On January 26, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google, Cisco, WordPress,.
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
28 Jan	366,953,855	5,657,105

Deaths this week: 63,459

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 January 2022

In The News This Week

FBI warns over Iranian cyber group, tells organizations to up their defenses

The FBI has issued an alert detailing the tools, techniques and tactics of an Iranian group, giving US organizations tips to defend against its malicious cyber activities. Back in October 2021, a grand jury in the US District Court for the Southern District of New York indicted two Iranian nationals employed by Emennet Pasargad for computer intrusion, computer fraud, voter intimidation, interstate threats, and conspiracy offenses for their alleged participation in a campaign aimed at influencing and interfering with the 2020 US Presidential Election.
Read the rest of the story by Liam Tung here: ZDNet

Millions of Routers, IoT Devices at Risk as Malware Source Code Surfaces on GitHub

The authors of a dangerous malware sample targeting millions of routers and Internet of Things (IoT) devices have uploaded its source code to GitHub, meaning other criminals can now quickly spin up new variants of the tool or use it as is, in their own attack campaigns. Researchers at AT&T Alien Labs first spotted the malware last November and named it "BotenaGo." The malware is written in Go — a programming language that has become quite popular among malware authors. It comes packed with exploits for more than 30 different vulnerabilities in products from multiple vendors, including Linksys, D-Link, Netgear, and ZTE. BotenaGo is designed to execute remote shell commands on systems where it has successfully exploited a vulnerability.
Read the rest of the article by Jai Vijayan here : DarkReading

White House attempts to strengthen federal cybersecurity after major hacks

The White House plans to release an ambitious strategy Wednesday to make federal agencies tighten their cybersecurity controls after a series of high-profile hacks against government and private infrastructure in the last two years, according to a copy shared with CNN. It's one of the biggest efforts yet by the Biden administration to secure the computer networks that the government relies on to do business. Under the strategy, federal employees will need to sign on to agency networks using multiple layers of security and agencies will have to do a better job of protecting their internal network traffic from hackers. The strategy gives agencies until the end of the 2024 fiscal year to meet these benchmarks and others. The overhaul was inspired in part by a 2020 spying campaign by alleged Russian hackers that infiltrated several US agencies and went undetected for months, leaving US officials frustrated at their blind spots… Read the story by Sean Lyngaas here: CNN

First ever Government Cyber Security Strategy to step up Britain's defence and resilience

Britain's public services will be strengthened to further protect them from the risk of being shut down by hostile cyber threats, Chancellor of the Duchy of Lancaster Steve Barclay will say today. The minister will outline the cyber threat that government and wider public sector systems face in a speech today, as he launches the first ever Government Cyber Security Strategy. In the speech in central London, Mr Barclay will say that Britain is now the third most targeted country in the world in cyberspace from hostile states. The new strategy will be backed by £37.8 million invested to help local authorities boost their cyber resilience - protecting the essential services and data on which citizens rely on including housing benefit, voter registration, electoral management, school grants and the provision of social care. Read the rest of the article here: Gov.UK

South Africa's new traffic fine system exposed personal data

An online interface set up for the Administrative Adjudication of Road Traffic Offences (Aarto) system exposed the personal information of every South African who received an infringement notice under the new law. Personal data contained in the leak included full names, ID numbers, residential or business addresses, phone numbers, vehicle registration information, and infringement details. An anonymous security researcher who is a regular user of the system informed MyBroadband about the data leak. They did not wish to approach the Aarto system operator directly, because the researcher was concerned that the new Cybercrimes Act and Protection of Personal Information Act could be used to prosecute them, despite their good intentions. The Aarto Act established new processes for handling traffic infringements in South Africa, including a demerit point system. Pretoria's High Court however, declared the new act unlawful and unconstitutional on Thursday, 13 January…
Read the rest of the article here: MyBroadband

CCTV and Surveillance Camera Considerations for the DIY Buff

As the world around us becomes more and more volatile from a safety and security perspective, the need for home security measures increased exponentially. The increase in demand however, meant that fees for security systems and services went up dramatically too. Security companies are charging exorbitant fees for home installations and, with the current state of inflation, many just can't afford it. Many therefore are considering or already decided to go the DIY (D0-it-Yourself) route. With the online-shopping revolution over the last two years, finding the equipment became so much easier and with lower price tags in tow, became the preferred option more and more. However, the overwhelming choice of products can be daunting and you just don't know if it is a quality product or not. So if you go this route, do your homework, rather go for known brand names than for that item that is ten times cheaper. Don't be tempted, there is normally a really good reason why these items are so cheap, and the reason is never positive. So, in today's post, I want to expand on the post I wrote in October last year, "DIY Home Surveillance over the Internet, what you need to know?" and talk more about equipment choices and what to look out for.

As I mentioned in the October post, planning is everything, before you even start looking at the physical components you need, or think you need, do your homework. Go to the proverbial drawing board and first jot down your budget, then what areas you want to cover, and the best placement for maximum visibility. Think of aesthetics, the perfect place for the camera might not be the perfect choice from an aesthetics point of view, and you might need two cameras to cover the same intended area. Wired or Wireless? Power requirements, is there a power outlet where you want to place the camera, or do you need an electrician to put in new power points? Maybe you opt for a wired PoE (Power over Ethernet) solution? These things will all influence your budget and needs to be planned carefully. Let's look at the two main components, cameras and recorders.

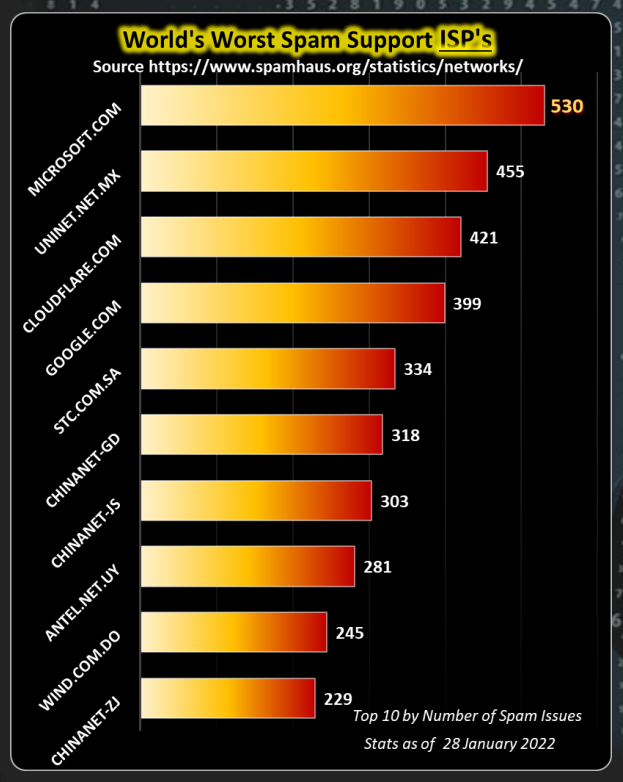
Cameras

There are a multitude of choices if you start looking around and no matter what the viewing requirements are, you will be overwhelmed with the choices. So here are a few things you have to look at: **(1)** Image Quality - CCTV image quality is measured in pixels. This refers to the number of horizontal and vertical lines across the image. The higher the number of pixels, the higher the quality of the image. This is particularly important if you're recording at further distances or need to zoom. For example, do you need a 4K Ultra HD camera or will a 1080p HD camera suffice? Look at this Practical Guide to CCTV Video Resolutions. **(2)** Infrared Night Vision - Infrared night vision is a useful feature as it enables your cameras to view and record in the dark. The distance that these cameras can record varies between products, so ensure you purchase a camera with the correct standard of night visibility to your surroundings. IR Cameras emit light at a much longer wavelength than white lights and are faintly visible to the human eye as a red glow or they are not visible at all. Infrared light is normally provided by specially designed light-emitting diodes (LEDs) and as a rule of thumb, the more diodes, the better or further you can see. **(3)** Static or PTZ (Pan Tilt & Zoom) Cameras – If the requirement is to see down a corridor, then a static camera will do, but if it is an outdoor area, you might need a PTZ camera. Using a PTZ camera will ultimately reduce the number of cameras you need to cover a large area, but on the flip side, a PTZ camera will always have a blind spot for the area outside of the pan or tilt direction. PTZ cameras are normally more costly than static cameras, so, depending on the make and budget, two or three static cameras could give you better visibility at more or less the same price. **(4)** Wired, Wireless, or Wire-free - Wired cameras are the most traditional, and as evidenced by the name, these cameras require cables for power, internet connection, and video transmission. PoE (Power over Ethernet) enabled systems only require one cable which provides both power and internet connection. Wireless camera systems aim to address the most significant downside to a wired security camera system: installation. The key difference between a wired and a wireless camera system is that footage is transmitted wirelessly from the camera to the recorder via Wi-Fi, however, they still require wired power though. Wire-free cameras are the most flexible and easy to install. Due to advances in battery technology, wire-free cameras have evolved significantly and are a great option. Wire-free cameras require no cables at all, but they come at a premium, these systems are not cheap.

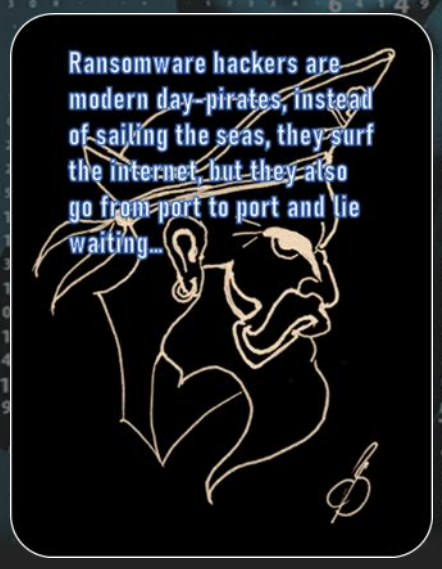
DVR and NVR (see the October post to decide if you need a recorder or not)

(1) Digital Video Recorder (DVR) - Digital Video Recorders are used with analogue CCTV. This option uses a BNC cable to connect the cameras to the digital recording device. Analogue CCTV is the older option on the market. The option requires wiring to be installed from the cameras to the Digital Video Recorder (DVR). Analogue CCTV is typically lower resolution and is the most cost-effective option and will suffice within most homes. Analogue CCTV is best suited to customers where high levels of detail are not required.
(2) Network Video Recorder (NVR) - Network video recorders are used with IP CCTV. The cameras transfer footage to your network video recording device using your physical or Wi-Fi home network. Depending on your camera choice these can be connected to the NVR without wires, or alternatively, an ethernet cable can be used. It is generally the more expensive option.
(3) Storage – The size of your DVR/NVR storage device depends on your storage requirements and will affect the price. Calculator

Resources: DHS.Gov, Optiview, Ryman, Seagate, Mr. Right

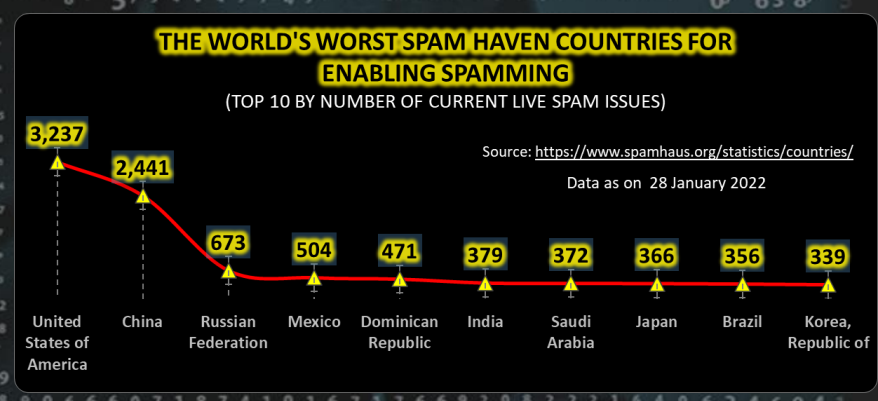


For Reporting Cyber Crime in the USA go to the Internet Crime Complaint Center (IC3)



Other Interesting News and Cyber Security bits:

- NSA Announces Winners of annual Best Scientific Cybersecurity Research Paper Competition
- Apple unveils AirTag safety guide amid stalker fears
- UK - New smart devices cyber security laws
- SANS Daily Network Security Podcast (Stormcast)



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