



**COMPUTER SECURITY ADVISORY FROM THE INFORMATION SECURITY GROUP
– DEFENCE SIGNALS DIRECTORATE**

Australia's national authority for communications and computer security. Playing a key role in the protection of Australian official communications and information systems.

Targeted Trojan Email Attacks

DSD'S CONCERN

The National Infrastructure Security Co-ordination Centre (NISCC) in the United Kingdom (UK) released a briefing on email-borne electronic attacks against both Government and non-Government agencies on Thursday, 16 June 2005.

DSD has reviewed the NISCC briefing and advises that Australian Government and other organisations consider the recommendations provided in the context of securing their networks from similar electronic attacks.

Key Points:

- A series of Trojanised email attacks are targeting Government and companies.
- The attackers' aim appears to be covert gathering and transmitting of commercially or economically valuable information.
- Trojans are delivered either in email attachments or through links to a website.
- The emails employ social engineering, including use of a spoofed sender address and information relevant to the recipient's job or interests to entice them into opening the documents.
- 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 (e.g. HTTP, DNS, SSL) and can be modified to avoid anti-virus detection.

The briefing document provides detection and protective advice. There is no complete mitigation for computers connected to the Internet.

RECOMMENDATION

Consider the advice provided in NISCC Briefing 08/2005 issued 16 June 2005.



REFERENCE

For more information refer to:

- * The NISCC Briefing 08/2005:
<http://www.niscc.gov.uk/niscc/docs/ttea.pdf>

ISIDRAS REPORTING

As with any other information security incident, reports of an exploitation of this vulnerability must be made under the Information Security Incident Detection Reporting and Analysis Scheme (ISIDRAS).

More information regarding the scheme and copies of the reporting form can be obtained from DSD's web site:

http://www.dsd.gov.au/infosec/assistance_services/incident_reporting.html

Please note: information provided through ISIDRAS remains confidential within DSD. Information is never passed to outside agencies except in aggregate.

FURTHER ASSISTANCE

DSD is available to provide assistance in reviewing an agency's threat and risk assessments or to provide further information on the recommendations contained in this advisory.

You can contact DSD, through the Information Security Group, regarding this advisory or other computer security matters.

CONTACT DETAILS

Postal: Locked Bag 5076
Kingston ACT 2604
Email: incidents@dsd.gov.au
infosechelp@dsd.gov.au
Web: www.dsd.gov.au
Phone: 02 6265-0197
Fax: 02 6265-0328