On October 25, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Juniper, Cisco, Mozilla, and Google 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

01 November 2019

In The News This Week

Oops — Adobe leaves 7.5 million Creative Cloud accounts exposed.

Earlier this month, Adobe was the victim of a serious security incident that exposed the personal information of nearly 7.5 million users belonging to the company's popular Creative Cloud service.
According to security firm Comparitech, the software giant left an Elasticsearch Server unsecured that was accessible on the web without any password or authentication required. The leak, which was discovered on October 19, was plugged by Adobe immediately after it was alerted of its existence. The exposed database included details like email addresses, account creation dates, subscribed products, subscription statuses, payment statuses, member IDs, country of origin, time since last login, and whether they were Adobe employees or not. - Read the full story here: TNW

Facebook sues Israeli cybersecurity company NSO and claims it helped hack WhatsApp.

Facebook is suing an Israeli cybersecurity company over claims it hacked WhatsApp users earlier this year. In the complaint filed on Tuesday 29 October, Facebook alleges that NSO Group used WhatsApp servers to spread malware to 1,400 mobile phones in an attempt to target journalists, diplomats, human rights activists, senior government officials and other parties. The lawsuit says the malware was unable to break the Facebook-owned app's encryption, and instead infected customers' phones, giving NSO access to messages after they were decrypted on the receiver's device. NSO Group could not immediately be reached for comment. Facebook also names Q Cyber, a company affiliated with NSO, as a second defendant in the case. WhatsApp confirmed the vulnerability earlier this year but didn't name the perpetrator. Read the full story here: CNBC Article

Malicious Android Dropper App 'Xhelper' Reinstall Itself after Uninstall – Infected 45K.

The malware campaign started in May this year and slowly made its way to the top 10 mobile malware list, it targets Android devices by masquerading as legitimate apps. The malicious app infected more than 45,000 devices in the past six months. Upon execution, the malware will register itself as a foreground service, once it has gained a foothold on the device, it will execute its core malicious functionality by decrypting to memory the malicious payload embedded in its package. The malware then connects to the C&C server and waits for commands. Upon successful connection to the C&C server, additional payloads such as droppers, clickers, and rootkits, may be downloaded to the compromised device. Security experts suspect the malicious code is included in a system app pre-installed on the Android devices of certain phone brands. Read the full story here: Security Affairs

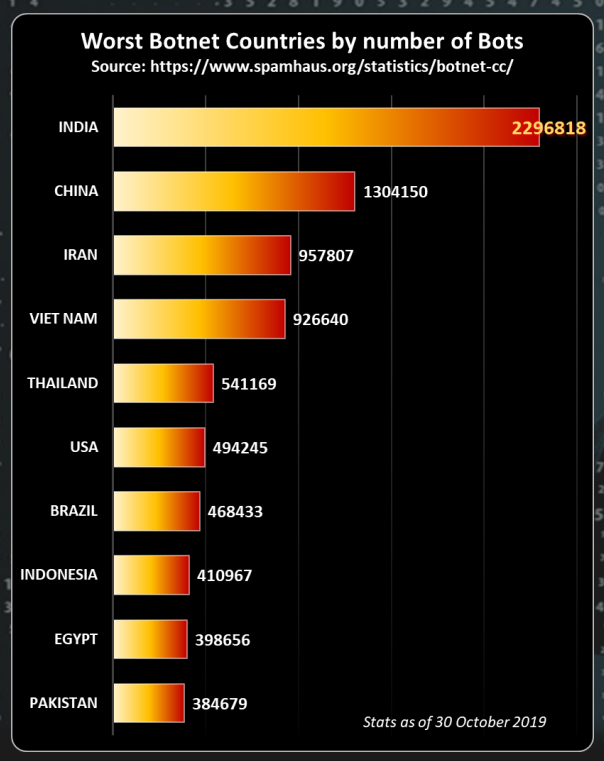
Hackers plead guilty in data breach that Uber covered up.

Two computer hackers have pleaded guilty to concocting an extortion scheme that entangled Uber in a yearlong cover-up of a data breach that stole sensitive information about 57 million of the ride-hailing service's passengers and drivers. The pleas entered Wednesday in a San Jose, California, federal court by Brandon Charles Glover and Vasile Mereacre resurrected another unseemly episode in Uber's chequered history. Glover, 26, and Mereacre, 23, acknowledged stealing personal information from companies that was stored on Amazon Web Services from October 2016 to January 2017 and then demanding to be paid to destroy the data.
Uber met the hackers' demand with a $100,000 payment, but waited until November 2017 to reveal that the personal information of both its riders and drivers around the world had fallen into the hands of criminals. U.S. Attorney David Anderson ripped into Uber for not immediately alerting authorities about the loss of so much personal information that could have been used for identity theft and other malicious purposes. "Companies like Uber are the caretakers, not the owners, of customers' personal information," Anderson said in a statement.
Uber declined to comment on the guilty pleas and Anderson's criticism. . Read the full story here: Washington Post

Summary of the Scariest Hacks in 2019 so far

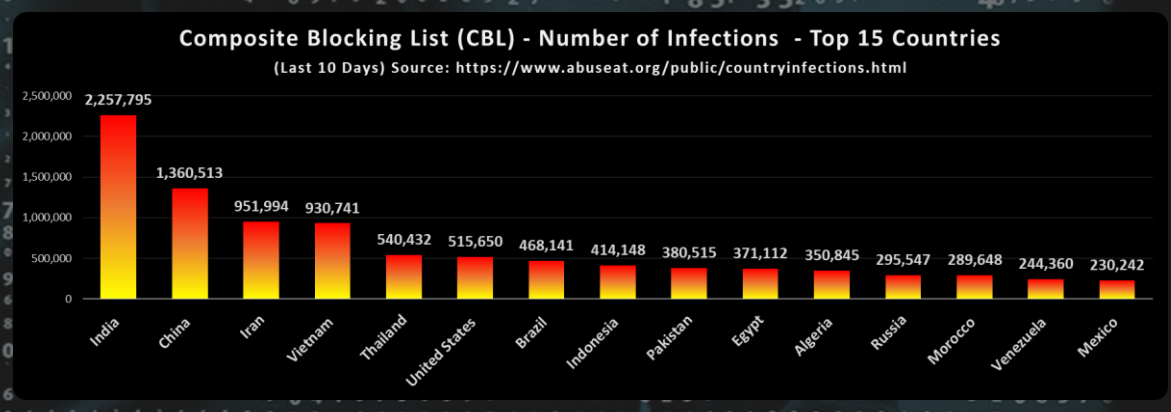
JANUARY – ❶Severe vulnerability in Apple FaceTime - A bug in Apple's FaceTime app let attackers call and self-answer a FaceTime call without any user interaction from the callee, opening the door for secret surveillance. ❷North Korean hackers infiltrate Chile's ATM network after Skype job interview - the article's title is self-explanatory, and the story is worth your time to read. ❸Hackers breach and steal data from South Korea's Defense Ministry - Seoul government said hackers breached 30 computers and stole data from 10. The hacked computers stored data on weapons and munitions acquisition.
FEBRUARY – ❶Leaky DB exposes China's Muslim-tracking practices - Security researcher Victor Gevers found a leaky DB from a Chinese company that exposed its Muslim-tracking facial recognition software, inadvertently revealing China's Uyghur-tracking practices. ❷Major WinRAR bugs exposed - Check Point researchers found a WinrAR bug that impacted all the WinRAR versions released since 2000. Over 500 million WinRAR users were at risk. The bugs eventually become widely used by cyber-criminals and nation-state hackers at the same time. ❸New WinPot malware can make **ATMs spit out cash** - WinPot has been on sale on underground forums since March 2018.
MARCH – ❶Hackers take tornado sirens offline before major storm - Yeah. That was just evil. ❷ The ASUS supply-chain hack - Hackers hijacked the ASUS Live Update utility to deploy malware on users' systems. The hack took place in 2018 but was disclosed in March. Over one million PCs were believed to have been impacted. ❸Ring of GitHub accounts promoting 300+ backdoored apps - GitHub ring consisting of 89 accounts promoted 73 repos containing over 300 backdoored Windows, Mac, and Linux apps.
APRIL – ❶United Airlines covers up seat cameras - The airline insists that the cameras have not been in active use; however, customers were still very disturbed and annoyed by the cameras' presence in the first place. ❷ Tens of thousands of cars were left exposed to thieves due to a hardcoded password - Security updates that remove the hardcoded credentials have been made available for both the MyCar Android and iOS apps since mid-February. ❸Facebook admits to storing plaintext passwords for millions of Instagram users - Incident comes after a month earlier, Facebook admitted to storing plaintext passwords for Facebook accounts too.
MAY – ❶A hacker wiped Git repositories and asked for a ransom - Thousands of repos were impacted, but almost all projects were recovered. ❷ New MDS attacks on modern CPUs - Researchers, academics detail new Microarchitectural Data Sampling (MDS) attacks, such as Zombieload, Fallout, and RIDL. ❸BlueKeep vulnerability - In mid-May, Microsoft warned about a new "wormable" RDP vulnerability that later became known as BlueKeep. Two new wormable BlueKeep-like vulnerabilities (DejaBlue) were later disclosed in August
JUNE – ❶Hackers breached 10 telecom providers - Researchers at Cybereason said a nation-state-backed intelligence operation has compromised at least 10 global telco companies - to such an extent the attackers run a "de facto shadow IT department". ❷ New Silex malware bricked thousands of IoT devices - Attack lasted for days, but the hacker eventually stopped and retired the Silex malware code. ❸NASA hacked because of unauthorized Raspberry Pi connected to its network - NASA described the hackers as an "advanced persistent threat," a term generally used for nation-state hacking groups, but didn't provide other details.
JULY – ❶Kazakhstan government intercepted all local HTTPS traffic - HTTPS interception efforts targeted Facebook, Google, Twitter, and other sites. Apple, Google, and Mozilla eventually intervened and banned the certificate used for HTTPS MitM attacks. ❷ Hacker steals data of millions of Bulgarians - A hacker stole the personal details of millions of Bulgarians and emailed download links to the stolen data to local news publications. The date, stolen from the country's National Revenue Agency, eventually leaked online. ❸Hackers breach FSB contractor - Hackers have breached SyTech, a contractor for FSB, Russia's national intelligence service, from where they stole information about internal projects the company was working on behalf of the agency -- including one for deanonymizing Tor traffic.
AUGUST – ❶SWAPGSAttack CPU flaw - Researchers detail hardware vulnerability that bypasses mitigations against Spectre and Meltdown CPU vulnerabilities on Windows systems - and impacts all systems using Intel processors manufactured since 2012. ❷ 14 iOS zero-days - Google finds exploits for 14 iOS vulnerabilities, grouped in five exploit chains, deployed in the wild since September 2016. Attacks aimed at Chinese Uyghur users. ❸Capitol One hack - A hacker breached Capitol One, from where she stole the records of 100 million users. She also hacked 30 other companies.
SEPTEMBER – ❶Simjacker attack - Security researchers detailed an SMS-based attack that can allow malicious actors to track users' devices by abusing little-known apps that are running on SIM cards. SIM cards in 29 countries were found to be impacted. A second attack named WIBAttack was also discovered. ❷ Smart TV spying - Two academic papers found that smart TVs were collecting data on users' TV-viewing habits. ❸Lumin PDF breach - The details of over 24.3 million Lumin PDF users were shared on a hacking forum in mid-September. The company acknowledged the breach a day later.
OCTOBER – ❶Avast hack - Czech antivirus maker discloses second attack aimed at compromising CCleaner releases, after the one suffered in 2017. Company said hacker compromised the company via a compromised VPN profile. ❷ Alexa and Google Home devices leveraged to phish and eavesdrop on users, again - Amazon, Google fail to address security loopholes in Alexa and Home devices more than a year after first reports. ❸Johannesburg held for ransom by hacker gang - A group named "Shadow Kill Hackers" is asking local officials for 4 bitcoins or they'll release city data online. Second major attack against Johannesburg after they've been hit by ransomware in July, when some locals were left without electricity.

The full Scariest Hack report from ZDNet is a **must read!** ,find it here: ZDNet – 2019 Scariest Hacks



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

According to the recently released LexisNexis 2019 Cybercrime Report **277 Million** human-initiated cyber-attacks from January to June 2019



Author: Chris Bester
chris.bester@yahoo.com