On May 6, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Magento, SaltStack and Google 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

08 May 2020

In The News This Week

CAM4 Hacked? - An Adult Cam Site Exposed 10.88 Billion Records

IT'S ALL TOO common for companies to leave databases chock full of sensitive information exposed to the great wide internet. But when that company operates an adult livestreaming service, and that data comprises 7 terabytes of names, sexual orientations, payment logs, and email and chat transcripts—across 10.88 billion records in all—the stakes are a bit higher. The site is CAM4, a popular adult platform that advertises "free live sex cams." As part of a search on the Shodan engine for unsecured databases, security review site Safety Detectives found that CAM4 had misconfigured an Elasticsearch production database so that it was easy to find and view heaps of personally identifiable information, as well as corporate details like fraud and spam detection logs. "Leaving their production server publicly exposed without any password," says Safety Detectives researcher Anurag Sen, whose team discovered the leak, "it's really dangerous to the users and to the company. CAM4 has taken the server offline, but not before it leaked 7TB of user data. There was no evidence that CAM4 were hacked though.
Read the full story here: Wired

Beware of Fake Microsoft Teams Notifications Aimed to Steal Employees Passwords

A new phishing campaign aimed to steal employees' login credentials by impersonating Microsoft Teams' notifications. Due to this COVID-19 pandemic situation, many companies moved to full-time remote work, attackers taking advantage of it. Attackers use crafted emails that appear to be automated notifications emails coming from Microsoft Teams. Once the user click's in the email it takes them to the fake landing that impersonates the real webpages of Microsoft Teams. The campaign was observed by Abnormal Security, according to researchers the "sender email originates from a recently registered domain, "sharepointonline-irs.com", which is not associated with either Microsoft or the IRS." Read the full story here: Cybercureme

India's Largest Online Education Platform Hacked and 22M Users Data Exposed on Dark Web

Recently, India's largest e-learning platform, Unacademy, which is based in Bangalore, is reported to be hacked, hackers gained access to Unacademy's, and to steal more than 22 million users' data. The popular Cyber Security firm, Cyble Inc. has reported about this massive data breach, and according to the security reports, all these stolen details have also been made available for sale on the Dark Web. Unacademy India's largest e-learning platform, which has recently received funding from Facebook, General Atlantic, and Sequoia. Apart from this, currently, Unacademy has a market value of 500 million US dollars. The leaked data includes username, email addresses, hash passwords, joining or previous login date, and many more details. Read the story here: GBHackers

News snippets from the past - Computers & crime

'It's easy to breach computer security – June 1987

The following news snippet was found in the Australian "The Age", June 26 1987 - from R. W. Pedder, (Commander RN, retd.) The recent abortion case in Melbourne has highlighted the ease by which illegal Information was obtained by the police from the Health Commission. The fact that it was obtained should sound a note of warning to all those interested in freedom. The introduction of the Australian Identity Card would increase the risk that confidential information might be transmitted to those not authorised to receive it. No computer Is safe from any person with the knowledge and desire to breach its security no matter how many times Dr Blewett assures us it is. The real reason for the introduction of the card is to give the Hawke Government the power to oversee and control the lives of ordinary people, not to winkle out dole cheats and tax evaders (there are many other ways that can be done) It would do well to remember that Hitler gave himself the same power and the Jewish Holocaust was the result. George Santayana wrote: "Those who cannot remember the past are condemned to fulfil it". Australians beware. Read the story here: GoogleArchives

Ever heard of Deepfake?

Wikipedia describe deepfakes as follows: "Deepfakes (a portmanteau of "deep learning" and "fake") are synthetic media in which a person in an existing image or video is replaced with someone else's likeness. While the act of faking content is not new, deepfakes leverage powerful techniques from machine learning and artificial intelligence to manipulate or generate visual and audio content with a high potential to deceive. The main machine learning methods used to create deepfakes are based on deep learning and involve training generative neural network architectures, such as autoencoders or generative adversarial networks (GANs)". Sounds ominous right? Professor of electrical engineering at the University of California, Los Angeles, John Villasenor, said "Anybody who has a computer and access to the internet can technically produce a "deepfake" video". "The technology can be used to make people believe something is real when it is not," said Peter Singer, cybersecurity and defense focused strategist and senior fellow at the New America think tank. A CNBC article by Grace Shao describes the phenomena of deefakes in an easy to understand non-technical way. Below is a shortened and adapted version of Grace's article. (I challenge you all to Google some deepfake videos, its quite incredible)

Camera apps have become increasingly sophisticated. Users can elongate legs, remove pimples, add on animal ears and now, some can even create false videos that look very real. The technology used to create such digital content has quickly become accessible to the masses, and they are called "deepfakes." Deepfakes refer to manipulated videos, or other digital representations produced by sophisticated artificial intelligence, that yield fabricated images and sounds that appear to be real.

Such videos are "becoming increasingly sophisticated and accessible," wrote John Villasenor, non-resident senior fellow of governance studies at the Center for Technology Innovation at Washington-based public policy organization, the Brookings Institution. "Deepfakes are raising a set of challenging policy, technology, and legal issues." In fact, anybody who has a computer and access to the internet can technically produce deepfake content, said Villasenor, who is also a professor of electrical engineering at the University of California, Los Angeles.

What are deepfakes?

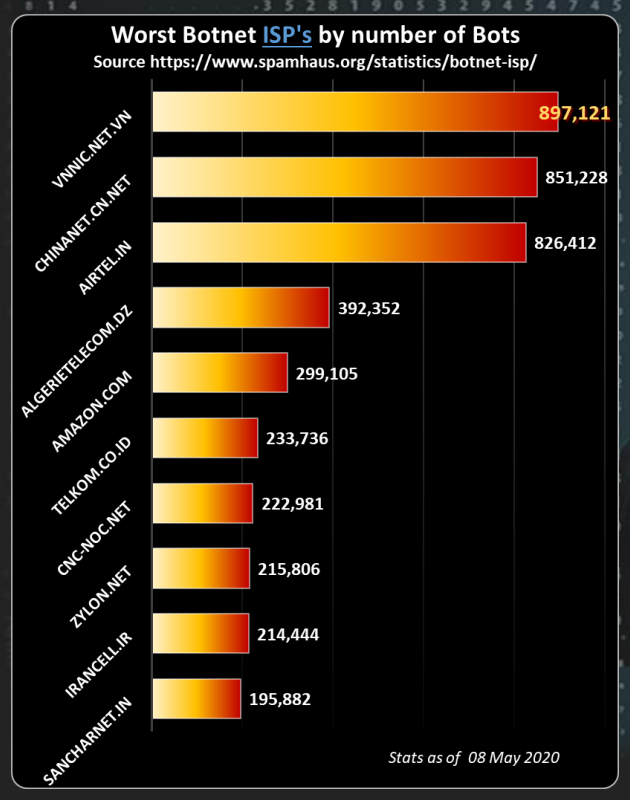
The word deepfake combines the terms "deep learning" and "fake," and is a form of artificial intelligence. In simplistic terms, deepfakes are falsified videos made by means of deep learning, said Paul Barrett, adjunct professor of law at New York University. Deep learning is "a subset of AI," and refers to arrangements of algorithms that can learn and make intelligent decisions on their own. But, as stated earlier by Peter Singer, the danger of that is "the technology can be used to make people believe something is real when it is not," Singer is not the only one who's warned of the dangers of deepfakes. Villasenor told CNBC the technology "can be used to undermine the reputation of a political candidate by making the candidate appear to say or do things that never actually occurred." "They are a powerful new tool for those who might want to (use) misinformation to influence an election," said Villasenor.

How do deepfakes work?

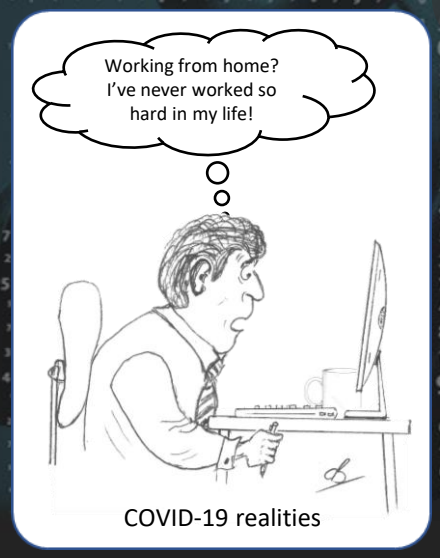
A deep-learning system can produce a persuasive counterfeit by studying photographs and videos of a target person from multiple angles, and then mimicking its behaviour and speech patterns. Barrett explained that "once a preliminary fake has been produced, a method known as GANs, or generative adversarial networks, makes it more believable. The GANs process seeks to detect flaws in the forgery, leading to improvements addressing the flaws." And after multiple rounds of detection and improvement, the deepfake video is completed, said the professor.
According to a MIT technology report, a device that enables deepfakes can be "a perfect weapon for purveyors of fake news who want to influence everything from stock prices to elections." In fact, "AI tools are already being used to put pictures of other people's faces on the bodies of porn stars and put words in the mouths of politicians," wrote Martin Giles, San Francisco bureau chief of MIT Technology Review in a report. He said GANs didn't create this problem, but they'll make it worse.

How to detect manipulated videos?

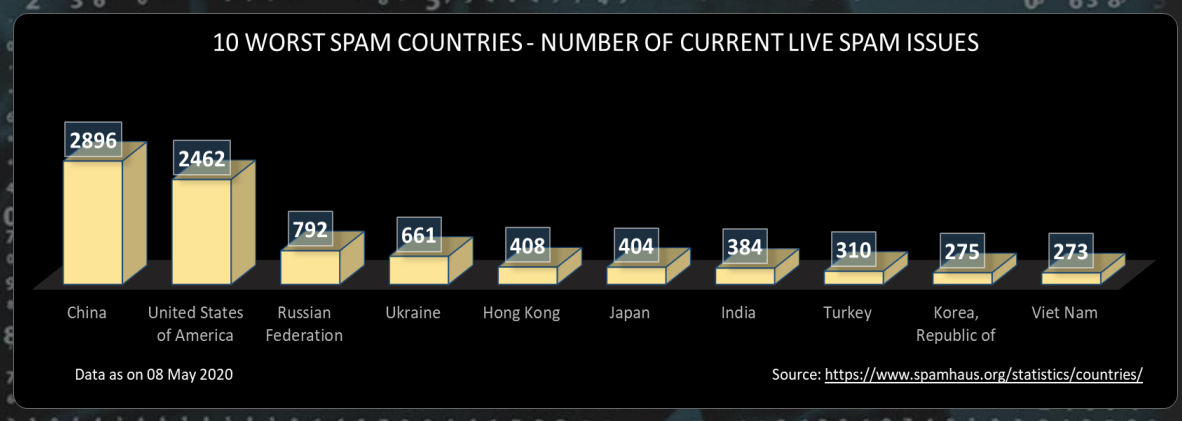
While AI can be used to make deepfakes, it can also be used to detect them, Brookings' Villasenor wrote in February. With the technology becoming accessible to any computer user, more and more researchers are focusing on deepfake detection and looking for a way of regulating it.
Large corporations such as Facebook and Microsoft have taken initiatives to detect and remove deepfake videos. The two companies announced earlier this year that they will be collaborating with top universities across the U.S. to create a large database of fake videos for research, according to Reuters.
"Presently, there are slight visual aspects that are off if you look closer, anything from the ears or eyes not matching to fuzzy borders of the face or too smooth skin to lighting and shadows," said Singer from New America.
But he said that detecting the "tells" is getting harder and harder as the deepfake technology becomes more advanced and videos look more realistic.
Even as the technology continues to evolve, Villasenor warned that detection techniques "often lag behind the most advanced creation methods." So the better question is: "Will people be more likely to believe a deepfake or a detection algorithm that flags the video as fabricated?"



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



COVID-19 realities



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