On October 17, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google, Adobe, and Oracle 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

18 October 2019

In The News This Week

Building China's Comac C919 airplane involved a lot of hacking, report says.

A report published on Wednesday 16 October 2019, shines a light on one of China's most ambitious hacking operations known to date, one that involved Ministry of State Security officers, the country's underground hacking scene, legitimate security researchers, and insiders at companies all over the world. The aim of this hacking operation was to acquire intellectual property to narrow China's technological gap in the aviation industry, and especially to help Comac, a Chinese state-owned aerospace manufacturer, build its own airliner, the C919 airplane, to compete with industry rivals like Airbus and Boeing. The published Crowdstrike report shows how this coordinated multi-year hacking campaign systematically went after the foreign companies that supplied components for the C919 airplane. The end goal, Crowdstrike claims, was to acquire the needed intellectual property to manufacture all of the C919's components inside China. Crowdstrike claims that the Ministry of State Security (MSS) tasked the Jiangsu Bureau (MSS JSSD) to carry out these attacks. The Jiangsu Bureau, in turn, tasked two lead officers to coordinate these efforts. One was in charge of the actual hacking team, while the second was tasked with recruiting insiders working at aviation and aerospace companies. The hacking team targeted companies between 2010 and 2015, and successfully breached C919 suppliers like Ametek, Honeywell, Safran, Capstone Turbine, GE, and others. But unlike in other Chinese hacks, where China used cyber-operatives from military units, for these hacks, the MSS took another approach, recruiting local hackers and security researchers. According to Crowdstrike and a Department of Justice indictment, responsible for carrying out the actual intrusions were hackers that the MSS JSSD recruited from China's local underground hacking scene. Crowdstrike says that some of the team members had a shady history going back as far as 2004. To read the full story and see pictures of the component breakdown and hacker profiles go here: ZDNet Article (1)

Stalker zoomed in on Japanese idol's eyes to find out where she lived

According to media reports, an obsessed fan assaulted a J-Pop star after determining where she lived by zooming in on selfies she had posted on social media and examining the reflection in her eyes. 26-year-old "fan" Hibiki Sato attacked Japanese idol Ena Matsuoka outside her home, after zooming in to a reflection of a sign in her eyes' pupils in a photograph she had posted online.

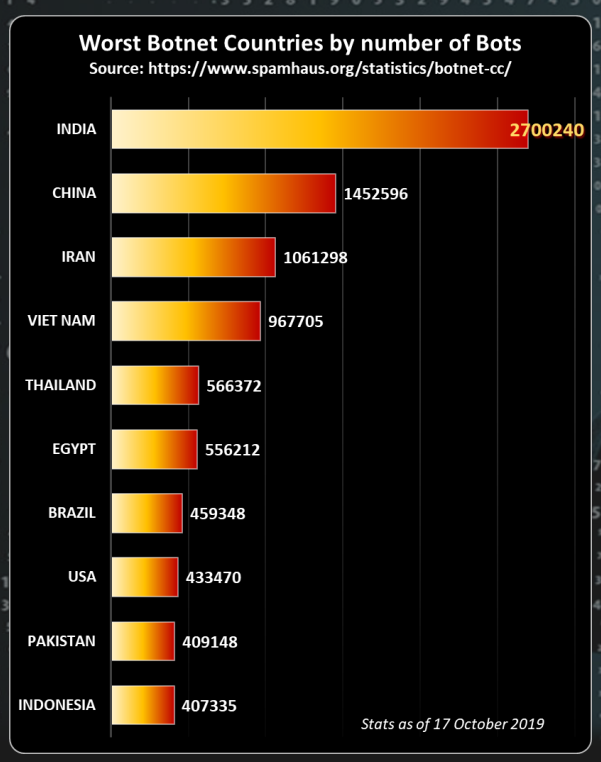
According to AsiaOne, Sato was able to uncover the general location through Google Maps' Street View. He was then able to further narrow down the location of 21-year-old Matsuoka's home by studying other photos she had published online, including ones which included her curtains and by examining the angle of sunlight.

On the day of the assault, September 1st, Sato lay in wait at the station after the young member of the Tenshi Tsukinukeni Yomi J-Pop group had performed a concert and followed her back to her home where he dragged her into a corner and molested her.

Sato was arrested on September 17th, and immediately admitted to police that he had both committed the assault and that he was a big fan of Ena Matsuoka.

According to media reports, Tenshi Tsukinukeni Yomi confirmed via social media that it was Ena Matsuoka who had been attacked. Read the full article by Graham Cluley here: GCluley

The moral of the story here is; be careful what you load on social media, examine your photos before you share it, you never know who is looking deeper than the intention of the photo.



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

According to SafetyDetectives,

38%

of all malware are disguised as MS Word

".Doc"

files where ".exe" filetypes were previously the biggest percentage

How to Tell If Your Security Camera Has Been Hacked

We have been writing about online Internet of Things (IoT) devices and security around that and in this bulletin we want single out online cameras specifically. As the popularity of online surveillance cameras increases so does the opportunities for nefarious perpetrators to take advantage of the security weaknesses normally associated with these devices. The below article is adapted from a post by Amanda Li touching on this topic. Read the full article, including preventative tips here: ReoLink

How to Tell If Your Security Camera Has Been Hacked

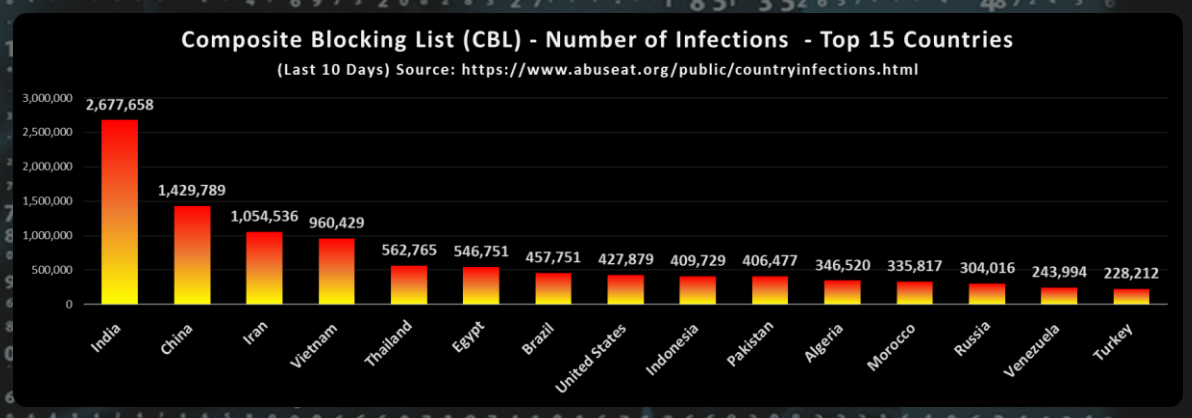
"Can my security camera be hacked?" "How do I know if someone is watching me through my home security IP camera?" Maybe few of you have ever considered this carefully. Neither did Jennifer, a mother in Houston, until she found the security camera in her daughter's room hacked and live streamed over the internet, according to Mashable. While it is easy to hook a security camera up so that it provides live stream footage that you can monitor, it is also incredibly easy for your security cameras to get hacked: Hackers may tap into your security camera, pick up, watch and even broadcast the footage that you are recording.

When your security cameras are hacked, your watchful eye becomes their watchful eye – and could potentially become the watchful eye of hundreds, thousands or even millions, especially these days when security camera hacked websites can easily be found online. In order to avoid the threat, you should be mindful for tell-tale signs of a hacked security camera. Below we explore several ways for you to tell if your security camera has been hacked, or if your baby monitor or nanny cam has fallen victim to these attacks.

How to Find Out If Your Security Camera Has Been Hacked

Your security cameras can be hacked in several ways. Lack of elementary security features, using default settings and simple passwords, and security camera hack apps all result in cameras and baby monitors or webcams getting hacked. Unfortunately, it's not always possible to know if your home video surveillance camera or webcam have been in the Unsecured IP Camera list.

1. Check Out Strange Noises from Your IP Camera or Baby Monitor
   Signs that your IP camera has been hacked can mostly be difficult to detect. But here is an obvious one. If you hear a strange voice coming from your security camera, no doubt that your security camera has been hijacked, and someone is spying on your through the camera.
   Baby monitor hacked news and videos show that hackers interact with your kids through the hacked security camera remotely, listen to your conversations, and more. Terrifying, isn't it?
2. See If Your Security Camera Rotates Abnormally
   If you find out that your home security camera is following your movement, your camera has more than likely been hacked. Someone hacks your pan-tilt camera and control over it on his side. Your hacked security camera or baby monitor may rotate by itself or point to a different position than usual.
3. Check If the Security Settings Have Been Changed
   It is a necessary step to check if the security settings have been changed and password has been set to default. The person hacks into your security camera may leave some information on the settings. There are some proud hackers who even change the camera names to something like "Upgrade Firmware" to show off their hacking talents.
4. Can you see a Blinking LED Light
   If you see that the LED light is blinking randomly, your security camera is probably being hacked. In that case, reboot your computer. If the light flashes again after 10 minutes or so, open up your Task Manager, click on the "processes" tab and search for "winlogon.exe." If you see more than one copy of the program, disconnect your computer from the Internet and use an anti-virus program to run a full system scan to ensure your computer has not been infected with a Trojan.
5. Is there an Illuminated LED Light when the camera is supposed to be off
   If you notice that the LED light is turned on, but you didn't enable it, that's a tell-tale sign that your security camera has been hacked and accessed. When someone hacks your security camera, they have the ability to control it, which includes turning it on and off. If that LED light is on and you know for sure you haven't turned your camera on, follow the steps above to tell whether your security system has been hacked or not.
6. Check the Data Flow of Your Security Camera
   How can you detect if your security camera has been hacked? You can also track the data flow on your network, and on your video surveillance camera. Pay special attention to sudden spikes in your network traffic, which reveals something unusual invalid login in your video feed.



Author: Chris Bester
chris.bester@yahoo.com