On November 6, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google and Microsoft 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

08 November 2019

In The News This Week

Alexa, Siri, Google Assistant smart speakers – they're all open to remote laser attacks.

Researchers have found that MEMS microphones are so sensitive they can interpret light as sound, allowing an attacker to shoot silent commands to voice assistants from afar with laser beams and instruct smart locks and garage doors to open. Since the bug is general to MEMS (microelectromechanical systems) microphones, the attack can work against all devices that use them, including Google Assistant, Amazon Alexa, Facebook Portal, and Apple Siri. Injecting voice-commands to smart speakers from a long range might not sound like a major threat, but devices from Google, Amazon, and Apple are shaping up to be a main hub for controlling gadgets in the smart home, including lights, smart locks, and garage doors.

Amazon says that 85,000 smart home gadgets now integrate with Alexa, while Apple is trying to get more gadgets to work with its HomeKit system. Given smart gadgets' central role, the MEMS mic vulnerability could allow an attacker to issue commands to do things like open a garage door, open doors protected by smart locks, or even unlock and start a Tesla that's connected to a Google account.

The laser study was conducted by researchers at the University of Electro-Communications in Tokyo and the University of Michigan, who detail their work in a new paper, 'Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems'. "We show how an attacker can inject arbitrary audio signals to the target microphone by aiming an amplitude-modulated light at the microphone's aperture," they explain.

"We then proceed to show how this effect leads to a remote voice-command injection attack on voice-controllable systems. Examining various products that use Amazon's Alexa, Apple's Siri, Facebook's Portal, and Google Assistant, we show how to use light to obtain full control over these devices at distances up to 110 meters and from two separate buildings." The attack, dubbed LightCommands, works because the diaphragm in microphones converts sound into electrical signals. The research details how an attacker can use silent laser beams to cause vibrations in the diaphragm and then issue commands. - (My comment on this "Although the attack vector has been highlighted by researchers, it has not been seen in the wild") –

Read the full story here: ZDNet Article(1)

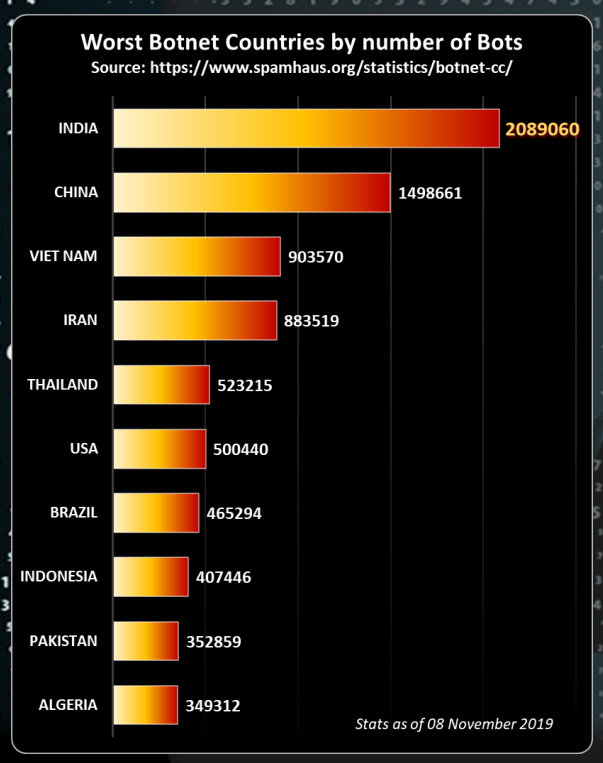
Amazon Ring doorbells exposed home Wi-Fi passwords to hackers.

Security researchers have discovered a vulnerability in Ring doorbells that exposed the passwords for the Wi-Fi networks to which they were connected. Bitdefender said the Amazon-owned doorbell was sending owners' Wi-Fi passwords in cleartext as the doorbell joins the local network, allowing nearby hackers to intercept the Wi-Fi password and gain access to the network to launch larger attacks or conduct surveillance. "When first configuring the device, the smartphone app must send the wireless network credentials. This takes place in an unsecure manner, through an unprotected access point," said Bitdefender. "Once this network is up, the app connects to it automatically, queries the device, then sends the credentials to the local network." But all of this is carried out over an unencrypted connection, exposing the Wi-Fi password that is sent over the air.

Amazon fixed the vulnerability in all Ring devices in September, but the vulnerability was only disclosed today. It's another example of smart home technology suffering from security issues. As much as smart home devices are designed to make our lives easier and homes more secure, researchers keep finding vulnerabilities that allow them to get access to the very thing they're trying to protect.

Amazon has faced intense scrutiny in recent months for Ring's work with law enforcement. Several news outlets, including Gizmodo, have detailed the close relationship Ring has with police departments, including their Ring-related messaging. It was reported this week that Ring had bragged on Instagram about tracking millions of trick-or-treaters this Halloween.

Read the full story here: TechCrunch



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

Image manipulation and fake news – Using reverse image search for verification

In today's social media culture, perpetrators know that a fake message with the right content can spread like wildfire and can reach millions in a blink of an eye. Whether it is misinformation to discredit politicians or celebrities or fuelling racial hatred or to rally up support for a cause that would generally not get any attention, the fact is, someone is taking the time on a daily basis to spread fake images to specific audiences or across the world.

Recent examples included photoshopped fake photos of prominent politicians like Donald trump and former South African president Jakob Zuma and many more flooding social media to add fuel to media frenzies that was doing the rounds at the time. The topic has become so rampant that several in-depth university studies and other papers and articles has seen the light addressing the impact on society and media reliability.

Here are some examples - An article by Cuihua Shen of the University of California states "*Fake or manipulated images propagated through the Web and social media have the capacity to deceive, emotionally distress, and influence public opinions and actions.*"

In a paper by Pennycook, G. & Rand, D. G. Who falls for fake news? it more or less states "*Inaccurate beliefs pose a threat to democracy and fake news represents a particularly egregious and direct avenue by which inaccurate beliefs have been propagated via social media*"

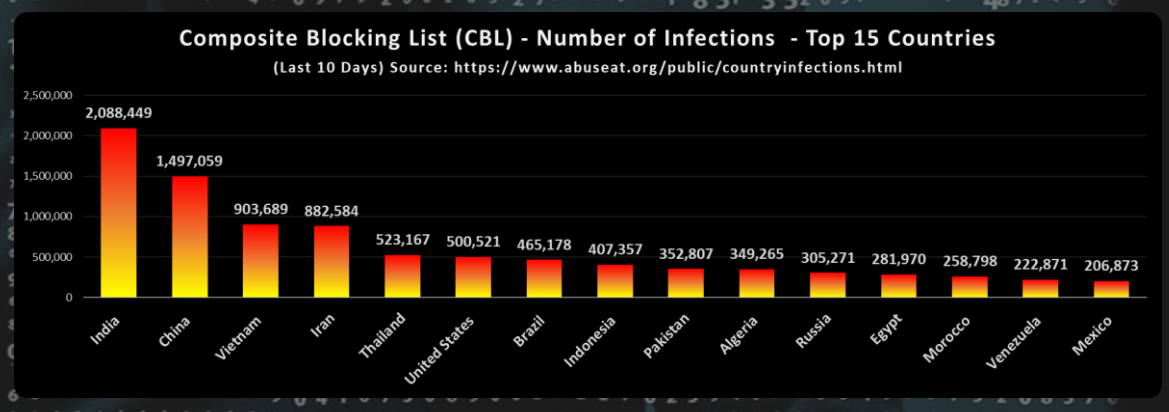
So the issue is recognised as a global problem, but how do we know that the images we received via social media on our phones or other mobile devices are real or fake? Specially if it is touching on controversial or sensitive social issues.
One of the techniques that you can use is called a "Reverse Image Search", so what is this and how does it work?

What is Reverse Image Search
Reverse image search is based on search engine technology called "Content-Based Image Retrieval" (CBIR) that takes a sample image file (Jpeg, PNG, etc.) as input and run a query and returns results related to the image. For example, if you upload a photo you received on social media that show two people (Like the fake one with ex-president Zuma and a prominent singer), you can get results back that show the real photos that was used to create the combined photo.

How do I do it and where do I get it?
There are many search engines and web services that offer "Reverse Image Search" for free but the main contenders for me are Yandex, Google, TinEye and Bing and Ryan Weaver is doing a stellar comparison on the DOMIANTOOLS website which I highlight below. You basically link to one of the engines mentioned above and upload the image you want to investigate or the URL link where the image is found and click "Search" and the magic will happen ☺. G2 provides a useful Reverse Image Search Guide for Beginners to get you on your way. G2 also highlights that Reverse image search is not all for doom and gloom and fake research, it can also be used for many positive applications.

Following is an extract of Ryan Weaver's tool comparisons:
Google Images - Google does its best to identify what is the subject of an image and not who. Results are generally split between three sections: A few search results for what the algorithm thinks is in the photo, visually similar (but not identical) results, and pages that include identical images. *(On Google Search, click "Images", then click on the little camera icon in the search bar)*
Yandex - Yandex, which is akin to a Russian Google, is a goldmine for reverse image searching. It provides additional sizes of the same image, visually similar images, and lots of results where similar images are featured on pages. Yandex tends to be the strongest search engine for face matching and location identification. If you've got a photo of an obscure riverbend somewhere in Europe (thanks Aric!) this is likely where you'll find some results.
Bing Images - Bing has a unique feature that I really enjoy - you can crop down areas of your photo in it and see live results. This is great for high quality images with a lot of identifiable subjects. Additionally, compared to Google, Bing tries to identify elements within a photo and find images that contain all of those elements. So a picture of an antique car parked next to a tree would trigger matches that contain a tree and an antique car, whereas Google picks a single strong subject and follows that. Bing also sets itself apart by trying to proactively identify faces, products, and other elements within images. A high definition image of several famous subjects will highlight each one of them.
TinEye - TinEye's original sole purpose was finding other sizes of the same image, and for many years it provided just that. It's my opinion that they've powered up their matching algorithm in the last year or so and now match on more visually similar images. This means you're likely to find your image used within other images here, and if it's a photo you might find other photos of the exact same composition. I want to note here that TinEye shouldn't be seen as a direct competitor to these other engines. TinEye focuses wholly on finding other usage of the same image, which usually makes it the winner when dealing with purely digital media (avatars, logos, buttons, etc.). I've personally found it useful for tracing user avatars between forums where they may have a different username.

Go on, test it, load a photo of yourself and reverse search it and see what comes up.. Don't worry, none of these engines will store your image ☺



Author: Chris Bester
chris.bester@yahoo.com