



NEWSLETTER

CENTRE for
CRITICAL INFRASTRUCTURE
PROTECTION

Volume 3, Issue 2

March 2004

BAGLES ON THE MENU

A lot of news for a short month. On the virus front; Netsky, Mydoom, Doomjuice and Bagle have all been significant. Mydoom.A started the month off by launching a Distributed Denial of Service (DDoS) attack on The SCO Group's website. Followed by subsequent variants of the virus which attacked the websites of both Microsoft and the Recording Industry Association of America. Mydoom installed a backdoor which is now

exploited by Doomjuice. Bagle variants are being produced as fast as anti-virus vendors are distributing definition files. One anti-virus vendor is quoted as saying "It appeared the writer was monitoring the anti-virus vendors and, when detection was added, he changed the worm." As of this newsletter, Bagle.K is the latest variant. Many viruses will be halted if executable e-mail attachments are stripped.

However, a new trend to bypass anti-virus scanning is compressing the executable and password protecting is compressed file. This evasion technique is utilised by the later Bagle variants.

Microsoft has produced a Windows Security Update CD containing critical security updates for; Windows XP, Me, 2000, 98, and 98 SE through to October 2003. Click [here](#) to order your copy.

IN THIS ISSUE:

Bagles on the Menu	1
Mydoom & Gloom	1
Single Sign-on	2
Recent Significant Alerts & Advisories	3
Virus Activity	3
Port Scan Activity	4

MYDOOM & GLOOM

Mydoom.A is a mass-mailing worm that spreads via e-mail and through the peer-to-peer (P2P) file sharing program KaZaA. Mydoom.A's primary purpose was to launch a DDoS attack against the SCO Group's website. The SCO Group is an organization that claims to own the rights to the UNIX operating system. Mydoom.A was first discovered on 25 January 2004, and has surpassed Sobig.F as the fastest spreading worm ever.

called Shimgapi.dll which created a backdoor on the infected PC that can allow an attacker to gain access to the computer and change or delete files.

- Extracted addresses from the infected machines and targeted files with the following extensions: .wab, .adb, .tbb, .dbx, .asp, .php, .sht, .htm, .txt. It would then use its own SMTP engine to e-mail itself to these addresses.

information leading to the conviction of the author of the Mydoom worm. Speculation exists that members of the Linux community may have planned the DDoS attack against SCO. SCO has been in ill repute with some members of the Linux community for claiming that portions of the open-source operating system fall under the company's copyrights.

Mydoom.A's DDoS payload is now complete, but the vast network of machines that are infected with Mydoom's backdoor component are still open to compromise. It is important that computer users keep their anti-virus programmes up to date by downloading the latest anti-virus signatures. Since the discovery of Mydoom.A, several variants of the worm have been detected.

Mydoom.A Overview

- Arrives as an attachment via e-mail or by copying itself to any available shared directory used by KaZaA.
- Programmed to launch a DDoS attack on the www.sco.com web site, starting on 1 February and ending 12 February 2004.
- Installed a component

On 1 February, the DDoS attack commenced from thousands of computers worldwide and resulted in SCO's website becoming unavailable. Shortly after, SCO responded by taking their domain name out of the DNS and began using www.thescogroup.com as an alternate site. SCO has offered a US \$250,000 reward for

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

SINGLE SIGN-ON

"Effective access control mechanisms can lessen the risk of unauthorised access to information and systems"¹.

"Effective access control mechanisms can lessen the risk of unauthorised access to information and systems".

There are many aspects to this statement; two of which being identity management and access control.

One of the key components to effective access control is a Single Sign-on (SSO) implementation.

SSO is the ability to sign onto a site only once and obtain access to one or more applications in a single domain or across multiple domains.

If your organisation is considering a SSO solution or you are interested in the components comprising a SSO solution, grab a cup of coffee and fire up your browser as this article will provide links to SSO articles and reports that will:

1. Give an overview of SSO.
2. Look at some specific SSO technologies.
3. Describe some current developments in identity management and access control.

Overview of SSO

Two recent papers give an excellent overview of the topic. The first, [Evaluating Enterprise Single Sign-on](#), by Mick Smith, CTO, Protocol Development Systems, is a nontechnical guide in which the author describes what SSO is and what it is not. He provides a brief glossary of some SSO jargon to get you started and gets you thinking about some pertinent questions. An example of these are:

- Does your organisation need SSO?
- What does it cost?

- How do I compare SSO systems?

Following on from this is a white paper from BNX Systems, [Enterprise Single Sign-on: Balancing Security & Productivity](#). This article looks at SSO issues in a bit more depth. It also provides a checklist, which differentiates between core and advanced SSO requirements. The main chapters of the paper focus on:

- Background: The goals of Enterprise Single Sign-on.
- SSO Architectures: From Consumer to Enterprise.
- Integration Approaches: SSO Technology Models.
- SSO & Security.
- Total Cost of Ownership.

Another couple of papers offer other useful references that may fill any holes or lead you down other paths:

- [Introduction to Single Sign-on](#), from the Open Group.
- [The New Face of Single Sign-on](#), by Philip Carden.

Specific SSO Technologies

This list is by no means exhaustive and some of these links are included as they also provide good overviews of SSO and related issues:

- [Microsoft Identity and Access Management Solution](#): comprises two guides, [Planning and Designing an Identity & Access Management Solution](#) and [Implementing an Identity & Access Management Solution](#). Together these papers provide the information and tools to plan, design and

implement an identity and access management solution.

- Also relevant to the Microsoft world is [Single Sign-on for Windows Networks](#), which describes SSO within Windows 2000 Domains and Heterogeneous Networks.
- IBM has also recently published a paper, [Simplify Enterprise Java Authentication with SSO](#), by Faheem Khan. This paper describes the process for implementing SSO on the Java platform.
- [Single Sign-on for Your Web Applications with Apache and Kerberos](#), by Jason Garman. This article provides an update to his book, [Kerberos: The Definitive Guide](#), which describes the process to enable Apache-based web servers to allow for transparent domain authentication through Active Directory.
- Enterprise Management Associates have produced a white paper, [Citrix Metaframe Password Manager: A Technology Profile and ROI Analysis](#), which not only focuses on this Citrix product but also provides some very useful data regarding SSO issues.
- Further reports include: [Enforcing Security and Improving Efficiency with user Management and Provisioning](#), from Abridgean, [Security Packet-level, Identity-based Network](#), from Trusted Network Technologies, and,

(Continued on last page)

RECENT SIGNIFICANT ALERTS & ADVISORIES

Date	Description	Reference
01/03/04	Microsoft Internet Explorer Cross Frame Scripting Restriction Bypass	iDefense
01/03/04	WinZip MIME Parsing Buffer Overflow Vulnerability	iDefense
01/03/04	Security Vulnerability Involving the passwd(1) Command	Sun
01/03/04	Vulnerability in SMB Parsing in BlackIce and RealSecure	ISS
26/02/04	Malicious Software Report - W32/Netsky.c@MM	UNIRAS
23/02/04	Security Vulnerabilities in Oracle9i Application and Database Servers	Oracle
17/02/04	Check Point bulletin update	Check Point
16/02/04	Multiple Vulnerabilities in Microsoft ASN.1 Library	US-CERT
11/02/04	Samba 3.0.2 Available for Download	Samba
11/02/04	ASN.1 Vulnerability Could Allow Code Execution	Microsoft
03/02/04	Cumulative Security Update for Internet Explorer	Microsoft

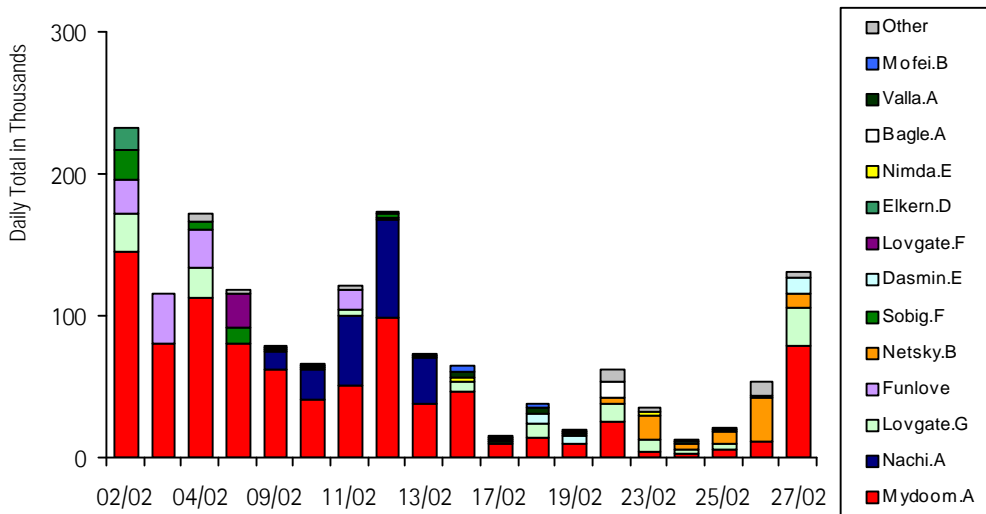
Scanning for TCP port 3127 and TCP port 3128 is new for February.

New Zealand Port Scan Activity page 4

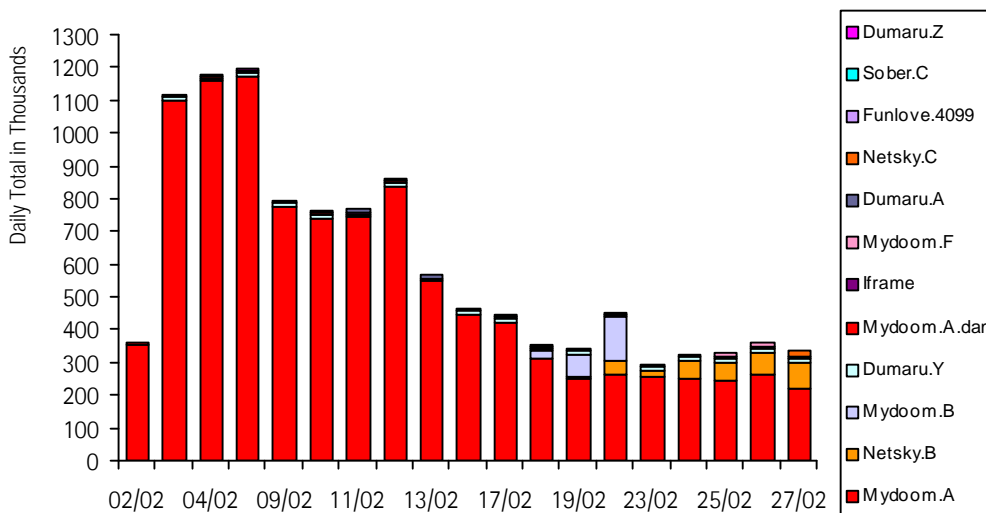
Please refer to the CCIP website for a complete list of alerts & advisories.

VIRUS ACTIVITY

Daily top 5 viruses captured worldwide by TrendMicro for February



Daily top 5 viruses captured worldwide by RAV for February



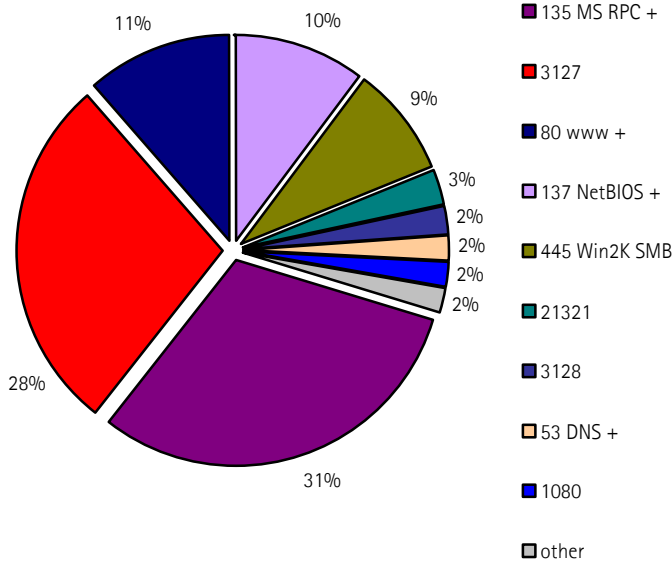
As many of the issues raised by SSO continue to be addressed for access to 'internal' systems, security in the provision of web services tends to dominate current thinking.

Single Sign-on page 4



NEW ZEALAND PORT SCAN ACTIVITY

New Zealand port scanning activity by port number for February.



TCP/UDP ports 135, 137 and 445 continue to appear in the daily top five scanned ports. However, scanning for TCP ports 3127 and 3128 is new for February. The recent Mydoom variants listen on port 3127, or 3128 if 3127 is bound. Analysis would suggest this scanning activity is most likely the Doomjuice worm variants scanning for the Mydoom backdoor, which these worms attempt to disable by deleting files the worm assumes are related to Mydoom.A. For more information see Incidents.org.

SINGLE SIGN-ON (cont.)

(Continued from page 2)

[Managing e-Business Security](#), from Computer Associates.

Some Current Developments in SSO

As many of the issues raised by SSO continue to be addressed for access to 'internal' systems, security in the provision of web services tends to dominate current thinking. Identity & Access Management and Federated Identity Management, which securely link users and applications across business boundaries, are two terms currently in vogue, especially in the provision of Web Services. The World Wide Web Consortium is continually assessing new proposals and has recently published a proposed [Web Services Architecture](#), which "identifies the functional components and defines the relationships among those components to effect the

desired properties of the overall architecture". The Organisation for the Advancement of Structure Information Standards (OASIS) announced the release of the Security Assertion Markup Language (SAML) in September last year. At the recent RSA Conference in San Francisco, eleven vendors, including Sun and HP, joined with the United States General Service Administration (GSA) to show interoperability of SAML and authorisation information.

If you are keen to keep up with latest developments, listen in to a webcast, [Federated Identity Management - It&AM's Next Frontier](#), sponsored by RSA Security, which is scheduled to be broadcast on 10 March 2004.

Meanwhile, a group including Microsoft and IBM continue to develop the WS-

Federation specification which "introduces an identity provider as a class of security token service. As such, it uses the mechanisms of WS-Trust and WS-Federation to create and broker trust within and across federations. Also, mechanisms are defined for single sign-in and sign-out, sharing of attributes based on authorization and privacy policies, and integrated processing of pseudonyms (aliases used at different sites/federations)".

Finally the [Liberty Alliance Project](#) also continues to develop their standards for federated network identity.

¹ [The Standard of Good Practice for Information Security](#), Information Security Forum, 2003

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

E-mail: info@ccip.govt.nz
 Web: www.ccip.govt.nz

PO Box 12-209
 Wellington, New Zealand