On March 18, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Adobe 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

20 March 2020

In The News This Week

Internet's largest social networks issue joint statement on COVID-19 misinformation

On the 17th of Marche 2020, Facebook, Google, LinkedIn, Microsoft, Reddit, Twitter, and YouTube put out joint statement promising to fight COVID-19 fraud and curb misinformation. - The internet's largest social networks have issued a joint statement on the coronavirus COVID-19 outbreak, promising to fight fraud and curb misinformation shared on their platforms. Signatories include Facebook, Google, LinkedIn, Microsoft, Reddit, Twitter, and YouTube. The joint statement comes after multiple US tech companies attended a teleconference last week with White House officials. During the teleconference, which allegedly lasted for more than two hours, US government officials asked US tech companies to help stop the spread of coronavirus conspiracy theories online, among other things. In their joint statement, the seven social networks said they are now coordinating and working together with each other and government healthcare agencies across the world on tackling COVID-19-related misinformation. "We're helping millions of people stay connected while also jointly combating fraud and misinformation about the virus, elevating authoritative content on our platforms, and sharing critical updates in coordination with government healthcare agencies around the world," the companies said. The joint statement doesn't go into detail on how the companies will be handling COVID-19 fraud and misinformation; however, it comes to quench criticism about misleading coronavirus content that has recently surfaced on some of their platforms.
Read the full story by Catalin Cimpanu here: ZDNet Article(1)

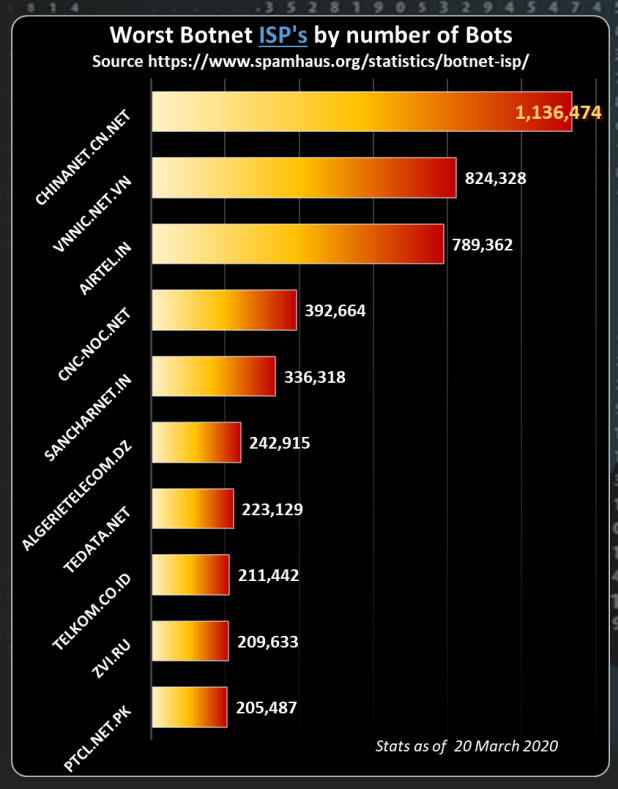
United Kingdom - Rights Group: APP Bank Fraud Cost Consumers £1bn

Financial institutions could have prevented hundreds of millions of pounds worth of fraud over the past three years by implementing a simple payee-checking service online, a consumer rights group has claimed. The Which? Group estimates that £1.1 billion has been lost to bank transfer fraud since 2017. In these cases, a scammer posing as a trusted entity tricks the victim to transfer money to a bank account under their control — known as "authorized push payment" (APP) fraud. Because the victim has technically initiated the payment, up until recently they have had no way to claim these funds back. However, things are changing: most UK bank users now receive a warning notice when making payments online, reminding them to check the details of any payee. This is to be followed by a new Confirmation of Payee (CoP) initiative, whereby customers will receive a pop-up warning if the name of the payee doesn't match the bank account details entered by the customer. However, Which? Group is frustrated by the glacial pace of its implementation, with the system originally meant to go live in July 2019. It is now slated for March 31, 2020, but not all lenders will be forced to implement it. "Only the six largest banking groups are being forced to sign up to CoP and there is even a chance that some won't meet the new deadline," it said. Read the full story here: InfoSec

News snippets from the past - Computer crime

What make a hacker worlds's most wanted? - 1996

The following news snippet was published in The Daily Courier - Jan 29, 1996 – *"The Associated Press – The hero was Tsutomu Shimomura, a cool, brilliant scientist who brought an evil hacker to justice as a matter of honor, and whose good looks and flowing mane had woman scouring the internet for his e-mail address. The villain was Kevin David Mitnick, a dangerous, anti-social computer wizard, a thief who stole 20,000 credit card numbers, who legend has it broke into the North American Air Defence Command computers as a teen and later wreaked millions of dollars in damage on corporate computer networks. The day after his arrest in connection with a daring and mysterious Christmas Day 1994 break-in on Shimomura's computer, Mitnick's bloated , sullen face peered out from newspapers across the country – the uber-hacker in custody."* Read more here: GoogleArchives



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

Simple Cyber Security Awareness tips when working from home or from another remote location

It's been a while since we spoke about general cyber security awareness, and since many of us are forced to work from home during the Corona Virus pandemic, I believe it is a good time to refresh our memories and go over the basics once more.

We must take heed of the fact that our home network is probably not as secure as your corporate network and that you have to take the basic precautions when you work remotely. As we reported in last week's newsletter, the criminal element in our various societies swooped down on the opportunity to use the emotional response and misinformation spread through social media and other sources as a launchpad for criminal activities. Therefore, we have to be vigilant in our approach to secure our environment and be informed and aware of the threats we are facing. Below is some point the take in consideration.

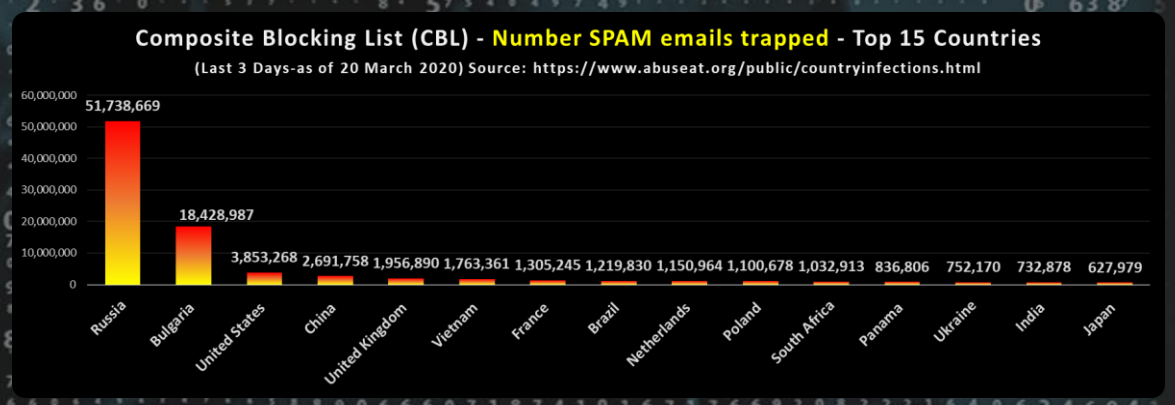
1. Be Informed – make sure you do not succumb to the social media frenzy and unconfirmed statements and opinions by doing the following.
   a) Trust the information shared by your company or organisation if any, they would have done their homework before they send out a corporate communique.
   b) Make sure the links that you receive from friends, or other means, are legitimate. The general rule is, if you are not sure, don't open it. (We've seen last week how the Johns Hopkins Corona Dashboard were duplicated but with malicious elements imbedded). I'll list a few legitimate links at the end of this article.
2. Phishing Emails – since the middle of January, phishing emails with a Corona undertone soared and many already fell victim to it. Below are a few tips:
   a) Never respond to requests for personal information via email. Businesses will never ask for personal information in an email.
   b) Do not enter personal information in a pop-up screen when you are browsing, ever.
   c) Do not click on any links listed in an e-mail message. Copy and paste the URL into your browser and if it looks strange or phishy don't open it. Remember if it is important enough, people will eventually phone you.
   d) Many mail engines nowadays have an option to report bad mails, in Google or Yahoo, you can mark phishy emails as spam. In outlook, use the "report' function to mark it as a phish if the function is enabled. The service providers analyse this data and it is more likely that the real phishes will be blocked.
   e) Make sure your anti-malware software is up to date.
3. Use a VPN (Virtual Private Network) connection to your office environment – If you work in an corporate environment, it is highly likely that they will have a VPN facility, if you don't have it or don't know what it is, ask your local IT department and have it set up.
4. Lock it when you leave – Remember, you are working from home or a remote location, make sure that passers by or family members don't see what they are not supposed to see.
   a) It takes only a few seconds to secure your computer and help protect it from unauthorized access. Lock down your computer every time you leave your computer, simply press the windows button …. and the letter "L"
   b) Set up a screensaver that will lock your computer after a pre-set amount of idle-time time and require a password to log back in. If it is a corporate machine this is probably already enforced.
   c) If your computer is used by more than one person, create individual accounts, with unique login and passwords for each Choose a strong password. A good password should always include upper and lowercase letters, numbers, and at least one special character.
   d) Do not set the option that allows a computer to remember any password. Use a passphrase to make it easier to remember.

Below is some valid links you can explore to get more information:

a. Johns Hopkins Corona Dashboard
b. Stay Safe Online
c. FCC Smartphone security checklist
d. Protect your privacy on the internet (Microsoft)
e. Trust me, I'm Certified – GIAC Podcast (33 mins)

Some fun and interesting links:

a. See all the aeroplanes in the sky at this very moment
b. See all marine traffic in the water at this moment



AUTHOR: CHRIS BESTER (CISA,CISM)
chris.bester@yahoo.com