The Villages Computer Club will meet at 1 p.m. Friday Oct 25th at Lake Miona Recreation Center.

The program will feature a presentation on " Dealing with the Demise of Windows XP" by Peter Cronas and John Campbell.

What can you expect from Microsoft if you have an XP computer? What advice should I give to my friends that ask me about their XP computers? Just how long can I hold off upgrading? These questions and more will be addressed during this presentation.

Following the presentation will be refreshments, door prizes and a problem solving session.

If you have a computer problem you can't resolve, fill out the troubleshooting request form found at thevillagescomputerclub.com and bring it to the meeting. Forms are also available at the meeting. Ask for one when you pick up your door prize ticket.

Guests are always welcome, please bring your village ID card. For information or to sign up to be on the VCC email list, visit the website or email Paul Rabenold at TVCC.Pres@gmail.com

thevillagescomputerclub.com

****

WAKE UP GUYS THE CREEPS ARE AT IT AGAIN!!!

CryptoLocker: A particularly pernicious virus

By Susan Bradley

Online attackers are using encryption to lock up our files and demand a ransom — and AV software probably won't protect you.

Here are ways to defend yourself from CryptoLocker — pass this information along to friends, family, and business associates.

Forgive me if I sound a bit like those bogus virus warnings proclaiming, "You have the worst virus ever!!" But there's a new threat to our data that we need to take seriously. It's already hit many consumers and small businesses. Called CryptoLocker, this infection shows up in two ways.

First, you see a red banner on your computer system, warning that your files are now *encrypted* — and if you send money to a given email address, access to your files will be restored to you.

CRYPTOLOCKER IS NOT MAKING IDLE THREATS.

The other sign you've been hit: you can no longer open Office files, database files, and most other common documents on your system. When you try to do so, you get another warning, such as "Excel cannot open the file [filename] because the file format or file extension is not valid," as stated on a TechNet MS Excel Support Team blog.

As noted in a Reddit comment, CryptoLocker goes after dozens of file types such as .doc, .xls, .ppt, .pst, .dwg, .rtf, .dbf, .psd, .raw, and .pdf.

CryptoLocker attacks typically come in three ways:

1) Via an email attachment. For example, you receive an email from a shipping company you do business with. Attached to the email is a .zip file. Opening the attachment launches a virus that finds and encrypts all files you have access to — including those located on any attached drives or mapped network drives.

2) You browse a malicious website that exploits vulnerabilities in an out-of-date version of Java.

3) Most recently, you're tricked into downloading a malicious video driver or codec file.

There are no patches to undo CryptoLocker and, as yet, there's no clean-up tool — the only sure way to get your files back is to restore them from a backup.

Some users have paid the ransom and, surprisingly, were given the keys to their data. (Not completely surprising; returning encrypted files to their owners might encourage others to pay the ransom.) This is, obviously, a risky option. But if it's the only way you *might* get your data restored, use a *prepaid debit card* — not your personal credit card. You don't want to add the insult of identity theft to the injury of data loss.

In this case, your best defense is prevention

Keep in mind that antivirus software probably won't prevent a CryptoLocker infection. In every case I'm aware of, the PC owner had an up-to-date AV application installed. Moreover, running Windows without admin rights does not stop or limit this virus. It uses social engineering techniques — and a good bit of fear, uncertainty, and doubt — to trick users into clicking a malicious download or opening a bogus attachment.

Your best prevention is two-fold:

1) Basic method: Ensure you keep complete and recent backups of your system. Making an image backup once or twice a year isn't much protection. Given the size of today's hard drives on standalone PCs, an external USB hard drive is still your best backup option.(I save all my important stuff to an external drive. I've been doing this for 3 years.Jmax)

A 1TB drive is relatively cheap; you can get 3TB drives for under U.S. $200. For multiple PCs on a single local-area network, consider Michael Lasky's recommendations in the Oct. 10 Best Hardware article, "External hard drives take on cloud storage."

Small businesses with networked PCs should have automated workstation backups enabled, in addition to server backups. At my office, I use Backup Box by Gramps' Windows Storage Server 2008 R2 Essentials (site). It lets me join the backup server to my office domain and back up all workstations. I run the backups during the day, while others in the office are using their machines — and I've had no complaints of noticeable drops in workstation performance.

The upcoming release of Windows Server 2012 R2 Essentials (site) will also include easy-to-use, workstation-backup capabilities. Recently announced Western Digital drives will also act as both file-storage servers and workstation-backup devices.

2) The advanced method: If you have Windows Professional or higher, you can tweak your systems to protect them against CryptoLocker. You'll want to thoroughly test the impact of the settings changes detailed below — and be prepared to roll back to your original settings if needed. (After making some of these changes, you might not be able to install or update some applications.)

All business and Pro versions of Windows include the ability to prevent certain types of software from launching from specific locations. CryptoLocker launches from a specific location and in a specific way

(well, for now). By implementing Windows' Software Restriction Policies rules, we can block CryptoLocker from launching its payload in your computer.

Software Restriction Policies (more info) were first introduced in Windows XP and Server 2003. In a domain setting, you can use Group Policy to set up these restrictions or rules; on standalone machines, you can use Local Security Policy. (Windows Home Premium doesn't support Group or Local policies, so none of the following settings changes is supported.)

Again, be sure you test these settings changes on a single workstation first before rolling them out to other systems. Also, take the extra step of *undoing* the changes and checking whether the test system still runs as expected. Most important: Back up *all* systems before making the changes.

To make the changes, click Start/Control Panel/Administrative Tools. Click Local Security Policy and locate Software Restriction Policies under the Security Settings heading. Right-click it and select New Software Restriction Policies. Right-click Additional Rules and select New Path Rule to open the new-rule dialog box .

Creating a new path rule to block Cryptolocker

The following rules block applications such as CryptoLocker from running in the defined locations. For example, the first set of rules applies to the specific user folder %Appdata%, which equates to user\{yourusername}\appdata\roaming.

Enter the following sets of Path, Security Level, and Description information as separate rules:

For Windows XP, enter the following:

- Path: %AppData%*.exe
- Security Level: Disallowed
- Description: Don't allow executables from AppData

and

- Path: %AppData%**.exe
- Security Level: Disallowed
- Description: Don't allow executables from AppData

For Windows Vista and higher, use the above settings plus the following:

- Path: %localAppData%*.exe
- Security Level: Disallowed
- Description: Don't allow executables from AppData

and

- Path: %localAppData%**.exe
- Security Level: Disallowed
- Description: Don't allow executables from AppData

Additional paths for blocking ZIP-file locations are described in the bleepingcomputer.com CryptoLocker Ransomware Information Guide and FAQ. The following will ensure the virus can't launch from embedded or attached .zip files.

- Path: %Temp%\Rar**.exe
- Security Level: Disallowed
- Description: Block executables run from archive attachments opened with WinRAR.

From archive attachments opened with 7zip:

- Path: %Temp%\7z**.exe
- Security Level: Disallowed
- Description: Block executables run from archive attachments opened with 7-Zip.

From archive attachments opened with WinZip:

- Path: %Temp%\wz**.exe
- Security Level: Disallowed
- Description: Block executables run from archive attachments opened with WinZip.

From archive attachments opened using Windows' built-in .zip support:

- Path: %Temp%*.zip*.exe
- Security Level: Disallowed
- Description: Block executables run from archive attachments opened using Windows' built-in ZIP support.

When you're done entering new rules, reboot your system so that the changes take effect. Again, if you discover you can no longer update some applications or install software, you might need to undo some of these changes. Look in your application event log — or in the admin section — for the specific rule that's misbehaving. (To open the log, click Control Panel/Administrative Tools/Event Viewer; then, in the navigation pane, click Windows Logs/Application. For more on the Event Viewer, see the Oct. 27, 2011, Top Story, "What you should know about Windows' Event Viewer.")

As the malware authors change their tactics, you might need to revisit the rules settings; I'll try to post updates into the Windows Secrets Lounge whenever needed.

For even stronger CryptoLocker protection, those folks with solid IT savvy might want to consider application whitelisting — i.e., setting up a list of applications approved to run on their workstations. All other software installations are blocked. See the National Security Agency (yes, *that* NSA) document (downloaded PDF), "Application whitelisting using Software Restriction Policies."

Be aware that application whitelisting is a highly advanced tactic. Take some time to determine *all* allowed applications in order to properly set up application whitelisting.

Once again, keeping your AV software up to date is not the panacea for CryptoLocker. The hackers using this exploit are adapting the virus so quickly that AV vendors can't keep up with the many CryptoLocker variations in play. It's up to individual users to stay vigilant about what they click. The bad guys just keep getting worse.

****

In my last Jmax Bits Newsletter when I sent out info about the new Yellow DNR form, there was not one for the State of Florida, so I just pick one from another state. But now, I have found a copy of the DNR for the State of Florida. You may want to print it and read it carefully.
http://www.floridahealth.gov/public-health-in-your-life/patient-rights-and-safety/do-not-resuscitate/_documents/dnro-form-multi-lingual2004.pdf

****

I do not know the person personally who sent this to me, but Villagers BEWARE.

" The "No Motor Vehicle Registration" citations are the speed violations. Once over 20mph, the cart is considered a motor vehicle, not unlike a Low Speed Vehicle, and must be registered. Although,
This list does not include the auto violations due to the

number of pages, the Sheriff Office is also issuing speeding tickets, lot of them.

PERSONAL STORY: Golf Cart Citation - **The real thing**

"Recently my wife and I were going to Spanish Springs to meet another couple for dinner and a movie. Somewhere along Morse Blvd., out of the blue, I see a Deputy Sheriff on a motorcycle with his lights flashing behind me in the (Golf Cart) 'Diamond Lane'. I pulled to a stop and the Deputy informed me that I was exceeding 20mph in my "golf cart". He gave me a slip of paper which stated that the Florida Statute 320.01 defines a golf cart as a vehicle which is **NOT CAPABLE** of exceeding 20 mph. Because of this, when I exceeded 20 mph I was no longer in a golf cart but I was driving a motorized vehicle on public roads without proper registration or license. He then served me with a citation to that effect and told me it was a criminal offense. He also said that if I produced a certified letter from a golf cart shop that the golf cart was adjusted to not exceed 20 mph the judge may let me off with just court costs. The citation had a date that I was to appear in the county court in Bushnell, FL. It also stated "Criminal Violation court appearance required".

I thought to myself - here I am enjoying one of the most talked about benefits of "Florida's Most Friendly City" on my way to a movie and I end up as a **criminal**.

I was very anxious so when I got home I searched the internet trying to find out how hot the water was that I was

in. I went to TalkOfTheVillages and found some discussion related to my situation.

I went to the Sumter County Clerk website and found that a CLASS 2 Misdemeanor was a Criminal offense punishable with a fine of up to $500 and 6 months in the county jail.

I thought WHAT! - Morse Blvd. has a speed limit of 30mph - I was not going any speed close to the limit and I could end up fined and in jail because I was in a golf cart and not in a car. And in addition to that I will now have a **CRIMINAL RECORD**.

I appeared in court in Bushnell at 9:00 a.m. on the proper date. Misdemeanor offenses are prosecuted in Courtroom B of the court house. The Judge took time to explain in great detail how the pleading process worked and the procedure that followed each type of plea. He also said that he puts everyone on probation, usually for six months, to allow them time to pay the costs incurred. One important note stated by the judge is that he evaluates each case on its own merits, so a person should not expect the same sentencing as any other person who committed the same violation. His questions to each person who I witnessed appearing before him, including myself, were to clarify the violation and circumstances related to it.

When I was called to come before him, he read the charge and ask me for my plea. My plea was “No Contest” because I had no Idea I was creating a criminal offense by

driving the golf cart in excess of 20 mph. I now know I was wrong, but I didn't even think I was speeding since Morse Blvd. has a 30 mph speed limit.

The Judge was very pleasant and professional while carrying out his duties. He didn't fine me but told me I had court costs to pay and that he was withholding adjudication for which I am very grateful. Also, I was placed on probation until the costs were paid.

I then had some papers to sign in the court room. After this I went to the County Clerks office to setup payment and find out the amounts due ($253-court costs) and then to the cashiers office to pay - cash, credit card, (no personal checks). She sent me down the street to take the probation clerk my receipt. The lady at this office had me fill out more papers of personal info. for their system and pay them $50. This could only be a money order, nothing else - no cash, no check, no credit card only a money order. The lady in the office said I could get a money order at the Shell gas station on the corner. I walk to the gas station and gave the clerk $51.50 for the $50 money order. After I gave the lady in the probation office the $50 money order she said the case was closed and I should get written notification within a week.

THE GOOD

All the people at the court house were nice and pleasant to deal with. That includes the clerks, the deputies, and the Judge.

THE BAD
It cost $304.50 at the court house and approximately $125.00 for the certification of the golf cart. TOTAL $429.50

THE UGLY
At the end of the process you have a CRIMINAL RECORD.

NOTE: Before you can enter the court room you must be wearing long pants (no Shorts), a tucked in shirt that is buttoned up, no hat, no sunglasses, no chewing gum.

My advice - **Don't exceed 20mph in a golf cart** - Drive your car if you need to go faster."
****

Jmax

Jmax's Website http://www.jmaxbits.com/
Jmax Bits Newsletter is now posted each Monday & Thursday on the website. You have the option for a .pdf or a .rtf file.

1.For help with a computer problem, put HELP in the subject line and give me info about the computer you're using, if you know it.

2.To view or print Jmax Bits Good Services List in the Villages area, click link www.jmaxbits.com

3. To sign up for the non-computer newsletter, send an email to VLGSClassifieds@aol.com. Put SUBSCRIBE in the subject line. To send an Ad, place AD in the subject line.

4. The Villages Computer Club's web page: Click here: Welcome To The Villages Computer Club
To add your name to the VCC announcements list, send email to TheVCC-subscribe@yahoogroups.com

5. Fred Benson's website www.thevillagescomputerbasics.com