



**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.

Haxdoor Trojan

DSD'S CONCERN

The Haxdoor Trojan steals personal information (including bank account details and login credentials) and sends the information back to a location in Russia. Whilst this Trojan does not appear to be specifically targeting government agencies, home users of online government services may be at risk.

Background

The Haxdoor Trojan, and its numerous variants, has been around for several months. Older variants are being detected by anti-virus products and successfully removed, however newer variants may not be detected or removed.

The Trojan is a backdoor with an advanced rootkit functionality that cloaks both files and processes. This Trojan may arrive as file **iespr.sys**.

Required Actions

The following actions may assist agencies to ensure integrity of data stored:

- Update anti-virus signatures, even though they may not *currently* detect and remove new variants.
- Implement email content filtering, blocking file **iespr.sys** and the email address **corpse@mailserver.ru**, or other email message going out to Russia.
- Implement host-based Intrusion Detection Systems.

Unclassified

- Look for the following files:

cm.dll
draw32.dll
hm.sys
memlow.sys
vdnt32.sys
vtd_16.exe
wd.sys
pptp16.dll

pptp24.sys
pz.dll
qz.sys
klgcptini.dat (not malicious file)
ms87.dat (not malicious file)
klo5.sys

FURTHER ASSISTANCE

Any agency that has seen the Haxdoor Trojan (any variant) in their corporate network is asked to advise DSD.

Further information on the Trojan can be found at:

- www.symantec.com
- www.sophos.com

CONTACT DETAILS

Postal: Locked Bag 5076
Kingston ACT 2604

Email: incidents@dsd.gov.au

Web: www.dsd.gov.au

Phone: 02 6266-0009

Fax: 02 6265-0328

Unclassified