On February 24, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Webkit and Mozilla products.

Covid-19 Global Stats

Date	Confirmed Cases	Deaths
26-Feb	113,551,251	2,519,338

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

26 February 2021

In The News This Week

10K Microsoft Email Users Hit in FedEx Phishing Attack

Researchers are warning of recent phishing attacks targeting at least 10,000 Microsoft email users, pretending to be from popular mail couriers – including FedEx and DHL Express. Both scams have targeted Microsoft email users and aim to swipe their work email account credentials. They also used phishing pages hosted on legitimate domains, including those from Quip and Google Firebase – allowing the emails to slip by security filters built to block known bad links. "The email titles, sender names and content did enough to mask their true intention and make victims think the emails were really from FedEx and DHL Express respectively," said researchers with Armorblox on Tuesday. "Emails informing us of FedEx scanned documents or missed DHL deliveries are not out of the ordinary; most users will tend to take quick action on these emails instead of studying them in detail for any inconsistencies. Read the full story by Lindsey O'Donnell here: ThreatPost

New York issues cyber insurance framework as ransomware, SolarWinds costs mount

The state looks to protect one of its core industries, which is threatened by mounting and potentially "unsustainable" losses due to the SolarWinds and ransomware attacks. On February 4, 2021, New York became the first state in the nation to issue a cybersecurity insurance risk framework to all authorized property and casualty insurers. In releasing the framework, New York's Department of Financial Services (DFS) said that "[f]rom the rise of ransomware to the recently revealed SolarWinds-based cyber-espionage campaign, it is clear that cybersecurity is now critically important to almost every aspect of modern life—from consumer protection to national security. "The framework applies to all property or casualty insurers that write cybersecurity insurance. However, the DFS wants all insurers, even though those that don't offer cybersecurity insurance, to "still evaluate their exposure to 'silent risk' and take appropriate steps to reduce that exposure." **DFS advises against paying ransom demands** - Noting that ransomware insurance claims jumped by 180% from 2018 to 2019 and doubled from 2019 to 2020, DFS advised insurers to not make ransomware payments for three reasons (which you can find by reading the full article by Cynthia Brumfield here: CSO

Quantum computer solves decades old problem 3 million times faster

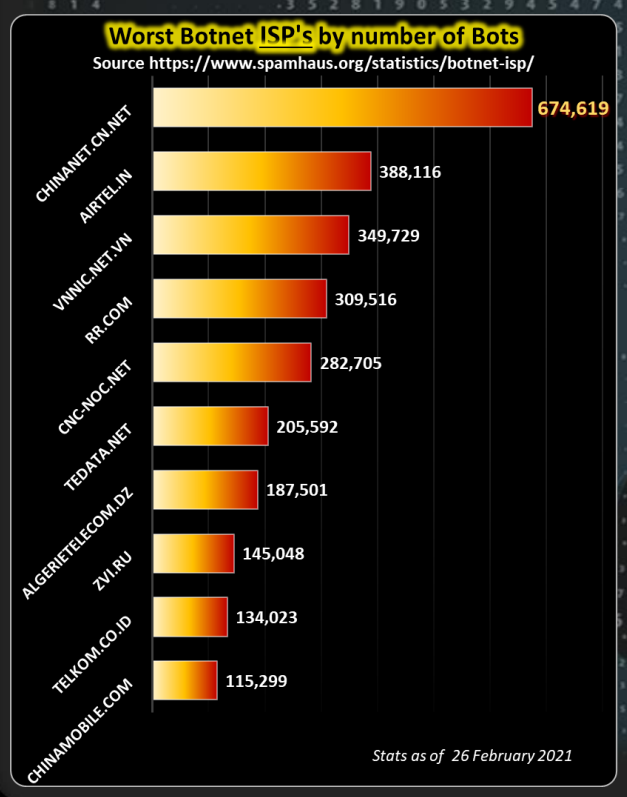
A quantum computer just solved a decades-old problem three million times faster than a classical computer - Scientists from quantum computing company D-Wave have demonstrated that, using a method called quantum annealing, they could simulate some materials up to three million times faster than it would take with corresponding classical methods. Together with researchers from Google, the scientists set out to measure the speed of simulation in one of D-Wave's quantum annealing processors, and found that performance increased with both simulation size and problem difficulty, to reach a million-fold speedup over what could be achieved with a classical CPU. . . Read the full story by Daphne Leprince-Ringuet here: ZDNet

Nigerian government launches National Cyber Security Policy

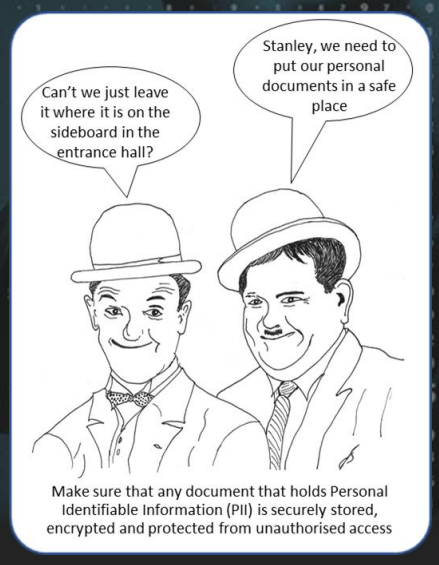
President Muhammadu Buhari has launched the Nationwide Cyber Safety Coverage and Technique 2021, ThisDay reported. The doc will present a framework to harness the efforts of the personal sector, academia, and trade in direction of progressive financial and nationwide improvement. It should present a platform for technical training, digital expertise acquisition and indigenous expertise manufacturing, creating youth job alternatives supporting Nigeria's resolve to alleviate poverty and increase the economic system, he said.
Read the full story here: InfoDigest

Botnet Uses Blockchain to Obfuscate Backup Command & Control Information

The tactic makes it much harder for defenders to take down botnets via sinkholing and other standard techniques, Akamai says. The operator of a known botnet used for cryptocurrency mining has started using a relatively rare technique for maintaining persistence that, if more broadly adopted, could make botnet takedowns much harder to accomplish. Researchers at Akamai recently observed the technique being used in infection attempts targeting customers of its security intelligence response team. In a new report, the company describes the tactic as involving the use of the Bitcoin blockchain to obfuscate configuration information pertaining to secondary command-and-control (C2) infrastructure for the botnet. The decentralized nature of the blockchain makes the botnet infrastructure more reliable and harder to sinkhole, Akamai says..
Read the full story by Jai Vijayan here: DarkReading



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



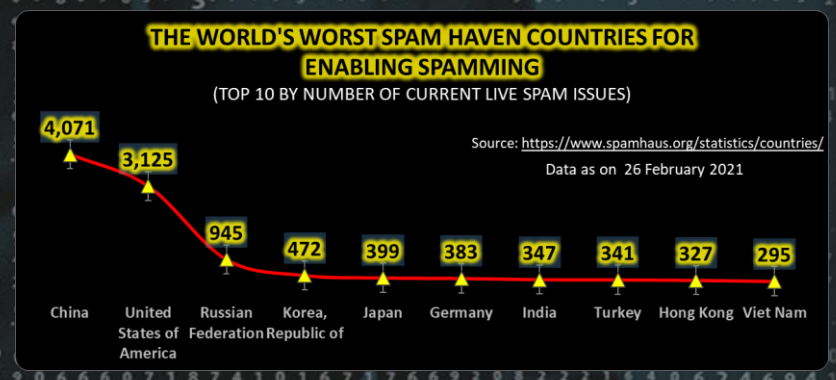
Working from Home? - 10 Tips to Secure Your Home Network

The Covid-19 pandemic has brought about massive changes in the way we work and operate, and working from home became a new normal. With this came new challenges for cyber security as criminals also moved their focus to the more insecure home networks. We have seen that once a remote workers computer has been compromised, gaining access to the networks they traverse became so much easier. Today I will focus on some tips on how to beef up security on your home network.
References: Heimdal, PhoenixNAP, CSO, Comparitech, MetaCompliance

1. **Change the name of your default home network** – Let's start with changing the name of your Wi-Fi network, also known as the SSID (Service Set Identifier). Changing your Wi-Fi's default name makes it harder for malicious attackers to know what type of router you have. If a cybercriminal knows the manufacturer name of your router, they will know what vulnerabilities that model has and then try to exploit them. When choosing a name for your network, used a non-descript name, you don't want them to know at first glance which wireless network is yours when there are probably three or four other neighbouring Wi-Fis.
2. **Set a strong and unique password to secure your wireless router** – Every router comes with a default user ID and password; in many cases it is "admin" with password "admin". So, when you set up your router, make sure you change them immediately. Make the password at least 10 characters long with a mix of upper case, lower case, numerals, and special characters. Remember, the longer the password, the harder it is to crack. If a device allows for it, use a password phrase which will make it easier for you to remember. A simple example is "Fix my 26 scrapy pants" or anything that you can creatively come up with that is easy to remember. Use this LINK the get some good password ideas.
3. **Set up a strong Pre-Shared Key (PSK)** – Now don't get confused between the router password and your PSK. The Pre-Shared Key or WPA_PSK is the "password" or "pin code" that you use to gain access to your Wireless Network (or the code you give to your visiting friends to connect to your network). WPA-PSK stands for "Wi-Fi Protected Access" – "Pre-Shared Key" and is part of your Wi-Fi encryption settings. When you click on the network name (SSID) that shows up on the network selections on your device, it will ask for your password or "WPA-PSK". This encryption and access settings are set up in your router and you can follow the same password rules as described in section 2 above.
4. **Wi-Fi Router location** - Where your Wi-Fi router is placed in your home can have an impact on your security. Place the wireless router as close as possible to the middle of your house. Why? First of all, it will provide equal Internet coverage to all the rooms in your home. Secondly, you don't want to have your wireless signal range reach outside your home too much, where it can be easily intercepted by people with ill intent.
5. **Change the default IP-Address on your router** – All routers come with a pre-set IP address in the range of either 192.168.0.0 or 10.0.0.0. Every hacker in the world knows this and it is the most common default setting on the router that no one changes. Changing your default IP address will increase security on your home network and make it more difficult for hackers to track it.
6. **Turn on your home router's firewall** – Nowadays, all Wi-Fi routers comes with a built-in firewall, but this not always switched on by default. Scroll through the various options in your routers admin console, you will normally find the firewall under the security setting. You don't need to be a Network or Security specialist to configure the firewall, just make sure it is switched on, the default configuration is normally good enough.
7. **Turn off Remote Management** - The console of a router should only be accessible from devices connected to the network. However, a standard router setting enables remote access. This means that you can access the console over the internet, from another location. Unfortunately, if you can do that, so can anyone else. So, turn off remote access.
8. **Limit WPS** - Wi-Fi Protected Setup (WPS) offers an easy way to get new devices to recognize the network and connect to the router. WPS uses one of two methods: If your router has a WPS button on the back, pushing it will send out a signal that adds the device to the network and passes it log in credentials so you don't have to enter a text password (works like Bluetooth Pairing). The second method uses an eight-character numeric code entered into the network settings of the device. The second method however has security weakness because the code method is easy to crack. If your router has a WPS button, then turn off the WPS code capabilities and rely on the button. If you don't have the button, turn off WPS completely because the code option is a serious problem for your network security.
9. **Additional Security: Hide the network** - Your router doesn't have to broadcast its SSID. If you block your router from sending out its identifier, your home Wi-Fi becomes a hidden network. Those devices that already have connection data stored will still be able to connect, but passers-by won't see it. In many cases, the network list that others see will include a line that says, "Hidden network." If you don't know the name of the network, it is impossible to connect to it.
When you buy a new gadget that needs to "see" the network to be set up, you can always temporarily turn on the SSID broadcast to let your new device see the network. Once you have set up a connection with the password, make the network hidden again. Hiding the network makes it easier to block visitors from getting on the network. If they can't see your router in their list of available networks, they will be less likely to ask for the password.
10. **Additional Security: Switch the router off when not in use** – When you are not at home, it is a good idea to switch off the router, apart from saving a small amount of electricity, it will also limit the possibility of some external tampering to go unnoticed. The less time your Wi-Fi system is active the less possibility there will be for an intruder to gain access.

Other Interresting News and Cyber Security bits:

- Top 10 cybersecurity predictions for 2021
- SolarWinds cybersecurity spending tops $3 million in Q4, sees $20 million to $25 million in 2021
- Biden To Order Review Of U.S. Semiconductor, IT Supply Chains



AUTHOR: CHRIS BESTER (CISA,CISM)
chris.bester@yahoo.com