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

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. (Unchanged from last week)

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

06 March 2020

In The News This Week

Hackers Can Use Ultrasonic Waves to Secretly Control Voice Assistant Devices

Researchers have discovered a new means to target voice-controlled devices by propagating ultrasonic waves through solid materials in order to interact with and compromise them using inaudible voice commands without the victims' knowledge. Called "SurfingAttack," the attack leverages the unique properties of acoustic transmission in solid materials — such as tables — to "enable multiple rounds of interactions between the voice-controlled device and the attacker over a longer distance and without the need to be in line-of-sight." In doing so, it's possible for an attacker to interact with the devices using the voice assistants, hijack SMS two-factor authentication codes, and even place fraudulent calls, the researchers outlined in the paper, thus controlling the victim device inconspicuously. The research was published by a group of academics from Michigan State University, Washington University in St. Louis, Chinese Academy of Sciences, and the University of Nebraska-Lincoin.

Read the full story and how it works here: The Hacker News

Guy who named 'BlueKeep' Windows flaw joins Microsoft Threat Protection

Microsoft gains a cybersecurity expert who thinks too much snake oil is being sold by cybersecurity vendors. Kevin Beaumont, the UK cybersecurity expert who named the wormable Windows BlueKeep bug, is joining Microsoft Threat Protection. Beaumont, a widely quoted security expert who's run large security operations centers, has offered insights from the trenches into new attacks via his popular DoublePulsar blog and Twitter for the past few years, covering issues including WannaCry, NSA exploits, the rise of malicious Office macros, and BlueKeep. The move to Microsoft Threat Protection, which is responsible for Microsoft Defender antivirus, is notable in part because Beaumont has been "largely suspect" of cybersecurity vendors and "occasionally critical of Microsoft".

Read the full story here: ZDNet Article(1)

World Health Organisation issues warning over new coronavirus scam

Criminals are disguising themselves as health officials to steal money and sensitive information amid the coronavirus outbreak, the World Health Organisation (WHO) has said. Cyber criminals are using a type of fraud called phishing to take advantage of fears caused by the virus, which has reached more than 90,000 confirmed cases worldwide. The global health agency said anyone contacted by a person or organisation that appears to be from WHO should verify if they are authentic before responding. WHO said it is aware of a number of suspicious email messages "attempting to take advantage" of the coronavirus outbreak.. Read more here: Yahoo

Let's Encrypt revoke 3 million certificates on March 4 due to software bug

Let's Encrypt issued 3,048,289 TLS certificates without checking the CAA field for the requesting domain. The Let's Encrypt project will revoke more than 3 million TLS certificates on Wednesday, March 4, 2020, due to a bug it discovered in its backends' code. More specifically, the bug impacted Boulder, the server software the Let's Encrypt project uses to verify users and their domains before issuing a TLS certificate. The bug impacted the implementation of the CAA (Certificate Authority Authorization) specification inside Boulder. CAA is a security standard that was approved in 2017 and which allows domain owners to prevent Certificate Authorities (CAs; organizations that issue TLS certificates) to issue certificates for their domains. Domain owners can add a "CAA field" to their domain's DNS records, and only the CA listed in the CAA field can issue a TLS certificate for that domain. All Certificate Authorities -- like Let's Encrypt -- must follow the CAA specification by the letter of the law or face steep penalties from browser makers. In a forum post on Saturday, February 29, the Let's Encrypt project disclosed that a bug in Boulder ignored CAA checks. Read the full story here: ZDNet

Medical Devices and Cybersecurity

This week the U.S. Food and Drug Administration (FDA) informed patients, health care providers and manufacturers about a set of cybersecurity vulnerabilities, referred to as "SweynTooth," that – if exploited - may introduce risks for certain medical devices. (FDA Announcement) This prompted me to look a bit deeper into the subject.

Connected healthcare devices are developing rapidly and in this technology age and the so called 4th Industrial revolution where boundaries between the physical, digital, and biological worlds are fizzling out, our medical treatment options are expanding exponentially. We are talking about medical devices that are pushing these boundaries to the extreme and it ranges from the more common pacemakers and insulin pens to ambitious projects like medical smart contact lenses that can potentially prevent diseases like glaucoma and so on. The point, however, is that they are all somehow connected to the web or some near-field communication enabled devices, and if it is connected, it can be hacked. To expand on that, I've included the article below that were published by the FDA as a general guideline on the subject.

Medical Device Cybersecurity: What You Need to Know

Pacemakers, insulin pumps and other medical devices are becoming more advanced. Most contain software and connect to the internet, hospital networks, your mobile phone, or other devices to share information. So, it is important to make sure medical devices are cyber secure. New technologies are being applied to all different types of devices—those that are implantable or wearable, or used at home or in health care settings. The advances can offer care that is safer, timelier and more convenient. For example, patients with an implanted heart device can be monitored remotely and possibly spared a visit to the doctor's office. People with diabetes have new options for managing their blood-sugar levels because some glucose meters and insulin pumps can essentially talk to each other. And hospitals aiming to improve care and efficiency are using more pieces of equipment that are networked together to share data.

Anytime a medical device has software and relies on a wireless or wired connection, vigilance is required. The software behind these products, like all technologies, can become vulnerable to cyber threats, especially if the device is older and was not built with cybersecurity in mind.

FDA's Role in Keeping Medical Devices Cyber Secure

The U.S. Food and Administration (FDA) regulates medical devices and works aggressively to reduce cybersecurity risks in what is a rapidly changing environment. It is a responsibility the Agency shares with device makers, hospitals, health care providers, patients, security researchers, and other government agencies, including the U.S. Department of Homeland Security and U.S. Department of Commerce.

The FDA provides guidance to help manufacturers design and maintain products that are cyber secure. And on behalf of patients, the FDA urges manufacturers to monitor and assess cybersecurity vulnerability risks, and to be proactive about disclosing vulnerabilities and solutions to address them.

If a weakness in software that could pose a risk is identified, the FDA may issue what is called a "safety communication." These messages contain information about the vulnerability and recommended actions patients, providers and manufacturers can take. Nine cyber safety communications have been issued since 2013. The FDA wants to make these messages as helpful as possible without causing unnecessary worry or burden on patients.

Patients Can be Active Participants in Keeping Their Devices Safe

Medical devices are intended to improve health and help people live longer, healthier lives. Patients should feel assured about the safety and security of their medical devices, knowing the FDA is being proactive and working with manufacturers throughout the entire lifecycle of a product. Patients and caregivers can also play a critical role. Consider the following tips:

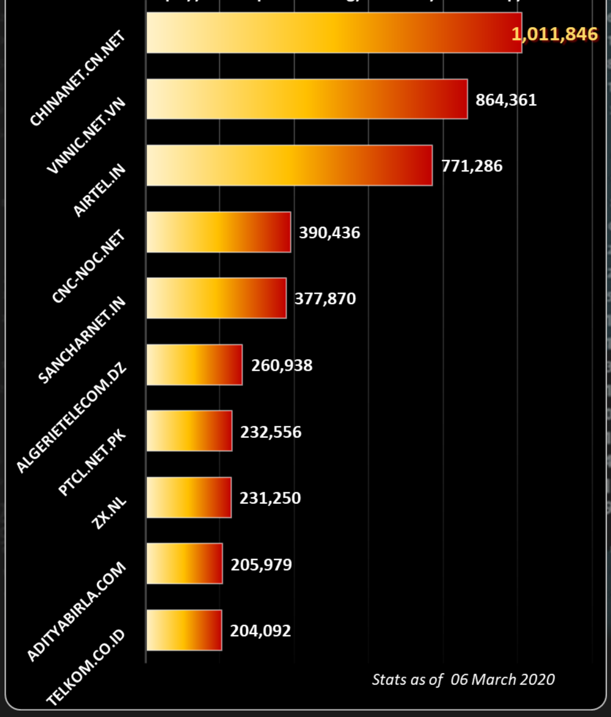
- Technology evolves over time, so software will need to be updated. Recognize the value of applying those updates and talk with your health care provider if you have any questions about them.
- Register your device with the manufacturer. It is an extra step, but it may help the manufacturer reach you more quickly to send you important information.
- Be observant and vigilant. If you think your device is not functioning as it should, do not ignore it. Discuss it with your health care provider. Notify the device manufacturer and report it to the FDA's MedWatch.
- Involve your family or caregivers. Educate them about your device or enlist their help if you are not tech savvy.
- If there is a serious event, seek medical attention.

For more resources about medical device cybersecurity visit FDA.gov, or contact DICE or mailto:CyberMed@fda.hhs.gov

In Europe contact European Health Management Association and In other countries, please consult your local Health Care Authority for more information.

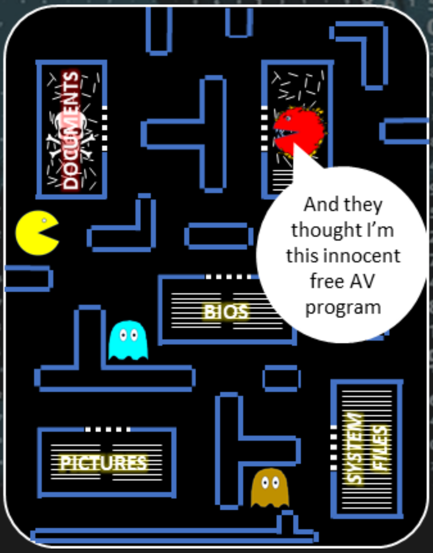
Worst Botnet ISP's by number of Bots

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



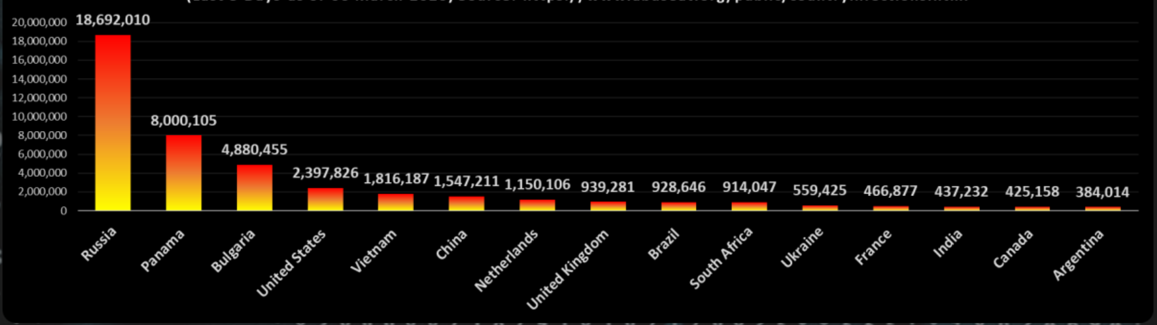
Stats as of 06 March 2020

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



Composite Blocking List (CBL) - Number SPAM emails trapped - Top 15 Countries

(Last 3 Days-as of 06 March 2020) Source: https://www.abuseat.org/public/countryinfections.html



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