January 2014

Microsoft REGISTERED Refurbisher

Charlotte County Computer Group

30th YEAR Anniversary

1984 - 2014

The Next General Meeting of CCCGC will be January 7, 2013

See us on the Web www.cccgc.net

Official Publication of the Charlotte County Computer Group Corp.

PROMOTING COMPUTER LITERACY AND EDUCATION IN CHARLOTTE COUNTY

VOL. XXVI

No. I

Inside this issue:

Charlotte County Computer Group

2280 Aaron Street
Port Charlotte, FL 33952

Phone: 941-295-7672
941-625-4175 x244
E-mail: office@cccgc.net

The President's Platform by Ron Wallis, President CCCGC

As we look forward to a new year it's time to reflect a little on the past one. We have given out over 400 computer systems to the needy in the county, a record number for our club. Also we have helped a record number of members with their computer problems through our members help program.

We are teaching a number of classes to help educate our members. We wish to thank all those who have helped to make these things possible. We also wish to thank the outgoing officers for the great job they have done getting us to this point.

2014 is the 30th anniversary of our club and to celebrate that, on the first Tuesday of March in lieu of our regular meeting we will have a social get together. There will be hors d'oeuvres, tea sandwiches, beverages, (coffee, tea & lemonade), cash bar, and door prizes, etc. It will be in Centennial Hall (our meeting room) from 5:00 PM to 7:30 PM. All members are welcome and may bring one guest.

In order that we know how many will be there, attendance will be by ticket only. Tickets are free and will be available at the Jan. meeting and in the office until Feb. 14th.

We hope to see you all there for this celebration of our club.

The executive board hopes you all had a joyous Christmas, and we wish all of you a happy and healthy New Year.

Ron

Charlotte Bytes

Computer Drawing

Phil had little time to sit down before he got up to claim the computer.

He just wanted his picture taken for the second time.

You must be lucky to win twice in the same evening. Anyway, good luck to Phil with the smart looking computer system.

To all those other ticket holders, hope you win the next time.

50/50 Winner

Caroline Faber jumped right up when the number was called.

With Christmas not far away, we are sure she can find a place for the money.

Door Prize Winners

Left to Right

Shaneen Wahl (Not Pictured)

Ron Muschong

Jeanne Niosi

Gale Coney

Phil Gale

WELCOME

New Members

Janee Morrison
John Porter
Alfred DePinho
Sherry Williams
William Matchat
Myrna Charry
Daniel Voglund
Jack Brown
Ray Hardesty
Rad Petrovic
Ann Alcantara
Lue Danitz
Jerry Williams
Seeb Post
Jackie Gard
Selvarajah Sunderavel
Lee Willett
Mary Brown
Alice Bradley

The Executive Board and Members of CCCGC welcome each of you to the group. We're Here To Help. Membership Has Its Privileges.

If you have any questions, concerns or need computer help, please contact us at the office. We will endeavor to help you any way we can.

87 members attended the December meeting and enjoyed Scott Baty's presentation on Wireless Security.

We were told to beware of the wireless bandits. One man had a wireless router that didn't have password protection on his system. He lost all that he owned and valued because a very smart guy used his wireless to download porn. The individual was charged for the crime. It is your responsibility to make sure you are protected.

The courts are still arguing which party is responsible for the internet usage, the account owner or the person accessing the signal.

A wired (plugged into device) Broadband or DSL line is the most secure connection. It is more dependable and operates faster.

Wireless has all the same features as wired, plus a base station which signals through the airwaves. This allows all the devices to connect to the internet.

SSID is the public name of a wireless network and it means "Service Set Identifier device." Most routers come with a generic name like Linksys or Netgear. You need to change the name of the network. You must plan on changing the password when installing the system. In almost all cases, the network name is ADMIN and the password is PASSWORD.

After lots of questions from the audience, hopefully we understand the wired and wireless mystery. You might want to look at your internet bill to see if you are paying for rented equipment. It might be more economical for you to purchase a modem or router. All of the information discussed is included in a downloadable Power Point covered in Scott's presentation. Go to www.cccgc.info to the section Links and connect to Wireless Security. Now you don't have an excuse. It is up to us to make sure we are secure.

L ydia

Program High-Lights

Charlotte Bytes

Charlotte County Computer Group

Information: (941) 295-7672

(941) 625-4175 x244

Official publication of the Charlotte County

Computer Group Corporation

2280 Aaron Street

Port Charlotte, FL 33952

www.cccgc.info

www.cccgc.net

Acronis 2014

Title: Selecting the Best Backup Approach

By Gene Barlow

Description:

Doing regular backups of your computer is the best possible way to protect your computer and its files. Today, we are inundated with many different ways to do backups, that it is difficult to know which approach is best. They do not give you all the same protection, so you may end up surprised when you have a hard drive crash and find out that the backup approach that you picked cannot get your computer running again quickly.

In this presentation, we will inspect the five most common backups approaches on the market and tell you the advantages and problems with that backup approach. We will also describe why and where you would want to use each type of backup available. Most important of all, we will tell you why one backup approach is vastly superior to all of the others.

This is an important topic on backup technology and one that you will not want to miss.

Presenter: Gene Barlow has worked with computer systems for over 50 years and has specialized in backup technology and hard drive utilities for the past 20 years.

He can make a complex topic easy for everyone to understand, yet still provide lots of details that you need to know. He is one of the most popular presenters to user groups and have presented to thousands of user group audiences. You will find his presentation easy to understand and very interesting.

Be sure to attend this session.

Microsoft® REGISTERED Refurbisher

For more information go to www.cccgc.info

View/download Bytes

Please be sure to register online for classes

Charlotte County Computer Group

30th YEAR Anniversary 1984 - 2014

Classes & Events Calendar

January 2014 CCCGC Events Calendar

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
1			1 	2 **Back To Basics** 2 to 4 PM Dick Evans	3	4
5	6 **Libre Office** 2 to 4 PM John Palmer	7 **General Meeting** 7:15 PM Classes 5:00PM 6:00 PM	8 **Presentation** 2 to 4 PM Larry Hurley	9 **Back To Basics** 2 to 4 PM Dick Evans	10	11
12	13 **EaseUs Backup** 2 to 4 PM Yvette Pilch	14	15 **Maintenance** 2 to 4 PM Ron Wallis	16 **Back To Basics** 2 to 4 PM Dick Evans	17	18
19	20 **Libre Office** 2 to 4 PM John Palmer	21 **Windows 8.1** 2 to 4 PM Ron Wallis	22 **Photos** 2 to 4 PM Larry Hurley	23 **Back To Basics** 2 to 4 PM Dick Evans	24	25
26	27 **Windows 8.1** 2 to 4 PM Yvette Pilch	28	29 **Maintenance** 2 to 4 PM Ron Wallis	30 **Back To Basics** 2 to 4 PM Dick Evans **Board Meeting** 6:30 PM	31	
		NOTICE All Non Meeting Night Classes will be held in **Our New CCCGC Office.**			**Notes:** OFFICE HOURS: 10:00 AM-2:00 PM MONDAY -FRIDAY **Please sign up for classes ONLINE:** http://www.cccgc.info	

Charlotte Bytes

Malwarebytes UNPACKED

See us on the Web
www.cccgc.net

CCCGC

Malwarebytes 2013 Threat Report

December 4, 2013 | By Adam Kujawa

The past year turned out to be an interesting introduction into the new types of threats users are facing as well as what they will continue to face, at greater levels, in the coming years.

We have continued to see the use of scammer and "assumed guilt" threats such as Ransomware and the emergence of even greater threats using similar tactics. We have seen the rise and fall of a very popular exploit kit and had an entire year of cautious surfing because of drive-by exploits and watering hole attacks.

Phone scammers have shown us that it's not always safe to trust people who claim to be technical specialists and the battle against mobile threats has raged on in greater severity.

As we enter a new year, we can expect these threats to continue with more destructive force than we have ever experienced.

Our world is changing and much of our personal communication; banking and overall well-being is now accessible online. This trend will only continue as we adopt a new 'online life', where all sorts of criminals are taking advantage of those inexperienced with internet security.

We are lucky that we have been able to learn from the past year's challenges and adopt new strategies to remain safe online. The lessons learned are invaluable when dealing with future threats; however, perhaps the greatest lesson of all would be the individual's understanding of online threats and proper security measures. For example, while most Antivirus programs provide adequate protection, none of them will keep you safe if used improperly.

A few years ago, I said the internet was most like the 'Wild West,' where people were free to start their own adventure. There were outlaws, for sure, but at the same time law men who would protect the innocent.

Unfortunately, I can't say that any more about our current situation: the cowboys are gone, and have been replaced with soldiers. The internet today is a warzone, and everybody online is part of the fight.

Biggest Threats of 2013

Ransomware

In the outlook report from 2012, we mentioned that it was the greatest year for Ransomware, and I still attest that based on uniqueness, novelty and diversity, that is true.

However, as far as damage goes, 2013 has it beat. Ransomware, as you may know, is short for Ransom Software/Malware that attempts to lock the user out of their system or encrypt their Tiles, holding their livelihood "Ransom", in return for cash.

Last year, we saw Ransomware that frequently posed as government agencies, such as the FBI, and demanded the user pay a fine. I called this type of scam "assumed guilt" because it accused users of crimes that they probably didn't commit but might believe they had by accident.

Ransomware last year and into this year, was mostly spread via exploit kits. It took a while and numerous arrests but the numbers have decreased and some of the big players have even ended development of new variants.

Continued on Page 8

Charlotte County Computer Group

30th YEAR Anniversary

1984 - 2014

The Charlotte County Computer Group Corp.

Is a non-profit 501(c)3 organization as classified by the Internal Revenue Service.

Donations, gifts, bequests, legacies, devices and transfers are deductible under federal laws.

Officers and Board of Directors for 2014

President: Ron Wallis

Vice President: A Yvette Pilch

Secretary: Ron Muschong

Treasurer: Larry Hurley

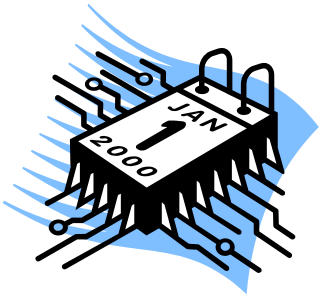
Director: John Hegard

Director: Grover Mudd

Director: Lydia Rist

Director: Frank Messina

Director: Mava Graves



We're on the Web
www.cccgc.net

Charlotte County Computer Group Corporation

General Meeting Minutes

12/03/2013

Larry Hurley and John Hegard are not pictured

As our bylaws require, elections must be held at the General Meeting. At our December 03-2013 general meeting, the elected Officers and Directors were installed into office by Harold Nixon, the nominating chairman and outgoing President.

The new Executive Board consists of the following members:

Ron Wallis, President

Yvette Pilch, Vice President

Larry Hurley, Treasurer

Ron Muschong, Secretary

The Directors elected:

John Hegard

Frank Messina

Lydia Rist

Grover Mudd

Mava Graves

This new board takes the helm of our group at the December board meeting to be held on 12-26-2013. Lets embrace these board members and offer any help that is needed to make the organization grow.

Minutes taken by Yvette Pilch, Secretary

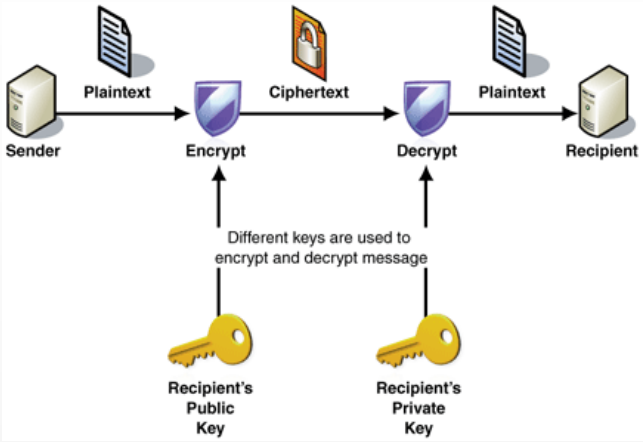
Cryptolocker

Malwarebytes UNPACKED

Reveton and Urausy were two of the biggest ransomware groups of the last year but their operations do not hold a candle to the kind of damage caused by the infamous Cryptolocker.

Discovered in September, Cryptolocker actually double encrypts a user's personal files (such as images and documents) with both a local AES key as well as a remotely created and remotely stored RSA-2048 key.

So what about RSA-2048? Can't you break it?



Well, hypothetically, yes, we could break it; however, the time it would take to break that kind of encryption would take more time than we will be alive. To put it into perspective, using a normal desktop system to try to revert your files back to normal, without the use of the private key, would take roughly 6.4 quadrillion years.

If you had a massive amount of super computers and the smartest cryptographers and mathematicians in the world working on it, it might take a little less time but nobody knows because nobody has done it yet.

The price to unlock your files has changed a bit depending on the type of currency accepted. It started out with MoneyPak cards, same as with older Ransomware but then evolved into only Bitcoins. The price was set at ~$300.

Cryptolocker informed the user that if they did not pay within the time allocated (usually 72-96 hours), the remotely stored private key would be erased and their files would never be decrypted…or so we thought.

Whether it was their original intention or not, the creators of Cryptolocker decided to give their victims a break at the cost of ~$2000 and a website was setup to allow victims to pay 10 Bitcoins and receive the key to unlock their files.

So this begs the question, was the key ever really destroyed as advertised by the Cryptolocker ransom screen? If they are able to unlock a system after the fact then the answer is no, it was stored away somewhere for later use.

The other possibility is that all distributions of a certain Cryptolocker variant used the same key with every system it infected and it is just a matter of finding those infected with the correct variant that can pay the $2k.

Either way, to unlock the files, the user has to re-infect their system with Cryptolocker and then pay an immense fee, something we highly recommend NOT to do.

The security community is still working hard on battling this threat and the threats that we will surely see in the future that imitate it.

Continued on Page 9

Malwarebytes UNPACKED

For now, our best defenses are proactive protection to stop the malware before it has a chance to infect the system. Be it though stopping the executable or preventing the malware from reaching out to its command and control server, therefore preventing the encryption of the files in the first place.

We will visit Cryptolocker again in our section on 2014 predictions but be sure that this is not the last we will see of this style of Ransomware.

Phone Scams

Phone scammers work along the same lines as Fake AVs, where you have a third-party source telling a user that they have tons of malware on their system and it needs to be cleaned up, usually for a high price.

Phone scammers are not exclusive to 2013 but the amount of reports we get and the different types of scams these guys are using seem to be peaking.

In 2013, we have seen scammers:

Pose as Microsoft

Pose as an antivirus company

Pretend they can remove malware from a Mac

Claim that not being able to connect to an inactive web server means you are infected

Pose as law enforcement

…and much more!

Our Senior Researcher Jerome Segura has made three videos based on phone scammers and the tactics they use to fool unsuspecting users; I highly recommend checking them out.

http://www.youtube.com/watch?v=3P6uv8Fy3ik

http://www.youtube.com/watch?v=FDJWixw4TCI

http://www.youtube.com/watch?v=s60jLxInYb4

The biggest defense against this type of scam is knowledge, you will most likely never receive a call from a legitimate software company or antivirus/anti-malware firm to remove malware they have "detected" on your system.

To help our users and readers in educating themselves on these threats, we have created a 'Tech Support Scams – Help & Resource Page' on our blog that is updated when new scams appear to reflect the current threat landscape.

The principles of identifying scams is age old. However, when presented with evidence of a problem in a method that the normal person does not understand, those principles go out the window. That is what these scammers try to exploit so do not become a victim.

Continued on page 10

Android Malware

Since we knew mobile phones were going to run operating systems, we knew that mobile malware would be inevitable. And 2013 showed us an increase in mobile scams and malware.

A large portion of mobile malware consists of what we refer to as SMS Trojans, malware that sends premium text messages or makes premium phone calls without the phone owners knowing about it. The user doesn't discover what has happened until after they have received the bill. While these types of attacks are primarily seen in Eastern Europe, others exist worldwide.

A similar threat example is the Perkle crimeware kit; it infects the user's desktop, poses as an authentication measure for the user's banking web site and requires the scan of a QR code that downloads malware onto the user's mobile device.

The mobile side waits for confirmation texts sent by the bank, intercepts the codes and sends them back to the desktop to gain access to the victim's bank account.

Either way, the amount of mobile malware seen this year has increased substantially enough for the community to consider it something we are going to be dealing with much more in the future.

Blackhole Exploit Kit

In 2012 and a large portion of 2013, the BlackHole Exploit Kit was the primary method of malware delivery for cyber criminals looking to setup drive-by attacks. It hosted an assortment of different malware, depending on the need of the criminal using it, for example:

- Zeus Trojan
- ZeroAccess Rootkit
- Reveton Ransomware
- And more

The kit was sold on cyber-crime forums and black markets to would-be criminals to setup on their own (or compromised) web servers. The criminals would define which payload was to be loaded (the malware) and what exploit to use. From there, once a user visited an exploit page, the malware would be installed.

In many cases, exploit kits are rented out, purchased for a high price from one criminal and then offering to host another criminals malware for a fee.

In early October, law enforcement arrested the creator of the BlackHole Exploit Kit, "Paunch", and since then, the use of BlackHole has steadily decreased.

With older versions still lingering and being used by cyber criminals as well as modified versions released by third-party sources.

As we enter 2014, we may see less and less of the older variants of BlackHole, however it's doubtful that it will drop off the map entirely.

At the same time, we may see the emergence of a brand new dominant exploit kit that has all the ability and threat of BlackHole but with new exploits targeting more current operating systems.

Continued on Page 11

Microsoft REGISTERED Refurbisher

Official Publication of the Charlotte County Computer Group Corp.

PROMOTING COMPUTER LITERACY AND EDUCATION IN CHARLOTTE COUNTY

CCCGC

Malwarebytes UNPACKED

DDoS (Distributed Denial of Service) Attacks against Banks

2013 had its fair share of bank attacks, be it through the use of malware or just hacking. One of the most notable examples were attacks against US banks in August: The attack began as a Distributed Denial of Service Attack against the target bank, the IT staff was able to respond and worked hard to fend off the attack, keeping their servers and services available to customers.

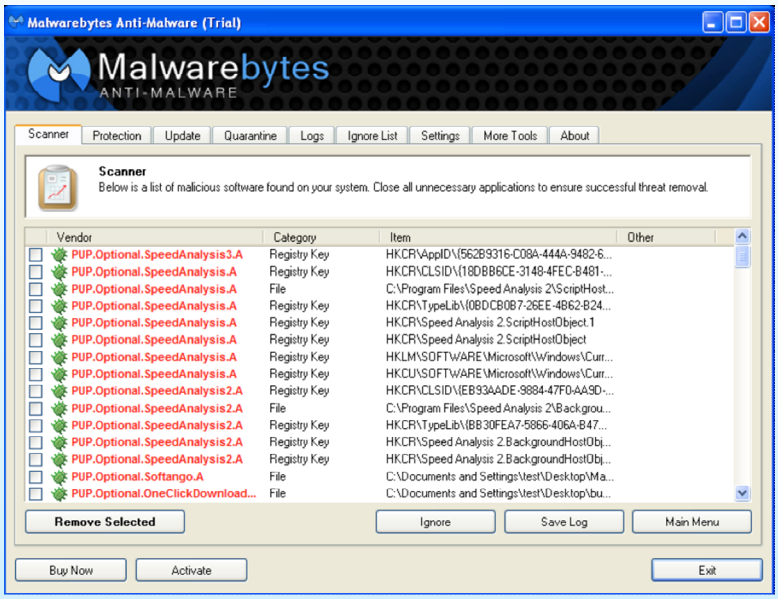
However, while the staff was busy dealing with the DDoS attack, malicious attackers were able to infiltrate the banks systems, unnoticed due to being concealed under the massive amount of traffic from the DDoS.

The attackers made off with a significant amount of money in this highly organized and effective cyber bank robbery.

Crime on all levels has been duplicated online, bank robbery included. Will we see more attacks? Definitely. Will they get worse? Yes. However, with every attack comes the lessons learned and shared with the community, making banking experiences even more secure.

PUPs (Potentially Unwanted Programs)

Potentially unwanted programs are the slightly less harmful cousins of malware, installing things on your computer you neither want or need, devouring system resources and making your computing experience a nightmare.



You might be wondering what exactly PUPs are, well a few examples are:

- Toolbars
- Search Agents
- Value Finders
- Etc

In July of 2013, Malwarebytes Anti-Malware began detecting PUPs and offering their removal to our users, we do not automatically flag them for removal but allow the user to choose whether they want to run the software or not.

In late November, we discovered a new type of threat with some PUP peddlers, the inclusion of a Bitcoin miner installed on the system. This is a serious threat in that running a miner on a system that is not designed to do so may cause serious damage to the system itself.

We expected such things from malware like Ransomware, however, it is an entirely different story when programs that were potentially harmless, are now doing harm to unsuspecting users.

For an official listing of what we at Malwarebytes consider "Potentially Unwanted" check out our criteria for PUP classification:

http://www.malwarebytes.org/pup/

Continued on page 12

CCCGC

Microsoft REGISTERED Refurbisher

Charlotte Bytes

Malwarebytes UNPACKED

2014 Predictions

Ransomware Evolution

2012 and then 2013 showed us the peak of Ransomware and the kind of damage it could do. From being simple psychological games that barely prevent you from continuing use of your computer, to accusing you of crimes and eventually encrypting all the files you hold dear.

Will we continue to see it in 2014 though? Most definitely.

While many people seem to know about the threats of Ransomware and properly protect themselves from it; cyber criminals just change around their attack method to counter our protections.

Seeing as how often it has been used in the wild, we can say that the attack is highly successful and therefore we can expect to see its continued use.

However, if we look at some recent activities made by the criminals using Cryptolocker, we can see that they are getting somewhat desperate. Cryptolocker now offers a "post timer" option to decrypt files, by hosting a site that offers decryption for a higher fee.

Did they do this because they weren't seeing a very good return in investment from the original infections? Maybe they are just trying to reel in even more cash from users that were unable to pay the original fee. (Though in my opinion, if you think that users who are unwilling to pay a ransom of $300 how can you expect them to pay $2,000 or more.)

I predict that for 2014, we will see continued evolution of Ransomware, figuring out new ways to infect users and force them to pay a fee.

We will see Ransomware making more of a presence on previously less targeted platforms, such as OS X and mobile devices.

However, unlike the end of 2012 and early 2013, we will see fewer cyber gangs using Ransomware tactics. For example, there were numerous families in the wild, spreading very similar Ransomware but different enough and originating from different sources, while 2014 will most likely have fewer sources but more advanced, and therefore dangerous, malware.

Mobile and Device based Malware

Speaking of mobile malware, you can expect the continued threat of malicious software and scams targeting your mobile device in 2014.

As mentioned previously, we've seen an uptake in mobile malware in 2013 as mobile devices became the primary source of internet use, eCommerce and social interaction for many users.

This user trend is unlikely to go into decline as technology gets even more portable and more powerful, therefore where the users go, the criminals will follow.

Those of us in the west have been lucky that we have not endured the types of mobile threats our friends in the east have, such as Russia. SMS Trojan attacks are far more frequent in that part of the world than they are in the U.S. However, there are plenty of avenues malware authors could take to steal our money.

Continued on page 13

For example, we could see mobile malware that uses the saved Google Store credentials to buy apps that you don't want or need. They could also use your device for malicious attacks, such as DDoS, and adding your tablet or phone to a botnet.

In addition, it is not farfetched to think that mobile devices are the next big target for remote access trojans, allowing your phone to become a surveillance camera, microphone and in the case of Bluetooth, a transmission device.

Also mentioned previously was the discovery of malware tactics that infected the desktop as well as the mobile device; you can count on the fact that we will see an increase in that type of threat.

Many online services, banks, stores, etc. are using authentication measures that require codes sent to mobile phones, making it a requirement for cyber criminals to intercept calls, text messages or anything else for the purpose of accessing secured services.

Luckily, many antivirus and Anti-Malware vendors (including us) are migrating their already trusted malware protection solutions to mobile devices to counter these threats.

Mac OS Malware

2014 will have more attacks against Mac operating systems, period.

If you've kept up with yearly predictions from security companies in the past, we have all said this before and usually the impact isn't quite what we expected. It's almost like a "boy who cried wolf" thing, but just like the story goes, those who don't heed the warnings will inevitably become victims.

Recent history has shown us that Macs are being targeted with similar attacks as PC users. We've seen Ransomware, malicious browser plugins, rogue antivirus software and a slew of other malware.

In addition, computer repair scams exist for Mac users just as much as for PC users, a threat that doesn't even require a malware infection but rather just an unsuspecting and uninformed user.

Finally, many of the plugins, extensions and third-party applications that are exploited on Windows are also used on Mac platforms and therefore susceptible to the same threats when it comes to remote code execution.

New Methods of Privacy

The biggest story in security this year has been the leaks released about the National Security Agency (NSA) and their ability to collect, intercept and decrypt all kinds of electronic communication.

Due to the new concern users may have about their privacy while online, we may very well see an increased development of privacy technologies.

From enhanced biometric software to three factor authentication, 2014 will most surely see the average user taking precautions in securing their personal data online.

As an unintentional bonus, this will in turn protect users from online scams and even malware that would otherwise be able to infiltrate and steal confidential information. Hopefully the fear of government surveillance will be enough to safeguard otherwise unprotected users and therefore starve the cyber criminals.

New Dominant Exploit Kits

As I mentioned when explaining the previous year's threat from the BlackHole Exploit Kit, there will likely be a successor to the dominant exploit kit throne.

I predict that by the middle of 2014 we will see a new and more powerful exploit kit that possesses similar traits to BlackHole and will either be very cheap for cyber criminals to purchase or be leaked to the underground community to use for free.

However, 2013 was a great year for law enforcement, with arrests of the BEK author, numerous criminals behind the rampant use of Ransomware and even arrest of actors behind DNS Changer. The next year may follow that trend and as soon as we see a new BEK, it won't take long for it to be taken down.

Hardware Exploits

Attacking software is easy and very effective. Users use the same software across the board, be it different versions. A cyber-criminal has a high probability of success when they target something like Java or Flash.

The other end of the spectrum is hardware attacks, where attackers use specially created software to exploit vulnerabilities in user's firmware running on some piece of hardware. These attacks are not as common however they are incredibly powerful.

The problem is that so many users use different types of hardware in their systems and predicting what a user has running is a nearly impossible without targeted intelligence. Therefore, we only really see hardware attacks used in state-sponsored operations, where one government is trying to infiltrate the networks of another.

With the migration from PCs to Macs, we may very well see more attacks aimed at certain types of Mac hardware, only because Macs use a standard hardware build for their products.

A clever cyber-criminal might look at the most commonly used Apple product and then investigate possible ways to exploit that particular system. An attack aimed in that direction has a higher chance for success than a similar attack on the PC. The potential for information stealing, disruption and even being undetected is much greater.

The good news is that hardware attacks are very hard to come by, regardless of whether or not intelligence gathering has been performed.

For the average user, there is little likelihood that cyber criminals would target their systems because of time and resources required to develop such a threat.

It is still more likely that hardware attacks would be developed and aimed at state-sponsored entities, though as we continue to adopt new technologies and policies like "bring your own device," the threat of infection becomes greater.

Conclusion

Casual use of the internet is no longer an option, your system should look like it's ready for a fight, the same as you would look if you were to enter a warzone. Equipped with the proper tools, a user has a chance of being safe from online threats, an updated antivirus, a firewall, additional protection software like Anti-Malware and Anti-Exploit tools, up to date operating systems and third-party extensions and a trustworthy and secure browser.

However, all those protections would be worthless without the proper knowledge.

You can always wait until the news has reported on a threat, luckily our society treats cyber-crime as newsworthy and important as bank robberies or serial killers, hopefully that trend continues.

Though what you read or watch on the news is only a part of the required knowledge, telling you about the biggest and flashy attacks but not so much on the threats you face every single day.

To obtain the knowledge of those threats, read security vendor blogs, follow a couple of security vendors or professionals on social networking sites, listen to podcasts and other programs devoted to computer security.

Then, after you have armed yourself with enough survival knowledge that you are confident online, share it. The biggest targets for cyber-criminals are people who aren't informed, help out your fellow-man by educating your friends and family, even if it's in passive conversation. Share links to articles and ask questions.

This war will not be won with passive defense, installing security software and then ignoring it for a year. It must be fought with an active offensive to prevent as many victims as possible. If we can do that, if we can limit the amount of people susceptible to attacks by cyber-criminals, we will eventually starve them out of information and money.

If we can make the cyber-crime business less lucrative, we will shrink the amount of threats we experience drastically. It all starts with you.

Thanks for reading and safe surfing!

CCCGC

Charlotte Bytes

makeuseof

10 End-Of-The-Year Tech Related New Year Resolution Recommendations

by Bakari Chavanu

New Year's Resolutions

As the year comes to close and a new one begins, it's a good time to make fresh goals or carry out tasks we have put off for quite some time.

The following list is my personal recommendations for tech related tasks--from the vitally important, backing up your computer hard drive, to the most difficult challenge of spending a whole day without getting on your computer. My list includes links to MUO (Make Use Of) articles that provide ideas for how to carry out specified tasks, but you're also encouraged to of course research other ideas and solutions. I also welcome your recommendations for tech related tasks I didn't include in this list.

1. Backup Your Computer Hard Drive

Technicians who repair computers say that, still less than half of computer users back up their hard drive. While with most newer computers, hard drive failures may occur less, it only takes one for it to happen and loss of all your data.

Justine's article on Redo Backup is a good one for PC users, while the default Time Machine and Super Duper are good programs for Mac users. A full backup of your system requires an external hard drive that is larger than the memory of your computer's internal drive. Create an automatic system so backups can be done and checked on a regular basis.

2. Backup Media Files

If you are storing photos, music, and other important media files on your computer, these files should be a part of your backup system, but I suggest you also keep a special off-site backup of photo files that are most important to you. Precious photo files can't be replaced, so copying them to an external drive, such as a thumb drive, can be serious insurance against loss of most your important photos.

If you have enough room on a Google, Dropbox,or any other cloud storage account, backing up precious media files to a dedicated storage is another data recovery solution. It's simply a matter of dragging and copying important files to another location.

3. Change Passwords

Change the password of your financial and administrative accounts, your router, and other sensitive accounts or pieces of hardware. I know it's a mental challenge http://www.makeuseof.com/tag/create-strong-password-forget/?utm_campaign=newsletter&utm_source=2012-12-31 to memorize new passwords, but for the accounts you access on a regular basis, it's well worth the effort.

4. Clean Out The Hard Drive

Take an hour and clean out your computer's hard drive of files and applications you no longer use. Especially look for those files that are over a few hundred megabytes and determine if you still need them. http://www.makeuseof.com/tag/visualize-disk-usage-windows-scanner/?utm_campaign=newsletter&utm_source=2012-12-31

Conclusion on next page

makeuseof

5. Create a Photo Book

After you have backed up all your photos, create a book of the year's most memorable photos. Sure, it's great to have your photos stored on Facebook or Flickr.com, but a printed book is still more tangible and attractive for viewing your precious memories. http://www.makeuseof.com/tag/create-photo-book-photoshop-elements/?utm_campaign=newsletter&utm_source=2012-12-31

Even if you have lots of low-resolution photos, on your smart phone for instance, they can still be published in a photo book. In the U.S., stores like Walgreens and Costco have fairly easy online ways to layout and order printed photo books.

6. Budget Your Money

If you're not doing a good job of keeping track of your finances and budgeting your money, sign up for a free Mint.com account. Allowing Mint http://www.makeuseof.com/tag/mint-budget-spending-online/?utm_campaign=newsletter&utm_source=2012-12-31 to download your financial accounts is one of the best ways to monitor and budget your spending. It's like the old envelope budgeting system, but it's all digital.

7. Cook New Meals

If your typical dinner meals are becoming a little stale, subscribe to one or more online recipe sites, and commit to cooking at least 5-10 new dinners next year.

I use the Paprika iPhone app to download recipes and keep track of favorite meals.

8. Cancel Subscriptions

Go through your email client and unsubscribe http://www.makeuseof.com/tag/mass-unsubscribe-nuisance-email-newsletters-unsubscribr/?utm_campaign=newsletter&utm_source=2012-12-31 to newsletters and social website notifications you haven't been responding to. Reducing email clutter can reduce the amount of time you spend reading and managing emails, and thus help you make time for other things.

9. Automate Computer Tasks

If you haven't been using automation workflows and keyboard shortcuts, you're probably not being as productive on your computer as you could be. There are ways to automate tasks on a PC, Mac , and Ubuntu without knowing a single word of code. There are even ways to automate online tasks, using tools like ifttt. http://www.makeuseof.com/tag/10-great-ifttt-recipes-automate-web-life/?utm_campaign=newsletter&utm_source=2012-12-31 Make a goal of creating a few automation hacks. Once you do a few, you'll no doubt want to do more.

10. No Computer Day

Choose one day a week in which you avoid getting on the computer. As much as the computer is a part of our daily routine, it can cause us to become detached from other important responsibilities and social interactions. I try to avoid getting my computer either on Saturday or Sunday, unless it's related to work.

Well, these are my ten recommendations. What are yours? Start today and make a list of the tech related tasks you need to get done.