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

On February 19, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Adobe, Mozilla, 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

21 February 2020

In The News This Week

Iranian hackers have been hacking VPN servers and planted backdoors in companies around the world - 2019 will be remembered as the year when major security bugs were disclosed in a large number of enterprise VPN servers, such as those sold by Pulse Secure, Palo Alto Networks, Fortinet, and Citrix. A new report published this week reveals that Iran's government-backed hacking units have made a top priority last year to exploit these VPN bugs as soon as they became public in order to infiltrate and plant backdoors in companies all over the world. According to the report from cyber-security firm ClearSky, Iranian hackers have targeted companies "from the IT, Telecommunication, Oil and Gas, Aviation, Government, and Security sectors." Some attacks happened hours after public disclosure and dispels the notion that Iranian hackers are not sophisticated, and less talented than their Russian, Chinese, or North Korean counterparts. ClearSky says that "Iranian APT groups have developed good technical offensive capabilities and are able to exploit 1-day vulnerabilities in relatively short periods of time."
Read the full story by Catalin Cimpanu here: ZDNet Article

97 of 100 World's Largest Airports are Vulnerable to a Cyberattack

New research finds that 97 out of 100 the world's largest airports have security risks related to vulnerable web and mobile applications, misconfigured public cloud, Dark Web exposure or code repositories leaks. The report from web security company ImmuniWeb is based on its analysis of cybersecurity, compliance and privacy of the world's largest airports. During the research, ImmuniWeb identified three international airports that successfully passed all the tests without a single major issue being detected: (a) Amsterdam Airport Schiphol (EU), (b) Helsinki-Vantaa Airport (EU) and (c) Dublin Airport (EU). The reports states alarming security statistics including the following: 97% of the 100 airport websites contain outdated web software; 100% of airport APPs contains at least 2 vulnerabilities; 66 out of the 100 airports are exposed on the Dark Web in one way or another; and the list goes on. Thanks to my friend Yazan Shapsugh for pointing me to this snippet. Read the full story here: Security Magazine

MGM Resorts confirms data breach of 10.7 million guests

MGM Resorts has acknowledged that personal information of about 10.7 million hotel guests was published on a hacking forum earlier this week. The data exposure was confirmed to CNET sister site ZDNet by MGM Resorts on Wednesday. Included in the data were full names, phone numbers, addresses, emails and dates of birth. ZDNet confirmed the data's accuracy by reaching out to some customers whose information was published on the hacking forum. The data was accessed via a security incident in 2019, an MGM Resorts spokesperson told ZDNet, during which all affected customers were notified. "Last summer, we discovered unauthorized access to a cloud server that contained a limited amount of information for certain previous guests," the hotel chain told ZDNet, adding that no financial or credit card data leaked.
Read the full story here: CNet Article

Craziest IoT Device Hacks - Hackable medical devices

In 2017, the US Food and Drug Administration (FDA) confirmed that St. Jude Medical's implantable cardiac devices could be easily hacked. Such devices are usually used to monitor patients' heart functions and control heart attacks. However, due to transmitter vulnerabilities, hackers could control shocks, administer incorrect pacing, and deplete the battery. And it's not the only time when the FDA issued similar warnings. Earlier this year a new alert was issued on the security of Medtronic insulin pumps, which hackers could remotely access and control. Find more crazy hacks here: Finance Monthly

Top Online Scams you need to avoid

At least once or twice a week someone will report some sort of a scam they were exposed to either by email or social media. Some of these are so obvious but we do have some naïve users that cannot believe that someone will do them in. The scams varies from promises of big sums of money, unbelievable vacations, a relative/friend in dire need or an incredibly safe and lucrative pyramid scheme and so on. It is scary to see how many people actually fall for it and while they do, the scams will carry on. With this in mind I was scanning the web for the worst and most commons scams that is prevalent out there and I came across a highly informative article by Ioana Rijnetu of Heimdal Security. Below is an adapted extract of her article showing the top 4 of 19 scams running at this moment. Please visit the Heimdal site (above) for the full article and list.

Online Scams, how cybercriminals use them to trick you

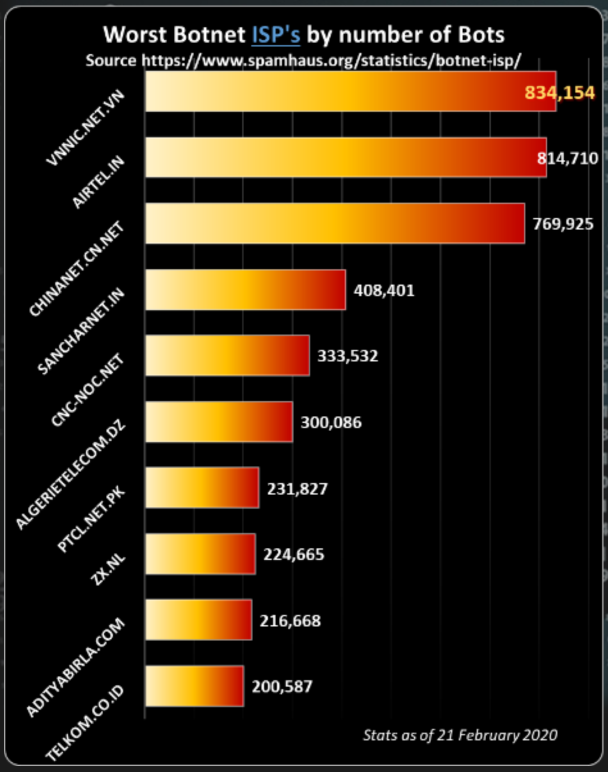
We truly want to believe that the Internet is a safe place where you can't fall for all types of online scams, but it's always a good reminder to do a "reality check". We, humans, can become an easy target for malicious actors who want to steal our most valuable personal data. Criminal minds can reach these days further than before, into our private lives, our homes and work offices. And there is little we can do about it. Attack tactics and tools vary from traditional attack vectors, which use malicious software and vulnerabilities present in almost all the programs and apps (even in the popular Windows operating systems), to ingenious phishing scams deployed from unexpected regions of the world, where justice can't easily reach out to catch the eventual perpetrators. According to a report from the Federal Trade Commission (FTC), millennials are particularly more vulnerable to online scams than seniors, as shocking as it may seem. The research finds that "40 percent of adults age 20-29 who have reported fraud ended up losing money in a fraud case".

(1) Phishing email scams - More than one third of all security incidents start with phishing emails or malicious attachments sent to company employees, according to a new report from F-Secure. Phishing scams continue to evolve and be a significant online threat for both users and organizations that could see their valuable data in the hands of malicious actors. Phishing scams are based on communication made via email or on social networks. In many cases, cyber criminals will send users messages/emails by trying to trick them into providing them valuable and sensitive data (login credentials – from bank account, social network, work account, cloud storage) that can prove to be valuable for them. Moreover, these emails will seem to come from an official source (like bank institutions or any other financial authority, legitimate companies or social networks representatives for users.) This way, they'll use social engineering techniques by convincing you to click on a specific (and) malicious link and access a website that looks legit, but it's actually controlled by them. In order for their success rate to grow, scammers create a sense of urgency. They'll tell you a frightening story of how your bank account is under threat and how you really need to access as soon as possible a site where you must insert your credentials in order to confirm your identity or your account.

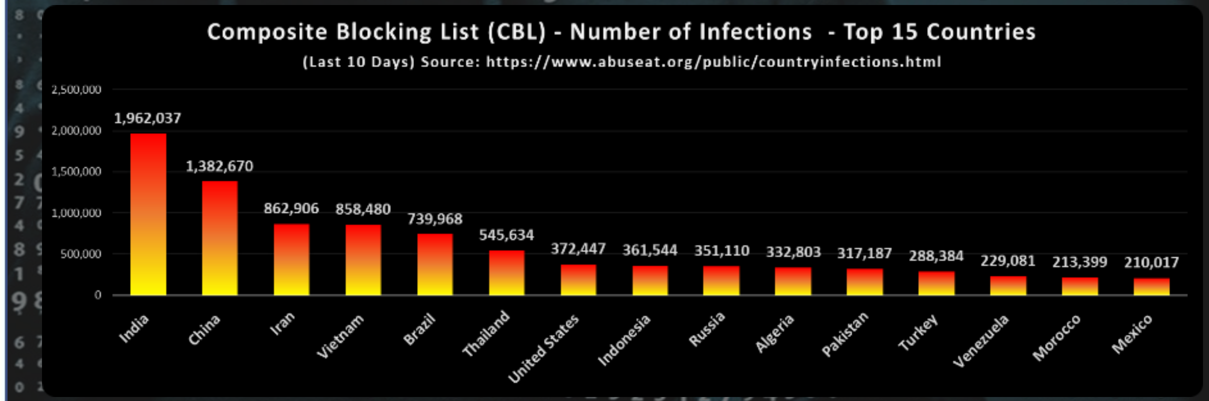
(2) The Nigerian scam - Probably one of the oldest and most popular Internet scams used mostly by a member of a Nigerian family with wealth to trick different people. It is also known as "Nigerian 419" and named after the section of Nigeria's Criminal Code which banned the practice. A typical Nigerian scam involves an emotional email, letter, text message or social networking message coming from a scammer (which can be an official government member, a businessman or a member of a very wealthy family member – usually a woman) who asks you to give help in retrieving a large sum of money from a bank, paying initially small fees for papers and legal matters. In exchange for your help, they promise you a very large sum of money. They will be persistent and ask you to pay more and more money for additional services, such as transactions or transfer costs. You'll even receive papers that are supposed to make you believe that it's all for real. In the end, you are left broke and without any of the promised money.

(3) Greeting card scams - Whether it's Christmas or Easter, we all get all kind of holiday greeting cards in our email inbox that seem to be coming from a friend or someone we care. Greeting card scams are another old Internet scams used by malicious actors to inject malware and harvest users' most valuable data. If you open such an email and click on the card, you usually end up with malicious software that is being downloaded and installed on your operating system. The malware may be an annoying program that will launch pop-ups with ads, unexpected windows all over the screen. If your system becomes infected with such dangerous malware, you will become one of the bots which are part of a larger network of affected computers. If this happens, your computer will start sending private data and financial information to a fraudulent server controlled by IT criminals.

(4) Bank loan or credit card scam - People can be easily scammed by "too good to be true" bank offers that might guarantee large amounts of money and have already been pre-approved by the bank. If such an incredible pre-approved loan is offered to you, ask yourself: *"How is it possible for a bank to offer you such a large sum of money without even checking and analysing your financial situation?"* Though it may seem unlikely for people to get trapped by this scam, there's still a big number of people who lost money by paying the "mandatory" processing fees required by the scammers. Follow this link for 9 warning signs and sneaky tactics to watch out and avoid becoming the victim of a business loan scam. As regards to credit card scams, a recent report from the Identity Theft Resources Center said that the number of credit and debit card breaches have been on the rise last year. To better safeguard your data and prevent thieves from getting access to your payment card details, consider: (a) Watching your accounts closely and monitor your online transactions; (b) Taking advantage of free consumer protection services; (c) Signing up for free credit monitoring.



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



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