On September 1, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) , No further update this week.
See Latest CIS Advisories

Covid-19 Global Stats

Date	Confirmed Cases	Total Deaths
10 Sep	224,020,120	4,620,773

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
10 September 2021

In The News This Week

Hackers Leak VPN Account Passwords From 87,000 Fortinet FortiGate Devices

Network security solutions provider Fortinet confirmed that a malicious actor had unauthorizedly disclosed VPN login names and passwords associated with 87,000 FortiGate SSL-VPN devices. "These credentials were obtained from systems that remained unpatched against CVE-2018-13379 at the time of the actor's scan. While they may have since been patched, if the passwords were not reset, they remain vulnerable," the company said in a statement on Wednesday. The disclosure comes after the threat actor leaked a list of Fortinet credentials for free on a new Russian-speaking forum called RAMP that launched in July 2021 as well as on Groove ransomware's data leak site, with Advanced Intel noting that the "breach list contains raw access to the top companies" spanning across 74 countries, including India, Taiwan, Italy, France, and Israel. "2,959 out of 22,500 victims are U.S. entities," the researchers said. Read the full story by Ravie Lakshmanan here: The Hacker News

New Mēris botnet breaks DDoS record with 21.8 million RPS attack

A new distributed denial-of-service (DDoS) botnet that kept growing over the summer has been hammering Russian internet giant Yandex for the past month, the attack peaking at the unprecedented rate of 21.8 million requests per second. The botnet received the name Mēris, and it gets its power from tens of thousands of compromised devices that researchers believe to be primarily powerful networking equipment. News about a massive DDoS attack hitting Yandex broke this week in the Russian media, which described it as being the largest in the history of the Russian internet, the so-called RuNet. Information collected separately from several attacks deployed by the new Mēris (Latvian for 'plague') botnet, showed a striking force of more than 30,000 devices. From the data that Yandex observed, assaults on its servers relied on about 56,000 attacking hosts. However, the researchers have seen indications that the number of compromised devices may be closer to 250,000.
Read the full story by Ionut Ilascu here: Bleeping Computer

South Africa - Justice Department hit by ransomware

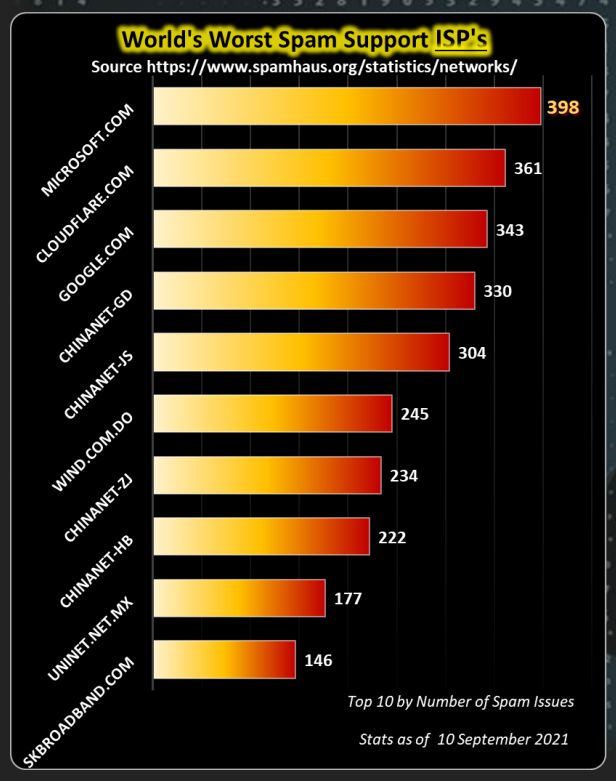
The justice and constitutional development department has been hacked. Spokesperson Steve Mahlangu said the breach was affected through ransomware on Monday evening. "This has led to all information systems being encrypted and unavailable to both internal employees as well as members of the public. As a result, all electronic services provided by the department are affected, including the issuing of letters of authority, bail services, e-mail and the departmental website. "The department would want to assure all affected parties that our IT teams are working tirelessly to restore services as soon as is practically possible. The department said it had activated its business continuity plan and had put contingency measures in place to ensure that the IT system challenges do not affect court operations around the country. Read the story here: Twitter and TimesLive

International Money Launderer Sentenced to over 11 Years over Cyber Crime Schemes

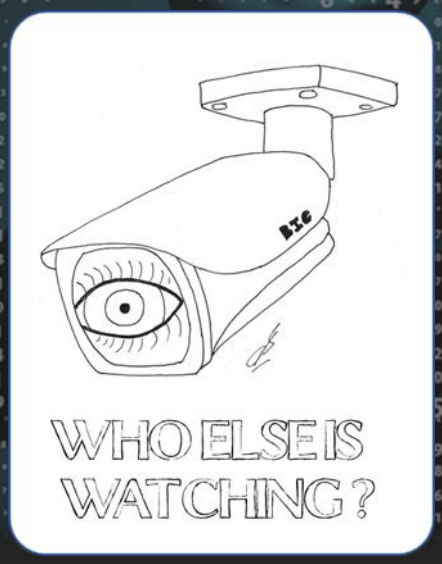
SAVANNAH, Georgia – A Canadian man was sentenced today to 140 months in federal prison for conspiring to launder tens of millions of dollars stolen in various wire and bank fraud schemes, including a massive online banking theft by North Korean cyber criminals that is part of a pending case in Los Angeles. Ghaleb Alaumary, 36, of Mississauga, Ontario, who is a dual Canadian and U.S. citizen, was sentenced after pleading guilty to two counts of conspiracy to commit money laundering in two cases, one of which was filed in Los Angeles. As part of his sentence that covers both cases, Alaumary was ordered to pay more than $30 million in restitution to victims. According to court documents, Alaumary and his co-conspirators used business email compromise schemes, ATM cash-outs, and bank cyber-heists to steal money from victims and then launder the money through bank accounts and digital currency. Read the full article here: US Department of Justice

Microsoft has a $20 billion hacking plan

In the wake of increasingly sophisticated criminal hacks of companies like SolarWinds, Colonial Pipeline, and JBS Foods that touched on fears of national security weaknesses, U.S. politicians all the way up to the White House have been adamant on one cybersecurity requirement: organizations needed to spend more on it to protect the nation. But there's a problem: in many cases, increased spending on cybersecurity in recent years hasn't resulted in better protection against hackers…. Read the full story here: CNBC



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



Top Security Camera and Webcam Hacking Incidents

Two weeks ago, I wrote about how easy it is for hackers to break into an online home or business security camera. It was just after the big Verkada hack made the news that took place in March this year. The question was asked, "How real is the threat?". This week I'll share some real-world incidents where video footage was used for spying or other criminal or perverted motives to illustrate the real dangers if your security or webcam is not secure. (Click on the titles to open the original stories)

1. Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals

A group of hackers breached a massive trove of security-camera data collected by Silicon Valley start-up Verkada Inc., gaining access to live feeds of 150,000 surveillance cameras inside hospitals, companies, police departments, prisons and schools.
Companies whose footage was exposed include carmaker Tesla Inc. and software provider Cloudflare Inc. In addition, hackers were able to view video from inside women's health clinics, psychiatric hospitals and the offices of Verkada itself. Some of the cameras, including in hospitals, use facial-recognition technology to identify and categorize people captured on the footage. The hackers say they also have access to the full video archive of all Verkada customers."

2. Somebody's Watching: Hackers Breach Ring Home Security Cameras

Ashley LeMay and Dylan Blakeley recently installed a Ring security camera in the bedroom of their three daughters, giving the Mississippi parents an extra set of eyes — but not the ones that they had bargained for. Four days after mounting the camera to the wall, a built-in speaker started piping the song "Tiptoe Through the Tulips" into the empty bedroom, footage from the device showed. When the couple's 8-year-old daughter, Alyssa, checked on the music and turned on the lights, a man started speaking to her, repeatedly calling her a racial slur and saying he was Santa Claus. She screamed for her mother..

3. ADT technician hacked hundreds of customers' security cameras

A former security technician for home security company ADT admitted he secretly accessed customers' home security cameras more than 9,600 times over more than four years, particularly in homes of women to spy on them.
Telesforo Aviles, a 35-year-old former ADT employee, pleaded guilty to computer fraud on Thursday before Magistrate Judge David Horan. According to plea papers, Aviles admits that contrary to company policy, he routinely added his personal email address to customers' "ADT Pulse" accounts, giving himself real-time access to the video feeds from their homes. In some instances, he claimed he needed to add himself temporarily in order to "test" the system; in other instances, he added himself without their knowledge.

4. Private moments captured on home security cameras being live streamed again on website

An elderly woman in bed next to a commode toilet in Quebec, a child playing in a living room in Alberta, a woman working from home in Ontario and kitchen staff working in a coffee shop. These private moments have all been visible to anyone on the internet through a website that's live streaming thousands of unsecured cameras around the world in real time. When an employee at a downtown Toronto coffee shop learned that he and other staff were being watched, he said he was surprised because his manager is typically thorough when it comes to security. CBC News is withholding the employee's full last name because he says he feels uneasy after his privacy was already breached. Andy C. said a woman called the Second Cup to alert them that the video from one of their cameras at the back of the store was visible on the website and described what they were doing in real time. "As soon as she revealed she wasn't in the area, I was like, 'OK, how do you know all this stuff?' She was able to identify key traits of people who were working; me and another person," he said. "Definitely uncomfortable." Andy said he disconnected the security camera immediately.

5. Singapore home cams hacked and stolen footage sold on pornographic sites

Clips from the hacked footage have been uploaded on pornographic sites recently, with several explicitly tagged as being from Singapore. The videos, which can last from under a minute to more than 20 minutes, feature couples, breastfeeding mothers and even children. Most of them are in various states of undress or compromising positions. Many faces can be clearly seen in locations such as the living room and bedrooms. Some are seen using the toilet with the door ajar. In one video, time-stamped March 2020, a teenage girl can be seen in a white T-shirt and panties with school books around her. One of them is an O-level Ten-Year Series book used by students preparing for the exam.

6. Louisville family says stranger hacked their baby monitor

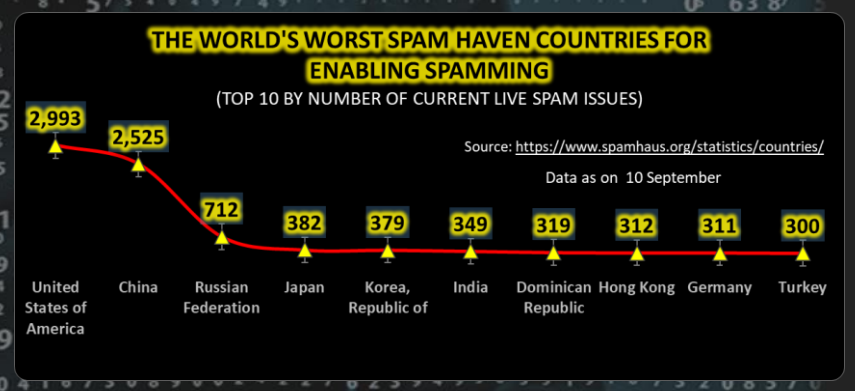
(One Louisville couple said they were shocked when their son told them his baby monitor was talking to him. "'Daddy, mommy talked to me in my camera last night,'" the mother said her child told her husband when they woke up in the morning. The couple did not want to share identifying information, including their names, because of the sensitive nature of the story. When asked what mommy said, the couple said their son responded, "How old are you?" The mother said she never asked her child the question through their monitor. Both parents asked a few more questions, then realized their monitor had been hacked. A day before, they said the monitor randomly panned across the room. While they didn't think anything of it, the couple said they just thought their son was going through a monster phase when he named the monitor "Bad Guy" shortly after they purchased it in January.
"My concern is that this has been going on for a while," the mother said, "which is nauseating."

7. 'I'm in your baby's room': A hacker took over a baby monitor and broadcast threats, parents say

At first, it was a beeping that woke Ellen and Nathan Rigney in the middle of the night. Then it became something more sinister. A stranger's voice, spouting "sexual expletives," wafted through a baby monitor in the Rigneys' room — one that was linked to a Nest camera in their infant's room upstairs, according to KRPC News..

Other Interesting News and Cyber Security bits:

- 20 Years Later, 2 More 9/11 Victims Have Been Identified Using New Technology
- There's been another huge quantum computing breakthrough
- Three ways terrorist attacks of September 11, 2001 changed our world



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