majority (81 percent) of port scanning activity detected in New Zealand, as reported by [incidents.org](#).

Of note in the "Other" category, for seven days from November 4, an increase in scanning for port 53 (DNS) was recorded. This activity was seen worldwide and not isolated to New Zealand. Scanning for port 27374 also featured during this period. This port is used by a plethora of malware. Trojan lists indicate that 1i0n, a Linux worm, utilises both of these ports.

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



SIX VULNERABILITIES AND A TROJAN (cont.)

(Continued from page 1)

The Authenticode and ActiveX vulnerabilities from [MS03-41](#) and [MS03-42](#) allow the execution of code hosted on a malicious website.

A detailed analysis of the trojan is available from the [LURHQ Threat Intelligence Group](#).

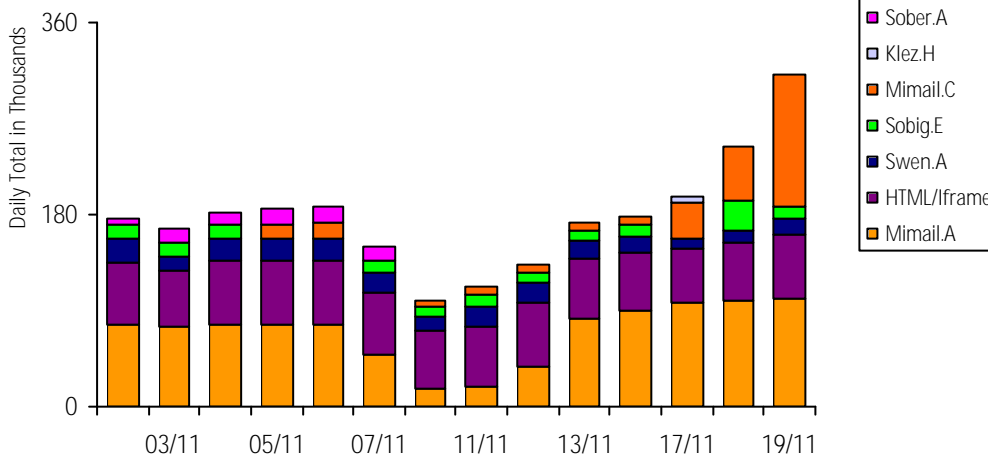
Malware embedded in code on websites is an emerging attack vector. It is

potentially even more dangerous than current mass-mailers.

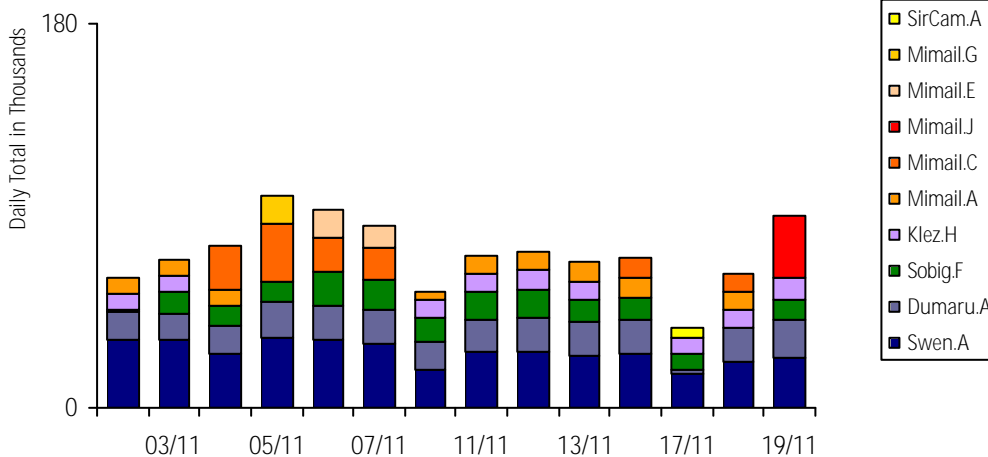
This leaves one simple recurring message – keep patches up-to-date and practice defence in depth.

VIRUS ACTIVITY

Daily top 5 viruses captured worldwide by **RAV**



Daily top 5 viruses captured worldwide by **MessageLabs**



RECENT SIGNIFICANT ALERTS & ADVISORIES

Reference	Description	Date
@stake	SAP DB Privilege Escalation/Remote Code Execution	18/11
ISS	PeopleSoft IClient Servlet Remote Command Execution Vulnerability	14/11
UNIRAS	Corsaire - PeopleSoft Advisories	14/11
Clearswift	MAILsweeper Malformed Zip Archive Virus Detection Bypass	06/11
OpenSSL	OpenSSL Denial of Service in ASN.1 parsing	05/11

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.

