On December 2, the Cyber Threat Alert Level was evaluated and being lowered to Green (Low). Organizations and users are advised to update and apply all appropriate vendor security patches to vulnerable systems and to continue to update their antivirus signatures daily.
(First Green flag in a very long time)

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
04 December 2020

In The News This Week

South Africa - Absa data leak: Details emerge of how rogue employee sold client data

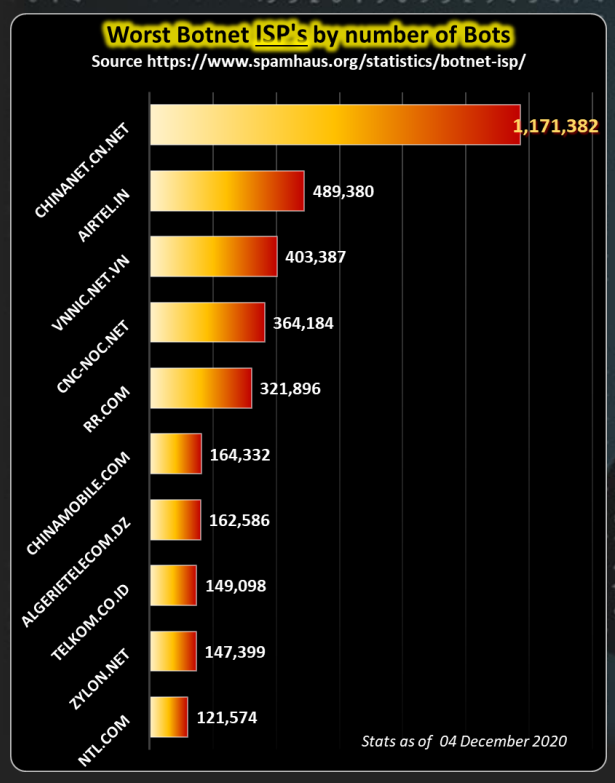
An Absa Bank employee accused of leaking some of the bank's South African customer data to third parties provided the information, which included client ID numbers, bank account numbers, credit card numbers and mobile phone numbers, to several third parties in return for payment. Respond to questions from TechCentral on Tuesday, the bank said the information shared specifically does not include passwords or Pin codes. However, Absa said it is worried fraudsters could still try and take advantage of the situation. Absa said in a statement on Monday evening that the employee — whom it has not named — "unlawfully made selected customer data available to a small number of external parties". It has laid criminal charges against the employee. "The leaked data relates to a small portion of Absa South Africa's customer base, although investigations continue."
When it discovered the contravention, the bank secured high court orders allowing search-and-seizure operations at various premises and secured "all devices" containing the leaked data.
Read the full story by Duncan Mcleod here: TechCentral

Ransomware gang says they stole 2 million credit cards from E-Land

Clop ransomware is claiming to have stolen 2 million credit cards from E-Land Retail over a one-year period ending with last months ransomware attack. E-Land Retail, a subsidiary of E-Land Global, operates numerous retail clothing stores, including New Core and NC Department Store. Last month, E-Land Retail had to shut down 23 NC Department Store and New Core locations after suffering a CLOP ransomware attack. At the time of the attack, E-Land Retail stated that sensitive customer data was safe as it was encrypted on another server. "Although this ransomware attack caused some damage to the company's network and system, Customer information and sensitive data are encrypted on a separate server." "It is in a safe state because it is managed," E-Land Retail CEO Chang-Hyun Seok disclosed in a notice on their web site. However, in an interview with BleepingComputer, the CLOP ransomware operators claimed to have breached E-Land over a year ago and have been quietly stealing credit cards using POS malware installed on the network. "Over a year ago, we hacked their network, everything is as usual. We thought what to do, installed POS malware and left it for a year. Before the lock, the cards were collected and deciphered, for a whole year the company did not suspect and did nothing," the CLOP gang told BleepingComputer. Using the installed POS malware, CLOP told BleepingComputer that they stole the Track 2 data for 2 million credit cards over the past year. POS malware is used to scan the memory of point-of-sale (POS) terminals as credit card transactions occur and transmits it back to the threat actor's server.
Read the full story here: BleepingComputer

8% of all Google Play apps vulnerable to old security bug

Developers have not updated a crucial library inside their apps, leaving users exposed to dangerous attacks. Some of the vulnerable apps include Microsoft's Edge browser, Grindr, OKCupid, and Cisco Teams. Around 8% of Android apps available on the official Google Play Store are vulnerable to a security flaw in a popular Android library, according to a scan performed this fall by security firm Check Point. The security flaw resides in older versions of Play Core, a Java library provided by Google that developers can embed inside their apps to interact with the official Play Store portal. The Play Core library is very popular as it can be used by app developers to download and install updates hosted on the Play Store, modules, language packs, or even other apps. Earlier this year, security researchers from Oversecured discovered a major vulnerability (CVE-2020-8913) in the Play Core library that a malicious app installed on a user's device could have abused to inject rogue code inside other apps and steal sensitive data — such as passwords, photos, 2FA codes, and more. Google patched the bug in Play Core 1.7.2, released in March, but according to new findings published today by Check Point, not all developers have updated the Play Core library that ships with their apps, leaving their users exposed to easy data pilfering attacks from rogue apps installed on their devices. Read the full story here (Including a partial list of affected apps): ZDNet



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

ONLINE SAFETY TIPS FOR SENIORS

The National Cyber Security Alliance has a number of excellent security resources that can help you to be safe online. Today I want to share a tip sheet that will be specifically helpful in the upcoming festive season as fraudsters are targeting our senior citizens. Please download or read the original tip sheets from the National Cyber Security Alliance resource pages and pass it on to the senior citizen circles you are exposed to.

Being online lets you stay abreast of current events, connect with friends and family, shop, manage your finances, play games, and anything else you can think of. Just as you fasten your seat belt before driving, take precautions before using the Internet to be sure you are safe and secure.

PERSONAL INFORMATION IS LIKE MONEY. VALUE IT. PROTECT IT.

KNOW THE RED FLAGS - To begin with, if anyone contacts you and insists on payment by a wire transfer or gift card, it's a scam. End the conversation immediately.

VERIFY TO CLARIFY - Be suspicious of emails, text messages, or phone calls that create a sense of urgency and require you to respond to a crisis or give sensitive information, such as your credit card number or bank account information. Don't respond immediately. Hang up or walk away from the computer and contact a trusted source to verify the legitimacy of the request.

WHEN IN DOUBT, THROW IT OUT - Links in email, tweets, texts, posts, social media messages and online advertising are the easiest way for cyber criminals to get your sensitive information. Be wary of clicking on links or downloading anything that comes from a stranger or that you were not expecting.

KEEP A CLEAN MACHINE - Keep all software on all internet connected devices current. These updates not only improve the security of your device, but also improve its functionality. Stop clicking postpone on that update. Pro Tip: Configure your devices to automatically update or to notify you when an update is available.

LOCK YOUR DEVICES - You lock the front door to your house, and you should do the same with your devices. Require a passcode to unlock your phone or tablet. Securing your devices keeps prying eyes out and can help protect your information in case your devices are lost or stolen.

MAKE A LONG, UNIQUE PASSPHRASE - Length trumps complexity. A strong passphrase is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember.
(for example, "IL0veCountryMusic!."). Everyone can forget a password. Keep a list that's stored in a safe, secure place away from your computer.

OWN YOUR ONLINE PRESENCE - Every time you sign up for a new account, download a new app, or get a new device, immediately configure the privacy and security settings to your comfort level for information sharing. Regularly check these settings (at least once a year) to make sure they are still configured to your comfort.

SHARE WITH CARE - Be cautious about how much personal information you provide on social networking sites. The more information you post, the easier it may be for a hacker or someone else to use that information to steal your identity, access your data or commit other crimes such as stalking. Just because a website asks you for your address, photo, or mother's maiden name, doesn't mean you actually have to answer honestly.

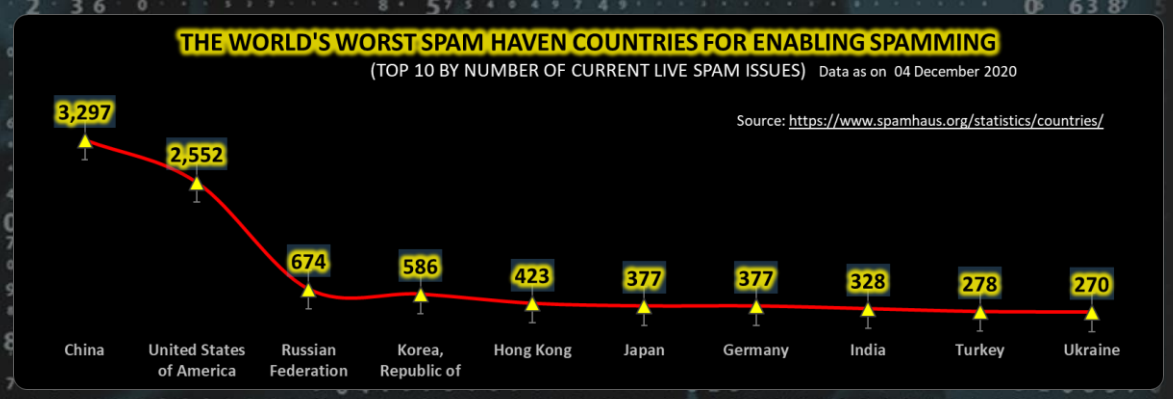
PEOPLE AREN'T ALWAYS WHO THEY SAY THEY ARE ONLINE - Adults of all ages need to be wary of strangers and those appearing to be your friends or loved ones online. It is too easy for criminals to hide their true identity and appear trustworthy. If someone asks to be your friend on a social media platform, only accept their request if you know them. If someone online asks you for money or sensitive information, pick up the phone and call a trusted number. Dating online? Don't send money or sensitive financial or personal information to anyone you have never met.

GIVE AND TEACH

Purchasing an Internet-connected device for a loved one? Don't assume they know how to use it securely. Take a moment to teach recipients how to configure privacy settings, how to deactivate any unnecessary features, and how to use the device responsibly and securely. Don't let your loved ones learn the hard way. If you give them the gift, own your role in helping them understand how to use it securely.

PASS IT ON

The FTC has found that older adults are more likely than younger consumers to report losing money on tech support scams, prize, sweepstakes & lottery scams, and family & friend impersonation. To learn more about these scams so you can educate yourself and those you love, visit: www.ftc.gov/passiton



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