On May 12, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded). Advisory May 25 - Multiple Vulnerabilities in VMWare Products that Could Allow for Information Disclosure.

Covid-19 Global Stats

Date	Confirmed Cases	Total Deaths
28-May	169,623,439	3,525,023

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

28 May 2021

In The News This Week

Russian hackers target aid groups in new cyber-attack, says Microsoft

Microsoft says another wave of Russian cyber-attacks has targeted government agencies and human rights groups in 24 countries, most in the US. It said about 3,000 email accounts at more than 150 different organisations had been attacked this week. The group responsible was the same one that carried out last year's SolarWinds attacks, which Russia's Foreign Intelligence Service (SVR) is accused of orchestrating, Microsoft said. Russia has denied both cyber-attacks. Read the full story here: BBC News

Biden proposes billions to strengthen U.S. Cyber Security

Billions of dollars would be allocated to upgrade the nation's cybersecurity defenses and modernize networks should President Biden's $2 trillion infrastructure proposal to secure the nation's critical systems gain Congressional approval. The American Jobs Plan, as the White House has named the measure, would see funding directed to improve energy infrastructure at the state and local levels to secure the power grid, improve cyber defenses, update technology, expand broadband and other advances. "Cybersecurity is a core part of resilience and building infrastructure of the future, and the American Jobs Plan will allocate opportunities and resources to bolster cyber defenses," the White House said in a Fact Sheet outlining the proposal's basic elements. The Jobs Plan summary draft follows the President's executive order on cybersecurity of May 12, 2021.
Read the rest of the story here: MSSP Alert

Health Care and the Building Cyber-Security Crisis

Last week the Government Accountability Office published a report on cyber insurance, finding that demand for cyber insurance is growing in the health care industry. At the same time, however, "insurer appetite and capacity for underwriting cyber risk has contracted…especially in certain high-risk industry sectors such as health care." Increasing cyberattacks on health care companies paired with growing demand for expanded telehealth services mean that health care policy conversations will increasingly need to focus on data security. In late April, cancer treatments for some U.S. cancer patients were disrupted when the Swedish-based Elekta—a company that provides precision cancer radiation treatment systems—had to take down its cloud system amid a data breach.
Read the article by Christopher Holt here: American Action Forum

German cyber security chief fears hackers could target hospitals

German hospitals may be at increased risk from hackers, the head of the country's cyber security agency said on Saturday, following two high-profile digital attacks this month on the Irish health service and a U.S. fuel pipeline. Ireland's health service operator shut down its IT systems last Friday to protect them from a "significant" ransomware attack, crippling diagnostic services, disrupting COVID-19 testing and forcing the cancellation of many appointments. German clinics have been targeted by a series of cyber attacks over the last five years, and Arne Schoenbohm, president of the BSI federal cyber security agency, told Zeit Online newspaper he saw "a greater danger at hospitals". Read the story here: Reuters

Security company is now using drones to track criminals in South Africa's suburbs

Private security group Fidelity says it has become one of the first providers in South Africa to use drones to track criminals in suburban areas. The group said that the drones will first be trialled in the greater Fourways area for two months and then extended to other suburbs, estates and shopping centres. Wahl Bartmann, chief executive officer of the Fidelity Services Group, said that the offering consists of a mobile command centre with a qualified drone pilot and a fully equipped state-of-the-art drone. "The command centre is linked to a tactical response unit for both reactive and proactive purposes.
Read the full article here: BusinessTech

Raspberry Pi

Yesterday TechRepublic published a piece on the recent developments of the Raspberry Pi which reminded me that two years ago I reported in this bulletin how NASA was hacked using a simple Raspberry Pi. More recently, in November 2020, a Belgian researcher hacked Tesla with a Raspberry Pi. For those not familiar with a Raspberry Pi, it is a small single-board computer with enormous capabilities, developed in the UK and highly popular in IT and Robotics circles. Other than the Italian-based Arduino (Another popular single-board computer used in robotics), the Raspberry Pi is a full-fledged microprocessor computer where the Arduino is more a microcontroller. The Arduino is typically used in robotics where repetitive functions are the order of the day.
Today I just want to explore some developments in Raspberry Pi since I reported on the NASA hack and some projects where you can use it as a security tool.

First, let's talk about the physical and computing capabilities of these little fellas. It comes in a few models of which the 4 US Dollar Raspberry Pi Zero is the smallest (just a bit bigger than a stick of gum), up to the flagship Raspberry Pi 4 Model B. The Raspberry Pi 4 is a tiny dual-display single-board computer that retails at about $35 USD and literally fits in the palm of your hand. The recent addition of the Raspberry Pi 400, based on the Pi 4, but built into a compact keyboard, completes the line-up. That is only talking about the computing units though, a ton of Raspberry and third-party add-ons has been developed over the last few years which extends its capabilities immensely. You can explore the technical specs of the various models on their website but I'll just highlight a few specs of the Raspberry Pi 4 Model B.

The Raspberry Pi 4 Model B sport some of the following specs: A 1.5GHz Quad-core 64-bit CPU, Gigabit Ethernet, Blue Tooth, up to 8Gb SDRAM, 40 pin GPIO header, 4 x USB, 2 x HDMI, 40 pin GPIO header, MIPI CSI camera port, PoE, MicroSD slot, and so on.

As you can see, with specs like that, no wonder they could hack NASA with it, and that was with the older P3 model. With its Power over Ethernet (PoE) capability, it basically hanged undetected in a server rack, powered by the switch, for quite some time capturing and pumping out data to an outside entity.

Can you imagine the possibilities? Many retailers are reverting to use Raspberry Pi's as Point-of-Sale (POS) terminals to save cost. All you need is a Pi, a keyboard, a mouse, and a screen. An ex-colleague of mine built 3D printers in his spare time, with a Raspberry Pi to drive them. For my son's 11th birthday I bought him an Arduino Uno to start him off on basic robotics, going towards 13 he was begging me for a Raspberry Pi, guess what he got for his 13th birthday? Today, almost 2 years later and he is still smiling.

TechRepublic reports that "Raspberry Pi was one of the first companies to see the impact of the overnight shift to remote working in 2020. That's because households, which might have found one PC enough for a family in normal times, suddenly needed to meet the needs of multiple family members working and learning from home simultaneously." "Demand rocketed, and in March 2020, sales of Raspberry Pi devices hit 640,000, the second-biggest sales month in the company's history." A good alternative for homeschoolers where the most expensive part of the computer is the screen. You can probably have a good set-up for less than $100.

Now here is where the security and cyber side come into play. With the addition of the 12.3 megapixels Raspberry Pi High-Quality Camera and 8 megapixel Infra-Red camera modules and a plethora of available sensors, you can now build sophisticated security surveillance systems. A nice security project for the DIY home or small office owner and if you are brave enough include a more advanced feature like facial recognition. (See project here). You can even combine your security project with home automation.

From a Cyber Security perspective, why not use your Raspberry Pi to launch a pen-test. See this ethical hacking blog, to see how it is done.

Following are a few Raspberry Pi projects that you can delve into for fun.

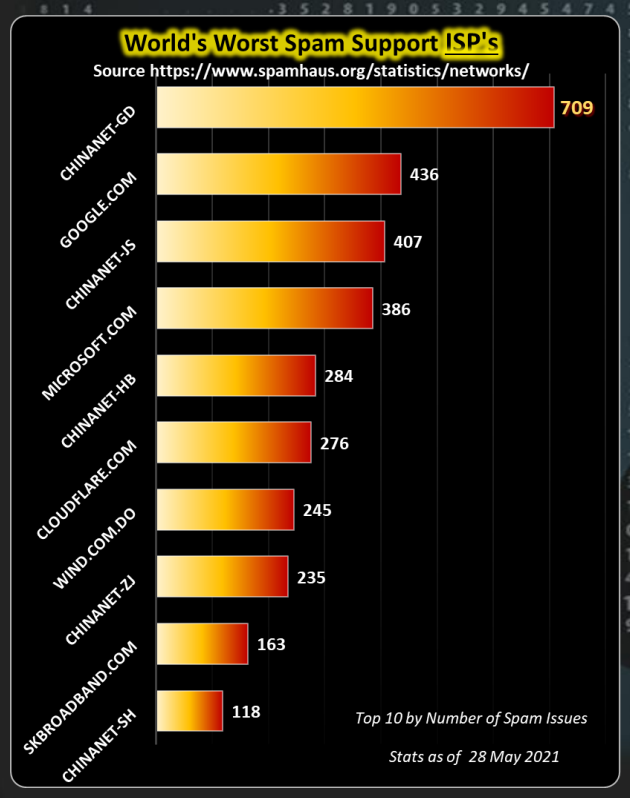
USB key sanitizer - If you work in security, you've probably had someone show up at your office with a questionable USB drive they want you to check out. (In fact, the "I found this USB drive" tactic is a classic red team war game scenario.) The Computer Incident Response Center in Luxembourg has released a tool that lets you safely and securely scan these questionable drives for malware and viruses. This is an excellent entry-level Raspberry Pi project with real-world applications that lets new users test the waters.

Network Scanner - We all need to know what devices are on our networks. For sites with sensitive information, such as financial services offices, it might be important to know when a new device signs on at the moment it joins the network. More advanced than many others, the Networkscan Raspberry Pi automatic network device scanner sends an alert to your phone if a new Bluetooth device is seen, or a new system joins your network.

Smart Home Security System - It is possible to design a simple home security solution by using Raspberry Pi and utilizing the power of IoT (Internet of Things)

That is all I have space for this week, but please follow the links to dive deeper into the Raspberry Pi world or discover all the alternatives that are out there.

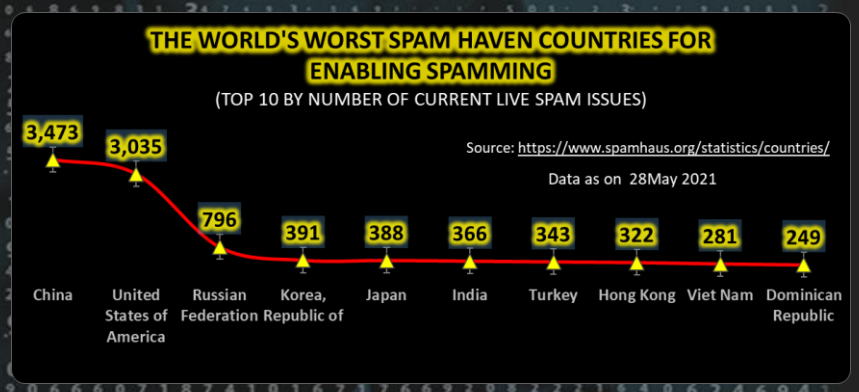
References: BBC News, Raspberry, TechRepublic, Engineers Garage, ITPro, Robotica DIY, Newegg Studios, Electronics Hub



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

Other Interesting News and Cyber Security bits:

- Cybersecurity in Vietnam has anything changed?
- Deepfake dubs could help translate film and TV without losing an actor's original performance
- Building Multi-layered Security for Modern Threats



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