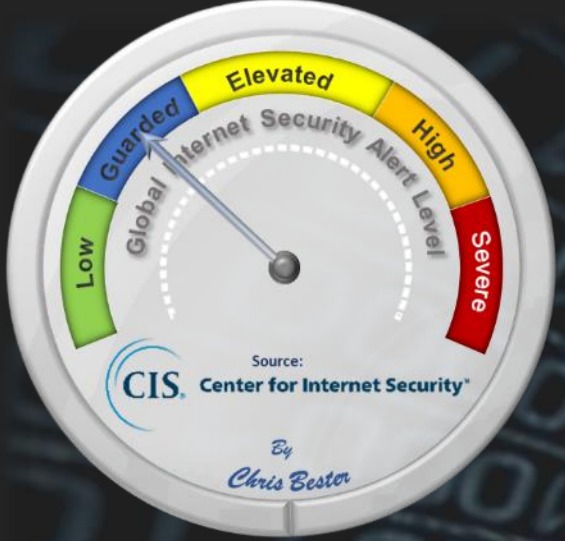

Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

On May 20, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Palo Alto, PHP 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

22 May 2020

In The News This Week

Supercomputers across Europe hacked to mine cryptocurrency

Compromised SSH credentials allowed a criminal group to install malware on multiple supercomputers. - Multiple supercomputer clusters across Europe have been breached and used by hackers to mine cryptocurrency. According to a ZDNet report, researchers from facilities in Germany, Switzerland, the UK and Spain have all reported intrusions. The process of "mining" sees individuals or groups compete to solve advanced mathematical puzzle, with a quantity of cryptocurrency awarded to the successful party. The process is compute-intensive, which means the more powerful the hardware the more likely the miner to receive a cryptocurrency reward - which makes supercomputers a prime target for hacking attempts. The University of Edinburgh, which runs the ARCHER supercomputer, was the first to notify the public of the breach. Soon after, five supercomputing clusters in Germany were forced offline for the same reason, followed by a supercomputer in Barcelona.

Read the full story here: ITProPortal

Hacker behind largest-ever data heist arrested in Ukraine

Ukrainian authorities have arrested a hacker accused of orchestrating one of the biggest data leaks in history. The man, only known as Sanix, allegedly publicized a database with over 700 million email addresses, digital currency wallet credentials and other personal data. The Security Service of Ukraine (SBU) arrested the hacker, acting on a tip that he resided in Ivano-Frankivsk, a region in Western Ukraine. Authorities raided his house, arrested him and seized computers that had 2 terabytes worth of stolen data. They also seized phones and over $10,000 in cash. Sanix now faces charges of unauthorized interference with computers and unauthorized sale of information. If convicted of both, he faces up to eight years in prison. Sanix grabbed headlines in January 2019 after he released what came to be known as Collection #1, a database containing over 772 million unique email addresses. According to security researcher Troy Hunt, Sanix published the data on a popular hacking forum. He also made it available briefly on the MEGA cloud service. He claimed that he had aggregated over 2,000 leaked databases to compile Collection #1. Read the full article here: CoinGeek

New Bluetooth Vulnerability Exposes Billions of Devices to Hackers

Academics from École Polytechnique Fédérale de Lausanne (EPFL) disclosed a security vulnerability in Bluetooth that could potentially allow an attacker to spoof a remotely paired device, exposing over a billion of modern devices to hackers. The attacks, dubbed Bluetooth Impersonation Attacks or BIAS, concern Bluetooth Classic, which supports Basic Rate (BR) and Enhanced Data Rate (EDR) for wireless data transfer between devices. "The Bluetooth specification contains vulnerabilities enabling to perform impersonation attacks during secure connection establishment," the researchers outlined in the paper. "Such vulnerabilities include the lack of mandatory mutual authentication, overly permissive role switching, and an authentication procedure downgrade." Given the widespread impact of the vulnerability, the researchers said they responsibly disclosed the findings to the Bluetooth Special Interest Group (SIG), the organization that oversees the development of Bluetooth standards, in December 2019. Read the full story here: TheHackerNews

8 Million customer records stolen in hack of meal kit delivery service Home Chef

Meal kit delivery service Home Chef is the latest company to suffer a data breach, with the details of some 8 million customers stolen. The hack was not detected by the company but only came to light after stolen customer records from the company were offered for sale on the dark web, a shady part of the internet reachable with special software. The stolen data includes email addresses, encrypted passwords, the last four digits of credit cards, gender, age, subscription information and more.

Read the story here: SiliconAngle

Cyber Range – What is it, what is it used for and who is using it?

It is basically like a Shooting Range where soldiers get trained how to identify and shoot at a specific target and can do it over and over and over again until they perfect their skill and become an excellent marksman or even a sniper.

Now with that picture in mind, a Cyber Range is a controlled virtual cyber or IT environment where, cyber security students or professionals can be trained or hone their skills to perfection to defend their respective environments against cybercrime targets. The Cyber Range is isolated from your corporate or other computing environments, and is normally a repairable environment meaning, if they break it, they can easily roll back and start it up again, and again, and again…

It is a perfect environment where cyber security experts can simulate cyber attacks and learn how to respond to various complicated and highly treacherous cyber threats. It is also a perfect environment to dissect reigning attacks and develop or build proactive controls to defend against them in future.

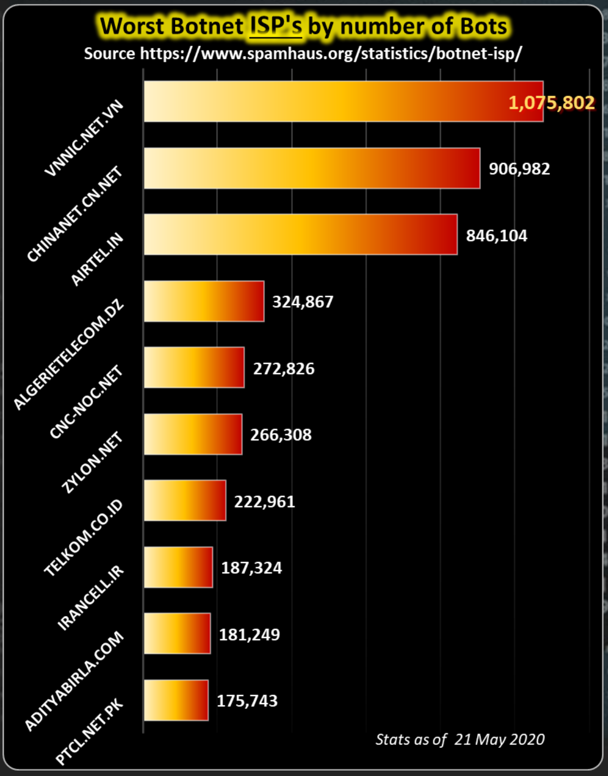
Cyber Ranges were traditionally a costly setup and almost exclusively used by the military and other state security organisations. Some large private organisations who could afford it also built their own inhouse Cyber Ranges.

Nowadays however, there is a Cyber Range around each proverbial corner hiring out their services and due to the number of them around brought to price down and in reach of medium to large organisations who do not previously had a budget to do so. I did a quick Google scan and it seems that there is a number of Cyber Ranges to choose from in most of the developed countries. As I traversed through the net, I came across an article written by in the Government Technology Magazine (gt) by Dan Lohrmann - Chief Security Officer & Chief Strategist at Security Mentor Inc., interviewing two seasoned professionals and Cyber Range experts, which I thought would be of interest for those who want to dig a little deeper into the subject. Below is just a short extract of the interview just to wet your appetite. Feel free to visit the govtech website to read the full interview.

Digging Deeper on Cyber Ranges with Dr. Joe Adams and Jason Brown from Merit Network
So why is this happening now? What is so special about these cyber ranges?

To answer this question, Dan turned to two experts in the field who eat, breath and live in (or near) cyber ranges. Dr. Joe Adams is the vice president of research and the director of the Michigan Cyber Range. He joined Merit Network in 2012 after a very successful military career, including CIO of the National Defense University. Jason Brown is the chief information security officer at Merit, and a former security architect for the state of Michigan government.
"I have known and worked with both Joe and Jason for many years, and they are both outstanding security professionals who are very well respected throughout the security industry. Their thought leadership and expertise has propelled the Michigan Cyber Range to international prominence over the past several years."

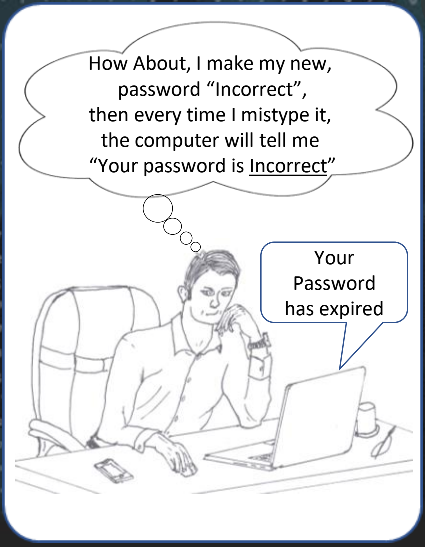
Here's a short extract of Dan's interview:
Dan Lohrmann (DL): Are you seeing an uptick in interest and involvement in cyber ranges?
Dr. Joe Adams (JA): Definitely. As we develop content applicable to more and varied sectors of the prospective workforce, more organizations (i.e., government, academic and commercial) step forward to become involved. The Michigan Cyber Range has contributed to a variety of projects in conjunction with the state of Michigan and others that involved high school students, unemployed veterans and employers seeking to attract and retain talent.
Not only are the organizations that generate qualified cyber workers interested in cyber ranges, but manufacturers are recognizing that the concepts of constant connectivity, autonomy, and all the other aspects of the Internet of Things make cyber-trained employees necessary.
DL: In what areas are clients most interested? (Does this include public and private sector or mainly government-only?)
JA: There are two main lines of effort. The first is by states and government entities who are seeking workforce development and skills training. Prompted by the gap between trained cyber workers and open cyber positions, these entities want to improve the skills of the existing workforce, while also making their state attractive to organizations that are seeking to move to locations with a workforce. The Michigan Cyber Range is an example of this kind of range.
The second line of effort is being pursued by universities and academic organizations for the purposes of expanding their programs and attract students. These ranges can be differentiated from the workforce training ranges in that they service enrolled students of an academic institution and rarely, if ever, seek to provide certification training to those students. Instead, these ranges focus on educational experiences that contribute to a student's academic experience. The Information Warfare lab, known as IWAR, at the U.S. Military Academy at West Point is an example of this kind of range.
If you read the EdScoop article mentioned earlier, the "ranges" at Regents and University of West Florida fall into the second category as well. They're basically classrooms and buildings with a closed network for cyber courses.
DL: Why do you think cyber ranges are growing in popularity now?
JA: I think we're seeing the results of the work done by [the National Institute of Standards and Technology] through the [National Initiative for Cybersecurity Education] program, the Cyberseek initiative, and other efforts. As they highlight the talent gap and, in my opinion more importantly, help define the KSAs [knowledge, skills and abilities] applicable to each job function in cybersecurity, they have cut through the media hype and vendor advertising to develop an effective workforce. …… read more

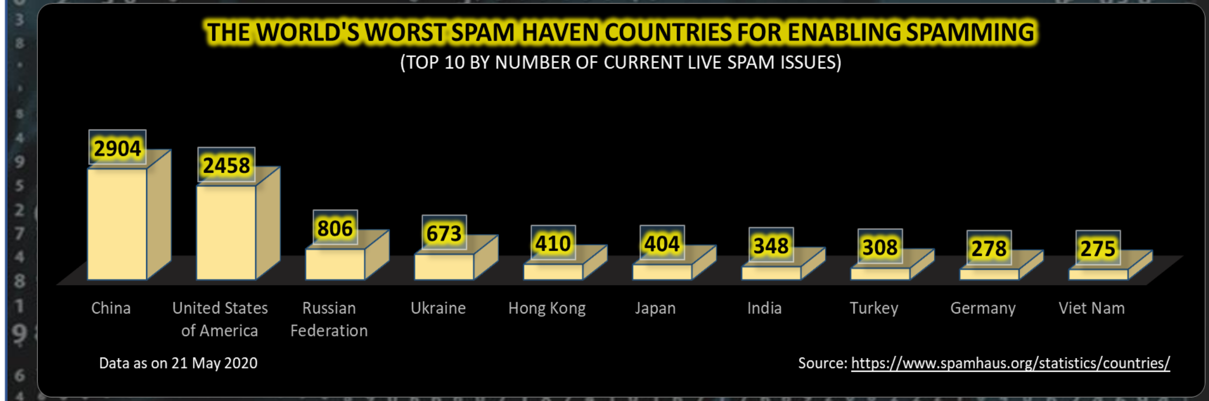

Worst Botnet ISP's by number of Bots
Source https://www.spamhaus.org/statistics/botnet-isp/

Stats as of 21 May 2020

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

(A big thank you to my good friend and Cyber Security specialist Yazan Shapsugh who inspired this week's cartoon with a WhatsApp message he sent)


How About, I make my new, password "Incorrect", then every time I mistype it, the computer will tell me "Your password is Incorrect"
Your Password has expired


THE WORLD'S WORST SPAM HAVEN COUNTRIES FOR ENABLING SPAMMING
(TOP 10 BY NUMBER OF CURRENT LIVE SPAM ISSUES)

Data as on 21 May 2020
Source: https://www.spamhaus.org/statistics/countries/

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