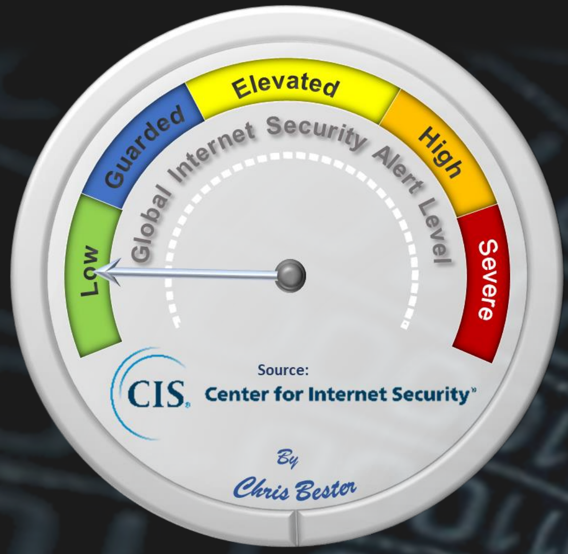

Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security®
By
Chris Bester

On December 18, 2019, the Cyber Threat Alert Level was evaluated and is being lowered to Green (Low).

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

27 December 2019

In The News This Week

Apple's Bug Bounty Opens for Business, $1M Pay-out Included

The tech giant is looking for full working exploits with any vulnerability submission. Apple has officially opened its historically private bug-bounty program to the public, while boosting its top pay-out to $1 million. Bounty hunters seeking that $1 million will need to provide a working exploit for a zero-click remote chain with full kernel execution and persistence on Apple's latest shipping hardware. The exploit will need to include a bypass for Apple's kernel pointer authentication code (PAC), which is a cryptographic signature mechanism. Other pay-outs range from $25,000 to $500,000 across a range of products, including Macs, iPhone and iPad, and Apple TV. Vulnerability types encompass those that enable lock-screen bypasses; unauthorized iCloud account access; attacks that require physical access to the device; and network-based attacks with or without user interaction that result in information exfiltration, code execution and more (these include attacks carried out via both physical and wireless/Wi-Fi/Bluetooth networks). Apple is also offering pay-outs for vulnerabilities that can be exploited via malicious applications. These include bugs that would allow an app to access sensitive data; execute kernel-level code; or carry out CPU side-channel attacks. Read the full story by Tara Seals here: ThreatPost

Apple Pulls the Emirati messaging app ToTok from its App Store

It Seemed Like a Popular Chat App but it is Secretly a Spy Tool. - ToTok, has been downloaded to millions of phones, is the latest escalation of a digital arms race. It is billed as an easy and secure way to chat by video or text message with friends and family, even in a country that has restricted popular messaging services like WhatsApp and Skype. But the service, ToTok, is actually a spying tool, according to American officials familiar with a classified intelligence assessment and a New York Times investigation into the app and its developers. It is used by the government of the United Arab Emirates to try to track every conversation, movement, relationship, appointment, sound and image of those who install it on their phones. ToTok, introduced only months ago, was downloaded millions of times from the Apple and Google app stores by users throughout the Middle East, Europe, Asia, Africa and North America. While the majority of its users are in the Emirates, ToTok surged to become one of the most downloaded social apps in the United States last week, according to app rankings and App Annie, a research firm. At the time of this writing, ToTok was still available for download from other app stores like Huawei's fledgling app marketplace. Read the full story here: NewYorkTimes

Hackers keep dumping Ring credentials online 'for the giggles'

Over the past two weeks, hackers have published thousands of valid Ring camera account credentials on hacking forums and the dark web. In most cases, they did it to gain a reputation in the hacking community, but also "for the giggles," in the hopes that someone else would hack Ring users, hijack their accounts, play pranks, or record users in their homes. These lists of credentials were compiled using a technique called credentials stuffing. Hackers used special tools and apps that took usernames and passwords leaked via data breaches and tested their validity against Ring's account system. Read the full story by Catalin Cimpanu here: ZDNet Article

Funniest Hacks - Hacked Road Signs Showed Hilarious Messages

Road signs play an important role in traffic management, informing drivers of obstacles ahead or the duration of a construction project. However, they make incredibly easy targets to hack thanks to the fact operators rarely change the system's default password. Even if the password happens to be changed, simply pressing "shift" and "ctrl" and typing out "DIPY" will reset the password back to "DOTS." This led to a spate of hacks in the late 2000s where pranksters put their own messages onto the machines. Passing drivers, likely confused as hell, saw anything ranging from jokes to song lyrics and even warnings about incoming zombies..

Read more funny hacks by Nathan Gibson here: Ranker

A decade of hacking: The most notable cyber-security events of the 2010s (Part 3)

Over the past decade, we've seen it all. We've had monstrous data breaches, years of prolific hacktivism, plenty of nation-state cyber-espionage operations, almost non-stop financially-motivated cybercrime, and destructive malware that has rendered systems unusable. This is part 3 of an adapted article from ZDNet

**~~~ 2016 Cont. ~~~**

The Shadow Brokers - Between August 2016 and April 2017, a group of hackers calling themselves The Shadow Brokers teased, auction, and then leaked hacking tools developed by the Equation Group, a codename for the US National Security Agency (NSA). These tools were top-shelf quality hacking tools, and they made an immediate impact. A month after the final Shadow Brokers leak, one of the tools (an exploit for the Microsoft SMB protocol, known as Eternal Blue) was used as the main engine behind the WannaCry global ransomware outbreak. To this day, the world has not found out who the Shadow Brokers are.

Mirai and the IoT nightmare - A blog post in early September 2016 introduced the world to Mirai, a strain of Linux malware designed to work on routers and smart Internet of Things devices. In the next 90 days, Mirai would become one of the most well-known malware strains in the world, after being used to launch some of the biggest DDoS attacks. Mirai's source code was released online, and it's one of today's most widespread malware family, with its code being at the base of most IoT/DDoS botnets. Mirai single-handedly made everyone understand that the S in IoT stands for security.

**~~~ 2017 ~~~**

The three ransomware outbreaks - We can't have this list without mentioning the three ransomware outbreaks of 2017 -- namely **WannaCry** (mid-May), **NotPetya** (late June), and **Bad Rabbit** (late October). All three were developed by government-backed hackers, but for different reasons. WannaCry was developed by North Korean hackers looking to infect companies and extort ransom payments as part of an operation to raise funds for the sanctioned Pyongyang regime, while NotPetya and Bad Rabbit were cyber-weapons deployed to damage Ukrainian businesses as part of the Russian-Ukrainian conflict. None of these entities meant to cause a global outbreak. The problem is that they relied on the **EternalBlue** exploit leaked moths before by the Shadow Brokers, an exploit that they didn't fully understand at the time, and each ransomware strain spread far beyond what creators initially intended. Ironically, despite being developed by the Russian government, NotPetya and Bad Rabbit ended up causing more damage to Russian businesses than companies in any other country, and this is most likely the reason why we haven't seen another untethered ransomware outbreak since 2017.

The MongoDB apocalypse - System administrators have been leaving databases exposed online without a password for years, but 2017 was the year when hackers finally started taxing admins and companies who did this. Informally known as the MongoDB Apocalypse, it started in late December 2016, but picked up steam by January the next year, with hackers accessing databases, deleting their content, and leaving ransom notes behind, asking for cryptocurrency to return the (non-existent) data. The first wave of attacks targeted exposed MongoDB servers, but hackers later expanded to other database technologies such as MySQL, Cassandra, Hadoop, Elasticsearch, PostgreSQL, and others.

Equifax hack - Mystery still surrounds the Equifax hack of 2017, during which the personal details of more than 145.5 million Americans, British, and Canadian citizens were stolen from the company's systems. Although we have a post-mortem, and we know the breach was caused by the company failing to patch a critical server, we still don't know who was behind the intrusion, or what were their motives -- if it's a cyber-espionage operation, or just good ol' cybercrime.

Cryptojacking - The rise and fall of cryptojacking can be tied directly to Coinhive, a web service that made it feasible to mine cryptocurrency via JavaScript, as a file that could be added to any website. Developed as an alternative to classic advertising, hacker groups took the idea and ran wild with it, placing cryptojacking scripts on any place that could run JavaScript -- from hacked websites to video game modules, and from router control panels to browser extensions. From September 2017 to March 2019, when Coinhive shut down, cryptojacking (also known as drive-by mining) was a scourge for internet users, slowing down browsers, and driving CPU usage through the roof, even if the technique wasn't particularly profitable.

Vault7 leaks - Vault7 was WikiLeaks' last good leak. It was a trove of documentation files describing the CIA's cyber-weapons. No source code was ever included; however, the leak provided a look into the CIA's technical capabilities, some of which included tools to hack iPhones, all the major desktop operating systems, the major browsers, and even smart TVs. At the time, WikiLeaks said it received the Vault7 data trove from a whistle-blower, who was later identified as Joshua Adam Schulte.

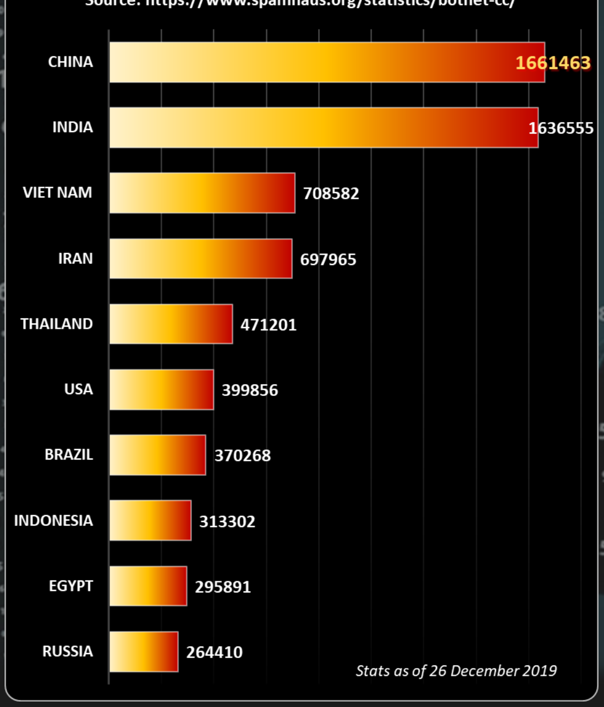
**~~~ 2018 ~~~**

Cambridge Analytica and Facebook's fall from grace - While nobody particularly liked Facebook before 2018, most people who had a problem with the company usually complained about its timeline algorithms that buried friends posts under a heap of useless garbage or the slow-loading UI that seemed to get more crowded each day. Then, Cambridge Analytica happened in early 2018, and the world had an actual reason to hate the social network and its data hoarding practices. The scandal, just one of the many which would follow in the months to come, exposed how data analytics companies were abusing Facebook's easy to grab user data to create profiles that they'd sell to political parties in order to sway public opinion and manipulate elections. From a place where users would visit to keep in touch with friends, Facebook became in many people's views the place where you'd be inundated with political propaganda disguised as internet memes and blatantly false information disguised as news articles. The Great Hack is a great documentary to watch if you ever need an insight look at the whole scandal..

In the fourth and final part next week, we will explore "Meltdown", "Spectre", the "Marriot hack" and others, taking us up to 2019.

Worst Botnet Countries by number of Bots

Source: https://www.spamhaus.org/statistics/botnet-cc/



Stats as of 26 December 2019

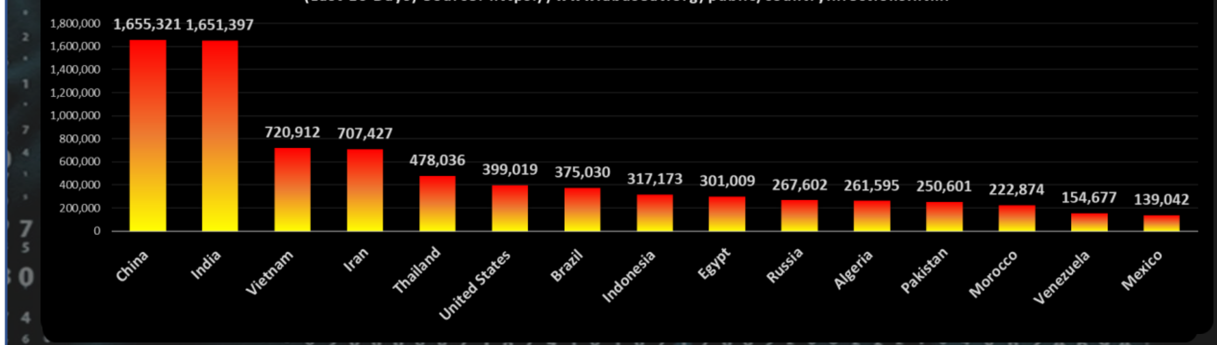
For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

Humour

No ma'am, according to our policy, your password must contain an Uppercase letter, a special character, a smiley face, a sprig of hyssop and an Egyptian scarab!

Composite Blocking List (CBL) - Number of Infections - Top 15 Countries

(Last 10 Days) Source: https://www.abuseat.org/public/countryinfections.html



Author: Chris Bester
chris.bester@yahoo.com