Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

On August 26, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Cisco, IBM, Google, and Mozilla 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

28 August 2020

In The News This Week

New Zealand's stock exchange hit by second cyber attack

Trading on New Zealand's stock exchange was halted for several hours on Wednesday after what appeared to be a second offshore cyber attack in as many days, bourse operator NZX Ltd (NZX.NZ) said. The cyber attack was similar to one late on Tuesday, the bourse said, where its network provider faced a distributed denial of service (DDoS) attack - a common way to disrupt a server by overwhelming the infrastructure with a flood of internet traffic until they can no longer cope with the scale of data requested. NZX said cash market trading was halted at 11:24 a.m. local time (2324 GMT) on Wednesday and resumed at 3:00 p.m. Trading in the final hour on Tuesday was also affected. The NZX website and markets announcement platform were also impacted. "NZX's network provider continues to investigate the source of the issue. We will provide further information once available," the company said in an emailed statement.." Read the article here: Reuters

North Korean hackers ramp up global bank heists

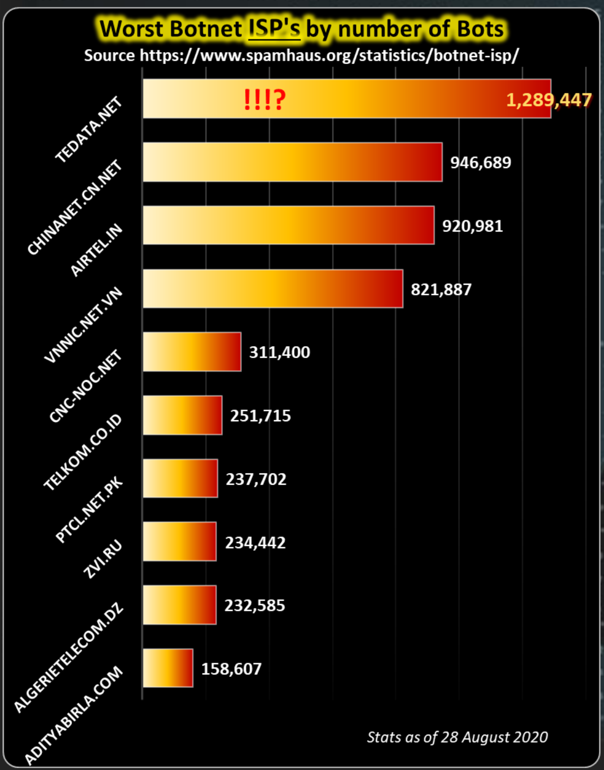
North Korean hackers are tapping into banks around the globe to make fraudulent money transfers and cause ATMs to spit out cash, the U.S. government warned on Wednesday. A technical cybersecurity alert jointly written by four different federal agencies, including the Treasury Department and FBI, said there had been a resurgence in financially motivated hacking efforts by the North Korean regime this year after a lull in activity. "Since February 2020, North Korea has resumed targeting banks in multiple countries to initiate fraudulent international money transfers and ATM cash outs," the warning reads. U.S. law enforcement titled the hacking campaign "**Fast Cash**" and blamed North Korea's Reconnaissance General Bureau, a spy agency, for it. They described the operation as going on since at least 2016 but ramping up in sophistication and volume recently.
Read the full story here: FOX Business

Russian arrested for trying to recruit an insider and hack a Nevada company

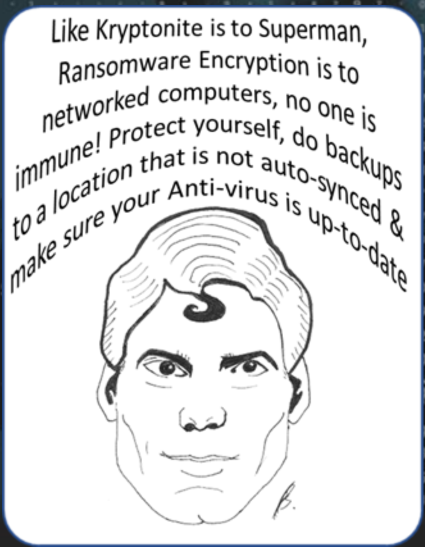
The US Department of Justice announced charges today against a Russian citizen who travelled to the US to recruit and convince an employee of a Nevada company to install malware on their employer's network in exchange for **$1,000,000**. According to court documents unsealed today, Egor Igorevich Kriuchkov, a 27-year-old Russian, was identified as a member of a larger criminal gang who planned to use the malware to gain access to the company's network, steal sensitive documents, and then extort the victim company for a large ransom payment. To mask the theft of corporate data, Kriuchkov told the employee that other members of his gang would launch DDoS attacks to keep the company's security team distracted. Kriuchkov and his co-conspirators' plans were, however, upended, when the employee they wanted to recruit reported the incident to the FBI. FBI agents kept Kriuchkov under observation during his stay in the US, and eventually arrested the Russian national on Saturday after they had gathered all the evidence they needed to prosecute. Read the full article and a chronological timeline of Kriuchkov's time in the US here: ZDNet Article

Popular iOS SDK Accused of Spying on Billions of Users and Committing Ad Fraud

A popular iOS software development kit (SDK) used by over 1,200 app, with a total of more than **a billion mobile users,** is said to contain malicious code with the goal of perpetrating mobile ad-click fraud and capturing sensitive information. According to a report published by cybersecurity firm Snyk, Mintegral, a mobile programmatic advertising platform owned by Chinese mobile ad tech company Mobvista, includes an SDK component that allows it to collect URLs, device identifiers, IP Address, OS version, and other user sensitive data from compromised apps to a remote logging server. The malicious iOS SDK has been named "**SourMint**" by Snyk researchers. "The malicious code can spy on user activity by logging URL-based requests made through the app", Snyk's Alyssa Miller said in a Monday analysis." This activity is logged to a third-party server and could potentially include personally identifiable information (PII) and other sensitive information." Read the full story here: HackerNews



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


Like Kryptonite is to Superman, Ransomware Encryption is to networked computers, no one is immune! Protect yourself, do backups to a location that is not auto-synced & make sure your Anti-virus is up-to-date

Using your Mobile phone as an SOS device?

Most mobile phones today provide a powerful emergency or SOS feature that you might not be aware of. This is apart from the numerous emergency contact Apps available in the various App stores. If you prefer to go this route though, it requires your target emergency contact to have the same app installed. The built in SOS feature is available on both Apple and Android devices but before we get into it, I just want to remind you that you should at least have the basic phone security option of a lock screen enabled preferably with a 6 digit pin code. (And for those using the pattern swipe option, avoid using the 1-to-3-to-7-to-9 or "Z" pattern, the easiest one to guess). Without further ado, following is information adapted from various sources on how SOS on you phone works. - Sources: Click2Houston, TheVerge, GadgetHacks, Huawei, TheBreeze, Samsung, Apple

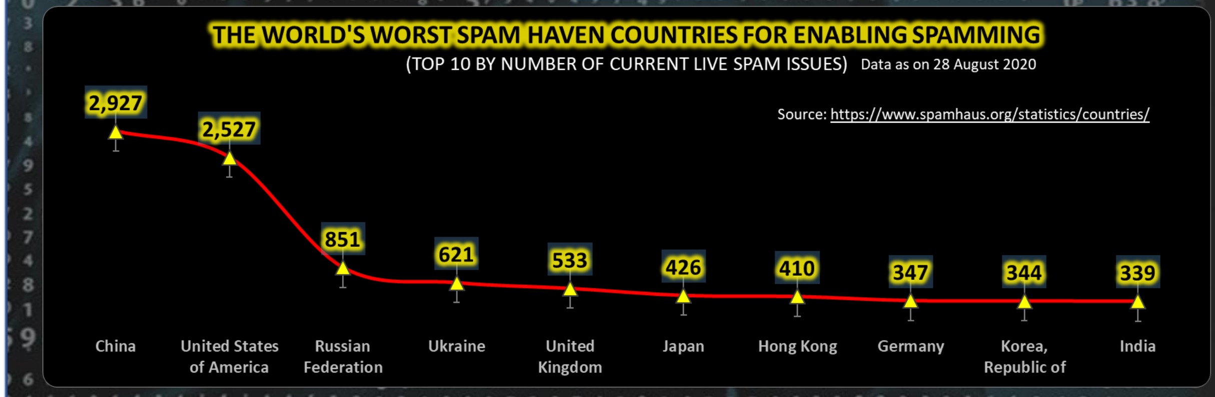
Emergency (SOS) feature

Apple iPhone: When you make a call with SOS, your iPhone automatically calls the local emergency number for your area (Typically in the USA it will be 911). You can also add emergency contacts. After an emergency call ends, your iPhone alerts your emergency contacts with a text message, unless you choose to cancel. Your iPhone sends them your current location, and, for a period of time after you enter SOS mode, sends updates to your emergency contacts when your location changes.
Here's how to make the call on **iPhone X, iPhone 8, or iPhone 8 Plus (Apple): (1)** **Press and hold the side button and one of the volume buttons** until the Emergency SOS slider appears. **(2)** Drag the Emergency SOS slider to call emergency services. If you continue to hold down the side button and Volume button, instead of dragging the slider, a countdown begins and an alert sounds. If you hold down the buttons until the countdown ends, your iPhone automatically calls emergency services. Here's how to make the call on **iPhone 7 and earlier models: (1)** **Rapidly press the side button five times**. The Emergency SOS slider will appear. **(2)** Drag the Emergency SOS slider to call emergency services. After the call ends, your iPhone sends your emergency contacts a text message with your current location, unless you choose to cancel. If Location Services is off, it will temporarily turn on. If your location changes, your contacts will get an update, and you'll get a notification about 10 minutes later. To stop the updates, tap the status bar and select "Stop Sharing Emergency Location." If you keep sharing, you'll get a reminder to stop every four hours for 24 hours.
Remember: If you use the Emergency SOS shortcut, you need to enter your passcode to re-enable Touch ID, even if you don't complete a call to emergency services.
If you started an emergency call by error or accident, press the "Stop" button, then tap "Stop Calling."
You can add emergency contacts from the Health app on your iPhone. Just remember: You can't set emergency services as an SOS contact. For more information, including how to set up this feature on your Apple Watch, follow this link AppleWatch

Android – Samsung Galaxy: If you use a Samsung Galaxy smartphone, Samsung has included a similar feature called SOS Messages. To use it, you add up to four contacts who will receive an emergency alert when you **press the power button on your device three times in succession**. When triggered, an emergency message with your location, a picture of your situation, and an audio message will be sent automatically. Here's how to set it up on your Samsung Galaxy: **(1)** Open your phone's settings, go to "Personal," select "Privacy and Emergency," and click "Send SOS Messages." **(2)** You can enable the feature by clicking the toggle at the top right. It will prompt you to agree to a disclaimer. Once you accept the terms, you will be able to set up SOS Messages. **(3)** Click "Send messages to" to choose up to four emergency contacts to receive your emergency alerts. You can add new contacts or select from contacts already on your phone. Note that 911 cannot be created as an emergency contact. In addition to sending your location, you can choose to enable two additional SOS messaging features. **(4)** "Attach pictures" allows you to attach photos taken from both the front and rear cameras before the emergency alert is sent. **(5)** "Attach audio recording" allows you to attach a five-second audio recording to the message.

Android – Huawei Phones: (1) Enable GPS and allow the Emergency SOS feature to access your location. **(2)** Go to Settings > Security > Emergency SOS , enable Also send SOS message, then set your emergency contacts. **(3)** Once you have enabled the Emergency SOS feature, if you encounter an emergency, **press the Power button five times in quick succession** and your phone will automatically send a message with your current location to your emergency contacts. Once the message is sent, your phone will bring up the emergency call screen, from which you can quickly call an emergency service or one of your emergency contacts.

Other Android Devices: Unfortunately not all Android devices have a similar all-in-one function, though it does provide a way to offer emergency services information about a preassigned emergency contact from the lock screen. While the setup may differ somewhat depending on what phone you have and which version of Android it runs, the basics should be the same. **(1)** Go to your phone's lock screen. (You don't have your lock screen enabled, please do so! Its important) **(2)** Look for the word "Emergency" at the bottom of the lock screen. Tap on that. **(3)** Tap on "Emergency information" and then on the pencil symbol (or, depending on your phone, on "Add"). You'll be asked to put in your PIN or lock pattern. **(4)** This will bring you to your Emergency information screen where you can add personal information (such as blood type or any existing medical conditions) and any contacts you want to be notified in an emergency situation.
Should your Android device not support the features described here, you can download the Google's Trusted Contacts app for Android and use that instead. You can also enquire about the SOS feature if you go to the particular phone manufacturer's website.



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