



# NEWSLETTER

CENTRE for  
CRITICAL INFRASTRUCTURE  
PROTECTION

Volume 4, Issue 4

July 2005

## ADVISORY ON TROJAN EMAIL ATTACKS

Earlier this month the CCIP issued an advisory concerning targeted trojan email attacks. This advisory was based on information contained in a [briefing note](#) published by the United Kingdom's National Infrastructure Security Co-ordination Centre (NISCC). The CCIP recommends careful attention to the NISCC note as the information and advice it contains are equally as important to New Zealand.

Some of the key points from the NISCC note are:

- Trojanised email attacks are targeting Government entities and private companies.
- The attackers' aim appears to be the covert gathering of commercially or economically valuable information.
- Trojans are delivered either in email attachments or through links to a website.
- Once installed on a user machine, trojans may be used to obtain passwords, scan networks, exfiltrate information, and launch further attacks.
- Anti-virus software and firewalls do not give complete protection. Trojans can communicate with the attackers using common ports (for example, HTTP, DNS, and SSL) and can be modified to avoid anti-virus detection.

The briefing note offers a number of techniques to detect and mitigate the threat, but they should be implemented in line with organisational operations and security policies.

## WINDOWS REMOTE DESKTOP SECURITY

Windows Administrators should be aware of the 'Remote Desktop Connection' facility that is available in Windows XP Professional. Its purpose is to let you remotely access your PC.

There have been a number of articles in recent times extolling the benefits it can offer, such as the ability to work from home, getting access to your files while on a business trip, and on how simple it is to set up. Remote access can have benefits in the corporate environment, but there is a lack of awareness on the security compromises this can create.

Take the example of a simple corporate network. Initially, all incoming ports might be blocked, and then a staff member reads about Remote Desktop Connections. This may lead to the network administrator opening port 3389 (refer [Internet Storm Center](#) for current activity on this port) and forwarding it through to the workstation with remote desktop enabled. Just as if

someone had bypassed your physical security, an intruder now has the ability to 'sit in front of this desktop' and attack until they get in. The only chance of detecting an intrusion with this configuration would be by careful monitoring of your security logs.

Fortunately, there are techniques to help you secure your environment. Examples would be restricting by IP address, configuring a list of clients who are allowed to connect, and setting the hours of the day during which they are allowed to do so.

However your organisation first needs to consider the following five questions:

1. Do you have sensitive information on your network?
2. Would it be acceptable for an employee to have all this information outside of your work environment?
3. Do all your employees really need 24 hour access?

4. Would you know if someone tried to breach your security?
5. Can you detect if someone was able to log in as you and copy your files?

Serious consideration must be given to all of these questions and if your organisation can still justify remote access, then consider installing a server dedicated to this function using the following guidelines:

- Install a 'hardened' Windows 2003 Terminal Server
- Only allow users who really need access
- Limit access to required applications
- Use strong password policies
- Use stringent logging and alerting procedures

Remember, using remote desktop in an I-Café will not protect against key loggers, or other monitoring programs. The most important thing to keep in mind is that there are people out there who will take any opportunity to exploit your system.

### CONTENTS

<i>Windows Remote Desktop Security</i>	1
<i>Biometrics – The choices</i>	2
<i>Don't Let the Web Bugs Bite</i>	3
<i>VoIP Security</i>	3
<i>Virus Activity</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  
 Email: [info@ccip.govt.nz](mailto:info@ccip.govt.nz)  
 Web: [www.ccip.govt.nz](http://www.ccip.govt.nz)  
 Mail: P.O. Box 12-209  
 Wellington  
 New Zealand

References and further reading for Windows Remote Desktop Security:

1. [Get Started Using Remote Desktop](#)
2. [Windows Server 2003 Security Guide](#)

References and further reading for Biometrics - The Choices:

1. [International Association for Biometrics](#)
2. [Iris Recognition for Personal Identification](#)
3. [Biometric Technical Assessment](#)
4. [Biometrics & the Courts](#)

## BIOMETRICS – THE CHOICES

*Bio (life) and metric (to measure).*

The world of biometrics is extensive and complex. This article summarises the more common techniques, their pro's and con's, and to what purpose these techniques may be best suited.

Biometrics follow a fundamental premise: if a unique aspect of a being or a unique pattern of behaviour can be identified then a system can be developed to exploit the characteristic(s) as a form of authentication.

Early evidence of biometrics dates to the late 14<sup>th</sup> century, when Portuguese historian and explorer Joao de Barros encountered Chinese merchants stamping childrens inked palm and foot prints on to paper to distinguish the children from one another.

This presaged the most relied upon biometric to date - fingerprinting. But the field has now diversified with a number of approaches. Some key techniques include:

### 1. Iris scanning

An iris scan system examines both irises of an individual's eyes. It then takes advantage of small details in the iris stromal (connective tissue) pattern in order to attempt positive identification of an individual.

Type: Physiological.  
 Pros: Extremely reliable, scans can be done at distances ranging from just a few centimeters and up to a metre away. Non intrusive. Fast acceptance rates.

Cons: Acceptance of a scan relies on healthy eyes. Afflictions of the eyes such as blindness or cataracts can cause a failure to enroll on to the system.

### 2. Retina scanning

Scans the blood vessels at the

back of the eye with a low intensity light.

Type: Physiological.  
 Pros: High accuracy.  
 Cons: Intrusive, afflictions of the eyes such as blindness or cataracts can negatively affect enrollment and authentication, expensive.

### 3. Facial recognition

A method for automatically identifying a person from a digital image. It does so by comparing selected facial features in the live image and a facial database.

Type: Physiological.  
 Pros: Able to detect faces in crowds provided enough of the face is visible.

Cons: Lower reliability rates; privacy issues; enrollment onto a system without person being aware; identification can be hampered by facial reconstructions, facial hair and wearing of accessories.

### 4. Finger scanning

This method scans the indentations and lines that comprise the finger print. These patterns are simplified and stored using software to reduce the data size. This increases the ability to retrieve and match information against a database of known finger scans.

Type: Physiological.  
 Pros: Cleaner than using ink, non-intrusive, fast input matching.  
 Cons: Fingers can be affected by injury or calluses.

### 5. Hand geometry

Hand recognition by matching lines and basic hand geometry.

Type: Physiological.  
 Pros: Hand injuries have little effect on readings (except amputations), quick,

non-intrusive, very accurate.

Cons: Equipment expensive, identical twins can have identical hand geometry.

### 6. Voice recognition

Not to be confused with speech recognition, this technique involves the identification of sounds generated by the throat and nose during speech that are uniquely identifiable.

Type: Behavioural.  
 Pros: Non-intrusive, simple for user.

Cons: Background noise can interfere with identification, easy to fool (sound playback), illness can affect reliability.

### Other techniques

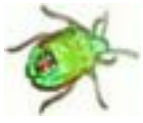
Some examples of other techniques include: facial thermograms, signature recognition, keystroke dynamics, palm vein, knuckle crease and odour recognition. The future of biometrics is likely to include more sophisticated concepts such three dimensional imaging of a person or feature of a person.

### Potential issues

The different types of biometrics clearly have advantages and disadvantages and different vendors are having varying levels of success with their systems. This means that much research has yet to be done in employing such systems and some key issues that need to be addressed are: user security, acceptance, cost, privacy issues, potential religious issues and reliability.

An important security concern is the use of detached body parts to deceive a biometric system. An example was a thief's use of a car owner's severed thumb to fool the vehicle's thumbprint security system. Limb prints can also be faked using gelatin etc.

## DON'T LET THE WEB BUGS BITE



A web bug is a graphic embedded in a web page or HTML-based email message that is designed to collect information about the system browsing the web page or email message. Collected information may be used to profile user surfing habits and/or display relevant web advertising based on profiled information. Web bugs are also used to confirm that a user has read an email, a technique often used by 'spammers', confirming the validity of functional email accounts. Unlike cookies, the presence of web bugs is often invisible to users. Users are therefore unaware that they are being monitored and do not have the opportunity to reject them.

### What do web bugs look like?

Web bugs are often 1-by-1 pixel in size, though any sized graphic could be used, making them virtually invisible to the naked eye. Viewing the source code of a web bugged HTML document will help uncover the web bug and its tracking computer's URL. However, not all invisible graphics are web bugs. Sometimes web pages employ invisible graphics, usually called 'spacer gifs', which are used for page alignment. The difficulty lies

in being able to distinguish the difference between them, but usually web bugs reside on different servers than that of the web page.

Example HTML using a spacer gif:

- ``

Example HTML for a web bug:

- ``

### What information do web bugs collect?

- The computer's IP address that accessed the HTML document containing the web bug.
- The URL of the page that the web bug is located on.
- The URL of the web bug.
- The time the web bug was viewed.
- The type of browser that fetched the web bug.
- A previously set cookie value<sup>1</sup>.

The use of web bugs is often not disclosed on web sites but should be included in a site's privacy policy.

### Dealing with web bugs

A number of commercial and

non-commercial products have been developed to detect, reveal and block web bugs; for example, Bugnosis, Web Washer, Desktop Armor. No current product provides 100% coverage and there are often a number of 'false positives'. One technique is to filter all web content through a proxy, but legitimate content may also get blocked.

Defeating web bugs in HTML email messages can be achieved by forcing all HTML email messages to be displayed as plain text. Turning off the preview pane in certain email clients prevents the email from displaying automatically. This gives users the opportunity to delete unsolicited and potentially web bugged email, by viewing the subject header, without the web bug executing.

The level of security measures users employ is determined by the level of privacy required. Web bugs are just another mechanism used to monitor user behaviour but it is useful to know of their existence.

### Miscellaneous

Alternate names for web bugs include: web beacon, tracking bug, pixel tag, 1-by-1 GIF, invisible GIF and clear gif.

## VOIP SECURITY

Further to the newsletter item on the subject of Voice over IP, published in our April issue, we conclude our coverage of this topic with a look at some of the security issues associated with this emerging technology. Following is an extract from the complete report which is available on our [website](#).

Much has been made of hacking and virus incidents and most Internet users will have experienced some difficulty with

software updates, device conflicts, system incompatibilities and so on. In the world of telephone conversations, however, there is an expectation that there will be no such difficulties and there is a high expectation of privacy. Telephony hackers usually had a high degree of technical skill and had developed specialised tools and techniques. Very few hackers are adept in both data and telephony systems. With the convergence of the technologies, the exposure

has increased and concerns around privacy and security will become more prominent for both users and system owners.

Cybercrime activities also present particular risks. Such activities may include Denial of Service (DoS) attacks for the purposes of extortion, hijacking of services for the purposes of reselling and, in some cases, money laundering, and theft of

*References and further reading for Don't let the Web Bugs Bite:*

1. [Bugnosis](#)
2. [Yahoo! Privacy Center: Web Beacons](#)
3. [Microsoft: Managing Outlook Web Access](#)

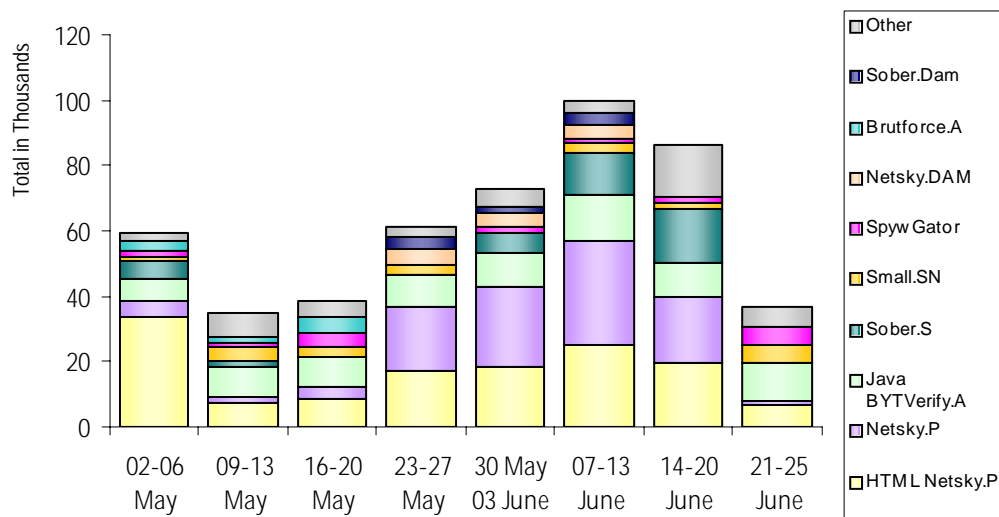
*References and further reading for VoIP Security:*

1. *Security: The threat within is greater than you think*, Marguerite Reardon, Cnet News.com, 12 January 2005, <http://news.zdnet.com/>, accessed 11 February 2005

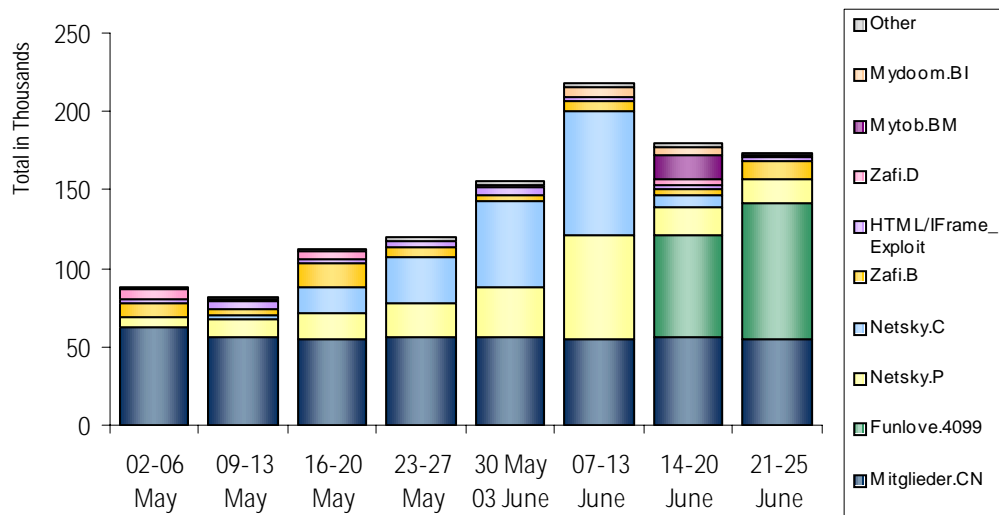
## VIRUS ACTIVITY

The Migleider trojan continues to dominate the RAV statistics this month with almost twice as many reports as the runner up, Funlove.4099. Trailing in third and fourth spot with very similar numbers of reports are Netsky.P and Netsky.C respectively. TrendMicro, on the other hand, have the Netsky variants in their top two positions with Java\_BYTVerify.A following close behind in third place. In general, the number of reports are holding steady which is an encouraging trend for security professionals and network administrators.

**Daily Top Five: viruses captured worldwide by TrendMicro for May and June.**



**Daily Top Five: viruses captured worldwide by RAV for May and June.**



## VOIP SECURITY

*Continued from page 3*  
intellectual property through eavesdropping.

To complicate matters, VoIP traffic requires different treatment to data traffic. For example, you cannot quarantine incoming calls without significantly affecting QoS. Other challenges may include, for

example, call tracing. Operating in a hostile Internet environment, network hygiene and the fundamental principles of well designed and implemented network security controls, policies and technologies are essential to protecting information assets, providing security of service and managing any attack on a VoIP network.

It is also important to protect the systems against insider as well as outsider attacks. While some insider attacks are malicious, most are caused by negligence or error. A recent survey indicated that almost 40 percent of internal security breaches were attributed to poor handling by well-intentioned employees and 30 percent were malicious.

## 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 New Zealand 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 expressed 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

**Email:** [info@ccip.govt.nz](mailto:info@ccip.govt.nz)

**Web:** [www.ccip.govt.nz](http://www.ccip.govt.nz)

**Mail:** P.O. Box 12-209  
Wellington  
New Zealand