On January 16, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded), due to the MS-ISAC advisory on the Cryptographic Library Crypt32.dll vulnerability affecting Microsoft 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
17 January 2020

In The News This Week

Apple has reignited a privacy battle with the Trump administration by declining to unlock a mass shooter's iPhones

Attorney General William Barr reignited a feud between Apple and the US government over its refusal to let officials access encrypted data on iPhones. He said Apple wasn't doing enough to help the FBI access two phones used by Mohammed Alshamrani, the Saudi officer who opened fire in December on a naval base in Pensacola, Florida. Barr said the FBI needed encrypted information from Alshamrani's iPhones to properly investigate the shooting, which officials on Monday declared was an act of terrorism. Apple said it had helped as much as it could but would never code a "backdoor" to allow law enforcement access to users' encrypted information. The argument is effectively a replay of a 2015 struggle between Apple and the Obama administration, which wanted to access a cell phone after the mass shooting in San Bernardino, California. Apple has said such backdoors would make all users' phones vulnerable to bad actors. Read the full story here: Business Insider

EU considers banning facial recognition technology in public spaces

A potential ban could last for five years to allow lawmakers to catch up - The European Union is debating a potential ban on the use of facial recognition technologies in public areas. Facial recognition-equipped systems, such as those found in mobile devices and cameras, are advocated by law enforcement as a way to track missing persons and as useful tools in criminal investigations. As the development of facial recognition technologies gains traction, lawmakers have been left with the task of working out how to control its use. The EU, as reported by Reuters, is considering a ban of up to five years on facial recognition in public areas -- potentially including locations such as parks, tourist hotspots, and sports venues -- to give politicians time to thrash out legislation to prevent its abuse. The proposals, as seen by the publication, are part of an 18-page whitepaper that suggests a ban could permit the time to create a "sound methodology for assessing the impacts of this technology and possible risk management measures. However, exceptions could be made to a blanket ban for the purposes of security and research. Feedback on the proposals will be sought before a decision is made.
Read the full story here: ZDNet Article

Satan Ransomware Reborn as "5ss5c" to Torment Businesses

A ransomware with the un-snappy moniker of "5ss5c" has emerged on the scene and appears to be in active development. According to independent researcher Bart Blaze, the malware is the successor to the Satan ransomware, and its authors are still experimenting with focused targeting (China, for now) and features. Blaze said in a blog posted Tuesday that 5ss5c and Satan share many code characteristics. Satan, he noted, disappeared from the ransomware milieu a few months ago, right after adding an EternalBlue exploit to its bag of tricks. 5ss5c appears to be picking up where Satan left off. "The group has been working on new ransomware – 5ss5c – since at least November 2019," Blaze noted. "There are several Satan ransomware artefacts [and shared tactics, techniques and procedures (TTPs)]. One of these is, for example, the use of multiple packers to protect their droppers and payloads. Read the full story by Tara Seals here: ThreatPost

Craziest IoT Device Hacks – Ocean's 14?

When it comes to stealing data, hackers will use any means at their disposal. Casinos are some of the most secure organizations/facilities on the planet, which is why one group of hackers elected to hack a casino via a thermometer in an aquarium in the lobby. After accessing the casino's network, hackers located the high-roller database and extracted it via the thermostat. This heist might not have been as daring as Ocean's Eleven, but for those high-rollers who had their personnel data compromised, both they and the casino were left with a losing hand. Find more crazy IoT hacks by Mike O'Malley here: RadwareBlog

"Juice Jacking"

"Juice Jacking" is a phrase coined by cyber-security expert, Brian Krebs at DEF CON 2011 and is all about a security exploit using compromised USB charging cables or USB charging ports to hack into your mobile phone. The threat is real enough for the Los Angeles County District Attorney's Office to issue a travel alert urging travellers to be careful where and how you charge your phone. The exploit is rearing its head more and more these days as criminals use public USB-charging stations to steal information from users phones and other electronic devices. I dug a bit into the issue and found many reports of people who has fallen victim to "Juice Jacking". A number of security articles touch on the subject but I found one published by GritDaily most informative and I encourage you to visit their site to get a good rundown on the subject. Here are a few video links that carry information on the topic as well: Fox12 , 13wmaz & Denver7. A special thanks to my good friend and security expert Yazan Shapsugh who got me curious enough about the subject to write about it.

How It Works

Juice Jacking happens when a cyber criminal loads malware into a public charging station he or she hacked into. Malware could also be loaded onto the charging cable itself. (See section about USBHarpoon below). Once connected, the malware infects your device and executes a some code which can then potentially lock your phone or device, send private information, including your passwords, addresses, or even a full backup of the phone to an undisclosed recipient. It also have the potential or ability to monitor the phone in real time with the user non-the-wiser. This means the perpetrator can listen in on conversations, see what you are typing in your social media apps, skim al your financial information when you do online transaction, hijack your emails and so fourth. Sometimes the phone can be cloned completely and even if the original phone is switched off, can still be used on the cloned device as if it is your phone. No phone or GSM enabled mobile device is immune to this attack and that include all Windows, iOS and Android devices. Juice Jacking operates in a similar manner as credit card skimmers used on ATM machines.

The USB Connector

Most of us know that the USB port operates as a power source and can be used to transfer data from your phone to a PC or vice versa, but the reality is that it can be used for much more. A USB connector has 5 pins, one of those pins carries a low wattage 5 Volt power current which is used to charge or power the receiving end. Two pins are used for data transfer which leaves the other three pins open for vendors or criminals to use for a variety of things including what is known as BadUSB and USBHarpoons. In standard charging cables, the latter three pins are normally unused. By default the native data transfer mode is disabled and is only invoked when you start an app for this purpose (or this is how I understand it).

Juice Jacking currently in the wild

1. Data theft – Data exfiltration while a phone or other mobile device is charging
2. Device cloning – Since public charging stations are normally IoT enabled the compromised port and IoT system is used to dump a complete backup of the phone which is then retrieved from the destination system and used to create a identical clone of the device including data and call credits.
3. Malware infection – malware is pre-loaded on a compromised port or cable and "dropped" on the device the moment it is connected (plugged in). The infections are ranging from less dangerous adware to lethal ransomware.

What You Can Do to Prevent being a victim of Juice Jacking

1. Avoid using public charging stations
2. Use your own changer and charging cable and rather get yourself an external battery bank.
3. Be aware of street vendors offering real cheap charging cables
4. Rather use the AC outlet with your own charger than the USB AC ports find in some public areas

USBHarpoon

USBHarpoon Is a BadUSB Attack with A Twist and follows on our story on Juice Jacking above. In an article by Bleeping Computer they describe it as follows: (Adapted version)

Several security experts have built a malicious version of a USB charging cable, one that can compromise a computer in just a few seconds. Once plugged in, it turns into a peripheral device capable of typing and launching commands.

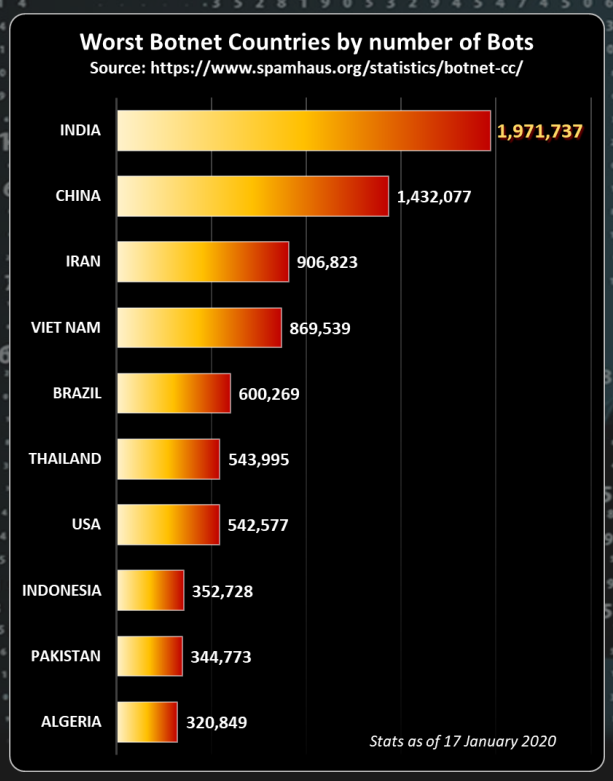
USBHarpoon, as its makers call it, relies on the BadUSB research from Karsten Nohl and his team at Security Research Labs. Their work showed that an attacker can reprogram the controller chip of a USB drive and make it appear to the computer as a human interface device (HID). The type of HID can be anything from an input device like a keyboard that issues a rapid succession of commands, to a network card that modifies the system's DNS settings to redirect traffic.

With USBHarpoon, security experts replaced the USB drive with a charging cable, something that is as ubiquitous, but less likely for users to be cautious of. The cable comes with modified connectors that allow both data and power to pass through so it will fulfill the expected function. This feature enables it to be accompanied by any type of device that powers through USB (fans, dongles distributed at conferences), without raising suspicions about plugging the cable.

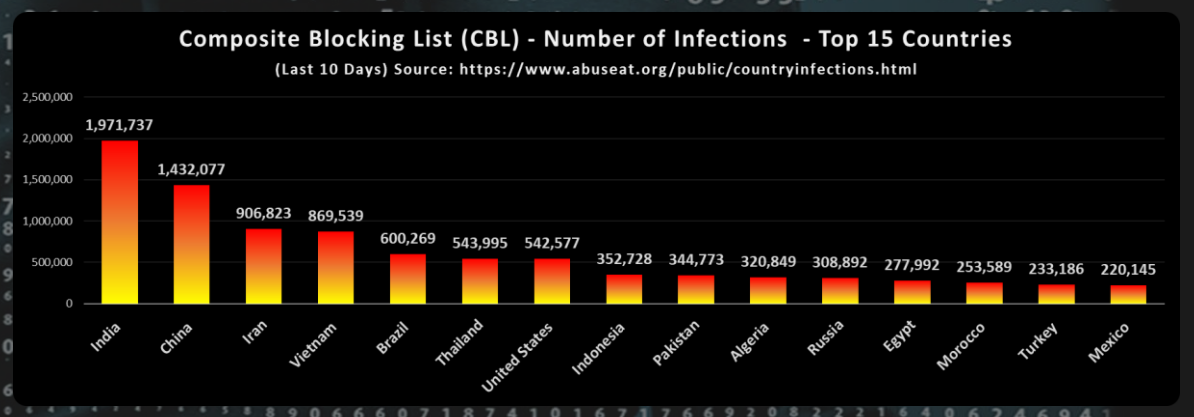
Behind the USBHarpoon project are Olaf Tan and Dennis Goh of RFID Research Group, Vincent Yiu of SYON Security, and Kevin Mitnick, who catalyzed the entire collaboration. Yiu stated that, in collaboration with friends and fellow researchers, the managed to successfully weaponize the cable but It turns out that a weaponized charging USB cable already existed and was developed by a security researcher using the Twitter handle MG.

As shown in the two videos in the article, MG was able to create USB cables that could perform HID attacks when plugged into a computer's USB port.

MG also showed that the attack, which he calls BadUSB cable, would work with a USB-C connector, used in MacBook chargers, informing that it "work on just about any device with a USB port," including phones.



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



Author: Chris Bester
chris.bester@yahoo.com