

NEWS SUMMARY

Nation Officially in Recession

The U.S. fell into recession in March 2001, bringing to an end the longest business expansion in its history, the official group of economists who call the nation's highs and lows said.

CEOs Demand IT Results: Poll

A majority of CEOs are now demanding regular reports measuring IT's contribution to business results, according to a survey by California-based consultancy ClarITeam.

VPN Sales Dip

According to a study released this week by Infonetics Research, San Jose, Calif., sales of dedicated VPN hardware and software dipped by 2 percent this quarter over last, but should improve as the year ends. Firewall sales, however, were up slightly.

Life Tips

You cannot depend on your eyes when your imagination is out of focus.

- Mark Twain

OpenAxis News is intended to provide useful information regarding Information Technology to our clients and friends.

The news covers new version releases, hotfix file update, and some IT tips.

Warning: New Virus may spread after Thanksgiving

A revised version of the Badtrans worm from April 2001 is loose on the Internet. The new virus, Badtrans.B loads a password-stealing Trojan horse that can log keystrokes and reveal password and credit card information to malicious users. It uses a vulnerability in Internet Explorer that automatically opens the e-mail attachments when previewed, just like Nimda virus spread in September.

How it works

Badtrans.B arrives as e-mail. It replies to old e-mail, so the subject line is one that someone has already sent you, so you might be inclined to open it. The e-mail message itself is empty. Badtrans.B includes an attached file whose name is created from the following list:

FUN

HUMOR
DOCS
S3MSONG
Sorry_about_yesterday
ME_NUDE
CARD
SETUP
SEARCHURL
YOU_ARE_FAT!
HAMSTER_NEWS_DOC
New_Napster_Site
README
IMAGES
PICS

The attachment is a DOC, MP3, or ZIP file, with a second extension of either SCR or PIF. For example, an attached file might be named Readme.doc.scr.

Users need not open the attached file to infect their machines. Badtrans uses a known vulnerability in Internet Explorer that automatically opens attachments. In this case, the attached file contains Troj.PWS-AV, a password-stealing Trojan horse. Troj.PWS-AV records all keystrokes and the application name where a keystroke

was typed, storing it in encrypted form. The Trojan then connects to a SMTP server to send the log file to a Hotmail e-mail address.

Prevention

Badtrans.B uses a known vulnerability in Outlook Express that is included in Internet Explorer 5.01 and 5.5. Microsoft has released a patch. Users who have not loaded the patch are encouraged to do so or to upgrade to Internet Explorer 6.

Removal

Most antivirus software companies have updated their signature files to include this worm.

*For more information,
Please call
(323) 265-3000
Yuji Ioriya or
Hendry Sondjaja*

Report: Business fails on global security

This article is cited from <http://www.zdnet.com/zdnn/stories/news/0,4586,5099609,00.html>

Multinational corporations are still far off from securing their networks and seem to be focusing on the wrong threats, according to a report expected from Big Five accounting firm KPMG this week.

For the risk assessment

report, KPMG interviewed 500 executives in August and discovered that although 85 percent felt they gave enough attention to protecting their information, nearly four out of 10 thought their company could suffer a serious

breach of security.

The majority believes that the fix is to buy the right technology, but that's plain wrong, Stuart Campbell, partner for KPMG's Risk and Advisory Services practice, said in a statement.

(Continue on the back)

At OpenAxis, we focus on the implementation of IT solutions for small- and medium-sized businesses.

We provide management and computer consulting services by identifying issues, implementing solutions, and managing all your IT needs.

Comprehensive Solution:

Accounting Solution
Operation Solution
Manufacturing Solution
Other Integrated Solution
Customized Solution
E-Commerce Solution

OpenAxis, Inc.

901 Corporate Center Dr. Suite 400
Monterey Park, CA 91754

Phone: (323) 265-3000

Fax: (323) 265-3330

Email: info@openaxis.com

www.openaxis.com



Report: Business fails on global security

(Continued from the front)

"Until more executives regard information security as a strategic business issue, organizations will remain vulnerable," he said. "This issue doesn't begin and end with technology solutions and technology departments."

Rather than buy new software and systems, companies should be looking toward education, training and policy initiatives. Almost 90 percent of the executives said they had an ongoing program of such training, but only 11 percent said that non-management employees were informed about security policy.

"Companies need to move aggressively in educating and informing employees," said Campbell. "A security environment aimed primarily at preventing outside intrusions is destined for failure."

Making the problem worse, companies seem to be focusing on the wrong risks. The report found that a third of executives considered hackers attacking from the Internet to be the greatest threat, but the reality, it said, is that almost 80 percent of attacks originate from inside a company's network.

Another study may complicate that finding, however.

Last March, the 2001 Computer Crime and Security Survey found that although attacks by online vandals didn't account for major dollar losses, the Internet has become a major source of attacks for most organizations. Companies that found themselves the victim of attacks via the Internet increased to 70 percent in 2001, but the number of companies experiencing insider attacks fell to 31 percent.

Still, some results of the KPMG study indicated that companies were improving information security.

Nearly eight out of 10 multinational corporations had developed a catastrophic response plan, and almost six out of 10 had hired full-time security specialists.

MS Office Tips:

IE security patch now released.

In last OpenAxis News, I introduced the security hole of Internet Explorer 5.5 and 6.0. Now Microsoft released the patch to fix this problem. Actually, this patch, when installed, eliminates all known security vulnerabilities affecting Internet Explorer 5.5 and 6.0. So I strongly recommend to install it.

<http://www.microsoft.com/windows/ie/downloads/critical/q312461/default.asp>

Also, if you disabled Active Scripting, here is to turn it back on.

- On the Tools menu, click Internet Options, click the Security tab, and then click Custom Level.
- In the Settings box, scroll down to the Scripting section, and click Enable under "Active scripting" and "Scripting of Java applets".
- Click OK, and then click OK again.



Have a question for Microsoft Windows or Office Product?

Ask our specialist and they can answer on this newsletter.

Please feel free to email your question to techsupport@openaxis.com.