

Net education the best defence against network threats, spam

Internet security firm mizag Ltd. estimates that digital attacks from hackers and viruses have resulted in over \$100 billion in damages to websites worldwide in 2003. A record level of attacks—20,000, in the month of January alone—helped make Internet security one of the leading issues in the online world in 2003. It is predicted that these numbers will continue to increase with the total economic damage from all types of digital attacks worldwide passing the \$250 billion mark in 2004. This poses a serious threat to online businesses, but it's a threat that can be combated through proper education on the subject. This is the message being relayed internationally by WSI, the world's largest network of Internet Consultants.

Once a business has made the decision to go online there are a number of important considerations beyond the development of the site itself. Concepts such as security — an ongoing and evolving process — is rarely given the attention it deserves. Through the consulting services offered by WSI, a business can acquire the critical knowledge it needs to protect itself from becoming an Internet security statistic.

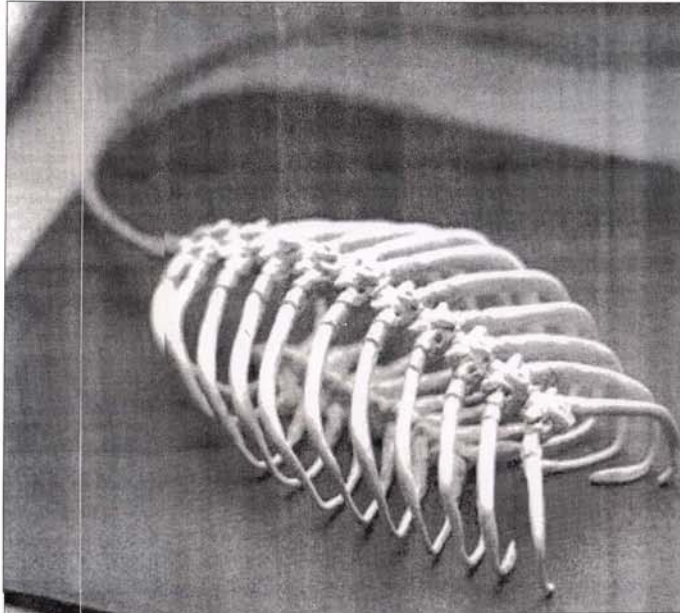
"Education is the key to a business protecting itself online," explains WSI Internet consultant Rene Garcia. "Everyday companies unknowingly make mistakes that leave their systems vulnerable to digital attacks. With the proper knowledge and software in place these mistakes can be avoided, saving money and increasing productivity and efficiency in the process."

Typically, the news media focuses on attacks to large corporations and government agencies, leaving small- to medium-sized businesses with the impression that Internet security isn't an issue that concerns them. Unfortunately this isn't the case. Any business, no matter what its size or function faces potential threats from hackers each day for numerous reasons. By teaching companies how to defend their systems, WSI Internet Consultants strive to keep their clients informed and safe. As WSI clients know, one of the largest daily threats is the increased reliance on email—one of the most versatile and important tools to any online business. However, email as a communication medium is insecure and opens the door to potential attacks such as virus distribution and unsolicited advertisements or "spam".

The popularity and widespread adoption of email is no accident; it is often more efficient than other means of communication and allows customers to quickly contact a business from anywhere in the world at any time of day. But as inboxes fill up with orders, inquiries, and correspondence, they also fill up with spam. In November 2003, measurements by Brightmail's Probe Network showed that 56 per cent of all email was spam-related. This has caused many industry insiders to predict that by mid-2004 spam will surpass the 60 per cent mark.

And with ever-increasing spam comes larger threats to security. Spam in itself is an annoying nuisance that many businesses find drains productivity, distracts employees, and can be offensive. It also has a negative effect on server and storage space and can slow down connection time. In addition to this effect on valuable network resources, spam can also contain malicious code, and in some cases has been connected to credit card fraud and software piracy.

With thousands of email messages being received and sent by individual companies each day, many businesses are making themselves an



easy target to hackers, viruses, and spam. By utilising WSI's industry leading technology such as intrusion detection applications, authentication devices, and firewalls, a business can position itself to avoid the costly consequences associated with digital attacks.

Few can forget how fast the Sobig.F virus spread through the online world this past August, crippling entire network systems with the sheer volume of email traffic it produced. In just a few short weeks, this email-based threat caused \$29.7 billion worth of damage to companies worldwide that were caught unprepared for such an attack.

Businesses can avoid costly security threats by practicing safe online behavior and employing server-based traffic filtering technologies, such as those offered by WSI's hosting environment. As each busi-

ness is different, WSI Internet Consultants can assess which methods will suit a particular company best and then deploy those solutions to protect their clients. As WSI Internet Consultant Garcia says, "Knowledge is power and with the right information in hand, most Internet security threats can easily be avoided."

WSI, headquartered in Toronto, Canada, is ranked the #1 Internet Services Business in the world and the 4th fastest-growing International Franchise. With systems that have been developed, utilised and proven by over 700 Internet Consultants in 87 countries worldwide, WSI delivers thousands of e-Business solutions to small and medium sized businesses annually. Visit www.wsicorporate.com for more information.

Microsoft Corporation promised Thursday to pay \$250,000 to anyone who helps authorities find and prosecute the author of a fast-spreading computer virus.

The cash reward is the third so far under a \$5 million programme Microsoft announced in early November to help US authorities nab authors of unusually damaging Internet infections aimed at consumers of the company's software products.

The "MyDoom.B" virus, spread by e-mail, causes victims to launch an electronic attack starting Tuesday against Microsoft's own web site, and prevents victims from visiting the web sites of leading antivirus companies. The virus poses as an authentic-looking error message.

Among the only clues to the identity of the possible author was a mysterious message inside the virus, "Andy: I'm just doing my job, nothing personal, sorry."

Microsoft offers reward

"This worm is a criminal attack," said Brad Smith, Microsoft's senior vice president and general counsel. "Microsoft wants to help the authorities catch this criminal."

Microsoft urged anyone with information about the author of the "MyDoom.B" virus to contact the FBI, Secret Service or Interpol. The company targeted by an earlier version of the same virus, The SCO Group Inc., previously offered a \$250,000 reward for information leading to the arrest and conviction of the creator of the MyDoom.A version, which is more widespread. Experts have said the same person prob-

ably created both versions.

Government officials and others have described the \$250,000 rewards as the highest in recent memory funded entirely by the private sector — akin to cash bounties paid in the late 1800s by Western banks to vigilantes who hunted robbers.

Internal FBI documents, obtained by The Associated Press, indicate the government is a cautious supporter of Microsoft offering cash bounties.

FBI officials in October gave conditional approval to Microsoft for the concept. But they cautioned that they won't share secret details of any investigation

with Microsoft executives and won't promise to launch any formal investigation whenever the company announces a reward.

In the documents, obtained under the US Freedom of Information Act, the FBI said it was developing "a more formal operating protocol for working with Microsoft" and with other companies that want to offer similar rewards.

Microsoft said residents of any country are eligible for the \$250,000. The company has said previously it will not pay rewards to anyone involved in creating the viruses.

Previous rewards of \$250,000 each were offered for information about those responsible for the Blaster and Sobig viruses, which spread rapidly last summer among hundreds of thousands of computers running Windows.

Worst email worm in virus history

The Mydoom email worm, which was first found on January 26, 2004, has already spread more than 20 million times. The Sobig.F worm spread massively in August 2003 and until now has held the title of the fastest spreading email worm in history. Email worms are currently the most common virus type in the world. Automatic network worms can spread even faster, but they are not nearly as common. There are three main reasons behind the fast outbreak of Mydoom:

- Social engineering: the worm masks the infected emails to look like system error messages, prompting people to click on them. Also, some of the infected attachments are inside ZIP archives, which might seem less dangerous to users.
- Time zones: Unlike most other recent email worm outbreaks, Mydoom was found in the middle of business hours in USA and several large corporate networks got infected immediately.
- Aggressive collection of email addresses: in addition of sending itself to email addresses found from users' files, the worm also creates new addresses by guessing common user names and addresses. It can also bypass some of the tricks people use to hide their email addresses from spammers.

Virulent worm poised to outdo predecessor

A new variant of the Mydoom computer worm, which has been clogging up the Internet for days, was poised to overtake its predecessor to become the most widely spread computer bug ever, experts said.

The so-called Mydoom.B computer worm was designed to spread by users opening their e-mail, even if they leave attachments closed, making it more virulent than anything seen previously. Mikko Hypponen, of Finnish anti-virus firm F-Secure, said:

"Some variants of the Mydoom.B version will run automatically from the e-mail, it's enough to just open and read the mail," he told AFP.

"It will cause it to spread quite quickly," Hypponen said.

In the first version of the bug recipients of infected e-mails had to open an attached file in order to have their computers contract the worm.

Further testing showed however that due to faulty programming by Mydoom's author, this function did not always work as intended.

First detected Wednesday, the latest variant also uses a backdoor

function of the first version to update itself and attack more computers.

After infecting a computer, it immediately scans for other infected computers in the network, using the earlier version's backdoor function to update itself, Mikael Albrecht, also with F-Secure, said.

Although still smaller than the A version, "the Mydoom.B variant is spreading quite quickly now," and will become as big as its predecessor, "if not bigger," Albrecht said.

Some variants of the Mydoom.A was detected on Monday night it has clogged the Internet by sending hundred of millions of infected e-mails throughout the world.

But ironically, the success of Mydoom.A would curb the pace of proliferation of its successor, as it has severely slowed down the Internet and corporate computer networks, causing huge delays in the delivery of e-mails, Hypponen noted.

The bug was not believed to impair the normal functioning of not even notice that their machine had been infected, experts said.

Most of the e-mails generated will never reach their destinations however, having been stopped by the anti-virus protection of corporate computer networks, analysts said.

Wednesday evening it was estimated that one in three e-mails sent worldwide was generated by the Mydoom.A bug.

The spread of the virus prompted a FBI investigation and a scramble to update software protection, but analysts said it was unlikely that the author of the Mydoom bugs would ever be caught.

The proliferation of the first variant was however leveling out on Thursday, experts said, as many computer users had updated their anti-virus software.

Since the new variant slips into computers unnoticed by the detection software made for the Mydoom.A version, security experts urged computer users to update their anti-virus software frequently to make sure they are immune from the latest bugs.

Some posted detection software and instructions on how to get rid of the

Mydoom strains on their web sites free of charge.

While the first version was designed to attack the web site of Utah-based software vendor SCO, the new version also launched an assault on Microsoft's page www.microsoft.com, virus crackers said.

These attacks might be just diversions however from the bugs' real intention of infecting computers and opening backdoors on them, enabling their creator to access infected machines from a distance, possibly to relay spam, experts warned.

Mydoom spreads through e-mail attachments and downloads from the popular Kazaa file-sharing service, which lets Internet surfers share content such as games, movies and music with each other for free.

Part of Mydoom's "success" is that it — unlike many earlier bugs — poses as an error note with the main users to open the attachment to read it, thereby inadvertently launching the worm.