On August 25, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Adobe products.
See Latest Advisory 26 AUG 2021

Covid-19 Global Stats

Date	Confirmed Cases	Total Deaths
27 Aug	215,477,312	4,488,570

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
27 August 2021

In The News This Week

Samsung Can Remotely Disable Any of Its TVs Worldwide

On July 11, a distribution center located in KwaZulu-Natal, South Africa was looted and an unknown number of Samsung televisions were stolen. However, all of those TVs are now useless as Samsung has revealed they are fitted with remote blocking technology. What you may be surprised to hear is that Samsung can do this to any of its TVs, regardless of where they are in the world. The company admitted as much in its latest Samsung Newsroom post detailing how the TVs in South Africa were stolen and then disabled. The technology is called TV Block and it's "pre-loaded on all Samsung TV products." Whenever a TV is confirmed as being stolen, Samsung logs the serial number of the TV and then waits for it to be connected to the internet. At that point a Samsung server is connected to by default, the serial number is checked, and if it's on the list, "the blocking system is implemented, disabling all the television functions." Read the full story by Matthew Humphries here: PCMag

Vulnerability allowed hackers to tamper medication in infusion pump

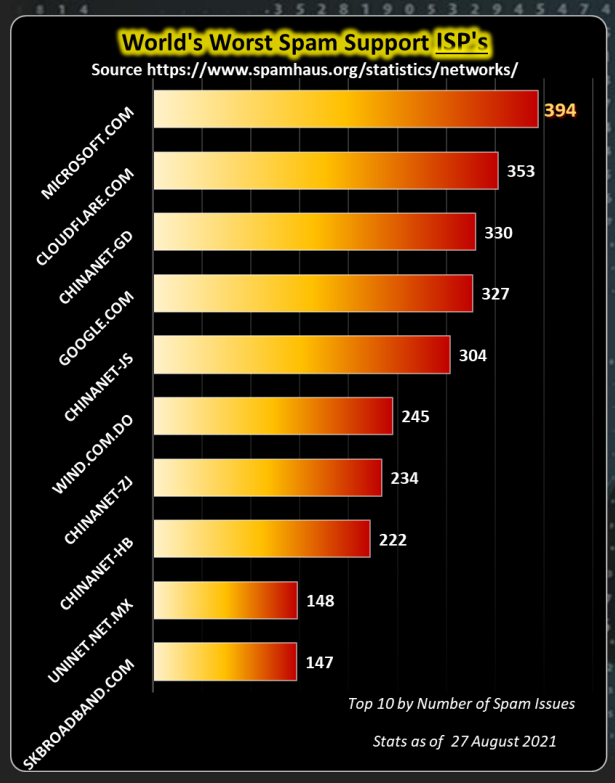
McAfee Enterprise's Advanced Threat Research Team disclosed five unreported security vulnerabilities that existed in German healthcare giant B. Braun's Infusomat Space Large Volume Pump and SpaceStation. Researchers reported that hackers could use these vulnerabilities to change doses without authentication to access the device. For your information, these devices are used in adult and paediatric healthcare facilities to help doctors and nurses to avoid manual infusions. The study was conducted in collaboration with Culinda. "Modification could appear as a device malfunction and be noticed only after a substantial amount of drug has been dispensed to a patient, since the infusion pump displays exactly what was prescribed, all while dispensing potentially lethal doses of medication," researchers noted. . Read the full story by Deeba Ahmed here: HackRead

Biden's cybersecurity summit shows interdependence of government and industry

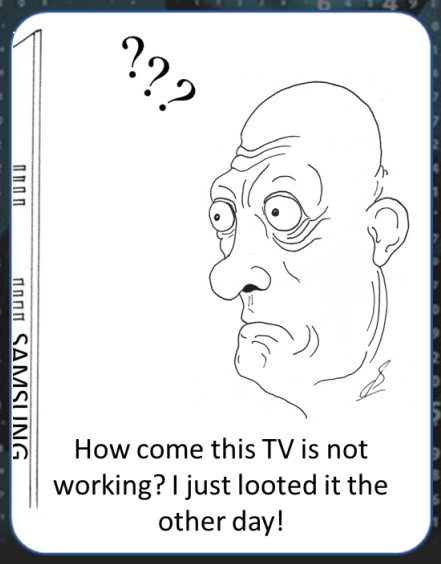
After assembling a team of tough-minded regulators to take on big technology companies, the Biden administration on Wednesday called on many of those same companies to work with the federal government to address a growing wave of cyberattacks.
Driving the news: A White House summit between President Biden and tech leaders Wednesday, including the CEOs of Apple, Google, Amazon, Microsoft and IBM, concluded with a raft of announcements of new cybersecurity projects and spending plans.
(1) Microsoft said it would spend an additional $20 billion over five years on "security by design" and offer $150 million in technical services to federal, state and local governments. (2) Google plans to spend $10 billion over five years on zero-trust programs and other measures to bolster software supply chains and open-source security.
(3) Amazon said it would offer the public free access to the same "security awareness training" it provides its employees. (4) IBM said it would train 150,000 people in cybersecurity skills over three years and partner with 20 historically Black colleges and universities to create cybersecurity leadership centers. (5) Apple said it was starting a new program to enhance supply chain security. Read the story by Scott Rosenberg here: Yahoo

Google Issues YouTube Security Warning For 2 Million Creators

While Google continues to come under scrutiny from those preaching the privacy gospel, there's one area where the technology titan deserves to be applauded: security. Earlier this year, Google announced it would suddenly flip the security switch on millions of Gmail accounts, a switch that will now also be toggled for two million YouTube creators. Just as gaining access to a Gmail account is good news for bad actors, so is taking control of well-monetized YouTube channels with high subscriber counts. Credential compromise, be that through the brute-forcing of passwords or using shared credentials that have been exposed in data breaches from other services, is far and away the most common route to such account takeover. The TeamYouTube community manager, Jensen, has posted an announcement that, as of November 1, Google will "require all monetizing YouTube channels to enable **two-step verification**." While this will not impact ordinary users of YouTube, it does mean that the two million creators in the YouTube Partner Program only have a few weeks to get their access security houses in order. Read the full story by Davey Winder here: Forbes



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



Security camera hacking

In the last few months, we saw many reports of security camera vulnerabilities and consequent hacks that led to footage leaked in the media and so on. Just this week we saw an Iranian official apologizing for videos of prisoner abuse leaked. If you scan the net you will see many similar stories. This prompted me to once again write about home security system weaknesses and what to do about them. In many parts of the world, as in my own home country, security and camera surveillance systems have become a necessity rather than good to have. In cases where multiple break-ins took place, insurance companies are starting to insist that security systems be upgraded to full surveillance systems with captured footage stored in the cloud. To that end, I found this handy article from CNET that I want to share on how to stop someone from hacking your home security cameras. Below is an extract of the article.

Security camera hacking: It can happen to you. Here's how to stop it

The truth is hackers can compromise home security camera feeds, but there are ways to block spying eyes.
Installing a Wi-Fi-connected security camera in your house won't necessarily bring a wave of hackers to your network -- but losing privacy thanks to a device's security shortcomings is surprisingly common. Last year, an ADT home security customer noticed an unfamiliar email address connected to her home security account, a professionally monitored system that included cameras and other devices inside her home. That simple discovery, and her report of it to the company, began to topple a long line of dominoes leading back to a technician who had spied, over the course of four and a half years, on hundreds of customers -- watching them live their private lives, undress and even have sex. ADT says it has closed the loopholes that the technician exploited, implementing "new safeguards, training and policies to strengthen ... account security and customer privacy." But invasions of privacy are not unique to ADT and some vulnerabilities are harder to safeguard than others.

Is my security system vulnerable?

Before jumping into solving the problems of device insecurity, it's helpful to understand how vulnerable your devices really are. Major professionally monitored security systems -- and even individually sold cameras from reputable developers like Google Nest and Wyze -- include high-end encryption (which scrambles messages within a system and grants access through keys) almost across the board. That means as long as you stay current with app and device updates, you should have little to fear of being hacked via software or firmware vulnerabilities.

How could my cameras be accessed?

There are plenty of cases of remote hacks, and even quality devices with high levels of encryption aren't necessarily safe from hacking, given the right circumstances. There are two primary ways a hacker can gain control of a video feed, security expert Aamir Lakhani of FortiGuard told CNET: **locally and remotely**. To access a camera **locally**, a hacker needs to be in range of the wireless network the camera is connected to. There, they would need to obtain access to the wireless network using a number of methods, such as guessing the security passphrase with brute force or spoofing the wireless network and jamming the actual one.
Within a local network, some older security cameras aren't encrypted or password-protected, since the wireless network security itself is often considered enough of a deterrent to keep malicious attacks at bay. So once on the network, a hacker would have to do little else to take control of the cameras and potentially other IoT devices around your house.
Local hacks are unlikely to affect you, though, as they require focused intent on the target. **Remote** hacks are the far more likely scenario, and examples crop up fairly often in the news cycle. Something as common as a data breach -- such as those at Equifax or Delta -- could put your login credentials in the wrong hands, and short of changing your password frequently, there's not much you could do to prevent it from happening.
For hackers with a little know-how, finding the next target with an unsecured video feed is only a Google search away. A surprising number of people and businesses set up security camera systems and never change the default username and password.

How to know if you've been hacked

It would be almost impossible to know if your security camera -- or perhaps more unnervingly, baby monitor -- has been hacked. Attacks could go completely unnoticed to an untrained eye and most people wouldn't know where to begin to look to check. A red flag for some malicious activity on a security camera is slow or worse than normal performance. "Many cameras have limited memory, and when attackers leverage the cameras, CPU cycles have to work extra hard, making regular camera operations almost or entirely unusable at times," said Lakhani. Then again, slow performance could be due to a number of other technical reasons.

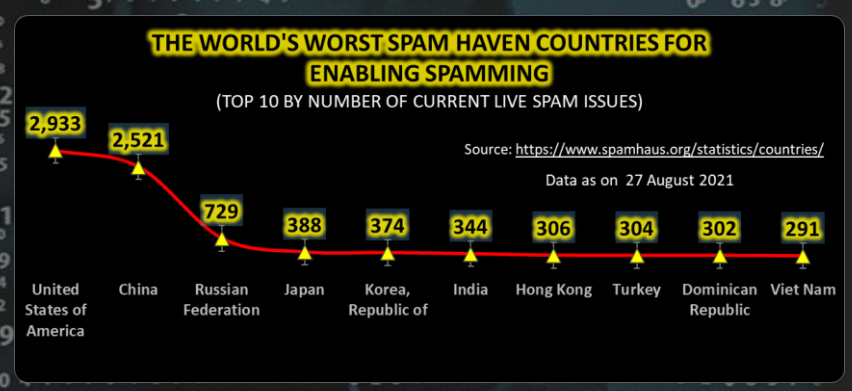
How to protect your privacy

While no one system is impervious to an attack, some precautions can further decrease your odds of being hacked and protect your privacy in the case of a hack. (1) Use cameras from reputable manufacturers, whether they are part of a professionally monitored security system or a DIY device. (2) Use cameras with high-level, end-to-end encryption. (3) Change your credentials to something that cannot easily be guessed (in particular, avoid using passwords you already use for other online accounts). (4) Update the camera firmware frequently or whenever possible. (5) Use two-factor authentication if possible.
Another important step is simply avoiding the conditions for an invasion of privacy. Hacks are unlikely and can be largely avoided, but keeping cameras out of private rooms and pointed instead toward entryways into the house is a good way to avoid the worst potential outcomes of a hack.
Lakhani also suggested putting standalone security cameras on a network of their own. While this would doubtless foil your plans for the perfect smart home, it would help prevent "land and expand," a process by which an attacker gains access to one device and uses it to take control of other connected devices on the same network.

That is all we have space for this week, please visit CNET to read the full article. More references: IFSEC, IPVM, Forbs,

Other Interesting News and Cyber Security bits:

- Google Dragnets Gave Cops Data On Phones Located At Kenosha Riot Arsons
- Automotive Cyber Security Market worth USD 8.94 billion by 2028
- Naval Dome completes rig cyber security project



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