On April 14, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded).

Covid-19 Global Stats

Date	Confirmed Cases	Deaths
16-Apr	139,673,809	2,999,377

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

16 April 2021

In The News This Week

Mexico's Senate approves creation of biometric cellphone registry

MEXICO CITY, April 13 (Reuters) - Mexico's Senate approved on Tuesday the creation of a registry to store millions of cell phone users' biometric data in a bid to crack down on kidnapping and extortion. The reform to the federal telecommunications law was approved with 54 votes in favour, 49 against and 10 abstentions, a Senate representative said. Lawmakers were still discussing whether to make modifications. The legislation, which had already passed in the lower house, aims to counter crime by requiring telecoms companies to collect customer data, including fingerprints or eye biometrics, for a national registry managed by Mexico's telecoms regulator, the IFT. Lawmakers in support of the registry, including from President Andres Manuel Lopez Obrador's MORENA party, have said it would be harder for criminals to remain anonymous when purchasing new phone lines, which can currently be sold at convenience stores without registration.
Read the story by Cassandra Garrison here: Nasdaq

Samsung's new Galaxy Quantum 2 uses quantum cryptography to secure apps

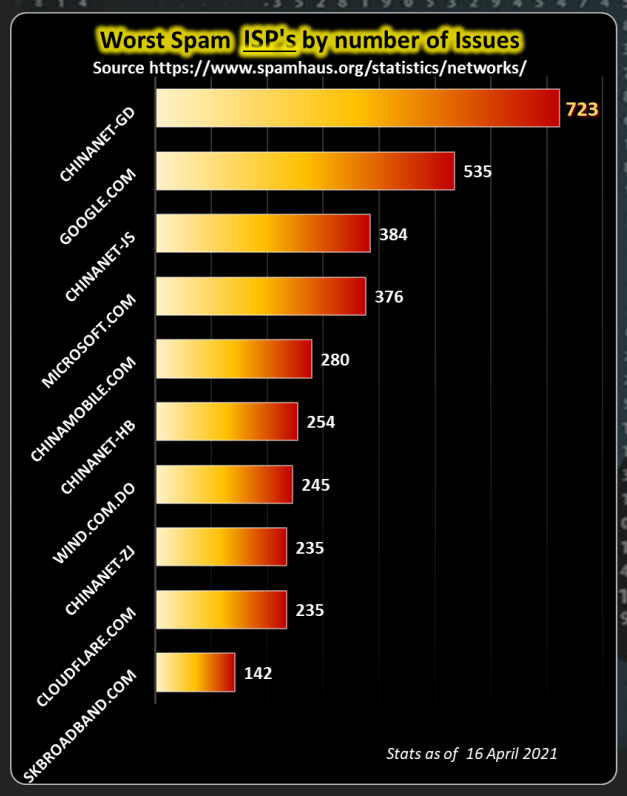
Samsung is launching a new smartphone equipped with quantum cryptography technology, which promises to deliver a new level of security to consumer applications like mobile banking. Developed together with South Korean telecoms giant SK Telecom, the Galaxy Quantum 2 device will be -- at least for the foreseeable future -- only available to the South Korean public, and is the second quantum-equipped smartphone released by Samsung. The Quantum 2's predecessor, called the Galaxy A Quantum, made its debut last year in South Korea, as the world's first 5G smartphone with integrated quantum cryptography technology. Like the new Quantum 2, the Galaxy A includes a quantum random number generator (QRNG) that's designed to secure sensitive transactions against the most sophisticated attacks. Read the full article by Daphne Leprince-Ringuet here: ZDNet

SolarWinds: US and UK blame Russian intelligence service hackers for major cyberattack

US agencies NSA, FBI and CISA, along with the UK's NCSC, accuse 'Cozy Bear' Russian APT group of campaigns against SolarWinds. Organisations are urged to patch the five VPN and cloud vulnerabilities being exploited in ongoing attacks. -Hackers working for the Russian foreign intelligence service are behind the SolarWinds attack, cyber-espionage campaigns targeting COVID-19 research facilities and more, according to the United States and the United Kingdom. The US accusation comes in a joint advisory by the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI), which also describes ongoing Russian Foreign Intelligence Service (SVR) exploitation of five publicly known vulnerabilities in VPN services. Read full the story by Danny Palmer here: ZDNet

Talon Cyber Security Raises $26 Million to Develop Next-Generation Cyber Security for a Distributed Workforce

- TEL AVIV, Israel--(BUSINESS WIRE)--Talon Cyber Security, the leader in cyber security solutions for the distributed workforce, today announced that it has secured $26 million in seed funding from Lightspeed Venture Partners, Team8, serial entrepreneur Zohar Zisapel, and leading cyber angel investors. The company is developing a first-of-its-kind cyber security technology that protects from the unique threats emerging in today's era of distributed work. To protect employees from COVID-19, many enterprises rapidly shifted to make distributed work possible while maintaining business productivity. Forced to accelerate digital transformation initiatives, these changes led to gaps in visibility and security, ultimately playing into the hands of attackers. There were fundamental challenges that could not be addressed using traditional security solutions such as zero trust models or VPN.
Talon's unique technology makes it possible to turn an organization's security weaknesses into resilience against cyber attacks without compromising an employee's privacy or productivity. Talon's novel approach enables all employees, no matter the device they are using, to access their corporate resources in a secure way. By enabling workforce productivity and flexibility while safeguarding security, Talon allows organizations to operate and innovate with confidence. The market for cyber solutions to support distributed work is expected to reach $42 billion by 2026.. Read the full article here: BusinessWire



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

Deepfakes

About a year ago I wrote about the "Deepfake" video phenomena and quoted some parts of a CNBC article by Grace Shao that gives a good rundown of what deepfakes are. Although mostly referring to video manipulation, recent developments with AI in audio manipulation also got some attention.
The topic came up again as AI video manipulation technology is getting better and better and identifying fake videos is getting extremely difficult for the average person out there. It was even highlighted as one of the real-world examples in last week's Social engineering article.
Deepfake technology is used in different ways today, some for laughs, some to trick people, and some to stir up society with impersonation and fake speeches. In the movie industry, it is successfully used in many ways even to put a new actor in an old movie. The success is demonstrated when the '70s and '80s actress Linda Carter was "rebooted" as Gal Gadot's Wonder Woman, with astonishing results. See the YouTube clip of the tech demo here. (the people in the clip are not real)
However, as the movie industry has millions of dollars to make the perfect fake, the average person on the street doesn't, but that doesn't mean they don't have access to the technology. Nowadays you can download an app and make your own deepfakes, all you need is a smartphone and a photo or two. As a recent article by Geoffrey A. Fowler in the Washington Post said, "you can make Abraham Lincoln sing a disco song or Marilyn Monroe blow you a kiss. A number of these apps are available already and I'm sure by the end of the year we will have plenty more. With one of the iPhone apps, Avatarify, you only need one single source photograph of anyone to make a fake video of that person saying what you are actually saying during the recording. Using your phone's selfie camera, whatever you do with your own face happens on theirs.
Granted, these are not as sophisticated as the pro-videos out there, but it is still scary to know that the technology is in the hands of friend and foe.

From the security side, how do we protect ourselves from being manipulated to think in a specific direction or coerced into doing something we would not normally do by a speech or content in a deepfake video? We have seen in recent times how perpetrators with a certain political or religious agenda flood social media with fake speeches to either swing public opinion or discredit a prominent figure whose views are different from theirs.
There is no sure way for the common person in the street to determine whether the video is fake or not. My advice though, always use your common sense. If something sounds out of whack, it probably is. If all-of-a-sudden a political figure sings a different tune or if you hear something from a person in a video you didn't expect to hear, be wary, check the source if you can. Don't react immediately, wait a day or so and keep your eye on the media (not social media) to see if anyone refutes the claims or statements. If possible, always check the date, old videos have a knack of reappearing in social media a year or more later. Look for obvious anomalies like frame jumping, lip-sync, and so on.

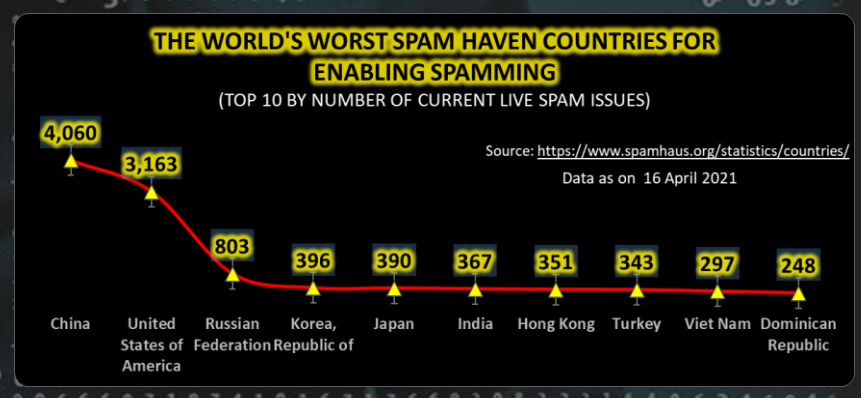
Let's look at some examples:

1. Obama/Jordan Peele - Probably one of the more famous ones is where comedian Jordan Peele, an avid Obama impersonator made a video to demonstrate how easy it is and how convincing it can be if you have the right equipment. This video was created using Adobe After Effects CC and the free tool called FakeApp.
2. Trump & Biden - This comical video shows Donald Trump and Joe Biden singing rap music in a large assembly. Not as good as some of the others but showing the funny side of the spectrum (**Warning, the song contains some strong language**)
3. Mark Zuckerberg – This convincing fake Instagram clip is supposedly showing Mark Zuckerberg where he said his real goal is to own you. This stirred up quite a frenzy at the time and resurfaced in the recent WhatsApp debacle.
4. Historic Figures come to life – This video demonstrates how historical portraits can be brought to life using AI technology. Rendered from old photographs or even painted portraits of the fifteen hundreds. – More here
5. Donald Trump on Aids – Here is an example of how social awareness on a certain topic can be boosted when a French charity organization published a deepfake of Trump in October 2019 saying 'AIDS is over'. For me, it is a bit obvious but if the same video was made today using the advances in AI technology, it would be more convincing than ever.
6. Holograms – This a recording of Supasorn Suwajanakorn's presentation at a TED conference talking about fake videos of real people and even holographic interviews with people long gone using AI technology. He also points out how to spot fake videos.
7. Salvador Dalí comes back to life – Digital artists produced an AI masterpiece that Dalí would surely have appreciated himself when they resurrected the Catalan artist as a charismatic host at the Dalí Museum in Florida.
8. Technical Demo – here we have a demonstration put together by Emily Zendt showing and talking about how the department of defense is taking notice and starting to develop techniques to identify and protect world leaders from deepfakes.

Watch this space as AI technology advance, I'll post more on the topic. Stay sharp and be vigilant.

Other Interesting News and Cyber Security bits:

- LinkedIn - An update on report of scraped data (Alleged Breach)
- How data poisoning attacks corrupt machine learning models
- Will a vaccine passport help international flights take off?



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