



# NEWSLETTER

CENTRE for  
CRITICAL INFRASTRUCTURE  
PROTECTION

Volume 2, Issue 7

October 2003

## THE MONTH IN REVIEW

Administrators were kept busy in September patching a variety of critical vulnerabilities in common Microsoft and UNIX packages - and dealing with the effects of the Swen.A, Sobig.F, Blaster and Nachi worms and viruses. The main discussion article for this month is on the SoBig family of viruses, one of which was the most

prevalent virus for the month of September. Guidelines are also included for reducing the spread of malware.

The Crimes Amendment Act 2003 came into effect today. This act defines specific computer related crimes in New Zealand for the first time. Computer crimes had previously been prosecuted

on such charges as fraud. Now damaging or interfering with computer systems are crimes in their own right, as is accessing a computer system without authorisation. For further information on the Act, refer to CCIP Newsletter Volume 2 Issue 5 issued in August this year.

## SOBIG - PURPOSE AND MOTIVATION

In January 2003, computer users began receiving e-mails purportedly from the e-mail address [big@boss.com](mailto:big@boss.com). These e-mails carried the original Sobig virus, Sobig.A. Eight months later, five variants have emerged. The latest incarnation, Sobig.F, has been developed and refined to become the world's most rapidly spreading e-mail virus to date. The evolution of new features in each new variant, and the inclusion of an expiry date for the spreading routine present in all but Sobig.A, indicate that the author(s) have been developing Sobig for some larger goal. At its peak, Sobig.F was present in an average of one in every 17 e-mails processed by MessageLabs (a managed e-mail service provider), and caused global e-mail traffic to increase by 25 percent.

Sobig.F was first detected on 18 August, originating in the US. The FBI traced it to an Internet message board,

where it had been embedded inside a pornographic image posted to several newsgroups. A stolen credit card was used to open an account from which the image was posted. The "image" was actually an executable file. Computer users who downloaded it inadvertently infected their machines, which allowed Sobig.F to propagate.

The prime objective of Sobig.F appears to have been to establish an anonymous network of proxy servers. The network could be used to send millions of spam e-mails or conduct Denial of Service (DoS) attacks. With around 70 percent of spam distributed through open mail proxies, and the recent number of DDoS attacks against real-time server Blackhole Lists (RBLs), there seems to be a link between the spam community and the Sobig author(s). The FBI has noted this connection

and according to FBI spokesperson Paul Bresson, the FBI along with the US Department of Homeland Security are "continuing to aggressively investigate [the Sobig virus]".

Sobig.F's expiry date has now passed, but the virus' characteristics are worthy of more discussion. Sobig.F would scan a victim's hard drive to collect e-mail addresses found in text and HTML files. It would then send copies of itself, using a built-in multithreaded SMTP engine, to the e-mail addresses that it had found. The Sobig family (from Sobig.C) also spoofed the "from" address to create the impression that the e-mails were being sent from a trusted address. They also used a variety of subject headings and attachment names, e.g., Re: "Movies",

*(Continued on page 2)*

i RBLs help counter Spam by listing IP addresses of open proxies, enabling them to be blocked.

## IN THIS ISSUE:

<i>Sobig - Purpose and Motivation</i>	1
<i>Fending Off Malware</i>	3
<i>Virus Activity</i>	3
<i>New Zealand Port Scan Activity</i>	4
<i>September E-mail Alerts Issued by CCIP</i>	4

Communication regarding this newsletter should be addressed to: [newsletter@ccip.govt.nz](mailto: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](mailto:info@ccip.govt.nz)  
Web: [www.ccip.govt.nz](http://www.ccip.govt.nz)

PO Box 12-209  
Wellington, New Zealand

## SOBIG - PURPOSE AND MOTIVATION (cont.)

*(Continued from page 1)*

Re: "Document", etc. All recent Sobig variants have used these in an attempt to coax users into opening the attachments. Recipients who believed that the e-mails were sent from a trusted source were more likely to open the infected attachments. All Microsoft Windows operating systems have been vulnerable to Sobig infections.

Sobig.F, like most of its predecessors, had a three-stage life cycle:

1. The first stage involved the seeding and spreading of the virus via e-mail and open network shares. The infection routine was programmed to spread until the completion of stage two.
2. The second stage was to install a backdoor Trojan horse program via a download routine, which first appeared in Sobig.C, from one of 20 IP addresses encrypted in the virus' code. The download was due to occur on Friday 22 August 2003.
3. In the third stage Sobig.F would try to download and install a proxy server on to the infected systems.

In the recent outbreak, Sobig.F failed to achieve stage two as the IP addresses were decrypted by anti-virus researchers and shut down before the virus' download routine was set to activate. The five-day period between the initial propagation and Trojan installation may be reduced

in future variants. The effect of shutting down the 20 IP addresses prolonged the infection stage which appeared to allow the virus to continue propagating. MessageLabs were still recording a substantial number of newly infected computers (over 100,000 per day) up to 10 September, Sobig.F's expiry date.

Various methods of avoiding detection from anti-virus software and mail filtering gateways have been seen in the different variants. For example, the use of compressed or "zipped" attachments used by Sobig.E was quite effective at bypassing gateway mail filters. The virus contained a coding error which corrupted the .zip attachment in some cases, limiting its potential. Sobig.F used polymorphism, or changing the "look" of the code, in an attempt to thwart anti-virus software. In its current form, most anti-virus software works in a reactive context and is only as good as the latest virus signatures. They cannot detect viruses for which they do not have a signature, allowing viruses to infect and damage systems until a new signature becomes available. The recent virus outbreaks have spread at a much higher rate than the distribution and installation of anti-virus signatures. Signature based virus detection is effective in detecting viruses that it knows. Heuristics, which are essentially a set of loose rules and probabilities, are capable of detecting suspect code without a specific signature. This is currently a hot topic in anti-virus

research.

A large number of e-mail gateways are configured to inform "infected" senders of their infection and to "bounce" the e-mail back to the "from" address. Increasingly, viruses are spoofing their "from" addresses, and the bounced e-mail thereby amplifies the amount of e-mail sent during outbreaks.

Each new variant has been more dangerous than its predecessors, and the number of Sobig variants indicate that the virus writers may have some larger goal in mind. The LURHO group have undertaken extensive research of the Sobig variants and their findings. This report, "Analysis of Sobig", is available from the [LURHO website](#). To give some indication of the potential of this distributed open proxy network, the administrators of the somewhere.com domain (a domain name used in many text files and documents as example e-mail addresses) received nine million e-mails addressed to 19,000 nonexistent addresses from 200,000 individual IP addresses.

Sobig.F never reached stage two of its life-cycle. New variants could build on the lessons learnt from Sobig.F and result in greater impact. A recent posting to the Bugtraq mail list posed the following questions: "What if Sobig.F had spread for just six hours and then stopped? How many more people would never realize they were infected?"

*This month, ports 1296 and 31819 have also appeared in the top 10. Scanning activity on these two ports was isolated to a few days and only reported in New Zealand.*

New Zealand Port Scan Activity  
page 4

*With malware like Mimail, Nachi, Swen, Blaster and Sobig variants spreading at ever increasing speed, how can you protect your users and systems?*

Fending off Malware  
pages 3 & 4

## FENDING OFF MALWARE

With malware like Mimail, Nachi, Swen, Blaster and the Sobig variants spreading at ever-increasing speed, how can you protect your users and systems?

The following list covers some basic safety measures to minimise the risks your organisation faces from malware.

### Computer User Issues

- Ensure all passwords follow password best

practices, including those on routers, servers, databases etc.

- Treat any e-mail received with care and think twice before viewing attachments.
- Consider whether active content is required in your browser or e-mail applications and disable if not required.
- Use computer protection software, e.g., anti-virus software, personal firewall.
- Operate your computers

in accordance with your organisational policy.

### Infrastructure Issues

Protect and prepare:

- Establish acceptable use policies and incident handling processes.
- Consider architecture issues, e.g., disable or remove unneeded protocols, services, file/printer shares, and applications.
- Disable or remove

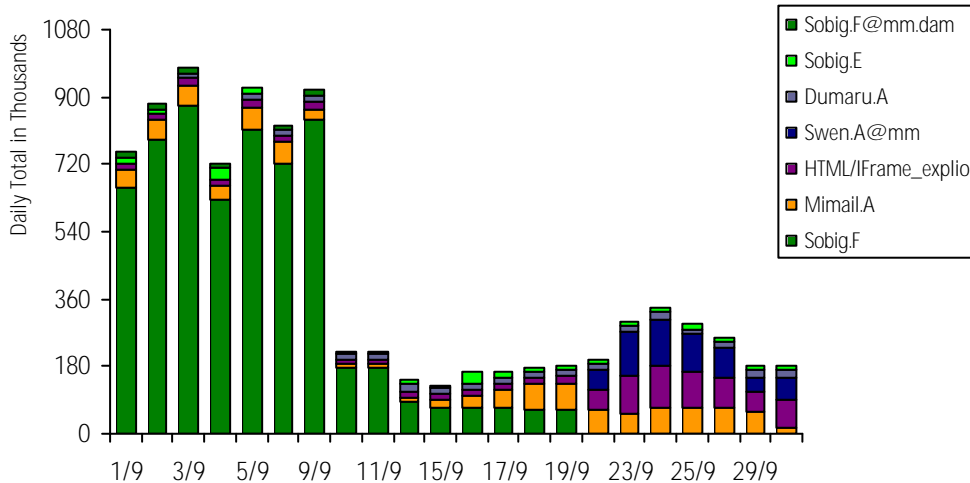
*Each new [Sobig] variant has been more dangerous than its predecessors, and the number of Sobig variants indicate that the virus writers may have some larger goal in mind.*

Sobig - Purpose And Motivation pages 1 & 2

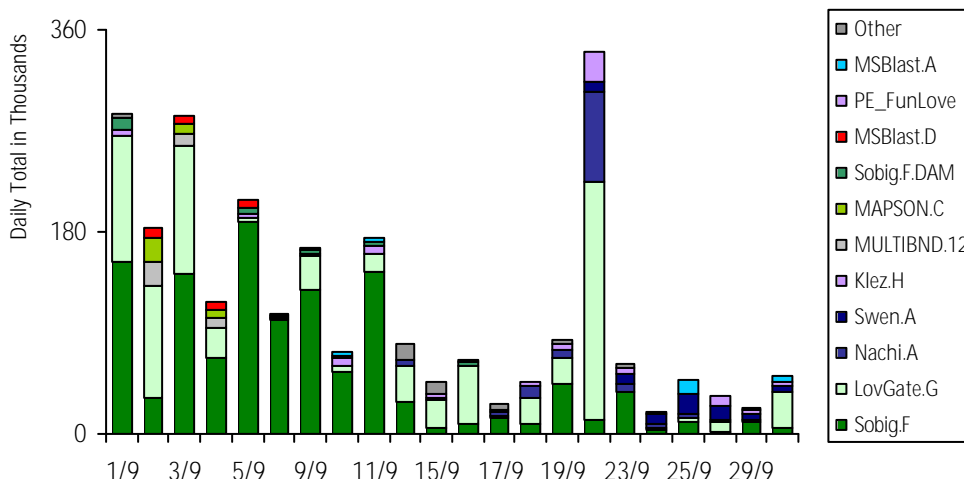
(Continued on page 4)

## VIRUS ACTIVITY

Top 5 viruses captured worldwide by RAV



Top 5 viruses captured worldwide by TrendMicro



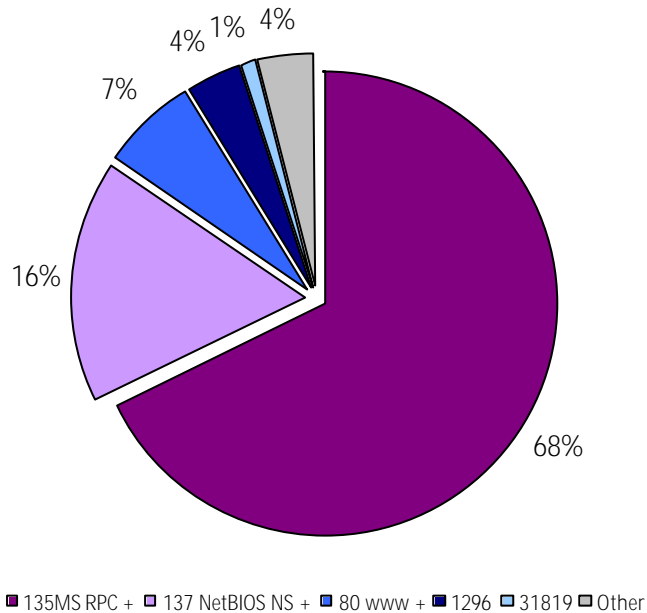
*Swen.A arrives as what appears to be a patch from Microsoft. Since Swen.A is being captured in significant numbers, users should be aware that Microsoft does not send patches via e-mail.*

Virus Activity



## NEW ZEALAND PORT SCAN ACTIVITY

New Zealand port scanning activity by port number from 1 to 30 September.



Ports 135 and 137 remain high in the list of the top 10 scanned ports, accounting for about 85 percent of scanning activity in New Zealand. This is most likely scanning for the Microsoft RPC vulnerabilities as documented in Microsoft security bulletins MS03-026 and MS03-039. This month, ports 1296 and 31819 have also appeared in the top 10. Scanning activity on these two ports was isolated to a few days and only reported in New Zealand.

For more information see [incidents.org](http://incidents.org).

## RECENT SIGNIFICANT ALERTS & ADVISORIES

Reference	Description	Date
Sun	Security Issue Involving the Solaris sadmin Daemon	23/9
CERT	Buffer Overflow in Sendmail	19/9
CCIP	Exploit Code Available for MS03-039 RPC Vulnerability	17/9

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

## FENDING OFF MALWARE (cont.)

(Continued from page 3)

- unused accounts and rename 'administrator' accounts.
- Filter ports at ISP and gateways, internally, and on a per host basis as appropriate e.g., use personal firewalls.
- Install, use and maintain anti-virus software.
- Keep software, patches and service packs/hot fixes up to date.

### Detect:

- Ensure detected viruses are quarantined and users alerted.
- Monitor traffic flows.
- Utilise system integrity checking software.
- Subscribe to alert services.

### React:

- Follow a prepared incident handling process.
- Filter affected port(s).

- Disable affected services (short or long term).
- Patch the affected software, follow vendors' mitigation recommendations.
- Inform the CCIP.
- Trace the instigator and prosecute where applicable.

CCIP Incident Reporting forms are available on the [CCIP website](http://www.ccip.govt.nz).

### SEPTEMBER E-MAIL ALERTS ISSUED BY CCIP:

- 23/9 Remote Root Exploitation of Default Solaris sadmind Settings
- 11/9 Buffer Overflow in Microsoft RPCSS Service Could Allow Code Execution
- 04/9 Microsoft Visual Basic for Applications Could Allow Arbitrary Code Execution

## 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](mailto:info@ccip.govt.nz)  
 Web: [www.ccip.govt.nz](http://www.ccip.govt.nz)

PO Box 12-209  
 Wellington, New Zealand