On October 7, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google products.

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN

09 October 2020

In The News This Week

H&M receives €35 million fine for violating the GDPR

The German subsidiary of H&M has received a €35,258,707.95 (about £31.9 million) fine from the Hamburg Data Protection Authority for violating the GDPR (General Data Protection Regulation). The infringement relates to a 2019 data breach that revealed that H&M was gathering excessive personal data on its employees. The fashion retailer had been collecting and storing information about its employees' private lives, including their holiday experiences, family issues, religious beliefs and symptoms of illness and diagnoses. The information was collected during one-to-one conversations between employees and their supervisors as part of a "welcome back talk" when employees took time off work. Some of the data was accessible by up to 50 other managers.
Read the full story here: GRCI Law *(Thank you to my good friend Yazan Shapsugh who pointed me to this story)*

Data from Airlink International UAE leaked on multiple dark web forums

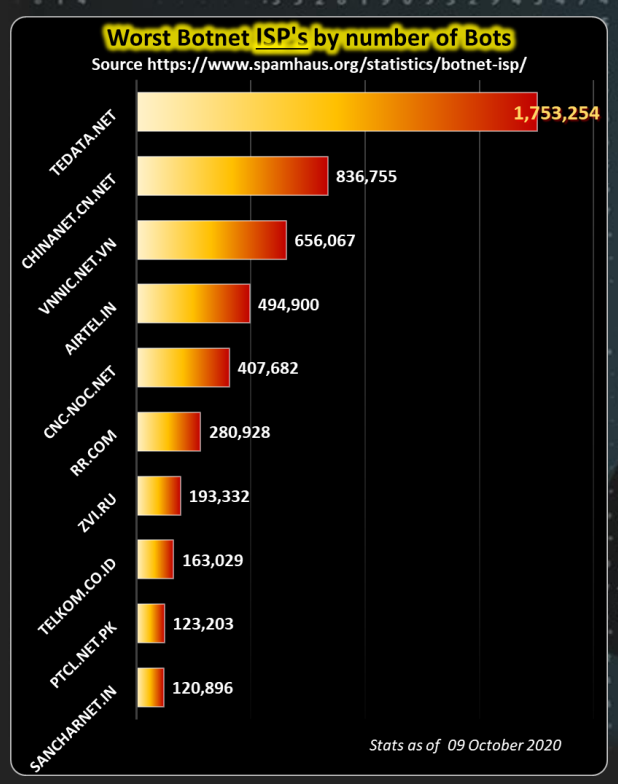
Cybersecurity researchers from Cyble have found a threat actor sharing leaked data of Airlink International UAE for free on two platforms on the dark web. The availability of the data on the dark web could expose organizations to serious risk, threat actors could use this data to carry out multiple malicious attacks. Airlink International U.A.E. is a leading company for any travel and logistics requirements. It has more than 200 employees with around $250 million in revenue. The data leak is the result of a misconfigured server containing 60 directories with approximately 5,000 files each. The data leak was first reported on May 30, 2020, the data have been posted online by the collective KelvinSecTeam. Read the full story by Pierluigi Paganini here: SecurityAffairs

Hackers disguise malware attack as new details on Donald Trump's COVID-19 illness

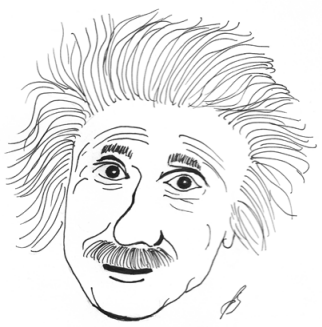
The confirmation that US President Donald Trump has been infected by the Coronavirus, and had to spend time this weekend in hospital, has – understandably – made headlines around the world. And there are plenty of people, on both sides of the political divide, who are interested in learning more about his health status. It's no surprise, therefore, to discover that cybercriminals are exploiting that interest with the intention of infecting users' computers. Hot on the heels of the developing coverage of Donald Trump's hospitalisation and return to the White House, hackers have spammed out emails designed to trick the unwary into clicking on a malicious link by offering more details related to the US President's health. Security researchers at Proofpoint, who last week warned of a malware campaign claiming to come from the Democratic National Committee, posted details on Twitter of the new and active malicious attack they had seen targeting hundreds of US and Canadian organisations."
Read the story by Graham Cluley here: Tripwire

Microsoft cloud outages continue as Office and Outlook customers report problems

Microsoft's cloud services problems are continuing this week with more Azure and Microsoft 365 services issues for some customers. Here's what's happened and why. Last week, a major Azure Active Directory authentication issue affected users worldwide. A follow-up Exchange/Outlook issue later in the week affected European and Indian Office 365/Microsoft 365 customers. This week, Microsoft's cloud services issues are continuing, affecting a number of Exchange, Outlook, Teams and SharePoint users. Microsoft was still warning some Office 365/Microsoft 365 customers as this week kicked off of some possible residual Exchange/Outlook issues, including problems accessing the admin center and syncing issues between Outlook mobile and desktop. I asked Microsoft if these issues were related to last week's Azure Active Directory authentication problems, but was told the company had no comment. On October 7, users, primarily in the U.S., began reporting in the afternoon ET they were having issues accessing their admin center dashboards. Around 2:30 p.m. ET, users took to Twitter and other social channels to report they were unable to access Microsoft 365 services, including Teams, Exchange Online, Outlook.com, SharePoint Online and OneDrive for Business. At the same time, warnings of issues with Azure Active Directory and Azure Networking services popped up on the Azure status page. - Read the story here: ZDNet Article



For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov



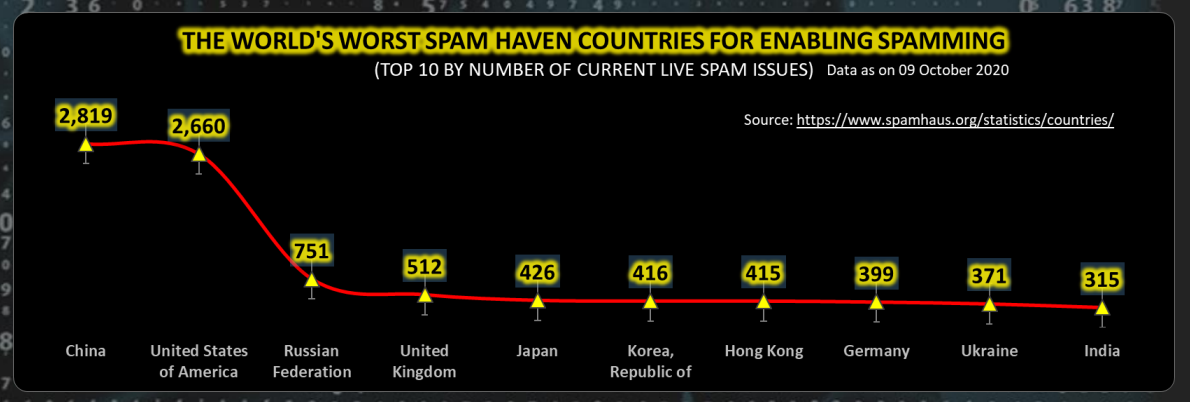
Beware!! There are many crooked Einsteins out there who wants your money! Change your online banking passwords regularly!!

Malware infected Apps removed from Play Store & App Store

Following on the last two week's phone hacking articles, recent news also highlighted the fact that not all apps on the various app stores can be fully trusted. Although the vetting process on Google's Play, Apple's App Stores and others are very thorough, perpetrators are constantly trying to find loopholes and weaknesses in the process they can exploit. Many apps that slips through the cracks are not necessarily obvious malware but are subtlety circumventing the rules on privacy and are collecting and sharing private information on individual users they shouldn't. Thanks to security research centres and the various bounty hunting schemes, researchers are constantly exposing these offending apps and the app store owners are quick to respond and remove them from their stores. This is where you as the user come in though, these apps that are removed from the various app stores are not automatically removed from your phone, and for good reason. The app store owners like Apple and Google don't have legal jurisdiction on your phone, they can't just remove stuff even if they can and the same goes for the phone manufacturers. **You need to remove these apps from your phone yourself**. The problem is how do you know if an app is dodgy? There is generally no warning message that pops up when you open the app or if you look at your purchased apps on the app store, there is no indication that the app is bad. You should also know that there is a difference between apps that were banned and apps that are infected or malicious. In recent weeks we saw in the media that many apps were banned by various governments for political and other reasons and these apps were removed by the app store owners from the regional sores to comply with the local laws. Infected apps are a different story though, and these are the ones we are talking about here. Once an app is proven malicious or infected, the various app store owners will remove them from the store and generally make a media statement to this effect. However, I couldn't find a single or specific source where you can see which malicious apps were removed from the various app stores in the past that might still dwell on your phone. (If anyone know of a site, please let me know). In general, just keep an eye on your local news and social media sources or from time to time (like I do) scan the internet and search for phrases like "apps removed from google play store" or "apps removed from Apple Appstore", "apps removed from Microsoft store", or search for apps removed from whatever app store you are using.

Below is a list of apps recently removed from Google Play Store and also some older ones removed from the Apple App Store.

Android apps infected with "Joker" malware	Apple App Store - Removed 2019
All Good PDF Scanner	RTO Vehicle Information
Mint Leaf Message-Your Private Message	EMI Calculator & Loan Planner
Unique Keyboard – Fancy Fonts & Free Emoticons	File Manager – Documents
Tangram App Lock	Smart GPS Speedometer
Direct Messenger	CrickOne – Live Cricket Scores
Private SMS	Daily Fitness – Yoga Poses
One Sentence Translator – Multifunctional Translator	FM Radio – Internet Radio
Style Photo Collage	My Train Info – IRCTC & PNR (not listed under developer profile)
Meticulous Scanner	Around Me Place Finder
Desire Translate	Easy Contacts Backup Manager
Talent Photo Editor – Blur focus	Restaurant Finder – Find Food
Care Message	BMI Calculator – BMR Calc
Part Message	Dual Accounts
Paper Doc Scanner	Video Editor – Mute Video
Blue Scanner	Islamic World – Qibla
Hummingbird PDF Converter – Photo to PDF	Smart Video Compressor
Convenient Scanner 2	
Emoji Wallpaper	
Fingertip GameBox	
Push Message- Texting & SMS	
Safety AppLock	
Separate Doc Scanner	
com.cheery.message.sendsms (two different instances)	
com.contact.withme.texts	
com.file.recovefiles	
com.hmvoice.friendsms	
com.imagecompress.android	
com.LPlocker.lockapps	
com.peason.lovinglovemessage	
com.relax.relaxation.androidsms	
com.remindme.alram	
com.training.memorygame	



Author: Chris Bester (CISA,CISM)
chris.bester@yahoo.com