On August 22, 2019, the Cyber Threat Alert Level was evaluated and is being lowered to Green (Low). The status is unchanged for this week.

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

30 August 2019

In The News This Week

CamScanner App with Over 100 Million Downloads Removed From Google Play Store Over Advertising Malware - Google Play Store has actively been weeding out apps for engaging in malicious behaviour ranging from ad fraud to seeding harmful code. But despite the vigilant approach, some malware loaded apps are spotted from time to time and are booted off the app repository after raking in a tonne of downloads. The latest app to get booted from the Play Store is CamScanner, an app that converts photos of documents into PDF format and is fairly popular among users. CamScanner was found to contain malware that could seed ads and prompt users into signing up for paid services. As per the findings of Kaspersky researchers, CamScanner's recent versions shipped with an advertising library containing a malicious module. The malicious Trojan Dropper module, which has been identified as "Trojan-Dropper.AndroidOS.Necro.n", has previously been observed in some Chinese apps as well. What this module did is it extracted and ran another malicious module from an encrypted file that is found in the app's resources. The resource-linked module, which is also called a "dropped" module, was found to be a Trojan downloader that downloaded even more harmful modules. After that, it would depend on how a malicious party intends to exploit these modules. Read the story here: Gadget360

Russian police take down malware gang that infected 800,000+ Android smartphones - Russian authorities have arrested members of the TipTop cybercrime group, believed to have infected more than 800,000 Android smartphones with malware since 2015. The group operated by renting Android banking trojans from underground hacking forums, which they later hid inside Android apps distributed via search engine ads and third-party app stores. TipTop has been active since 2015, and operators have been making between $1,500 and $10,500 in daily profits, according to Group-IB, the cyber-security firm who helped Russian authorities track down the gang's members. The group's favourite malware was the Hqwar (Agent.BID) banking trojan, which they rented and used in most of their campaigns. Hqwar is capable of reading SMS messages, recording phone calls, and initiating USSD-requests. However, its primary function is to show fake login screens on top of legitimate banking apps, and steal victims' login credentials. Read the whole story here: ZDnetArticle-1

Google launches bounty program to spot misuses of Google API, Chrome, and Android user data - Google follows Facebook's steps and launches program to spot app devs stealing or misusing Google user data. Google announced Thursday, August 29, a new bug bounty program through which security researchers can report cases of abuse where third-party apps are stealing or misusing Google user data. The new bounty program is named the Developer Data Protection Reward Program (DDPRP), and security researchers can report cases of potential data abuse in third-party apps that have access to the Google API, in Android apps listed on the Play Store, and in Chrome apps and extensions listed on the Chrome Web Store. Google said, "The program aims to reward anyone who can provide verifiably and unambiguous evidence of data abuse". In particular, the program aims to identify situations where user data is being used or sold unexpectedly or repurposed in an illegitimate way without user consent." Reports of Google user data abuse can be filed via the DDPRP page on HackerOne, a bug bounty platform where Google runs some of its bounty programs. Google will investigate any cases of abuse and suspend offending apps. Security researchers who file valid data abuse reports are eligible for rewards of up to $50,000, Google said. Read the full story here: ZDNetArticle-2

Smart and IP based cameras, how secure are they?

Looking at the smart and IP based camera world and how it can be exploited by criminals and how to make them secure.

Experts forecast that approximately 45 billion cameras will be deployed throughout the world by 2022, and a large percentage of them will be smart cameras. While IP cameras are nothing new, smart cameras pack new features that make them more appealing to users. With features from face recognition to various image sensors and connectivity options, such as Bluetooth and Wi-Fi, smart cameras can detect human behaviour and even vehicle number plates, making them a perfect residential or commercial surveillance or tool.

For years, security researchers have found a plethora of vulnerabilities in smart cameras, warning consumers and manufacturers of the dangers that attackers could control them remotely and spy on owners, affect the overall security of home networks, or even impact the global internet infrastructure. We even saw that the infrared sensors on IP based night-vision cameras can be exploited to gain access to your network. (See Here)

Remember the Mirai IoT attack in October 2016, one of the largest IoT botnets attacks, where an estimated 600,000 vulnerable cameras and devices were remotely controlled by threat actors to perform a massive denial of service on critical internet infrastructure services. Bad news is, Mirai is still out there and if you don't take the appropriate mitigation steps, you can get a surprise! (Mirai explained by corero)

Bitdefender researchers also did a recent analysis on four smart cameras, only to find that all of them have several vulnerabilities that criminals could remotely exploit to tamper with, control, or fully compromise them.

How do we secure our IP based smart cameras?

In an article Andy O'Donnell from livewire, we explore some steps you can take to protect yourself by following some common-sense security-hardening procedures.

Update Your Camera's Firmware – Most modern IP security cameras feature user-upgradeable firmware. If a security vulnerability is found, the IP security camera manufacturer will often fix the vulnerability by issuing a firmware update. Usually, you can update your camera's firmware from the admin console through a web browser. You should frequently check your IP security camera manufacturer's website for updated firmware so that you can make sure the version you are using doesn't contain an unpatched vulnerability that could be exploited by hackers and online voyeurs.

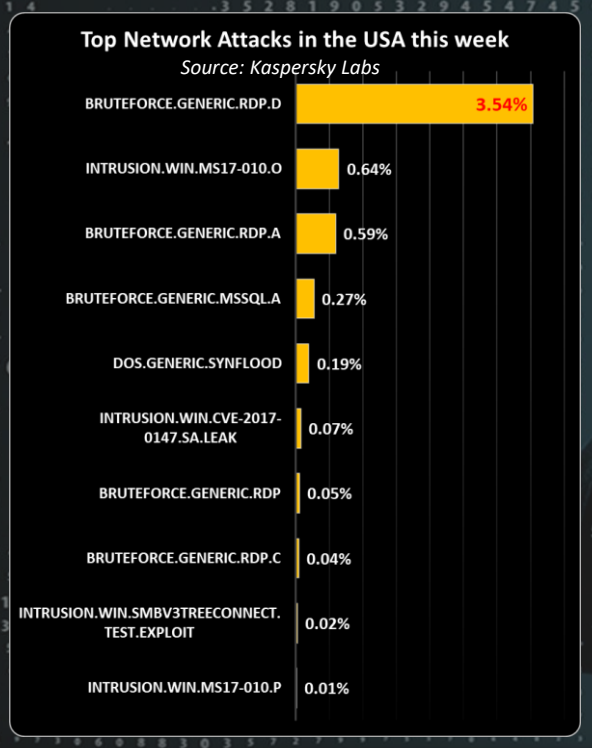
Keep Your Cameras Local – If you don't want your camera feeds to end up on the internet, then don't connect them to the internet. A bit tricky if you want to view your cameras on your phone while you are way, but, if privacy is your top priority, then you should keep your cameras on a local network and assign them non-routable internal IP addresses (i.e. 192.168.0.5 or something similar). Even with non-routable IP addresses, your cameras could still be exposed by camera software that sets up port forwarding or uses UPNP to expose your cameras to the internet. Check your IP camera's website to learn how to set up your cameras in local-only mode.

Assign Passwords to Your Cameras – Many IP cameras don't have password protection turned on by default. However, some people forget to add password protection after the initial setup and end up leaving the cameras wide open for all to access. Most cameras offer at least some form of basic authentication. It may not be super robust, but at least it is better than nothing at all. Protect your camera feeds with a username and a strong password and be sure to change it periodically.

Rename the Default Admin Account and Set a New Admin Password - Your camera's default admin name and password, set by the manufacturer, is usually available by visiting their website and going to the support section for your camera model. If you haven't changed the admin name and password, then even the most novice hacker can look up the default password and view your feeds or take control of your camera.

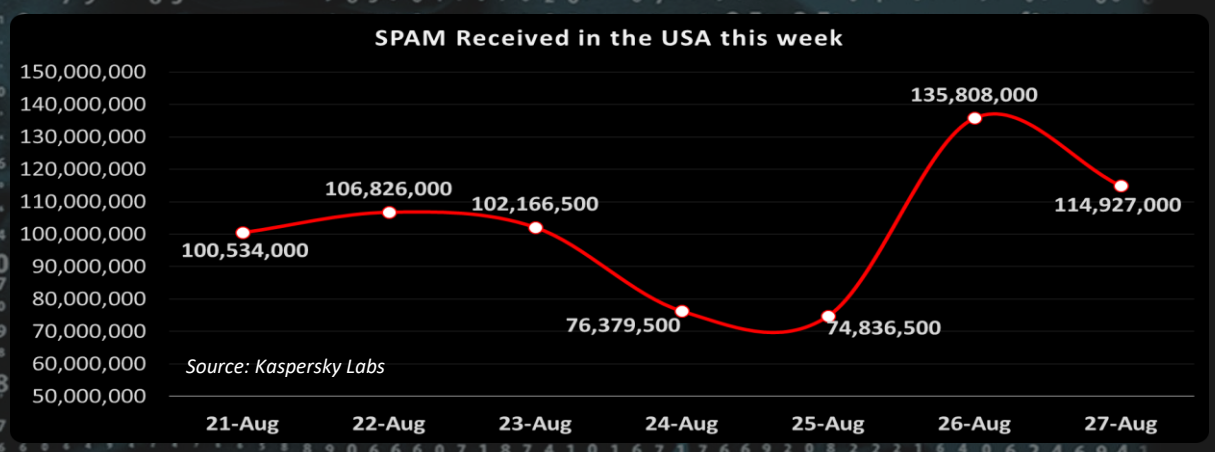
If Your Camera Is Wireless, Turn on WPA2 Encryption – If your camera is wirelessly capable, you should only join it to a WPA2-encrypted wireless network so that wireless eavesdroppers can't connect to it and access your video feeds.

Don't Place IP Cameras Where They Don't Belong - Don't put an IP security camera inside areas of your house where you wouldn't feel comfortable being seen by strangers. Even if you think you've secured your cameras in every way possible, there is always the possibility of getting blind-sided by a Zero-Day vulnerability that hasn't been found by your manufacturer yet.



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

According to an Email gap analysis done by Cyren on a sample of **4.2 Million** emails across multiple companies with existing SaaS or appliance security controls, **9.1%** of SPAM, Malware & Phishing Mails are still filtering through.
Read the report here: CYREN



Author: Chris Bester
chris.bester@yahoo.com