Bits and Bytes

AUGUST 2013

Arkansas' Premier Computer Club

Bella Vista Computer Club - John Ruehle Center

Highlands Crossing Center, 1801 Forest Hills Blvd, Suite 208, Bella Vista, AR 72715

Web Site: www.bvcompclub.org

E-mail: jrc@bvcc.arcoxmail.com

Richard Clark, President

Don Hood, Newsletter Editor

LEARNING OPPORTUNITIES

Microsoft Excel —Aug 13, Aug 15,
       10 am to noon
Internet (IE 9 or 10)—Aug 13, Aug 15,
       1 pm to 3 pm
PC Maintenance Part 1 "Cleaning"
       Aug 14, 9 am to noon
Genealogy Special Interest Group —
       August 17, 10 am
File Management Aug 22,
       9 am to noon
Using Windows 8 Part 1 "Programs"
       Aug 22— 1 pm to 4 pm
Digital Photography Part 2 "Camera to
       Computer"—Aug 28, 9 am to noon
Using Windows 7 Part 3 "Projects"
       Sept 3—1 pm to 4 pm
Setting Up Windows 8 Sept 5,
       1 pm to 4 pm
Pre-registration is required for all classes and are free to all Computer Club members. Call Marie Herr (273-2558) for more information and to pre-register.

WELCOME NEW MEMBERS

Jim Moore	Karen Moore
Robert N. Benson	Will Sadler
Billie Sadler	Max Waugh

GEEK VS REVO: Which is best?

While Revo Uninstaller remains a great choice, we've become fond of Geek Uninstaller lately, for one reason: Simplicity and speed. Geek is faster than Revo Uninstaller and is simpler to use. The user doesn't have to decide "Are you sure?" when removing leftover items. With Geek you don't have to select any leftover items, you just click "Finish" after it does a scan for leftover items after the software program has been remove. When it's done scanning – you're shown the leftover registry items, folders, etc. and you only have to click "Finish".

And another reason why we've been using Geek Uninstaller more and more — Revo is not fully functional on 64-bit system. Many Windows 7 computers are 64-bit and virtually all Windows 8 computers are 64-bit. While Revo will function on 64-bit machines, it doesn't show a complete listing of programs installed and there are some functions which may not work correctly.

We have seen some comparative tests done between the two, and it thoroughness, Revo wins by a narrow margin. Both are good. We still think Revo is a great program, but Geek is too. It's faster and easier to use — so we use Geek and we think it's a good choice for you too. But were not dismissing Revo. If you prefer Revo, then by all means keep using it. You should at least give Geek a try.

Geek is now offering a paid version with more features — but for our money, we'll stick with the free version.. *The above article is copyright 2008 by Cloudeight Internet, http://thundercloud.net/infoave/index.htmt*

EMSISOFT?

Editor's Note: At the July 8th Club Meeting, Jason Hummel, ArTech PC, informed the Club Members that it was his belief that the best Anti-malware program is "Emsisoft". Jason stated in a email July 24th "I have always used the emergency kit for cleanup or the free version to just scan every couple of weeks to keep the system clean. I've not actually ever used their Antivirus Product. If you installed the paid version that has Antivirus included then you are correct, it should remove your previous antivirus as two antivirus on the same machine is bad. I actually do rate it above the others as of late, but stuff always changes Malwarebytes used to be my number one but I would say they are my number two on cleaning and detection now."

On July 16, Cloudeight also reported Emsisoft is the best anti-malware program and recommended it over all other programs such as Malwarebytes, SuperAntispyware, and Spybot. This program does have a free program as well as a paid program. The paid program also serves as a anti-virus program. The following article is the news release by Cloudeight.

EMSISOFT ANTI-MALWARE IS OUR #1 CHOICE FOR MALWARE PREVENTION AND DETECTION!

After weeks of testing many free and commercial anti-malware programs, and after communicating back and forth with Emsisoft, we're very pleased to tell you that our number pick for anti-malware protection and detection is Emsisoft Anti-Malware… and we have no doubt at all about our decision. We know it's the right one for you and for us.

We've installed it on all of our machines and it's working flawlessly, protecting all of them.

(continued):
You all know that the best way to get rid of malware is to not get infected with it in the first place. Of all the programs we tested, Emsisoft Anti-Malware detected every bundled installer we threw it at. It protected our virtual machine we used for testing better than any other anti-malware by far. And it detects most installed malware quickly and easily.

You can't always be on guard, there are some very sneaky software distributors on the Web — some of them small companies, but many of them big-name companies you recognize. You can't always be on guard, but Emsisoft can. Emsisoft provides you with not only excellent detection of malware already on your computer — but helps you from ever getting any more. And this is what we've been looking for, for a long time.

We've worked on hundreds and hundreds of computers with our Cloudeight Direct Computer Care, and almost all of them have some malware, most of them have a lot of malware. Malware can literally wreck browsers, slow your Web browsing to a crawl, cost you minutes in boot-up and shut-down time, use memory unnecessarily, hurt your computer's performance, and negatively impact your privacy.

Some companies are now trying to sell you on the idea that you actually want the malware that comes with bundled freeware and trial ware. We know better — you've seen and we've seen how poorly a computer loaded with this kind of malware runs. We've discussed this with Emsisoft and they're committed to providing you with the best protection and detection you'll find anywhere — and not just for the short term, but for the long haul These folks are as committed to your privacy and your safety as we are.

We rank Emsisoft Anti-Malware #1 in protection and detection of malware. With their excellent support staff, company commitment to fight malware, and their dedication to each customer, we think we've made the right choice…and we know you will too. *The above article is copyright 2008 by Cloudeight Internet, http://thundercloud.net/infoave/index.htmt*

ADD A SHUTDOWN BUTTON TO WINDOWS 8

The default Windows 8 shutdown process forces PC users to scramble for power option menus or try to drag in charm bars. Don't do it. Instead, set up your own custom shutdown button in about a minute with this simple fix.

Log into Windows 8, right-click any empty spot on your desktop, and then select *New , then Shortcut. Type* **shutdown /s /t 0** exactly as shown here (that last character is a zero) into the location field, and press *Next.* Name the shortcut **Shutdown** (or whatever you like to name it), and click the *Finish* button. The shortcut will pop on your desktop with a default icon which you can swap out for a big red power button by right-clicking the new icon and selecting *Properties.* Open the *Shortcut*, click the *Change Icon* button. Select a new icon from the list. Be careful through: Clicking the power button will immediately shut down your PC. *"PC World, August 2013—PCWorld.com*

MALWARE & VIRUSES
WHAT'S THE DIFFERENCE?

A common question in various forums is whether anti-malware software, such as Emsisoft Anti-Malware also protects against viruses. The short answer is: yes. The term "malware" is short for "malicious software". As computer viruses are undoubtedly malicious, they fall into the category of malware, just as Trojans, rootkits or spyware do. In the end, it can be likened to dachshunds and dogs: every virus is malware just as every dachshund is also a dog. But just as every dog is not a dachshund, not every piece of malware is a virus, but rather belongs to a subcategory. In fact, there very few new viruses these days, as the majority of current malware is made up of other virtual parasites.
(Emsisoft Newsletter Security)

ANTI-VIRUS: A CONFUSING TERM IN TODAY'S WORLD

It is unfortunate that many software providers use the terms "virus" and "anti-malware" ambiguously. Some users are led to believe that anti-virus solutions are more effective than those that protect against malware, whereas the latter is actually the generic term. The matter is complicated further by the fact that today, all common anti-virus programs do also protect against other types of malware. What's more: the term "anti-malware" is sometimes used by software that doesn't offer comprehensive protection against all threats, but rather specializes only in certain categories or on particularly stubborn malware.

In order to correct the issue, these anti-virus programs would need renaming. The term dates back to the origins of computer security in the late 1980s. It was then that the first computer viruses appeared, with the first one to gain major media coverage being Michelangelo in 1992. These "early specimens of malware" were not independent programs, but rather smuggled malicious code into normal applications that then acted as a host to spread them.

Hence the term "computer virus" was born. Just as a biological virus needs a certain host cell that it can insert its DNA into in order to spread further, a computer virus also needs a certain program in order to reproduce. This explains why the first protection was named "anti-virus". Many software vendors never changed their name, as it had become so well known by their customers. They didn't want to risk losing their brand identity even though many modern anti-virus tools are, as previously mentioned, also complete anti-malware solutions. One look at the description, and you can see what type of virtual parasites a security program protects you against, regardless of whether its labeled anti-virus or anti-malware. What counts is the content, not the name or the packaging. *(Emsisoft Newsletter Security Tips)*

WHAT TYPES OF MALWARE ARE THERE?

Everyone knows about viruses, and almost everyone is familiar with Trojans, spyware or adware. But what about rootkits, ransomware and rogues? Here is a brief introduction to the different types of malware.

Virus: A computer virus spreads itself by smuggling its code into another program. The name is an analogy to its biological counterpart. Not only does a computer virus spread many times and make the host software unusable, but also exhibits malicious behavior.

Trojan horse/Trojan: A Trojan horse is a type of malware that is disguised as a useful program. The goal is for the user to execute the Trojan, allowing it to take full control of your PC and use it for its own agenda. This typically results in the installation of additional malware (such as backdoors or keyloggers) to your system.

Worms: Worms are malicious software that aim at spreading as fast as possible once your PC has been infected. Unlike viruses, they don't require a host program , but instead spread themselves via storage devices such as USB sticks, communication media such as e-mail or vulnerabilities in your OS. Their propagation causes a reduction in the performance of PCs and networks, and they may also implement direct malicious behavior.

Keyloggers: Keyloggers secretly record everything you type on your keyboard, which allows attackers to get their hands on your passwords or other important data such as online banking details. *(continue on next column)*

Open house for Computer Repair & Help

Aug. 21st (10 am—1 pm) (Wednesday)

Sept. 4th (1 pm—4 pm) (Wednesday)

Sept. 7th (10 am—1 pm) (Saturday)

Backdoor/Bot: A backdoor is a portion of code that is usually implemented into a program by the software's author, to enable access to your PC or an otherwise protected software function. Backdoors are often installed by Trojans once they have been executed, so that the attacker can gain direct access to your PC. The infected PC, also known as a "bot", becomes part of a botnet.

Exploit: Exploits are used to systematically exploit vulnerabilities in a computer program. Using them, an attacker can gain either partial or full control of your PC.

Spyware: Spyware is software that spies on you, i.e. by collecting various types of user data from your PC without your knowledge.

Adware: Adware is derived from the word "advertisement". In addition to the actual function of the program, the user will be presented with advertisements. Adware itself is not dangerous, but the display of countless adverts is generally considered undesirable and is thus detected by good anti-malware solutions.

Rootkit: A rootkit usually consists of several components that grant the author unauthorized access to the target system. In addition, these programs hide their processes and actions using other software. They can be installed, for instance, through an exploit or a Trojan.

Rogues/Scareware: Also known as "Rogue Anti-Spyware" or "Rogue Anti-Virus", rogues pretend to be security software. They frequently use fake warnings to trick users into purchasing the software, which the attackers then profit from illegally.

Ransomware: "Ransomware" is exactly what it sounds like. Ransomware encrypts the user's personal data or may even lock the entire PC. You are asked to pay a "ransom" via an anonymous service in order to unlock your computer.   (Emsisoft Newsletter Security Tips)