

Abort,
Retry,
Ignore...



Computers Are Easy User Group

June 2001

Suggested Retail Price \$1.95

Volume XIV

Issue 6



Protecting your computer from viruses, worms, and trojans

by: By Ira Wilsker, GTPCC

If you have been following the news recently, you have undoubtedly heard of viruses; "worms," programs that "eat" through your files; and "trojans," programs that hide under the guise of other more innocent looking programs.

Regular listeners to my radio show (KLVI 560AM, 6-7 p.m. Tuesdays) have heard warnings about these threats to computers, and a multitude of callers who have been the victims of these software creatures. A virus, worm, or trojan is a piece of software that was written to be mischievous, and loaded discretely onto the victim's computer. According to some computer security publications, there are now over 60,000 identified viruses, worms, and trojans; new ones appear at a rate averaging 100 - 400 a week! It is imperative that all PC (and MAC) users have a modern antivirus installed, properly configured, and updated frequently, at least weekly. There is no good reason not to have an antivirus program installed, other than they slightly degrade performance as they scan incoming data for "signatures" of potential threats. They do this by comparing this data to a file of known threats. Most antivirus programs can also identify some new threats, because they are often minor variations of existing threats, or use otherwise known code. Cost should not be a problem; a review of the Sunday sale books in most weeks will reveal that the local electronics or office supply stores have the top selling antivirus software titles (NAI's McAfee ViruScan, or Symantec's Norton Antivirus) on sale, often for as little as \$5 - \$10 after rebates. There are several dozen other publishers of quality software as well. For those who like "free," there is the excellent InoculateIT Personal Edition from Computer Associates Inc., one of the largest software publishers in the world. This can be downloaded from <http://antivirus.cai.com>. After a simple registration (free), a serial number is

(con't on page 4)

TABLE OF CONTENTS

PROTECTING YOUR COMPUTER FROM VIRUSES, WORMS, TROJANS BY IRA WILSKER.....	1
HELPLINE.....	3
MINUTES OF CAEUG MEETING MAY 26 BY AL SKWARA.....	5
THE LAMP POST - NUMBER 19 BY JOHN SPIZZIRRI.....	6

Calendar
of
Events

!!! IMPORTANT !!!

Meeting dates for
2001

See page 10
for all
confirmed
dates.

Time and Place
remain the same.

Upcoming
CAEUG meeting
Saturday,
June 23
2001
9:45-12 noon

Computer Central

Next show date
SUNDAY, June24
 College of Dupage
 9:30 A.M. to 3:00 P.M.
 Chicagoland's Oldest and Largest
 Multi-Vendor PC Show & Sale for
 Home and Business

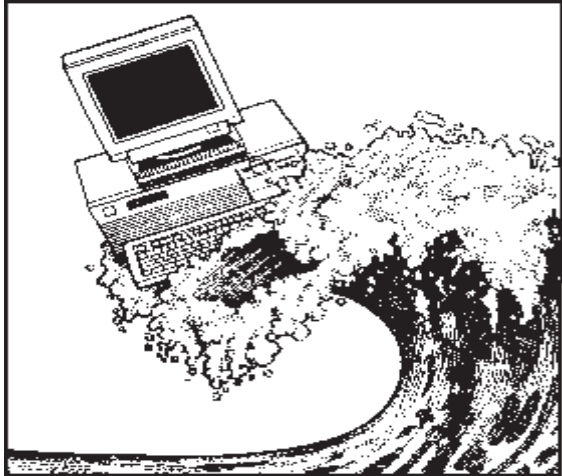
COLLEGE OF DUPAGE
 Main Arena of Physical Education Building
 Corner of Park Blvd & College Road
 Glen Ellyn, IL
 FREE PARKING
 Admission - \$6.00
 (With this coupon admission \$5.00)
 www.computercentralshows.com
 E-mail address:
 compcent@megsinet.net

COMPUTERCENTRAL
 2001 dates
 June 24, July 29, August 26
 September 30
 COD

PICTURE YOUR AD HERE!
FREE !!

IF YOU ARE A MEMBER OF CAEUG THIS SPACE
 COULD SELL ANY COMPUTER
 RELATED ITEM FREE OF CHARGE.

JUST CONTACT ANY CLUB OFFICERS
 OR THE NEWSLETTER EDITOR TO PLACE YOUR AD IN
 THE NEWSLETTER.



In order to have your article or item for sale
 appear in ARI they must be received by the
 10th of the month prior to publication.

MEMBERS HELPLINE

Any member with a specific expertise
 can volunteer to be on the Members
 Helpline. Contact Carl Schow.

Beginners Helpline.....Billy Douglas

Beginner hardware
 problems.....Dick Fergus

QuickBooks, Turbo Tax, IBM Lotus, MS
 Excel, Corel's Quattro Pro....Terry Moye

Win 9x, NT, 2K.....Rick Scalzo
 e-mail.....mitsufan@webcentrix.net

Hardware problems
 & WIN NT4, Linux.....John Spizzirri

Start UP Discussion Group

Ask questions and discuss computer
 experiences with the Start UP group.
 Such as:

1. New to Computers? (basic topics)
2. How to use the Web or download
 information
3. How to install hardware/software
4. Discuss how to troubleshoot
 hardware conflicts, learn boot up
 emergency tricks
5. What do you want to know??

Meets before regular meeting from
 9:15 to 9:45

issued, and free updates and support become available. CAI posts frequent updates almost daily to the Net, and they can be downloaded and installed by opening the program, and clicking on TOOLS AUTO DOWNLOAD. In the past, most viruses were transmitted by the exchange of floppy disks, but now most are transmitted by e-mail, often as attachments. Some e-mail programs, especially the widely used Microsoft Outlook and Outlook Express, are very vulnerable to attack. This vulnerability is often the target of virus authors, who create viruses to utilize the fact that the Outlook products are directly connected to a browser (Internet Explorer), the Windows operating system, and utilities that can execute viruses written in the popular Visual Basic (the recent Anna virus was a simple Visual Basic program), machine code, Microsoft Office scripts, or the Java language.

While the old adage "don't run an e-mail attachment from someone you don't know" may still be a good idea, the majority of newer viruses will be e-mail attachments from people you do know, maybe even with a message title replying to one you sent. This is because many of the new viruses, worms, and trojans actually hijack the Outlook address book and replicate themselves to the e-mail addresses in the address book. AOL mail is also another common target, simply due to the large number of AOL users. While still vulnerable, users of other popular e-mail programs such as Eudora and Pegasus are much less frequently the targets of the virus writers. Web based e-mail, such as Hotmail, Net Address, and Yahoo Mail are not immune, especially if attachments are run or downloaded. The modern rule of thumb is either do not open or download attachments, or be very suspicious. To get around the suspicion, many virus authors attempt to hide their evil within a nice or innocent looking name or extension. The recent Anna attacks were made to look like a common JPEG image, but with the otherwise unlikely file extension

".jpg.vbs." This looked at first like a typical JPEG image file, but the VBS indicated to the observant user that it was a program written in visual basic script.

While the antivirus software can typically detect and remove most viruses, worms, and trojans, there are also other threats that are now becoming more common. Any time users are online, or connected to a network, their computers are vulnerable to a variety of additional threats. In reality, with a Windows PC, there are about 65,000 "ports" or places of entry for the exchange of information. While online in any fashion, a PC can be a target of either someone trying to electronically break in, or a previously undetected "backdoor" secretly installed on the user's computer may attempt to send information from the computer to someone else. Trojans with the names of Back Orifice or Backdoor-G have become extremely common; there are hundreds of others as well. These programs allow someone else almost unrestricted access to anything on the user's computer any time they are online. Ranging from a simple irritant to industrial espionage or sabotage, these trojans are just one type of threat to the online user. Another surprisingly common threat is someone trying to break into the user's computer while it is online. If successful, then everything from keystrokes typing usernames and passwords, to data theft and manipulation become possible.

In order to minimize the chance of an outsider gaining access to a user's computer while online, a program generically called a "firewall" is often a necessity. Originally only used by large institutions on their networks, firewalls have become a security essential on millions of home or small business computers on a network or online. A firewall functions by either closing vulnerable ports, or monitoring incoming and outgoing data,

con't on page 5

issuing an alarm when a suspicious data transfer is found. While a lesser (but still common) problem with dial-up Internet access, a firewall may be a necessity on a computer with DSL or cable modem access. Being "always online" makes a computer an easily identifiable target. While there are some very good commercial firewalls for PCs, such as BlackIce, Norton Internet Security, and McAfee Firewall, one of the most popular is the top-rated Zone Alarm from Zone Labs. Zone Alarm is free for personal use, and available for download at www.zonelabs.com. Just like the antivirus software, the firewall publishers often make updates available on the Internet. There are a variety of free websites that can identify online security breaches. One of the most popular is the Shields Up test available free at <http://grc.com>. To paraphrase a popular unrelated warning, all computer users "need to practice safe HEX."

Author's note: Ira Wilsker is an Instructor IV of Management Development at Lamar Institute of Technology. Ira has been working with computers since 1965 when he took his first computer class at the Illinois Institute of Technology in Chicago. Ira is a frequent guest on the local television news, and has lectured internationally on a variety of computer topics ranging from computer and Internet basics, to CyberCrime, and Community Oriented Policing.

Minutes of CAEUG Meeting
May 26, 2001

Rick Scalzo called the meeting to order at 9:42 am.

Rick welcomed one visitor and invited him to sign in.

There were 38 in attendance.

The next meeting is scheduled for June 23, 2001.

Raffle items included: Money, Quicken Version 8, Eudora Pro, a book titled Computers Simplified, Power Point for Win95.

Volunteers for the COD show were discussed. Anyone willing to represent the club at the show can get a free admission. The show lets two members in free and the club will reimburse two other members who work at our table. The reimbursement does not happen until the next monthly meeting.

The minutes were approved as published in the Newsletter. The Income for March was \$228.85 not \$328.85 as reported giving us a starting balance of \$4,668.14.

The Financial Report showed a starting balance of \$4,668.14, income of \$307.00 and expenses of \$151.28 for an ending balance of \$4,823.86.

OLD BUSINESS

Rick is still searching for an upgraded projector for the club.

New Business

There was an update on the club web site.

This month's disk of the month is the Linux Operating System and Linux Software.

A picnic chairperson was requested. Mike Goldberg and Roger Kinzie volunteered to serve as co-chairpersons. The club picnic has been scheduled for Seven Gables Park from 11am to 3pm on August 25, 2001

Three ink cartridges were offered for sale for the benefit of the club.

The presentation was made by John Spizzirri on the Linux Operating System, which he installed on a system.

Respectfully submitted,

Al Skwara



The Lamp Post

Number 19 by John Spizzirri
June 10, 2001



The United States Air Force Academy (USAFA) Computer Science Department analyzed the Love Bug virus and the conditions that permitted it to profligate. They found that 15% of adult Americans received at least one copy of the virus. One of every 25 of those adults opened the message thus infecting themselves and others. They examined Microsoft's (MS) response to the outbreak and found the Outlook 2000 SR-1 (Service Release i.e. bug fix) could be easily defeated using code fragments that appear on the Microsoft Developers Network (MSDN) Web site (<http://msdn.microsoft.com/default.asp>)! They notified MS of the weakness. MS responded saying that it could not be done the way the Air Force did it. The USAFA made specific recommendations to strengthen the security of Outlook "given the current limitations of the Windows operating system." You can read the entire six-page story at <http://www.usafa.af.mil/dfcs/papers/mcc/ieeesmc2001.pdf>.

Open Source Software (OSS at <http://www.opensource.org>), Free Software, Gnu, Linux... what do these terms mean. I recently attended a lecture by Bradley Kuhn, Vice President of the Free Software Foundation (FSF at <http://www.gnu.org/fsf/fsf.html>), held at the Fermi National Accelerator Laboratory (<http://www.fnal.gov>) in Batavia. Kuhn explained that OSS was a movement started in 1998 while the FSF has been around since 1984. He went on for an hour about linguistics and the preachy socio-political differences between free software and OSS. He said 'free software' did not mean cost free but the freedom to examine, change, and use software. A free software definition is at <http://www.gnu.org/philosophy/free-sw.html>. Kuhn said the OSS definition is 'almost' right but contains flaws primarily about the sale of software and restriction of its use. The OSS definition is at <http://www.opensource.org/docs/definition.html>. He made a point about Cygnus Solutions being a 'pure' free software company before its merger with Red Hat (<http://www.redhat.com>) in 1999. Red Hat is a 'Linux and open source' company now. Kuhn said that Debian (<http://www.debian.org>) is now the closest to a free software company. He said that Linus Torvalds, the person responsible for Linux at <http://www.cs.helsinki.fi/u/torvalds>, selected the Gnu General Public License (GPL) as the legal protection for Linux for no particular reason other than 'he liked it'. The GPL is the instrument that defines free software legally. It is sometimes called copyleft as opposed to copyright. Kuhn seemed to have a religious fervor about this issue and did not let the facts get in his way. His attitude is similar to the attitudes of people who are in love with MS, Mac, BeOS, and any number of other operating system/hardware platforms. These zealots cannot be convinced that their point of view is just one of many viewpoints. It must be their way or the highway. The next paragraph will then come as no surprise. For more information on Debian try these:
<http://www.libranet.com/>
<http://cdimage.debian.org/ch3111.html> - for image download
<http://www.debian-cd.com/>
<http://www.weikert.de/debwall/> - firewall and documentation
<http://www.debiandiary.f2s.com/?clkd=iwm> - Documentation
<http://www.debianplanet.org/debianplanet/>

Over the last few months you may have heard the spew of vitriol by the likes of Jim Allchin, Craig Mundie, and Steve Ballmer. Allchin, Windows product manager, came out four square against Linux and open source software (OSS). Mundie, Senior Vice President, said that MS customers wanted 'clarity of Intellectual Property Ownership' and 'Predictability of the Development Process'. If you have ever read your Window License Agreement, you know that MS owns the intellectual property and you own nothing. As for the predictability of development, how often has MS promised a product by a certain date only to have that date pushed back and pushed back again? This is the same Craig Mundie who blasted the Gnu General Public License (GPL) in what some pundits call a "bizarre ideological campaign" against open source software. Recently, Mundie announced that he would debate OSS at the premier open-source conference—O'Reilly's Open Source Convention, which takes place in San Diego in late July – watch for the news on this one. You can get the MS arguments about why "shared source", the MS marketing ploy, is better than open source software at <http://www.microsoft.com/Business/Licensing/SharedSource>. On June first, Steve Ballmer told the Chicago Sun Times that Linux and the GPL are a 'cancer'. The whole interview is available at <http://www.suntimes.com/output/tech/cst-fin-micro01.html>. You would think that these are the ravings (or whining) of executives going broke because of predatory competition. MS is far from broke but I think they are scared – scared that their customers will find out how and by how much they are being fleeced.

Group Vice President Jim Allchin said that MS will spend "hundreds of millions of dollars" marketing XP. The hype-meisters are already spreading the story that people are waiting with baited breath for the release of Windows XP. Don't believe it. I have yet to see any chat rooms or Web sites where real people are even mildly enthusiastic about XP. You can read the story at <http://www.infoworld.com/articles/hn/xml/01/05/09/010509hnxp.xml>.

The British Prime Minister (PM), Tony Blair, appeared at Microsoft's UK headquarters promoting Office XP and the October release of Windows XP. "If you ask nicely, we'll give you one free," a Microsoft employee told Blair on British TV. This came before his re-election as PM and antagonized his opponents. "Yet again the Prime Minister's judgment is suspect when it comes to using commercial connections for party political purposes," a Tory spokesperson said. A spokesperson for Blair insisted that the PM didn't endorse any Microsoft products, but the televised visit's timing—came one day before Office XP's release and less than a week before the election, which Blair won by a landslide.

MS killed its "snitch" program. The company promised to reward customers for tattling on other MS customers who used unlicensed software. Admitting that the program was "stupid," MS stopped it after an industry news organizations publicized the plan. "It was a super-brief pilot program that was admittedly stupid but absolutely didn't share information [with authorities]," said an MS spokesperson. "It was just an opportunity to contact customers to explain the limits of their site licenses." Yeah, right! Microsoft admits that its complex licensing agreements probably play a bigger role in licensing misunderstandings than any desire to willfully pirate software.

How to spot a hoax in your email. I have received numerous hoax emails in the past three months. There had been a lull of about a year since the last one so I thought that perhaps people were getting wise to the whole concept. In March, I got one and ignored it. Then in April came some more. I wrote back to the people that sent them and notified them of the hoaxes. The trouble with hoaxes is they clog mail servers and waste the time and resources of the receiver. Whenever any

email comes to you that requests that you pass it on – DON'T do it until you have checked one or more of the sites listed here to see if it is a hoax.

<http://www.snopes2.com/index.html>

<http://www.zdnet.com/zdhelp/filters/ehoax/> by Dr. D. Bunk

<http://www.symantec.com/avcenter/hoax.html>

<http://vil.mcafee.com/hoax.asp?>

<http://hoaxbusters.ciac.org/>

Two months ago I reported that Michael Dell, owner of Dell Computers (<http://www.dell.com>), stated that Dell was going to take the lead in the computer market. This past month Gateway is getting into that price war. Gateway (<http://www.gateway.com/index.shtml>) announced that it "will not be undersold". They will beat any advertised price for comparable machines with 800MHz processors or better but only from Compaq, Dell, HP, IBM, Sony, or Toshiba.

Steve Gibson of Gibson Research (<http://grc.com>), the creator of SpinRite and Shields Up software, recently had his Web site taken down by distributed denial of service (DDoS) attacks. He investigated the attacks and found a flaw in Windows XP. MS denies that such a flaw exists. His report on the problem is at <http://grc.com/dos/grcdos.htm>. He predicts dire consequences for the Internet unless MS does something to change this.

Where do you fit in? The vast majority of Web surfers spend all of their browsing time at the four largest Web destinations. A study by Jupiter Media Metrix reported that the four largest sites, AOL (<http://www.aol.com/>), Microsoft/MSN (<http://www.msn.com/>), Yahoo!

(<http://www.yahoo.com/>), and Napster (<http://www.napster.com/>), control more than 50 percent of all Web-browsing time. Obviously, Napster will drop out of the top 10 by next year. The 50% used to be divided by 11 Web destinations just 2 years ago. Only 14 Web sites control 60 percent of overall Web-browsing time, down from 110 sites 2 years ago.

If you were not aware, Lernout & Hauspie Speech Products, maker of Dragon NaturallySpeaking, declared bankruptcy last year (<http://www.lhsl.com/default2.htm>). This past week a majority of their creditors voted in favor of the restructuring plan proposed by the company's new management, which calls for a quick breakup of the company. The whole story of the breakup and speculation about what will happen to the software and other assets is at <http://www.infoworld.com/articles/hn/xml/01/06/06/010606hnlhbbreak.xml?0606wepm>.

Road Runner Medic, <http://help.rr.com>, has a Web site that has step by step tutorials on many Windows topics. Some of the tutorials are animated with sound tracks. If you are having a problem, give them a try. In the same vein is Windows Guide Network at

<http://www.winguides.com>. No videos here but lots of helpful tweaks and advice. If you are looking for the more esoteric things in Windows, try Registry Tricks at

<http://budkwan.virtualave.net/tutes/regtrick.htm>. Bob Cerelli also has a site with hints, tips, and tweaks at <http://www.onecomputerguy.com>.

Those of you who are getting ready for Linux or are already trying your hand at it may want to look at Open Office. Open Office is what Sun's Star Office is based on. You can download, check features, and look at screen shots at <http://www.openoffice.org/>.

A Linux link site with lots of cool connections <http://www.linuxopenoffice.com/> .

Amazon.com will start selling PCs. Considering the no holds barred price war that is no going on and the decline in PC sales, it does not seem logical but Jeff Bezos never was.

Juno and NetZero merged. The details will be competed by the end of the year. They have to work out the law suit (Juno is suing NetZero for patent infringement). The whole story is at

http://www.internetnews.com/isp-news/article/0,,8_781391,00.html .

I have become a Linux advocate of late. The moves being made by MS, RIAA and the ATA, I see leading to a bleeding of the public with built in charges for just about anything computer or entertainment. I think that Linux and/or open source software will stymie the moves by these powerhouses of capitalism by creating new powerhouses like Red Hat(?). With that said here are 10 reasons to switch to Linux that I found on the net.

1. A Linux "Distribution" has thousands of dollars worth of software for no cost or just minimal cost.
2. Linux is a complete operating system.
 - It is Stable. Even if an applications crashes, it is unlikely it will bring down the system.
 - It is Reliable. Linux servers are often up for hundreds of days without error, as compared to the regular reboots required with Windows.
 - It's a powerhouse.
3. It comes with a complete development environment, including C,C++, Fortran compilers, and toolkits such as Qt and scripting languages such as Perl, Awk and Sed.
4. Excellent Network capabilities, allowing you to share CPU's, share modems and more- all of which are not included or available in Windows 95.
5. Linux is the ideal environment to run servers such as a Web Server (Apache, etc.), or an FTP server.
6. A wide variety of commercial software is available if the free software doesn't satisfy your needs.
7. It is an operating system that is easily upgradeable. After any length of time a typical installation of Windows and software gets into a complete mess! Often, the only way to clear out all the debris is to reformat the hard disk and start over again. Linux, however is much better at maintaining the system.
8. Supporting multiple processor is standard.
9. True multitasking, with the ability to run more than one program at the same time.
10. Linux includes an excellent window system called "X," the equivalent os Windows but much more flexible.

Between you, me and The Lamp Post that's all this month.

FIRST CLASS MAIL

CAEUG
P. O. Box 2727
Glen Ellyn, IL 60138

Meeting place and date information:

The next REGULAR meeting will be held at the Glen Ellyn Library in Glen Ellyn at 9:45 am on
Saturday, June 23, 2001

The library is located 1 block west of Citibank at the corner of Prospect & Duane FREE PARKING
Directions: Park to Duane; go west on Duane to Prospect Street. Please park at the West end of the
lot, away from the building. Thank you.

The meeting(s) are not library sponsored and all inquiries should be directed to Carl Schow . Individuals
with disabilities who plan to attend this program and who require certain accommodations in order to
observe and/or participate in the program are requested to contact CAEUG president,
Rick Scalzo at , at least five (5) days prior to the program, so that reasonable accommodation can be
made for them.

Confirmed Meeting dates for 2001:	June 23, July 28 August 25 CAEUG annual picnic Saturday, September 22, October 27, November (no meeting), December 1 (Nov/Dec meeting),
Confirmed Meeting dates for 2002:	January 26, February 23, March 23, April 27, May 25

Program for June 23: An install and more of Red Hat 7.0 and, if time permits
additional software, on a pc will be given by John Spizzirri. If you would like Red
Hat 7.0 installed on your pc, you will need to bring the cpu, monitor and contact John
at spizman@iwon.com so he can be prepared. The suggested configuration is at least a
1 gig hard drive and 32 Meg of memory.