Antelope Valley Microcomputer Users Group

A V M U G N ewsletter

March, 2004

Next AVMUG Meeting:

- *Wed. March 17, 2004*
- *7:00 P.M.*
- *Lancaster Senior Center*
- *777 West Jackman*
- *Lancaster, CA*
- *Information: 661/942-1912*

February Meeting

The President welcomed all our members, tonight and announced that the V.P. would give a presentation on MS Office Suite that was provided by 'Mindshare' of Microsoft.

Frank, past president withdrew his resignation, and is now on the active role.

Ruth Moore, Treasurer, reported the bank balance of $542.97.

He also reminded each member to always update their email addresses with Marty so they will be able to receive all communications from the club.

Ray Coronado, Librarian & Webmaster, talked about all the 'Freeware' that he has added to the 'Club CD' this month. He also asked the membership to go into the website and look around and email him any comments and/or suggestions you may have. Ray will be giving a 'Work-shop' around May and is interested in all ideas our members may have concerning what they would like to hear and learn about. He plans to have the newsletter and club CD on the Website, also.

Many new ideas and plans have been suggested for the year as follows:

Bob would like to add the members of the 'Talent Pool' to the board even though they wouldn't have a board vote.

J.B. is interested in knowing any places that the members think would be good to display our new 'club brochures'. He has set a goal of 40 members for our club this year. We all need to work on this.

He would like to give credit to magazines we get for their articles.

Bob Swank took the information given to him and designed and printed the new brochures at no cost to the club. We are still working on a logo.

J.B. is door monitor and will help collect the new name tags after each meeting.

Members are asked to return tables and chairs to their original position after the meeting.

Bob would like some help to up-date our 'By-Laws'

Gerry, (VP). gave a presentation on MS Office Suite 2003. Note that Outlook 2003, is much improved, more secure and has many additional special features.

Congratulations to the following members who won our door prizes.

1. Dena Anthony
2. Don Bogart
3. J.B. Brown
4. Ed Groth
5. Curt Crawford
6. Alan Rinker
7. Don Adams

Respectfully yours,

Marty Graham, Secretary

Our Leaders:

Robert Lion	President
avmug.president@verizon.net	
Gerry Anderson	Vice Pres.
avmug.vicepresident@verizon.net	
Marty Graham	Secretary
avmug.secretary@verizon.net	
Ruth Moore	Treasurer
avmug.treasurer@verizon.net	
Ray Coronado	Librarian
avmug.librarian@verizon.net	
Dick Thompson	Editor
avmug.editor@verizon.net	

Our Internet Site:

http://www.avmug.av.org

Our Phones:

AVMUG	661/942-1912
MUG Flaps	661/946-3249

Under Attack by Cyber Worms

If you use email, as you most likely do, you may have noticed the recent increased onslaught of worms and viruses. Using a variety of techniques, the latest attacks are once again flooding our inboxes with dangerous content, as well as seeking out security holes in our systems and attacking us through our internet and network connections.

One insidious family of new pests is the group referred to as the "Bagel" or "Beagle" virus and worm family. Now spreading endemically, as I type this, are sixteen variants, referred to by the sequential letters "A" through "K". These nasties were explicitly designed to slip through most spam filters, and many antivirus scans by concealing their malicious payload in a password protected zip (compressed) file, which can only be opened by opening the email, and clicking on the attachment, and entering the password shown. The rapid appearance of the many variants also makes it easier to slip through our antivirus defenses, and more difficult to protect against. While most of us are reluctant to click on attachments from unknown senders, these creatures try to use "human engineering" to trick us into opening the email and activating the attachment. This is accomplished by spoofing the "From:" line and making it falsely appear to be from the management, tech support, email server, billing department, or other department of your ISP (Internet Service provider). They use an internal template to create a variety of subjects and messages incorporating the name of the ISP in order to appear to be authentic. Some of the common subject lines are "E-mail account security warning", "Warning about your e-mail account", "Email account utilization warning", "E-mail account disabling warning", and similar subjects.

Under Attack by Cyber Worms (Continued)

The body of the message typically starts with some variation of “Dear user of (the name of your ISP)”, followed by text indicating that your email account is about to be disabled, you have been sending out infected emails, the email server will be shut down, and similar attention getters. The punch line may be of the type "For more information see the attached file" or "Please, read the attachment for further details." To make it look even more legitimate and secure (and to bypass spam and virus filtering) it may contain a closing line to the effect of “For security reasons attached file is password protected” or “The password is (password)."

The infected email is signed with "Sincerely," or "Best wishes," or some nicety, and often has a tagline "The team, http://www.(the name of your ISP)"

Attached to the email is an innocent looking file possibly with the filename (ending in ".zip") “Information”, “Readme”, “Document”, “Message” or some other innocuous name. If this file is opened, and your antivirus software does not detect the payload, the computer will be instantly infected. Once infected, the worm will search your computer for any email addresses, and use its built-in email utility to replicate itself to the email addresses found on your computer, again spoofing the name of the recipients ISP as the sender. If you think about it, this is both a clever way to entice even a suspicious victim into opening the attachment and infecting his computer, and an insidious thing to do to countless thousands of innocent victims. One of the common payloads in the Bagel/Beagle series is a utility that deactivates many of the popular antivirus programs, and prevents them from being updated, leaving the computer open to later attacks. Some versions also open a port through a firewall (ZoneAlarm is often targeted) allowing ex-

Under Attack by Cyber Worms (Continued)

ternal “backdoor” access to the computer, and broadcasting the IP address of the vulnerable computer over the Internet. Fortunately, many of the Bagel/Beagle variants have code in them that will cease their propagation between March 14 and 25.

In another trick, some of the new virus and worm writers are trying to fool us into believing that their content is safe by including a falsehood either in its subject or as a closing tagline that the message has been scanned by a major antivirus program (most often Norton AntiVirus). Just because an email is from someone you know, and contains a line indicating that it is certified as safe, do not believe it. The creator of the worm is lying to you by concealing the real sender by spoofing the “From:” line to appear that it is from an acquaintance, and including the “certified virus free” tag.

The massive recent attacks by the authors of the Netsky, MyDoom, and Bagel/Beagle viruses and worms have created a battle among themselves, indicated by messages encoded in their respective payloads. According to several antivirus companies, the code includes attacks on each other, such as when Netsky attacks a computer already infected with MyDoom or Bagel/Beagle, Netsky tries to deactivate them, while installing its own malicious code, and stating “We kill malware writers. They have no chance”. The author of Bagel responded in a quickly released variant “Hey Netsky... Don't ruin our business. Wanna start a war?". Later variants of these three malicious products have continued the dispute.

Wouldn’t it be nice if these virus authors spent more time and effort fighting each other, and less time trying to infect our computers?

FREE online virus scans are available at the following websites:

housecall.antivirus.com

www.pandasoftware.com

www.bitdefender.com

us.mcafee.com

By *Ira Wilsker*

This article 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.

President's Corner

March has arrived and I am happy to report that your board members/talent pool have organized and are working together to take on the critical challenges we face. Extraordinary efforts is the norm to build the tools necessary and lay the groundwork for a more beneficial and interactive club. Ray Coronado has done an outstanding job getting our web site operational once again, in addition to his other duties as Librarian. His expertise, time, and improvement efforts are greatly appreciated and are crucial to our club's rejuvenation.

As everyone pitches in and does something for the club, we continue to gain strength and unity. I am especially happy to see members make donations to the club to help conserve our reserve funds-every effort helps! I also appreciate those members who come early and help set up and later, take down the room. Unity and cooperation will be further enhanced with our upcoming workshop organization. Everyone will have an opportunity to share their ideas and individual experiences in their future workshop group. I know we have a lot of latent talent and expertise in our membership, just waiting for an opportunity. Our strength lies in our combined efforts and sharing and the workshop groupings should provide the medium.

Workshop Concept: Briefly, at a meeting without a presenter, I envision the club general membership meeting, and conducting about 20 minutes of business, then breaking into groups of about 5 or more members, who all share common interest and similar expertise levels. Each group would chart its own course of activities and each member could play an active role. One person would be selected as leader/coordinator (this could be a rotating function). This would give you an opportunity to really get to know your fellow workshop members, share information, and do some real hands on interesting activities. You could visit other groups anytime. Your board is working on this concept now, and would like to hear your ideas for our May trial month-the adventure continues.

This month, we are privileged to have Mr. Dan Kozina, of Complete Computer Care, return to AVMUG to provide us with another of his informative programs. I think everyone has had the experience of losing a hard drive, and with it goes all your important email information. Dan will explain how to back up and protect your Outlook and Outlook Express entries. Dan is known for his professional presentations, practical information and functional handouts-welcome Dan.

Bob Lion