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

20 December 2019

In The News This Week

International repercussions as South African based Conor hit by massive data breach

Conor, a subsidiary of South African based IT company Adapt IT, suffered a massive data breach that exposed users' data. The breach was discovered by cyber security firm vpnMentor led by analysts Noam Rotem and Ran Locar. According to vpnMentor, the breached database contained daily logs of user activity by customers of ISPs using Web filtering software built by Conor. It exposed all Internet activity of these users including their search history, along with their Personal Identifiable Information (PII) data. This included highly sensitive and private activity, including pornography. vpnMentor says not only did Conor expose users to embarrassment by revealing such browsing activity, but they also compromised the privacy and security of people in many countries. They were also able to pull users social media logins. Conor is an information and communications technology company that develops software products for clients in Africa and South America and has an estimated 80 million mobile subscribers to their products, with some high-profile clients, including Vodafone and Telkom. Read the full story by Admire Moyo from ITWeb here: ITWeb

The humble Raspberry Pi has now sold 30 million tiny single-board computers

Developers and makers around the world have snapped up 30 million units of the Raspberry Pi since the diminutive British-designed computer began selling in February 2012. Raspberry Pi Foundation co-founder Ebert Upton had far more modest expectations at the outset, predicting sales of just 10,000 units. But the $35 mini computer — which has grown through four generations and branched out to the smaller form factor Raspberry Pi Zero — has turned into a permanent fixture on the DIY tech scene. Oracle earlier this year hailed its cluster of 1,060 Raspberry Pi boards the 'world's largest' Pi supercomputer, sporting 4,240 cores. NASA Jet Propulsion Laboratory (JPL) also uses the boards for its Mars mission. (This is a funny turn of events as I reported in this bulletin in June this year how NASA was hacked using a Raspberry Pi)
Read the full story of the Raspberry Pi success story by Liam Tung here: ZDNet Article

Ransomware 'Crisis' in US Schools: More Than 1,000 Hit So Far in 2019

Ransomware attacks have continued pummelling US schools, with 11 new school districts — 226 schools — hit since October, while major US cities such as New Orleans and Pensacola gradually recover from attacks this month. New data published by security firm Armor shows a total of 72 US school districts or individual educational institutions so far have suffered ransomware attacks this year, which means the number of victimized schools could be at 1,040 to date. Even more unnerving: 11 of those school districts — some 226 schools — have been attacked just since late October.," Read the full story by Kelly Jackson Higgins here: DARKReading

Funniest Hacks - The World's First Technological Hack: The Marconi Telegraph Troll

In 1903, the "father of modern radio," Guglielmo Marconi, was stationed on a cliff ready to demonstrate his new-fangled telegraph to the Royal Academy of Sciences. As he braced his fingers, ready to send a message more than 300 miles across the airwaves, the machine at the receiving end of the communication began pulsing strongly. The decoder spelled out the pulses into "RATS" several times before the messages launched into a seemingly random limerick. "There was a young fellow of Italy, who diddled the public quite prettily," it pronounced rudely, before launching into other miscellaneous quotations. It turned out a wireless engineer named Nevil Maskelyn from the Eastern Telegraph Company had set out to prove a point: that these telegraph messages weren't private. Indeed, they weren't.
Read more funny hacks by Nathan Gibson here: Ranker

A decade of hacking: The most notable cyber-security events of the 2010s (Part 2)

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 2 of an adapted article from ZDNet

**~~~ 2014 Cont. ~~~**

Carbanak starts hacking banks - For many years, experts and users alike thought that hackers seeking money would generally go after consumers, store retailers, or companies. The reports on Carbanak (also known as Anunak or FIN7) showed for the first time the existence of a highly skilled hacker group that was capable of stealing money directly from the source -- namely, the banks.
Reports from Kaspersky Lab, Fox-IT, and Group-IB showed that the Carbanak group was so advanced it could penetrate banks' internal network, stay hidden for weeks or months, and then steal huge amounts of money.
Mt. Gox hack - Mt. Gox was not the first cryptocurrency exchange in the world to get hacked, but it remains the biggest cyber-heist of the cryptocurrency ecosystem to this day. The hack, still surrounded in mystery today, occurred in early 2014, when hackers made off with 850,000 bitcoins, worth more than $6.3 billion today. At the time, Mt. Gox was the biggest cryptocurrency exchange in the world.
Phineas Fisher - The summer of 2014 is when the world first learned of Phineas Fisher, a hacktivist who liked to breach companies that make spyware and surveillance tools. The hacker breached Gamma Group in 2014 and HackingTeam in 2015. From both, the hacker published internal documents and source code for the companies' spyware tools, and even some zero-days. Phineas' leaks helped exposed the shadowy world of companies that sell hacking, spyware, and surveillance tools to governments across the world.
Heartbleed - The Heartbleed vulnerability in OpenSSL is one of those rare security flaws that are just too good to be true. The bug allowed attackers to retrieve cryptographic keys from public servers, keys they could use to decrypt traffic or authenticate on vulnerable systems. It was exploited within days after being publicly disclosed and led to a long string of hacks in 2014 and beyond, as some server operators failed to patch their OpenSSL instances, despite repeated warnings.

**~~~ 2015 ~~~**

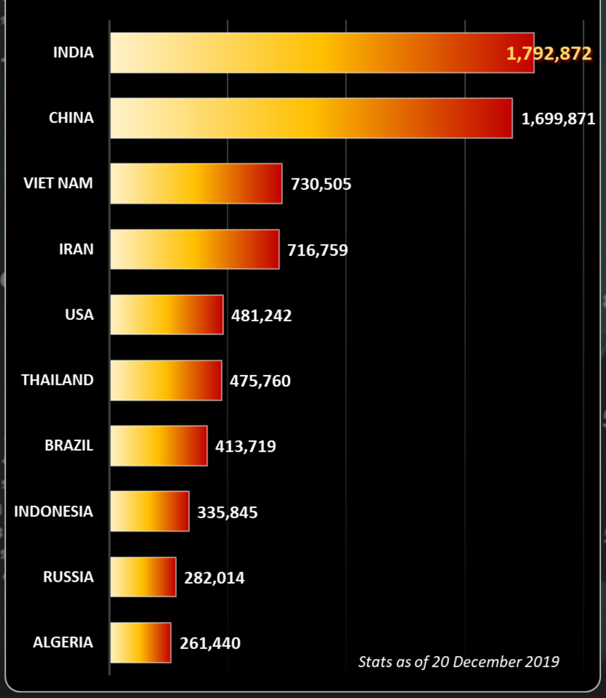
Ashley Madison data breach - There have been thousands of data breaches in the past decade, but ZDNet chose the most important one to be the Ashley Madison 2015 breach. The breach took place in July 2015 when a hacker group calling themselves the Impact Team released the internal database of Ashley Madison, a dating website marketing itself as a go-to place for having an affair. Users registered on the site faced extortion attempts, and some committed suicide after being publicly outed as having an account on the site. It is one of the few cyber-security incidents that led directly to someone's death.
Anthem and OPM hacks - Both hacks were disclosed in 2015 -- Anthem in February and the United States Office of Personnel Management (OPM) in June -- and were carried out by Chinese hackers backed by the Beijing government. They stole 78.8 million medical records from Anthem and 21.5 million records for US government workers. The two hacks are the crown jewel of a series of hacks the Chinese government perpetrated against the US, for the purpose of intelligence gathering.
SIM swapping - SIM swapping refers to a tactic where hackers call a mobile telco and trick the mobile operators into transferring a victim's phone number to a SIM card controlled by the attacker. Reports about attacks where SIM swapping was first used date back to 2015. Initially, most SIM swapping attacks were linked to incidents where hackers reset passwords on social media accounts, hijacked sought-after usernames, which they later resold online. SIM swapping attacks grew in popularity as hackers slowly realized they could also use the technique to gain access to cryptocurrency or bank accounts, from where they could steal large sums of money.
The Ukraine power grid hacks - The cyber-attack on Ukraine power grid in December 2015 caused power outages across western Ukraine and was the first successful attack on a power grid's control network ever recorded. The 2015 attack employed a piece of malware known as Black Energy and was followed by another similar attack the next year, in December 2016. This second attack used even a more complex piece of malware, known as Industroyer, and successfully cut off power to a fifth of Ukraine's capital. The group behind the attacks is referred to as Sandworm and is believed to be a section of Russia's military intelligence apparatus.

**~~~ 2016 ~~~**

Bangladesh Bank cyber-heist - In February 2016, the world found out that hackers attempted to steal more than $1 billion from a Bangladeshi bank, only to be thwarted by a typo and only get away with $81 million. While initially, everyone thought this was a bumbling hacker, it was later revealed that North Korea's elite hackers were behind the attempted cyber-heist, which was only one of the many similar hacks they tried that year -- successfully pulling others, in other countries.
Panama Papers - In April 2016, a consortium of the world's leading investigative journalists published extensive reports collectively named the Panama Papers that exposed how the world's richest people, including businessmen, celebrities, and politicians, were using tax heavens to avoid paying income taxes. The leak is considered the biggest of its kind and came from Panamanian law firm Mossack Fonseca. While journalists said they received the data from an anonymous source, many believe the data came from a hacker who exploited flaws in the law firm's outdated WordPress and Drupal sites to gain access to its internal network.
DNC hack - The hack that keeps on giving. In the spring of 2016, the Democratic National Committee admitted it suffered a security breach after a hacker going by the name of Guccifer 2.0 started publishing emails and documents from the organization's servers. Through forensic evidence, it was later discovered that the DNC had been hacked not by one, but two Russian cyber-espionage groups, known as Fancy Bear (APT28) and Cosy Bear (APT29). Data stolen during the hack was used in a carefully staged intelligence operation with the aim of influencing the upcoming US presidential election.
In Part 3 next week, we will explore "Shadow Brokers", "Mirai", the "Yahoo hack" and many more

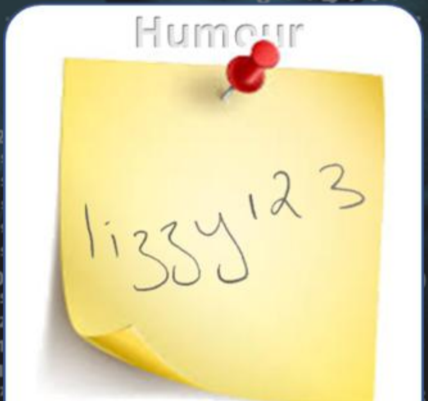
Worst Botnet Countries by number of Bots

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



Stats as of 20 December 2019

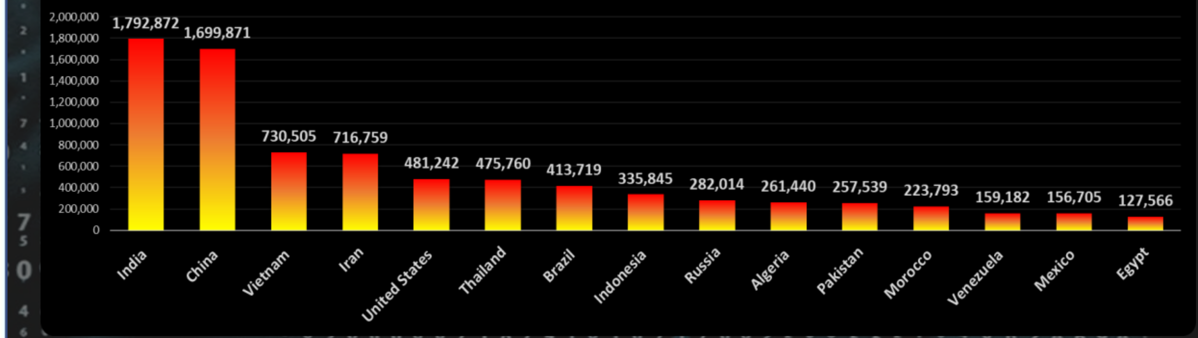
For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov



Post-it Notes, keeping passwords "*safe*" since the early eighties !

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