http://www.tpcug.org

Bits of Blue

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

October in Tampa

Vol. 28 No. 10 October 2015

Meeting

The Latest Hardware

by

Steve Singer

Wednesday, October 14, 2015

6:30 PM

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

INSIDE THIS ISSUE

Meeting Preview: Steve Singer will tells us about the latest in computer hardware. There will be the usual Windows SIG preceding the presentation.

Editor's Comments

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

Last month I wrote about in the newsletter and did a presentation at our monthly meeting on Windows 10 On Many Devices. A part of the meeting focused on my running Windows 10 programs I had written on the credit card-sized computer know as the Raspberry Pi 2. Some of the programs were standard Win 10 programs that displayed photos, etc. on the attached monitor. But a couple of the programs were meant only for the Pi and not other Windows 10 devices. They were simple programs that used sensors to make LEDs connected to the Raspberry Pi blink when the sensor detected something.

But the Raspberry Pi and Windows 10 IoT (Internet of Things) can do much more than that in the hands of programmer who is also an electrical engineer. In short, in the hands of someone much more talented than I. And I have an example for you created by one of the area's Microsoft developers. If you go to the link, https://microsoft.hackster.io/en-US/cyborg-gibson-11/ultimate-kegerator, you will see how to control all the various

Comments.....Continued on page 2

November 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 September 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 subject of the presentation was Windows 10 On Many Devices, and the presenter was William LaMartin. William demonstrated Windows 10 running on his Surface Pro 2 (a laptop/tablet), a Dell Venue Pro tablet, a Windows Phone running Windows 10 and a credit card sized computer called a Raspberry Pi 2 to which he had connected a 23 inch monitor, a keyboard and a mouse. He ran a couple of the Win 10 Universal apps he had written on all of these devices.

The meeting ended with a general discussion of Windows 10. ◆

Comments.....Continued from page 1

aspects of a four-keg beer dispenser with the Raspberry Pi 2.

There is a video there where the creator, Kevin Wolfe, describes the project, and there are photos displaying various steps in the project. If you would like to view more projects of this nature, go to https://microsoft.hackster.io/en-US. There are so many talented people out there. Page 6 of the newsletter has a screen capture of the kegerator.

New Microsoft stuff

On the heels of the recently released Windows 10, Microsoft just previewed the latest versions of their hardware products that will be available later this month or in November. The video of what is termed

Comments.....Continued on page 6

ATM Cashout Fraud
Highly Coordinated, Highly Profitable

By Dave Palmer, Tampa PC Users Group
DKP205@HOTMAIL.com

ATM fraud has been growing steadily over the past decade. There are many varieties of ATM fraud, from simply stealing a PIN and withdrawing money illegally, to reprogramming an ATM machine to spit cash out on demand, to installing skimmers to steal customer data for later use. But the type of operation called 'Unlimited Operations' by both the criminal underground and the U.S. Secret Service takes ATM fraud to a new level.

The cyber crime groups attempting these crimes combine two different types of criminals. On one side are the highly skilled masterminds and technicians. They formulate the plan and break into the bank networks using combinations of social engineering, malware and technical skill. They recruit and coordinate the other team, the street criminals, and carefully monitor the withdrawals and flow of cash. The street team consists of multiple 'cashout crews,' or cashers, those who withdraw and forward the money to the money launderers. The laundering crew purchases expensive items then liquefy them to erase any connection to the cyber crime group.

Let's look at several of these crimes in some detail.

2008 attack against RBS WorldPay - $9 million
The group used sophisticated hacking techniques to compromise the data encryption that was used by RBS WorldPay to protect customer data on payroll debit cards. Payroll debit cards are used by various companies to pay their employees. By using a payroll debit card, employees are able to withdraw their regular salaries from an ATM.

Once the encryption on the card processing system was compromised, the hacking ring raised the account limits on compromised accounts, and then provided 44 counterfeit payroll debit cards to several cashout crews.

The hackers then sought to destroy data stored on the card processing network in order to conceal their hacking activity. The cashers were allowed to keep 30 to 50 percent of the stolen funds. They then transmitted the bulk of those funds back to the ringleaders.

Within a span of 12 hours the cards were used to withdraw more than $9 million from over 2,100 ATMs in at least 280 cities worldwide, including cities in the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan and Canada.

Federal prosecutors in the U.S. alleged that the 2008 RBS theft was orchestrated by at least eight men from Estonia and Russia — the alleged ringleader, Sergei Tsurikov, was extradited to face charges in the United States. In October of 2014 Sergei Tšurikov was sentenced to eleven years in prison for conspiracy to commit wire fraud and computer intrusion for his involvement in an elaborate scheme.

Another key figure in that case was Viktor Pleschuk of St. Petersburg, Russia, who monitored the fraudulent ATM withdrawals remotely and in real-time using compromised systems within the payment card network. Pleschuk and Russian accomplice Eugene Anikin were arrested and charged in Russia. Prosecutors asked the court for five- and six-year sentences, but those requests were ignored. Pleschuk and Anikin agreed to plead guilty for their roles in the RBS heist in exchange for suspended sentences (probation, but no jail time!!).

ATM Fraud.....Continued on page 4

"You know, you can do this just as easily online."

ATM Fraud.....Continued from page 3

2011 attack against Fidelity National Information Services (FIS) - $13 million

In May 2011, Fidelity National Information Services (FIS) said it had incurred a loss of approximately $13 million related to unauthorized activities involving one client and 22 prepaid cards on its Sunrise, Fla. based eFunds Prepaid Solutions, which was acquired by FIS in 2007.

Jacksonville, Fla. based FIS is one of the largest information processors for the banking industry today, handling a range of services from check and credit card processing to core banking functions for more than 14,000 financial institutions in over 100 countries. Cyber thieves broke into the FIS network and targeted the Sunrise platform's "open-loop" prepaid debit cards. The balances on these prepaid cards aren't stored on the cards themselves; rather, the card numbers correspond to records in a central database, where the balances are recorded. Some prepaid cards cannot be used once their balance has been exhausted, but the prepaid cards used in this attack can be replenished by adding funds. Prepaid cards usually limit the amounts that cardholders can withdraw from a cash machine within a 24 hour period.

The crooks were able to drastically increase or eliminate the withdrawal limits for 22 prepaid cards that they had obtained. The fraudsters then cloned the prepaid cards, and distributed them to co-conspirators.

The thieves then waited until the close of business in the U.S. on Saturday, March 5, 2011, to launch their attack. Working into Sunday evening, conspirators in Greece, Russia, Spain, Sweden, Ukraine and the United Kingdom used the cloned cards to withdraw cash from dozens of ATMs. Armed with unauthorized access to FIS's card platform, the crooks were able to reload the cards remotely when the cash withdrawals brought their balances close to zero. The heist netted around $13 million in cash.

As a result FIS came under heavy scrutiny from banking industry regulators in the first quarter of 2011. The Federal Deposit Insurance Corporation (FDIC) found the company failed to enact some very basic security mechanisms. For example, the FDIC noted that FIS routinely use blank or default passwords on numerous production systems and network devices. Analysts say FIS's problems almost certainly stem from having to cobble together various networks and systems that it inherited from a long series of corporate acquisitions over the past few years.

Feb 2013 - $45 million cashout attack across 24 countries

In two precision operations that involved criminals across two dozen countries acting in close coordination and with surgical precision, thieves stole $45 million from thousands of ATM's in a matter of hours. In the first operation, hackers infiltrated the system of an unnamed Indian credit-card processing company that handles Visa and MasterCard prepaid debit cards. Such companies are attractive to cybercriminals because they are considered less secure than financial institutions, say computer security experts.

The hackers, who are not named in the indictment, then raised the withdrawal limits on prepaid MasterCard debit accounts issued by the National Bank of Ras Al-Khaimah, also known as RakBank, which is in United Arab Emirates.

With five account numbers in hand, the hackers distributed the information to individuals in 20 countries

ATM Fraud.....Continued on page 6

Internet Picture of the Month

Microsoft Surface Book

From the site http://blogs.microsoft.com/blog/2015/10/06/microsoft-unveils-new-era-of-windows-10-devices-at-event-in-nyc/. For more information on this new, powerful and expensive laptop, go to http://www.microsoft.com/surface/en-us/devices/surface-book.

October's Links

Tampa PC Users Group (that's us)	http://www.tpcug.org
Birds of Florida #1	https://en.wikipedia.org/wiki/List_of_birds_of_Florida
Birds of Florida #2	http://www.pbase.com/r_paul/r_pauls_birds&page=all
Computer History Museum	http://www.computerhistory.org/
Inside the Creation of the Surface Book	http://mashable.com/2015/10/07/microsoft-surface-book-inside-story/?utm_cid=hp-hh-pri#uZXQOsTH9Gq0

ATM Fraud.....Continued from page 4

who then encoded the information on magnetic-stripe cards. On Dec. 21, 2012, the cashing crews made 4,500 ATM. transactions worldwide, stealing $5 million.

In the second operation, 12 account numbers were secured for cards issued by the Bank of Muscat in Oman and raising the withdrawal limits, the cashing crews were set in motion. The crews made 36,000 transactions and withdrew about $40 million from machines in the various countries in about 10 hours. In New York City alone, the thieves responsible for ATM. withdrawals struck 2,904 machines over 10 hours starting on Feb. 19, 2013, withdrawing $2.4 million. This New York street crew however, was the first to be caught, their pictures captured as they traveled the city withdrawing money and stuffing backpacks with cash.

In May 2013, eight defendants were charged with stealing $2.8 million from New York banks in the 2 separate attacks. The indictment and criminal complaints in the case offer a glimpse into what the authorities said was one of the most sophisticated and effective cybercrime attacks ever uncovered. Prosecutors said it was one of the largest heists in New York City history. Alberto Yusi Lajud-Peña, the leader of the New York cashing crew, was later found murdered in the Dominican Republic on April 27.

In June 2015, Ercan "Segate" Findikoglu, a 33-year-old Turkish man who investigators say was the mastermind behind several of these ATM cashout crimes appeared in the U.S. court system for the first time. The investigation is ongoing.

Sources

http://www.justice.gov/usao-edny/pr/eight-members-new-york-cell-cybercrime-organization-indicted-45-million-cybercrime

http://money.cnn.com/2013/05/09/technology/security/cyber-bank-heist/index.html

http://krebsonsecurity.com/2011/08/coordinated-atm-heist-nets-thieves-13m/ ◆

Comments.....Continued from page 2

the Microsoft Devices Briefing may be viewed at http://www.microsoft.com/october2015event/en-us/live-event. I found it quite interesting. Here is a list of the items discussed:

- HoloLens
- Microsoft Band
- Lumia Phones
- Surface Pro 4
- Surface Book laptop

The **HoloLens** virtual reality thing will not be available until 2016 even for developers, who have to pay $3,000 for a development kit. The other items will be available later in October or in November.

There is a new version of the **Microsoft Band** that is more aesthetically pleasing with its curved design and which also has several new health features. It is available for pre-order at $250, $50 more than the original Band, which I have and find useful for monitoring my sleep, calories burned and my walks, just some of the features it has. This should be available by the end of the month.

I am particularly interested in the new **940 and 940 XL Lumia phones** since my current Windows phone is over two years old. Unfortunately for me, at least at first, the phones will only be GMS type phones available from the Windows Store and from AT&T. I saw no mention of CDMA phones that would work on

Comments.....Continued on page 7

Comments.....Continued from page 6

the Verizon network where my account is. The same goes for Sprint customers. However, since T-Mobile is a GSM carrier, one of these phones purchased from the Microsoft Store will probably work there. At the Microsoft Store, their prices will be $549 and $649, respectively, definitely high-end phones.

The **Surface Pro 4** looks fantastic, thinner with a slightly larger screen, faster processor and up to 16 GB of RAM and one terra byte of storage. You may pre-order the Surface Pro 4 now for delivery by October 26. The base model with an Intel Cor M processor, 4 GB of RAM and 128 GB of Storage will run you $899. The top of the line Intel Cor i7 with 16 GB of RAM and 1 TB of storage will run you $2,699. Oh, and don't forget the detachable keyboard is extra at around $130. These are not cheap devices. But they are well-made and cutting-edge.

And to the big surprise, a Microsoft laptop named the **Surface Book**. It has a 13.5-inch PixelSense™ touchscreen display with (3000 x 2000) resolution. It weighs only 1.6 lbs. The base version has an Intel Core i5 processor, 8 GB of RAM and 128 GB of storage and will cost you $1,499. Not cheap because you are paying for the slim packaging and quality construction and the superb screen. The top version has an Intel i7 processor, 16 GB RAM and 512 GB of storage and will cost you $2,699. This is a very high end machine, twice as fast as the Mac Book Pro, as I recall, and intended for power users. And after seeing the screen moved to all sorts of different positions as is normal with a laptop, the surprise in the presentation came when the presenter simply detached the screen and turned the screen into a tablet, which he preferred to term clipboard mode, as you can do with the Surface Pro.

All of these devices may be viewed online at the Microsoft Store http://www.microsoftstore.com/store/msusa/en_US/home. And, I am sure they will soon have them at the Microsoft kiosk at International Plaza and then when it opens sometime in November, as I have been told, at the full Microsoft Store at International Plaza.

One of the most amazing things demonstrated was using your new Windows 10 phone as a computer via a small Display Dock pictured below connected wirelessly to a mouse and keyboard and to a monitor.

I am excited about all this new Microsoft hardware. I know it is expensive, and if you want to get a new touch enabled laptop running Windows 10 there are many options out there from other vendors that will suit almost any budget. However, I doubt any will match these new microsoft products in performance and styling. Personally I am content with my Surface Pro 2 since I do most of my work on one of my two desktop Win 10 computers. But I would really like one of those new phones. Unfortunately Microsoft and Verizon do not seem to be on the same page at the moment. ◆

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

First Class Mail

☐ *Member: Your membership is up for renewal*

ATM Fraud.....Continued from page 6