On February 26, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Cisco, PHP, Google, and Open SMTPD 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 February 2020

In The News This Week

KrØØk: Serious vulnerability affected encryption of over a billion Wi-Fi devices

ESET researchers discovered a previously unknown vulnerability in Wi-Fi chips and named it KrØØk. This serious flaw, assigned CVE-2019-15126, causes vulnerable devices to use an all-zero encryption key to encrypt part of the user's communication. In a successful attack, this allows an adversary to decrypt some wireless network packets transmitted by a vulnerable device. KrØØk affects devices with Wi-Fi chips by Broadcom and Cypress that haven't yet been patched. These are the most common Wi-Fi chips used in contemporary Wi-Fi capable devices such as smartphones, tablets, laptops, and IoT gadgets. Not only client devices but also Wi-Fi access points and routers with Broadcom chips were affected by the vulnerability, thus making many environments with unaffected or already patched client devices vulnerable anyway. Our tests confirmed that prior to patching, some client devices by Amazon (Echo, Kindle), Apple (iPhone, iPad, MacBook), Google (Nexus), Samsung (Galaxy), Raspberry (Pi 3), Xiaomi (RedMi), as well as some access points by Asus and Huawei, were vulnerable to KrØØk. This totalled to over a billion Wi-Fi-capable devices and access points, at a conservative estimate. Further, many other vendors whose products we did not test also use the affected chipsets in their devices Read the full story by Miloš Čermák and Robert Lipovsky here: WeLiveSecurity

Africa – Kenya's disputed Computer Misuse and Cybercrimes Act, 2018 now effective

20 February marks a turning point for Kenya's controversial Computer Misuse and Cybercrimes Act, 2018 (the "Act"). The suspension of critical provisions that have been a subject of dispute since the Act partially came into force on 30 May 2018, has now been lifted. Yesterday, the High Court of Kenya ("High Court") dismissed the Bloggers Association of Kenya's ("BAKE") petition challenging the constitutionality and legality of several provisions of the Act. Read the full story here: ENSafrica (Thanks to Neels Muller who pointed me to this news snippet)

Canada - Personal information of nearly 360,000 Quebec teachers exposed in data breach

The personal information of nearly 360,000 teachers in Quebec may have been stolen in a data theft, the Quebec government confirmed on Friday 21st of February. Quebec's Treasury Board took stock in the wake of the ongoing investigation by the Sûreté du Québec (SQ) into identity theft of people working or having worked as teachers. The hackers had access to a database containing personal information after stealing a user code and password, Quebec's Treasury Board statement said. The reliability of the government's computer systems is not called into question, since the theft would have been carried out using a fraudulent password and access code, the board said on Friday. The Ministry of Education obtained confirmation on Wednesday that their personal data may have been stolen. The government has said that those affected will be able to take advantage of free credit monitoring services. Letters will be sent shortly to the individuals concerned. The SQ is continuing its investigation, in collaboration with the Ministry of Education. Read the full story here: GlobalNews

Chrome 80 update cripples top cybercrime marketplace

A small change in the Google Chrome 80 browser has had a devastating effect on one of today's top cybercrime marketplaces. According to new research shared with ZDNet this week by threat intelligence firm KELA, the Genesis Store is currently going through a rough patch, seeing a 35% drop in the number of hacked credentials sold on the site. KELA says Genesis administrators are scrambling to fix their inventory deficit and feed the store with new credentials before customers notice a drop in new and fresh listings. If they don't address the issues caused by the new Chrome 80 update, the store's entire future hangs in the balance. Read the full story here: ZDNet

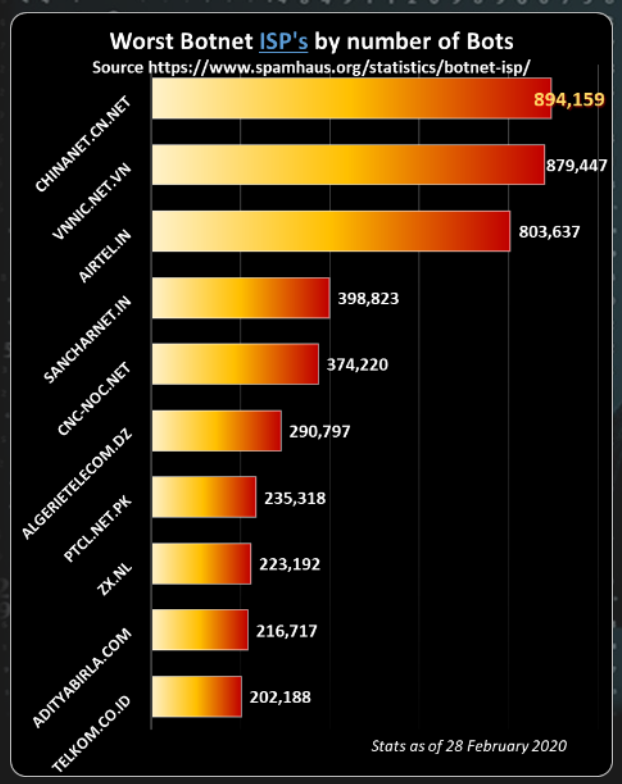
5G has arrived, what does that mean? What is 5G anyway?

The next-generation cellular technology is said to be between 20 and potentially 100-fold faster than our current 4G cellular and broadband networks and today we will explore what is reality versus the marketing hype. We will also look at the general security challenges we are facing with technology using 5G.

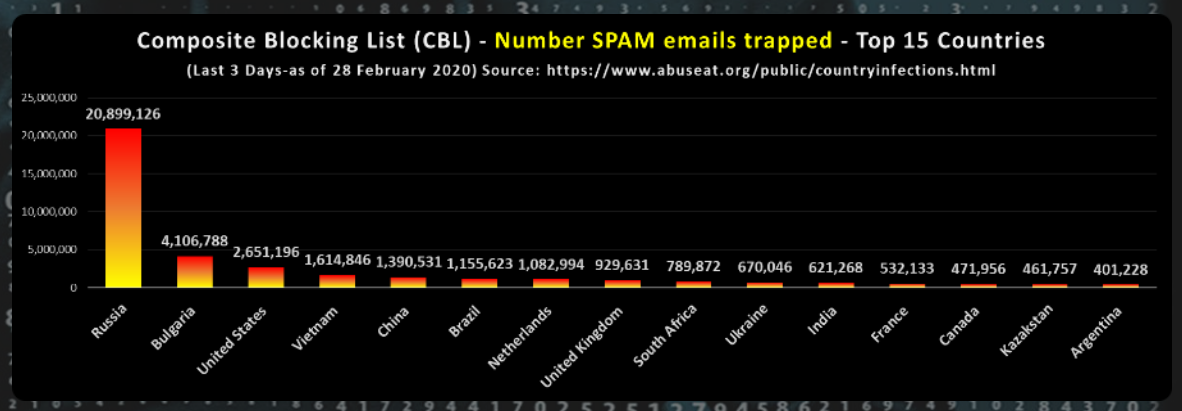
First, what is 5G? - 5G stands for "Fifth-Generation Cellular Wireless standard" which were initially set at the end of 2017. If we roll back a little and look at the previous generations and start with the first generation (1G) which represents the analogue cellular networks launched in the mid-80s and were basically used to make voice calls only. Then second generation (2G) mobile networks came along in the early 90s and we saw the advent of the GSM cellular networks which were capable of voice calls and text messages (SMS) and could handle limited data transfer through GPRS. The 2001 introduction of 3G brought about a mini cellular revolution as additional features such as mobile Internet access, video calls, mobile TV and more were literally in the palm of our hands, initially at speeds up to 42MBps. Although 2G was still the primary voice carrier, 3G was all about data. 3G went through a series of iterations and ended up with 3.9G deployed in 2008 also known as HSDPA (High Speed Data Access) which allow throughput of 10MBps. The introduction of 4G (LTE) did not bring so much extra from a feature perspective but it was much, much faster and essentially brought broadband to your phone at 100MBps compared to only 10KBps on 1G and 170KBps on 2G. Now, 5G is said to be faster and more efficient than any previous generation. It promises mobile data speeds that far outstrip the fastest home broadband network currently available to consumers. With speeds of up to 100 gigabits per second! 5G is set to be as much as 100 times faster than 4G. The trade-off for speed between the generations is distance and density of cell towers (Antennas) where a 2G tower's coverage is up to 10 Km, and as you go faster the distance get smaller meaning an increase in tower density. 3G coverage is only about 3 Km and the higher frequency 5G network have a range of more or less 1.5km (Approx. 1 Mile). Although the "towers" became much smaller, 5G antennas can literally sit on top of existing lamp posts.
With the Internet of Things (IoT) explosion, soon 4G networks will just not be able to handle the huge number of connections and this is really where 5G will come to it rights. It is estimated that by the end of this year there will be more than 20 billion connected devices all pushing data back and forth.
As a last word on what 5G is, don't get confused between 5G cellular (what we are talking about here) and 5G Wi-Fi. If you click on the wi-fi network icon normally on the bottom right on your computer you will see available wi-fi networks, and sometimes you'll see a network name with "_5G" added on the back end. 5G in this case refers to the 5GHz wireless frequency as opposed to the more general 2.4 GHz frequency network and is not 5G Cellular.

Reality of current available 5G options – In general, what 5G will give you is bigger channels (to speed up data), lower latency (to be more responsive), and the ability to connect a lot more devices at once (for sensors and smart devices). In the current market place, we mainly see three varieties on offer, low, mid and high-performance. The low-performance offering is in the region of 20 – 30Mbps and the mid-performance should perform at 200MBps or more which is a significant jump, and is much faster than any domestic broadband offering currently out there. I didn't see many high-end offerings available yet. At this stage coverage is mostly limited to the larger cosmopolitan areas in countries where it is available, and it will take a while before it will extend beyond the major centres. The reality is that 5G rollout and adoption is still in its baby shoes and it will follow the same trend as when 4G (LTE) came out in that the technology is available but the devices, applications and services now needs to evolve and catch up to fully utilise the technology.

Security Concerns – According to an article posted by Raconteur last week, 94% of Telecoms operators and industry experts believe security challenges will escalate exponentially with the advent of 5G networks. Security concerns were real enough for the European Union member states to publish a risk report in October 2019 assessing the cyber security risk associated with 5G networks. The assessment spanned over 7 typical threat actor groups and besides the generic and expected technical vulnerabilities, highlighted several major vulnerabilities. The real concern however is the massive expansion of connected devices, the very thing 5G was mostly invented for. This range from smart homes and its connected devices, home security systems, autonomous cars, connected healthcare equipment, and so forth, collectively known as the Internet of Things (IoT). And we know, as reported in this bulletin several times in the past, the number of unprotected IoT devices out there are staggering and now with the capabilities of 5G, this number will increase rapidly and exponentially. Cyber criminals already wreaked havoc targeting these devices on the 4G network, and that with all its limitations, but now with most of those limitations fading away with 5G, can you imagine how ripe the proverbial orchard will become for ill intended pickings. The service providers and IoT device vendors will have to step up their game on the security side and make sure that security controls are up to scratch and their user base be well informed on security matters.



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



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