Yui Kee Computing Ltd.

Newsletter

September 2003

Contents

Incident Update

W32/Swen.A@mm, also known as W32/Gibe-F, started spreading on 18 September. It arrives in an email that appears to be a security patch sent by Microsoft. Microsoft never emails security patches. Further information is available:

http://www.sophos.com/virusinfo/articles/gibef.html
http://www.sophos.com/virusinfo/analyses/w32gibef.html
http://www.f-secure.com/v-descs/swen.shtml
http://www.hkcert.org/valert/vinfo/w32.swen.a@mm.html

Microsoft Applications Vulnerabilities

Microsoft has announced in MS03-035 that an important flaw in Microsoft Word could allow macros to run automatically. The vulnerability affects:

Microsoft Word, all versions
Microsoft Works Suite, all versions

Further Details:

http://www.microsoft.com/technet/security/bulletin/MS03-035.asp

A second vulnerability, this one also important, is a buffer overflow bug in one of the Office converters. It affects:

Microsoft Office (all versions)
Microsoft FrontPage (all versions)
Microsoft Publisher (all versions)
Microsoft Works Suite (all versions)

Further Details:

http://www.microsoft.com/technet/security/bulletin/MS03-036.asp

Another security bulletin, MS03-037, announces a critical flaw in Visual Basic for Applications that could allow arbitrary code execution. The affected products are:

Microsoft Access 97
Microsoft Access 2000
Microsoft Access 2002
Microsoft Excel 97
Microsoft Excel 2000
Microsoft Excel 2002
Microsoft PowerPoint 97
Microsoft PowerPoint 2000
Microsoft PowerPoint 2002
Microsoft Project 2000
Microsoft Project 2002
Microsoft Publisher 2002
Microsoft Visio 2000
Microsoft Visio 2002
Microsoft Word 97
Microsoft Word 98(J)
Microsoft Word 2000
Microsoft Word 2002
Microsoft Works Suite 2001
Microsoft Works Suite 2002
Microsoft Works Suite 2003
Microsoft Business Solutions Great Plains 7.5
Microsoft Business Solutions Dynamics 6.0
Microsoft Business Solutions Dynamics 7.0
Microsoft Business Solutions eEnterprise 6.0
Microsoft Business Solutions eEnterprise 7.0
Microsoft Business Solutions Solomon 4.5
Microsoft Business Solutions Solomon 5.0
Microsoft Business Solutions Solomon 5.5

Further Details:

http://www.microsoft.com/technet/security/bulletin/MS03-037.asp

MS03-038 announces a buffer overflow vulnerability that may allow an attacker to run the code of their choice in Access. This flaw affects:

Microsoft Access (all versions)

Further Details:

http://www.microsoft.com/technet/security/bulletin/MS03-038.asp

Microsoft Windows Vulnerability

Another three vulnerabilities in the RPCSS service of Windows have been announced by Microsoft in MS03-039. The critical flaws affect the same service that W32/Blaster exploited. The following versions of Windows affected:

Microsoft Windows NT Workstation 4.0
Microsoft Windows NT Server® 4.0
Microsoft Windows NT Server 4.0, Terminal Server Edition
Microsoft Windows 2000
Microsoft Windows XP
Microsoft Windows Server 2003

It does not affect:

Microsoft Windows Millennium Edition

Further Details:

http://www.microsoft.com/technet/security/bulletin/MS03-039.asp

Sophos Fights Spam

Combined company poised for global leadership in enterprise anti-virus and anti-spam protection

Sophos, a world leader in anti-virus protection for businesses, today announced that it has acquired ActiveState, a North American software company that develops anti-Spam software for enterprises and professional tools for open source language programmers.

Driven by mounting pressures to ensure a secure and low-cost infrastructure, organisations are increasingly demanding consolidated protection against security threats such as viruses, Spam and policy breaches. The transaction, worth $23 million in cash, thrusts UK-based Sophos into the leading position in meeting the expanding secure content management needs of businesses worldwide.

ActiveState is based in Vancouver, British Columbia, and serves more than two million customers, including HP, Intel and Microsoft. Sophos has purchased all the shares of ActiveState, and will retain all of ActiveState's 100-plus employees. ActiveState's headquarters in Vancouver will become an additional centre for research and development for Sophos and will also provide local market support in Canada as well as expanding Sophos's west coast support.

ActiveState's product lines for open source programmers will continue to be developed and sold under the ActiveState brand. As a division of Sophos, the existing ActiveState team is committed to continuing its support of the open source language community.

Industry analysts Gartner Inc. claim that up to 50% of the average business mailbox is spam.1 Although both the US and UK governments are proposing legislation against spammers, the problem is threatening to swamp businesses, preventing them from operating efficiently. Acquiring ActiveState leaves Sophos well positioned to meet enterprise demands for consolidated email protection. As Arabella Hallawell, research director, Gartner Inc., reports, "There is growing enterprise demand for combined anti-spam and anti-virus product and service capabilities at the email boundary."

Industry analysts Ferris Research agree. "Sophos and ActiveState have a shared vision, strong and complementary products, and a similar culture of engineering excellence," says David Ferris, president, Ferris Research. "Enterprises increasingly look to a single vendor for protection against spam and viruses at the gateway, so the acquisition of ActiveState by Sophos makes a lot of sense."

"The proliferation of Spam, combined with our existing customers' increasing desire to receive anti-virus and anti-Spam protection from the same source, means that now is a very strategic time for us to expand into spam filtering," said Peter Lammer, founder and joint CEO of Sophos. "With a focus on serving business environments, ActiveState has a very similar company culture to Sophos. There is also a good technical fit between both companies' proprietary technologies. ActiveState's proven technology, its impressive customer base, its expertise in the open source world, and in particular the quality of its staff are very valuable additions to Sophos."

ActiveState's President, Steve Munford, will be taking a key role in driving the anti-Spam element of Sophos's business, becoming a member of the executive management team. Munford takes the post of Global VP Messaging, and will attend Sophos Plc board meetings.

"For the last three years, Sophos has significantly outperformed the anti-virus market as a whole. This impressive growth is a reflection of Sophos's unwavering focus on the enterprise market and its commitment to customer service," said Munford. "These qualities combined with our proven technology means that the company is well placed to meet the IT security needs of businesses. We are excited to be joining the Sophos team."

Sophos's anti-virus technology will be integrated with PureMessage, ActiveState's enterprise email protection software, to deliver industry-leading anti-virus and anti-spam protection in a single, consolidated solution - Sophos PureMessage. PureMessage currently supports AIX, HP-UX, FreeBSD, Linux and Solaris.

Third Arrest in Blaster Case

On the 26th September, prosecutors in Seattle announced the arrest of a juvenile for "intentionally causing damage and attempting to cause damage to protected computers," in connection with the release of one of the variants of the Blaster worm.

This is, possibly, the third arrest in connection with a variant of the Blaster worm. The first was Jeffrey Lee Parson, 18 of Hopkins, Minnesota, USA. He has pleaded not guilty and will next appear in court on 17 November. Previous virus writers who were charged, including David L Smith, Christopher Pile and Simon Vallor have pleaded guilty, so this could become an important test case.

The second arrest was reported to be of Dan Dumitru Ciobanu in Romania, but authorities have since said that no arrest has occurred.

Interestingly, the original author of W32/Blaster.A, has not been identified or arrested. W32/Blaster.A was the first and most widespread variant, and all later variants were derived from it.

"It is common for a successful virus to be followed by various minor variants, often written by people with not enough technical skills to write a virus from scratch", said Allan Dyer, Chief Consultant for Yui Kee Computing. "In this case, the copy-cats were caught by the authorities' search for the originator, presumably they were also less able at covering their tracks. It can only be a good thing if the message that writing and releasing malicious code is wrong and will be punished is hammered home by the due course of the law."

PureMessage is #1 Anti-Spam Solution for Higher Education

VANCOUVER, BC, 2003/08/20

As students head back to school this fall, many will experience a dramatic decrease in the volume of Spam and viruses that land in their email in-box. Behind the scenes, the IT departments of leading institutions world-wide are taking control of their email with PureMessage, a server-based email filtering solution by ActiveState.

ActiveState provides anti-Spam software to more than 80 of the world's largest and most prestigious educational institutions, including: Duke University, Stanford University, University of California at Berkeley, Cornell University, New York University, University of North Carolina, University of Washington, Texas A&M, Temple University, University of Leeds, and Hong Kong University of Science and Technology. PureMessage is also used by hundreds of leading corporations worldwide.

Scalability and Reliability

The education sector is challenged by the need to stop the growing spam problem with limited budgets and resources. However, many IT departments at educational institutions operate on a scale similar to a Fortune 500 company, serving up to tens of thousands of users, all of whom require access to email, including students, faculty, staff, and alumni. Heterogeneous IT infrastructures across multiple departments and schools, and the use of a variety of UNIX, Windows, and Macintosh email clients, often create a diverse and complex environment in which to deploy new products.

PureMessage by ActiveState provides a cost-effective, comprehensive email filtering solution for the education sector that scales to accommodate hundreds of thousands of users, and can be easily integrated with existing systems. Using a unique combination of heuristics, spam directories, spam signatures, and learning algorithms, PureMessage safely identifies and quarantines more than 98% of spam. As a result, schools ensure computer resources are being used efficiently and end-users regain productivity losses caused by spam. Customers are also attracted to PureMessage's per-CPU licensing, which further reduces costs by removing the need to track and report individual users.

Ranked as College of the Year among Research Institutions, Indiana University advocates the PureMessage solution. Says Rob Henderson, associate facilities director for the Computer Science department, "The utility versus cost of PureMessage is exceptional. I would not hesitate to recommend PureMessage to my educational colleagues."

Protecting Academic Freedom and Privacy

In recent months, academic IT departments have become overwhelmed with spam complaints from end users, elevating internal concerns about the institution's reputation as a thought-leader, and introducing the possibility of lawsuits related to unsolicited email. Yet many schools have a policy protecting academic freedom and privacy, which must be balanced with the need to protect their IT infrastructures and end users.

Using the "tag and pass" option, PureMessage automates the spam identification process, while providing the ability for end users to determine how they want to handle such messages.

"Whether you're an administrator managing an international business school, or a student communicating with a professor online, email has become just as important function in academia as it has in the workplace and the home. That function is being threatened by spammers' ability to evolve new spam techniques, and obtain valid student and faculty email addresses over the Internet," said Chris Kraft, director of PureMessage product management, ActiveState. "PureMessage provides the education sector with a cost-effective solution to define, monitor, and manage their email."

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2555 0209 Fax: 28736164
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/computer/


One Stop Anti-virus
&
Information
Security Partner
- Anti-Virus
- Firewall
- Communication Encryption
- File & Folder Encryption
- VPN
- Smartcard Token
- Content Security
- Security Check Services:
Vulnerability Scanning,
Penetration Test,
Risk Assessment ...etc.
YUI KEE