

## in this issue

1

Microsoft plans to hit tools, database deadline

•

Microsoft Delivers Pair of Internet Explorer Betas

2

Webroot: Spyware Rampant in the Enterprise

3

Are Contactless Payment Cards Tickets to Wholesale Fraud?

4

Hitachi Unveils World's First Terabyte DVD Recorder

•

COMING!!  
January 1, 2006  
Roth 401(k)

## Microsoft plans to hit tools, database deadline

Microsoft next month intends to hand out nearly finished versions of its off-delayed database and flagship development tool.

The software giant plans to have a "release candidate" of Visual Studio 2005 and a "community technology preview" of SQL Server 2005 at its Professional Developers Conference in Los Angeles the week of Sept. 12—barring any production-related glitches, said Prashant Sridharan, lead product manager in Microsoft's developer division.

Sridharan added that both products will be available to all customers on Nov. 7, the latest delivery deadline for the products.

Developers will be able to use the products to build applications and get support from

Microsoft, although the tools will likely have a few remaining bugs, he said.

Also in September, Microsoft will release the third beta for the server component of the Visual Studio Team System collaborative programming application, which will ship in the first quarter of next year, Sridharan said.

Microsoft has struggled to meet its initial deadlines for Visual Studio 2005 and SQL Server 2005, having pushed out the delivery dates about one year.

A relatively small group of developers complained about the quality of the second beta version of Visual Studio 2005 and requested that the company have a third beta and delay the product until next year.

## Microsoft Delivers Pair of Internet Explorer Betas

Microsoft Corp. made available to beta testers on Wednesday two slightly different test versions of Internet Explorer 7.0, the next version of the company's Web browser.

Microsoft included IE 7.0 bits in the Beta 1 build of Windows Vista that the company began distributing, via download, to beta testers on Wednesday. It also released a separate beta of IE 7.0 that currently will run on Windows XP Service Pack (SP) 2 machines only. (Ultimately that stand-alone beta will run on Windows Server 2003 and Windows XP Professional x64 systems, too.)

Microsoft made the stand-alone IE 7.0 Beta 1 version available only to the same set of testers that are part of the Vista beta program.

"We are using the same distribution channels [for IE 7.0 Beta 1] as Vista is," said Gary Schare, a director of product management with Microsoft's Windows client unit.

Those include Microsoft Developer Network, TechNet and Microsoft Connect for the preselected individuals who are part of the Vista beta program.

Both beta versions of IE 7.0 contain almost the identical core set of features and functionality.



# Webroot: Spyware Rampant in the Enterprise

The number of Web sites distributing malicious software has quadrupled in the last year to more than 300,000, as the spyware problem continues to fester on the Internet, according to an upcoming report from Webroot, an antispyware software company.

Webroot Software Inc.'s State of Spyware Report for the second quarter of 2005, claims that 80 percent of enterprise computers are infected with some kind of adware or spyware. Rates of infections of malicious programs such as Trojan horse and keylogging software did not decrease between the first and second quarter, despite more awareness of the danger of spyware.

The report comes as the online criminal groups that are responsible for spyware switch from pay-per-click advertising to identity theft as a way to profit from their activities, said Richard Stiennon, vice president of threat research at Webroot.

The State of Spyware Report presents the results of spyware scans of almost 60,000 systems at 20,000 companies, Webroot said.

The average number of spyware infections on computers increased almost 20 percent to 27 per machine since the last quarter, despite more public awareness of the spyware problem and the availability of a number of new tools for detecting and removing spyware from infected computers, Stiennon said.

The reason may be that spyware makers are wising up to detection tools such as Microsoft Corp.'s Antispyware and Webroot's Spy Sweeper, Stiennon said.

Evidence collected by Webroot researchers indicates that spyware authors are testing their creations against those programs and adopting techniques from stealthy programs known as "root kits" to avoid detection, he said.

Online scam artists are switching their focus from installing advertising software that generates revenue from pop-up ads and pay-per-click advertising to spyware and remote-system monitoring tools that are used to steal identities, Stiennon said.

The spyware can generate far higher revenue, per install, for the online criminals, he said.

"We're seeing adware-type spyware evolving into system monitoring spyware," he said.

Software from mainstream adware vendors was actually less prevalent on systems scanned by Webroot, according to Webroot's data. That may indicate that improved installation practices and end-user license agreements from mainstream adware companies are having an affect. However, the



decline in legal adware is offset by the continued strength of malicious spyware such as keyloggers and Trojan horse programs, Webroot.

Cool Web Search, a ubiquitous form of spyware, was found on about 8 percent of the machines Webroot scanned in the second quarter, and keyloggers were on about 7 percent of all machines—comparable to the rates of infection last quarter, Stiennon said.

IT administrators should actively scan and monitor their network hosts for spyware infections. They should also avoid complacency about the problem, Stiennon said.

Keyloggers, Trojans and other spyware are much more common today than they were five years ago. However, they still pose a serious security risk to enterprises and should be taken seriously.

"I think the data loss news that is hitting us is an indicator of how serious this problem is," Stiennon said.

A new enterprise version of Spy Sweeper, which is being released Monday, will be able to detect and remove sophisticated spyware that changes the configuration of Windows systems and interacts with the operating system at a low level, said Brian Kellner, vice president of enterprise products at Webroot.

Spy Sweeper Enterprise 2.5 has a new spyware scanning engine and CRT (Comprehensive Removal Technology) that can remove even tricky spyware programs such as Look2Me and Cool Web Search variants without harming Windows systems, Kellner said.

Spy Sweeper Enterprise can also scan systems more quickly, uses smaller spyware definition files, and has a Web-based management dashboard with new reporting features and the ability to control and configure Spy Sweeper clients across an enterprise network, he said.

# Are Contactless Payment Cards Tickets to Wholesale Fraud?



can simultaneously process a legitimate credit-card payment on a POS system and store the card's data for illicit use later on.

This method is simple and reasonably covert with just a little sleight-of-hand practice.

For example, take a full-service restaurant where the bill is presented to the customer at the table. What if the waiter has a mini "contactless" reader in his pocket?

Such a device could read a card anywhere in reasonably close proximity; it need not even be from someone at the particular table that he is cashing out.

All that the waiter must do is to meander through the dining room, walking close to seated customers.

And given that a card is secretly read, the waiter can substitute that information in settling the check and simply pocket the cash from the customer.

Does this example sound too difficult? Or, might "contactless" payment not be permitted in full-service restaurants?

OK, let's try another scenario.

Assume that we are in a retail store that we frequent to purchase gas and pick up a soda for the road.

What if the cashier simply moves the contactless card reader to the edge of the counter, where it is directly up against the customers that typically lean against the counter while purchasing their items.

Up to the counter walks a woman with several items. The cashier says "That will be \$22.75, ma'am."

The customer sets her purse on the counter, digs into her wallet and hands the cashier \$30, receives change and leaves .

Unbeknownst to the customer, however, the proximity reader has picked up data from the contactless card in her purse; she never realizes the cashier actually

used the contactless card to process the order, while pocketing the cash.

Sound wild and unlikely?

In one pilot test to date, there has been at least one such unintentional/unexpected reading of a contactless card. It wasn't done with fraud in mind, but it certainly surprised both the cashier and the customer.

Thankfully, there are solutions to such issues. But can measures be implemented to thwart all such fraudulent activity? Or even to make contactless-payment fraud more difficult?

The simplest of all methods is to simply manufacture the contactless card with a touch sensitive activation dot on the card; essentially an "on/off" switch.

Press on the dot and the card will permit its data to be read. Don't press on the dot and the card will refuse to transmit any data via short distance radio wave.

Quite simply, the card cannot be read without the card-holder intending that it should be.

That method could be extended to incorporate fingerprint-based biometric security that will allow the card to recognize only the cardholder.

Certainly that would raise the cost of the card, but it would render a lost card useless to anyone other than the original owner.

Such contactless cards could have a fingerprint reader window in one corner of the card. Only the cardholder's finger would activate the card.

While such measures are not presently in place, I am confident that such are being actively discussed by Providers and that many more alternative solutions have been identified. I am also confident that some type of anti-fraud measures will be incorporated in future generations of contactless cards.

Until then, opportunity for fraud does indeed exist with contactless cards and the creativity, ingenuity and tenacity of the thief should never be underestimated.

Do you know who has been contacting your "contactless payment card," or those of your customers? You may not. With today's magnetic-stripe credit cards, you at least know who you have given your card to.

To use your account, thieves must get their hands on your card; or, if they gain access to online records, they have to get not only your credit-card number, but also its expiration date (and more recently, the authorization code on the card back).

However, the new "contactless" payment systems present new opportunities for fraudulent activity that are far less obvious than with mag-stripe cards.

A thief need not have possession of a victim's contactless card in order to capture all the relevant information. He or she only has to intercept the data during the wireless connection between the card and a point-of-sale system.

And to read the encrypted data, one only needs to get in reasonably close proximity to the victim. Contactless radio signals are very short range, but can be picked up from three to six feet. A thief can simply "walk by" the victim.

Proximity or "contactless" cards are used exclusively in physical locations which, not coincidentally, is where the majority of credit-card fraud occurs.

Worse, the majority of fraud is perpetrated by employees; by insiders, whose access to cards and ingenuity in misappropriating data are a deadly combination.

Small mag-stripe readers are easily "palmed," for example, so the employee

# Hitachi Unveils World's First Terabyte DVD Recorder

**COMING!!**  
**January 1, 2006**  
**Roth 401(k)**

TOKYO (Reuters)—Japan's Hitachi Ltd. on Wednesday unveiled the world's first hard disk drive/DVD recorder that can store one terabyte of data, or enough to record about 128 hours of high-definition digital broadcasting.

Hitachi, Japan's largest electronics conglomerate, is still a relatively small player in the DVD recorder market, trailing industry leaders Matsushita Industrial Co. Ltd., Sony Corp. and Toshiba Corp.

But it hopes its new line-up, which also includes models able to store 160 gigabytes, 250 gigabytes and 500 gigabytes of data, will help boost its market share and turn its loss-making DVD recorder business profitable in October-March, the second half of the business year.

"We entered the market last year and have only been able to grab about 3 percent of the market. It's been hard to earn a decent return on investment with such (low) volumes," Norio Ogimoto, general manager of Hitachi's storage media group, told a news conference.

"But we plan on being profitable with these new models given the volumes and prices we expect to see from them," he said.

Hitachi said the new models would be the first on the market able to simultaneously record two high-definition programs, and it hopes this will be a key selling point given the spread of terrestrial digital broadcasting in Japan.

The recorders will go on sale in Japan from next month. They are expected to retail from about 130,000 yen for the cheapest model to 230,000 yen for the one-terabyte recorder, which stores data on two 500 gigabyte hard

disk drives.

One terabyte is equal to 1 trillion bytes of data. One gigabyte equals 1 billion bytes.

Hitachi said it did not have concrete plans for launching the products in overseas markets, explaining that consumers in Europe and the United States were not as keen on high-end recorders.

Japan accounts for more than half of the global DVD recorder market. DVD recorders have been slow to take off in other markets such as the United States, where TV set-top boxes with hard drives, such as those made by TiVo Inc., are popular.

MM Research Institute predicts that Japan's DVD recorder market will grow 26 percent to 5.6 million units in the current financial year to next March, up from 4.43 million in 2004/05.

Matsushita was the top seller of DVD recorders in Japan in 2004/05, controlling 27 percent of the market. Sony was next at 20.6 percent, Toshiba at 15.6 percent, and Sharp Corp. came in fourth with a 10.2 percent share.

Hitachi said it was aiming to grab 35 percent of the Japanese market for high-definition DVD recorders in the second half of this business year. High-definition recorders currently make up about 15 percent of the overall market, but that percentage is expected to grow strongly over the next several years.

Shares of Hitachi closed down 0.87 percent at 681 yen, underperforming the benchmark Nikkei average, which gained 0.24 percent on the day.

Beginning in 2006, 401K plans will be permitted to allow employees to designate their contributions as Roth contributions. These Roth contributions will be subject to the same rules as Roth IRAs. This means the contributions must remain in the plan for 5 years to receive the tax free advantage.

The IRS provisions of the Economic Growth and Taxation Relief Reconciliation Act made the following changes affecting 401K plans:

Catch-up contributions were added to provide for additional elective contributions for participants age 50 and older.

The 401K regulations are to be changed to shorten the period of time that an employee is stopped from making elective contributions under the safe harbor rules for hardship distributions.

Distributions from 401K plans are permitted upon severance from employment rather than separation from service.

Faster vesting is required for matching contributions.

The Roth 401(k) will be an incredible opportunity for millions of employees. The contribution amounts into a Roth 401(k) would be identical to the contribution amounts for a regular 401(k) - with the exception of pre-tax consideration. And after meeting the necessary requirements, the distributions would be tax free!

The IRS regulations on Roth 401(k)s has not been finalized. Visit the IRS website at [www.irs.gov](http://www.irs.gov) for the latest developments on this incredible opportunity.

