

“A Little Neglect May Breed Mischief...”

Rich O’Hanley

Today, Bugbear is on top of the news. It has hit hard and fast (no surprise there) and most, it seems, were stunned (again, no surprise). Yet, various vendors’ reports over recent months have all listed Bugbear among the top-ten threats. Both Symantec and Panda identified Klez.I as 2002’s most virulent malicious code, with Panda reporting Bugbear in second place (see [Exhibit 1](#)). In fact, Symantec reported that in 2002, 80 percent of all malicious code submissions were caused by only three blended threats: Klez, Opaserv, and Bugbear. So, why is everyone surprised that Bugbear has worked its way up the list?

In the May/June issue of *Information Systems Security*, Ken Dunham explained why Klez is still so widespread. Klez was first identified in October 2001. Among the reasons it continues to be so prevalent is that it exploits a known vulnerability in Internet Explorer v 5.01 and v 5.5 without SP2. So, we have a virus that continues to spread because a known upgrade was not installed. What Ben Franklin observed is relevant today:

A little neglect may breed mischief: for want of a nail the shoe was lost, for want of a shoe the horse was lost, and for want of a horse the rider was lost.

The problem of patch and configuration management will continue. It may be just too big a problem to solve by throwing people

and money at it, assuming one has both to expend. So, what is to be done? There is the familiar litany of keeping anti-virus and IDS signatures updated, improving user awareness, keeping track of the legion of vulnerabilities and patches announced each day. So, if this is not working, what will?

In this issue of *Information Systems Security*, Steven Hofmeyr points out that the complexity of information systems gives attackers many ways to exploit weaknesses and unexpected interactions, which makes it difficult for users and administrators to secure the systems effectively. Yet, this problem is similar to that faced by the human immune system (IMS). In “A New Approach to Security: Learning from Immunology,” Hofmeyr explains how the IMS works and demonstrates how we can borrow from the IMS response to threats to improve system security.

VIRUSES ARE NOT THE ONLY THREATS

Trojans horse programs are appearing more often in the wild and are more troublesome than ever before. Even so, most who should know do not fully understand the capabilities, methods, and impact that a Trojan can have on a compromised computer. Unfortunately, most Trojan incidents are never reported, unlike massive worm outbreaks. As a result, thousands of Trojans are successfully deployed against specific targets on a weekly basis. Furthering his mission to

EXHIBIT 1 Monthly Reports of Top Viruses from Security Product Vendors

MailWatch January 2003	Panda February 2003	Panda March 2003	Command Center March 2003	Symantec March 2003	Symantec April 2003	Symantec May 2003
W32/Klez.H	W32/Klez.I	W32/Klez.I	Worm/Klez.E	W32.Klez.H	W32.Klez.H	W32.Klez.H
W32/Sobig	Trj/Pornspa.D	W32/NiceHello	W32/Yaha.E	Backdoor.Dvldr	W95.Hybris.worm	W32.Sobig.B
W32/SirCam	W32/Enerkaz	W32/Enerkaz	Worm/Yaha.M	HTML.Redlof.A	W32.HLLP.Handy	HTML.Redlof.A
W32/Klez.dam	Trj/Pornspa.F	Trj/JS.NoClose	Worm/Avril.B	W95.Hybris.worm	Backdoor.Sdbot	W32.HLLW.Fizzer
W32/Lirva.a	Trj/JS.NoClose	W32/Elkern.C	Worm/Sobig.A	W95.Spaces.1445	W32.Kwbot.C.Worm	W95.Hybris.worm
W32/Yaha.k	W32/Elkern.C	W32/Nimda	Worm/Avril.A	W32.FunLove.4099	W32.Pinfi	W32.HLLP.Spreda
W32/Yaha.g	W32/Klez.C	W32/Klez.C	Worm/BugBear	W32.Nimda.E	W32.Bugbear	W32.Nolor
W32/Bugbear	W32/Bugbear	W32/Bugbear	W32/Funlove	W32.HLLW.Deloder	W32.Gibe.B	W32.HLLW.Lovgate.G
W32/Lirva.c	W32/Nimda	W32/Parite.B	Worm/Yaha.L	W32.Bugbear	W32.Sobig.A	W32.Nimda.E
W32/Lirva.gen	W32/Sobig	W32/Sobig	Worm/Sircam.C	W32.HLLP.Handy	W32.Opaserv.Worm	W32.Pinfi

educate us about malware, Ken Dunham, in “The Trouble with Trojans,” explains what they are and how they work, qualifies the risk of such malicious code attacks, and overviews a common Trojan in the wild today, Assassin.

A NEW SCIENCE OF DIGITAL FORENSICS

Investigators of digital incidents generally think in terms of using digital forensics and the digital investigative process for the purpose of identifying the perpetrator of the incident. However, many organizations today are more concerned with finding out what weaknesses allowed the attack to be successful and identifying effective countermeasures for the future.

This is a specialized branch of digital forensic science that does not necessarily deal with the legal aspects of a digital investigation. In some regards, postmortem analysis must be more rigorous than a typical investigation because the future security of the organization may turn on the outcome. As well, in some cases, insurance settlements may depend on an accurate appraisal of the root cause of the incident and its damage.

In “A Structured Approach to Incident Postmortems,” Peter Stephenson discusses the digital investigative process in light of postmortem analysis, offers a structured approach based on a consensus investigative framework, and suggests cautions that the investigator should keep in mind during the postmortem process.

SECURE E-COMMERCE: AN OXYMORON?

Despite the bad rap E-commerce has received in the aftermath of the dot.com collapse, most businesses today are using the Internet for transactions. This creates a problem of balance. Web technology has enabled many organizations to form an E-enterprise for effective communicating, collaborating, and information sharing. To gain competitive advantages, E-enterprises must integrate entire lines of business operations and critical business data with external organizations or individuals over the Web, which may introduce significant security risks to the organizations’ critical assets and infrastructures. “Building E-Enterprise Security: A Business View” provides a multidimensional E-enterprise security view. This view puts forward practical steps and sustainable solutions for tackling the unique security challenges arising in an E-enterprise environment.

MANAGING UP

Imagine you are the Chief Information Security Officer and your boss, the CIO or CEO, is asking some simple questions: “How secure are our information systems? Is security getting better or worse? How do you know that?” You could describe the successful installation of the newest firewalls, the performance of the intrusion detection systems, the centralized deployment of up-to-date anti-virus solutions, the application of software patches on all network devices, and the popularity of your security awareness program. But that is not

an answer to the questions. Your boss wants to know not only *what* you have done to lower the risk, but also *how effective* you have been. It is all about process, metrics, trend monitoring, and, of course, money.

“Information Security Governance Reporting” presents a framework for information security governance reporting that addresses three primary objectives: to inform, to educate, and to influence top executives. It also describes a set of metrics that was found effective in communicating the status of information security, the high-priority issues, and proposed solutions to continuously improve the security posture of the organization.

The availability of cheap, powerful personal computers has put strong cryptographic systems, which were once restricted to military channels, within the reach of any computer user. Virtually everybody recognizes that there is a legitimate business need for strong cryptographic systems to protect electronic business. Even so, there are concerns that the availability of strong cryptographic systems represents a threat to national security, especially after recent terrorist attacks. The same technology that protects purchasers from fraudulent credit card transactions may also prevent law enforcement officials from learning about criminal activity.

CRYPTOGRAPHY ADVANCES

Cryptography raises concerns about national security and our rights to privacy and freedom of expression. Most Americans have an instinctive distrust of governmental intrusion into their personal activities. Ed Freeman’s column deals with constitutional issues of cryptography and how the courts and Congress are meeting the challenges of the new technology.

Ralph Spencer Poore reports that at the *RSA™ Conference 2003* in San Francisco, the Cryptographers’ Track produced over 400 pages of proceedings representing 28 presentations and more than 60 scholars. Each paper, in turn, referenced, on average, a dozen additional scholarly works. The past few years have seen major advances in

both symmetric key and asymmetric key cryptography. Researchers have developed new cryptographic algorithms and enhanced the efficiency of existing implementations. Cryptanalysts have advanced the state of their art through powerful new analytical methods and more efficient algorithms that leverage the ever-increasing computational power of both stand-alone and distributed systems. In Poore’s opinion, these advances have two important consequences. First, the art and science of cryptography moves in the academic realm at a speed too great for the commercial realm to find useful. Second, the advancement provides exploitation strategies and tools more readily used by those who would break cryptographic security measures than by those who must implement commercially viable cryptographic security measures.

WHO GUARDS THE GUARDS?

Recently, I attended *InfoSecWorld*, sponsored by the MIS Training Institute. Although it was well attended, with a good program, and surprisingly buoyant, given the overall weakness in the economy and the number of our colleagues who are still unemployed, there did not seem to be too much new and exciting on the floor. Now, maybe I am jaded after having attended too many InfoSec conferences, but I do not take that as a good sign. It also seems that the same old problems persist, along with the same solutions, with far too much attention given to perimeter security — keeping the outsiders out — and much too little to internal threats.

Ben Rothke sounds off on one aspect of this in “Who Guards the Computer Security Guards?” This is an important question for anyone involved with information systems and network security. A more meaningful question might be: “How do we know we can trust the internal infosecurity guards?”

TOP ISSUES IN INFORMATION SECURITY

One event at *InfoSecWorld* that set me thinking, however, was a roundtable with CEOs or C-somethings from RSA, ISS, CA, Symantec, and Cisco. Being a publisher,

with long lead times to consider, I was more interested in the future than the present. So, when they presented their list of top information security concerns, I took notes — both to pass on to *you* and to guide *me* in the coming year. Those concerns include:

- IDS and intrusion prevention
- Security knowledge management

- Web services and ID management
- Wireless LAN security
- Creating strong authentication
- Configuration and patch management

Although we have covered many of these areas in the past, upcoming issues of *Information Systems Security* will provide more frequent, in-depth coverage. Stay tuned. ■

THE FORUM ON Information Warfare



The International Leader
in Audit & Information
Security Training

Information Operations 2003

*Government, Military, and Industry's Response
to Emerging Cyber Security Threats*

December 3-4, 2003 *Washington, DC*

Optional Workshops *December 2 & 5*

Vendor Expo *December 3*

FEATURED SPEAKERS

- **Congressman Steve Israel**
- **Kenneth A. Minihan, Lieutenant General, US Air Force (Retired)**
former Director, NSA, DIA; President of the Security Affairs Support Association; Principal, Paladin Capital Group Homeland Security Fund
- **Major General James D. Bryan**
Vice Director, DISA; Commander, Joint Task Force - Computer Network Operations

SPECIAL HIGHLIGHTS

- **Classified Workshop**
(clearance required)
- **War Games Workshop HANDS-ON!**
- **Two Interactive Panel Discussions**
- **Exciting Technology Roundtable**

MIS Training Institute, 498 Concord St., Framingham, MA 01702

www.misti.com E-Z ACCESS IW03