

Microsoft's Anti-Virus Strategy Keeps Users Guessing

Microsoft®

One year after it surprised rivals and partners by jumping into the anti-virus market, Microsoft Corp. still has no clear AV strategy, and users are still hanging on to the promise of integrated Windows protection.

Until recently, Microsoft officials had said there were no immediate plans to build AV into Windows. They even promised to build a better API to make it easier for third-party AV products to work with Windows.

But now, 12 months later, Microsoft has done little to clear up the uncertainty surrounding its intentions for the GeCAD technology. Although Mike Nash, vice president of the Security Business and Technology Unit at Microsoft, reiterated last week in a widely publicized meeting with reporters in Seattle that the company is on track to offer its own AV solution, there has been no decision made about what form that solution might take.

While Microsoft officials stressed that the AV solution will initially be a stand-alone product, separate from Windows, security industry observers speculated that the company will eventually integrate AV protection into Windows. In fact, they said this most likely will happen in the next release of the Windows client, code-named Longhorn, which isn't expected until 2006 and is already scheduled to include a wide range of security upgrades.

"We would evaluate Microsoft's solution, but I would be hesitant to use their built-in AV software exclusively. I would be more comfortable with the approach of using a non-Microsoft vendor for virus-scanning engines and virus definitions," said James Jones, LAN administrator with a large health care system on the East Coast. "Better integration with Microsoft's OS is a definite plus. I guess the question comes down to trust. Microsoft

is headed in the right direction with their security, but the industry isn't convinced yet, and it will be some time before we will be."

Executives at big AV vendors, meanwhile, said they see no immediate reason to alter their strategies, despite Microsoft's history of partnering with other vendors, only to compete against them.

"Traditional vendors who rely upon selling primarily individual point products or hawking cures for the latest Internet scare will find the security market cold and unresponsive," said Sam Curry, vice president of eTrust Security Management at CA, in Islandia, N.Y.

While Microsoft officials stressed that the AV solution will initially be a stand-alone product, separate from Windows, security industry observers speculated that the company will eventually integrate AV protection into Windows. In fact, they said this most likely will happen in the next release of the Windows client, code-named Longhorn, which isn't expected until 2006 and is already scheduled to include a wide range of security upgrades.

"We would evaluate Microsoft's solution, but I would be hesitant to use their built-in AV software exclusively. I would be more comfortable with the approach of using a non-Microsoft vendor for virus-scanning engines and virus definitions," said James Jones, LAN administrator with a large health care system on the East Coast. "Better integration with Microsoft's OS is a definite plus. I guess the question comes down to trust. Microsoft is headed in the right direction with their security, but the industry isn't convinced yet, and it will be some time before we will be."

Security specialists say that if and when that happens, customers would likely—at least in the short term—be able to stay with their current AV vendor.

ISI insight isi

a monthly resource by Intelligent Solutions, Inc.

September 2004 - Vol.09-04

in this issue

1

Premier Financial

•

Aol Employee Arrested on Spam Charges

2

Buying Medicines From Abroad...

•

Drugs From Canada are Cheap but Risky

•

Reports of Phishing Attacks Up Again in May

3

Six Reasons Linux Has Enterprise Appeal

4

Microsoft's Anti-Virus Strategy Keeps Users Guessing



ISI is proud to announce our latest corporate division - Premier Financial Solutions.

Offering Accounting and Tax solutions for personal or business entities, PFS assists greatly in Intelligent Solutions' vision to become a single point of contact for all of our clients' business needs.

You can find out more information on Premier Financial by logging on to www.pf-sacctg.com or call 708.532.8488 ext. 240 and speak to Mike Koziol.

AOL Employee Arrested on Spam Charges

An employee of America Online Inc. was arrested Wednesday morning for stealing AOL user screen names and selling them to a spam e-mail operation, AOL said in a statement.

AOL said it discovered the screen name thefts and passed the information on to federal law enforcement agencies, leading to the arrest. AOL has fired the employee, it said in the statement, and is committed to his full prosecution.

No member credit card or password information was compromised, AOL said.

U.S. media reports said that the number of screen names stolen totaled 92 million and that the e-mail spammer had also been arrested. The

AOL employee received over \$100,000 for the list of names, media sources said. The pair face up to five years in jail and heavy fines if convicted under the U.S.'s new Controlling the Assault of Non-Solicited Pornography and Marketing Act, known as the CAN-SPAM Act, which came into effect at the beginning of the year.

In the statement, AOL said it is reviewing and strengthening its internal procedures as a result of this investigation and arrest.

The incident comes the day after AOL, along with Yahoo Inc., Microsoft Corp. and EarthLink Inc., formed the Anti-Spam Technical Alliance and released a set of recommendations for eliminating spam.

isi

18530 Spring Creek Drive - Tinley Park, IL 60477

tel: 708.532.8488 - fax 708.532.8493

www.intelligentsolutions.net

Sun Opens Its 3-D 'Looking Glass' Linux Desktop



Sun will put into the hands of the open-source community Project Looking Glass, its next-generation, 3-D Linux desktop system that has been receiving rave reviews. As work continues on Looking Glass, Sun has open-sourced Java 3D.

SAN FRANCISCO—By open-sourcing its next-generation Linux desktop technology, Sun Microsystems Inc. is turning over some of its most innovative work to date to the open-source community, sources said.

Officials at the Santa Clara, Calif., systems maker said at JavaOne here that Sun plans to turn its next-generation Linux desktop, Project Looking Glass, over to the open-source community. The open sourcing of its Looking Glass technology represents a significant move by Sun, which has been under pressure by the open-source community to “open” some of its technology, specifically Java itself.

However, Project Looking Glass has won Sun rave reviews as well as accolades within and outside the company for its creator, Hideya Kawahara, a senior staff engineer at the company.

Kawahara, a humble developer who in an interview with eWEEK simply referred to himself as “a geek,” turned heads with his three-dimensional Linux desktop system with features that rival, and some even say surpass, those of next-generation desktops from

Apple Computer Inc. and Microsoft Corp. “All rendering is done in 3-D space,” Kawahara said. “And you can use all your legacy apps,” he added, showing a Microsoft Word document on the screen during a demo for eWEEK shortly after the technology was unveiled last year.

The desktop, which features other components such as Sun’s Star Office, the Mozilla browser, RealPlayer support and other components, enables users to “fly around in 3-D and access applications and files in unique and interesting ways,” said Peder Ulander, director of desktop solutions at Sun.

While Sun plans to open-source Looking Glass, it can’t yet because the technology isn’t finished. Kawahara said it will soon be completed and then turned over to open source. In the meantime, Sun did announce that it has open-sourced Java 3D, with Looking Glass to follow soon.

“I believed 3-D would be the next user interface,” Kawahara said. “So I started a side project using my spare time.”

Kawahara said he worked for more than a year using at least two hours a day—plus weekends—of his spare time to create Looking Glass. He

said he took no vacations, worked through Thanksgiving and Christmas vacations and risked his relationship with his girlfriend to complete the project.

“I knew Microsoft and Apple were designing next-generation desktops,” he said. “So I searched the Web about Linux, and I couldn’t find anything that had this, so I figured this is what I could do to advance Linux.”

Asked why he didn’t try to take the technology out on his own and commercialize it, Kawahara said: “I am just a geek. I am interested in working with the community, and because this is Java it has very good productivity and is good for Sun.”

With Sun’s move to open-source Looking Glass, Kawahara gets his wish of supporting the community.

Said Ulander, “This will change the way people look at their desktop, at online games and how you interact with your file system.”

Buying Medicines From Abroad...

Buying medicines from abroad comes with a hefty tax price, the cost is not deductible as a medical expense, according to IRS. That’s because federal law bars importing prescription drugs from Canada and other countries. For the same reason, the cost of these medicines cannot be reimbursed by flex plans or health reimbursement arrangements. Remember that when figuring how much you’ll save by buying imported drugs.

Drugs From Canada Are Cheap but Risky

Filling your prescriptions through an online Canadian pharmacy is a tempting and increasingly popular way to save money, but be careful. Not only is it illegal, it can be difficult to distinguish between legitimate pharmacies and scammers. If you decide to defy the law, first call the provincial licensing authority to check that the business you are dealing with is licensed and in good standing (a list of licensing authorities is available at www.napra.org) Confirm that your drugs will be shipped directly from the pharmacy, and to expect to receive your medicine in sealed factory containers. Consult your doctor if you receive a substitute drug. Stay away from any site that does not require a doctor’s prescription, or a Canadian pharmacy that supports to sell drugs approved by the U.S. Food and Drug Administration. Drugs sold in Canada are approved by the country’s own regulatory agency, Health Canada, not by the FDA.

Reports of Phishing Attacks Up Again in May

Incidents of phishing, a type of online identity theft, were up slightly in May, after surging in March and April, according to a report from an industry group.

The number of unique phishing attacks reported to the Anti-Phishing Working Group increased 6 percent in May to 1,197, with an average of 38.6 reports each day, slightly higher than in April. The numbers could have been higher, but scam artists may have taken a break for Memorial Day in the U.S., keeping the final tally low, the report said.

Phishing scams are a form of online crime in which unsolicited commercial (“spam”) e-mail is used to direct Internet users to Web sites controlled by the thieves, but designed to look like legitimate e-commerce sites. Users are asked to provide sensitive information such as a password, social security number, bank account or credit card number, often under the guise of updating account information.

Financial services companies continued to be the primary target of the scams, and Citibank Inc. customers were the most frequent target of phishers. Scams using the names of eBay Inc. and Paypal Inc., an eBay company, were also rampant in May, said the group, which is sponsored by Microsoft Corp., VeriSign Inc. and antispam company Tumbleweed Communications Corp., among others.

Phishing scams have surged in recent months to 1,100 in April, a 178 percent increase from March, according to figures from the Anti-Phishing Working Group’s April report. In May, the group received reports of over 300 attacks a week, with a big drop-off the week of May 29, possibly due to the Memorial Day holiday, the report said.

Faked sender, or “from” addresses on e-mail messages continued to be a popular tool of scam artists. At least 95 percent of e-mail messages submitted to the Anti-Phishing Working Group used such addresses.

The spoofed addresses are frequently identical to legitimate addresses at the companies being targeted by the phishers, for example: support@citibank.com and billing@aol.com were common spoofed addresses. The remainder of phisher e-mails submitted to the group came from so-called “social engineering addresses” -- online mailboxes at domains run by the scam artists that resemble actual e-commerce sites. The domains, such as eBay.billing.com, instead of eBay.com, or verify-visa.net, as opposed to visa.com, are designed to fool customers, the report said.

The phishing problem has received increased attention from the private sector and governments in recent months, as online criminals have seized on the scams as a lucrative and relatively simple way to make money.