

# Abort, Retry, Ignore...



Computers Are Easy User Group



May 2008

Suggested Retail Price \$1.95

Volume XXV

Issue 5



**!!!IMPORTANT!!!**

**\*\*\* NOTE \*\*\***  
**Confirmed**  
**2008 meeting**  
**dates will be on**

**May 24**

**CAEUG**  
**Picnic on**  
**JUNE 28**

**July 26**

**August 23**

**\*\* \* \* \* \***

**MEETING PLACE**  
**will be the**  
**Glenside Public**  
**Library**

**\*\*\*\***

**SEE YOU**  
**THERE!!**

**\*\*\*\***

**CODLinuxfest**  
**http://**  
**www.codlug.info/**

**The next meeting will be**  
**Saturday May 24, 2008**  
**Bill Douglas will present**  
**Computer Security**

### **Internet Security: iFrame Attacks**

By Brian K. Lewis, Ph.D.

Member and Contributing Columnist, Sarasota PCUG, Florida

<http://www.spcug.org>

[bwsail@yahoo.com](mailto:bwsail@yahoo.com)

Obtained from APCUG with the author's permission for publication by APCUG member groups.

I'm sure that most of you reading the title of this article are asking "What is an iFrame?". Well, sit back, get comfortable and I'll tell you about the latest method hackers are using to steal information from you.

First the definition of an iFrame, which is shorthand for inline frame. That clears it up doesn't it? I guess I'd better add some more to that. An inline frame is code within a web page that permits a second page to be imbedded inside the first page. For example, they can be used to imbed an ad that is located on a different web site. One example is the clickable scrolling ad you frequently find on web sites. IFrames generally load after the main page and may sometimes have their own scroll bar. The iFrame may contain Javascript programming code which can permit interactive content. Some iFrames may be invisible and may contain code which can redirect the user to

(con't on page 2)

### TABLE OF CONTENTS

INTERNET SECURITY: IFRAMES ATTACKS BY BRIAN K. LEWIS, PH.D . . . . .	.1
CAEUG PICNIC DIRECTIONS . . . . .	.4
LAMPPOST 95 BY JOHN SPIZZIRRI . . . . .	.5
CD OF THE MONTH BY JOHN SPIZZIRRI . . . . .	.8
HELPLINE. . . . .	.9

another page or download trojans or viruses.

Whenever your Internet browser sees an “iFrame tag” in the web page code it sets aside the space requested in the tag. It also goes out to the web page specified in the code to download the requested information.

So is this something new? I thought it was until I read a report in a tech newsletter (Windows Secrets) about an attack on the AskWoody web site. It turns out that iFrame attacks have been recorded since 2004. The first exploit implanted a worm on thousands of computers. The only thing that stopped it was a patch that Microsoft had to apply to Internet Explorer 6. In June 2007 over 10,000 pages were infected in Italy. In November 2007 Monster.com had to shut down as a result of an iFrame attack. Then, this year the AskWoody site had iFrame code added to its main web page. His research indicated that the code originated on a Russian web site, which subsequently disappeared. The code placed on the AskWoody web page linked to a web site in China and subsequently to the Russian web site. This was all done by a short length of code that setup a single, invisible pixel on the web page. The code was designed to load data from the Chinese web site. Anyone with an unpatched IE 6 that visited the AskWoody web site would probably have been infected. However, it was never determined just what was being delivered by the offshore web site.

The worst part of this scenario is that the owner of the AskWoody web site did not find out about the iFrame exploit until he started receiving messages from someone who advised him that their AVG Resident Shield said his site was infected. That was followed by Google advising him that his site was infected and down rating the site. Google also provided a warning to anyone attempting to link to AskWoody warning them that visiting the site might infect their computer.

The question becomes, how did the iFrame code become attached to the web page? The code pages on web sites are generally password protected. Access to these pages for the purpose of making changes is controlled by the web site host and the hosting software. However, there are several programs available which enable hackers to take advantage of holes in web site security. Some of these are described as “kiddie scripts”, indicating their ease of use. Others, such as Mpack, require a more sophisticated knowledge of programming. The problem is that thousands of respectable sites have been infected. The following are only a few that were reported in March 2008 by Dancho Danev’s blog (a security information web site):

eHawaii Portal - <http://ehawaii.gov> - 992 pages

The World Clock - <http://timeanddate.com> - 944 pages

Boise State University - <http://boisestate.edu> - 471 pages

The U.S. Administration on Aging (AoA) - <http://aoa.gov> - 425 pages

Gustavus Adolphus College - <http://gustavus.edu> - 312 pages

Internet Archive - <http://archive.org> - 261 pages

Stanford Business School Alumni Association - <http://gsbapps.stanford.edu> - 157 pages

BushTorrent - <http://bushtorrent.com> - 147 pages

ChildCareExchange - <http://ccie.com> - 131 pages

The University of Vermont - <http://uvm.edu> - 120 pages

Hippodrome State Theatre - Gainesville, FL - <http://thehipp.org> – 112 pages

Minnesota State University Mankato - <http://mnsu.edu> - 94 pages

Medicare – <http://medicare.gov> – 12 pages

In many instances it appears that the hackers were able to “harvest” passwords which gave them access to these sites. Then, if the site did not have current input validation patches, the iFrame could be added to web pages. In some cases, home users may have been the source of the initial password theft. By use of a keylogger a hacker can obtain passwords to any protected site visited by the user. In other cases clicking on a banner ad that attracts you can result in the download of a bot, a trojan or other spyware. This is especially true if you are still running an unpatched Internet Explorer 6. It appears that Firefox is less vulnerable to these types of exploits. Also, clicking on an executable file in IE 6 generally results in running the file. In Firefox you are usually only given the option to download the file. Obviously you should never download or run any file that you don't know or don't recognize. This is especially true when the site tells you that you need some kind of add-on or special viewer to see the information you want. This is the type of social engineering being used to tempt users into downloading spyware.

There is also a danger related to the firewall you are using on your computer. A keylogger or other trojan needs to be able to report “home” without the user being aware that information is being sent out. This is done by opening a “back door” to the Internet; an outgoing port in one of the thousands on every computer. If your firewall doesn't check on all outgoing data and requests permission for new unknown activity, then you will not be able to block the trojan's back door connection. So it is very important that your firewall check both incoming and outgoing data. Then, anytime your firewall requests permission for a program, one you don't recognize, to connect to the Internet, just say NO.

There is one other recognized method for obtaining the information needed to get into web page code. Hackers can purchase web site administrator information on the black market. One software application used to hack web sites, Mpack, sells for about \$1,000 US. The person behind this software is known as \$ash in the Russian underground. The software exploits six flaws in Windows and Internet Explorer. Thus for not a lot of money, hackers can obtain everything they need to exploit weaknesses in web pages.

As you can see, the iFrame attack is a real danger for those who surf the Internet. If you want to read more about these attacks, a Google search will provide you with tons of information. If you want to protect yourself from these attacks, your ability is limited. It is really up to your ISP and the web hosts to provide the security needed to prevent the web page intrusion of an iFrame. So what can a home user do? The following will help, but are no guarantee of protection.

1. Beware of pages that require software installation. Do not allow new software installation from your browser unless you absolutely trust both the Web page and the provider of the software.
2. Scan with an updated antivirus and anti-spyware software any program downloaded

through the Internet. This includes any downloads from P2P networks, through the Web and any FTP server regardless of the source.

3. Use only a firewall that checks both incoming and outgoing data.
4. Beware of unexpected strange-looking emails, regardless of their sender.
5. Never open attachments or click on links contained in these email messages
6. Enable the "Automatic Update" feature in your Windows operating system and apply new updates as soon as they are available
7. Always have an antivirus real-time scan service. Monitor regularly that it is being updated and that the service is running.
8. OR another option would be to verify that the address is safe before going to it. You can do this by checking it at: <http://linkscanner.explabs.com/linkscanner/default.asp>

As you can see, for Windows users, the Internet is becoming more of a hazard to navigation. You, as a user, must always be cautious about clicking on links or accepting downloads. If in doubt, don't do it! If everyone practiced safe-surfing, it would be harder for the hackers to succeed.

Dr. Lewis is a former university and medical school professor of physiology. He has been working with personal computers for over thirty years; teaching, developing software and assembling systems. He can be reached at [bwsail at yahoo.com](mailto:bwsail@yahoo.com).

This article has been provided to APCUG by the author solely for publication by APCUG member groups. All other uses require the permission of the author (see e-mail address above).

---

## CAEUG Picnic Directions

Directions to CAEUG Picnic at Seven Gables Park:

From Naperville and Butterfield Roads head NORTH on Naperville Road 0.8 mi.

Turn left (WEST) on Danada Road.

Follow Danada for 0.2 mi. to the stop sign at Brighton Road.

Turn right (WEST) on Brighton Road.

Stay on Brighton Road for 0.2 mi.

Turn right (NORTH) onto Winners Cup.

Follow Winner Cup 0.2 mi. to the entrance to Seven Gables Park . Entrance is on the left.

A short distance into the park is a stop sign, At the stop sign turn right. That road will take you past the football field.

We will be at the EAST end of the football field in an area that looks like a refreshment stand.

---

Check out the CAEUG web site at <http://www.caeug.net> Post your question or get useful tips.

**LampPost 95**  
by John Spizzirri  
May 18, 2008



Microsoft (MS <http://www.microsoft.com/>) released SP3 (Service Pack 3) for Windows XP on May 6th. It is only available via download. The up to 850KB download is not too large but will take some time on a 56K phone connection. Per the instructions, "Microsoft is not adding significant functionality from newer versions of Windows, such as Windows Vista, to Windows XP through XP SP3." I am hoping that is true. MS's download web site for SP3 is at <http://www.microsoft.com/downloads/details.aspx?FamilyId=5B33B5A8-5E76-401F-BE08-1E1555D4F3D4&displaylang=en>. The short answer to any questions you may have about Windows XP SP3 is do not download or install it. The instructions and notes about the SP are at <http://support.microsoft.com/kb/936929>. Searching the MS website, it appears that the SP3 is not available via CD. I first read about the troubles with the SP on the Softpedia site at <http://news.softpedia.com/news/XP-SP3-Download-Still-Live-Despite-Widespread-Problems-85346.shtml>. Also read this [http://www.theregister.co.uk/2008/05/12/windows\\_xp\\_sp3\\_reboots\\_amd/](http://www.theregister.co.uk/2008/05/12/windows_xp_sp3_reboots_amd/).

MS profits are down this last quarter because of resistance to Vista. Its called the client division. There was a 24% reduction in sales this year over last. Perhaps churning out bad products has caught up to them. The story is at [http://www.cbronline.com/article\\_news.asp?guid=F711912D-506B-464A-8876-13A532ECDADB](http://www.cbronline.com/article_news.asp?guid=F711912D-506B-464A-8876-13A532ECDADB).

The MicroCenter store in Westmont in the shopping center on the northeast corner of the intersection of Ogden Avenue and Midwest Road offers technical clinics for free. The schedule and subjects are at [http://www.microcenter.com/instore\\_clinic/sign\\_up.html](http://www.microcenter.com/instore_clinic/sign_up.html).

I received this e-mail from InfoWorld Magazine in their quest to save Windows XP - Sign the XP petition on line ( <http://www.savexp.com> )  
Dear "Save XP" petition participant —

Save XP.com Thank you for signing our "Save XP" petition. You're getting this message because you told us you wanted updates on new developments in the "Save XP" campaign. Here's what's happening:

Close to 200,000 people have signed the petition since January 14. However, Microsoft CEO Steve Ballmer thinks we're not serious about the Save XP movement, nor does he seem to take the people who signed it seriously. That's where you come in. Help us meet our goal of 300,000 unique petition signatures by June 2008. Please ask your friends, family and colleagues to join the movement by signing up at [http:// www.savexp.com](http://www.savexp.com) ( <http://weblog.infoworld.com/save-xp/> ).

And show Mr. Ballmer that there's a face behind each email address. How about

May 2008

Abort, Retry, Ignore..

uploading your own Save XP video plea to the InfoWorld section of FaceBook ( <https://www.facebook.com/login.php> )? You can also upload them directly to the InfoWorld site using our BrightCove player ( <http://video.infoworld.com/services/player/bcpid1526070313> ) form. We'll show off the funniest, most creative appeals to save XP on our "Save XP" video home page ( <http://www.infoworld.com/video/index.html?bcpid=1388789577&bclid=1527696845> ).

To stay on top of Windows-related developments, I'd also encourage you to sign up for our Enterprise Desktop newsletter. You can do that here ( <http://www.infoworld.com/newsletter/subscribe.html> ).

Thank you again for helping making IT professionals' voices heard. We promise to do our part to send the message to Redmond, loud and clear.

Best,  
Galen Gruman

MS cannot seem to shake its reputation as a monopoly. It is now appealing a \$1.39bn fine imposed by the European Commission (EC [http://ec.europa.eu/index\\_en.htm](http://ec.europa.eu/index_en.htm) ), the law enforcement arm of the European Union (EU [http://europa.eu/index\\_en.htm](http://europa.eu/index_en.htm) ). The fine was imposed because of MS's failure to comply with the EC's demands to end anti-competitive business practices. The story is at [http://www.cbronline.com/article\\_news.asp?guid=D584D33D-97A3-40CC-A562-14E80A6A0668](http://www.cbronline.com/article_news.asp?guid=D584D33D-97A3-40CC-A562-14E80A6A0668) . The fine was imposed due to a 2004 complaint that MS bundled the Windows Media Player (WMP) with the operating system (OS) and that MS did not release documentation for protocols for OS to operate with products similar to WMP. Two new complaints were filed this past January due to interoperability with other software products. The other problem for MS is about bundling of Internet Explorer (IE) with the OS. A complaint from a maker of another web browser engendered the new complaint.

Last month I reported about the ASUS eee ( <http://eeepc.asus.com/global/> ) computer being a reason MS extended the deadline on Windows XP sales. The eee is classified as an ultra mobile or a mini notebook PC. The eee has been out about a year. It costs from \$250 to \$400 depending on the extra features included. The higher priced eee's come with Windows XP. The eee 900 (the new, improved model) has yet to be offered for sale in the United States. Hewlett Packard (HP <http://www.hp.com/> ) has gotten into the mini notebook PC game with the Model HP 2133. The 2133 checks in at about \$700 when equipped with Vista and about \$500 for the Suse Linux version. The 2133 is heavier (aluminum case vs. plastic), hotter (hard drive moving parts), and larger dimensions to accommodate the large key keyboard. Specifications are at [http://h10010.www1.hp.com/wwpc/us/en/sm/WF05a/321957-321957-64295-321838-306995-3687084.html?jumpid=reg\\_R1002\\_USEN](http://h10010.www1.hp.com/wwpc/us/en/sm/WF05a/321957-321957-64295-321838-306995-3687084.html?jumpid=reg_R1002_USEN) .

Peter Nicchia, our membership coordinator, has had a heart attack. He had four way bypass surgery. He is home recovering as of May 12th. Cards can be sent to Peter at 642 Empire Way, Romeoville, IL 60446 or [pnicchia@sbcglobal.net](mailto:pnicchia@sbcglobal.net).

There is a new ploy by some PC sellers. The advertising says that the PC includes both Win XP and Win Vista but the fine print reads "Microsoft Windows Vista Business (Includes Downgrade rights to Microsoft Windows XP Professional)." An example of this type of advertising is at

**[http://www.microcenter.com/single\\_product\\_results.phtml?product\\_id=0280369&BrCs=498&BrCg=16181435&BrRc=1469058206](http://www.microcenter.com/single_product_results.phtml?product_id=0280369&BrCs=498&BrCg=16181435&BrRc=1469058206)** .

I covered the Digital Television (DTV) conversion a couple of months ago. There is now new information about it plus I did some shopping for a converter box. What I found out may be of help to you. To start, if you have cable or satellite television, you do not need a converter box. If you have any television that gets a signal from an outdoor antenna or 'rabbit ears' (such as a vacation home or RV television), you will need a converter box for it to work after February 17, 2009. The new information is that on September 8th of this year (six months after the program started and the date was set) the city of Wilmington, North Carolina will be the first test of the DTV transition. Gee, you would think that a test might be run before setting a drop dead date for transition and spending \$1.5 billion. I guess the government can afford to waste your money by kow-towing to the television broadcasters and hardware makers. Do I smell pay offs? My shopping excursion had some surprising results. I went to two different Best Buy stores (<http://www.bestbuy.com/>). The clerk in the store in South Elgin showed the Insignia (<http://www.insignia-products.com/pc-318-49-insignia-digital-to-analog-converter-for-analog-tvs.aspx>) model NS-DXA1. This is the only model that Best Buy sells. According to the clerks in the South Elgin and the Bloomingdale stores, this will be the only brand and model that Best Buy will handle. The South Elgin clerk gave me a DTV Transition for Dummies booklet (<http://www.dummies.com/WileyCDA/>) which has most of the information you may need in one convenient place. The Bloomingdale clerk gave me a print out of the specifications of the Insignia box. Neither clerk could answer my questions, knew much about the box, or how they worked. At Circuit City (<http://www.circuitcity.com/>), the clerks were nowhere to be found. I searched the television department and found only one converter box made by Zenith (<http://www.zenith.com/>) model DTT900 (<http://www.circuitcity.com/ssm/Zenith-Digital-to-Analog-TV-Tuner-Converter-Box-DTT900/sem/rpsm/oid/204154/rpem/ccd/productDetail.do>). I stopped at Radio Shack (<http://www.radioshack.com/home/index.jsp>) where the clerk was the most knowledgeable. He still could not answer my questions. He handed me a bifold brochure. Radio Shack sold the Digital Stream DTX9900 Digital-to-Analog Converter Box. The clerk told me that it was the only model they sold. The web site says they sell the Zenith DTT900 Digital-to-Analog Converter Box and that it is available in stores. As you can tell from my experience, there is a lot of confusion as to what is available and just basic knowledge. The interesting thing about the variety of converter boxes available is that no matter the store or brand, they all cost \$60 plus or minus five cents. Thus, with the \$40 government coupon they all cost \$20. I understand that WalMart (<http://www.walmart.com/>) has a cheaper one. None of them allow the connection of more than one device (TV). Each has its own remote control that only controls the converter box. Each comes with cables to insert it between the antenna and the TV. Now on to my questions and my research for the answers. Time management is the primary reason I

(con't on page 8)

have a videocassette recorder (VCR). The VCR allows me to record programs I want to see at broadcast time and watch them on my schedule (usually with out commercial interruption). The VCR is a great invention. As of February 17, 2009, the functionality of the VCR virtually ends. Each device that uses a rooftop antenna or 'rabbit ears' needs a DTV converter box. The reason is that the VCR must always be set to channel 3 in order to receive signal from the converter box. It will pass the signal on to the TV. So far so good. What is the problem you might ask? Well I occasionally like to watch one channel while recording another. If I want to do that, I must have two converter boxes - one for the VCR and one for the TV. That configuration requires I have a splitter on the antenna so two converter boxes can be connected. When I want to watch what has been recorded, I must disconnect the TV's converter box from the TV and connect the VCR's converter box to the TV to watch the recorded show. That is extremely inconvenient. If I am away for a few days and want to record a number of programs, I can do that provided that they are all on the same channel because the converter boxes require human intervention to change the channel. The last and most frequent inconvenience is that to change the volume or mute the television, the TV remote must be used. According to the clerks that said they knew, no universal remote is available for the converter boxes, as yet. I hope this has been helpful. If you have any information, let me know. FYI - Neither the pamphlet nor the booklet answered the questions.

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

---

### **May 2008 CD of the Month** compiled by John Spizzirri

101Clips - Multi-clipboard program  
ARI - May Newsletter  
CDOMLists - Comprehensive list of programs on the CDOM  
CIAfactbook2008 - This year's CIA book about all countries  
Disaffected - Arcade-like game  
Easy2share - Easy file sharing tool  
FileMenuTools - Customize right click file menu  
FreebieNotes - sticky notes with an alarm timer  
Freeciv - Strategy game  
GnuCash - Free cash management program  
K1 - Collects information about your system  
Keynote - Unique text / rich text format editor  
OldTimeRadio - Edgar Bergen shows  
RuartBook - Free on line book by Dr. Mary Ruart

Plus many more!!

### CAEUG OFFICERS

<b>President</b>	Mike Goldberg
<b>V.P. (Programs)</b>	Tom Anzalone
<b>Secretary</b>	Dean Holste
<b>Treasurer</b>	L. Johnson
Newsletter Editor	Kathy Groce
Membership Chairperson	Pete Nicchia
& Circulation Manager	
Webmaster	John Spizzirri



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

#### ABOUT THE NEWSLETTER:

This printed version of our newsletter was laid out using **Adobe's Pagemaker Version 7.0** for Windows.

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 newsletter, 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 publication 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.

#### Beginner's SIG

Ask questions and discuss computer experiences  
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??

SIG meets before regular meeting from **9:05 to 9:45**

#### MEMBERS HELPLINE

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

Beginner Helpline . . . . . Billy Douglas

Beginner hardware problems . . . Dick Fergus

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

CD OF THE MONTH FORMAT: Is now available in **two (2)** flavors. The **Basic CD** will be packed with the standard items, while the **CD of the Month** will have NEW and updated items.

#### NEW Money Saving Offer for CD of the Month

**Pre Order + Prepay = SAVE \$\$**

The club will offer the CD of the Month on a pre order, prepaid basis. The charge will be \$70.00 a year for 9 months. This is \$20 annual savings over buying them for \$9 each month. Lynn Johnson, the treasurer, will keep track of anyone placing a 9-month order.

MAIL Request - There will be a \$2.00 mailing charge per CD

#### Meeting Location and Special Accommodations

The Glenside Public Library is located at 25 E Fullerton Avenue, Glendale Heights, Illinois. The Library is located on Fullerton between Bloomingdale Road (stop light intersection) and Schmale Road (stop light intersection) on the south side of Fullerton. Fullerton is parallel to North Avenue (Route 64) and Army Trail Road. North Ave. is south and Army Trail is north of Fullerton. Please park away from the building. Thank you.

The meeting(s) are not library sponsored and all inquiries should be directed to Mike Goldberg at MikeGold60137@yahoo.com. 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, Mike Goldberg at MikeGold60137@yahoo.com, at least five (5) days prior to the program, so that reasonable accommodation can be made for them.

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

## FIRST CLASS MAIL

---

**\* ! \*\* ! \*\* Notice Date information \*\* ! \*\* ! \***

The next **REGULAR** meeting will be held at the **Glenside Public Library**  
**25 East Fullerton in Glendale Heights, Illinois**  
starting 9:45am on  
**Saturday May 24, 2008**

**CONFIRMED** Future Meeting dates for **2008** at Glenside Public Library:  
**May 24, 2008 :: CAEUG Annual Picnic on Saturday JUNE 28, 2008 ::**  
**July 26 Room B :: August 23 full room A+B**

---

**Next presenter on May 24**  
**Our next presenter: Bill Douglas will discuss**  
**Computer Security**  
**See page one for more information**

### Hope to see you there!

CAEUG website has a new home.  
Remember to change your bookmark to the  
new address to  
<http://www.caeug.net>

#### 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