Midland Computer Club

Midland Michigan

BITS AND BYTES

September 2016

http://mcc.apcug.org/

President Piper's Ponderings....

The Board Members continue to have questions about Win 10, so we decided that our September topic should be a round table discussion on Windows 10 for the entire membership. There are two major versions: 1607 and 1511. Microsoft has moved settings around in Windows 10, as well as making more of your information available to them by default. There also seems to be issues with browsers, which may or may not be related to Win 10. Edge, which is the replacement for IE in Win 10, has not caught on despite Microsoft's hard sell. The Club would be interested in hearing your comments about any IE updates you may have received, particularly for older OS versions. Both Chrome and Firefox seem to be under attack by scammers and spammers.

My track record has been 5 PCs updated to Ver 1511, and 2 others said they could update, but failed when I tried. Two other Win 7 machines just didn't have the oomph to go to Win 10. One of my five Win 10 upgrades failed to go on to Ver 1607. This PC and one of the four which did make it to 1607 have had periodic problems. Club members will want to hear about any of your pitfalls with upgrading and/or running Win 10.

As for other topics for the General Meeting, Joe will be giving a talk when he returns from a security conference. The rest of our months are open, so if you have a topic in mind, let me know.

Think about volunteering for one of the Club's four help sessions in the Computer Lab. Here is a chance to help others or just show up and get your own questions answered.

As always you can bring any computer related hardware or software which you are no longer using, and the Club will use it as a raffle or donation item.

We can always use new members, so don't hesitate to bring a friend to our meetings.

See you Wednesday, September 28 at our General Meeting.

(The above comments are the opinion of the author and do not necessarily reflect the views of the Midland Computer Club.)

GENERAL CLUB MEETING

Midland Community Center, 2205 S Jefferson Ave, Midland MI
Room K111, Barstow Shipps Wing

Wednesday, September 28, 2016
7:00 P.M.
Topic: Windows 10 Anniversary Update

2016 BOARD MEMBERS

MCC OFFICERS

President	Larry Piper	larryp56@chartermi.net
Treasurer	Jan Ensing	btiger6@yahoo.com
Membership	Gary Ensing	btiger6@gmail.com
Editor & Webmaster	Carol Picard	webbyte@yahoo.com

AT-LARGE BOARD MEMBER

Joe Lykowski	joseph@lykowski.com

PROGRAM COORDINATORS

Howard Lewis	lewis3ha@chartermi.net
Bill Tower	tower.w@gmail.com

Please let Howard or Bill know of topics you would like covered at future meetings.

PUBLICITY

Al Adams	aladams12@yahoo.com

Board Meeting

First Thursday of the month
7:00 PM
Chapel Lane Presbyterian Church,
5501 Jefferson Ave., Midland MI

Educational, Fun, and Interesting Web Sites: (submitted by Howard Lewis)

http://wxch.nl/2aEBu78
We think of bridges as something we use to go over rivers, ravines, etc., but some bridge designers think that they should also be pieces of art.

http://www.sciencebuddies.org/
Here are some creative science projects for your children or grandchildren.

http://www.reviewed.com/
Find reviews on a host of tech products at this site.

https://seatgeek.com/
If you are looking for seats to an event, you might just find the best prices here.

Editor's note: when clicking on this link from the newsletter - getting indication that browser (Chrome) is not up to date. However, can copy/ paste the url into Chrome and page opens.

http://bit.ly/2arUdRU
This is one happy penguin!

http://tinyurl.com/zp92khz
Like the images that Windows 10 displays on the lock screen? Here is a way to save them to use as regular wallpapers (from howtogeek.com)

Membership Enrollment Form

NAME ________________________________ *PHONE* _______________

ADDRESS ____

CITY _______________ *ZIP* _____________

EMAIL ADDRESS ____________________________________

Membership dues FAMILY ($20) STUDENT ($15) New Member ____ *Renewal* ____

Please fill out the above form and mail it along with payment of check or money order to :

MIDLAND COMPUTER CLUB
1816 Bauss Ct
Midland, MI 48642-4023

Attn: Membership Chairman

You may also pay for membership at a regular club meeting

Tips, Tricks & Techniques (submitted by Carol Picard):

If you get these errors when trying to sign in after adding a new user account to Windows 10: "The User Profile Service service failed the sign-in." "User profile cannot be loaded", the problem may be a corrupt Default user directory in the Users directory.

To correct, need to have another Windows 10 computer with a good Default directory.

On good computer:
Log in as user with administrator privileges

Default directory in the Users folder is hidden and contains system protected files.
  To view these files - in File Explorer
    click View tab
    click to place checkmark before Hidden items
    click Options
    click Change folder and search options
    click View tab
    click to remove checkmark before: Hide protected operating system files
      will be prompted to confirm that you want to do this

Copy Default directory to flash drive

Eject flash drive

Repeat above steps in File Explorer, but add checkmark to Hide protected operating system files and remove checkmark before Hidden items.

On problem computer:
Log in as user with administrator privileges

connect flash drive

Default directory in the Users folder is hidden and contains system protected files.
  To view these files - in File Explorer
    click View tab
    click to place checkmark before Hidden items
    click Options
    click Change folder and search options
    click View tab
    click to remove checkmark before: Hide protected operating system files
      will be prompted to confirm that you want to do this

open Users folder
    rename existing Default directory in Users folder, e.g., Default.bak

copy good Default directory from flash drive to Users
    in copied Default directory, there may be multiple files beginning with ntuser.dat
      Keep the file named ntuser.dat with file type of DAT file and delete all other files beginning with ntuser.dat
      e.g., with file type of: LOG1 File; LOG2 File; BLF File; REGTRANS-MS File
        ntuser.dat.LOG1; ntuser.dat{xxxx (where xxx is series of numbers)
    Documents, Downloads, Music, Video folders should all be empty. If there are files in those directories delete them. For example, if Default directory was from an HP computer, there may be HP related files in Documents.
    Do not delete any files from the AppData directory

Repeat above steps in File Explorer, but add checkmark to Hide protected operating system files and remove checkmark before Hidden items.

Should now be able to add new user to problem computer.

ARTICLE INDEX

Articles in this Newsletter have been obtained from APCUG with the authors' permission for publication by APCUG member groups. The Midland Computer Club has not verified the information contained in the articles nor tested procedures or hardware/software. Articles do not necessarily reflect the views of the Midland Computer Club.

Back to Basics - Organizing Digital Photos

By Jim Cerny, 2nd Vice President, Sarasota TUG, FL
October 2015 issue, Sarasota Technology Monitor -- www.thestug.org -- jimcerny123 (at) gmail.com

Many people, and probably you too, have been using digital cameras and computer devices to take photos. You take your smart phone with you everywhere anyway, so you always have a camera with you. But how do you keep your photos organized? Can you actually find your old photos easily? I hope this article will help you to organize your photos so you can find the ones you want quickly and easily.

My first tip is to select a place where you want to keep your photos. In my case, I choose to keep the most recent two years of photos on my laptop computer. This amounts to hundreds of photos – maybe even a thousand. I backup all my documents and all my photos that are on the main drive of my computer (the "C" drive) every month to a small disk drive. The more recent trend for many people is to keep their photos on the "cloud". The cloud is a storage place on the internet which is really owned by a company and you probably will have to pay to use their storage space. But using "the cloud" is really a whole different topic so let me save that for another article.

In the past, I used a nice small digital camera to take photos and these are stored on the memory card in the camera. These days I have a “smart phone” (an iPhone) that takes photos so I no longer use my digital camera. Other devices such as tablets (iPads) also have cameras built into them that take great pictures too. If you have been using such a device to take photos you probably have already learned how to view the photos you have taken and which are stored in memory in that device. If you use that device to access the internet you can send any photo with your email or text message too. And, if you no longer use a Windows computer (desktop or laptop) then you are keeping all your photos on the device you are using to take the photos, and that’s great if that works well for you.

But I still choose to keep all my photos on my laptop computer so I connect my iPhone to my computer and “download” or “copy” all the photos from my iPhone to the “My pictures” folder on my computer. It turns out that when I connect my iPhone to my computer, it works just like copying photos from the memory card of my digital camera. Of course I only copy the photos I want to keep and I delete the photos I no longer want. Once they are in my computer it is then that I can organize them and play with them. Here are the steps I use to organize my photos on my Windows 7 computer:

1. Create a folder for each YEAR of photos, such as “2013 Photos” and “2014 Photos”.
2. Move all the photos taken in that year to that folder.
3. View all the photos, one at a time. Double click on any photo to open it (on my Windows 7 computer it opens the photo in the Windows Photo Viewer program). In this program I can ROTATE the photo to make it “right side up”. You can click on the right or left arrow to go to the next or previous photo in that folder.
4. DELETE the photos you do not want. This is important. In just a year or two you will ask yourself “What was I thinking keeping that picture!” Photos can take up lots of computer memory space.
5. USE THE WINDOWS EXPLORER PROGRAM to DELETE photos, RENAME photos, and MOVE or COPY photos to new or different folders. There are other programs you can use to do this as well, such as Adobe Photo Shop, Picasa, and Fast-Stone Image Viewer. These and other photo programs also allow you to play with the photo – changing contrast, brightness, and using many other image altering tools. You should always make a copy of your original photo first, before changing how it looks. You may not like the results.
6. In each YEAR folder I create new folders based upon the photo events of that year. I create new folders such as “Christmas”, “July Cruise Vacation”, or “Joe and Grace Wedding”. Then I simply move or drag the photos into the appropriate folder. It really couldn’t be much easier. I always have some photos that I have taken in that year which do not belong in one of the sub-folders, so I just leave them in the folder for that year. I find that I never have many of these photos, but if I do, then I create a new sub-folder in that year to organize them. I do not “rename” all my photos. I can do that later if I want. If you do “rename” a photo, consider the names of the people in the photo – this avoids the “who are those people” problem in the future.
7. I backup all my pictures (that is, the entire “My pictures” folder) every month to another drive.
8. Every year I copy all the old photos (two years previous) from my “C” drive and put them on a CD-ROM disk and put the disks in my photo album (which now only has CD-ROM disks in it). I clearly label each disk with a good marking pen. Sometimes I have two or three disks for one year. So at the end of 2015, I will copy all my photos in my “2013 Photos” folder to CD-ROMs and label them. When I am done, I will have in the “My pictures” folder on my computer, a “2014 Photos”, “2015 Photos”, and a new “2016 Photos” folders for the new year (2016) on my “C” drive.

With this organization method, I only need to know the year in which the photo I am looking for was taken, then I can find the folder (or CD-ROM disk) and find the photo quickly. Hey, it works for me. But you can certainly name and organize your folders any way that works for you.

Important Considerations –

I have heard that CD-ROM disks DO deteriorate over time, some estimate that if the disk was manufactured of poor quality, they may deteriorate in 20 or 30 years. Others say they should last 200 years or more if stored properly. You may want to make sure you can read your old CDs. If you cannot read a CD (it may be scratched or damaged), you may be able to take it to a computer place that can.

Storage in “the cloud” on the internet is becoming more common and cheaper. Someday I will probably put all my stuff on the “cloud” which does have many advantages. Look to see what Google is doing in this area if you are interested.

Believe me, it is worth a few minutes once a month to review and organize your recent photos, it avoids the “oh no, I don’t know where to look for it” problem later. I wonder if some day we can back-up the memory in our brains, wouldn’t that be nice?

Word Preview Pane & Cursor Size - Q&A December 2015

By Mary Phillips, Member ICON Computer Users Group, MO
December 2015 issue, The ICON Newsletter
www.iconusersgroup.org -- Mary (at) iconusersgroup.org

Preview Pane

Q1. How do I turn off/on the Preview Pane in MS Word 2013?

Word Preview Pane & Cursor Size - Phillips.doc [Compatibility Mode] - Word

Word Preview Pane & Cursor Size - Q&A December 2015
By Mary Phillips, Member ICON Computer Users Group, MO

A1. If Word opens with the reading pane view by default and you do not want to have to change it each time the following is the way to disable it.

1. In MS Word, click on File –> Options.
2. On the General tab, towards the bottom of the screen look under Start up options for the setting Open e-mail attachments and other uneditable files in reading view.

Uncheck that box.

3. Click OK.

Cursor Size

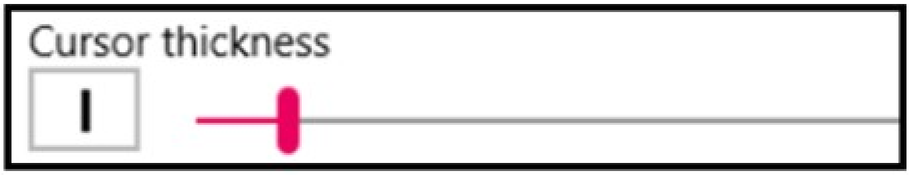
Q2. How do I increase the thickness of the blinking cursor in MS Word 2013 or Windows 10 WordPad?

A2. The blinking cursor in MS Word or WordPad may be too thin, small or slim for the eyes of many users. But you can always configure or set the thickness of the blinking cursor to a larger size so that the blinking cursor is easier to see.

To increase the size or thickness of the blinking cursor in MS Word:
1. Click on Start button, and then select Control Panel.
2. Select Ease of Access.
3. On Ease of Access window, click Optimize visual display.
Or you go into Ease of Access Center, select Make the computer easier to see.
4. Scroll to the section named Make things on the screen easier to see located at the bottom of the screen.
5. Select a number in the box next to Set the thickness of the blinking cursor option. The default value is 1. The larger the number, the thicker or fatter of the size of the cursor. There is preview available to determine what style fits you best.
6. Click OK

To increase the size or thickness of the blinking cursor in WordPad in Windows 10:
Follow steps 1 and 2 above,

3. In the Ease of Access Window, click on Other options
4. Under the Visual Options, place the mouse pointer to the right on the slider bar and click to adjust the thickness. That 's it.



Open Source Software of the Month - January

By Geof Goodrum, Potomac Area Technology and Computer Society
January 2016 Issue, PATACS Posts -- www.patacs.org -- linux (at) patacs.org

Double Commander – v0.6.6. http://doublecmd.sourceforge.net/. Free GNU General Public License source code with executables for Microsoft® Windows®, Apple® OS X® and GNU/Linux® by Alexx2000. Double Commander is a cross platform open source file manager with two panels side by side. It is inspired by Total Commander and features some new ideas:

Unicode support
All operations work in background
Multi-rename tool
Tabbed interface
Custom columns
Internal text editor (F4) with syntax highlighting
Built in file viewer (F3) to view files in hex, binary or text format
Archives are handled like subdirectories. You can easily copy files to and from archives. Supported archive types: ZIP, TAR GZ, TGZ, LZMA and also BZ2, RPM, CPIO, DEB, RAR.
Extended search function with full text search in any files
Configurable button bar to start external programs or internal menu commands
Total Commander WCX, WDX and WLX plugin support
File operations logging

[Screenshots at http://doublecmd.sourceforge.net/static_gallery_mirror/]

Kernel Source – v4.3. http://www.kernel.org/. Free GNU General Public License source code for GNU/ Linux by Linus Torvalds et al.

Origami Editor 3D – v1.2.7. http://sourceforge.net/projects/origamieditor3d/. Free GNU General Public License source code with executables for Microsoft® Windows®, Apple® OS X® and GNU/Linux® by Attila Bágyoni. Origami Editor 3D is a lightweight application for modeling the mechanism of three-dimensional paper folding. It can reproduce every operation in the Yoshizawa-Randlett system, with the exception of inflating (there still is a workaround to fold a water bomb with it).

The finished works can be exported to 3D files, animated GIF files or PDF documents containing auto-generated folding instructions for the model in a somewhat human-readable form.

Please note that this program was created mainly for fun and still is a work in progress. If you encounter a bug or have a suggestion, please post it on the Discussion forum.
Newest features:

A more intelligent PDF generation

Export as self-displaying origami: an origami file wrapped in a portable, minimalistic viewer

Difficulty level calculator

CTM export now works with textures!

[Screenshots at http://sourceforge.net/projects/origamieditor3d/]

SmallBASIC – v0.12.1. http://smallbasic.sourceforge.net/. Free GNU General Public License source code with executables for Microsoft® Windows®, Apple® OS X®, Google Android™ and GNU/Linux® by Nicholas Christopoulos and Chris Warren-Smith. SmallBASIC is a fast and easy to learn BASIC programming language interpreter ideal for everyday calculations, scripts and prototypes.
[Screenshots at http://smallbasic.sourceforge.net/?q=node/835]

winPenPack – v4.3. http://www.winpenpack.com/en/news.php. Free Open Source licensed executables for Microsoft® Windows® by various authors. winPenPack is an open source software environment comprising several portable applications grouped into suites (portable applications are applications that are modified to be executed directly from a USB flash drive, without prior installation). With winPenPack, any USB flash drive ceases to be a simple data storage device and becomes a self-contained environment, within which programs and files are homogeneously integrated.

Portable applications included in the winPenPack suites do not require any installation, do not leave their files or settings on the host computer, and can be easily transferred to another computer through any external device, such as a removable hard disk drive or a USB flash drive.

All you have to do is connect a USB flash drive to any free USB port on your host PC, and you will have your collection of pre-configured and ready-to-use programs instantly available, grouped in categories and executable through a user-friendly menu interface similar to the Start Menu, the winPenPack Menu. It will be exactly as if you are working on your own PC, with web browsers, email clients, image and drawing editors, chat clients, multimedia tools, PC maintenance and security tools, school and development tools, etc. Everything you need, completely free! All these features make winPenPack extremely useful in any situation.

Depending on your USB flash drive capacity, you can choose between winPenPack Essential and winPenPack Full, containing a collection of the best Open Source software available on the Internet, modified to achieve perfect software portability and divided into categories: Graphics, Multimedia, Internet, Office, System, Security and Utilities. You can also create your own winPenPack Personal by following our Tutorial, an option that allows you to integrate into the winPenPack package your favorite software programs, and to customize wPP to suit your needs.
[Screenshot at http://www.winpenpack.com/en/page.php?10#5]

Interesting Internet Finds - January

Steve Costello, Boca Raton Computer Society -- editor@brcs.org -- http://ctublog.sefcug.com/

In the course of going through the more than 300 RSS feeds, I often run across things that I think might be of interest to other user group members.

The following are some items I found interesting during the month of December 2015.

Credit vs. Debit: Which Card Should You Use Online?
http://www.thesimpledollar.com/credit-vs-debit-which-card-should-you-use-online/

The Simple Dollar blog gives the pros and cons of each, as well as the consequences. This is not some deep technical post, rather it is in very simple terms.

VirtualBox: Answers to frequent reader questions
http://windowssecrets.com/top-story/virtualbox-answers-to-frequent-reader-questions/

In this Windows Secrets free top story by Fred Langa, VirtualBox is demystified. I have been using VirtualBox for years to test operating systems, but there are even some things for me to learn in this post.

GT Explains: What is Li-Fi and How Can it Be 100 Times Faster Than Wi-Fi
http://www.guidingtech.com/53661/gt-explains-li-fi/

If you have been hearing about Li-Fi, but don't know what it is or how it works, check out this post

4 Chromecast Mistakes That Could Be Embarrassing or Worse
http://www.makeuseof.com/tag/4-chromecast-mistakes-embarrassing-worse/

If you have a Chromecast, this is a must read post from MakeUseOf. If you are not careful, you will be caught by one of these.

How To Format A USB Or External HDD So It Works On Both Windows & OS X
http://www.addictivetips.com/windows-tips/how-to-format-a-usb-or-external-hdd-so-it-works-on-both-windows-os-x/

Do you move between Windows and OS X? If so, this post will show you how to format a flashdrive or external hdd so it can be used by both systems.

Are Landlines Doomed to Extinction?
http://askbobrankin.com/are_landlines_doomed_to_extinction.html

Bob explains the many reasons landlines may not be around much longer. I know I use a cell phone almost all of the time, but I still have a landline for now due to hurricanes. I only pay for basic service, because I either use my cell or Skype for long distance.

****

Most Fridays, more interesting finds will be posted on the Computers, Technology, and User Groups Blog:
http://ctublog.sefcug.com/tag/interesting-internet-finds/

The posts are under Creative Commons licensing.

More security vulnerabilities disclosed for phones, carriers

October 2015. Ira Wilsker, *Assoc. Professor, Lamar Institute of Technology; technology columnist for The Examiner newspaper* www.theexaminer.com*; deputy sheriff who specializes in cybercrime, and has lectured internationally in computer crime and security.*

If you are like me, I carry my cell phone everywhere, carrying on voice conversations, sending and receiving text messages, utilizing countless apps, and surfing the Web. Until recently, I gave very little heed to the security of these external communications as our smart devices are supposed to be somewhat secure. GSM carriers like AT&T and T-Mobile utilize encryption to make communications secure; CDMA carriers like Sprint and Verizon also claim to have secure networks. Yes, I do have a major security app on my Android phone that scans new apps and text messages for malware, as well as protects from hazardous websites. Google created Android to be secure, with apps running in a somewhat closed memory space, called by some a “sandbox,” which is supposed to prevent purloined apps from talking over the phone. IPhone fanatics, along with many Apple fans in general, believe that their devices are immune to attack, as Apple would not dare to allow any threats to harm their beloved devices.

Now welcome to the world of stark reality. In a recent column, I wrote about two newly revealed vulnerabilities, known as “Stagefright” and “Certifi-gate,” that may threaten the security, safety and privacy of nearly a billion smart phones and tablets. Since then, others have come forward demonstrating previously unannounced security vulnerabilities that threaten the security of our smart phones, often including both iPhones and Android devices in their threat assessments.

One of these newly disclosed threats explicitly targets the most technology innocent and uninformed among us. Appropriately called “grandma malware,” this clever piece of malware sneaks onto Granny’s phone using a compound method of infection designed to defeat many of the simplest security precautions. While recently updated Web browsers and desktop security software, as well as updated phone operating systems, have likely patched the vulnerabilities, Granny’s often older and unpatched computer and phone may be vulnerable. The first step in the infection sequence occurs when the victim downloads an innocent looking app, often a game or simple photo utility, onto their computer using any one of the older versions of most of the common Internet browsers, which are still in wide use. This small utility, explicitly designed to appeal to a “grandma,” does not itself contain any malware, and will pass the scrutiny of many of the less sophisticated desktop security products. This utility sits quietly and apparently innocently on the victim’s computer, often performing its intended tasks. The app surreptitiously monitors Web surfing until Granny logs on to an app store, such as the Google Play Store. The malicious utility captures the logon and connection information from the app store; with this information, the malware is invisibly downloaded wirelessly to the smart device, installing itself on Granny’s phone. Once installed, this malicious app immediately gathers personal data from the phone and sends it to parties unknown. Even if this malware is detected and removed in a subsequent security scan by a third party security utility, it is too late; all of the personal information was stolen within seconds of the app being installed on granny’s phone. Granny’s private information has just been stolen, and she might very well become an identity theft victim; as is common in criminal enterprises, the most vulnerable among us are more likely to be victimized.

Despite the travesty of purposely going after Granny, it is not one of the most insidious of the newly announced threats imperiling our smart phone usage. In recent days, a pair of IBM cyber security analysts, Or Peles and Roee Hay, uncovered a flaw in the Android operating system still being used in over a half-billion Android smart phones. This vulnerability, not yet formally named but referred to as a type of “masque” attack, could allow hackers to take over and remotely control vulnerable Android phones. According to these researchers, “Masque attacks are defined as malicious apps uploaded, say, from e-mails directing victims to fake Web links.” According to Peles and Roee, Google has issued patches for devices running Android 5.1, 5.0, 4.4, and Android M, but as often the case for many Android devices (except some Nexus phones), it is up to the phone manufacturer or cell phone carrier to push these patches to their users, meaning that although the patches are available, over half of Android phones do not yet have the patches installed.

This “masque” attack vulnerability allows hackers to control the security privileges that are a part of the Android operating system, allowing compromised or counterfeit apps to access information on the phone that would otherwise be unavailable to the hacker. According to the researchers, this vulnerability allows the data thieves to steal personal information, capture banking information including logins and passwords, access the phone’s cameras, download contact lists, and pilfer stored files and e-mails, sending the stolen information to a remote server. While this particular Android vulnerability was recently discovered by IBM cyber security experts, it is very similar to one discovered several months ago by FireEye that explicitly targets Apple’s iPhones. The mechanism and modus operandi, as well as the data thefts, are almost identical between the Android and iPhone vulnerabilities.

A “masque” attack can occur when smart phone users download any of 11 authentic looking but counterfeit or contaminated apps that also appear to work properly when downloaded and installed. Among the most commonly downloaded iPhone and Android apps that enable this vulnerability are modified copies of Facebook, Twitter and WhatsApp. According to FireEye, iPhones are as vulnerable to these masque attacks as Android devices. According to Zhaofeng Chen, a senior research engineer and scientist at FireEye, the 10 tainted apps that most threaten Apple devices are “WhatsApp, Twitter, Facebook, Facebook Messenger, Google Chrome, Blackberry Messenger, Skype, WeChat, Viber, Telegram and VK." These apps are often downloaded from genuine-appearing links in e-mails or SMS text messages, and mimic the functionality of the genuine app, but allow for the remote access to this valuable personal content. FireEye was quoted as stating that this iPhone vulnerability can steal or access a variety of information from compromised phones. Among the dastardly deeds that this masque vulnerability can perform include recording and forwarding phone calls placed on Skype, Wechat and other voice apps; intercept text and SMS messages from iMessage, WhatsApp, Facebook Messenger, Skype and other SMS apps; send real-time and historical GPS locations; access website histories; steal contact information and lists; and download photos from the phone. Apple has created patches and upgrades closing this vulnerability, and pushed these patches to many of its users, but there are inevitably iOS device users who have not received or installed these patches.

In recent days, on the Australian version of the "60 Minutes" news magazine, another cell phone vulnerability was demonstrated where hackers in Germany were easily able to listen in on a cell phone chat between individuals in Australia and the UK. This ability to readily capture live calls is known as the "SS7 Vulnerability." SS7 technology is widely used, legitimate and necessary for cell phone carriers to properly direct calls and text messages to their intended recipients. ComputerWeekly.com said, "Like any protocol, SS7 is vulnerable to exploitation by sophisticated and well-funded third parties with criminal intentions." In another ComputerWeekly.com story titled "Security flaw exposes billions of mobile phone users to eavesdropping," the online magazine says, "Hackers, fraudsters, rogue governments and unscrupulous commercial operators are exploiting flaws in the architecture of the mobile phone signaling system known as SS7. ... Billions of mobile phone users around the world are at risk from covert theft of data, interception of their voice calls and tracking of their location." SS7 is not a vulnerability in the phones themselves, as the vulnerability is not brand or operating system dependent, impacting Android, iPhone, Blackberry and other systems equally, but is in reality a vulnerability in the switching system utilized by the cell carriers themselves.

For those of us who routinely use Android, iOS or Blackberry devices without much thought about the inherent security vulnerabilities of the phones and cellular carriers, keep at least a spark of consideration in mind. While I am fully cognizant of the risks, I will continue to use my smart devices pretty much as I have in the past.

What is an Exploit Kit?

By Dave Palmer, Member, Tampa PC Users Group, Florida
June 2015 issue, Bits of Blue -- www.tpcug.org -- dkp205 (at) hotmail.com

You may have heard the term 'exploit kit.' Maybe not. The term has become more prominent over the last decade as Internet crime has become more sophisticated. A few definitions will be helpful in explaining what an exploit kit is and how it's used.

A vulnerability is a weakness in a system that can be directly used by a hacker to gain access to a browser, a router, a system or a network. Vulnerabilities can result from mistakes in software, weak passwords or infected software. The vulnerabilities mentioned here are the software variety and require updates, patches, or fixes in order to prevent compromise by hackers or malware.

A zero-day vulnerability is a newly discovered vulnerability. It is completely unknown to the security community. It has not been recognized, analyzed or patched. Signature-based anti-virus software will not recognize it and cannot defend against it.

To take advantage of a specific vulnerability, hackers create software, called an exploit, specifically designed to take advantage it.

An exploit kit is a malicious software toolkit that automates the exploitation of browser and computer vulnerabilities for the purpose of spreading malware. I'm beginning to believe that 'toolkit' is too soft a term. 'Attack platform' is more accurate. The goal of an exploit kit is to automate the infection of computers or other systems.

Exploit kit basics

The earliest exploit kit was developed in Russia and was first seen in mid-2006. It was called WebAttacker, and it sold for $20 US and included tech support. Researchers and security analysts are currently tracking over 70 exploit kits around the world. Together they take advantage of more than 100 different vulnerabilities. While they can, and sometimes do take advantage of zero-day vulnerabilities, the vast majority of the time they attack vulnerabilities that have already been patched. Those computer users who are slow to patch their systems are therefore at highest risk.

Advantages of Exploit Kits

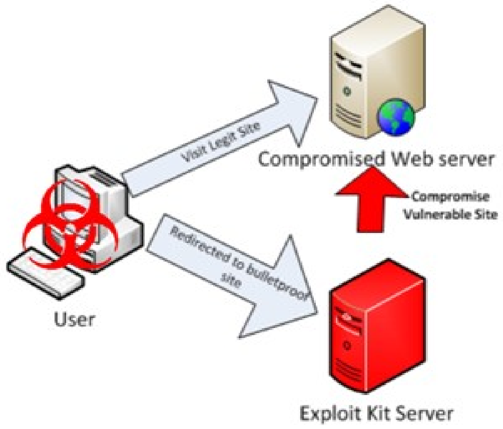
Easy to use - Exploit kits are designed from the beginning to be easy to use. Their target market includes criminals with only low-level tech skills. They also provide a console or dashboard to help attackers track the performance of the infection campaign and provide information about the victims system. Did I mention tech support is included?

Flexible – Most exploit kits probe for multiple vulnerabilities. Their initial payload can include multiple exploits, or they may download exploits to match the victim’s vulnerabilities. Customers can often customize specific features to fit their business model such as ransomware, bank heists, botnet building, etc.

Evasive – Some exploit kits can probe for anti-virus programs and virtual machines. If found, these exploit kits may stop themselves from running to avoid being found and analyzed. Some exploit kits don’t write their payload to disk but run directly in the memory instead to prevent detection by anti-virus programs. They are called ‘file less infections.’ Exploit kits also use a number of other evasive techniques.

Continuously updated – Subscribers are continuously updated with the latest exploits against such software as Java, Adobe Flash Player, Adobe Reader, Microsoft Data Access Components (MDAC), and other programs and browser plug-ins.

Good Communications – Once an exploit kit is discovered and analyzed, authorities and security firms can usually block communication URLs (web addresses) within 24-48 hours. To counter this, authors of some exploit kits provide fresh communication URLs every hour plus an automated process to update the URL to stay one step ahead.



How an exploit attack works

The hacker builds one or more websites that contain a 'landing page' and adds an exploit kit. To drive traffic to the exploit kit, the hacker has many options:

- Email spam - Spam campaigns using content such as warnings from the IRS, banks, and even police seem to work well. Fake alerts from legitimate companies that contain poisoned links are also popular. Unlike traditional phishing spam, the victim of these spam campaigns isn't taken to a look-alike site and asked for credentials. Instead they are directed towards a landing page that hosts an exploit kit.

- Purchased traffic – Underground markets have ‘traffic providers’ where traffic can be bought and sold.
- Compromised websites – When hackers compromise a website it's trivial to add a redirect. To slow down security analysts and authorities hackers typically add multiple redirects that change frequently.
- Malvertising – Malicious advertising is a relatively new and rapidly growing tool hackers have added to their arsenal. Hackers create fake companies and legitimate looking ads on existing online advertising systems to redirect victims toward exploit kits.

Just prior to connecting to the exploit kit, potential victims are screened by automated traffic direction systems (TDS). Hackers can filter out unwanted IP addresses (like security companies) or target specific countries or companies.

Once a potential victim encounters the poisoned landing page, the kit quickly (in fractions of a second) analyzes the browser and its components to see what’s out of date. If there is a usable vulnerability, the correct exploit is loaded and executed. The hacker is then notified which exploit was used as well as the victim's country, operating system, browser and which piece of software on the victim's computer was exploited.

As a result, and without your knowledge, the hacker now owns your computer. Additional malware will be added to prepare it to become a vehicle for further crime. Just as smart street criminals don't use their own vehicles for street crimes, cybercriminals don't use their own computers for Internet crime. They will either use it to commit crimes or rent it out to other criminals as part of a botnet.

Exploit kits facilitate the addition of most other types of malware such as backdoors, droppers, banking Trojans, spyware, ransomware, botnet malware, scareware, keyloggers, rootkits, viruses, worms, adware, remote access tools, and ad fraud malware.

Earlier I mentioned that exploit kits could and probably should be considered attack platforms. A comparison could be made between exploit kits and unmanned military drones. Both carry sensors. Both carry weapons. Both can be programmed to operate with little or no human oversight. Both can be assigned a variety of missions.

Exploit kits are commercial products developed by teams of specialists. A recent example is the Blackhole exploit kit developed by Dmitry Fedotov (aka Paunch) and his team. Blackhole was one of the most notorious exploit kits of the last decade. Popular and quite profitable, it was first offered in 2010 and lasted through the arrest of the Paunch and 12 others in late 2013.

The Blackhole product itself and the service and management of the business was quite sophisticated and business-savvy. The scripts that made the software work were protected by a commercial coder to prevent other criminals from lifting & reusing the code. Blackhole was reported to have had thousands of customers and making $50,000 a month. Paunch was the first to use a ‘rental’ business model for exploit kits. Other licensing agreements were also available, all of which included tech support.

How to protect yourself
The standard excellent advice you've heard dozens of times before still applies. Run in Standard User Mode, NOT Administrative Mode. Stay patched & updated. Don't click on links in e-mail. And I'll add one item not typically mentioned: Configure your browser(s) to deny redirects without permission.

More information

- http://krebsonsecurity.com/2013/12/who-is-paunch/
- https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-evolution-of-exploit-kits.pdf
- https://blog.malwarebytes.com/cybercrime/2013/02/tools-of-the-trade-exploit-kits/
- http://www.securityweek.com/black-hole-exploit-business-savvy-cyber-gang-driving-massive-wave-fraud

Working with PDF Files (Linux)

by Cal Esneault, Former President and leader of many Open Source Workshops & SIGs, Cajun Clickers Computer Club, LA -- December 2013 issue, Cajun Clickers Computer News
www.clickers.org -- ccnewsletter (at) cox.net

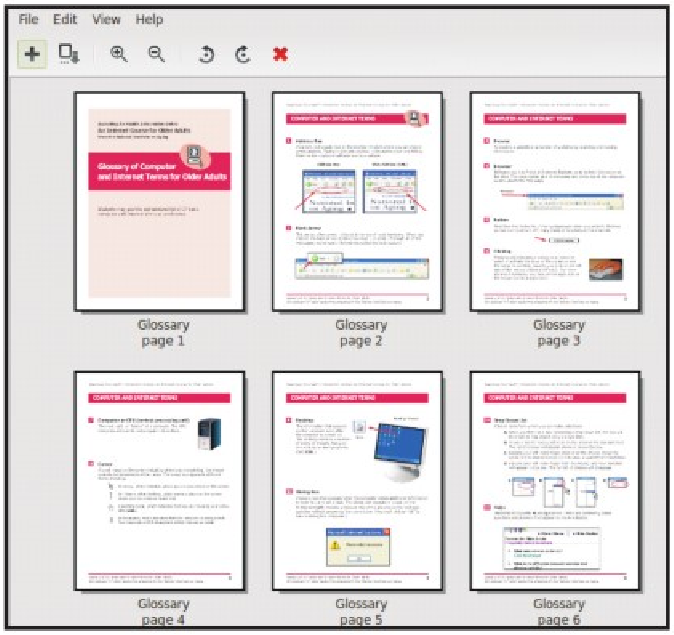
The Portable Document Format (PDF) file format is used extensively to pass documents between people and organizations that use different computer hardware and operating systems. Introduced as a proprietary format in 1993 by Adobe Systems, it was released as an open standard in 2008. With rare exception, if you have a PC you can read a PDF file (for example, Adobe Acrobat Reader for Windows OS). If you produce a document with almost any word processor, you can export a PDF version so that a recipient doesn't need to have your specific software to access it. As you browse the Internet, you will find many supporting documents are in PDF format for you to print them or for you to read them on an electronic display.

Although PDF files are easy to create and read, editing PDF files is more complex since the default is to produce a read-only file. You can usually copy text or images and paste them as components into other document software. However, many times we want to extract whole PDF pages without having to reformat the results after pasting smaller parts. PDF Shuffler, a small python-gtk open-source program for Linux, is a great method to easily rearrange, split, or merge pages from PDF files.

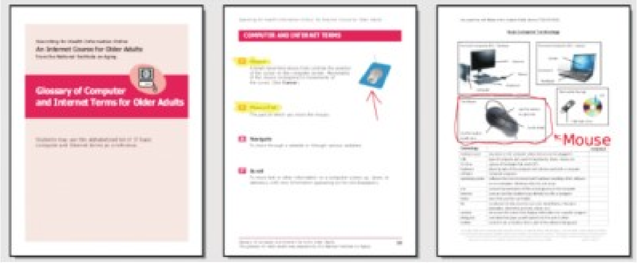
As an example, I downloaded a 14-page PDF file from federal government resources titled "Glossary of Computer and Internet Terms for Older Adults" and a 1 page PDF File titled "Basic Computer Technology" from the New York State Library. After starting PDF Shuffler, added and joined both files by hitting the "+" icon.

The following image is a screenshot of PDF Shuffler displaying the first 6 pages of the combined file. You can then select any page and delete it. Pages can be rearranged by a "drag-and-drop" mouse action.

I removed all but pages 1 and 10 from the "Glossary" file and left the single page from the "Technology" file. I next saved the 3-page result as a single PDF file with a new unique name. This shorter customized version can now be sent to a recipient with just the specific information I desired. The simplicity of PDF Shuffler is its greatest attribute.



Although you may not want to change the content on a PDF page, you may want to draw attention to specific points. Xournal is a Linux application for taking notes or sketching with a stylus. It also has an "Annotate PDF" feature. Within Xournal, select a PDF file to annotate. You are then able to add a layer of lines or text above the original page. Below is a view of the saved version of the customized PDF file described previously. Yellow highlighting, arrows, and text were added to accentuate points about a computer mouse.



An Internet Course for Older Adults

Glossary of Computer and Internet Terms for Older Adults

COMPUTER AND INTERNET TERMS

For filling out PDF forms, flpsed is an even simpler program for Linux systems which only inserts text.

The programs mentioned here are available in the repositories for many Debian-based distributions, such as Ubuntu or Linux Mint. Give them a try next time you are working with a PDF on your Linux box.

Freeware / Open Source SIG

March 26, 2015 Notes and Links

By Steve Costello, Moderator, Boca Raton Computer Society, Florida
www.brcs.org -- president (at) brcs.org

Freeware/Crapware

Old freeware download site favorites, such as download.com, CNET downloads, Tucows, etc., are now bundling crapware, including Superfish style malware. Even others like Source Forge and File Hippo are not as safe as they once were; they don’t wrap their downloads, but they do make it hard to find the right download link.

If what you want is on ninite.com, that is the safest way of getting it. If you must get it from somewhere else, make sure you don’t install using the defaults, check and only install what you need, not the crapware. Further, make sure you research it to make sure it is really what you want, and check for/ remove malware immediately after the install to make sure.

Sources

http://www.howtogeek.com/210265/download.com-and-others-bundle-superfish-style-https-breaking-adware/

https://discuss.howtogeek.com/t/download-sites-distributing-spyware-crapware/12449

http://www.ghacks.net/2015/03/13/report-all-major-download-sites-serve-potentially-unwanted-programs/

Google Search

Google Search now blocks crapware in the search results for downloads.

http://www.howtogeek.com/210568/google-is-now-blocking-crapware-in-search-results-ads-and-chrome/

f.lux

f.lux is an application to change your display to match the lighting by time of day.

https://justgetflux.com/

Web of Trust

https://www.mywot.com/en/aboutus says:

"Web of Trust (WOT) is a website reputation and review service that helps people make informed decisions about whether to trust a website or not. WOT is based on a unique crowdsourcing approach that collects ratings and reviews from a global community of millions of users who rate and comment on websites based on their personal experiences. "

Web of Trust is an add-on for Firefox, Google Chrome, Opera, Internet Explorer, and Safari browsers.

From the FAQ:

https://www.mywot.com/en/faq/add-on

"WOT shows you which websites you can trust based on millions of users' experiences around the world to help you stay safe when you search, surf, and shop online."

https://www.mywot.com/

Wi-Fi Slow Down

According to the HowToGeek blog, using slower Wi-Fi devices can slow your entire Wi-Fi network. The post explains why, and what you can do about it.

http://www.howtogeek.com/210062/how-802.11b-devices-slow-down-your-wi-fi-network-and-what-you-can-do-about-it/

Other Items Discussed

VPN - https://www.witopia.net/

Firefox Add-ons - https://www.mozilla.org/en-US/firefox/hello/ and https://addons.mozilla.org/en-Us/firefox/addon/ghostery/

On-line Spell Checker - www.afterthedeadline.com/