On June 17, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in IBM and 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

19 June 2020

In The News This Week

South African bank to replace 12m cards after employees stole master key

Postbank, the banking division of South Africa's Post Office, has lost more than $3.2 million from fraudulent transactions and will now have to replace more than 12 million cards for its customers after employees printed and then stole its master key. The Sunday Times of South Africa, the local news outlet that broke the story, said the incident took place in December 2018 when someone printed the bank's master key on a piece of paper at its old data center in the city of Pretoria. The bank suspects that employees are behind the breach, the news publication said, citing an internal security audit they obtained from a source in the bank. The master key is a 36-digit code (encryption key) that allows its holder to decrypt the bank's operations and even access and modify banking systems. It is also used to generate keys for customer cards. The internal report said that between March and December 2019, the rogue employees used the master key to access accounts and make more than 25,000 fraudulent transactions, stealing more than $3.2 million (56 million rand) from customer balances. Following the discovery of the breach, Postbank will now have to replace all customer cards that have been generated with the master key, an operation the bank suspects it would cost it more than one billion Rands (More or less $58 million).
Read the full story by Catalin Cimpanu here: ZDNet Article *(Thanks to Yazan Shapsugh who shared the news)*

Australian PM says nation under serious state-run 'cyber attack' – Microsoft, Citrix, Telerik UI bugs 'exploited'

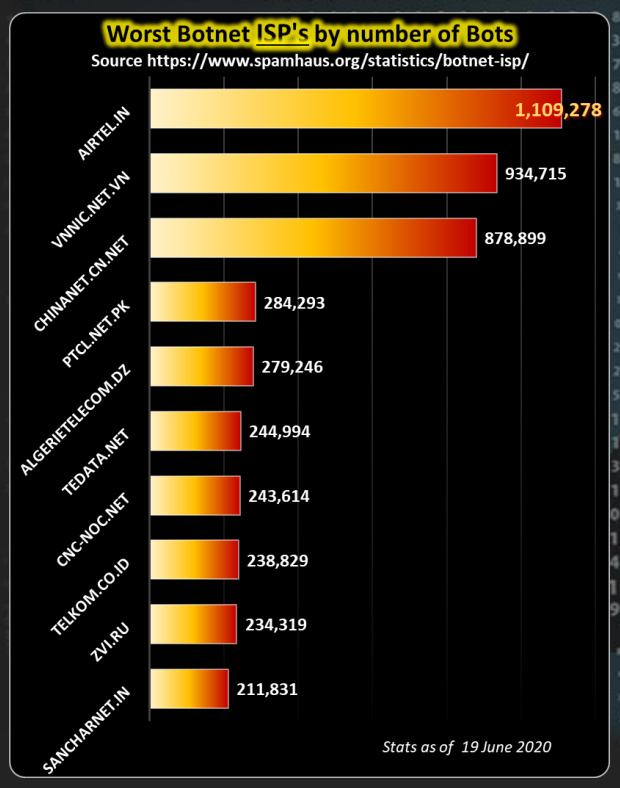
- Australian Prime Minister Scott Morrison has called a snap press conference to reveal that the nation is under cyber-attack by a state-based actor, but the nation's infosec advice agency says that while the attacker has gained access to some systems it has not conducted "any disruptive or destructive activities within victim environments." Morrison said the attack has targeted government, key infrastructure and the private sector, and was sufficiently serious that he took the courteous-in-a-crisis, but not-compulsory step, of informing the leader of the opposition about the incident. He also said that the primary purpose of the snap press conference was to inform and educate Australians about the incident. But Morrison declined to state whether Australian defence agencies have identified the source of the attack and said evidence gathered to date does not meet the government's threshold of certainty to name the attacker.. Read the full article here: The Register

AWS stops largest DDoS attack ever

Amazon has revealed that its AWS Shield service was able to mitigate the largest DDoS attack ever recorded at 2.3 Tbps back in February of this year. The company's new AWS Shield Threat Landscape report provided details on this attack and others mitigated by its AWS Shield protection service. While the report did not identify the AWS customer targeted in the DDoS attack, it did say that the attack itself was carried out using hijacked CLDAP (Connection-less Lightweight Directory Access Protocol) web servers and lasted for three days.
Read the full article here: Techradar

Zoom relents and agrees to give "free" users end-to-end encryption

When video conferencing company Zoom acquired Keybase, there was a great deal of excitement about the impending arrival of the much-needed end-to-end encryption. But then there was disappointment when it was announced that only paying customers would be granted access to the extra security feature. Zoom CEO Eric S Yuan said at the time that **free** customers were not getting end-to-end encryption "in case some people use Zoom for a bad purpose" -- something many users found insulting. But now the company has backtracked, announcing that users of free accounts will in fact get end-to-end encryption... but there is a slight catch. In a blog post Yuan goes on to explain that this means end-to-end encryption will be offered to everyone as an add-on. So what's the catch? Yuan explains: To make this possible, Free/Basic users seeking access to E2EE will participate in a one-time process that will prompt the user for additional pieces of information, such as verifying a phone number via a text message. Many leading companies perform similar steps on account creation to reduce the mass creation of abusive accounts..
Read the full story here: BetaNews



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

Comparison - popular mobile payment apps and associated security considerations.

PayPal – PayPal has been around since 1998 and is probably one of the oldest and most popular payment apps with close to 300 million active accounts. PayPal's owners claim that it is safe for both buyers and sellers if they follow the appropriate security protocols like using two-factor verification and take advantage of other security measures they offer to its account holders. The company states on its web site, "When you send a payment using PayPal, the recipient won't receive sensitive financial information like your credit card or bank account number". This is all good and well, but it begs the question though, why security measures like two factor authentication (2FA) are an option and not a mandatory default security setting. If you do use 2FA though and you lose your phone, the process of getting back in is painful according to users comments on Trustpilot. PayPal's website is secure and encrypted as it uses HTTPS but be wary of fake and lookalike PayPal sites that aren't. In February 2020 security experts discovered a hackable flaw in PayPal's systems that can potentially bypass the authentication process. There was no evidence that the flaw was exploited though. Available on most mobile platforms.

TransferWise – TransferWise is well suited for those who conduct a high volume of international transactions. It offers a "borderless account" that comes with a debit card and the transactions are generally less than PayPal but still not cheap. Following the regulatory requirements, TransferWise customers' funds are held in segregated accounts, apart from the company's own capital. The customers' personal account data is stored in secured servers and safeguarded by a 2-step (2FA) login and verification procedure. The company has not suffered any significant hacks or data breaches and has close to 8 million account holders. Available on iOS and Android.

Google Pay – With more than 1.5 billion Gmail account holders, Google Pay is becoming more and more a payment method of choice. This service is a fast, simple way to pay on websites, in apps, and in-store using cards registered on the individual's Google account. Google are making this payment option attractive to businesses by enabling them to deliver special mobile based offers, gift cards and more. The payment solution is mostly free for customers and businesses as there is no charge for bank transfers and debit card transactions and less than 3 percent transaction fees on credit card transactions. From a security perspective, payment information is always encrypted and Google keeps all payment information on secure servers. User's full card details are never stored on the user's phone or shared with merchants. Merchants are only provided with a virtual account number during transactions. You have to set up security on your smartphone to use Google Pay. You have to have your phone set to lock automatically or the Google Pay won't work. If the lock is turned off, your account numbers are removed from Google Pay. Ensuring your phone is locked helps protect someone from gaining access to your phone and stealing your numbers. I couldn't find any security comparison between this method and 2FA though, so I'm still a bit sceptical. Available on iOS and Android.

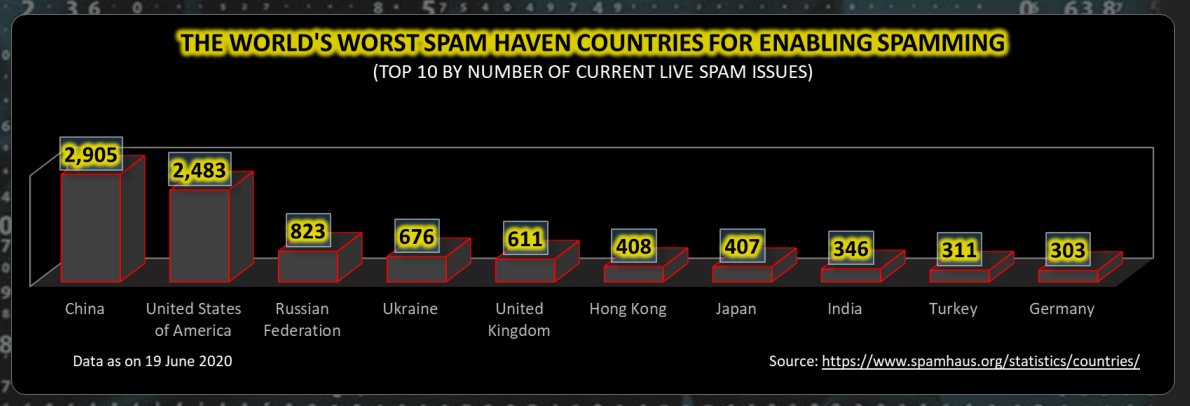
Stripe – Stripe is a popular alternative to PayPal, particularly for online businesses as they offer a simple API (application program interface) that allows them to easily integrate this payment method into their digital business platforms. Transaction fees however are the same as PayPal which are not the cheapest. Payments can be accepted from all over the world and Stripe will deposit your money directly into your bank account. Stripe is rated as a Level 1 PCI Service Provider which is the highest grade of payment processing security. Stripe supports two 2FA authentication methods namely, Text Messaging (SMS) authentication and Mobile Apps authentication. As in the case of PayPal though, enabling it is an option and not a mandatory security feature. Available on iOS and Android.

Amazon Pay – Amazon Pay was launched in 2007 and is a subsidiary of the huge Amazon organisation. Amazon has more than 320 million account holders and with almost 200 million visits to the Amazon website per month, it is no wonder that they have their own payment method. Amazon users can simply log into their accounts, use their saved payment details, and check out using the interface they already know. Amazon Pay is available on most mobile devices and can be used on Amazon.com or on third-party websites wherever Amazon Pay is accepted. They have an extensive fraud protection capability and are trusted by many. Amazon Pay offers 2FA authentication as an option and not as a mandatory security feature. On the backend though, Amazon has one of the most sophisticated and secure computing infrastructures in the world and as the news of this week shows, able to withstand immense targeted attacks.

Apple Pay - Apple Pay uses the near-field communication (NFC) chips embedded in your iPhone and Apple Watch to pay for goods and services by holding the device near a card reader, as you would a contactless debit card. You can also use Apple Pay to make single touch purchases within apps that support the feature. As a payment method, it's main limitation is its availability to apple account holders only meaning you must have an Apple device of some sorts that supports the payment method. It is generally not seen as an alternative to the payment methods mentioned above but with around 1.5 billion Apple devices out there merchants are eager to develop Apple approved apps to share in the pie so to speak. From a security side, Apple Pay uses security features built-in to the hardware and software of your device to help protect your transactions. In addition, to use Apple Pay, you must have a passcode set on your device and, optionally, Face ID or Touch ID.

This is just an overview of a handful of payment apps available today but whatever app you choose, make sure you look at the security features offered and that you are comfortable with it before you subscribe.

As a last note or disclaimer, I generally take due care to ensure the accuracy of the content but as the reviews are based on articles, documents and other information freely available on the Internet it is sometimes possible for minor factorial misrepresentation.



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