CAEUG
Computers Are Easy User Group

Abort,
Retry,
Ignore....

Founded 1984 **ARI** is the
Official Newsletter of
Computers **A**re **E**asy **U**ser **G**roup

April 2012
Volume XXIX Issue 4

Confirmed
meeting
dates for
2012
Room A

April 28
May 26
June 16 - Annual
Picnic

MEETING PLACE
will be the
Glenside Public
Library
** **
*** ***
** **
*** ***
Visitors
Welcome

HOPE TO SEE YOU
THERE!!

Our April 2012 Presenter:

Tom Soltis is demonstrate PhotoShop Elements.
If there is time, John Spizzirri will give a mini- presentation on using Make Your Own Ringtone.
Saturday April 28, 2012

Creating a Google-proof persona
by Ash Nallawalla on 14 August 2011

A persona is a fictitious person that has certain defined attributes. In product marketing, we create personas for major groups of users who will use the product. For example, a word processor's set of personas might include a high school student, a university student, a generic office worker, a specialist author, a manager, and so on.

In the world of black-hat SEO or spamming, a persona is usually a very shallow person, with no thought given to its creation. Beyond a rather implausible Western name and Gmail address, there is no sophistication, perhaps because the only purpose of that persona is to send once-off spam. Since you can create billions of fake Gmail/Yahoo/Rediffmail accounts without any worry, you can create a new one for each email if you wish.

Aaron Wall has written an interesting flight of fancy [https://plus.google.com/109555919001321700626/posts/EdHBHfQzezw}] (I mean it as a compliment) in Google+ and probably had a lot of fun speculating how Google could determine a persona to be a real

Con't pg 2

Table of Contents

person. You can almost hear the chuckles in Amit Singhal's and Matt Cutts' teams at the Googleplex.

Aaron speculates that the following behaviours help to brand a persona as a real person:

Quality of Gmail account and those of correspondents
Google Wallet and Checkout usage patterns
Google Maps use and travel patterns near credit card address
Use of YouTube
Use of +1 button

For the details you will need to see his Google+ post.
My take

Aaron has made a great start but IMHO other behaviours can be deduced. I spend most of my time with large corporate sites and reading the above with that lens made me shake my head. There is often no corporate Google account other than to create a WMT account at best. There wouldn't be a credit card tied to that account. It wouldn't use Maps to get directions. It wouldn't watch YT. etc

Such a filter is fine for removing scraper sites from further evaluation, but I have a problem with his statement: "Of course no user will score super high on everything, but they can get probabilities & toss out usage data on anything below an 80% level of confidence."

If this were so, then most corporate personas would fail, leaving their sites in peril.

I strongly believe that sites that pass a TrustRank (PDF) test with a high score are immune from checks that the rest of our sites have to endure.
Creating Google-proof personas

Let's leave spammers out of this article. At my Australia/New Zealand Directory I see many SEO companies submitting links on behalf of clients with a fresh Gmail address that is probably not used after an initial round of link submissions. They might use that address to submit some articles to directories and the really inept agencies might use it for comment and forum signature spam. That's it.

What's wrong with this picture? Anyone in our industry can spot one of these Gmail addresses as a fake often by looking at them. I delete whole chunks of waiting submissions merely by looking at the address and not the actual submission. They are always a text string that ends with some digits.

I am not a retail SEO, so I don't need to do this, but in the interests of improving the industry, here is how I would go about setting up a persona (leaving out details that might help the wrong people):

Create a spreadsheet with multiple columns and refer to it when using a persona. Place each persona on a new line.
Choose a realistic name that doesn't draw attention. A "Mark Smith" will pass visual scrutiny, but a Barr. Wardt Wodelt (a real example in my junk folder today) looks suspicious.
Find a realistic photo of someone who isn't a model. The plainer the better.

Fill the spreadsheet with the persona's CV and various details. If they were born in New York and live in Los Angeles, then they need to be seen to write various things as if they currently live in LA. Their high school and university could be in one of those two places.

Open accounts at various online places with the same nick and same personal details, so that a web search for the nick will produce a lot of results pointing to the same full name and location. A real person would usually have a Facebook account, so ensure that it has some activity at regular intervals and performs things that real people do, e.g. add apps, Like articles, leave comments etc. Their LinkedIn account would need to show the same educational institutions and locations.

Create many more personas as needed, not all at once.

I won't elaborate on how to make these personas more convincing, other than to say that they should have been created a long time ago, gradually, perhaps from different cities when you were visiting them. Creating 20 Gmail accounts from the same IP address in one session is a bad idea.

I don't use many Google services, such as Checkout, Picasa, Gmail.com address, etc, so I might score low in Aaron's list of checkpoints. However, I use addresses that were created in 1994 and 2002 and have left a vast trail all over the web since then. Spoofed spam has been sent from one of those, but I have not noticed any lasting damage to rankings, if any. I do participate in Google+, Groups, Orkut, WMT, Maps, and some other Google services, so my various accounts should look very human.

Ash Nallawalla is a member of the Melbourne (Australia) PC Users Group and is a Digital Strategy Consultant. This article can be viewed at http://bit.ly/tWJnLE

Lamp Post 136

April 22,2012

by John Spizzirri

Major Geeks (**1**) reports a new type of extortionware **(2**). I reported on this type of trojan in Lamp Post 113 (**3a**), February and March 2010 ARI... (**3**b). This is a new variant of it. Instead of telling you that your machine is infected with thousands of viruses, it encrpyts your data files and demands payment for the key to unencrpyt the files. Major Geeks suggests using Dr. Web Trojan.Encoder.94 Decryptor 1.4.27 (**4**) to attempt to unencrypt your files should you succomb to this variant of the trojan. That program is on the CD of the Month. The message sent with this trojan is in a file called "HOW TO DECRYPT FILES.TXT" and looks like this;

"Attention! All your files are encrypted!
You are using unlicensed programms!
To restore your files and access them,
send code Ukash or Paysafecard nominal value of EUR 50 to the e-mail Koeserg [at] gmail.com.
During the day you receive the answer with the code.

You have 5 attempts to enter the code. If you exceed this
of all data irretrievably spoiled. Be

Con't pg 4

careful when you enter the code!"

McAfee has a two and a half year old description of a trojan that does the same thing **(5)**. If this doesn't convince you to spend the time and money to back up you data, I don't know what will.

1) http://majorgeeks.com/
2) http://majorgeeks.com/story.php?id=34161
3a) http://www.caeug.net/newsletters/2010/Feb2010.pdf and
3b) http://www.caeug.net/newsletters/2010/Mar2010.pdf
4) http://majorgeeks.com/Dr._Web_Trojan.Encoder.94_Decryptor_d7716.html
5) https://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=239862

Consumer Reports (**1**) has an article that might be of interest to home owners. The first sentence in the article contains misinformation. It starts, "A home is robbed every 14.6 seconds...". The problem with that sentence is that robbery is a face to face crime. Gas stations, convenience stores, and banks are robbed. Robbery is done by a person doing or threatening violence on another person in order get control or ownership of property that does not belong to him / her (**2**). A house or home is broken into when no one is there and property is removed. That crime is known as burglary (**3**). The article correctly states that burglaries as reported to the police are down in the most recent reported year (2010). The newspapers and other media would have you believe otherwise but crime (in general) is down across the board. Cops like to take credit for that, but I suspect that there are numerous reasons that contribute to the statistic. As the economy spirals toward the drain, crime takes a slight upturn. Getting back to the article, Consumer Reports lists the things that you can do to lower your chances of being victimized by burglars (**4**). I would suggest one other item, if you have a burglar alarm. Have a flashing light mounted on the roof or other high point on the house. The alarm sound plus the light will send criminal scurrying away. You should remenber the old saying, 'When seconds count, the police are (only) minutes away. (**5**)"

1) http://www.consumerreports.org/
2) https://en.wikipedia.org/wiki/Robbery
3) https://en.wikipedia.org/wiki/Burglary
4) http://news.consumerreports.org/home/2011/09/burglaries-are-down-but-your-house-may-be-screaming-rob-me.html
5) http://www.democraticunderground.com/?com=view_post&forum=1172&pid=19589

I recently attended a lecture by Lori Andrews (**1**), author and law professor at Illinois Institute of Technology (**2**). She spoke about her book, "I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy" (**3**). The New York Times reviewed the book in January (**4**). In the book Andrews talks about how David Cameron (**5**), Prime Minister of England, met with another world leader, Mark Zuckerberg. Mark is the CEO of Facebook. Facebook (**7**) has about 845 million members. If the members were considered citizens, Facebook would be the third largest country in the world after India and China. Facebook has two and a half times more members than the United States has citizens (**8**). Andrews proposal for privacy is a Social Network Constitution (**9**). I like the idea but I think it is unenforceable and thus a waste of time. Meanwhile in Congress, a new bill is going through the process of becoming law. It is called The Cyber Intelligence Sharing and Protection Act (CISPA (**10**)). It will allow (or maybe compel) e-mail companies to read your e-mail for content

Con't pg 5

and allows the government full access to that data without court order. Incidentally, Lamar Smith will be reintroducing PIPA if he survives this election cycle.

1) **http://www.loriandrews.com/**
2) **http://www.iit.edu/**
3) **http://www.amazon.com/Know-Who-You-Are-What/dp/1451650515**
4) **https://www.nytimes.com/2012/01/29/books/review/i-know-who-you-are-and-i-saw-what-you-did-social-networks-and-the-death-of-privacy-by-lori-andrews-book-review.html?_r=1&pagewanted=all**
5) **https://en.wikipedia.org/wiki/David_Cameron**
6) **https://en.wikipedia.org/wiki/Mark_Zuckerberg**
7) **https://en.wikipedia.org/wiki/Facebook**
8) **https://en.wikipedia.org/wiki/List_of_countries_by_population**
9) **http://www.socialnetworkconstitution.com/**
10) **https://www.eff.org/deeplinks/2012/04/cybersecurity-bill-faq-disturbing-privacy-dangers-cispa-and-how-you-stop-it**

If you read any of the substantive material above, you may now have a different view of privacy and the Internet. There have been a number of articles written about how to lower or eliminate your presence on the Internet (**1**,**2**,**3**). There is the 6, 12, and 5 step methods. The 12 step method seemed to be the most thorough. Another site that suggests ways to purge 'public' databases (**4**). It looks like some of the suggestions may work. The only thing that was not suggested is to stop using the Internet. I know that is extreme but would work in the long run. As data ages it becomes less and less valuable until it is useless. Storing useless data costs money. No company can afford to store useless data in perpetuity. Private companies purge data periodically. Only the government can store information forever. The government sometimes recognizes that newer data is better than older data and puts the older data into long term, hard to access stroage. A site that Gerry Fish showed me gathers data from the government and telephone companies (**5**). That site is scary. Put the address of some random house into the site. Names, addresses, and phone numbers of the surrounding properties are returned. There is an amazing amount of data that is publicaly available.

1) **http://howto.cnet.com/8301-11310_39-57417419-285/how-to-delete-yourself-from-the-internet/?tag=postrtcol;posts**
2) **http://www.wikihow.com/Delete-Yourself-from-the-Internet**
3) **https://www.pcworld.com/article/223682/erase_yourself_from_the_web.html**
4) **http://www.ehow.com/how_4947199_remove-public-records-internet.html**
5) **http://neighbors.whitepages.com/**

I was able to tour Argonne National Laboratory (**1**) Advanced Photon Source experiment (**2**) and the Argonne Leadership Computing Facility (**3**) supercomputer. The tour guide told us that when the machine, and IBM Blue Gene/P, was installed 5 years ago, it was the fastest computer on Earth. Now it is 28th fastest. It cost $77 million and will be retired in 2 years. It will be given away in pieces (probably to universities). It is being replaced with an IBM Blue Gene/Q (**4**), at a cost of $137 million. It will be the fastest supercomputer on Earth. The current computer is utilized 97% of the time. The operating system is SUSE Linux Enterprise Server (SLES (**5**)). The new machine will run Red Hat Linux (**6**). The current computer is capable of running 517 terraflops or 517 trillion operations per

Con't pg 6

second. We were told that the results of all the processing that was done over the years more than paid for the costs in increased industrial efficiency. They did not tell us about the military uses of the computer. I am sure that there must be military spending involved on the site because they told us that they were not getting many cutbacks on spending. Interestingly, Fermi National Accelerator Laboratory (**7**) spending is being cut way back. I attended 'The Intensity Frontier: A New challenge for Fermilab' lecture (**8**). Funding cuts were explained. All in all the Argonne tour was fascinating. We were allowed to take pictures of anything we wanted except the security check points or the guards. Paranoia is pervasive.

1) http://www.anl.gov/
2) http://aps.anl.gov/
3) http://alcf.anl.gov/
4) http://www-03.ibm.com/systems/deepcomputing/solutions/bluegene/& 5) http://www.suse.com/products/server/
6) https://www.redhat.com/products/enterprise-linux/scientific-computing/
7) http://www.fnal.gov/
8) http://www.fnal.gov/culture/NewArts/Lectures/11-12/wojciki.shtml

Kathy Groce and I attended the WGN Tornado and Severe Storm seminar featuring Tom Skilling (**1**). Dr. Louis W. Uccellini, Director of NOAA's National Centers for Environmental Prediction (**2**), was excited about the new supercomputer The National Oceanic and Atmospheric Administration (NOAA (**3**)). The current computer operates at 77 terraflops. The new computer will operate at about 140 terraflops. When I heard that, I wondered if NOAA could use a machine that was 5 times faster that was available at no cost? I wrote Dr. Uccellini about the Argonne supercomputer that was free in two years. This is his response to my e-mail;

"John: Thanks for your note. Our operational computers are leased, and not owned, which means that the winning company to the open bidding/procurement process has to provide the computing capacity with a guarantee they can meet the 99.9% on time delivery of the entire improved model production suite with the highest level of IT security available. IBM won this bid and rightfully decided to meet these requirements with the next generation computer system which uses much less power and has lower cooling needs than any previous system. This means that more resources are used for the leased computer and less for the leased space and electrical support requirements. Thus the cost effective, leasing approach becomes even more cost effective while also providing a new computer capability that scales to our model systems (making for an easier code transition process which also saves money). My review of those OPERATIONAL units that have tried using older "used" computer systems wind up regretting those decisions from a cost, code transition and sustainability perspectives, as the computer industry itself literally walks away from maintenance and IT security aspects of older systems as they focus on the new systems. Hope this helps. Louis Uccellini

On 4/17/2012 8:55 AM, John Spizzirri wrote:
> Hello Doctor Uccellini,
>
> Your presentation at the Tornado and Severe Storm Seminar held at the Fermi National Accelerator Laboratory was very informative. You mentioned that NOAA was getting a new IBM iDataPlex

Con't pg 7

computer that would double the computing power of the current IBM Power6 system. In early April I toured Argonne National Laboratory computer center. They have a five year old IBM Blue Gene/P capable of 515 teraflops (trillion calculations per second). It is being decommissioned in 2014 and will be given away. Perhaps NOAA could use a machine like that at little cost to taxpayers.
>
> Regards,
> John Spizzirri
> spizmann@yahoo.com

-- Louis W. Uccellini
Director
National Centers for Environmental Prediction
DOC/NOAA/NWS/NCEP
Phone: 301.763.8016
Fax: 301.763.8434"

Now you know why your federal taxes are so high.

1) http://blog.chicagoweathercenter.com/2012/04/announcing-tornado-severe-weather-seminar.html
2) http://www.ncep.noaa.gov/director/profile/
3) http://www.noaa.gov/

Between you, me and the LampPost, that's all for now.

Crime and Conflict Over the Internet

By Greg Skalka, President,
Under the Computer Hood User Group, CA
October 2011 issue, Drive Light
http://www.uchug.org president (at) uchug.org

Recently my family and I were in Las Vegas and while we were there, another hacking incident hit the news. Zappos.com, an online shoe and clothing retailer, announced that they had been the victim of a cyber-attack. Being based in nearby Henderson, the reports on this company that I was previously unaware of (you can imagine how much online shoe buying I do) dominated the Las Vegas local news. Customer address, phone and email information had been stolen, but fortunately credit card info and account passwords remained secure.

This was just one more incident in an increasing trend of crime and conflict conducted over the Internet.

Reports of hacked computers and stolen commercial data have become commonplace. The Internet appears to be a prime medium for crime, with organized crime elements taking advantage of the easy access and anonymity. I've so far avoided being part of one of these data thefts from a major company that I've entrusted with some of my personal information, but it is probably just a matter of time until I'm a victim too. I'm also under siege on a smaller scale, receiving several scam emails every day. Most are such obvious scams that I almost have to laugh. Is the head of the FBI or Secretary of State Hillary Clinton really going to email me about claiming foreign funds I

Con't pg 8

previously knew nothing about? I have seen some pretty realistic emails from banks (mostly ones I don't do business with, but a few that I do), advising me to click on a link to avoid a loss of account access. A little restraint and outside research show even the most polished of these to be fakes intended to trick you out of personal information or plant malware on your computer.

The worst of these online scams try to use your own friends and family to trick you into lowering your guard. I recently received an unsolicited email from my sister, which was also addressed to a number of other family members. It contained only a vague greeting and a link. I recognized it as a scam, but my wife did not.

Fortunately, it appears the link only led to a Viagra-peddling website, as repeated cleanings of her computer turned up no malware. It appears that someone gained access to my sister's email account and used it to send this message to everyone in her email address book. After receiving this sham email herself at work, she changed her email account password and sent a warning out to all her contacts. That showed good web etiquette. I receive similar emails periodically from a friend's account, but he never responds to my warnings about his email account being hijacked. If you lose control of an email account in this way, at least let the provider know so the account can be closed. If you simply abandon the compromised account, you'll likely leave a zombie account out there to continue pestering your friends.

In addition to the criminal element, the political conflicts of our world are starting to creep into the Internet.

While electronic personal communications can play a positive role in exposing repression around the world, and can be a tool for change towards more open and free political systems, the access to information can also be a weapon. Enemies of our country and way of life hack our government and commercial web sites to steal information and deny legitimate access. Our businesses and institutions may be under attack through the Internet by factions related to or agents of China, Russia or our middle-eastern adversaries. Our own government has formed cyber warfare elements and acknowledges that future battles may include skirmishes in cyberspace. It is speculated that the Stuxnet worm, which appears to have targeted uranium processing facilities in Iran, may have been the product of U.S. or Israeli intelligence agencies. Palestinian hackers steal and release account information from banks and institutions in Israel, leading some in Israel to do the same with information on Palestinians.

Where will all this lead? I'd hate to see the "Information Superhighway" that was supposed to be our free and open Internet turned into the electronic equivalent of the highways in "Mad Max", where danger lurks everywhere and lawlessness abounds. And speaking of laws on the Internet, we have recently witnessed online protests over U.S. Internet piracy legislation. A number of prominent web sites, including Google and Wikipedia, conducted partial shutdowns or redirections to protest pending legislation and solicit support from their users. The Stop Online Piracy Act (SOPA) and Protect IP Act (PIPA) are bills under consideration by the U.S. Congress to protect intellectual property. Opponents claim the proposed legislation would harm free speech and reduce technical innovation on the web. I acknowledge online piracy is a problem, but also don't want a solution at the expense of an open Internet. Hopefully our own government won't soon be in the censoring business. We all have an interest in how this issue is resolved.

With all this conflict on and over the web, it makes me wonder if I'm taking all the reasonable measures I can to protect myself and my assets as I use the Internet. It is sometimes difficult to determine where "reasonable" fits in between "it won't happen to me" and a bunker mentality. As I've moved my finances and shopping online, I've realized I've become more dependent on the Internet. By conducting all my banking activities, including bill payment and monitoring of

Con't pg 9

accounts, on the web, I hope I've not made myself more vulnerable in the process. Am I safer not having bank statements mailed to me, or am I now more open to theft by hacking or scams? How would I access my money in a web-only bank account if the Internet should for some reason go down? It is great to be able to surf where I want, but does that surfing potentially expose me to malware that could capture my account information when I bank with the same computer? Is it paranoid to consider using a separate computer for banking and another for other web access?

It is exciting to think that the whole world can be accessed through that little RJ-45 Ethernet jack on your cable or DSL modem. It should also be sobering to consider that the whole world could be there in that connection.

Tablets of Clay

The crooks are not only after us on the Internet, but also in our electronics stores. Over this last Christmas, a number of iPad purchasers got the wrong kind of tablet. In Canada, a number of customers that purchased iPads at reputable stores like Best Buy and Walmart later found the box contained not a tablet PC but a slab of modeling clay. In perhaps more than a dozen reported cases, it appears crooks purchased iPads at these stores with cash, replaced the items in the box with the same weight in clay and expertly resealed the boxes. The boxes were returned to the stores for refunds, and since they appeared to be unopened, they were replaced on the shelves to be purchased by unsuspecting customers. The first customer discovering this switch was thought to be a scammer by the store, but after additional cases were discovered, he was reimbursed and given an iPad.

Quality Assurance

A toothpaste factory had a problem: they sometimes shipped empty boxes, without the tube inside. This was due to the way the production line was set up. Understanding how important it was to have 100% accuracy, the CEO of the toothpaste factory got the top people in the company together and decided to start a new project, in which they would hire an external engineering company to solve their empty boxes problem. The project followed the usual process: budget and project sponsor allocated, RFP, third-parties selected, and six months (and $8 million) later they had a fantastic solution on time, on budget, high quality and everyone in the project had a great time.

They solved the problem by using high-tech precision scales that would sound a bell and flash lights whenever a toothpaste box would weigh less than it should. The line would stop, and someone would walk over and yank the defective box out of it, pressing another button when done to re-start the line.

A while later, the CEO decides to have a look at the ROI of the project: amazing results! No empty boxes were shipping out of the factory after the scales were put in place. Very few customer complaints and they were gaining market share. "That's some money well spent!" he says, before looking closely at the other statistics in the report.

It turns out the number of defects picked up by the scales was zero after three weeks of production use. It should've been picking up at least a dozen a day, so maybe there was something wrong with the report. He filed a bug against it, and after some investigation, the engineers came back saying the report was actually correct. The scales really weren't picking up any defects, because all boxes that got to that point in the conveyer belt were good.

Puzzled, the CEO travels down to the factory, and walks up to the part of the line where the precision scales were installed. A few feet before the scale, there was a $20 desk fan, blowing the empty boxes out of the belt and into a bin.

"Oh, that," says one of the workers. "One of the guys put it there because he was tired of walking over every time the bell rang."

April 2012 CD of the Month

ARI - April newsletter
Audacity - Updated audio editor
Auslogics - Updated disk Defrag tool
BootVis - Utility to optimize the boot process of XP
cCleaner - Updated Hard drive cleaner
CDOMlists - Lists of past CDOMs
ConverterLite - Converts audio/video files to various formats
FireFox - Updated browser
FotoMix - Photo special effects and manipulator
FotoMorph - Photo animator
FreeOTFE - On the fly encryption
GeoSetter - Shows and changes geo data and other metadata
Geotag - Shows geotag data in digital photos
ImgBurn - Updated CD/DVD burner
InfraRecorder - Afree CD/DVD burning solution
InSSider - Wi-Fi scanning software
Irfanview - Updated compact graphic viewer
JetClean - Cleans junk files and unneeded registry entries
MBRcheck - Checks the legitimacy of the Master Boot Record
MemberContributions - Things e-mailed to me from members
Netalyzr - Tests your Internet connection
NotePadPP - Updated code editor and Notepad replacement
OldTimeRadio - Old time radio broadcasts
OSforensics - Sophisticated HD analyser
PCLoginNow - Reset the password for Windows
RKill - Terminate known malware processes
SleuthKit - Sophisticated HD analyser
SuperAntiSpyware - Updated anti spyware program
TDSKiller - Detects and removes rootkits (malware)
Texter - Text substitution that replace a hotstring with a larger piece of text
Threatfire - Antivirus software
Thunderbird - E-maill client
TimeFreeze - Clones your system for virtual use
Tweaking - Tweaks to your system to increase speed and stability
VLC - Updated media player
WinDirStat - Updated HD usage display

Meeting Location and Special Accommodations

The Glenside Public Library address is at 25 E Fullerton Avenue, Glendale Heights, Illinois. Please park away from the building. Thank you. The meeting(s) are not library sponsored and all inquiries should be directed to Mike Goldberg at MikeGold60137(at)yahoo.com. Individuals with disabilities who plan to attend this program and who require certain accommodations in order to observe and / or participate in the program are requested to contact CAEUG president, Mike Goldberg at MikeGold60137(at)yahoo.com, at least five (5) days prior to the program, so that reasonable accommodation can be made.

Members Helpline
Any member with a specific expertise can volunteer to be on the Members Helpline.

Beginner Helpline
- Billy Douglas

Beginner hardware problems
- Dick Fergus

Hardware problems, XP, Win 7 & Linux
- John Spizzirri