©2003 by CAEUG

FOUNDED 1984
The Official Newsletter of THE
COMPUTERS ARE EASY USER GROUP

# Abort, Retry, Ignore...

CAEUG Computers Are Easy User Group

September 2003 | Suggested Retail Price $1.95 | Volume XIV | Issue 9

Calendar of Events

!!! IMPORTANT !!!
Meeting dates for 2003
See page 10
for all confirmed dates. Time and Place remain the same.

September 27
John St. Clair will cover video editing and DVD's on your pc

SEE YOU THERE!!

Info about auction at September meeting of the BYOC pc on page 4

COD Dates
2003 dates
September 28
October 26
November 23
December 21

## XP Boot Disk
## by Larry Bothe, 9/19/03

In the September issue of Foxtales publication of FVPCA Craig Landes presented yet another informative computer article; this one was about having an emergency boot disk available in the event that something happens and your computer won't boot up in the normal fashion. Your machine most likely boots from the hard drive. If your hard drive crashes, or you have some other software or hardware glitch that prevents a hard drive boot, you will have to boot from some other source. That is typically your CD drive or 3.5" floppy drive, so you will need a bootable CD or floppy disk in order to get the machine to run.

Now, I am aware that Craig Landes is an Information Technology professional, and that means under normal circumstances, relatively speaking, I wouldn't even be qualified to carry around his toolbox. But I had a very recent experience that seems to contradict one of Craig's statements with respect to booting up Windows XP from the installation CD. In the section of his article that Craig calls XP Upgrade Installation he discusses the differences between the upgrade and full versions of XP. Besides the $100 cost difference he states that "The critical difference is that the upgrade versions do NOT come on a bootable CDROM".

Here's my story. One day last week I heard these unpleasant (human) noises coming from our home-office. I found my wife looking at a black & white screen containing text informing her that Windows XP had failed to start correctly and asking her to make a choice to start in one of four different modes. The modes were the basic safe mode, two other safe modes with some drivers loaded, and finally normal mode using last known settings that worked. Well, guess what, none of the modes were successful. Each time we tried, the computer would attempt a restart but eventually end up at that same text screen. XP just wouldn't run. My wife wasn't very happy. We had gone through some other problems which were mostly solved by upgrading to XP in late July, and now here was yet another showstopper. And it was all the more mysterious because the text

(con't on page 4)

TABLE OF CONTENTS

XP BOOT DISK BY LARRY BOTHE . . . . . .1
HELPLINE. . . . . .3
THE LAMP POST - NUMBER 44 BY JOHN SPIZZIRRI. . . . . .5

## CAEUG Officers & Chairpersons

| | |
|---|---|
| President | John Spizzirri |
| V.P. (Programs) | Billy Douglas |
| Secretary (& donuts) | Al Skwara |
| Treasurer | L. Johnson |
| Newsletter Editor | Kathy Groce |
| Membership Chairperson & Circulation Manager | Pete Nicchia |
| CAEUG COD Coordinator & Publicity | Terry Moye |
| Software Reviewer | Brian Noon |
| Webmaster & Technical Consultant | Richard Scalzo |
| Coffee Service | Joan Thompson |
| Picnic Chairpersons | Mike Goldberg<br>Roger Kinzie |

Reminder: You'll get better, faster service if you use CAEUG in the subject of your e-mail.

CAEUG
Computers
Are
Easy
User
Group

## CAEUG LIST OF SUPPORTING RETAILERS

The retailers listed below have in one way or another supported CAEUG and we thank them.

COMPUTER MAINTENANCE, INC.
1433 W. Fullerton Avenue, Suite M
Addison, IL 60101
630/953-1555

BOOKS & BYTES, INC.
Retail store is closed
630/416-0102
http://www.bytes.com/

ABOUT THE NEWSLETTER:

This printed version of our newsletter was laid out using Adobe's Pagemaker Version 7.0 for Windows and was printed on a HP Laserjet III. Our group's membership database is maintained using MS Access and address labels are printed using MS Access software. Our checking account records are kept in Quicken software.

The opinions expressed in this newsletter are not necessarily those of the CAEUG Officers, members or other contributors. CAEUG, its officers, newsletter editor, authors or contributors are not liable in any way for any damages, lost profits, lost savings, or other incidental or consequential damage arising from the use of the information provided herein. Every reasonable effort has been made to confirm the accuracy of the contents of this newletter, but that accuracy is not guaranteed.

Permission is granted to reproduce any or all parts of this newsletter for personal use. Also granted is permission to reproduce for public ation any part of this newsletter provided that a copy of the publication is mailed to CAEUG, immediately following publication and CAEUG is given credit.

The CAEUG newsletter is published eleven times annually. Contributions by members are encouraged and will be gratefully acknowledged in the newsletter. We have a policy of exchanging newsletters with other users groups across the nation. Several CAEUG member articles have already been picked up and reprinted.

## Great Midwest Computer Show

Next show date
SUNDAY, Sept 28
College of Dupage
9:30 A.M. to 3:00 P.M.

The Midwest's oldest and largest
Multi Vendor PC show and sale for
Home & Business

COLLEGE OF DUPAGE
Main Arena of Physical Education Building
Corner of Park Blvd & College Road
Glen Ellyn, IL
FREE PARKING
Admission - $7.00
(With this coupon admission $6.00)
www.CODSHOW.COM
E-mail address:
info@codshow.com

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 Rick Scalzo.

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

Hardware problems,
Win 9x, NT, 2K & Linux.....John Spizzirri

## Great Midwest Computer Show © 2003 dates

Sept 28, Oct 26, Nov 23, Dec 21

A Note from CAEUG President:

Due to suffering from a bout with food poisioning the CAEUG Survey results will be in October ARI.

## Membership Costs.....

| | First Yr. | Renewal |
|---|---|---|
| Individual | $25.00 | $20.00 |
| Family | $30.00 | $25.00 |
| Corporate | $30.00 | $25.00 |
| Associate | $20.00 | $15.00 |

## Beginner's SIG

Ask questions and discuss computer experiences with this 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 9:05 to 9:45

screen suggested that the cause was likely some recent hardware or software addition. But we hadn't changed anything on the machine for several weeks, and it had in fact run just fine earlier in the day.

After opening up the machine to make sure there weren't any unseated cards or loose cable connections we tried again; all four modes. No luck. Then I disconnected all the unnecessary peripheral equipment (scanner, printer, speakers) and tried again. I even changed mice. We still got the same result, a stall at the screen with the boot mode selection. No matter what we selected it always came back to that screen.

Then I had this brilliant idea (about 2 hours too late); why not feed it the Windows XP Home Upgrade CD and see what happens? In order for that to work I had to go into the BIOS and change the order of boot devices to make the CD-ROM drive boot first. Fortunately I knew how to do that so in short order I was ready to try the umpteenth restart of the day. Wa-la! After loading a lot of stuff off the CD it came up and asked if I wanted to reinstall Windows XP or go into recovery mode. Recovery was just what I needed, so I selected that. I got a DOS-like screen that offered a whole bunch of repair utilities. I ran two that appeared to be appropriate (one was CHKDSK) and then typed EXIT. That got me out of the DOS screen and Windows XP started right up. Since I didn't really know what I was doing I was quite relieved by that result.

After we finally got the good XP start I didn't know what else I should do so I entered the BIOS again to change the boot order back, removed the XP Upgrade disk from the CD drive and shut the machine down. Now of course was the moment of truth; would it again boot properly from the hard drive? And it did. We ended up concluding that somehow the registry must have gotten hosed up. The one good start and subsequent shutdown rewrote enough of the registry that a normal boot into XP was again possible. We have not had any more trouble with the machine since that time. If it was in fact a registry problem we have no idea how it got loused up. We're just hoping it doesn't happen again.

So, with all due respect to Mr. Landes, I found that you can, in fact, boot a computer from an XP Upgrade disk; you don't need the full version. The only explanation I can offer is that my recently acquired XP Upgrade includes Service Pack 1 on the CD. Perhaps Craig's experience was with the first release before any service packs, and that wasn't bootable. The service pack may have added the boot feature.

Larry Bothe is an associate member of CAEUG and an "honorary" member of FVPCA. He was President of CAEUG for a while back in the 90's when he lived in the Chicago area. He presently resides in southern Indiana where he is retired from industry and teaches people to fly airplanes. He can be contacted at Lbothe@aol.com.

---

## Auction Auction Auction

At the September meeting the club is auctioning off the computer that was built for the July BYOC (build your own computer) presentation by Ryan Noon.

Specifications --

Motherboard: ASUS A7V8X-X 3 PCI slots, USB ports, 10/100 Ethernet
CPU: AMD Athlon XP2500+ w/333MHZ FSB
Memory: 256 MB PC2700
VideoCard: GForce 4MX440 w/128MB AGP 8X
Hard Drive: Western Digital 80GB w/8MB cache
Sound: SoundMAX Digital Audio 6 channel audio onboard MoBo
Drives: 32X CD-ROM, 3.5 inch floppy
Modem: 56K
Case: ANTEC SLK3700SMB 350W MIDTOWER Bays: 4-5.25",7-3.5"
Misc: Optical mouse, keyboard, monitor
OS: Win98

Bidding will start at $500 with $5 increments. If you cannot attend but want to bid, send the president your top bid. The president will bid for you at the lowest possible price. E-mail: spizman@iwon.com

P.S. We already have a bid of $500.

# The Lamp Post Number 44
by John Spizzirri
September 15, 2003

Brianna LaHara, an honors student at St. Gregory the Great school, lives in a New York Housing Authority apartment for low to moderate-income families. She is 12 years old. She owes the Recording Industry Association of America (RIAA http://www.riaa.com ) $2000. Hers was the first RIAA copyright infringement lawsuit settled out of court. The 261 lawsuits were against individuals that had downloaded 1000 or more songs from the Internet using the KaZaa peer-to-peer service ( http://www.kazaa.com ). The lawsuits were initiated on the premise that the 'recording artists' should be compensated for stolen songs (downloaded but not paid for). By law, each song downloaded could result in a charge of $150,000.00. The RIAA says it's only going after major copyright violators. If we assume that just 1000 songs were downloaded and the lawyer's fee was just 33%, that leaves $1.34 per song. Do you think the RIAA will go through the songs on the computer and distribute the money to each artist? Does the RIAA represent artists? If your answers to these questions does not seem to make sense, perhaps you should check your premises.

Cary Sherman. President of the RIAA, appeared before the Senate Judiciary Committee hearing recently. Illinois Senator Richard Durbin asked Sherman, "Are you headed to junior high schools to round up the usual suspects?" Sherman replied, "Yes, there are going to be some kids caught in this, but you'd be surprised at how many adults are engaged in this activity." What does Sherman's answer mean to you? My take is that if you allow access to your computer to anyone including children or grandchildren, you risk an RIAA lawsuit if they download something the RIAA considers their property.

Bryd Parmelee sent me a site that had cam links. The first overlooks Lake Superior in the area of the Duluth harbor: http://134.156.98.1/lakecam/ . The second is a Peregrine falcon cam atop a stack at Boswell Energy Center; http://134.156.98.1/falconcam/ . The falcons migrate so the shots shown now are selected from earlier this year.

Japan's Ministry of Economy requested Microsoft (MS http://www.microsoft.com ) to release a "security cd" with every copy of Windows XP. I reported earlier, that a new copy of XP with service pack 1a (SP1a) requires over a 100MB download to apply all security patches released since SP1a was issued. Japan recognized that most consumers in that country have dial-up connections and a download of that size is a burden. MS complied with Japan's request. MS must believe that most Americans have DSL or cable and don't need a patch disk. In an unrelated story, Steve Ballmer and Bill Gates each received a pay raise of about $112,000.00. Go figure.

Quietbuy.com ( http://www.quietbuy.com ) is a new service that just opened in Elmhurst, IL. If you purchase anything on the Internet with the exception of guns, pornography, or contraband, Quietbuy.com can make your purchase anonymous.

Lindows ( http://www.lindows.com ) has an interesting offer. Some people across the country are getting rebates certificates on MS products they purchased due to legal action taken on their behalf by regulating bodies in their respective states. Lindows is offering to accept the rebate(s) as partial or full payment on Lindows 4 OS (operating system).

The Swen virus (worm) hit this week. Below is the description and method of cleaning from the McAfee Web site http://us.mcafee.com/default.asp :

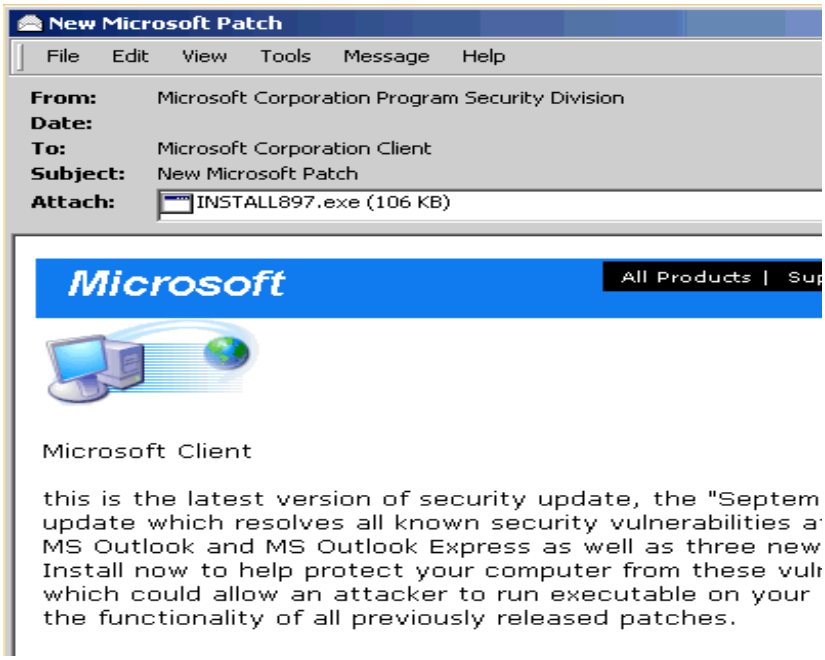
Sometimes purporting to be a Microsoft Security Update, this worm is intended to propagate via various mechanisms:

* mailing itself to recipients extracted from the victim machine
* copying itself over network shares (mapped drives)
* sharing itself over the KaZaa P2P network
* sending itself via IRC

The worm is written in MSVC. Though in a different HLL, it bears similarities to W32/Gibe.b@MM (original Gibe variants were written in VB).
The worm terminates processes relevant to various security and anti-virus products (see below).
Proactive Detection : This worm is detected as “virus or variant New Worm” with the 4120 DATs or greater (with program heuristics enabled).

Mail Propagation
The virus contains its own SMTP engine to construct outgoing messages.
Various outgoing messages are created. Some make use of an IE exploit to ensure the worm attachment is run upon viewing the email. See Microsoft Security Bulletin (MS01-020) . One such message bears the following characteristics:

Subject : Returned Response
From : Email Delivery Service (kmailengine@yahoo.com)
Body : Undeliverable mail to (email address )
Messages constructed to take advantage of this vulnerability will be detected as Exploit-MIME.gen.exe with the 4215 DATs or greater (and earlier as Exploit-MIME.gen).
Multiple subject lines and attachment names are constructed from pools of strings within the worm to be used in outgoing messages. Target email addresses are extracted from files on the victim machine.
At least one message masquerades as a Microsoft update:




(con't on page 7)

Share Propagation

The worm copies itself to the startup folder on mapped network drives. A random filename is used. The following network locations are targetted:

* windows\all users\start menu\programs\startup
* windows\start menu\programs\startup
* winme\all users\start menu\programs\startup
* winme\start menu\programs\startup
* win95\all users\start menu\programs\startup
* win95\start menu\programs\startup
* win98\all users\start menu\programs\startup
* win98\start menu\programs\startup
* document and settings\all users\start menu\programs\startup
* document and settings\default user\start menu\programs\startup
* document and settings\administrator\start menu\programs\startup
* winnt\profiles\all users\start menu\programs\startup
* winnt\profiles\default user\start menu\programs\startup
* winnt\profiles\administrator\start menu\programs\startup

IRC Propagation

The worm drops a SCRIPT.INI file (123 bytes) into the mIRC program folder in an attempt to propagate via IRC (using dcc send). This file is proactively detected as MIRC/Generic with the 4149 DATs or greater.

P2P Propagation

The worm makes copies of itself in a directory (random name) within the system temp directory. Enticing filenames are used, for example:

* SIRCAM CLEANER.EXE
* YAHOO HACKER.EXE
* HALLUCINOGENIC SCREENSAVER.EXE
* etc etc

The following Registry key is modified to share these copies via the KaZaa P2P network:

HKEY_CURRENT_USER\Software\Kazaa\LocalContent

“Dir99” = 012345:C:\WINDOWS\TEMP\(random directory name)

Propagation via Newsgroups

Within the list of servers carried in the worm are multiple NNTP servers. Analysis is currently ongoing to determine exactly how these are used (email address harvesting and/or replication).

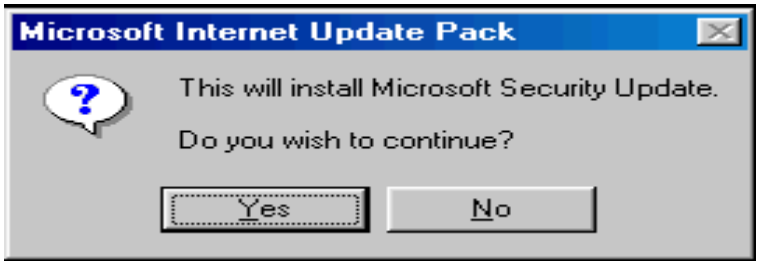
Indications of Infection

* Display of the above dialog boxes
* Unexpected termination of AV/security product
* Inability to run RegEdit on the victim machine

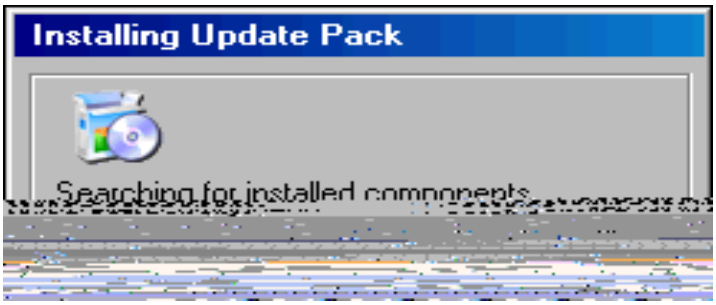
Method of Infection

Installation

When run on the victim machine, a sequence of fake message boxes are displayed:




(con't on page 8)




The worm installs itself (using a random filename) into %WinDir%, for example:
C:\WINDOWS\ZNFUL.EXE
A Registry key is added to hook system startup, for example (random string and filename will obviously change):
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\Run “(random string)” = ZNFUL.EXE autorun
Various Registry keys are modified to hook the execution of the following file types:

* BAT
* COM
* EXE
* PIF
* REG
* SCR

For this, the following Registry keys are set:
HKEY_CLASSES_ROOT\batfile\shell\open\command
“(Default)” = %filename% “%1” %*
HKEY_CLASSES_ROOT\comfile\shell\open\command
“(Default)” = %filename% “%1” %*
HKEY_CLASSES_ROOT\exefile\shell\open\command
“(Default)” = %filename% “%1” %*
HKEY_CLASSES_ROOT\piffile\shell\open\command
“(Default)” = %filename% “%1” %*
HKEY_CLASSES_ROOT\regfile\shell\open\command
“(Default)” = %filename% showerror