

Bits & Bytes

A Publication of the Kern PC Users Group



**STEVE GARCIA PRESENTS
IP COP SOFTWARE**

AT 7:00 PM OCT 9



Board Members

President:

Rhonda Pierce 661-363-0771
Pierce27@earthlink.net

Past President:

Bill Peacock 661-328-0180
bpeacock@pacbell.net

Vice President:

Rick Daney
rdaney@bak.rr.com

Secretary:

Tony Rizos 661-872-5622
trizos@ncinternet.net

Treasurer:

William Lowell 661-664-1244
wlowell@bc.cc.ca.us

Director:

Steve Garcia
sgarcia@bak.rr.com

Director:

Caroline Corser 661-871-9201
Cmcorser@pacbell.net

Director:

Lee Lentz

Director:

Dr. Leonard Liss 661-663-8834
lissmd@earthlink.net

Newsletter Editor:

David Chalmers
dcchal@pacbell.net

Education/SIG Coord

Rick Daney

Kipug Webmaster

Sarah Perelli-Minetti
sarahpm@sbcglobal.net

The following rates are for one insertion in the **KIPUG** newsletter. All copy must be received camera-ready, no later than the 15th day of any given month for publication in the following month's newsletter.

Camera-ready copy should be submitted to Bits & Bytes, c/o Dave Chalmers, P.O. Box 2780, Bakersfield, CA 93303

KIPUG members who have computer related items for sale or trade or who have information they would like to share with other members may do so **FREE** of charge as space permits. Ads larger than business card size are subject to 50% of normal advertising fees. Non-members are subject to the normal advertising fees.

Business Card \$ 5.00
Quarter Page \$ 15.00
Third Page \$ 20.00
Half Page \$ 30.00
Full Page \$ 60.00

ADVERTISERS

KIPUG will mail your direct computer user targeted mail advertisement (fully prepared for mailing, including postage) to our entire membership at a reasonable fee. For more information, please contact Rhonda Pierce, President, at pierce27@earthlink.net.

Table of Contents

Attack of the Worms	pg 4
Pentium 3.06	pg. 6
Should have learned	pg. 8

The Prez Sez

Well, well fall will soon be upon us, however somebody forgot to tell the weather that it's October, giving us temperatures in the high ninety's. I personally like fall and spring. The only problem is in Bakersfield, we don't get much of either season.

Our group is trying to purchase a new updated computerized projector for guest speakers or our members to use at our monthly meetings. We don't want to use our treasury money if we don't have to for the projector. So we decided to have a fund raiser for the group. We are going to have a raffle drawing selling tickets for \$2.00 each or 6 for \$10.00. We would like all the members to help sell and buy tickets. The prizes will be raffled off at the February Meeting and you don't have to be present to win. So talk to all your friends, relatives, neighbors and co-workers to sell, sell, sell.....

We are going to raffle off a wonderful training opportunity provided by New Horizon's Computer Learning Center as first prize and second prize will receive a really nice cordless keyboard and cordless mouse. We hope everyone will rally around this fund raiser, as it will benefit all of the members.

This month we have Steve Garcia speaking on IP COP software. A big thanks to Steve for speaking on KNOPPIX and IP COP. We really appreciate your efforts. See you there on October 9th. Rhonda [:-)

Attack of the WORMS - Did We Learn Anything?

By Ira Wilsker

Recent weeks have seen the most prolific spread of computer viruses and worms in history. While computer viruses and worms have been around for years, the recent attacks of Blaster and Sobig-F, broke all records for the speed of dissemination and the numbers of computers infected. Fortunately, the payloads carried by these programs was quickly identified and neutralized before they could wreak more havoc on our cyber infrastructure. While annoying and troublesome, they apparently did not carry a very dangerous payload.

My first indication of the Blaster attack was a cryptic call I received asking about some bizarre error statement that appeared in a window that popped up; she had opened no suspicious emails, and had updated antivirus software installed. A quick search turned up a warning from Microsoft dated mid-July that there was an identified vulnerability in Windows NT, 2000, and XP, and that Microsoft had released a "Critical Update" patch. Users were advised to download and install this patch immediately. Other references, also from mid-July, were news stories on computer security that there was this vulnerability in some version of Windows, and that Microsoft had released a patch to eliminate the threat. Some pundits also

speculated that it was only a matter of time until someone took illicit advantage of the vulnerability. I told her to download and install the patch, to see if that resolved the problem. Minutes later my daughter called from Miami and said that she just had this weird window open on her computer, and a cryptic statement appeared, identical to the other caller's. Likewise, she had opened no email attachments, and had updated antivirus software installed.

Two strange but identical symptoms within a matter of minutes, on two XP computers, hundreds of miles apart, seemed to be more than a coincidence, but was likely some type of new virus. I posted a request on the restricted "High Tech Cybercrime Consortium" mail list to see if anyone else had encountered such a strange occurrence. Within minutes I received several replies indicating that others had similar inquiries, but other than a suspicion that it was some type of new virus, no one had any other information. A search of the major antivirus sites turned up no new alerts. Within the next hour, I had received several more phone calls and emails appealing for help. By that time the first security alerts traversed the net that a new computer worm, named "Blaster" or "LoveSan" had been identified. Blaster was transmitted directly from computer to computer over the internet or networks without the traditional vector of email, by using a sophisticated

utility that searched for other vulnerable computers to infect, and then infected them. The victim had no warning other than to find that his computer was compromised. Carrying a denial-of-service payload, Blaster would have all infected computers attack the Microsoft

Windows Update server at predetermined times, in a coordinated attack. Most of the antivirus software publishers promptly updated their detection files, and provided a free downloadable utility to detect and remove Blaster from infected computers. Microsoft launched a media blitz encouraging users to download and install the security patch which had been released a month earlier, and published instructions on removing the worm. Microsoft took down the server that was the target of the attack. While there are many computers still infected with Blaster, it can no longer shut down Microsoft.

Before we had a chance to catch our breath following the Blaster attack, inboxes were flooded with a variety of emails with the topics “Details”, “Thank You”, “Your Application”, “Approved”, “That Movie”, “Wicked Screensaver”, or some variation, possibly using “Re:” as a prefix. That first morning of the Sobig-F assault, I turned on my computer, updated my antivirus software, and was greeted with an over-filled email box containing over 700 emails with suspicious topics. I

use a free program, Mailwasher (www.mailwasher.net), to screen my email, and allow me to delete spam and viruses before they can get on my computer. Even though I was then not aware of Sobig-F, I knew better than to open suspicious emails, and to delete them. As with the Blaster attack, a similar sequence of notifications, antivirus updates, patches, and other fixes were made available in the hours following the onslaught. By that evening, I had received over 1200 copies of Sobig-F; the following day, I turned on my computer and found over 2000 infected emails, with additional emails arriving at the rate of several per minute; by the time I shutdown that evening, I deleted several thousand more emails. Sobig-F hijacks the address books of infected computers and repeatedly sends out emails with randomly selected “From:” lines concealing the source. Many servers automatically bounced infected emails, contributing to the avalanche.

Containing a payload that could launch a denial of service attack on multiple servers, as well as connect to a porn site, Sobig-F is scheduled to self-destruct on September 10.

So, what have we learned from this double-barreled attack? First, no matter how good it is, antivirus software may not protect us from rapidly spreading viruses and worms that become endemic before the publishers can respond; still, there is no

excuse for not having frequently updated antivirus software installed. While Blaster spread through stealth, Sobig-F was a suspicious email attachment that often came from an acquaintance.

Practicing “safe hex” would prevent Sobig-F infections. Also, we had better pay attention when Microsoft announces critical security updates, and install them. We must frequently check for these patches at windowsupdate.microsoft.com, and install them.

It was bad enough to become a victim of the insidious attacks. It will be even worse if we do not learn from them, and act appropriately. More such attacks will inevitably follow.

Ira Wilsker is the Advisor for Region 8, APCUG Representative & Bylaws Chair for the Golden Triangle PC Club, a columnist for The Examiner in Beaumont, Texas, and has two radio shows. He also graciously shares his articles with the APCUG editors.

There is no restriction against any non-profit group using this review as long as it is kept in context with proper credit given the author. This review is brought to you by the Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organization of which this group is a member.

Intel Pentium 4 3.06GHZ Processor/Motherboard

Dennis Kemper-Executive Director
Las Vegas PC User Group

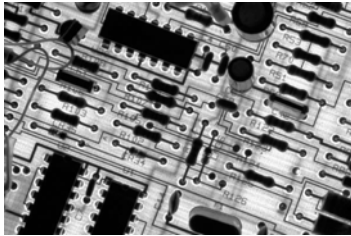
Last year at the annual Association of Personal User Groups Conference – APCUG for short, we had a "new" vendor as a sponsor...this company is very well known in the PC Industry, and many of you have their products on your computers. You might remember phrases like 8086, 386, 486, and Pentium...oops I gave it away....this company is called Intel.

Intel is located in Santa Clara, California where they have been doing business for close to 35 years, they are the leading company in the development of microprocessors and are at the center of the digital revolution. We can thank them for the product we use so much in our daily lives -- the personal computer. One can only speculate at what point this industry would be without Intel, it is impossible to think that it would be anything close to what it is today without them.

During the conference, Intel asked the million-dollar question, what could be done to help computer user groups

from their end. The reply from "your officers" was to offer special pricing to user group members. Our focus has always been to interact with vendors in the PC Community, to form a mutually beneficial relationship with them that benefits computer user groups and with Intel, I believe, for the most part, we have been able to accomplish this.

Four months after the initial contact Intel started the ball rolling in our relationship, they offered a deal for the 2002 Fall Conference attendees ... a Pentium 4 3.06GHZ Hyper-threading Processor and an Intel D850EMV2 Motherboard for a discounted price, along with creating a special page for user groups. I believe this is the start of more things to come. Of course I had been lagging in the "latest and greatest hardware department" as usual (my current computer was over a year old) so a new case, memory, soundcard and DVD Drive were in order. The greatest aspect of this opportunity was the visit to "Fry's Electronics! This store has to be one of the ten wonders of the world!



At this point, we are dealing with an empty case, boxed processor, bare motherboard, memory sticks, and the assorted cards to toss in the system along with a "quick install sheet" that is suited more for a drink coaster than an installation guide. However, in fairness they do say that this guide is intended for professional installers only...the full manual is available from Intel but it weighs in at 64 printed pages. The change in performance from the old machine is about double 1.4GHZ to 3.06GHZ.

The most intriguing feature of this combination is the Hyper-Threading Technology that enables multi-threaded software applications to execute threads in parallel. This level of threading technology has never been seen before in a general-purpose microprocessor. Internet, e-Business, and enterprise software applications continue to put higher demands on processors. To improve performance in the past, threading was enabled in the software by splitting instructions into multiple streams so that multiple processors could act upon them. Today with Hyper-

Threading Technology, processor-level threading can be utilized which offers more efficient use of processor resources for greater parallelism and improved performance on today's multi-threaded software. This boils down to much faster loading and execution time for applications that are multi-thread enabled. I have noticed a huge difference in Norton Antivirus and Adobe applications.

At the time of this writing Intel has started to offer another round of products, the 865-875 Motherboards, 3.0, 3.8, 2.6 GHZ 800MHZ Front FSB Processors, all of which deliver higher performance than what is listed in this article. For more information on Intel products please visit their website at <http://www.intel.com> .

There is no restriction against any non-profit group using this review as long as it is kept in context with proper credit given the author. This review is brought to you by the Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organization of which this group is a member.

What We Should Have Learned By Now

By Ira Wilsker

Hopefully by the time you read this column the attack of the SOBIG-F worm should be history, as it was scheduled to self destruct on September 10. That does not mean that all attacks will cease, as there are still many users who have incorrect dates on their computers. That means if your date is "slow" then any Sobig-F worms that may be residing on your computer will not know to self-destruct, and will continue to send infected emails to others without your knowledge.

I routinely received readers' messages which have headers placed by their email program giving the wrong year. Unless the computer is under the control of an administrator who does not allow changes, the time and date can easily be reset by simply clicking on the clock and resetting the date and time. If for some reason the clock is frequently incorrect that may be an indication of a more serious error, and possibly a pending problem. For those who would like to keep their computer clocks correct there are several programs available that will automatically reset the clock to some standard, such as the Naval Observatory, NASA, or the National Bureau of Stan-

dards. My personal favorite is “About Time” available for free download at vps.arachnoid.com/abouttime. I use About Time to reset my computer clock to U.S. Naval Observatory time on an almost daily basis.

Sobig-F, and its predecessors, flooded our inboxes with undesirable emails that eventually became easy to detect and identify. I would estimate that on all of my email accounts I received over 10,000 Sobig-F emails. Since each was about 100k in size, I received about a gigabyte of trash email due to Sobig-F alone. If I had to download those messages before deleting them, that would be an enormous amount to download. At broadband speeds, the time needed to download all of those bogus emails would be considerable; at dialup speeds the volume and frequency of Sobig-F emails may mean that downloading all of the email could be interminable. Since I still get along at home with dialup internet access, I needed a method to screen my email before downloading it to my computer. This allowed me to delete or otherwise process spam, and delete possible virus-bearing and other unwanted email. My local ISP accounts provide for some type of web based method to view email without physically downloading it to my com-



puter. By viewing suspicious emails using web mail without physically downloading them, a degree of protection from dangerous content is provided. I choose to view online email in text only, and not in HTML. Almost all web mail systems offer this option, and I strongly advise that users choose to view emails in text format only, and configure their web mail to that setting.

In local discussions, I have found that many internet users are unaware of the availability of web based email from their ISPs. I suggest that such users either check their ISP website support link, or contact their ISP to inquire about web based email. One warning;

many web mail systems place deleted messages in some form of online trash folder. Please remember to purge that folder frequently. Once unwanted email has been deleted using the web based email viewer, there is less email to download, and a decreased chance of catching an email borne virus or worm.

There is an excellent utility available that can provide assistance in identifying email that possibly contains spam or viruses, and I use it on all of my computers. It is MailWasher, published by Firetrust, of New Zealand. Available in a free version, or a more powerful “Pro” version

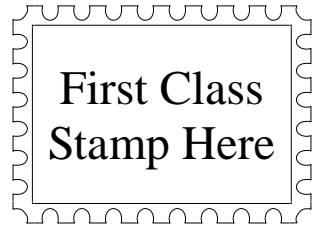
(\$29.95), MailWasher allows for the easy screening of emails. MailWasher is very fast, even on a dialup connection, because it only downloads the message headers, and a selected number of lines in the body of each email, rather than the entire email. Utilizing some of the internet “blacklists”, services that compile information on spammers, many suspicious emails are labeled by MailWasher as possible spam. Using the integral “bounce” feature, spam can be bounced back to the sender giving the appearance of a defective email address. While I can give no proof that spammers delete bad email addresses, and there is always a risk of a forged email address, it is fun to bounce those critters. Many of the Sobig-F infected emails were labeled as “possible virus” making them easy to identify and delete. Since Sobig-F infected emails were about 100k in size, I sorted the list of emails by size, and the Sobig-F emails all clustered together, enabling fast deletion of them all from the mail server. Emails can also be sorted by any column, such as date sent, size, from, subject, status, and other factors. MailWasher can be set to automatically check for new email at any desired interval. MailWasher is available for download at www.mailwasher.net.

A companion product, “Benign”, works with MailWasher, and is available from Firetrust at www.firetrust.com (\$34.95). Benign adds additional email screening

and filtering functions for viruses (in addition to your antivirus software), malicious code, and other possibly harmful content from email before reaching your computer.

Ira Wilsker is the Advisor for Region 8, APCUG Representative & Bylaws Chair for the Golden Triangle PC Club, a columnist for The Examiner in Beaumont, Texas, and has two radio shows. He also graciously shares his articles with the APCUG editors.

There is no restriction against any non-profit group using this review as long as it is kept in context with proper credit given the author. This review is brought to you by the Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organization of which this group is a member.



P.O. Box 2780
Bakersfield, CA

We are on the web at
WWW.KIPUG.ORG

Your Address Here

Sarah Perelli-Minetti Webmaster

Meetings are held on the second Thursday of the month
at the Kern Superintendent of Schools Building.
17th and L streets Downtown
Meeting Time is 7 pm