Southern Districts Computer Users Club Inc.

Supporting inexperienced users with local expertise

Vol.: — 20
No : — 03

March, 2020

SDCUCI NEWS

Contacts: Web Site: — http://sdcuci.com
E-mail: — sdcucinc@gmail.com

Newsletter Editor: David Porteous - daibhidhp@aussiebb.com.au

Meetings are held monthly on the third Wednesday at 7.30 pm, in the hall at the rear of St Mary's Catholic Church on the Corner of Bains and Main South Roads, Morphett Vale

Cost $3.00 per person per meeting. This includes a copy of our Newsletter, plus coffee/tea and supper

Visitors are always most welcome

After 3 visits, you are requested to become members

Annual Subscription:
Single — $20.00
Family — $30.00

Both Novice and Experienced computer users will be most warmly welcomed

The Brownpaddock Chatter

March 2020

I realise that from time to time we all deal with health issues of our own, but I would like to commend two of our Committee members for their diligence in attending Committee meetings.

Val McMartin has been most seriously ill for some months and David Porteous has had a lower back operation with associated lack of movement. Despite this they have both soldiered on attending as many Committee meetings as they could. Full marks to both of them!

With the purchase of our new Projectors, we can now offer our previously loved units for sale.

One is an "NEC V260X" comes with a 2000 lumen brightness. The second is a "Benq MW519". This has a 2800 lumen. (This difference in brightness is why they looked different on the screen). Both are dated but are still quite functional.

If anyone is interested please see me or one of the other Committee members with a reasonable offer!

Jim Greenfield

Problems with VirusTotal

By Jim Greenfield

In response to the article on VirusTotal in February Newsletter, if you don't know what VirusTotal is yet, it is a "Free Online Virus Malware (and URL) scanner". Although many users of VirusTotal are relying on the front-end service to identify whether a file is identified as malware by any of the large number of anti-virus engines, the service is more like Facebook and Google where the regular users are the ones actually providing the service. On the back end, VirusTotal is actually a project of Hispasec Sistemas that relies on the public contribution of new files to provide samples to anti-virus companies for analysis. I have a few concerns with how the front-end service is being used and how it is being provided.

Cached results

I believe large number of malware authors are using VirusTotal to scan their own software. This is risky for the malware author, because VirusTotal indicates that if just one anti-virus engine identifies the software as malware, that a sample of the software will be sent to the other anti-virus engine vendors that didn't identify it as malware.

However, if none of the anti-virus engines identify the software as malware, the author not only knows that they have a great 0-day to release, but also that they have just stored cached results on VirusTotal indicating that the file is clean. Many VirusTotal users will now be lead to believe that the software is clean, because the users will be presented with cached results when they scan the file themselves, using VirusTotal.

VirusTotal should always reanalyze the file with the current anti-virus definitions and optionally offer historic results to those interested in

(continued on page 3)

Index

(continued from page 2)

No warnings

Since I've had to explain to VirusTotal users the problems with trusting VirusTotal's results, I know that users aren't always reading the VirusTotal TOS and FAQs. VirusTotal needs to explain exactly what they're providing and how it might be used, on the front page, or with the results that they provide.

VirusTotal's file scanning is being offered with no service level agreement, scanning is not being performed in a typical environment, cached/old results are often being displayed, your submission will be stored indefinitely and may be shared with third parties, and results that do not indicate the presence of malware do not indicate the absence of malware. Assurances from members of VirusTotal's "community of trust" can actually do the reverse of providing warnings, by offering false assurances.

VirusTotal should clearly provide these warnings up front and reign in their VT Community project.

Not enough transparency

It's probably not a good idea for the VirusTotal team to detail the environment that they run the anti-virus engines in, because the malware authors would quickly adapt to make VirusTotal useless to Hispasec's intended use of the project. However, it would be nice to minimally know which options the anti-virus engines are being run with, such as what heuristic levels are being used.

Without this type of information, using VirusTotal purely as the research project that it should be, is rather useless as a research project. Citing Virus Total is therefore like citing Wikipedia.

Additionally, once a file is submitted, control is lost over that data. There is no way to know how it is stored, for how long, and who it will be revealed to. If they track an IP address to you, will they be able to show the world all of the files that you submitted? It's likely that you violated a software license by submitting any files that you didn't write and aren't open source.

Not all bad

VirusTotal is adding new features and new anti-virus vendors. They obviously have some goal in mind, and they are likely meeting their customer's needs. Unfortunately, those customers are the anti-virus vendors, and not the users. VirusTotal may have a purpose to its users. I just haven't figured exactly out what it is yet. Please let me know how you currently use VirusTotal and how you would like it to change to meet your needs. 

Avast Antivirus Caught Spying on User Data

Avast antivirus is one of the popular antivirus programs for Windows 10, which has been offering its services for free for many Home users. Shockingly, they have been caught spying on user data. A joint investigation by PCMag and Motherboard reports some scary findings. It turns out they had not been offering their service for free, but trading by first collecting sensitive user data, and then selling it — all through subsidiaries, but it is happening. If you are using Avast Antivirus, we highly recommend you to switch to Windows Security for complete security.

Avast antivirus sells user data

The report from PCMag and Motherboard comes via leaked documents. These documents talk about how they use the user data they collect, and confidentially sell on to some of the biggest tech giants in the industry. The leaked data came from Jumpshot, a subsidiary of Avast. It is responsible for making the data presentable and available to clients, including Google, Yelp, Microsoft, McKinsey, Pepsi, Sephora, Home Depot, Condé Nast, Intuit, and many others. The data includes information about user movement across the internet, what they click, and more.

The data collected is so granular that clients can view the individual clicks users are making on their browsing sessions, including the time down to the millisecond. While the collected data is never linked to a person's name, email or IP address, each user's history is nevertheless assigned to an identifier called the device ID, which will persist unless the user uninstalls the Avast antivirus product.

How Avast collected the data via Jumpshot

It uses the sneaky method where it gets a users' consent to an agreement. Post this, Jumpshot tracks user data in various ways.

- It tracks keywords and the results that were clicked.
- Tracks which videos a user is watching on YouTube, Facebook, and Instagram.
- All Clicks Feed which offers device IDs attached to each click
- Data points like the URL string referring URL, timestamps, suspected age and gender of the user, etc.

That said, the whole thing looks like a big setup where the parent companies are hiding behind their subsidiaries. Jumpshot is a subsidiary of Avast, and Annalect is a subsidiary of Omnicom. Annalect offers technology solutions to help companies merge their customer information with third-party data. That makes sense because they have exact data that can help any tech company.

Android Malware Can Steal Google Authenticator Codes

New-found Android malware — Cerberus — is capable of stealing security codes from your Google Authenticator app. Earlier this year, Cerberus authors created a new variant to provide features akin to Remote Access Trojans (RAT) enabling them to steal device screen-lock credentials (PIN code or swipe pattern) and 2FA tokens from the Google Authenticator application.

In case you thought no security threat could ever outsmart the Google Authenticator app, this discovery renders that very doubtful.

According to ThreatFabric, Cerberus seems able to outwit Google Authenticator and is able to steal secret codes from inside the app. Such is the extent to which Android malware has advanced.

Google Authenticator provides an additional layer of security to prevent others from gaining access to their online accounts by using a one time only, two-factor (2FA) authentication.

Supporting websites of Google Authenticator enable users to enter their login credentials including usernames and passwords, followed by a **unique one-time only** passcode visible inside the Google Authenticator app.

The Cerberus issue is not limited to circumventing Google's 2FA Authenticator. It goes deep into your file system and downloads its contents. Bad to worse, the malware can also launch TeamViewer and setup connections, further providing hackers with full remote access of the victim's device.

Cerberus is also equipped with the screen-lock credentials theft mechanism. It simply provides hackers with more ways to remotely gain access to the victim's device. However, researchers believe the Cerberus authors are yet to release this variant of the malware and it's currently in a test phase.

Beware of the Corona Virus Scam

A PHISHING email claiming to be from the World Health Organisation (WHO) has prompted a warning from police.

The email contains a button to "seek more information" about safety measures to protect yourself from coronavirus.

When the button is clicked, the user will be taken to a website that appears to be a WHO page.

It prompts the user to enter details, including their email and password. Police warn the phishing attack could attempt to obtain information and commit identity theft.

"EmoCheck" Tool to Check for Emotet Malware

The Coronavirus malware that recently started infecting computers by luring the consumers about information about the new preventive measures for coronavirus-related pneumonia has a solution. This malware delivered the Emotet payload.

The official antidote comes from JPCERT Coordination Centre, which maintains the JPCERT/CC's official repositories. They have developed this using Microsoft Visual Studio Community on Windows 10. The tool Checks for Emotet malware infection, and reports its exact location.

The EmoCheck tool appears to be the solution for an Emotet malware infection on the computer. Emotet is known to generate its process name from a specific word dictionary and C drive serial. EmoCheck Tool scans the running process on the host, and finds Emotet process from their process name.

Using this tool is simple. Download the (32 or 64 bit) version from *https://github.com/JPCERTCC/EmoCheck* and double click to run the scanner. Once done, you should get a similar message to the below, if the computer is infected with the virus.

Below is a Sample Report of EmoCheck Tool Scan

Emocheck v0.0.1]
Scan time: 2020-02-03 13:06:20
[Result]
Detected Emotet process.
[Emotet Process]
Process Name : khmerbid.exe
Process ID : 10508
Image Path : C:\Users\[username]\AppData\Local\khmerbid.exe
Please remove or isolate the suspicious execution file.
The report will be exported to the following path:
[path of emocheck.exe]\yyyymmddhhmmss_emocheck.txt
Once you open the report, you will have the exact filename of the malware. We suggest booting your computer into safe mode without network, and then delete the file.

That said, while you can remove the virus from the computer, remember that there is a second module that is part of the payload. This module can steal user credentials, sensitive documents, browser history, and more. It would probably be best to reset your computer to stay safe providing you are backed up!

Since Japan was hit with this malware, the developers have tested it on Windows 10 1809 64-bit Japanese Edition, Windows 8.1 64-bit Japanese Edition, Windows 7 SP1 32-bit Japanese Edition, and Windows 7 SP1 64-bit Japanese Edition. Technically, it should work on all Windows 10 versions.

Once you are through, or better, before you are infected, make sure to enable Tamper Protection in Microsoft Security, and in the future, never open an email that asks you to enable content to view what is inside.

YOU HAVE BEEN WARNED. 

Hackers show we are prime targets

PICTURE this – you wake up one day, flick on *Sunrise*, and Kochie is in a flap:

"Overnight the internet was hit with the biggest co-ordinated data hack in history. Everyone is exposed," he warns.

You whip out your phone and check your accounts, but it's too late:

All your secrets have already been flushed out into the world: all your (private) messages, all your (private) photos, all your passwords, all your credit card and bank details ... everything is out there.

Here's you: "Yeah, nah. That is not gonna happen."

Here's me: "I have three words for you: Jeff. Freaking. Bezos."

Word has it that the wealthiest person on the planet clicked a dodgy WhatsApp link that hacked his phone. The result?

The internet got to see a pic of a very different type of "package" that Jeff had delivered to his girlfriend.

(Suffice to say the old boy was Amazon "Primed".)

Here's the point: Bezos has built a trillion-dollar internet business. Yet even he got hacked.

Right now your kids are swiping at your phone with their grubby, jam-stained fingers, poking around at one of the hundred apps you've downloaded and long forgotten about.

So the question is: are you feeling lucky, punk? I'm not.

And you shouldn't either: according to the Government's Australian Cyber Security Centre, Australians are reporting cybersecurity incidents every 10 minutes – and in 2018 almost one in three Australian adults was affected by cybercrime.

So here are three things that I do to avoid getting hacked.

Dumpster diving

I have a rotary phone, a fax machine, a pager on my belt, and a CB radio in my ute. I'm joking.

(Alright, so I do have the CB in my ute, but that's none of your damn business, Victor Charlie, Charlie).

While you'd think going to the olden days may save you from being hacked, the truth is it's even more dangerous. The easiest way to steal your identity is not to hack into your computer, it's to simply fish through your rubbish bin.

So I do whatever I can to stop receiving snail mail, and instead get everything emailed instead. When I went full digital, I scanned all the old mail I had lying around – and destroyed it. (On the farm we have an incinerator ... but if you're in a more urban setting a $40 shredder from Officeworks is fine.)

Use protection

On all my accounts I've turned on two-factor authentication (Google it). I also use Dashlane to securely store my passwords, Malwarebytes to protect my computer, and TunnelBear as a VPN (to keep web browsing secure). For about $100 a year, it's cheap insurance.

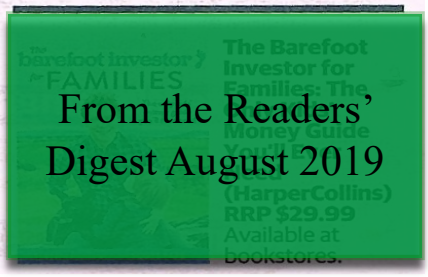
Also, my social media accounts don't give away my location. (Unlike Terry the Tosser: "Here we are in Mykonos #richlife" ... and back in Melbourne your house is getting robbed, #thuglife.)

Stay alert

I have a premium alert service set up on my credit file (and given I have no credit, it shouldn't be dinging too much). However, if you get scammed, your credit file is one of the first places it will show up, as scammers apply for credit in your name.

Here's the deal: You don't have to be mega-rich to be scammed – in this interconnected world, we're all targets. So don't wait for the big hack to come to realise you weren't covered.

Because, as the Amazon founder himself will tell you, there's no returns policy once your junk is on the internet.



From the Readers' Digest August 2019

If you are unfortunate enough to get hacked, believe me, it is a very unpleasant feeling. I know, I was hacked not so long ago despite having all the barriers up. What happened was, a company from whom I had made a purchase several years ago was hacked and their files with all their customers' details on were stolen, including mine.

Now comes the bit our President highlighted last meeting. Yes! you are right — **change your password regularly.** I had not done so and the bas***d used my password to hack into my email account. He downloaded lots of goodies — of course I mean **his** goodies — including a key logger, meaning that if I logged into my bank account, he could see my pass-word.

To cut a long story short, I had free but good security. It managed to find the key logger and killed it. But as our Jim told me, he probably also put in a sleeper key logger as well. If he has, I have not been able to find it yet.

I changed from my free security to BitDefender which is considered to be the top of the range security provider. That, too, has been unable to find anything "yet" — even after a 14 hour in-depth search. Keep Tuned!

LinkedIn's Stories Feature

Short-lived stories on social media have been a grand hit! So naturally, everybody wants to do it. It is quick and easy to create and well, nobody needs to remember what you said last week or the week prior to that. Now that almost every other social media and messaging app is cashing in on the growing popularity of ephemeral stories, it is hardly surprising to see even LinkedIn considering implementing it on its platform.

The idea behind ephemeral stories on apps like Snapchat and Instagram is to be quick, creative and create up to 15-second content that will no longer be visible to your followers after 24 hours (unless you highlight it on your Instagram profile).

LinkedIn is boosting efforts to make inroads into content creation and distribution. Their Editorial division focuses on creating content that is relevant to specific interest groups and is easy to consume.

Effectively, LinkedIn has figured out that content is king and now it wants users to engage with content (created by users or LinkedIn itself) in addition to experimenting with new ways to help users create, distribute, and discover it.

P Davies, Senior Director of Product Management at LinkedIn, put it like this:

> *"Stories first appeared on Snapchat, with other platforms like Instagram and Facebook adopting them soon after. They spread for a good reason: They offer a lightweight, fun way to share an update without it having to be perfect or attached to your profile forever."*

LinkedIn is a professional social networking and job discovery platform. Will LinkedIn Stories, therefore, be a good fit? LinkedIn has already confirmed that it has learned about 'unique' possibilities of LinkedIn Stories in a professional context.

LinkedIn is currently testing LinkedIn Stories internally and will start testing it with users in the coming months. If you have a view about introducing "Stories" , let LikedIn know at *https://gethuman.com/phone-number/LinkedIn/report-new/Other*.

Why not register for

Be Connected

https://beconnected.esafety.gov.au/

Keeping Abusive Trolls at Bay?

Twitter wants to provide users with more control over who can reply to their specific tweets. Twitter is working to implement a new feature that should help users keep abusive trolls at bay.

Twitter Conversation Controls

Twitter is testing "Twitter Conversation Controls", an option that allows users to lock down a specific conversation and decide who is allowed to reply to a particular tweet. Twitter proposes to allow users to choose from certain conversation types, as follows:

- ***Open*** – *Anyone on Twitter can reply to your tweet.*
- ***Community*** – *Anyone you follow and mention can reply to your tweet.*
- ***By invitation*** – *Anyone you mention in the tweet can reply to your tweet.*

This could be a solution for anyone trying to prevent abusive trolls from replying to their tweets or hi-jacking their conversations. As an example, if you select the option "Open", any Twitter user can reply to your tweets.

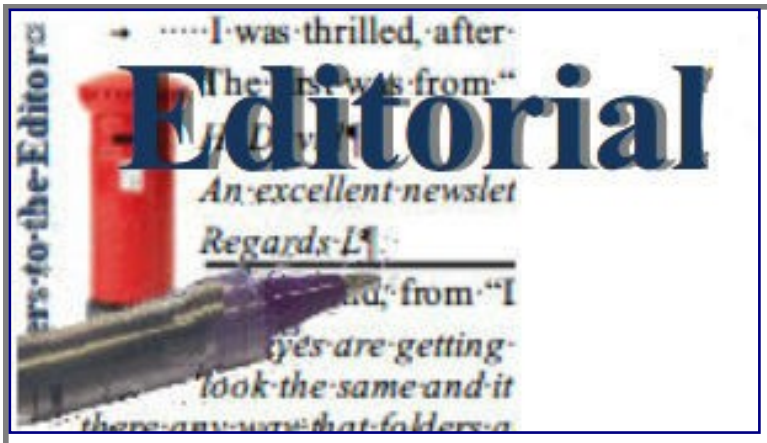
On the other hand, by selecting "Community", only those you follow on Twitter can reply to your tweet. If you mention someone you don't follow, they, too, can reply to your tweets. So, it is recommended that you be careful whom you interact publicly on Twitter.

The last option, "By Invitation" allows only people you mention in the tweet to reply to your tweet.

Last month, Twitter's Suzanne Xie announced that Twitter was planning to provide users with the following set of options:

- ***Global*** – *Anyone can reply to your tweet*
- ***Group*** – *People you follow can reply to your tweet*
- ***Panel*** – *People you mention can reply to your tweet*
- ***Statement*** – *Nobody but you can reply to your tweet*

There is one major difference between LinkedIn's offering and Twitter's shared egg. The latter does not include a control where nobody can reply to your tweet. This feature is currently in progress by Twitter but with no immediate timeline for release. 



In this issue I have added a few articles beyond the usual Windows articles.

For example, there is an article on Twitter's latest offering.

There is also an article relating to LinkedIn's Stories.

As always, I would love to get some feedback from readers whether these alternate features are of interest to you. "Silence may be golden" in certain circumstances, but I would much prefer to hear some **shouting** or even a bit of whispering from readers — anything but 'SILENCE". So, **PLEASE COMMUNICATE!**

As always, an article by our President, Jim Greenfield, is always worth taking note of. His words of wisdom come from many years of practical experience.

I have also included a news paper article relating to "Hacking". This was of particular interest to me as I have been hacked recently. In fact I have been Hacked twice despite taking every precaution. My bank account was hacked in January and my computer more recently. As Jim said at our last meeting **"Change your passwords frequently".** Why not **do it now**!

Jest a Minute

DIVORCE HEARING IN ITALY

This is a true story!

A man and his wife were getting a divorce at a local court in Italy, but the custody of their children posed a problem.

The mother jumped to her feet and protested to the judge that since she had brought the children into this world, she should retain custody of them!

The judge knew the man also wanted custody of his children so he asked him for his side of the story.

After a long moment of silence, the man rose from his chair and replied:

"Your Honour, when I put a coin into a vending machine, and a Coke comes out, does the Coke belong to me or to the machine?

DON'T LAUGH . . . ***HE WON***!

~ Tonight's Topic ~

BACKING UP DEVICES

PRESENTER: LINDSAY CHUCK

— For Your Notes —

Our April Members' Meeting

Online shopping incorporating eBay and Paypal.

This meeting will lead us through the mysterious world of Online shopping incorporating eBay and Paypal. If you have ever - or never - used these facilities, come along and hear this exposé.

MEETING RULES

We are allowed to use the facilities at the Hall at the rear of St Mary's Catholic Church, on the corner of Bains and Main South Roads, Morphett Vale in return for a small fee plus respect for their property. We ask for your co-operation in respect to the above.

Whilst we have no control over what our members do away from our Club meetings, piracy of copyright material cannot be condoned at our meetings. Please respect copyright laws at all times.

IT & COMPUTERS

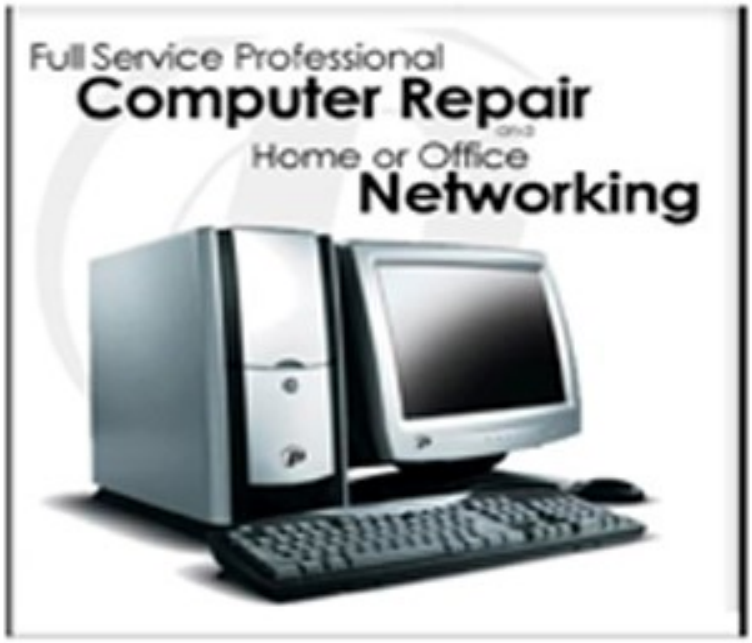
Shop 6, 76 Beach Road
Christies Beach 8186 2736
(Same block as Woolies on Beach Road)
Contact: Jamie or Ash
For all your computing needs
available locally

Need help with your computer?
Looking to purchase a new one?
Need additional peripherals?
Home site visits available !

Looking for excellent customer and after sales service?

New Computers
Repairs
Virus removal
New software & Upgrades

Peripheral units:
Wireless Keyboard Mouse
Sound Boards & Systems
External & Internal Hard Drives



Tell IT & Computers
you are from
S.D.C.U.C.I.

S.D.C.U.C.I can
recommend the
customer service
offered by
IT&Computers