



ITWEB JOBS

- [Register](#)
- [Post your CV](#)
- [Find your job](#)

BRAINSTORM

- [Subscribe](#)
- [Read online](#)
- [Get 3 trial issues](#)

FREE NEWSLETTERS

- [News Daily](#)
- [News Weekly](#)
- [Other newsletters](#)

ONLINE STORE

- [Special editions](#)
- [Conference DVDs](#)
- [Brainstorm Magazine](#)

RESEARCH

- [IT Directory](#)
- [Salary Survey](#)

SALES KIT

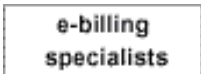
- [Advertising](#)
- [Sponsorships](#)
- [Press Office](#)

[▲ HOME](#)
[→ SALES INFO](#)
[↓ BROUGHT TO YOU BY](#)

[TOP ▲](#)

Copyright (c) 1996 - 2006 ITWeb Limited. All rights reserved.

Would you like to see your news here? Contact us for more details at itnews@itweb.co.za



SEARCH

BUSINESS

- ▶ [ISA in new BEE talks](#)
- ▶ [Business Objects unveils EIM strategy](#)

[more in business...](#)

advertisement

Loading...

FINANCIAL

READ IN THIS STORY:

- ▶ World of Hackercraft
- ▶ School ties
- ▶ Rise of the zero-days
- ▶ Three's a crowd

This week we examine an increase in bots, clever online gaming hackers, poor online policies at top-ranked universities, a rise in zero-day flaws and an update on the latest Microsoft IE flaws.



Bringing you voice solutions that make a difference

Mitel IP Telephony, VOIP, Cynos Unified Communications and professional advice that makes business sense

We offer a free communications consultation.

Click here to learn more.

- ▶ [Trematon eyes unlisted assets](#)
- ▶ [Is BCX's new bidder making mischief?](#)

[more in financial...](#)

COMPUTING

- ▶ [Java to get Linux-friendly](#)
- ▶ [SAP creates multi-tenant facilities for portal](#)

[more in computing...](#)

INTERNET

- ▶ [Film piracy costs Hollywood \\$6.1bn](#)
- ▶ [Zambia rolls out rural network](#)

[more in internet...](#)

ENTERPRISE

- ▶ [Four steps to recovery for insurance sector](#)
- ▶ [Hop on the bus to deliver service-oriented software](#)

[more in enterprise...](#)

NETWORKING

- ▶ [Siemens develops small telephone network](#)
- ▶ [BCX bid shrouded in mystery](#)

[more in networking...](#)

TELECOMS

Security experts at MicroWorld Technologies are drawing attention to recent survey results showing a frightening 47 million computers have been transformed into botnets and zombies, with control sitting with botmasters.

In 2005 the number of bots increased three-fold compared with the previous year, according to MicroWorld, and numbers are steadily increasing in both home and office PCs. "Slave" computers are taken over by hackers to launch, direct and manage fraudulent activities, online crimes and malicious attacks.

World of Hackercraft

Online gamers need to take special precautions. A new variant of the password-stealing Trojan, Trojan-PSW.Win32.WOW.x is targeting World of Warcraft account holders. World of Warcraft is a cyber game played against other online gamers in real time.

The Trojan retrieves a gamer's password, which the hacker uses to transfer the gamer's "goods" into another account. These goods are then converted into liquid currency through the Gaming Currency Exchange Web site.

We, the slaves

"The number of botnets and zombies, controlled by botmasters, has risen to 47 million."

to the vicious designs of identity thieves."

And beware, the Trojan can shut down anti-virus and firewall software.

School ties

Top-ranked US universities are not measuring up in terms of their online security policies, a recent study has shown.



- ▶ [Shortage of Vodacom HSDPA cards](#)
- ▶ [Trematon eyes unlisted assets](#)

[more in telecoms...](#)

CHANNEL

- ▶ [Milestone wins brand leadership award](#)
- ▶ [Rectron offers Gigabyte graphics accelerator](#)

[more in channel...](#)

advertisement

The survey investigated 175 000 Web pages from America's "best colleges". Watchfire, a company specialising in online risk management software, crawled each institution's home page, undergraduate admissions, human resource and athletics sections.

Results revealed a large percentage of schools lacked adequate privacy notice links, used faulty collection practices and had at least one page with an unsecured data collection form.

"It's not that they are trying to hide anything; they just aren't aware they needed a privacy notice," the survey says. "Basically, colleges and universities still enjoy a high level of trust among the public."

Rise of the zero-days

The SANS Institute has recently observed a sharp increase in zero-day flaws, many of them in programs long considered to be safe alternatives to Windows.

For example, an increasing array of zero-day vulnerabilities appeared in Mozilla's Firefox browser and Apple Computer's Mac OS X operating system.

SANS also saw a sizable increase in financially motivated zero-day attacks, as well as an ongoing problem with attacks exploiting Web application flaws.

"We've observed 80 to 90 flaws in Web applications a week," said Rohit Dhamankar, project manager for the SANS top 20 effort. "Immediately after the flaw is disclosed, public exploit code emerges that can compromise back-end data or the Web server quite easily."

According to SANS, the top eight trends in its spring update of the top 20 vulnerabilities list include:

- * Rapid growth in critical Mac OS X flaws, including a zero-day hole
- * A substantial decline in the number of critical flaws in Windows services, offset by flaws in client-side software, including the Windows Meta File (WMF) vulnerability and flaws in Internet Explorer (IE)
- * The continued discovery of multiple zero-day flaws in IE
- * Rapid growth in critical Firefox and Mozilla vulnerabilities
- * A surge in commodity (cheap) zero-day attacks used to infiltrate systems for profit
- * Rapid growth in critical flaws allowing direct access to databases, data warehouses and backup data

- * A continued surge in file-based attacks, especially those using media and image files, Microsoft Excel files, and more
- * A rapid spread, especially among defence and nuclear energy sites, of successful spear-phishing attacks

Although there is a rising trend in non-Microsoft browser software, Microsoft remains the target of industry scrutiny following several high-profile flaws, including the recent WMF and IE createTextRange glitches, SANS concludes.

Three's a crowd

Two more IE flaws have surfaced recently, bringing the number of flaws discovered to three since the 11 April security flaw patches issued by Microsoft.

A Microsoft spokesman confirmed the company has investigated the latest reports and determined the new flaws would be difficult to exploit.

The first problem is a [race condition](#) that appears when security dialogues are displayed and processed, prompting a user to install and execute an ActiveX control.

Attackers can exploit this to manipulate the dialogue box and remotely compromise a vulnerable system by convincing a user to visit a specially crafted Web page. Hackers then install or execute a malicious ActiveX control on the victim's machine.

The second problem is an origin validation error that appears when "mhtml:" url redirections are handled. Attackers can exploit this to read content and data served from another domain in the context of a malicious Web page.

Sources used: The Register, SearchSecurity, MicroWorld Technologies

[SEND TO A FRIEND](#) | [SEND SMS](#) | [PRINT](#) | [POST A COMMENT](#)

ABOUT THE AUTHOR

Ilva Pieterse is an ITWeb contributor.

🔗 [Latest columns from Ilva Pieterse:](#)

[Beating the plague of the PC](#) [28 Apr 2006]


[Biology, technology share battle grounds](#) [21 Apr 2006]

[Gadgets, games lose appeal](#) [13 Apr 2006]

[No honour among thieves](#) [10 Apr 2006]

[Mayday! Malware now child's play](#) [31 Mar 2006]

[More columns from Ilva Pieterse >](#)

MORE NEWS	MOST POPULAR
<ul style="list-style-type: none">▶ Zambia rolls out rural network▶ Is BCX's new bidder making mischief?▶ Users still fall for hoaxes, old viruses	 <ul style="list-style-type: none">▶ Vodacom cuts 3G prices▶ Telkom plans surveillance product▶ MTN makes R33.5bn acquisition

Sponsored links:

- ▶ [Download the Latest Symantec Internet Security Threat Report.](#)
- ▶ [Curious to know how well you understand basic IT security concepts? Click here to find out.](#)
- ▶ [The world runs on data. Critical data runs on Microsoft SQL Server 2005 Microsoft Windows Server System.](#)
- ▶ [ProCurve Identity Driven Manager 2.0 helps create a secure network.](#)
- ▶ [FUTUREX EXHIBITION & CONFERENCE – where ICTE and business connect.](#)


Web
brainstorm
Just Think.

FREE GIFT
when you subscribe

Subscribe to Brainstorm **TODAY** for only R199.95 and get: a **FREE APC Biometric Password Manager** (valued at over R450.00)

Full name:
Company:
Phone:
Postal add:
Area:
Code:
E-mail:
Payment:

*** FINAL MONTH ***
Free Gift



APC
Legendary Reliability™



5 May 2006

[Security](#)

WHO'S YOUR BOTMASTER?

SECURITY ROUNDUP



ILVA PIETERSE