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

On March 31, the Cyber Threat Alert Level was evaluated and is being lowered to Blue (Guarded). The MS-ISAC is still observing exploitation attempts of critical vulnerabilities in versions of Microsoft Exchange servers.

Covid-19 Global Stats

Date	Confirmed Cases	Deaths
02-Apr	130,186,556	2,840,296

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

02 April 2021

In The News This Week

Child tweets gibberish from US nuclear-agency account

A young child inadvertently sparked confusion over the weekend by posting an unintelligible tweet to the official account of US Strategic Command. The agency is responsible for safeguarding America's nuclear weapons. Some social-media users feared the account may have been hacked. But it has since been revealed a young member of the account's social-media manager's family was responsible for posting the tweet, ";l;;gmlxzssaw", which was then deleted within minutes.. Read more here: BBC, ZDNet

SolarWinds Experimenting With New Software Build System in Wake of Breach

SolarWinds is experimenting with a completely new software build process that CEO Sudhakar Ramakrishna says is designed to ensure much better security against intrusions of the sort that the company disclosed last December. In addition, SolarWinds' CISO has been given full autonomy to stop product releases from happening purely due to time-to-market reasons. A new committee for cybersecurity has also been established at the board level, which includes the CEO and two CIOs, Ramakrishna said in comments during a virtual panel discussion this week involving security leaders from multiple organizations.. Read the full article by Jai Vijayan here: Darkreading

Insurance Giant CNA Hit with Novel Ransomware Attack

The incident, which forced the company to disconnect its systems, caused significant business disruption. A novel ransomware attack forced insurance giant CNA to take systems offline and temporarily shutter its website. The attack occurred earlier this week and leveraged a new variant of the Phoenix CryptoLocker malware. The Chicago-based company - the seventh largest commercial insurance provider in the world - said it "sustained a sophisticated cybersecurity attack" on Sunday, March 21. "The attack caused a network disruption and impacted certain CNA systems, including corporate email" Though the company did not elaborate on the nature of the attack, a report in BleepingComputer said CNA was the victim of a new ransomware called Phoenix CryptoLocker. Cryptolockers are an oft-used type of ransomware that immediately encrypt files on the machines they attack and demand a ransom from the victims in exchange for the key to unlocking them.

Read the full article here: ThreatPost

Brown University disconnects & shuts down data center amid cybersecurity threat

Brown University has shut off its data center while it deals with a cybersecurity threat. According to an alert posted Tuesday at 2pm local time, a threat to the Providence, Rhode Island University's 'Microsoft Windows-based technology infrastructure' led to the company shutting down connections to its facility. "Given the nature of the threat, CIS has taken a number of aggressive steps to protect the University's digital resources, including shutting down connections to our central data center and systems within it," said Bill Thirsk, Chief Digital Officer and Chief Information Officer at Brown University. "We are working with colleagues across the University and are committed to getting systems back online as quickly as possible." Read more here: DatacenterDynamics, BrownDaily

Panasonic, McAfee team up to tackle vehicle cybersecurity

Panasonic and McAfee are joining forces to establish a vehicle security operations center (SOC) to tackle the ongoing threat of cyberattacks. Announced on Tuesday, the new partnership involves both companies jointly creating an SOC to "commercialize vehicle security monitoring services," with a specific focus on early detection and response. Smart and intelligent vehicle features, now becoming more common in new models, require connectivity. This is usually established through Bluetooth and internet connections, which -- unless properly protected -- can also give attackers a chance to establish a foothold into a vehicle's system. In addition, software vulnerabilities can also be exploited to tamper with a car's functionality. While everything from machine learning-based driver assistance, maps, and entertainment apps are being developed in the automotive industry to appeal to modern drivers, cybersecurity is not necessarily being given the same attention -- a gap Panasonic and McAfee aim to plug. This isn't Panasonic's first rodeo in vehicle-based cybersecurity. The company has already developed an automotive intrusion detection system, which can be mounted on a car, to scan for evidence of suspicious activities or cyberattack attempts… Read the story by Charlie Osborne here: ZDNet

Liveness?

If it comes to Biometric authentication, whether it is for opening your phone, accessing a computer or for physical access control, how accurate or reliable is it? How does the facial recognition system know it is not presented with a photograph or artificial face? How does the fingerprint scanner know it is not scanning a fake silicon copy? Well, the authentication system needs to be able to determine/recognize whether the biometric subject (person) is alive and whether the biometric subject is actually the unique subject it claims to be.

This is where the artificial intelligence (AI) part comes in and is called "Liveness" detection. (Note, the word is "Liveness", not "Liveliness"). The term was first coined by Professor Emeritus Dorothy E. Denning in her 2001 Information Security Magazine Article: It's "liveness," not secrecy, that counts. In her paper she states, "*What makes biometrics successful is not secrecy, but rather the ability to determine "liveness." I can easily distinguish the living, flesh-and-blood you from a statue or photograph of you, or even someone wearing a costume and mask that looks like you. If I don't know you well, I might be fooled by a lookalike, but in the non-Mission Impossible real world, the system generally works. If I don't know you at all, I might ask for a photo ID. But I would use such a photo only because I lack knowledge of your appearance. I authenticate you by comparing your live face against the photo, not by comparing one photo against another. For further proof, I may watch you sign your name and compare the live signature against the one on your ID card. The same principle applies in the digital world. Your biometric prints need not be kept secret, but the validation process must check for liveness of the readings*." She also states, "*This is the beauty of biometrics. Other forms of user authentication, including passwords, tokens, and encryption, all depend on protecting a secret or device from theft. Once that secret or device is compromised, the system fails until a new one is established. Moreover, these methods typically require users to hold a different secret with each and every device or service they use, thereby burdening the user. Imagine if every time you greeted a friend or colleague, you had to provide a different secret password*! "

Detecting "Liveness" is the real challenge that a digital biometric system needs to solve. How does it work? Let's roll back in history for a moment. In 1950, the British mathematician, Alan Turing set the principle still applied today when he developed the famous "Turing Test", documented in his paper "Computing Machinery And Intelligence". The "Turing Test" measures a computer's ability to exhibit human-like behavior. Conversely, Liveness Detection is Artificial Intelligence (AI) that determines if a computer is interacting with a living human being.

Bad actors are constantly trying to circumvent or outwit biometric authentication systems for whatever sinister motive they have. They do this by presenting the biometric sensor with fake "data" or a non-living object that exhibits human traits (an "artifact"), like a photograph instead of a real face in front of a camera or a false silicone fingerprint, etc. This is called biometric spoofing.

In her paper, "Presentations and Attacks, and Spoofs, Oh My", Stephanie Shuckers call this "Presentation Attacks", the term that is mostly used today. Liveness detection is then to enable more accurate Presentation Attack Detection (PAD)

Liveness Detection prevents criminals or any other bad actor from using stolen photos, deepfake videos, masks, or other spoofs to create or access online accounts, or enter an access-controlled facility, and so on. Liveness ensures only real living humans can pass the biometric authentication test.

How does it work? Examples of some types of modern biometric authentication that rely on Liveness detection:

Fingerprint - Fingerprint recognition is widely considered to be one of the oldest and most developed types of biometric recognition. Fingerprints are easy to capture and can be verified by comparing the unique loops, arches, and whorls in each pattern. After capturing the print, sophisticated algorithms use the image to produce a unique digital biometric template. The template is then compared to new or existing scans to either confirm or deny a match. Liveness detection methods include hardware build-in measurements like pulse oximetry, electrocardiogram, and even odor. Enhanced software algorithms will analyse perspiration-based features and sweat content. Multimodal scanners can also combine finger vein imaging (See the vascular section below).

Facial Recognition - Facial recognition software measures the geometry of the face, including the distance between the eyes, the distance from the chin to the forehead, and multiple other points on a person's face. After collecting the data, an advanced algorithm transforms it into an encrypted facial signature. Liveness detection in facial recognition relies on enhanced AI algorithms to analyse the data received from highly sensitive cameras and imaging sensors. This includes thermal imaging where first of all body temperature or the lack of it is detected. Secondly, the slight temperature variations when breathing in and out can be analysed.

Iris Recognition - In the human eye, the iris is the coloured portion in the shape of a ring. If you look closely, you will find it is made of many asymmetric thick thread-like structures. These thread-like structures are the muscles that help adjust the shape of the pupil and only allow the appropriate amount of light in the eye. By measuring the unique folds of these muscles, biometric authentication tools can confirm identity with incredible accuracy. Liveness detection measures include blinking and the "hippus movement" (the constant shifting and pulse that takes place in the eye) which are analysed with AI technology to determine if the subject is alive and present.

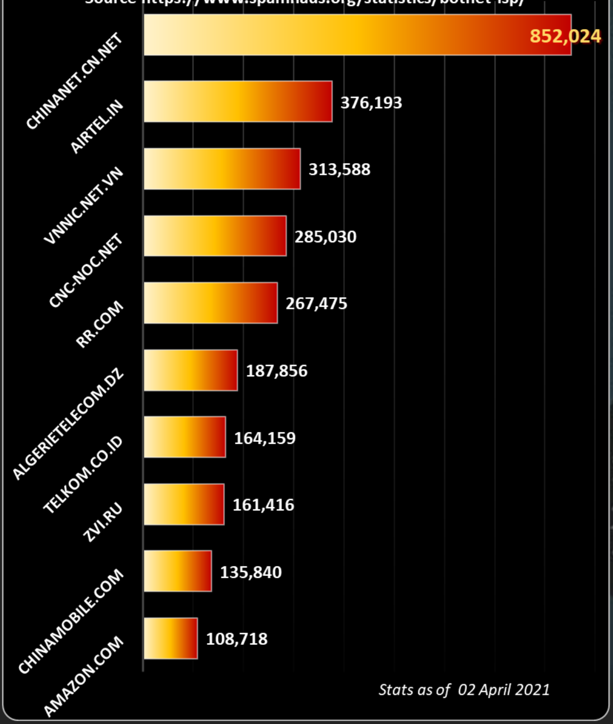
Retina Scan - Retinal scans capture capillaries deep within the eye by using unique near-infrared cameras. The raw image is first pre-processed to enhance the image then processed again as a biometric template to use during both enrolment and verification. Liveness detection includes things like retinal mood vasculature pattern matching.

Vascular - Vascular biometrics are a relatively new form of biometric authentication. It identifies an individual using the vein pattern inside one's fingers or palms. Vascular scanners such as a finger vein scanner or palm vein scanner utilize near-infrared lights combined with a special camera to capture vein patterns.

References: Liveness, Dorothy E. Denning, Alan Turing, Stephanie Shuckers, NICE, Thales, Odin Program, ISO/IEC 30107, Facetec

Worst Botnet ISP's by number of Bots

Source https://www.spamhaus.org/statistics/botnet-isp/



Stats as of 02 April 2021

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

Don't let security fall through the cracks this weekend

Other Interesting News and Cyber Security bits:

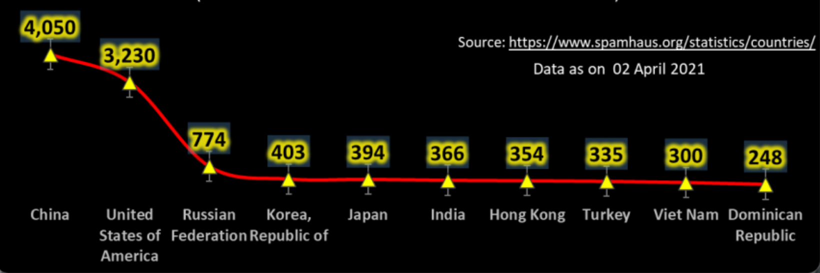
- The race to secure 5G
- How Next-Generation Endpoint Security Is Different from Traditional Endpoint Security
- **Automotive - With the advent of onboard HPC, how will auto cyber security develop?**

THE WORLD'S WORST SPAM HAVEN COUNTRIES FOR ENABLING SPAMMING

(TOP 10 BY NUMBER OF CURRENT LIVE SPAM ISSUES)

Source: https://www.spamhaus.org/statistics/countries/

Data as on 02 April 2021



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