http://www.tpcug.org

Bits of Blue

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

Vol. 28 No. 5 May 2015

May in Tampa

Meeting

Setting Up Your Business In The Cloud

by
Blain Barton from Microsoft

Wednesday, May 13, 2015

6:30 PM

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

INSIDE THIS ISSUE

Meeting Preview: Blain Barton from Microsoft will talk on the subject of his new book: *Setting Up Your Business In The Cloud*, available at Amazon.com. 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 Ron Weinberg with articles for the newsletter, for which I am very appreciative since, as you know, I do not have time to think about articles, at the present time.

Last month I mentioned a test version of our website at http://tpcugtest.azurewebsites.net. It is what is know as a responsive site that should work well on your phone. I said that I would move that content to our site at http://www.tpcug.org. I haven't done that yet, but I have made a similar responsive version of my personal site, http://www.lamartin.com which may be viewed at http://lamartincomtest.azurewebsites.net. That, being a much larger site, required more work. And there are pages there , mostly in the Large Images/Maps section, that you will not be able to view with any phone or non-windows tablet since they depend on the browser plug-in Silverlight. ◆

June 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 April 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 exporting Thunderbird mail, a demonstration of WinDirStat – a mostly file-size utility analysis of your hard drive, A discussion of SSD and (not) defragging.

This month we were very fortunate to have Andrew Sekela from the FBI White Collar Crime/Public Corruption section. Andrew is a very accomplished speaker, and he covered subjects that we're all interested in; cyber security, phone high pressure sales, phishing and "social engineering" via email and websites.

His section investigates white collar crime when the loss exceeds the threshold of $1 million. There is no minimum threshold for public official corruption. Andrew strongly advises reviewing activity reports from the three credit bureaus for unusual activity and filling a police report for any fraud loss, even small. He says that while small losses do not get investigated that your loss may fit into a larger pattern that may exceed the threshold. Also, to use the US government website http://www.ic3.gov. It's the "Internet Crime Complaint Center". "The IC3 serves as a clearinghouse and repository of cyber crime complaints from private citizens and industry. The IC3 refers complaints to law enforcement agencies for investigation and prosecution and provides analytical support for cyber crime investigations and prosecution." Looking at the site there is a lot educational materials on cyber crime and fraud to be read.

The presentation was excellent, well-prepared and fascinating. Our heartfelt thanks go to Andew Sekela for taking the time to speak to us. And to Doug for finding him! ◆

Recent Cybercrime News Highlights

By Dave Palmer, Tampa PC Users Group
dkp205@hotmail.com

A Clever Criminal
Back in 2014, Neil Moore, a 28 year old man awaiting trial in London's Wadsworth Prison, found a creative way to be set free. He used an illicit mobile phone to create a fake email account. Using that account, he then set up a fake web domain which closely resembled that of the court service's official web address. Moore registered the bogus website in the name of investigating officer Detective Inspector Chris Soole, giving the address and contact details for the Royal Courts of Justice. Posing as a senior court clerk, he then sent bail instructions to prison staff, who released him. Moore had previously used four different aliases to commit fraud worth £1,819,000 ($2,700.000). http://goo.gl/XoTfmy

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

Energy Sector Targeted
Researchers have uncovered an ongoing espionage campaign that uses custom-developed malware to siphon confidential data out of energy companies around the world. The majority of the targets were linked to the petroleum, gas and helium industries. The United Arab Emirates was the country most targeted by the attackers, followed by Saudi Arabia, Pakistan, and Kuwait.

Computers are initially infected through spam e-mails. The e-mails contain a malicious attachment that exploits a Microsoft Windows vulnerability. The vulnerability was patched in 2012. The malware, called Trojan.Laziok, acts as a reconnaissance tool that scours infected computers for data including machine name, installed software, RAM size, hard disk size, GPU details, CPU details, and installed antivirus software. The attackers use the acquired data to decide how to further infect the computer, using malware tailored for a specific compromised computer. http://goo.gl/lE0DX7

Did Elaborate Scheme Lead to Winning the Lottery?
Prosecutors say an Iowa man, Eddie Raymond Tipton 51, the information security director of the Multi-State Lottery Association, entered a locked computer room in 2010. They say he infected the computers with software to make sure the Random Number Generator picked his number in the December 2010 lottery. Although the room was monitored by a video camera, the cameras on that date recorded only one second per minute rather than running continuously like normal.

A little more than a month later Tipton was videotaped buying a Hot Lotto ticket that later won the $14.3 million payout. As an employee of the association, he was barred by law from buying lotto tickets or claiming lottery prizes. The winning ticket went unclaimed for almost a year. Hours before it was scheduled to expire, a company incorporated in Belize tried to claim the prize through a New York attorney. Weeks later Tipton was charged with two counts of fraud.

According to the prosecutor, the former security director "was 'obsessed' with root kits, a type of computer program that can be installed quickly, set to do just about anything, and then self-destruct without a trace." http://goo.gl/CaGU27

Dyre Wolf – a Sophisticated and Targeted Attack
The heist starts with highly targeted phishing email (called spear phishing) that attempt to trick people into

Recent.....Continued on page 4

Recent.....Continued from page 3

installing a strain of malware called Dyre. Researchers say this malware was undetected by the majority of antivirus products.

Once the infected victim tries to log in to one of the hundreds of bank websites for which Dyre is programmed to monitor, a new screen will appear instead of the corporate banking site. The page will explain the site is experiencing issues and that the victim should call the number provided to get help logging in.

One of the many interesting things with this campaign is that the attackers are bold enough to use the same phone number for each website and know when victims will call and which bank to answer as. This results in successfully duping their victims into providing their organizations banking credentials.

As soon as the victim hangs up the phone, the wire transfer is complete. The money starts its journey and bounces from foreign bank to foreign bank to circumvent detection by the bank and law enforcement. One organization targeted with the campaign also experienced a DDoS. IBM assumes this was to distract it from finding the wire transfer until it was too late. http://goo.gl/cxZlsb

Elusive Botnet Takedowns

Beebone – A small but highly elusive botnet called Beebone was taken down recently. It was a bit of a feat as the underlying malware, a worm, is extremely resistant to detection. Polymorphic downloader software at the heart of this malware updated itself many times a day. Beebone also relied on a pair of programs that re-download each other, acting as an insurance policy should one of them be removed.

Identifying a unique malware 'signature' is one of the oldest and most common methods of combating malware. This method is the standard among big-name anti-virus (AV) software such as Trend Micro, Norton, etc. The malware behind Beebone tries to overcome signature-based detection by changing its form every time it moves to a new system. It can also detect sandboxes and antivirus software, block connections AV websites, disable tools that try to terminate it, leverage encryption techniques, and dynamically change control server addresses and domain names. As a result, it has remained a threat since it was first discovered almost six years ago. The worm has been responsible for infecting tens of thousands of systems, and initial estimates from the sinkhole operation suggest that the botnet is considerably larger than our original estimates (more details to follow).

The takedown was carried out by "sinkholing" the Beebone command-and-control network. Sinkholing is the process of seizing all domain names and IP addresses used to communicate and update the infected machines. The whitehats performing the takedown set up their own command channel that prevented the computers from downloading malware updates or participating in any other botnet activities. http://goo.gl/tXnaOn

Simda – A week after the Beebone takedown, law enforcement groups and private security companies around the world said they have taken down a botnet that enslaved more than 770,000 computers in 190 countries. Simda, as the botnet was known, infected an additional 128,000 new computers each month over the past half year, a testament to the stealth of the underlying backdoor Trojan and the organization of its creators. The backdoor morphed into a new, undetectable form every few hours, allowing it to stay one step ahead of many antivirus programs.

Botnet operators used a variety of methods to infect targets, including exploiting known vulnerabilities in software such as Oracle Java, Adobe Flash, and Microsoft Silverlight. The takedown involved the seizing of 14 command-and-control servers that were located in the Netherlands, US, Luxembourg, Poland, and Russia

The malware modified the HOSTS file Microsoft Windows machines use to map specific domain names to specific IP addresses. As a result, infected computers that attempted to visit addresses such as connect.facebook.net or google-analytics.com were surreptitiously diverted to servers under the control of the attackers. Often the booby-trapped HOSTS file remains even after the Simda backdoor has been removed. Secu-

Recent Society.....Continued on page 6

Internet Picture of the Month

Kathmandu, April 27

"Damaged buildings lean to the side in Kathmandu" From CNN online at http://edition.cnn.com/2015/04/25/world/gallery/nepal-earthquake/ where you may view many more photos of the destruction.

May's Links

Tampa PC Users Group (that's us)	http://www.tpcug.org
New York Architecture	http://www.nyc-architecture.com
Internet Crime Complaint Center	http://www.ic3.gov
Mobile-Friendly Test	https://www.google.co.uk/webmasters/tools/mobile-friendly/
Microsoft HoloLens Official Site	http://www.microsoft.com/microsoft-hololens/en-us

Recent.....Continued from page 4

rity researchers advised anyone who may have been infected to inspect their HOSTS file, which is typically located in the directory %SYSTEM32%\drivers\etc\hosts. People who want to discover if they have been infected by Simda can check this page (https://check-ip.kaspersky.com/) provided by AV provider Kaspersky Lab. The page is effective as long as a person's IP address hasn't changed from when the infection was detected.

Taking down a botnet however, does not clean the infected machines. To be fully free infected computers still must be disinfected using AV software or, better yet, by having their hard drives wiped and operating systems reinstalled.

These takedowns are just the latest internationally coordinated botnet takedowns. They are encouraging because they demonstrate the growing ability of police and private industry to launch highly coordinated operations that can sever large, international criminal operations from the Internet in a single stroke. On the other hand, the need for a steady stream of takedowns demonstrates the persistence of the botnet problem. http://goo.gl/57zMIE ◆

Verizon FIOS Router Security

By Ron Weinberg, Member-At-Large, PC Users Group
rswjbr@verizon.net

Many of us who reside in the Tampa Bay area rely on Verizon as their ISP. We benefit from their fiber optic service FIOS. In most such cases, a router is supplied by Verizon to support home wired and wireless networks. The latter being essential for linking tablets, laptops, and smart phones.

TPCUG members well know the importance of Security in everyday electronic transactions. Your router is the door to all your connections and transactions. Is it secure?

I recently helped install a replacement Actiontec M1424 supplied by Verizon. The Wireless Password (WPA2), The router's controlling software (User Name: admin) and its password, are printed on the label permanently affixed to the Router. This is like leaving the key to your house in the lock.

The average customer, even if given instruction by Verizon on how to install this product, is unlikely to change these defaults. If you have an older Verizon Router you may wish to check it's settings. Bright House customers may wish to check their Routers also.

WPA2 is the highest level of security available on the Router. Verizon recommends using the default Pre-Shared key printed on the label rather than a Custom Pre-Shared key.

One might say that an intruder or hacker might have to come into your home to see these settings. Personally, I prefer to err on the side of more security, not less.

Changing the settings is simple, just log in to 192.168.1.1 through your browser. Sign in using the admin and provided password combination. The software is straightforward. ◆

Monthly Rambling

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

I want to mention three things this month: the availability of inexpensive printers with full features; inexpensive laptop and computers-on-a-stick; and Google Fi.

Google Fi

First, Google Fi is a new phone carrier, in competition with Sprint, Verizon, AT&T and T-Mobile. It's unique though. They don't own any infrastructure, but instead purchase coverage from Sprint and T-Mobile. In addition to cell coverage it switches to WiFi as if it were a cell whenever it can. So if you happen to be in an

Rambling.....Continued on page 7

Rambling.....Continued from page 6

area with no cell coverage, head for the nearest library, or bus. It's inexpensive as a result; unlimited phone and text coverage is just $20/mo, plus data at $10 per gigabyte per month.

There are a few catches (of course), but maybe it will suit you. Personally, I come close to liking all this but not 100%. First, the phone has to have the capability to do all this and there's but one expensive phone that works; a Phablet called Nexus 6, and, yes, it's a 6 inch phone and a superb phone/tablet at that if you have big enough hands and pockets. I'm considering one myself as a replacement for my current phone and Nexus 7 2012 tablet combined. The big downside is the $650 price. Wow. It's made by my favorite Motorola. But it's made to do all the carriers and WiFi calling too if you have the right SIM card. You can get the phone right now from carriers like Verizon and from Google, Amazon and others. Google Fi will be selling this phone for $27/mo on a two year contract.

You buy into the data plan in 1GB chunks, but unlike Verizon the cost per GB is linear and unlike everyone else they credit you for unused data! Even data overages cost the same as the plan!

This is where Verizon really stinks. You don't want to go over your data plan with Verizon, the cost is 50% more. There's no real reason to do that since you can monitor your usage and buy a higher plan at any time over your Verizon app, but still, you have to monitor it; especially if you share the plan with family members as I do.

So Google Fi isn't for everyone, for sure. Right now it's by invitation only, and I haven't been invited yet. Because of my shared plan, I'm paying $63/mo each at Vz, and if I broke away I'd be paying $75/mo each for the two, plus . . . man, my head hurts. I think this would be a no-brainer if I were on an individual Vz account and my trusty Nexus 7 tablet stopped holding battery charges.

Still, it's good for all of us to have this kind of competition. Verizon needs to dump their tiered data pricing. It makes no sense at all, and is not fair to anyone. Secondly, they need to lower the monthly charge when a phone goes off contract. In Verizon's defense, they provide the best coverage and reliable service. They have also finally gotten the billing statements so they're understandable.

Inexpensive notebook computers

ASUS notebook for $179 at Staples. It's Windows 8.1 and just 11” screen, 2GB memory and 32G SSD. Looking at the Staples and Office Depot ads, it looks like small Windows 8.1 notebooks are common at $250 and less. Maybe I don't want one, but it's intriguing. I certainly don't want a Windows 8.1 computer without a touchscreen, but I see a $250 one that is. What's happening? Well one thing is that Microsoft has essentially stopped charging manufacturers for the “Windows 8 with Bing” operating system. The other thing Intel is working hard on processors that compete with the ARM processors going into tablets and phones. They are years behind in this market. They have always made something, but the new requirements are stringent. Battery life and heat are the big problems that are solved only by smaller, more efficient cpu designs. And then Intel processors mean that Windows 8.1 is possible in small devices since the price for small memory storage modules has gotten reasonable.

So this $179 notebook has some serious limitations, but it's a good alternative to a tablet and keyboard combo, mostly cheaper, and if Windows 8 without touchscreen it doesn't suit you, installing a good Linux OS is just perfect. Using Chrome and Chrome Apps will get you pretty much everything and you can add Linux programs like LibreOffice and Netflix. I like it. If I drove away with it sitting on the roof of my car, I'd only be out the $179 bucks.

Quick review – new inkjet all-in-one – HP Deskjet 2540 - $59.

I was looking for a compact inkjet for my spouse' computer in our living room. “Compact” is a tough one. I gave up when all I can find are portables costing $300-$500. Not for me. But I did find that all the makers now have small inexpensive all-in-ones (Epson’s is “Small-In-One”). In this case All-In-One means

Rambling.....Continued on page 8

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

First Class Mail

☐ *Member: Your membership is up for renewal*

Rambling.....Continued from page 7

printer/copier/scanner, not FAX, and no scanner sheet feeder. Prints on one side, but is wireless! After checking prices thoroughly, Valerie bought this HP Deskjet 2540 wireless model in a retail store, a rarity for us. Several things are surprising. It was very easy to set up from a Windows machine since they provide software for Windows and Mac and no other; via a USB cable (supplied). Then the USB cable is no longer needed. The wireless connection needs to be set up, and from there on, printing is from anything. I can print anything directly from my Android phone or tablet. Scan, too! After setting it up, our computers and phones and tablets were easy. Two Linux computers, two phones, one tablet and one more Windows 7 computer found the printer and scanner and installed drivers. It isn't compact, but it isn't big either. After all, it has a flatbed scanner lid that determines the footprint. $59, one color, not pretty. ◆