



# The Bridge

The Journal of the Memphis PC Users Group

Volume 20 Number 8

August 2004

For group information  
please visit our Web site:  
[www.mpcug.org](http://www.mpcug.org)

## *The Bridge Staff:*

Editor  
Gil Hennon

Review Editor  
Rick Fischer

Publisher Emeritus  
Les Owen

## *In This Issue*

The School Bell	Page 2
Photoshop & Illustrator CS	Page 4
The Wizard's Tips	Page 6
Excel Formulas/Functions	Page 8
Out for Review	Page 9
CoolWebSearch	Page 10
Event Calendar	Page 14

## Main Meeting Wednesday, Aug. 25 Southwest Tennessee Community College

5983 Macon Cove, Memphis

---

**NOTE CHANGED MEETING LOCATION**

## Farris Auditorium

First Floor - Farris Building

---

**Wizards Session 6:30 p.m.  
Main Meeting 7:30 p.m.**

---

Preparations for the August Meeting were not completed prior to the deadline for the Bridge. Come prepared to be surprised and bring along a friend!





# The School Bell

## News From MPCUG Education Services

By Gil Hennon, Education Services Coordinator

Several recent articles and news stories prove that the "Inducing Infringement of Copyrights Act" (IICA) bill introduced in Congress last month is not the only example of technologically clueless legislation. The IICA makes illegal anything that aids in the act of duplicating copyrighted materials. While Senators Hatch and Leahy intended to target peer-to-peer networks that share music and video files, their bill, as written, will also outlaw business and government networks, copy machines, tape and video recorders, and computer storage devices. Apparently, the Senators didn't consider how extensively their loosely worded legislation might apply. Some other bills introduced in the U. S. Congress and State Legislatures that needed more thought include:

A proposed law from Representative Mary Bono (R-CA) intends to ban spyware and phishing, making it illegal for any software to transmit personal information. If enacted as Bono introduced it, the bill will also kill legitimate exchanges of credit card and shipping information between buyers and sellers. Some analysts believe it might even make email illegal, since the sender and receiver's email addresses must be in the message header.

The Can-Spam act, passed and signed by the President last year, looks good on the surface. We all get too much junk email. But the wording of the bill makes it applicable to "any commercial electronic email message," and imposes unnecessary requirements on even a single email sent from a company to a customer who

expects and wants the message. It classifies as "spam" even the most innocuous commercial message, such as a notification that an order has been shipped.

Other anti-spam laws that have been proposed infringe on the First Amendment rights of U. S. citizens by outlawing email nicknames and services that strip off identifying headers and forward email anonymously. Similar state laws have been struck down by numerous courts, defending citizens' right to make an anonymous protest and avoid personal recriminations. Apparently the forces that want to take away that right have brought it before Congress because they have failed so miserably on a state-by-state basis.

A bill named "Protecting Children from Peer-to-Peer Pornography Act" puts the government in charge of deciding what kind of software should be developed, and how it should be developed. Let's not forget that old adage about a mule being a horse that was designed by the government. This effort to shield children from the seamy side of the Internet imposes onerous rules upon any site that provides downloads to verify that users are not children, or if they are children, that they have parental consent to download. In an attempt to make this law applicable to individuals and organizations in other countries, it requires foreign download site operators to hire a resident, U. S. citizen as an agent of the site. This agent would be responsible for verification of user age, keeping records, and filing reports with the Federal Trade

Commission. Since foreigners seldom even read our laws, and rarely bother to comply with them, it's likely that U. S. companies and organizations will be the only ones burdened with this cost of doing business. The law doesn't just single out porno sites. It would apply to any site that is a repository where software or image files are available for downloading. The Congress and the Courts have not yet, even after more than forty years and hundreds of porno-related bills and laws, been able to provide a definition of pornography usable as evidence. This law assumes that everything capable of being downloaded is going to be pornographic. If this bill passes, we won't ever have to wonder about the definition of litigation either!

At the risk of once again beating a dead horse, Senator Fritz Hollings (D-SC) introduced legislation a couple of years ago to protect the copyrights of movies that are transmitted over television. But the wording of his bill barely mentions television broadcasts. Instead, it requires programmers and software firms to embed government approved copy protection in all of their code. Fortunately for all of us, Fritz's Folly never made it to the floor for a vote.

Lastly, a bill in the California Legislature was aimed specifically at Google's free email, but written so broadly that it would apply to all email providers and developers of email client software. It would make it illegal to include in the email reader software features like searching through mail or converting text into graphics to improve readability. Why features like these might be construed to be intrusive or violations of personal privacy was never made completely clear. At any rate, after giving the public a good laugh, the bill never made it to a vote.

One political analyst who came from a technical background commented that lawmakers often think they see a solution, but they seldom understand all of the technical ramifications that solution might have. For example, to prevent people from being injured by falling objects, a congressman might introduce a bill to make gravity illegal. Another example was Daylight Saving Time, a law passed to make the sun come up later.

At MPCUG Education Services, the Wizards consider all possible solutions and come up with the best one for each situation. Bring your computer problems to them before each main meeting and take home good advice that even money can't buy. You and your computer will both be glad you did!

--0--

This newsletter is a monthly publication of the Memphis PC Users Group, Inc. (MPCUG) Copyright ©1998 MPCUG. Unless otherwise indicated, articles may be reprinted in other non-profit publications without express permission, subject to the following conditions. Full acknowledgement must be given to the MPCUG, The Bridge, and the author. The article must be reproduced in its entirety from magnetic media, without editorial changes, deletions or additions. Two copies of the entire publication containing the reprinted article should be sent to The Bridge within 30 days of publication. All other rights reserved. Any changes to the article require the written permission of the author. All articles are made available through the APCUG BBS and on disk to qualified non-profit organizations.

Any opinions expressed belong to the author and not the Memphis PC Users Group, Inc. Articles in this newsletter may contain trademarks of various companies. Any proprietary right those companies have in those names is hereby acknowledged.

Unless otherwise indicated, all submissions to this newsletter become the property of Memphis PC Users Group, Inc., and are subject to editing by the staff. The MPCUG reserves the right to determine the suitability for publication of all items received.

Members are encouraged to submit articles for publication. By submitting articles, the author gives permission for publication in this newsletter and for publication by other user groups. The editor cannot guarantee that all submissions will be used.

The information contained in this newsletter is believed to be correct and accurate; however, the Memphis PC Users Group, Inc., cannot and will not assume responsibility for the consequences or errors contained in articles or misapplication of any information provided. Any information used from these articles is at the user's own risk. If a review of any hardware or software contains errors or inaccuracies, upon notification of these errors or inaccuracies by the manufacturer in writing, a correction will be printed in the subsequent issue following receipt of these corrections.

The Memphis PC Users Group, Inc., makes no warranty, expressed or implied, as to the suitability of any advertised product. You must determine that yourself. The Memphis PC Users Group, Inc., also expressly declines to assume liability for any use of any published software, and your use of same constitutes your agreement to hold us blameless.

Memphis PC Users Group, Inc.  
P.O. Box 241756  
Memphis, TN 38124-1756  
Internet: [www.mpcug.org](http://www.mpcug.org)  
Information Line: 901-375-4316

# Using Adobe Photoshop CS and Illustrator CS

---

*Book Review*

## Reviewed by Jin Yang

Even though rated as “beginning to intermediate” level, the *Using Adobe Photoshop CS and Illustrator CS* will probably be more favored by intermediate level readers.

The book can be divided into three parts: creative suite common concepts, *Photoshop CS* and *Illustrator CS*. It is well known that different persons have different learning styles: visual, auditory and kinesthetic. The book attempts to appeal to at least two different learning styles to some extent. For visual people, the book provides graphs and screen shots to show dialog boxes and illustrate steps. For those who prefer kinesthetic experiences, it is also possible to read through the book with *Photoshop CS* or *Illustrator CS* open on computer. However, the book is not a project oriented or hands-on experience-oriented entry level book.

### Version Cue

The author did a reasonable good job in explaining the common concept of the Creative Suite package (Version Cue) and its core technology (pdf) even though

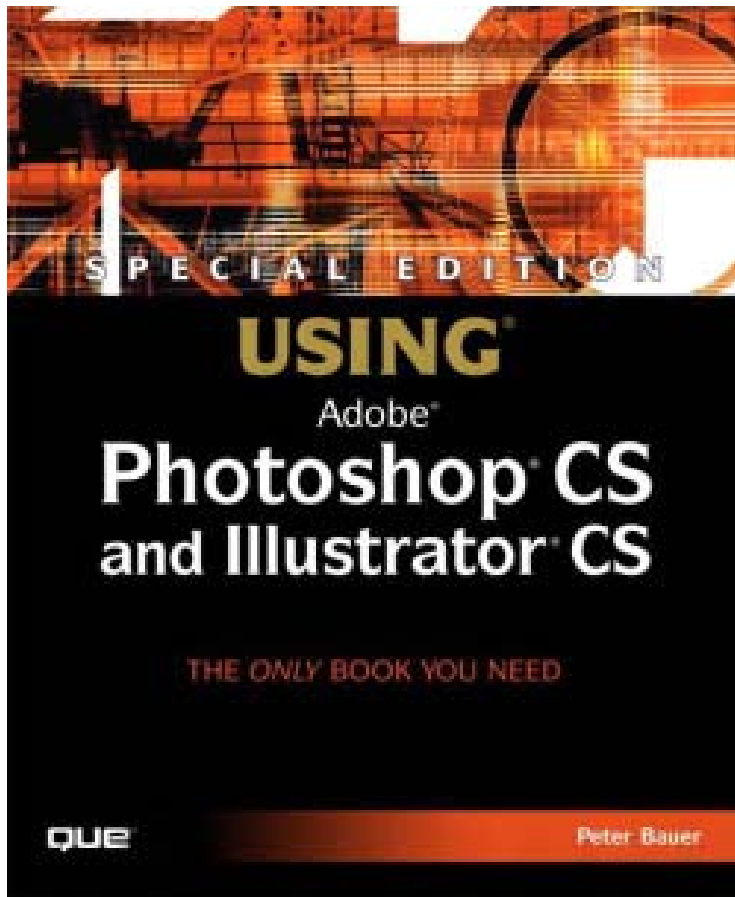
skipping the part will not affect the mastery of the editing skills covered at later chapters, which is probably in the best interest of readers. It allows for the book to be used as a tool book. I especially like the way the part on Version Cue is presented: from a brief introduction to Version Cue, enabling Version Cue, to accessing Version Cue features in the creative suite programs. The section on enabling Version Cue has a lot of screen shots for readers to visualize what appears on the computer screen, which is a very important learning aid for first time Version Cue users.

### Photoshop CS

If you need to find out why *Photoshop CS* is better than *Photoshop 7*, the author gives you a complete list of reasons and elaborates on the important new features. Even if you are not really interested in the new features and only want to learn *Photoshop* skills, the author did a very good job in explaining skills and concepts that can be confusing to *Photoshop* learners. For instance, most students in my Desktop Publishing and

Web Site Management classes find it difficult to understand the principle behind the mask and the usage of mask. The author did a reasonable job in instructing students on the principle of alpha channel functioning at the core of mask technique. He also walked through the key steps of applying the tool in the image editing process. The nice thing about the section is that the author set up a lot of illustrations to go with the words to allow readers to visualize what appears on the computer screen. For a short (20 minute) session of concentration, a learner may be able to get the point. What is absent in the section of the book, however, is the comprehensive approach to steps. For a beginner, it will probably take a longer time to figure out how to get to where the author started and began to pick up. It would be nicer if the author could always offer information on steps from step number 1 to step number 10 or whatever.

The thing I like and enjoy reading most is the information contained in the tip box, where the author offered many useful tips on the relevant



skills and techniques. But I know from experience that many readers ignore that part most of the time since that part is not a significant part of formal text. What can be improved, obviously, is to embed the tips into the formal text and “force” readers to get them.

Another thing that deserves mentioning is on reference to different pages. When I tried to do some sample reading, I always came across references. For instance, on page 307, the author talked about the type mask tools, which, by the way, is not a new feature of *Photoshop CS*. He pointed out there are two type masks: point type

and area type masks. However, only point type mask was explained on that page and the following page. Type mask page was not really focused on. Instead he referred people to Chapter 12 on page 392 for a detailed discussion. Even though it is nice to find the relevant information quickly by jumping from page 307 to 392, it would be beneficial if the author could at least give a quick overview of how to use area type mask.

#### **Illustrator CS**

As a vector art program, *Illustrator* enables users to draw customized shapes and art works by placing paths. The author did a good job in explaining the concept of path in comparison to raster or

pixel concept. Even for a beginning learner of *Illustrator*, it won't be difficult to get started with a basic understanding of anchor points by reading the relevant chapters in the book. However, for those who would like to quickly get the project done and move ahead, the book may take a longer-than-expected time to digest the concepts first. The detailed and comprehensive account of concepts will develop a genuine master of the *Illustrator CS* with time and patience available. For a person who wants to focus on hands-on experience and quickly get it, that expectation may fail.

Overall, the book's approach to *Photoshop* and *Illustrator* seems to be both concept-oriented and skill-oriented organized in a dictionary way. It might be a good reference book for an instructor of the program or a manual reader kind of person. After all, this is a book with 1,150 solid pages of information. Who, in the world, will dare to take in all the information provided page after page? But placing the book on the bookshelf to decorate the room and use it as an encyclopedia is not a bad idea at all.

Bauer, Peter. *Using Adobe Photoshop CS and Illustrator CS: The Only Book You Need*. 2004, Que Publishing. \$50.

# The Wizard's Tips

---



(From the Wizard's Inbox:)

Dear Pointy Headed Knower of All Answers,

I know that I can use Ctrl-Alt-Delete to bring up the Windows Task Manager, and that I can see all of the running background programs on the Processes Tab, but I can't make sense out of the process names listed there. They don't seem to have much relationship to the actual names of programs on my computer. I suspect that some are there without my permission and that I probably don't want them. How can I find out what these processes are and what they are doing?

Thanks . . . Process Clueless

---

Dear Clueless,

You probably think that those cryptic process names in the Windows Task Manager were put there to keep you from knowing what's going on behind your back. You're probably right. But there are ways to find out what those processes are. Here are three Web sites with process databases. Look up those cryptic names and find out what programs they represent.

[http://www.answerthatwork.com/Tasklist\\_pages/tasklist.htm](http://www.answerthatwork.com/Tasklist_pages/tasklist.htm)

<http://www.reger24.de/processes.php>

<http://www.liutilities.com/products/wintaskspro/processlibrary/>

The last one also sells a utility that will search your task list and identify all processes that are running on your PC.

You might also consider a couple of other useful utilities. You may have already found that some processes in the Windows Task Manager cannot be killed. Usually this is because the permissions associated with the process don't allow the user to exercise any control over them. Diamond Computer Systems makes a freeware utility named *Taskman+* which elevates the permissions of the Windows Task Manager program so that all processes can be killed. The user must be logged in as Administrator to use this utility. Get it at <http://www.diamondcs.com.au/index.php?page=products> or one of the well-known software download sites.

Several replacement "task manager" programs are available as shareware. They offer more features, such as expanded information or the ability to kill multiple processes that the standard Windows Task Manager can't handle. Most give full information and startup path of every background process. They usually allow starting, stopping, deleting, or sending a process to quarantine and show the memory and CPU resources each process uses. Some have a subjective "security risk" level assigned based upon typical traits exhibited by trojans, malware, spyware, and worms. The risk assignments can be helpful, but should not be accepted as fact, since some essential system and application programs will occasionally perform the same actions as malware. Most of these programs cost \$25-\$50 and have a free trial period. *Security Task Manager* from A&M Neuber GbR is a good example of this type software. Look it over at <http://www.neuber.com/taskmanager/index.html> and Web search

for similar products.

While we are on the subject of Windows Task Manager, here are a few tips on using the standard Microsoft version that Windows installs:

Tip #1 - In the Windows Task Manager Applications tab area, select an application. Right-click and choose 'Go To Process'. The task manager will automatically open the Processes tab and select the actual process (EXE) that runs the application.

Tip #2 - On the Applications tab page, more than one application can be selected to be killed. (This will not work on the Processes tab page.)

Tip #3 - Click the column headings on the processes tab page to resort the list. For example, click the CPU or MEM Usage (RAM) columns to bring the resource hogs to the top of the list.

Tip #4 - Some processes have sub processes running inside them. If the END PROCESS button won't kill the process, you may need to highlight it, right click, and choose END PROCESS TREE in order to kill all of the sub processes.

Tip #5 - Add more information columns to the Task Manager by clicking VIEW and SELECT COLUMNS. Some of this information is only useful in very specific circumstances, but a few items, like Virtual Memory Usage, can be helpful for troubleshooting. Page Faults tells how many times a page was loaded from storage because it was not available in virtual memory.

Whether you use the Windows Task Manager or one of the third-party replacements, these are very handy utilities for troubleshooting and for stopping "Trojan Horse" background programs. They can keep you from remaining "Process Clueless."



**TOTAL TRAINING  
PROUDLY PARTNERS WITH THE  
Memphis PC USERS GROUP**

**TO OFFER ITS MEMBERS  
10% OFF**

**When you call in to 1-888-368-6825  
and reference offer code: USRGP2004**

**Visit our web site [www.totaltraining.com](http://www.totaltraining.com)  
for information on all of our training products**

**Offer valid through August 31, 2004; cannot be combine with any  
Other offer; is valid ON ALL Total Training Products**

# Formulas and Functions with Microsoft Excel 2003

Book Review

Reviewed by Rick Fischer

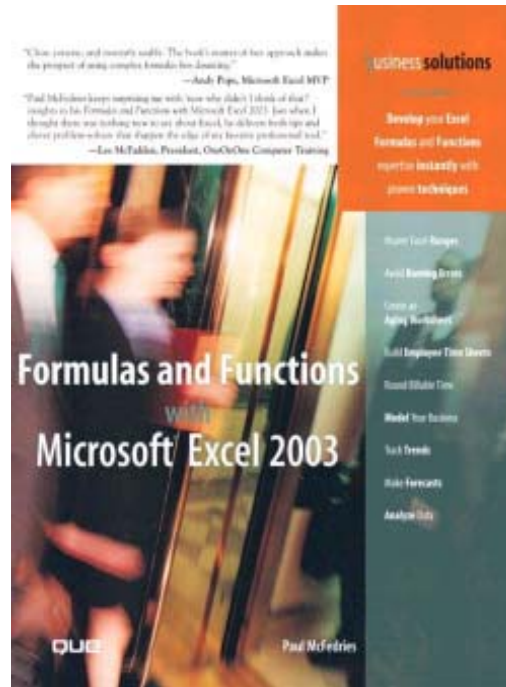
I earned a master's degree in management in the 1970s. We did transportation problems and linear programming by hand. We optimized and minimized and it was all done a line at a time with pencil and paper. I was amazed that someone knew how to get answers to these tough business questions.

Now, I am amazed that someone has made getting the answers so easy.

It is almost 30 years later and getting the answers is now possible with *Excel*. You still have to conceptualize the problem and solution, but the drudgery of going through the procedure has been significantly reduced.

I have *Excel 2003* and I didn't know it could do the things that McFedries demonstrates in the book. He also has a Web site where you can download the examples from the chapters. Just reverse engineer the examples to let them work for you.

*Formulas and Functions with Microsoft Excel 2003* is part of Que's business solutions series. Great idea!



## Solver

At the heart of working the problems requiring calculus is Solver. If you look in the *Excel 2003* Help menu you will find quite a few topics around the search term: solver. Try "linear programming" - nothing. "Calculus" - nothing. "Simplex" and "maximize" both return solver references.

Solver has a whole chapter devoted to it in the book. And, you get the samples on the Web site. With this I could figure it out.

## Natural progression

McFedries says that

the book "isn't meant to be read from cover to cover." Perhaps. But, that's just what I did. You have to understand ranges before you can apply formulas. And you have to understand formulas before you can build models. There's a definite training logic to all this and I didn't want any gaps in my understanding when I got to the unfamiliar parts.

There are lots of personal Post It tabs in this book. I thought in the early part that it would be a review, but I kept finding things that I never knew or forgot. For example, I wondered what those green triangles were in some of my spreadsheet cells. I learned that this is how *Excel* tells me it thinks there is an error in my formula. Having played with it, I now know that it can be wrong in its thinking. Nonetheless, I will check instance where I find the green triangle.

And, later on I found solutions to things I had wondered about in *Excel*, but didn't know where to start.

One of those solutions

# Out for Review

involved counting people in columns. I make up lists with graduate students, their adviser and so forth. I do the sums manually and place them in a summary box. Now I have a strategy to do it automatically.

And, those of you who have reviews out. I learned how to show how many days you are overdue with your review.

Almost every special function is explained, e.g., financial, logical, trig. I think he said he skipped a few. He tells you what to put in the variables and how it might be used in real life. That's also true for the statistics module, something not well covered in most books I've seen on *Excel*.

It us heavy on financial and business models, so our readers should be pleased.

Systematically going through *Formulas and Functions with Microsoft Excel 2003* should be real confidence builder. It will reinforce what you already know, but I suspect that you will learn just how much you didn't know about this very powerful program.

*Formulas and Functions with Microsoft Excel 2003* by Paul McFedries. 2005. Que. 486 pages. \$35. For intermediate users.



Here is a list of software, books, or other products you can expect to see reviewed here in the coming months. These members checked out items to review for the benefit of all.

Windows Me: The Missing Manual	Greg Adams
Teach Yourself GoLive 5 in 24 Hours	Allison Banks
Teach Yourself Adobe Photoshop CS in 24 Hours	Judith Bogan
Windows Security Handbook	Dorothy Drum
The Little Web Cam Book	Mike Heinrich
Microsoft Works 7.0	Jim Ingram
Zoo Tycoon	Jim Ingram
How to Use Microsoft FrontPage 2002	David Levine
The Complete Idiot's Guide to Starting A Business Online	David Levine
User Interface in C#	Jim McGee
Amazon Hacks	Vanessa Muldrow
Windows XP Pro (book)	Daniel Notowitz
FrontPage 2002 Unleashed	Carl Osborne
Using Excel 2003	Jim Redmond
HiJaak ver 5	John Schuster
Macromedia (book)	David Stowell
Windows XP (book)	Terry Thomas
eBay Hacks	Tommy Towery
SPSS	Jin Yang
Using Photoshop CS	Jin Yang

Thanks to all who checked out products for review. Let's keep the Group vital and provide value for membership.

# The Totally Not Cool Web

---

*Editorial*

by Gil Hennon

A while back, I made what some folks thought was a rash prediction. My opinion was that spyware and scumware would become a much bigger problem than viruses, worms, or even spam. I haven't changed my mind, even though I've listened to several challenging arguments. In fact, the recent experiences of a couple of friends have reinforced my position. They unfortunately became infected by CoolWebSearch (CWS), a form of scumware classified as a browser hijacker.

Browser hijackers work by changing a computer user's home page and search engine addresses to ones belonging to a "pay-per-click" advertising site, or one of its affiliates. Making these changes in a browser configuration is a simple deal, and usually it is just as easy for a user to change these settings back again. But some of the more sophisticated hijackers take a few more steps in order to make their changes as permanent as possible. They add keys to the registry that define new services to run on the computer, and they often replace the computer's HOSTS file of trusted and frequently visited Web sites. Just in case the user knows how to fix all of these problems, a secret EXE or DLL file is planted that restores the hijacking settings every time the computer is rebooted. Getting rid of a browser hijacker can be a time-consuming and frustrating ordeal.

While the purpose of the hijack is to make money, and not to cause damage, browser hijackers are considered "benign" by most of the information security community. They don't destroy any data, nor do they usually violate a users' privacy on computers they infect, but the underhanded and strong-arm methods they employ cause system instability,

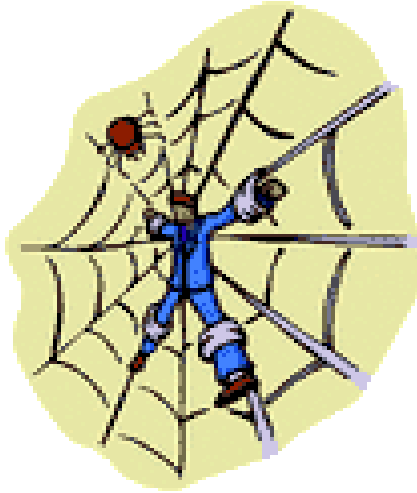
security vulnerabilities, and system slowdown.

Among browser hijackers, CoolWebSearch (CWS) is the one that's on steroids. The original infection was based on datanotary.com, a hacker site and tool for installing software on any connecting PC. Even though the Internet Explorer security vulnerability it exploits has been fixed by a Microsoft critical update patch, there are still plenty of unpatched PCs available and infectable. A cascading style sheet, configuration change tools, and the secret, hidden file that controls and restores CWS components are all dropped on a vulnerable PC through a back door. From that point, CoolWebSearch directs all Internet Explorer page requests to its own servers, and all searches to its own engines. Only sites affiliated with CWS and participating in click-through revenue can be accessed by the computer user. Most of the affiliated sites deal exclusively in pornography.

The first CoolWebSearch infection was discovered during the summer of 2003. In about a year, it has spawned about forty variants, some similar to the original, but many that are related only because they hijack users to the same group of Web sites. CWS and its affiliates have grown into a population of more than 1,000 Web sites, and although they have diversified a bit, porn sites are still the majority. CWS has also evolved into the most difficult to remove infection ever created. Almost every two weeks a new variant appears, each with additional "features" that embed the infection deeper within the system, each better hidden and more protected from anti-virus and spybot eradication tools, and each more complicated and frustrating to remove manually.

Where did CoolWebSearch come

from? The company registered under that name is located in Russia. It was begun as a pay-per-click search engine by Louise Vitte, who is still chief officer. She channeled



searchers to vendor sites and was paid a few cents for each “click-through.” In order to bring in more traffic, Vitte hired programmers Alex Hatkinson and Serge Stepantsov to create a tool that brings computer users to the CWS site every time they access the Internet. These tools are issued to “affiliate” sites. When an unpatched Internet Explorer browser visits an affiliate site, the tool invades the visiting computer and installs one of the CWS infections. The infection contains a unique code that identifies the affiliate site that installed it, and each time the infected computer clicks-through a CoolWeb Search engine on the way to a vendor site, the affiliate and CWS share the click-through payment. With this offer of free money, over a thousand affiliates have already joined, and estimates have been published that about one hundred new sites join each week. Even Louise Vitte probably does not know exactly how many affiliates are already out there infecting PCs for her, or how fast her ranks of affiliates are increasing. She does know that she has built a business that takes in many millions of dollars per year.

It could be a bona-fide Cinderella story if there wasn't a very seamy underside. First, CoolWebSearch exists only because it has been able to infect computers and effectively control where that computer can go on the Internet. Most of the places CoolWebSearch will let a computer go deal in pornography. A sideline

business of pop-up advertising also traffics heavily in porno, and when CWS replaces your “Favorites” list with its own, it is full of porno sites too. If this wasn't bad enough, the changes CWS makes to the computer cause frequent program and system crashes. Some communication and Internet related applications are corrupted and no longer work correctly. A back door is installed that allows third-party hackers to run various kinds of software on the infected machine. Even when an infected computer and all of its original applications still run, CoolWebSearch brings the speed down to a crawl.

The CWS affiliate sites may think it is great, but users who have experienced a CWS infection consider it the lowest of scumware. During its evolution to the latest and most obnoxious variant, combinations of the following nasty tricks have been used in the infecting software:

- Replace the browser Home Page URL with a CWS site or a blank line.
- Install a Web server on the computer at address 127.0.0.1 (localhost).
- Use the localhost server to point all searches to a CWS engine.
- Replace the DNS HOSTS file so the computer only goes to CWS sites.
- Replace the MSN address-bar search with CWS address-bar search.
- Spoof the URL window in IE so that it shows the address typed by the user while actually going to a site that belongs to CWS.
- Replace the font used in the URL window so addresses can't be read.
- Forces the browser into an error that defaults to a CWS site.
- Installs a secret, hidden “bootconf.exe” file that replaces deleted CWS components each time the computer is booted. In later variants, this file has a randomly generated name so it is more difficult to find.
- Adds coolwebsearch.com to the Trusted Sites list, allowing the site to download and run any software it wants to on an infected machine without trigger-

ing a Windows alert.

- Redirects Yahoo, MSN Search, and all countries versions of Google to coolwebsearch.com.

- Modifies INF files that control drivers and system functions in Windows.

- Installs registry keys that activate CWS every time the computer boots up.

- Installs a back door and Trojan software that can be used for denial-of-service and other mass attacks against anti-virus and spyware removal software Web sites.

- Turns off "pop-up" eliminator software and installs a pornographic "pop-up" advertisement generator.

These functions in CoolWebSearch infections are well written code. They perform many complicated and sophisticated tasks, all aimed toward getting the computer to access a CWS Web site or search engine while protecting CWS from any tools or procedures that might disable it. In the past month, two users discovered CWS on their computers and experienced the frustration of trying to remove a very elaborately defended infection.

Jim McGee, Treasurer of MPCUG, found one of the latest variants of CWS on his home computer. He tried all of the usual methods to eliminate it, then went to the Web and found several sites that provided some insight into what he was trying to fight. *CoolWebSearch Chronicles* at <http://www.spywareinfo.com/~merijn/cwschronicles.html> is the saga of Dutch software developer Merjin Bellekom's long-standing battle with CWS. He wrote the CWS shredder tool to remove early variants and gained a reputation for being the foremost of the anti-CWS combat troops. Unfortunately, Bellekom has thrown in the towel on this Trojan war. *The Register* (<http://www.theregister.com>) reported that the final update to CWS shredder was released at the end of June. Bellekom has been increasingly frustrated by the complicated infection methods of CWS and its aggressive variant release schedule. He does not have the tools nor the time to assemble automated CWS clean-up software anymore. Merjin

has linked some of the newer CWS variants to the "ByteVerify" hacker exploit of the Microsoft Java Virtual Machine, a vulnerability that has not been patched so far. Besides the technical difficulty of developing removal tools, Bellekom has been harassed with Denial-Of-Service attacks on his Web site from CWS infected zombie computers, and also has seen CWS versions that contain code to disable and corrupt his CWS shredder tool.

The variant that infected Jim McGee was not one that CWS shredder can fix. Jim had to resort to manually identifying files and registry settings belonging to CWS and removing them one-by-one. For a while, he was doing this regularly, because CWS was reinstalling all of its components whenever he rebooted his computer. Eventually, he found AVG Anti-Virus from Grisoft, Inc., a tool that was able to identify the randomly named, secret DLL that was reinfecting his computer. Although he was unable to delete the file, he was able to change the filename extension through a DOS window. The DLL is now inactive and no longer able to reinfect. Since it is still there, Jim gets daily notification that he has a virus from Norton. Other than that annoyance, Jim's computer is clean.

That wasn't the case for another user who is not an MPCUG member. She called and described conditions that were very similar to those Jim had encountered. One of the "tipoff" symptoms was an Internet Explorer Browser that always displays "about:blank" on the URL address line. Merjin Bellekom's CWS shredder tool could not remove this infection. The situation was more complicated than Jim's because her operating system is Windows XP, which uses the NTFS file system. NTFS makes command line entries obey its permissions settings, so the CWS hidden secret control file resisted all attempts to delete or modify it. Several different anti-virus and spyware removal tools also failed. Finally the only solution was a complete system reload from the manufacturer's "restore" CD-ROMs. The

first reload didn't last very long. Once the system was up and running, she reinstalled her backed-up data and reconnected to the Internet. Shortly, CWS was back, and another complete reload was done the next day. Suspecting that CWS somehow got into her backup files, she is scanning them carefully and bringing them back just a few at a time. Hopefully the infected file(s) will be caught before they can introduce the clean system to CWS again. After more than a month fighting CoolWebSearch, she will quickly tell you that this was an educational experience she really didn't need. CWS won all the battles in this Trojan war, and a complete system reload was the only strategy that restored peace.

Anti-virus software, such as McAfee and Norton's products, may recognize some of the CoolWebSearch Trojan variants. Win32.Startpage.C is the anti-virus engine name for some early variants, and JS.CSSPopup.B refers to some of the later ones. Other names for the same infections are Win32/IEstart.trojan and JScript/IEstart.Trojan. Spyware eradication software likewise can recognize some CWS components and remove them, but no tool has been devised—either spybot killer or anti-virus—that can successfully remove every component of CWS, especially the hidden secret DLL.

That secret DLL, the bane of everyone who tries to remove CoolWebSearch, might be an exploitation of another Windows bug. No documentation exists on its peculiar permissions level which allows copying, but no other manipulation by anyone including the Windows Administrator. With the permissions set in this manner, the file is invisible and its attributes cannot be changed to make it visible. In some variants of CWS, a registry key has similar permissions and cannot be seen. The trick to finding the secret DLL is to use a tool that will search and open every file it encounters. When the tool is unable to open the secret CWS DLL, an error message is generated that contains the path and file name. Then a

savvy CWS hunter knows what to delete.

Security experts blame Microsoft for the existence of these secret files. Some say it is a bug in Windows. Others believe it is one of the tricks that Microsoft reserves for its own use, and that the CWS developers just accidentally discovered it. In either case, CWS knows how to create and use an infernally difficult file to delete. Another Windows "flaw" exploited by CWS—one that Microsoft probably hears regular gripes about—is how Windows allows just about anything to write to the registry without any alerts or warnings to the user. Both of these bugs need to be fixed quickly.




When his Internet Explorer browser would no longer work properly, Jim McGee began using Mozilla's new Firefox browser, which CWS can't infect yet. The old Mozilla browsers, Opera, and a few others are also immune to CWS. After a month of using Firefox, Jim only goes back to Internet Explorer for his Windows Updates and when connecting to certain sites that contain Active Server Pages or Active X components.

The secret manipulations CWS performs on computer systems brings back memories of the days of DOS, when anything that messed around with CONFIG.SYS or AUTOEXEC.BAT without first asking permission provoked visions of gallows and guillotines. A basic survival instinct has been dulled by Windows convenience. We are not as protective of our system registry as we used to be of those two relatively simple DOS configuration files. Logic would say we should be extremely suspicious and riled when registry keys are added or modified without our permission, but we aren't. Maybe that's because we hardly ever know when it is happening. Maybe we need to change that. Maybe scumware like CWS will bring about that change. In the meantime, Microsoft needs to fix the bugs that CWS exploits, and we need better tools to fight CWS and other scumware.

--o--

For up to the minute information and special updates  
be sure to check our Web site at:

***www.mpcug.org***

	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
AUG 2004	9	10	11	12 VISUAL STUDIO	13	14 WEB WRITERS MS OFFICE
AUG 2004	16 WORDPERFECT	17	18	19	20	21
AUG 2004	23 CLIPPER	24	25 MAIN MEETING	26	27	28 INVESTMENT
AUG-- SEPT 2004	30	31	1	2	3	4 INTERNET HARDWARE
SEPT 2004	6 	7 DOT.NET	8	9 VISUAL STUDIO	10	11 WEB WRITERS MS OFFICE 
SEPT 2004	13	14	15 	16	17	18