NETWORK SECURITY

ISSN 1353-4858 November 2003

Incorporating E-Commerce, Internet and Telecommunications Security

Editor: Sarah Hilley

Senior Editor: Sarah Gordon

Editoral Office:
Elsevier Advanced Technology, PO Box 150
Kidlington, Oxford OX5 1AS, UK
Tel: +44-(0)1865-843645
Fax: +44-(0)1865-843971
E-mail: s.hilley@elsevier.co.uk

Subscription Price for one year:
(12 issues) US$736/€657 including first class airmail delivery subject to our prevailing exchange rate

Price valid to end of 2003

Subscription Enquiries:
Orders and Payments:

For customers residing in the Americas
(North, South and Central America)

Elsevier Customer Support Department
PO Box 945, New York NY 10010 USA
Tel: (+1) 212-633-3730
[Toll free number for North American customers:
1-888-4ES-INFO (437-4636)]
Fax: (+1) 212-633-3680
E-mail: usinfo-f@elsevier.com

For customers in the rest of the World:
Elsevier Customer Support Department
PO Box 211, 1000 AE Amsterdam, The Netherlands
Tel: (+31) 20-3853757
Fax: (+31) 20-4853432
E-mail: nlinfo-f@elsevier.nl

To order from our website:
www.compseconline.com

Computerized surveillance a top priority for Pentagon

Wayne Madsen

An unclassified budget document titled, "Fiscal Year 2003 Budget Estimates" provides a glimpse into some of the Pentagon's next generation computer surveillance programs. The document, prepared by the Defense Advanced Research Projects Agency (DARPA) describes how the Pentagon plans to use information technology to address asymmetric threats, described as the "most serious threats to our national security, today."

Continued on page 2...

Virus tracking moves back to basics

The Sobig and Blaster authors are proving so elusive, that Microsoft is forking out $250,000 for any leads.

This reward system comes at a time when tracking writers by network forensics is so difficult that traditional methods are being resorted to.

The reward is part of the Anti-Virus Reward Program, set up by Microsoft, which has a pool of $5 million.

The program is dangling money as an enticement to get the underground to talk.

Peter Stephenson, research scientist at Eastern Michigan University said: " Virtually all of the virus authors that have been caught so far were caught because they couldn't keep their mouths shut. They were tracked using traditional investigative methods."

The FBI, Secret Service and Interpol all back the Microsoft initiative.

Microsoft's decision to pay out for author leads may work believes Stephenson.

"Offering rewards is a traditional investigative technique and that is pretty much all that is working at the minute."

However, he is concerned that this approach will only work if the authors are not linked to criminal activity. People within the hacker community will typically know who virus authors are, he said. "However, terrorists, money launderers, and drug cartels may use 'professional' hackers and virus writers to accomplish their ends and these individuals don't brag about their feats in public. If a worm is used to cause damage for political, religious or economic reasons, it is unlikely that the source will ever be identified because of the immature state of forensic track back techniques."

It isn't just Sobig and Blaster that are proving to be a mys-

Continued on page 3...

Contents

This resistance to regulation was echoed repeatedly throughout the conference.

Geoff Smith, UK Department of Trade & Industry said: “Regulation isn’t the answer because it can’t keep up with technology.”

Clarke said that IT professionals have been watching the increasing deterioration of security for so long that they have failed to notice the drastic plummet over the past 12 months.

Clarke points out that two years ago there were 21 000 separate viruses. So far this year there are 114 000 viruses. “This is not just more of the same. Things have become unacceptably worse in the last year.”

So if laws can’t help safeguard the Internet, then what can? Clarke believes the answer to safeguarding security lies in authentication. He advocates that ISPs should provide subnets on trusted servers where visitors are authenticated. In an ideal world visitors could surf in a safe environment using universally accepted authentication.

John Fowler, CTO of Sun Microsystems also believes multifactor authentication is the way forward.

However, Fowler believes regulation can’t be given the slip so easily. “Government regulation won’t go away,” he said.

...Continued from front page (bottom)

tery for law enforcement, the Slammer worm's author is also still at large.

It is proving too complicated for law enforcement to track these virus writers because of the fast moving nature of worms, the immaturity of certain forensic techniques and the lack of jurisdiction over the Internet in some countries.

Stephenson said: "Most code contains little or no evidence that can tie a virus to an author. Also a very fast moving virus or worm, by its nature, covers its own tracks simply by the rapidity with which it infects large numbers of computers," he said.

"There is no single country that has jurisdiction over the Internet and the controls and laws from nation to nation can be very different or non-existent."

This makes international cooperation very difficult.

Stephenson believes it is childs play for virus authors to hide their identity to avoid detection.

He said: "They simply need to avoid traceable references that allow a back trace. Also, they need to infect many initial targets at the beginning and launch the infections from a computer or computers that cannot be traced to them. It's trivial to do."

Why virus authors get away:

- Forensic traceback techniques are too immature.
- The international nature of the Internet makes law enforcement difficult over national boundaries.
- Fast moving viruses infect many computers rapidly, making it difficult to trace the alpha victim.

In Brief

FTC SAY DISABLE MS MESSENGER

The US Federal Trade Commission has recommended that Windows Messenger Service should be disabled as it is a channel for marketing pop up ads.

WORLDPAY HIT BY DOS

Worldpay has been hit by a large denial-of-service attack. In a statement, Worldpay said: "Although we have been subject to a 'denial-of service' attack, the integrity and security of our systems and our customers' data is in no way compromised."

AOL TURN OFF MS MESSENGER

Aol has disabled Microsoft Messenger on its customers computers without notifying them. According to a report in the *Associated Press*, AOL has turned off Windows Messenger for 15 million customers.

ORBITZ SECURITY BREACHED

Orbitz, an online travel company, has suffered a security breach, which has allowed spammers to email its customers. Orbitz says a number of its customers has received spam from an authorized source.

AL JAZEERA HACKER SENTENCED

A Web designer has been sentenced to 1000 hours of community service for hacking into AlJazeera.net and redirecting traffic to a website displaying the American Flag.

MICROSOFT DISCLOSE 4 VULNS. IN NOV.

A buffer overflow in the Microsoft Workstation service has been discovered. According to ISS, as the vulnerability is a stack overflow, it is easy to exploit. Windows 2000 and XP are affected. Microsoft has released another three vulnerabilities for November including a cumulative security update for Internet Explorer, a vulnerability in Word and Excel and a buffer overrun in Microsoft FrontPage Server Extensions.

MICROSOFT OFFER SPAM BLOCKING

Microsoft is providing anti-spam technology as an add-on to Exchange 2003. The technology, known as Smartscreen has already been used in Outlook, MSN 8 and Hotmail. The technology works on a classification scheme based on judgements by hundreds and thousands of Hotmail users on what constitutes as spam.

EXPLOIT FOR MS NOV. VULNERABILITY

Exploit code is circulating for a vulnerability in Microsoft Workstation Service (MS03-049) affecting Windows XP and Windows 2000. Microsoft disclosed the vulnerability on 11 November.