



# Malicious Software Attacks Targeting Home Users and Businesses

Robert Lowe  
AusCERT



**AusCERT**  
Australian Computer Emergency Response Team

**COMPUTERWORLD**

An IDG  
company

QuickLink



Search

Computerworld



Home

News

Topics

Subscribe

Events

White Papers

Briefings

Webcasts

Bl

## **Cybercrime pays off more than drug trafficking, security expert says**

Proceeds from cybercrime in 2004 topped \$105B, says Valerie McNiven

News Story by Souhail Karam

NOVEMBER 28, 2005 ([REUTERS](#)) - Global

cybercrime generated a higher payback than drug trafficking in 2004 and is set to grow even further as the use of technology expands in developing countries, a security expert said today.

No country is immune from cybercrime, which includes corporate espionage, child pornography, stock manipulation, extortion and piracy, said Valerie McNiven, who advises the U.S. Department of the Treasury on the problem. "Last year was the first year that proceeds from cybercrime were greater than proceeds from the sale of illegal drugs, and that was, I believe, over \$105 billion," McNiven said.

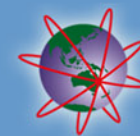
"Cybercrime is moving at such a high speed that law enforcement cannot catch up with it."

# Making cyber-crime pay



**AusCERT**  
Australian Computer Emergency Response Team

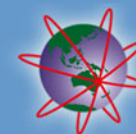
- Botnets
  - Spamming
  - DoS for extortion
  - Adware/spyware/malware installation
  - Hosting phishing, warez...
- trading in online commodities – “shells”, “carding” etc.
- malware distribution
- and the list goes on...



- Built to bypass security counter-measures
  - Disable firewall and AV
- Not detectable by up-to-date AV at release
- Using root-kit features
  - harder to detect and remove



- Malware development approaching commercial software: licensing, forums, support etc...
- Less technical knowledge required to deploy malware

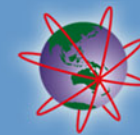


- Commercial Malware generator
- “keylogger”, proxy and more

The screenshot shows a configuration window for the Haxdoor malware. It contains several sections of settings:


- Self destruction:** Includes fields for 'day' and 'month' (both empty), and checkboxes for 'enable' and 'and kill' (both unchecked).
- Server actions:** A list of checkboxes including 'Kill firewalls' (unchecked), 'Block firewalls' (checked), 'Close before send mail' (unchecked), 'keylogger' (unchecked), 'Open ports in offline' (unchecked), 'Proxy server's' (unchecked), 'Send' (unchecked) followed by a field for the number of mails, 'Send key log' (unchecked), and 'Random proxy port's' (unchecked).
- Mail configuration:** Includes fields for 'mail:' (containing 'name@somemail.xx'), 'smtp:' (containing 'somemail.xx'), 'ID:' (containing '0000'), 'port:' (containing '16661'), and 'pass:' (containing 'PASSWORD').
- Advanced options:** Includes a checked checkbox for 'Block firewalls (L2)'.
- Alarm timeout:** A field containing the value '30'.
- Buttons:** A 'save as...' button is located at the bottom right.

# Haxdoor Case study: hooks



**AusCERT**  
Australian Computer Emergency Response Team

- 12 June
  - Over 50 AU web bulletin boards spammed with:

Author	Topic
<u>Jason Y Li</u> 1 Posts	<p>Posted - 12 Jun 2006 : 13:48:17</p> <hr/> <p>Just read: people starting panic withdrawals, some of the accounts were reported closed due to technical reasons, many ATMs are not operating. Does it seem that one of the Australia's greatest goes bankrupt?</p> <p>The full story could be found &lt;a href=http://www.cnruggiero.com.au/national.php&gt;here&lt;/url&gt;.</p> <p>Well, hope that isn't true... Anyway I'd rather check my balance...</p>
 Australia 14 Posts	<p>Posted - 12 Jun 2006 : 21:17:09</p> <hr/> <p>and this has exactly what to do with toddlers???</p> <p>don't click on the link people...could be a very nasty surprise for your computer there...</p> <p>has this site got any mods??? the link should be deleted just in case!!!</p>



- 15<sup>th</sup> June

- Large spam run using email similar to:

From: "xxx" <xxx@xxx.xxx>

To: <xxx@xxx.org.au>

Subject: National Bank goes bankrupt?!

People starting panic withdrawals, some of the accounts were reported closed due to technical reasons, many ATMs are not operating. Does it seem that one of the Australia's greatest goes bankrupt?

The full story could be found here:

<http://www.saltnlight-e.com/news.php>

Well, hope that isn't true... Anyway You'd rather check your balance...



# Haxdoor case study: infection



**AusCERT**  
Australian Computer Emergency Response Team

- Four domains initially identified
- More identified later
- Plus several other sites behind the scenes.

# Haxdoor case study: detection



**AusCERT**  
Australian Computer Emergency Response Team

- AV detection of Haxdoor:

AntiVir 6.35.0.13 06.14.2006 no virus found

Avast 4.7.844.0 06.13.2006 no virus found

AVG 386 06.14.2006 no virus found

BitDefender 7.2 06.15.2006 no virus found

ClamAV devel-20060426 06.14.2006 no virus found

DrWeb 4.33 06.14.2006 **BackDoor.Haxdoor.294**

eTrust-InoculateIT 23.72.38 06.15.2006 no virus found

eTrust-Vet 12.6.2256 06.14.2006 **Win32/Haxdoor!generic**

Kaspersky 4.0.2.24 06.15.2006 no virus found

McAfee 4784 06.14.2006 no virus found

Microsoft 1.1441 06.15.2006 no virus found

NOD32v2 1.1599 06.14.2006 **a variant of Win32/Haxdoor**

Panda 9.0.0.4 06.14.2006 **Suspicious file**

Sophos 4.06.0 06.14.2006 no virus found

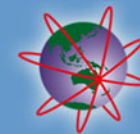
Symantec 8.0 06.15.2006 no virus found

VBA32 3.11.0 06.14.2006 **suspected of Trojan-Downloader.Agent.83**

VirusBuster 4.3.7:9 06.14.2006 no virus found



- **AusCERT's Response:**
  - Issued deregistration requests to registrar
    - Domains held or de-registered
  - Issued cleanup/data retrieval requests to ISPs and webmasters
    - Compromised sites being cleaned
    - Potential for re-compromise
  - Issued Alerts
    - AL-2006.0049, AU-2006.0019, AU-2006.0022,
  - Issued media release
    - Media Release - Response to recent media coverage of the A-311 Death (aka: Haxdoor) trojan



## *The* *Register*®

 Biting the hand that feeds IT

[The Register](#) » [Security](#) » [Spyware](#) »

Original URL: [http://www.theregister.co.uk/2006/06/19/bank\\_details\\_aussies/](http://www.theregister.co.uk/2006/06/19/bank_details_aussies/)

### **1,000 Aussies caught in NAB phishing attack**

By [Lucy Sherriff](#)

Published Monday 19th June 2006 10:45 GMT

A phishing email claiming that The National Australia Bank (NAB) is bankrupt has caught more than 1,000 of the bank's customers in its net.

The email warns the bank's customers that NAB might be bankrupt. It claims the bank's ATMs are not working and that people are starting panic withdrawals. It invites them to click on a link that will provide them with more information.

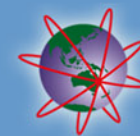
# Haxdoor case study: impact



**AusCERT**  
Australian Computer Emergency Response Team

- 3+ GB of data logs
- March to July 2006
- Over 1000 domains identified
- Information from 15 separate haxdoor variant “runs”
- >70% detection failure rate from 26 AV vendors at time AusCERT found it
- Contained rootkit and AV disabling functions
  - Won't be detected by AV if infected prior to the signature update

# How effective was it?



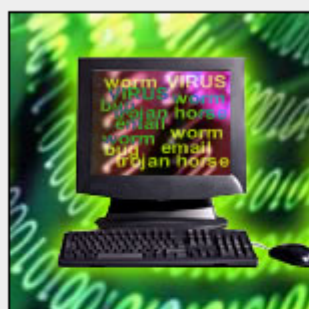
**AusCERT**  
Australian Computer Emergency Response Team

- About 34,000 unique infections from 149 countries

Australia	11,418	34%
Germany	4760	14%
US	3594	11%
Poland	2458	9%
NZ	1774	5%

Australia includes compromise of e-tax data...



[News Home](#)[Top Stories](#)[Just In](#)[World](#)[Australia/Local](#)[Business](#)[Politics](#)[Weather](#)[Sport](#)[Health](#)[Arts](#)[Sci-Tech](#)[Environment](#)[Rural](#)[Indigenous](#)[Opinion](#)[Offbeat](#)[Forums](#)[Services](#)[Help/Site Map](#)**ABC News****Video on Demand****Last Update:** Thursday, August 3, 2006. 4:10pm (AEST) [Print](#) [Email](#)

Trojan attack: A311 Death first hit people filing their tax returns online.

## Trojan infects 10,000 Australian PCs

By Simon Lauder for *The World Today*

A trojan known as A311 Death is estimated to have infected 10,000 computers in Australia.

The Australian Computer Emergency Response Team is investigating the program, which is believed to have come from Russia.

Chris Horsley, a AusCERT security analyst, says thousands of Australian PCs are infected, and the trojan is spreading fast.

"Our current estimate is around 10,000 but there's more infections worldwide," he said.

"They seem to be constantly feeding new runs of this particular trojan by a lot of different vectors."

The Australian Tax Office says the A311 Death trojan has been used to detect the tax file numbers of 200 people who have lodged their tax returns online.

Those people have all been offered new tax file numbers, and a spokeswoman says lodging a tax return online is still considered safe if users have the latest virus detection software.

But Mr Horsley says most anti-virus programs will not detect the trojan.

"Sometimes not. One of the methods that the trojan uses is disabling antivirus and also changing the operating system to hide its presence from the programs running on it," he said.

"So that's made detection in this particular case quite difficult."

But Peter Cassidy, from the US based Anti-Phishing Working Group, says virus protection is still a good idea.

"It offers probably as much protection as a seatbelt will," he said.



- On average each infected computer had about 120 web log transactions captured, including SSL sessions – form data and protected storage data (passwords)
- Average infection time 10 days
  - Minimum < 24 hours
  - Maximum 52 days





- Run up to date software
- Run as an unprivileged user (not Administrator)
- Be careful when opening attachments or clicking links in email, forums or chat
- Spam filtering
- Use security software
  - Personal Firewall
  - Anti-virus
  - Anti-spyware

# Questions



**AusCERT**  
Australian Computer Emergency Response Team

?