http://www.tpcug.org

Bits of Blue

A Monthly Publication of the Tampa PC Users Group, Inc.

Vol. 28 No. 6 June 2015

June in Tampa

Meeting

What Happens To Your Files When You Die

by Laurie O'Hall

Wednesday, June 10, 2015

6:30 PM

Pepin Distributing Co.
4121 N 50th Street
Tampa, Florida

INSIDE THIS ISSUE

Meeting Preview: Laurie O'Hall, an attorney with the O'Hall Law Firm will tell us what happens to our online files when we die. There will also be the usual Windows SIG for the first 30 minutes of the meeting.

Editor's Comments

By William LaMartin, Editor, Tampa PC Users Group
william@lamartin.com

Dave Palmer and Merle Nicholson are back joined by Roger Waters with articles for the newsletter, for which I am very appreciative. It means that I have to write less myself.

I don't usually mention such things in the newsletter, but since my wife, Karen, was my proofreader for all the years that I have edited the newsletter I feel it appropriate to mention that she died in the middle of May. Her cancer took a turn for the worse, and she was not able to do either the April or May newsletters. I think she had probably proofread every issue I have put out since I began in December of 1995, even doing that job while in the hospital at times. What that means is that now you most likely will find some missing or misplaced commas, some misspellings, occasional bad grammar and whatever else goes along

Comments.....Continued on page 7

July Meeting: To be announced

Bits of Blue is published by the Tampa PC Users Group, Inc., a State of Florida registered non-profit corporation, to provide educational information about personal computer systems to its members. Our mailing address is P. O. Box 3492, Tampa, FL 33601-3492.

However, for business concerning this newsletter, Bits of Blue, please contact the Editor, William LaMartin, at 813-251-3817, or william@lamartin.com.

Technical information found in this publication is not necessarily compatible with your hardware and software, plus other errors or misprints could occur from time to time. Therefore, the use of programs, commands, functions or anything of a technical nature appearing in this publication will be at your own risk.

RENEWING YOUR MEMBERSHIP?

WE CERTAINLY HOPE YOU WILL

MAIL YOUR CHECK AND ANY
ADDRESS OR NAME CHANGES TO:

TAMPA PC USERS GROUP
PO BOX 3492
TAMPA, FL 33601-3492

$25 Individual $35 Family
$60 Corporate = 3 employees + $20 each add'l employee

Go to our web site http://www.tpcug.org and click on the About Us | Join link to join or renew online

Check the address label for your renewal month

Friend of the User Group

We acknowledge
Pepin Distributing Co.
for their support

Affiliations

Florida Association of User Groups

Association of Personal Computer User Groups

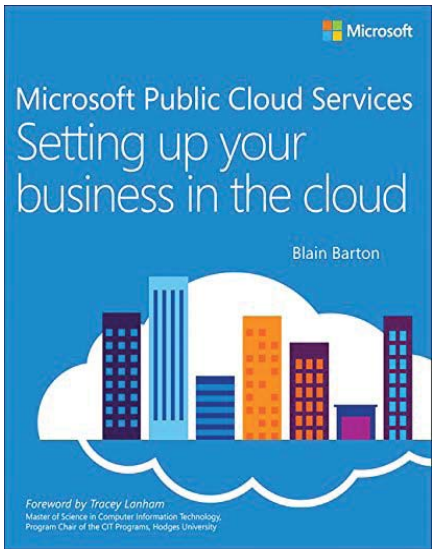
Minutes of the May Meeting

By Merle Nicholson, Secretary, Tampa PC Users Group
merle@merlenicholson.com

The Windows Special Interest Group (SIG) opens our monthly meeting. Bob LaFave, the SIG moderator introduces new or little known products and technological developments for discussion by the group. He accepts questions and requests for help in solving problems from attendees. This month in Bob's absence, Merle Nicholson was the substitute moderator. The discussion covered a demo of Portable Apps – a Windows program that packages and presents a menu of important and useful Windows application, all on a USB drive.

Our guest speaker was Blain Barton. We are very fortunate that Blain is willing to do a presentation to us yearly. Blain is a Microsoft Senior Technical Evangelist who focuses on cloud technologies. He has just completed a book entitled: *Microsoft Public Cloud Services: Setting up your business in the cloud*. A Paperback will be available June 27, 2015 at Amazon.

- Blain gave us an outline of the first chapter of his book Azure platform as a service
- SaS Software as a Service
- IAAS – Infrastructure as a service, licensing and delivering
- PAAS – Platform - web apps in a ready made cloud based environment



Finally, Blain gave us a pretty quick view of Windows 10, especially the menu system which looks to be a blend of Windows 8.1 and Windows 7. ◆

Robocall Help

By Roger Waters, Tampa PC Users Group
rvwaters@hotmail.com

During several past meetings comments were made about robocalls. This discussion will be for those that still have land lines. The frequent calls at supper and later can be disruptive. Many sign up for the Do Not Call list. I signed up for both the national (https://www.donotcall.gov/) and state (https://www.fldnc.com/) do not call list. It did not seem to help. I was still getting calls.

To understand why they keep coming is to understand the predictive dialers that are used. Some of these dialers run through area codes and office codes and then dial number 0000-9999. As an example my area code is 813 and the office code is 949. The dialer will dial 813-949-0000 through 813-949-9999. As you can tell, it will eventually hit my number. These dialers can dial every area code and office code. Most of them are set to target a specific area. The dialers can tell if they get an answer so an agent can be engaged for the sale. It can also tell if they have a dead number or intercept. Suggestions I have seen to reduce robocalls include putting a SIT tone at the beginning of your voicemail. The SIT (Special Information Tone) triggers the auto dialer to think the number is disconnected. The tone can be found on many sites. You just need to Google Special Information Tone. One example can be found here:
http://home.comcast.net/~mcbrides9/sit.html. I believe that it could also be useful for cell phone calls if placed before a voicemail message.

In April 2013, the Federal Trade Commission issued a Robocall Challenge. The FTC declared two winners. I believe one system was for a hardware device for your phone. The other solution was the one I am using. Aaron Foss was awarded $25,000 for his Nomorobo. This works with Voice Over Internet Protocol lines. This would be the phone service through the cable companies. I have Verizon FIOS. As part of the phone service you can put numbers on a list to block the call. To stop some of the calls I could set up a list of numbers to block. This helped with the fake calls from Windows about my computer having issues. As you can imagine, I would be all day blocking all numbers that call. That is why I signed up for Nomorobo. It stops most of the calls.

Nomorobo uses a service called "simultaneous ring" that is provided by most VoIP phone companies. This feature allows customers to have numerous phone lines ring at the same time. When a call comes in it also rings a number Nomorobo provides. The company uses caller ID and call frequency information to screen calls. When Nomorobo decides a call is a robocall, it hangs up after the first ring. That's how you know a call was blocked. You don't need to have caller ID on your phone for this to work and Nomorobo promises the information they collect is anonymous to protect subscribers' privacy. There are currently millions of phone numbers in the company's database of blacklisted phone numbers. These known robocallers come from complaints filed with state and federal regulators. The system isn't perfect. Robocalls do slip through. Nomorobo encourages users to report robocall numbers that are not in their database. It will not block schools, political campaigns or any emergency numbers. It works well for us. Since all calls are checked, you may not want to use the service. Their system will know all of your incoming calls. I don't worry about the privacy issues using the service. I just enjoy not having sales calls. If you are interested in using Nomorobo here is the link for them http://www.nomorobo.com The site has a video explaining the service and how to sign up. ◆

Creating a Windows Standard Account

By Merle Nicholson, Secretary, Tampa PC Users Group
merle@merlenicholson.com

Last month, Dave Palmer wrote an article "Recent Cybercrime News Highlights" in the May 2015 newsletter on page 3. One part stood out for me, and I'm reprinting it here:

> **Clear Evidence That Running in Admin Mode is a Threat** An analysis of Microsoft Patch Tuesday bulletins suggests that 97 percent of all 'critical' security vulnerabilities reported by Microsoft could have been mitigated simply by removing administrator rights. The figures are from the 2014 Microsoft Vulnerabilities
>
> Report by UK- based security firm Avecto, in which the company pulled data from every patch issued by Microsoft in 2014 - 240 in total. In 2013, the same report found that 92 percent of 147 total vulnerabilities with a critical rating could have been prevented via the same admin rights removal. The report goes on to say that user accounts with admin privileges are the primary targets for exploitation by malware, as they provide unrestricted access to a computer. http://goo.gl/vcpa8T

The solution is to create a standard user account for your normal everyday use and reserve the use of an Administrative account for the times you need to install software. The problem is that you don't want to disrupt your or your family's own use of your computer. That is solved by creating a user account with administrative rights and then change your existing account to standard. That way you won't have to rebuild the new account by copying documents and files. It's all here in a TPCUG newsletter article *Create a Standard Account*" in the October 2014 newsletter on page 3 at our website.◆

What is an Exploit Kit?

By Dave Palmer, Tampa P C Users Group
dkp205@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 'tookit' 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

Exploit Kit.....Continued on page 6

Internet Picture of the Month

Microsoft Band

The photo I used came from the German site http://www.stern.de/digital/smarthome/microsoft-band-ausverkauft-darum-wollen-alle-das-windows-wearable-2150052.html. However, you can find all about the Band in English at http://www.microsoft.com/Microsoft-Band/en-us.

June's Links

Tampa PC Users Group (that's us)	http://www.tpcug.org
Microsoft Windows 10	http://www.microsoft.com/en-us/windows/Default.aspx
Explore.org	http://explore.org/live-cams/
Dan Heller's Stock Photography	http://www.danheller.com/
David Stockman's Contra Corner	http://davidstockmanscontracorner.com/

Exploit Kit.....Continued from page 4

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 'fileless 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

Exploit Kit.....Continued on page 7

Exploit Kit.....Continued from page 6

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.org/intelligence/2013/02/tools-of-the-trade-exploit-kits/

http://www.securityweek.com/black-hole-exploit-business-savvy-cyber-gang-driving-massive-wave-fraud

https://en.wikipedia.org/wiki/Blackhole_exploit_kit

◆

Comments.....Continued from page 1

with not being an expert in such things entails.

Windows 10 will be here on July 29. And if you are running Windows 7 or Windows 8.1, you are eligible for a free upgrade. The Windows 8.0 people are eligible too, but, I believe, they have to first upgrade from 8.0 to 8.1. If you are running Win 7 or 8.1, you should now see a small new icon in your system tray that looks like a window. Clicking on that will begin the process of reserving a free copy for you when the upgrade dat arrives.

A friend asked me to work with him on apps for the Microsoft Band. But, I don't have a Band, I said. I don't need to know how many steps I have taken today. Yes but it does much more and will do more in the future. So I went to the Microsoft Store at International Mall and purchased one. And it does do a good bit more than I thought. The most interesting thing is the report on my sleep last evening: I had 2 hours 43 minutes of restful sleep and 3 hours 53 minutes of light sleep and woke up five times, etc. There is a lot more, but let's save that for the next newsletter. I have only had the item for 24 hours. ◆

Tampa PC Users Group, Inc.
P. O. Box 3492
Tampa, FL 33601-3492

First Class Mail

☐ *Member: Your membership is up for renewal*