

HNS Newsletter  
Issue 57 -01.04.2001  
<http://net-security.org>  
<http://security-db.com>

This is a newsletter delivered to you by Help Net Security. It covers weekly roundups of security events that were in the news the past week. Visit Help Net Security for the latest security news - <http://www.net-security.org>.

Subscribe to this weekly digest on:  
<http://www.net-security.org/text/newsletter>

Archive of the newsletter in TXT and PDF format is available here:  
<http://www.net-security.org/news/archive/newsletter>

Current subscriber count to this digest: 2139

Table of contents:

- 1) General security news
- 2) Security issues
- 3) Security world
- 4) Featured articles
- 5) Security software
- 6) Defaced archives

General security news  
-----  
-----

#### COMPANIES SEND EMPLOYEES TO 'HACKER' WORKSHOPS

The best way to keep a hacker from breaking into a computer system from the outside may just be to have a hacker on the inside. That's what John Brozycki and Darien Ford's company figured when it paid \$7,000 so they could learn to think like a computer interloper. "Ultimate Hacking: Hands On," a four-day course in Manhattan, gives them a legitimate opportunity to hack their way into computer systems. When they return to their regular jobs, keeping the network secure at a credit union in upstate New York, they'll be much better equipped. "You feel more confident, seeing how many of the exploits are done," Brozycki says, surrounded by fellow techies in a hotel conference room. "Once you see how they're done, you know how to prevent them."  
Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nandotimes.com/technology/story/0,1643,500467285-500714392-503919024-0,00.html>

#### UNCOVERING THE SECRETS OF SE LINUX: PART 2

In an uncharacteristic move, the U.S. National Security Agency recently released a security-enhanced version of Linux - code and all - to the open source community. Part 2 of this developerWorks exclusive delves deeper into the code, dissecting how the security\_av is computed and examining how other SE Linux security features are invoked.  
Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www-106.ibm.com/developerworks/linux/library/s-selinux2/index.html>

## FIREWALLS GO GIGABIT

In an attempt to put load-balancing vendors out of business, both Cisco and CyberGuard Corp. have upped the bandwidth ante by building mind-numbing throughput and performance into new enterprise-level firewalls. Engineered to handle the new wave of high-speed links, both products rise to the task with multiple Ethernet, Fast Ethernet and Gigabit Ethernet interfaces, preventing you from using "the firewall is my bottleneck" as an excuse. Both rack-mountable firewalls come with fail-safe features and various fault-tolerance levels. While they share many of the same capabilities, they differ in ease of configuration, management and performance.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.internetweek.com/reviews01/rev032601.htm>

## MACNN REVIEW: NORTON PERSONAL FIREWALL

In an effort to boost its already strong standing in the field of Macintosh utilities, Symantec last year licensed Open Door Networks' DoorStop software firewall utility, resulting in the creation of Norton Personal Firewall. With the number of broadband Internet connections (which are typically more susceptible to hacking than dial-up connections) increasing daily, as well as the number of intrusions into networks, Symantec is positioning Norton Personal Firewall as the utility of choice for Mac users looking for increased security with their Internet connection, and in doing so is going head-to-head with Intego's already established NetBarrier.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://reviews.macnn.com/reviews/nortonpersonalfirewall/nortonpersonalfirewall.phtml>

## LION VIRUS: HOW TO DETECT AND PREVENT

William Stearns, of the Institute for Security Technology Studies, has written a script called Lionfind to detect Lion. There is no removal program as yet. As prevention, users of BIND 4.9.8 and 8.2.3 distributions should download the latest patch from ISC. Users of the BIND 9.1 distribution should download this update.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2001/12/ns-21832.html>

## 'UNIVERSAL' KEY CLAIMED TO DISABLE MS OFFICE XP SECURITY

"Microsoft's vaunted Product Activation protection technology may not have been fully implemented in Office XP after all. Product keys claimed to be "universal" have been circulating on the Web for some weeks now, and a WinXP beta tester's newsgroup posting forwarded to The Register suggests that use of one of these keys circumvents the activation process. It is not at the moment possible to verify this completely. Warez copies of code claimed to Office XP "final" reportedly run without requiring activation if one of the keys is used, but those keys can't be said to be definitely universal until such time as they can be tested on production copies of Office XP sold at retail."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/4/17869.html>

## NOT ENOUGH PROTECTION

A majority (60%) of Canadians feel not enough is being done to protect Internet consumers against cyber crime, and over half (52%) feel threatened

or concerned by this activity, a new poll released by EDS Canada indicates.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newswire.ca/releases/March2001/26/c6703.html>

#### UN TO DEVISE STRATEGY FOR GLOBAL E-SECURITY

Delegates from the United Nations' 189 member countries this week will meet with representatives from the U.S. high-tech industry to devise new strategies for dealing with Internet crime and global e-commerce security requirements. However, to ensure a coherent global strategy, world leaders must be better educated about the need for global security standards and the threat that cybercrime poses to the global economy, said Percy Mangoaela, the UN ambassador from Lesotho.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/cwi/stories/0,1199,NAV47-68-84-88\\_STO58959,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/cwi/stories/0,1199,NAV47-68-84-88_STO58959,00.html)

#### HACKERS CLAIM DOUBLECLICK SECURITY HOLES

Data-collection company DoubleClick returned to the privacy spotlight after a French Web site uncovered evidence indicating several of the company's servers had security holes and may have been breached.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1003-200-5252461.html>

#### PRIVACY GROUP CRITICIZES TIVO FOR COLLECTING INFO

The leading TV recording service has collected information about viewers - programs watched or recorded, remote control buttons pushed - without adequately informing them, a research group says. The Privacy Foundation was warning about the practice in a report Monday on the personalized TV system, which makes it easier for consumers to record and watch their favorite programs. Analysts expect 14 million people to be using such video recorders by 2004.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2001/TECH/industry/03/26/tv.privacy.ap/index.html>

#### HACKER NATION

Computer intrusions have more than tripled in the last two years. Who are the people trying to get their hands on your data, and why? We got answers from some experts - including hackers themselves.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.pcworld.com/features/article/0,aid,44544,00.asp>

#### LESSONS IN LAPTOP SECURITY

The laptop is not only a teleworker's power tool. It's a thief magnet. Securing confidential or proprietary data when you're on the road or you work beyond the enterprise is a pressing issue. Think this is someone else's problem? Think again. In the U.S. in 1999, 319,000 notebook computers and 27,000 desktop computers valued at close to \$1 billion were stolen, according to Safeware, the Columbus, Ohio computer insurance agency.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nwfusion.com/net.worker/columnists/2001/0326zbar.html>

#### HACKING DANGER GROWS IN AUSTRALIA

Australia has experienced an increase in hacker attacks, with 22 web page defacements this year alone (?), according to Ernst & Young eRisk Solutions principal Eric Keser.

Link: [http://finance.news.com.au/common/story\\_page/0,4057,1838561%255E462,00.html](http://finance.news.com.au/common/story_page/0,4057,1838561%255E462,00.html)

#### ANTIGEN FOR LOTUS NOTES

Antigen is the anti-virus solution specifically designed to meet the security needs of Lotus Notes users. It detects and removes viruses, including Notes based viruses-before they reach mission-critical applications, and without compromising the integrity of your groupware servers.

Link: <http://www.security-db.com/product.php?id=46&cid=10>

#### HOW TO AVOID GIVING FREE INFORMATION TO ATTACKERS

This paper by Richard Bartley of Xinetica Ltd. explores techniques for the exploitation of corporate information that attackers may use to attack an organization. It focuses on what strategies an organization can implement to minimize the unnecessary disclosure of potentially dangerous information.

Link:

[http://www.securityfocus.com/templates/forum\\_message.html?forum=2&head=5144&id=5144](http://www.securityfocus.com/templates/forum_message.html?forum=2&head=5144&id=5144)

#### COMPARISON OF CLIENT METHODS TO BLOCK SPAM

"How do people deal with spam? While there are methods to address UCE at the server, legal, and mail client levels, the individual has only one way to deal with spam: through their mail client software. In this article, I will introduce various means of combatting junk email."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.unixreview.com/administration/articles/0103wa.shtml>

#### SAMBA NT DOMAIN CONTROLLER

Currently, Samba can go beyond merely emulating Windows shares to actually acting as the Primary Domain Controller for your Windows network. Of course, Samba can also become a NT domain member. In this article we shall look at both these options.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.freeos.com/articles/3842/>

#### ENCRYPTING AN ACCESS DATABASE

You might feel discouraged and ask yourself, "Why bother with security?" Do not despair! Fortunately, Access enables you to encrypt a database. The encryption process renders the data in the database indecipherable from data in word processors, disk utilities, and other products capable of reading text. When a database is encrypted, no one can decipher any of its data.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://softwaredev.earthweb.com/devtools/article/0,,12061\\_724731,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://softwaredev.earthweb.com/devtools/article/0,,12061_724731,00.html)

#### REMOTE USERS NEED FIREWALLS TOO

Last December, a bank in Southern California received a call from an online customer asking why one of the bank's computers was trying to hack into his system. It turned out that the machine doing the hacking belonged to the bank's president and had been remotely commandeered by an employee.

The president called Congquest Inc., an IT security services firm, which is now rolling out firewall software across the bank's 125 internal desktop, laptop and remote computers. Until recently, companies thought antivirus and VPN technologies would keep remote worker connections safe. But as more workers have been accessing the Internet through broadband services such as cable modems, exposure to hacking attacks through those machines has increased.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.itworld.com/Sec/2211/CWD010326firewalls/>

#### EMAIL FILTERING: THE REAL DEAL

"Email is probably my favorite Internet related service. It's also the one that causes me the most problems, with regard to security. People cannot live without email anymore. Email is probably the most convenient form of communication for most of us. It's an easy way to figure out whether the person you want to phone in Australia is awake or not. Email also allows us to easily send files, from simple text documents to spreadsheets - images to video clips. There are extremely few companies and organizations in the world that have an Internet connection but do not use email. Because of this, most Internet spam is now delivered by email, and more importantly, most viruses are now spread via email."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/closet/closet20010328.html>

#### A VIRUS THAT LEAPS PLATFORMS

A security company has identified what is believed to be the first virus with cross-platform abilities - it can infect both Windows and Linux operating systems. W32.Winux is not affecting many computers, nor is it apt to spread quickly, as people do not tend to share executable programs between machines running Linux operating systems and machines running Windows operating systems. Also called "Linux.Winux," W32.Winux is a non memory resident virus. It can replicate under Windows 95/98/Me/NT/2000 and Linux operating systems and it infects EXE (Windows executable) and ELF files (Linux executable). The infection method is not sophisticated. The virus overwrites the ". reloc" section of Windows executable files. If the .reloc section size is not large enough to hold the virus body, the file is not infected. It does not destroy data but can impact an infected machine's performance due to the background activity of the virus.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://wired.lycos.com/news/technology/0,1282,42672,00.html>

#### SECURITY BREACHES IN IT DIVISIONS

More than 35% of IT departments have experienced unauthorised access to computer systems, with half of the incidents made up of internal breaches, a survey has found.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://it.mycareer.com.au/networking/20010328/A32550-2001Mar28.html>

#### SECURITY SOLUTIONS IN THE REAL WORLD

The most secure computer system is the one that's unplugged and buried 10 feet underground, according to security expert Paul Raines. But there are specific steps a company can take to reduce security threats to their live systems - whether from external hackers or disgruntled IT workers. Raines,

head of global information risk management for Barclays Capital, laid out those steps to security professionals here at the eSecurity Conference & Exposition in his session entitled, "Security In the Real World."

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.networkweek.com/wire/story/TWB20010328S0007)

[bin/news.cgi?url=http://www.networkweek.com/wire/story/TWB20010328S0007](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.networkweek.com/wire/story/TWB20010328S0007)

#### EXPERTS DEBATE SEVERITY OF 'WINUX' VIRUSS

Even though there have been no reported cases of infection by the virus - which is incapable of spreading itself via the Internet or e-mail - some anti-virus vendors hailed the program, known variously as "Winux" and "Lindose," as marking the beginning of a new era of virus writing. "It's only interesting in the sense that it shows virus writers are becoming more interested in Linux," said Graham Cluley, senior technology consultant at Sophos Inc., a British anti-virus vendor with U.S. headquarters in Wakefield, Mass. "It's very simple and not likely to spread on any big scale. Its real effect is wasting people's time."

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/eweek/stories/general/0,11011,2702054,00.html)

[bin/news.cgi?url=http://www.zdnet.com/eweek/stories/general/0,11011,2702054,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/eweek/stories/general/0,11011,2702054,00.html)

#### CHECK POINT FIREWALL-1 ON LINUX, PART THREE

This is the third and final article in a series devoted to the exploration of Check Point Firewall-1 for Linux. In the first article we discussed single and multisystem installation and post-installation tasks. The second article explored Firewall-1 concepts such as network objects, firewall rules, address translation rules, and NAT, as well as features and limitations of Firewall-1. In this installment, we will go over aspects of Firewall-1 such as file and directory layout, rulesets, migrating existing Firewall-1 installations to Linux, and backup and standby configurations.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/linux/articles/checkpoint3.html)

[bin/news.cgi?url=http://www.securityfocus.com/focus/linux/articles/checkpoint3.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/linux/articles/checkpoint3.html)

#### SUEXEC KEEPS YOU IN CONTROL OF YOUR SYSTEMS

One of the biggest problems for both Web hosting providers and clients is server security. How do you provide a flexible server environment for the client while maintaining some level of security? In this article, Jamie Wilson explains how the Apache Web server and the suEXEC module make that possible.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.unixinsider.com/unixinsideronline/swol-03-2001/swol-0323-suexec.html)

[bin/news.cgi?url=http://www.unixinsider.com/unixinsideronline/swol-03-2001/swol-0323-suexec.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.unixinsider.com/unixinsideronline/swol-03-2001/swol-0323-suexec.html)

#### GETTING STARTED WITH NETWORKING FOR LINUX

Josh Boudreau writes a great tutorial on setting up a network with Linux, all the way from the various networking layers to running telnet and ftp on your Local Area Network (LAN).

Link: <http://www.linux.com/firststep/newsitem.phtml?sid=1&aid=11991>

#### REVIEWING YOUR X WINDOW SECURITY

"In this article we've shown you how insecure X communication can be and what to do in order to provide safe X client-server communication. Depending on the level of security you need to implement, use xhost, xauth or Secure RPC X authentication methods. But no matter what, make sure you implement

some form of security. Protect your own X server!"

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.elementkjournals.com/sun/0104/sun0141.htm>

#### WELSH HACKER FACES JAIL SENTENCE

A hacker who was tracked down to his home in a tiny village in Wales has admitted to hacking into websites between February and March last year for his own gain and may now face a jail sentence. In a pre-trial hearing in court yesterday, 19-year-old computer science student Raphael Gray admitted hacking into the websites of companies such as nettrading, salesgate, feelgoodfalls, mostorefront, albionsmo and the American Society of Clinical Pathologists. He also admitted to stealing credit card information from the exploited sites, using the details for his own gain and offering to supply them to other criminals.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://thebusiness.vnunet.com/News/1119903>

#### DEVELOPING A SUCCESSFUL INFORMATION SECURITY PROCESS

Part of any organization's information security program for protecting enterprise components and the information supporting business functions is the risk assessment process implemented and actually followed by that organization. Assessment results must provide cost-effective and management-approved corrective actions that mitigate potential risks down to an acceptable level for network operation and business function.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/risk20010329.html>

#### CONSIDERATIONS OF A FIREWALL: PART 1

If you're upgrading your firewall, or installing one on your network for the first time, you'll discover that firewall technology has changed a lot in the last several years. How do you select one that's appropriate for your business?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnetasia.com/biztech/security/story/0%2C2000010816%2C20192642%2C00.htm>

#### THE APRIL FOOLS 2001 BUG IN WINDOWS

There is a time-related bug in Windows. It turns out the bug is going to hit on this Sunday (01.04.2001). Applications built with certain versions of Visual C++ could start giving the wrong time of day starting on Sunday. The problem will last for a week.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://msdn.microsoft.com/visualc/headlines/2001.asp>

#### SUSE: KERNEL BACKDOOR (APRIL FOOL'S JOKE)

Roman Drahtmüller send this message to the suse-security-announce mailing list in regards to an April Fools joke that some people are taking a little bit too seriously...

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxsecurity.com/articles/hackscracks\\_article-2767.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxsecurity.com/articles/hackscracks_article-2767.html)

#### WAR DRIVING - THE LATEST HACKER FAD

The introduction of wireless networking has spawned a fresh sub-culture in the digital underground. It has brought script kiddies out of their bedrooms and onto the roads. War dialling, the hacking practice of phoning up every extension of a corporate phone network until the number associated with a firm's modem bank is hit upon, has been replaced by war driving with the introduction of wireless LANS. Our source tell us that war driving, which is apparently particular popular in Silicon Valley, involves motoring between likely target firms with a PC fitted with a LAN card and trying to break into their networks. Given the flakey state of wireless security models this is normally childishly simple with even basic cracking tools.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17976.html>

#### CEBIT - HACKERS GIVE SIEMENS NET FILTER MOCK 'AWARD'

The German hackers' group Chaos Computer Club (CCC) has presented its annual satiric Chaos CeBIT Award, at the CeBIT 2001 trade show, to Siemens AG for the company's "SmartFilter" software. The group said it was honoring Siemens's "special services" in the area of "Internet censorship and obstacles to communication." SmartFilter is a Web filtering tool based on a "control list" of Web site categories and blocked sites. The software is implemented on Siemens's internal servers, and is also available for sale to external customers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2001/TECH/industry/03/29/cebit.hackers.award.idg/index.html>

#### THE SECURITY IMPLICATIONS OF OPEN SOURCE SOFTWARE

Natalie Whitlock talks about the incongruence of closed security systems, and the open source solution. She discusses Eric Raymond's ideas, the famous "back door" in Microsoft's FrontPage, the concept of peer review, and the open source dilemma that no one is at the helm guaranteeing that everything will be checked. She then follows the idea from theory to practice and talks with leading IT executives about the viability and popularity of secure open source systems.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www-106.ibm.com/developerworks/linux/library/l-oss.html>

#### COPS NAB FIRST ITALIAN VIRUS SUSPECT

Italian police have arrested a man suspected of writing the Vierika computer virus, similar to the Kournikova virus which overloaded computer systems around the world last month. The man is believed to be the first Italian charged with virus writing. In a twist, however, Vierika is not believed to have caused much damage. Industry experts said the Italian authorities appear to be making an example out of the suspect, to discourage other virus writers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2001/12/ns-21943.html>

#### ENGARDE SECURE LINUX AVAILABLE FOR DOWNLOAD

EnGarde improves the security of existing versions of Linux in critical areas with advanced forms of data integrity management and assurance, a complete suite of e-business services, intrusion alert capabilities, improved authentication and access control utilizing strong cryptography, and complete SSL secure web based administration capabilities. Users familiar with the history of Linux have

become accustomed to its stability, versatility, and scalability. Now, with EnGarde, Guardian Digital has added unsurpassed security.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.engardelinux.com/announce.html>

#### HACKERS WORSE THAN TERRORISTS - ROBIN COOK

Hackers are a greater threat than terrorists, Foreign Secretary Robin Cook reckons. Speaking in Parliament yesterday, he said that a "computer-based attack could cripple the nation more quickly than a military strike". Cook made the claims in a debate on the work of the intelligence services. But where have we heard these claims before? Ah, yes the US National Security Agency, whose director Air Force General Michael Hayden said last November: "The virtual battlefield has "taken on a dimension within which we will conduct operations to ensure American security."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17986.html>

#### OPENHACK: DID HE WIN OR NOT?

A hacker is claiming that he has won Argus' ballyhooed OpenHack III competition by cracking its much-vaunted PitBull security system. Argus concedes the crack, but isn't awarding the promised big cash prize. The same challenge was offered at the European technology conference CeBit this week. This time, one person says he was able to crack the system. But he evidently missed the deadline. A hacker calling himself Bladez won't receive the \$4,250 prize offered by Argus because he says he misunderstood what time the competition ended and was under the impression that he had a few hours left to work. Bladez said that he is worried that Argus Systems will hail the CeBit competition as another success or "will simply stay quiet and thrive off their OpenHack coverage. In fact, an Argus Systems employee told me there would probably be no press release, though it wasn't clear if this was because of my hack or not."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,42747,00.html>

#### DON'T BE A FOOL

Be sure to update your software and be ready for hoaxes and bugs this April Fool's Day! Every year, users fall victim to pranks or malware attacks.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/fool20010330.html>

#### ENGARDE SECURE LINUX QUICK START

This EnGarde Quick Start guide is designed to help you quickly set up EnGarde Secure Linux, change user passwords, and manage certificates. Although this document is sufficient, we recommend you read the complete user manual for a full understanding of the system. EnGarde Secure Linux comes with an easy to use front-end for installing the operating system. Described in the following sections are the system requirements to successfully complete the installation and run EnGarde Secure Linux.

Link: <http://ftp.engardelinux.org/pub/engarde/1.0.1/docs/ESLQuick-1.0.1.pdf>

## HACKERS: CORPORATE SECURITY STINKS!

Companies are paying more attention to safeguarding their digital assets, but the overall state of corporate data security is still poor, said hackers and security experts attending the CanSecWest conference.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.msnbc.com/news/552177.asp>

## SYSTEM ADMINISTRATION OF APACHE / TOMCAT

Learn all about the pros and cons of JSP web applications at the sysadmin level, including installation and configuration of Apache /Tomcat. This article will give you the basics on object-oriented development efforts, making scaling of your Web site a simple process. Jump into the world of Java Servlets and JSP with Linux!

Link: <http://www.linux.com/sysadmin/newsitem.phtml?sid=1&aid=11992>

---

## Security issues

All vulnerabilities are located at:  
<http://net-security.org/text/bugs>

---

## ELRON IM PRODUCTS VULNERABILITY

At least two products of the Elron Internet Manager family of tools contain directory traversal vulnerabilities. The problem exists in the following products:

- IM Message Inspector
- IM Anti-Virus

Elron Internet Manager products that are not vulnerable are:

- IM Firewall

If the IM Web Inspector comes with Elron Software's proprietary web server as well, it is undoubtedly vulnerable as well.

Link: <http://www.net-security.org/text/bugs/985571836,4823,.shtml>

## AKOPIA INTERCHANGE E-COMMERCE PROBLEMS

A serious security vulnerability has been found in the default installation of the Interchange demo stores 'barry', 'basic', and 'construct' distributed in Interchange versions 4.5.3 through 4.6.3. Using a group login that had no password set by default, it is possible to log in to the back-end administration area and view and alter products, orders, and customer information.

Link: <http://www.net-security.org/text/bugs/985571971,72095,.shtml>

#### ILMI COMMUNITY IN OLICOM/CROSSCOMM ROUTERS

Crosscomm/Olicom routers have a undocumented community string ILMI (yes, the same as in cisco :) that has read and write permissions (i didn't check the whole tree, but you can set system.sysContact.0 for example). This was checked on a XLT-F router with software 'XL 80 IM Version 5.5 Build Level 2' (this was what it reported via snmp).

Link: <http://www.net-security.org/text/bugs/985632784,11513,.shtml>

#### MDAEMON IMAP DENIAL OF SERVICE

Some of the commands for the IMAP server do not have proper bounds checking, enabling a user to shutdown the service remotely. It should be noted that a user account is required. The commands affected are SELECT and EXAMINE. The SELECT command selects a mailbox so that messages in it can be accessed. EXAMINE works in the same way as SELECT, however the mailbox is marked as read- only and cannot be modified.

Link: <http://www.net-security.org/text/bugs/985632878,8973,.shtml>

#### RAPTOR 6.5 HTTP VULNERABILITY

The Raptor firewall is vulnerability for forwarding http request on other port numbers than 80, if a rule allows http traffic. Redirect rules does not affect this problem. When an extern or internal client, configures itself to use the nearest interface as proxy, it's possible to access other ports that 80 on the target host.

Link: <http://www.net-security.org/text/bugs/985632976,78240,.shtml>

#### BEA WEBLOGIC UNICODE DIRECTORY BROWSING

By requesting a URL and ending it with one of the following unicode representations: %00, %2e, %2f or %5c, it is possible to bypass the listing of the default document (eg. index.html) and browse the content of the web folders.

Link: <http://www.net-security.org/text/bugs/985658808,90631,.shtml>

#### PROBLEMS WITH WEBLOGIC 4.5.1 AND 5.1

It is interesting to note that similar (in fact, worse) behaviour is exhibited in both Weblogic 4.5.1 and 5.1. Appending a '%00' to the end of a .jsp request retrieves the source of the jsp.

Link: <http://www.net-security.org/text/bugs/985694957,71506,.shtml>

#### LINUX MANDRAKE - OPENSSH UPDATE

There are several weaknesses in various implementations of the SSH protocols. When exploited, they let the attacker obtain sensitive information by passively monitoring encrypted SSH sessions. The information can later be used to speed up brute-force attacks on passwords, including the initial login password and other passwords appearing in interactive SSH sessions, such as those used with su. Versions of OpenSSH 2.5.2 and later have been fixed to reduce the impact of these traffic analysis problems, and as such all Linux- Mandrake users are encouraged to upgrade their version of openssh immediately.

Link: <http://www.net-security.org/text/bugs/985695208,67583,.shtml>

#### ANACONDA CLIPPER VULNERABILITY

Comment: '.' and '/' are not filtered while processing user input, so it is possible to enter arbitrary values to retrieve files from remote sever, which should not be accessible normally (for ex., /etc/passwd).

Link: <http://www.net-security.org/text/bugs/985727518,50822,.shtml>

#### SOLARIS /USR/BIN/TIP VULNERABILITY

The tip program is installed setuid uucp by default in Solaris, it contains a vulnerability in handling data from environment variables, if this variable exceeds predefined length an exploitable stack overflow can occur.

Through exploiting this vulnerability an attacker can gain effective uid uucp and through that root.

Link: <http://www.net-security.org/text/bugs/985727795,52777,.shtml>

#### IMMUNIX OS SECURITY ADVISORY: KERNEL

The 2.2.19 kernel release fixes numerous security problems including the ptrace/execve race condition bug that was reported by Wojciech Purczynski.

Link: <http://www.net-security.org/text/bugs/985781896,12557,.shtml>

#### CONNECTIVA LINUX - LICQ UPDATE

"licq" is a very popular ICQ graphical client. Previous versions have two vulnerabilities that could be exploited by a remote attacker to execute arbitrary commands on the client host. The first vulnerability is a buffer overflow in a log function. The second vulnerability consists in the use of the system() function to invoke an external browser when an URL is received. This function will expand and interpret shell characters and this could be used to execute commands on behalf of the user running licq.

Link: <http://www.net-security.org/text/bugs/985781950,25662,.shtml>

#### LINUX MANDRAKE - VIM UPDATE

Users could embed malicious VIM control codes into a file, and as soon as any user opened that file in vim-enhanced or vim-X11 with the status line option enabled in .vimrc, the commands would be executed as that user.

Link: <http://www.net-security.org/text/bugs/985781974,91775,.shtml>

#### SONICWALL IKE PRE-SHARED KEY LENGTH BUG

The limitation of using only a 48 byte key as opposed to using a full 128 byte key degrades the overall security of the firewall.

Link: <http://www.net-security.org/text/bugs/985782130,58962,.shtml>

#### SYMANTEC RESPONSE REGARDING RAPTOR BUG

The first point we would like to make is that although we do agree with the authors as it relates to the security implication of the described HTTP functionality we do not accept the assertion that this is a product related issue with the Raptor Firewall (HTTP proxy). Rather, our Raptor Firewall HTTP proxy is RFC-compliant, and as such it is behaving consistently with the specification as described in RFC 2616. From a pure protocol perspective, this is a valid HTTP connection and thus the traffic is being allowed through the firewall with a proper rule. However, recognizing the security impact of this configuration, the Raptor Firewall provides you with the capability to shut down this functionality by setting a configuration option (http.noproxy)

through our configuration files or the RMC.

Link: <http://www.net-security.org/text/bugs/985782335,57110,.shtml>

#### PROBLEMS WITH DCOM VB T-SQL DEBUGGER

Microsoft Developer Studio version 6 installs a world-launchable DCOM object, known as the VB T-SQL Debugger, which contains an exploitable buffer overflow.

Link: <http://www.net-security.org/text/bugs/985782436,4158,.shtml>

#### MYSQL 3.23.36 FIXES SECURITY HOLES

This release should fix the final bugs we accidentally got into 3.23.34 and a long security bug that has been in MySQL a long time! The main fixed bugs are that UPDATE didn't always use keys when updating on something not based on a primary key and that 'affected rows' wasn't returned to the client if the mysql server wasn't compiled with support for transactions.

Link: <http://www.net-security.org/text/bugs/985782554,94105,.shtml>

#### VPN3000 CONCENTRATOR TELNET VULNERABILITY

Sending a flood of data to the SSL or regular telnet port can cause the Cisco VPN 3000 series concentrators to reboot. After rebooting, the equipment would function normally until the flood of data is sent again. To remove the vulnerability, Cisco is offering free software upgrades to revision 3.0.00 for all affected platforms. The defect is described in DDTs record CSCds90807.

Link: <http://www.net-security.org/text/bugs/985819001,59759,.shtml>

#### INFRAMAIL DENIAL OF SERVICE VULNERABILITY

There exists a parsing problem in the handling of 302 pages by the server serving both the webpages and the administration interface for the members of the Inframail product family. This allows for a DoS against the system through a malformed POST request consisting of a space followed by a long string (276 bytes or more) of characters. The running services will freeze and the program will need to be restarted to regain full functionality.

Link: <http://www.net-security.org/text/bugs/985819085,68042,.shtml>

#### SOLARIS 2.7 + IBM WCS 4.0.1 VULNERABILITY

Follow URL insert "/" will be downloading ".jsp" source.

Link: <http://www.net-security.org/text/bugs/985879982,82795,.shtml>

#### TOMCAT 3.0 FOR WIN2000 VULNERABILITY

A security vulnerability has been found in Windows NT/2000 systems that have Tomcat 3.0 installed. The vulnerability allows remote attackers to access files outside the document root directory scope.

Link: <http://www.net-security.org/text/bugs/985880053,23891,.shtml>

-----

Security world  
-----

All press releases are located at:  
<http://net-security.org/text/press>

-----

#### COVERT LABS ON INVALID CERTIFICATES - [26.03.2001]

McAfee AVERT (Anti-Virus Emergency Response Team) in conjunction with COVERT Labs (Computer Vulnerability Emergency Response Team) at PGP Security, divisions of Network Associates, Inc. advised computer users of recently discovered invalid digital certificates issued by VeriSign to an unidentified person posing as a Microsoft employee. The digital certificates, which normally are used to verify authorized issuers, could be used to authenticate viruses and malicious code. AVERT and COVERT report that no damage has been associated with the fraudulent certificates.

Press release:

< <http://www.net-security.org/text/press/985572246,4935,.shtml> >

-----

#### TEMPEST SOFTWARE SHIPS SITESHIELD - [26.03.2001]

Tempest Software, Inc. a premier provider of technology and products that facilitate secure, standards-based information exchange over the Internet, announced it is shipping Version 2 of SiteShield, the new "plug and play" software solution to secure websites. Based on Tempest's solid, proven technology, SiteShield protects all applications, data and information assets on a web server by keeping it securely behind a firewall closed to all incoming traffic. SiteShield addresses the need for e-business openness while protecting companies against potentially embarrassing and destructive hacking and security lapses.

Press release:

< <http://www.net-security.org/text/press/985633090,77204,.shtml> >

-----

#### CISCO SYSTEMS AND MICROSOFT PARTNER - [26.03.2001]

Cisco Systems, Inc. announces the first implementation of the 802.1x draft security standard shipping on its Cisco Aironet 350 Series of Wi-Fi (IEEE 802.11b) compliant wireless local area networking (WLAN) products. Cisco collaborated with Microsoft to develop, deliver and deploy the first enterprise authentication and security architecture based on the in progress Institute of Electrical and Electronics Engineers 802.1x and Extensible Authentication Protocol (EAP) standard. Through this cooperative effort between Cisco and Microsoft, enterprises can, for the first time, scale wireless deployments to thousands of users with a standard, centralized security management framework while streamlining network management and administration.

Press release:

< <http://www.net-security.org/text/press/985633141,91936,.shtml> >

---

SECURITYFOCUS' ARIS ANALYZER - [26.03.2001]

SecurityFocus.com is proud to announce ARIS (Attack Registry and Intelligence Service) Analyzer. The ARIS Analyzer is a free service that allows you to submit attack data collected by intrusion detection systems and helps you manage your security incidents. ARIS Analyzer also allows you to correlate your attacks with those seen by other people.

Press release:

< <http://www.net-security.org/text/press/985633561,34135,.shtml> >

---

SECURING NEW MICROSOFT TECHNOLOGY CENTER - [27.03.2001]

Rainbow Technologies, Inc., a leading provider of high-performance security solutions for the Internet and eCommerce, and iVEA Technologies, a Rainbow Technologies company, announced that Microsoft Corp. will feature Rainbow's iKey workstation security solution and iVEA's CryptoSwift eCommerce accelerator as critical components for the new Microsoft Technology Center - Silicon Valley (MTC-SV), opening in Mountain View, California. Rainbow and iVEA products are currently used in MTCs in Waltham, Mass. and Austin, Texas. The MTC-SV is a working lab dedicated to the development and rapid deployment of eCommerce solutions to both startups and established business-to-business (B2B) companies.

Press release:

< <http://www.net-security.org/text/press/985694527,1979,.shtml> >

---

SECURING ANY MESSAGING ENVIRONMENT - [27.03.2001]

Addressing the increasing need for secure messaging networks, Mirapoint, a leading provider of Internet messaging infrastructure products, was announced the release of the Mirapoint Message Director, the first system optimised for securing any messaging environment. The Message Director is a scalable and easy to deploy messaging solution that can be added to any enterprise or service provider messaging environment. BMW Group is the first customer of the Message Director and will use the new product to increase message security, management and performance.

Press release:

< <http://www.net-security.org/text/press/985694688,65075,.shtml> >

---

SYGATE PERSONAL FIREWALL 4.0 ANNOUNCED - [28.03.2001]

Sygate Technologies, a leading provider of Internet security software solutions, announced the release of Sygate Personal Firewall 4.0, the first personal firewall software that combines firewall and intrusion defense technologies to deliver comprehensive security and ease of use for home and small businesses. As a firewall, Sygate Personal Firewall 4.0 controls access to communication ports and monitors any port-scanning activity. As an intrusion defense agent, it only allows trusted communication and considers any other network activity `guilty`

until proven innocent.' As a result, Sygate Personal Firewall 4.0 secures computer systems, without the obtrusive and irrelevant alerting characteristics of other security solutions. When attacks do occur, Sygate Personal Firewall 4.0 offers forensic capabilities allowing users to find the source of intrusion and take appropriate action.

Press release:

< <http://www.net-security.org/text/press/985744343,74897,.shtml> >

---

#### NETWORK ICE WINS 'BEST OF SHOW' - [28.03.2001]

Network ICE, a leading provider of intrusion detection and protection for enterprises and consumers, won "Best of Show" at Upside Events' Preview Spring 2001 in Beverly Hills, Calif. Undercover journalists at the March 13 competition scored and ranked nearly 20 invited-only companies on innovation, user-friendliness and potential benefit to customers. ICEpac Security Suite, Network ICE's enterprise product, beat nearly 20 companies that demonstrated their latest products and technologies. ICEpac uses Network ICE's patent-pending BlackICE technology to detect, identify and block hackers' Internet attacks before they can compromise a system. The ICEpac suite is designed to protect an entire corporation's network including remote VPN users. It uses one of the most advanced intrusion detection technologies to single out hackers and stop them from breaking into your network or stealing valuable information assets.

Press release:

< <http://www.net-security.org/text/press/985744438,94075,.shtml> >

---

#### COMPUTER WORMS: FLASHBACK TO EARLY 90S? - [28.03.2001]

With more than two thousand new computer viruses rearing their ugly heads each month, it's the worms among them that keep "hacker trackers" up at night. Unlike simple viruses, which spread from file to file in one computer, worms live short but spectacular lives, inflicting major damage quickly because they use the network to spread from computer to computer. Now that network operating systems have been available for some time, there is mounting concern among Internet security experts that the ever increasing availability of information on the "guts" of network operating systems gives hackers clues to break in and compromise a network's security.

Press release:

< <http://www.net-security.org/text/press/985744630,4514,.shtml> >

---

#### CENTRAL COMMAND DISCOVERS W32.WINUX - [28.03.2001]

Central Command, a leading provider of PC anti-virus software and computer security services, and its partners announced the discovery of W32.Winux, the world's first cross platform virus capable of infecting computers using both the Microsoft Windows and Linux operating systems. "Today with the discovery of W32.Winux, we have received the world's first known virus capable of spreading on both Windows and Linux computer systems. While

people do not share executables between these operating systems, this new proof of concept virus represents a technology innovation that may lead to more destructive viruses in the future. Our Emergency Virus Response Team discovered this new virus and has analyzed it," said Steven Sundermeier, Product Manager at Central Command Inc.

Press release:

< <http://www.net-security.org/text/press/985783671,65011,.shtml> >

-----

#### FORENSICS EXPLORERS INTRODUCES NETINFORMANT - [30.03.2001]

Forensics Explorers introduces NetInformant, a suite of products that go far beyond other network security systems and solves problems most network security software cannot even detect. In addition, NetInformant is the only network security system that can guard against the most dangerous and difficult to detect threats: threats from an organizations trusted employees, clients and strategic partners, the people who operate behind the firewall. While most network security software merely tracks network activity and compares it to a list of known security risks, or calculates whether specific activity is statistically unusual, NetInformant audits and evaluates all network activity, flags network security management when potential client-specified issues arise, and produces action items which can be implemented immediately.

Press release:

< <http://www.net-security.org/text/press/985912691,88510,.shtml> >

-----

## Featured articles

---

All articles are located at:  
<http://www.net-security.org/text/articles>

Articles can be contributed to [staff@net-security.org](mailto:staff@net-security.org)

Below is the list of the recently added articles.

---

### TRACKING SPYWARE AND PROBES by M. E. Kabay

"I'd like to share with you a recent exchange I had with a friend of mine whose system seems to have been infected with spyware. Hopefully, this case study will help you when you examine your own systems."

Read more:  
< <http://www.net-security.org/text/articles/nwf/tracking.shtml> >

---

### TESTING PATCHES by M. E. Kabay

There are many firms, including AtomicTangerine, which can carry out penetration tests to verify that patches are up to date and functioning. Just be sure that you obtain contractual confirmation that the firm does not hire criminal hackers. The last thing you need is to have untrustworthy people testing your security.

Read more:  
< <http://www.net-security.org/text/articles/nwf/testing.shtml> >

---

### HTML MAIL THREATENS PRIVACY by M. E. Kabay

The threat to privacy from Big Brother (governments) sometimes overshadows the equal threat from "Little Brother" (industry).

Read more:  
< <http://www.net-security.org/text/articles/nwf/html.shtml> >

---

## Security Software

---

All programs are located at:  
<http://net-security.org/various/software>

---

### LIONFIND 0.1

Lion is a new worm, that is very similar to the Ramen worm. However, this worm is much more dangerous and should be taken seriously. It infects Linux machines with the BIND DNS server running. It is known to infect BIND version(s) 8.2, 8.2-P1, 8.2.1, 8.2.2-Px. BIND 8.2.3-REL and BIND 9 are not vulnerable. The BIND vulnerability is the TSIG vulnerability that was reported back on January 29, 2001. SANS developed a utility called Lionfind that will detect the Lion files on an infected system. Simply download it, uncompress it, and run lionfind. It will list which of the suspect files is on the system.

Info/Download:

< <http://www.net-security.org/various/software/985822791,25782,linux.shtml> >

---

### CHKROOTKIT 0.30

chkrootkit is a tool to locally check for signs of a rootkit. It contains:

chkrootkit: shell script that checks system binaries for rootkit modification.  
The following commands are examined:

basename, biff, chfn, chsh, cron, date, dirname, du, echo, env, find, fingerd, grep, identd, ifconfig, inetd, killall, login, ls, mail, netstat, passwd, pidof, pop2, pop3, ps, pstree, rpcinfo, rshd, sendmail, sshd, su, syslogd, tar, tcpd, telnetd, timed, top, traceroute, write

ifpromisc.c: checks if the interface is in promiscuous mode.  
chklastlog.c: checks for lastlog deletions.  
chkwtmp.c: checks for wtmp deletions.  
chkproc.c: checks for signs of LKM trojans.

The following rootkits and worms are currently detected:

Irk3, Irk4, Irk5, Irk6 (and some variants);  
Solaris rootkit;  
FreeBSD rootkit;  
t0rn (including latest variant);  
Ambient's Rootkit for Linux (ARK);  
Ramen Worm;  
rh[67]-shaper;  
RSA;  
Romanian rootkit;  
RK17;  
Lion Worm.

Info/Download:

< <http://www.net-security.org/various/software/985827056,98592,linux.shtml> >

Defaced archives

-----

[26.03.2001]

Original: <http://enlint003.ericsson.nl/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/26/enlint003.ericsson.nl/>

OS: Windows

Original: <http://pokemon.nintendo.es/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/26/pokemon.nintendo.es/>

OS: Windows

Original: <http://www.necworx.nec.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/26/www.necworx.nec.com/>

OS: Windows

Original: <http://www.suizhong.gov.cn/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/26/www.suizhong.gov.cn/>

OS: Windows

Original: <http://c3-svr.hq.nato.int/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/26/c3-svr.hq.nato.int/>

OS: Windows

Original: <http://www.intelsat.int/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/26/www.intelsat.int/>

OS: Windows

[27.03.2001]

Original: <http://www.tjciq.gov.cn/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/27/www.tjciq.gov.cn/>

OS: Windows

Original: <http://www.microsoft.economy.ru/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/27/www.microsoft.economy.ru/>

OS: Windows

Original: <http://www.shangyu.gov.cn/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/27/www.shangyu.gov.cn/>

OS: Windows

Original: <http://www.hertz.fi/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/27/www.hertz.fi/>

OS: Windows

Original: <http://www.foundry.sony.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/27/www.foundry.sony.com/>

OS: Windows

[28.03.2001]

Original: <http://www.yahoo.com.ph/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/28/www.yahoo.com.ph/>

OS: Unknown

Original: <http://www.volvo.com.tw/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/28/www.volvo.com.tw/>

OS: Unknown

Original: <http://www.travel.gov.cn/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/28/www.travel.gov.cn/>

OS: Windows

Original: <http://www.telefonica.com.uy/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/28/www.telefonica.com.uy/>

OS: Linux

[29.03.2001]

Original: <http://www.telfort.ericsson.nl/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/29/www.telfort.ericsson.nl/>

OS: Windows

Original: <http://enlint004.ericsson.nl/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/29/enlint004.ericsson.nl/>

OS: Windows

Original: <http://www.ebay.co.th/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/29/www.ebay.co.th/>

OS: Windows

Original: <http://www.agrisd.gov.cn/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/29/www.agrisd.gov.cn/>

OS: Windows

[30.03.2001]

Original: <http://www.contraloriadecundinamarca.gov.co/>

Defaced:

<http://defaced.alldas.de/mirror/2001/03/30/www.contraloriadecundinamarca.gov.co/>

OS: Windows

Original: <http://harita.intel.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/30/harita.intel.com/>

OS: Windows

Original: <http://www.camaragyn.go.gov.br/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/30/www.camaragyn.go.gov.br/>

OS: Windows

[31.03.2001]

Original: <http://shop.europe.creative.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/31/shop.europe.creative.com/>

OS: Unknown

Original: <http://www.canon-office.co.uk/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/31/www.canon-office.co.uk/>

OS: Windows

Original: <http://www.renault.pt/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/31/www.renault.pt/>

OS: Windows

Original: <http://www.peugeot.sk/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/31/www.peugeot.sk/>

OS: Unknown

Original: <http://www.martini.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/31/www.martini.com/>

OS: Windows

Original: <http://www.panasonic-office.co.uk/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/31/www.panasonic-office.co.uk/>

OS: Windows

-----  
Questions, contributions, comments or ideas go to:

Help Net Security staff

[staff@net-security.org](mailto:staff@net-security.org)

<http://net-security.org>

<http://security-db.com>