



MICROSOFT XP SERVICE PACK 2

Microsoft has released a draft document, which contains a description of the new security components in the upcoming Windows XP Service Pack 2 (SP2). The document focuses on two of the four security technologies aimed at improving XP's ability to withstand malicious attacks from viruses and worms.

1. Network protection

This consists of a number of enhancements including:

- Turning on the Internet Connection Firewall (ICF) in default installations of SP2.
- Closing ports except when they are in use.
- Improving the user interface for ICF configuration.
- Improving application

compatibility when ICF is on.

- Enhancing enterprise administration of ICF through group policy.

2. Memory protection

To help protect against buffer overruns, core Windows components are being recompiled with the most recent compilers. Support is also being included for hardware-enforced "no execute" (or NX) on microprocessors that contain the feature, including the AMD K9 and Intel Itanium. This would make it virtually impossible to execute code which was injected via a buffer overrun attack on a data page.

The two additional lower-profile security features

included in SP2 are:

- Improved default settings and attachment controls for Outlook Express and Windows Messenger.
- Internet Explorer will contain enhancements that include locking down the local machine zone to prevent the running of malicious scripts and harmful web downloads. There are also improvements to user controls and interfaces to protect against malicious ActiveX controls and software.

Full details of the new features are available in the original draft document on [the Microsoft website](#).

IN THIS ISSUE:

Microsoft XP SP2	1
Are Laptops Com- promising Your Security	1
Mass Web Page Defacements	3
Significant Alerts & Advisories	3
Virus Activity	3
New Zealand Port Scan Activity	4

ARE LAPTOPS COMPROMISING YOUR SECURITY?

The use of laptop computers provides many benefits to both organisations and their employees. Laptop portability makes them easy to carry between home and office, allowing employees to work from home or when travelling. However, laptop computers present significant additional risks to an organisation when compared with desktop computers.

This article will identify some of these risks and provide options for mitigating them.

The following three aspects, while not specific to laptops,

are fundamental to Information Technology (IT) security:

1. People

Staff that use mobile technologies, such as laptops and Portable Digital Assistants (PDAs), must be trained and aware of their responsibilities regarding the use of these devices. Staff should also know who is responsible for the different aspects of these devices, for example, the hardware, the software and the Intellectual Property (IP).

2. Process

A process for the configuration of devices by

IT staff and the maintenance of an inventory of these devices must be established. This process must be governed by policy, and understood by everyone in the organisation.

3. Technology

When mobile devices are outside the perimeter of the organisation, they are less protected - both physically (e.g. theft) and logically (e.g. connections to the internet from various points). Consequently the risks to which these devices are exposed are different to those of desktop computers. While the above three

(Continued on page 2)

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

ARE LAPTOPS COMPROMISING YOUR SECURITY? (cont.)

(Continued from page 1)

aspects relate to IT security in general, the following risks are associated with laptops specifically.

Theft

Because of their portable nature, laptops are particularly vulnerable to theft. As mobile hardware becomes smaller and more portable, the exposure to theft increases. Sometimes laptops are stolen by an organised crime ring (typically as theft-to-order or to obtain sensitive information). More commonly, laptops are stolen by opportunistic thieves - the motivation for the theft usually being to resell them and make a quick profit. The 2003 Australian Computer Crime and Security Survey found that 53 percent of the respondents had detected laptop theft with an average loss value, including IP and staff time, of approximately AUD\$ 27,000 per laptop.

Theft prevention

There are a number of countermeasures the laptop holder can take to reduce the likelihood of theft. These include:

Avoid leaving your laptop exposed:

- Never leave a laptop in open view or overnight in an unattended vehicle - take it with you.
- Never leave your laptop unattended in a public place, particularly at airports and hotels.
- Avoid leaving a laptop in a position that is visible through a ground-floor window.

Prevent access to the laptop:

- When working in an

office that may allow public access, consider either placing the laptop in a locked cabinet or locking your office door when you leave. The use of an anti-theft device such as a cable lock is recommended. However, this is only a deterrent to an opportunistic thief, and may not stop a professional.

Minimise the consequences of theft

Despite taking all reasonable precautions to prevent the theft of your laptop, it may still be stolen. There are a number of actions you can take to lessen the impact of the theft and increase the chances of your laptop being recovered.

Record laptop details:

- Make sure all laptop details are recorded for future reference (e.g. make, model serial number). This information will be needed by the police and insurance companies in the event of theft.
- Consider fitting tamper resistant tags to your laptop, the use of etching or ultraviolet markings, or the use of tracking software. This software can help track down the stolen laptop whenever it is connected to the Internet.

Take regular backups:

- Take regular backups of data stored on the laptop and store them in a safe place.
- Consider the use of removable USB drives or similar devices for storing information. This will make it possible to take the information with you when carrying a laptop would be inconvenient.

Consider using a BIOS password:

- Consider the use of a BIOS password - this may prevent thieves from accessing your data, particularly if the procedure for resetting the BIOS password requires the laptop to be sent back to the manufacturer.

Encrypt when necessary:

- To protect sensitive information such as research information and IP, consider encrypting the data on the laptop. If a thief does steal your laptop then it will be harder for them to read the information stored on it.

Disable wireless connectivity options:

- It may be possible for someone to connect to your laptop via wireless methods (e.g. Bluetooth, infrared, 802.11) and access your data. Consider disabling wireless connectivity options if they are not required.

Infection of the corporate network

The other significant risk associated with laptops is their ability to be used as a vector to infect "protected" networks.

CCIP is aware of at least two incidents within New Zealand's Critical Infrastructure, where a laptop was taken away from the office and became infected with malicious code. In each incident, the corporate networks were subsequently infected by the malicious code when the laptop was reconnected.

Use anti-virus and firewall software:

- To mitigate the effects

(Continued on last page)

The other significant risk associated with laptops is their ability to be used as a vector to infect "protected" networks.

Are Laptops Compromising Your Security?
page 1

Default operating system installations are often insecure.

Are Laptops Compromising Your Security?
page 1

MASS WEB PAGE DEFACEMENTS

A Brazilian hacker group has been implicated in carrying out two mass web page defacements of New Zealand websites in the last two days. In the first defacement, there were 189 NZ sites included in a worldwide total of around

750 sites. The affected ISP, Quik International, is based in Costa Mesa, California and are running Apache on AIX servers. The second defacement affected sites, hosted by a New Zealand ISP, running Apache on Linux.

To date the group has claimed responsibility for over 15,000 attacks, of which around 90 percent are mass web page defacements.

Further information is available from [Zone-H](#).

53 percent of the respondents had detected laptop theft with an average loss value, including IP and staff time, of approximately AUD\$ 27,000 per laptop.

Are Laptops Compromising Your Security?
page 1

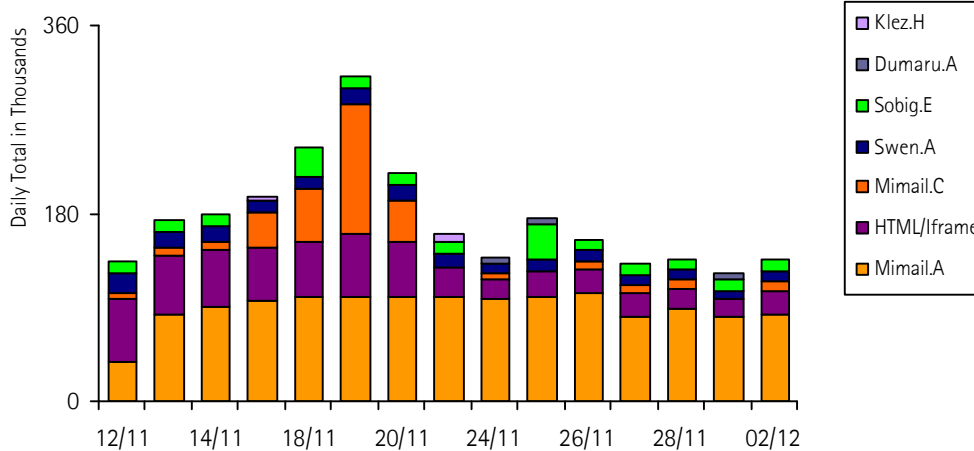
RECENT SIGNIFICANT ALERTS & ADVISORIES

Reference	Description	Date
AusCERT	rsync Security Advisory	05/12/03
CERT	CERT/CC Summary CS-2003-04	27/11/03

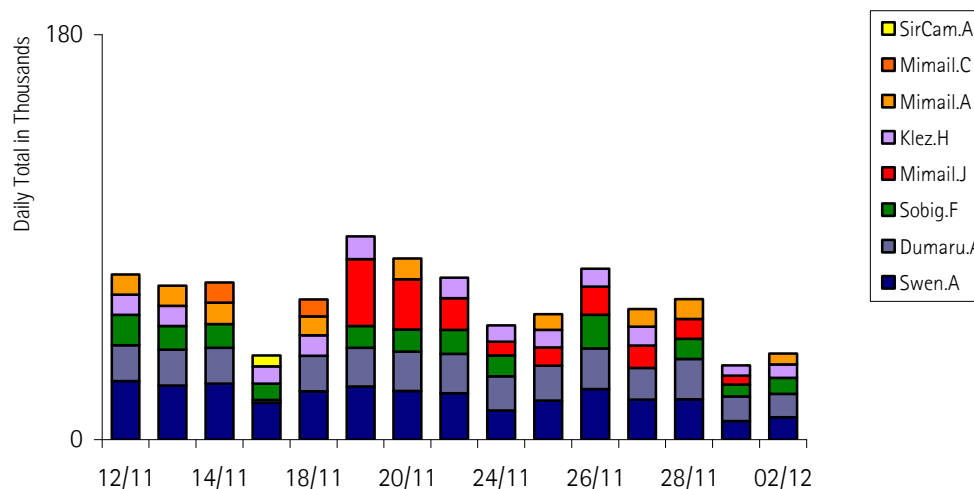
Please refer to the CCIP website for a more complete list of alerts and advisories.

VIRUS ACTIVITY

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



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



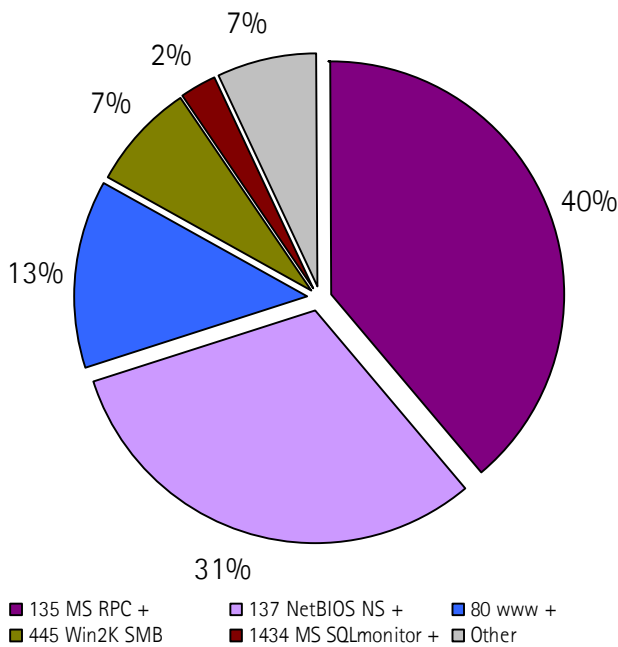
To date the group has claimed responsibility for over 15,000 attacks.

Mass Web Page Defacements
page 3



NEW ZEALAND PORT SCAN ACTIVITY

New Zealand port scanning activity by port number from 12 November to 30 November.



Port 135 continues to lead the New Zealand scanning activity charts for this period but has dropped its share from 59% to 40%. In second place, port 137 has increased its share of activity from 22% to 31%, as has port 80, from 9% to 13%. However total volumes are holding steady, the only noticeable increase being on 18 November when port 135 showed above normal activity. On the worldwide front, top honours are shared by port 135 and port 80, with ports 445 and 137 a discernable but distant third and fourth.

For more information see incidents.org.

ARE LAPTOPS COMPROMISING YOUR SECURITY? (cont.)

(Continued from page 2)

of malicious code, it is recommended that all laptops have up-to-date anti-virus software, including signature files, and personal firewalls installed. This is particularly important if a laptop is being taken out of an organisation and connected to networks where it doesn't have the benefit of the organisation's defences.

Use a VPN and strong authentication:

- Ensure connections to the corporate resources from mobile devices are through a Virtual Private Network (VPN), which creates an encrypted "tunnel" for the communications. This VPN should be implemented with a strong authentication method.

Ensure patches are current:

- Ensure that the operating systems and applications are patched to the latest revision levels. In some cases, code to exploit a newly announced vulnerability is available and being used by attackers within a week of that vulnerability being announced.

Harden operating systems:

- Default operating system installations are often insecure. Ensure that the organisation's IT staff secure and harden all corporate laptops before they are issued to staff. Newer operating systems offer the ability to permit secure logons and provide file level security; use of these features is encouraged.

Educate users:

- Users have a key part to play in laptop security. Educate users about their responsibilities with respect to laptop security and key issues such as the dangers of installing software from non-authenticated sources and what action they should take on discovery of a virus.

Laptop security policy:

- Last but not least is the policy. It is recommended that the issues listed above, including user and organisation responsibilities, are included in a laptop security policy. This should be clear and concise and conveyed to all relevant staff. If there is no policy and staff are not aware of their responsibilities, then it will be harder for an organisation to protect itself from such threats.

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