On March 25, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google and Microsoft 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

27 March 2020

In The News This Week

The news this week was once again dominated by criminals taking advantage of the COVID-19 pandemic, prying on the general fear, ignorance and paranoia of people worldwide. I urge you to be vigilant and treat any email, blog, news or social media clip focusing on the pandemic with care. Many of these mails and messages are carefully crafted by perpetrators and are sometimes masquerading as official communication from authorities. Be careful, don't get caught! - With this in mind, the news clips of the week will focus on other cyber security events that are somehow overshadowed by the COVID-19 pandemic.

FBI Takes Down a Russian-Based Hacker Platform, DEER.IO

A Russian-based cyber platform known as DEER.IO was shut down by the FBI on Tuesday the 24th, and its suspected administrator – alleged Russian hacker Kirill Victorovich Firsov - was arrested and charged with crimes related to the hacking of U.S. companies for customers' personal information. DEER.IO was a Russian-based cyber platform that allowed criminals to purchase access to cyber storefronts on the platform and sell their criminal products or services. DEER.IO started operations as of at least October 2013 and claimed to have over 24,000 active shops with sales exceeding $17 million. The platform was shut down pursuant to a seizure order issued by the Southern District of California Court.
Read the full story here: Attorneys' Office, Southern District of California

Chubb Cyber Insurer Allegedly Hit By Maze Ransomware Attack

Thursday, 26 March 2020 - Cyber insurer giant Chubb is allegedly the latest ransomware victim according to the operators of the Maze Ransomware who claim to have encrypted the company in March 2020. Chubb is one of the leading insurance carriers in the world with an extensive line of cyber insurance products that include incident response, forensics, legal teams, and even public relations. Ransomware is not unknown to Chubb, as in their 2019 Cyber InFocus Report Chubb explains that malware-related claims have risen by 18% in 2019, with ransomware being responsible for 40% of manufacturer's cyber claims and 23% of cyber claims for smaller businesses. In a new entry on their Maze 'News' site, the ransomware operators claim to have encrypted devices on Chubb's network in March, 2020. Read the full story by Lawrence Abrams here: BleepingComputer

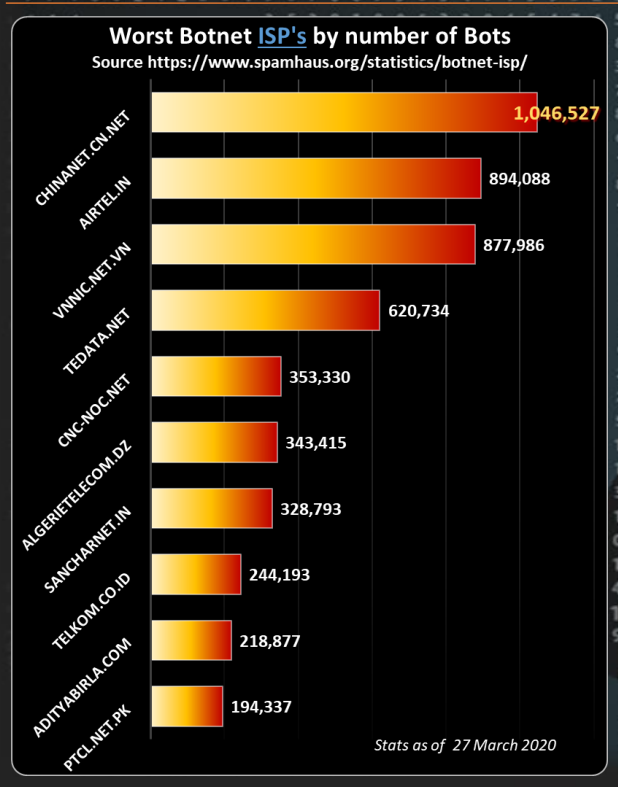
Germany - TrickBot now pushes Android app for bypassing 2FA on banking accounts

The operators of the TrickBot banking malware have developed an Android app that can bypass some of the two-factor authentication (2FA) solutions employed by banks. This Android app, which security researchers from IBM have named TrickMo, works by intercepting one-time (OTP) codes banks send to users via SMS or push notifications. TrickMo collects and then sends the codes to the TrickBot gang's backend servers, allowing the crooks to bypass logins or authorize fraudulent transactions. Read the full story by Lawrence Abrams here: ZDNet

News snippets from the past - Computer crime

Milwaukee hackers fit a computer bandit mold? - 1983

The following news snippet by Colin Covert was published in the Boca Raton News- Sept 6, 1983 – *"The computer raiders weren't whiz kids. They were Explorer Scouts. The seven technological guerrillas who played "War Games" with more than 50 computers are simply bright adolescents with time on their hands, their parents and lawyers insist. The group, who dubbed themselves "the 414s," after Milwaukee's are code, range in age from 16 to 22. Over a period of at least a year, they tampered with programs and read sensitive files in major computer installations across the country. Among the systems they entered were those of the atomic weapons research lab of Los Alamos Nuclear Facility, Manhattan's Memorial Sloan-Kettering Cancer center, Pacific Security Bank ....."*
Read the full story and more here: GoogleArchives



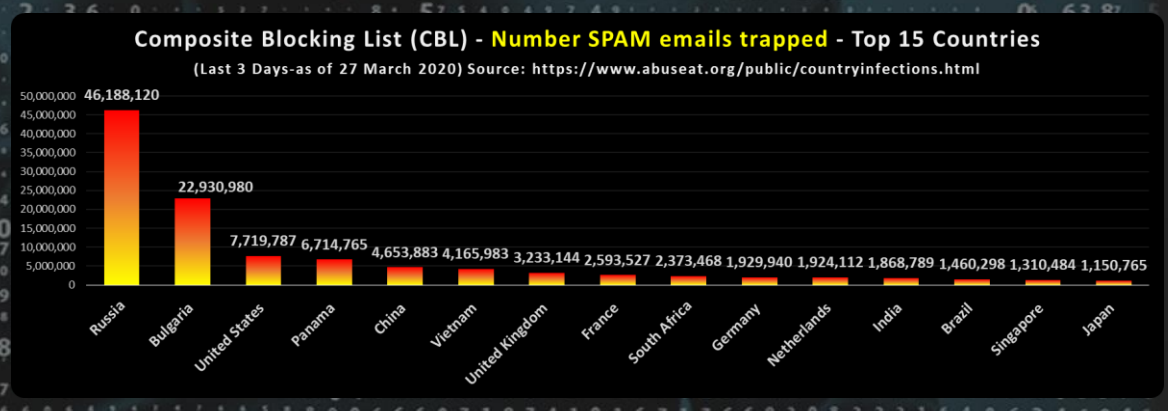
For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

Quarantine work attire

Apps of concern for Parents

The Corona virus pandemic threw most of our lives in disarray as schools are closing down , quarantine measures and national lockdown decrees are issued, forcing many people across the globe to stay at home or confined in other areas. Parents are finding themselves in unfamiliar territory as all of a sudden, the family are under one roof 24x7. Other than home-school households (where this is the norm), parents are challenged to come up with creative ways to keep their children busy and for many parents, allowing more screen-time is an easy out. Online screen-time is already a control challenge as it is. In this light, I want to highlight some apps that are generally good but come with concerns in how the kids interact with them that parents needs to bear in mind. Although there are ways and means to monitor what your kids do online, this is more meant to be a way to educate yourselves so that you in turn can convey the online dangers to your kids. Below we discuss just a few of these apps that you can find on the Family Education website which is one of many resources you can explore. I urge all off you to get familiar with apps your kids are frequenting and educate them of the dangers that lurk online.

1. **TikTok** - **Purpose**: TikTok is an app for creating and sharing short videos. Users can create short music videos of 3 to 15 seconds and short looping videos of 3 to 60 seconds. It encourages users to express themselves creatively through video. Special effects can be added to the videos.
   Why Parents Should Be Worried: Thirteen is the minimum age, but there isn't a real way to validate age so anyone can download the app. Also, parents express concern that there is a lot of inappropriate language in the videos so it's not appropriate for young children. Lastly, by default, all accounts are set to public so strangers can contact your children. For more information on TikTok, check out our Complete Parent's Guide to TikTok.
2. **YouTube** - **Purpose**: YouTube is a place to house and share your videos. You can control privacy settings. It's also a great resource for educational videos and entertainment.
   Why Parents Should Worry: Inappropriate content has been sliced into both all-ages content and children's content. Also, comments on videos can be extremely inappropriate and hurtful. YouTube also has a known paedophile problem which is major cause for concern.
3. **Tellonym** - **Purpose:** This is an anonymous messenger app. It calls itself "the most honest place on the internet." This app is extremely popular in middle schools and high schools and it allows kids to ask and answer questions anonymously.
   Why Parents Should Worry: It is a regular occurrence to see cyber bullying, violent threats, and sexual content. It also offers unmonitored access to the internet. The age restrictions are inconsistent ranging from 12 to 16, but this app is inappropriate for anyone younger than being in their late teens.
4. **Bigo Live** - **Purpose**: Bigo is a live streaming app. It is rated for teens 17 and up. Users can vlog about their lives, live stream video game play, and host their own shows.
   Why Parents Should Worry: There is no age verification and users have to provide personal info like their age and location. This is a place where bullying, nudity, violence, and profanity is common.
5. **IMVU** - **Purpose**: This is a virtual world game like SIMS. Users interact with each other as avatars. IMVU stands for Instant Messaging Virtual Universe.
   Why Parents Should Worry: There is nudity and sexual encounters in areas that are for 18+, but there is sexual talk and behaviours in the regular area of IMVU as well. There is a Chat Now feature that randomly pairs users with other users and can lead to inappropriate pairings and interactions. All profiles are public, and there can be bullying and predators trying to get other users to share their phone numbers and to send pictures.
6. **Houseparty**: - **Purpose:** Houseparty is a video chatting app that's pretty open. Friends can communicate with each other through live video and texts in chat groups.
   Why Parents Should Be Worried: There's no screening and the video is live, so there's nothing to keep kids from inappropriate content. Users can send links via chat and even take screenshots. There's also nothing keeping friends of friends joining groups where they may only know one person.
7. **Ask.fm** - **Purpose**: This app allows users to interact in a question-and-answer format — with friends, peers, and anonymous users alike.
   Why Parents Should Worry: The app is rated ages 13+ and is most popular in Europe but is catching on in the U.S. Some kids have used the app for hurtful cyberbullying that has been linked to suicides, including the death of 12-year-old Rebecca Sedwick of Florida. British schools have sent home letters calling for students to stop using ask.fm because of its use in several cyberbullying incidents there, and its loose regulation and lack of monitoring. In response to the uproar in the U.K., the site added a button where users can report abuse, but some parents feel it's too little, too late. Check out Webwise's Ask.fm Guide for Parents and Teachers.



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