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

On April 15, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google, Grandstream, Mozilla, 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 April 2020

In The News This Week

As most of us are still in lockdown or quarantine, I trust that the news snippets below will somewhat divert your attention away from the realities of the COVID-19 pandemic that is still dominating our lives and the news.

Travelex Paid $2.3 Million in Bitcoin Following Ransomware Attack

Foreign exchange giant Travelex paid hackers $2.3 million in bitcoin to regain access to their network following a ransomware attack. Travelex's website, application, and internal network were forced offline as a result of the attack. According to a report by the Wall Street Journal, London-based Travelex paid hackers 285 BTC after being advised by experts on how to handle the ransomware attack. The report claims Travelex was in communication with regulators and partners throughout the course of the ransom and confirmed the original attack when it occurred on New Year's Eve.

Read the full story by Michael LaVere here: CryptoGlobe

Hackers Are Selling Windows Zoom Zero-Day Exploit for $500,000

Earlier this month multiple vulnerabilities were discovered and reported in Zoom's Windows and macOS clients, those vulnerabilities allow attackers to escalate privileges with macOS and to steal login credentials with windows. Motherboard reported that hackers are now selling zero-day exploits on the dark web. By exploiting the vulnerability attackers can hack and spy on users. Adriel Desautels, founder of Netragard said that "From what I've heard, there are two zero-day exploits in circulation for Zoom, one affects OS X and the other Windows". Multiple anonymous sources confirmed the existence of the exploits on the hacker's forums, the exploit code has not been analysed yet, but the brokers offering sales has been contacted." Read the full story here: GBHackers

Google is blocking 18 Million coronavirus scam emails every day

Scammers are sending 18 million hoax emails about Covid-19 to Gmail users every day, according to Google. The tech giant says the pandemic has led to an explosion of phishing attacks in which criminals try to trick users into revealing personal data. The company said it was blocking more than 100 million phishing emails a day. Over the past week, almost a fifth were scam emails related to coronavirus. The virus may now be the biggest phishing theme ever, Google says. Google's Gmail is used by 1.5 billion people. Individuals are being sent a huge variety of emails which impersonate authorities, such as the World Health Organization (WHO), in an effort to persuade victims to download software or donate to bogus causes. Cyber-criminals are also attempting to capitalise on government support packages by imitating public institutions..." Read the full story here: BBC News

News snippets from the past - Computers & crime

Feds flunk computer security exam - 2001

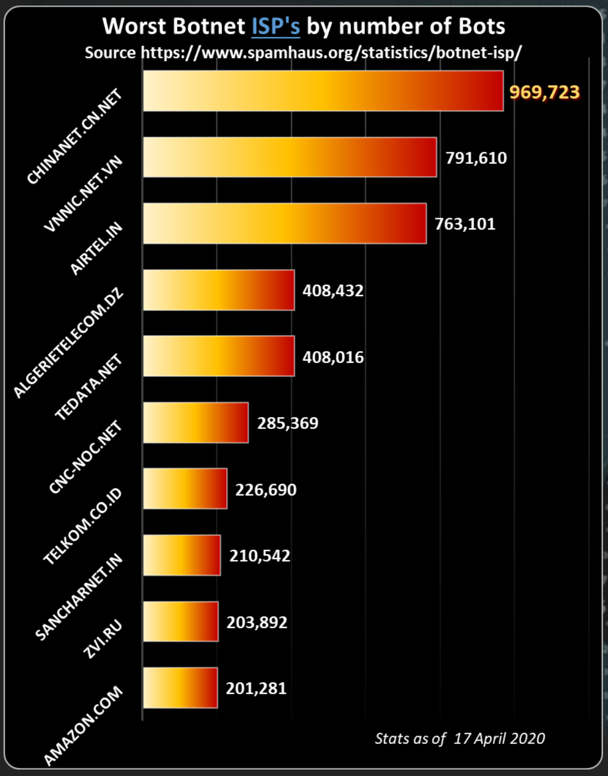
The following news snippet was found in Herald Tribune, Nov. 10, 2001

Washington – Despite dramatically tighter security at U.S. buildings since the terrorist attacks, a House panel is giving the government failing marks for lax protection of federal computers. The "F" grade dropped from "D minus" that the government earned in September 2000. Fully two-thirds of federal agencies – including the departments of Defence, Commerce, Energy, Justice and Treasury – flunked the latest "computer security report card".

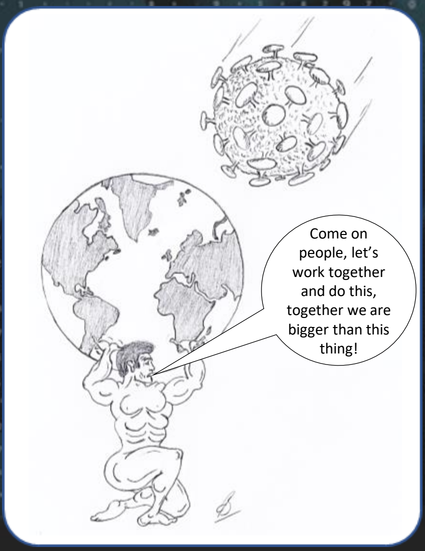
"The nation cannot afford to ignore the risks associated with cyber-attacks", said Rep. Stephen Horn, R-Calif., chairman of the House Government Reform subcommittee on government efficiency.

"Federal agencies rely on computer systems to support critical operations that are essential to the health and well-being of millions of Americans.

Read the full story and more here: GoogleArchives



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


Come on people, let's work together and do this, together we are bigger than this thing!

How saturated is our world with surveillance cameras?

Is it at all possible for modern day citizens not to be captured on some sort of a surveillance device?
Is individual privacy at all considered, or is this just an everyday reality that we all accept?

This week I'm exploring the extend of video surveillance across the world and I came across a recent study reported in CNBC World News that stated one billion surveillance cameras will be watching around the world by 2021. Already nine years ago, The Guardian reported that there's one CCTV camera for every 32 people in the UK. In November 2019, BBC News reported that there is now one CCTV camera for every 11 people in the UK. The report below indicates that on last count, the USA had 4.6 cameras per person and China approximately 4.1 cameras per person. The numbers are exponentially growing across the world as camera and facial recognition technology are forever improving and nowadays form part of a booming industry. This is fed by the rapidly growing mass production capability of the Chinese industrial engine. And don't kid yourself, everyone is buying from them. Another face of the surveillance picture is private home camera systems enabled, accessible and hackable through the phenomena of the Internet of Things or IoT for short. Let's also think of the real-time benefits surveillance systems like the Flir thermal cameras can produce in the current Covid-19 pandemic, where someone with a fever can be spotted a mile away.

But, before I get too carried away, for today, I'll bring to you two informative snippets I found starting with one written by Elly Cosgrove and published by CNBC which you can check out for yourself or read a slightly shortened and adapted version below.

CNBC Article

One billion surveillance cameras will be watching around the world in 2021— and more than half of those cameras will be in China — according to a report from IHS Markit published recently. The report comes as experts warn about the potential risks of such surveillance technology, including potential access to data by the Chinese government. There are an estimated 770 million surveillance cameras installed around the world today, and 54% of those cameras are in China, according to a pared-down version of the report, which CNBC has seen and that is set to be made widely available in Dec 2019.

China is home to some of the world's largest makers of video surveillance products, such as Hikvision, Huawei and Dahua.

China's push to export surveillance camera technology, which includes liberal democracies, has raised concerns over the risk of data being funnelled back to Beijing and the growing influence of the Communist Party, as experts told CNBC last year.

China has built a vast surveillance state that utilizes cameras powered by facial recognition software, including cameras perched on streets, buildings and lamp posts that can recognize and identify individual faces.

Chinese tech companies supply artificial intelligence surveillance technology to 63 countries — of those, 36 have signed onto China's massive infrastructure project called the Belt and Road Initiative, according to a September 2019 report by the Carnegie Endowment for International Peace think tank.

Some of these "smart city" projects are currently underway in countries like Germany, Spain, South Africa and France, according to analysis by the Australian Strategic Policy Institute (ASPI).

China currently has far more installed surveillance cameras than any other region in the world. The Americas are next in line, accounting for 18% of all installed surveillance cameras, and Asia, excluding China, accounted for 15%, the report said.

Those same regions will see the greatest growth of surveillance cameras over the next two years, the report said, driven by growth in developing countries like India, Brazil and Indonesia. These countries are expected to surpass Japan and the U.K. to join China and the U.S. as the top five largest markets for installed surveillance cameras.

The report also indicated that if the data were to be broken down by the number of installed surveillance cameras per person, the U.S. is actually not far behind China. In 2018, one camera was installed for every 4.1 people in China. In the U.S. during the same year, there was one installed camera for every 4.6 people.

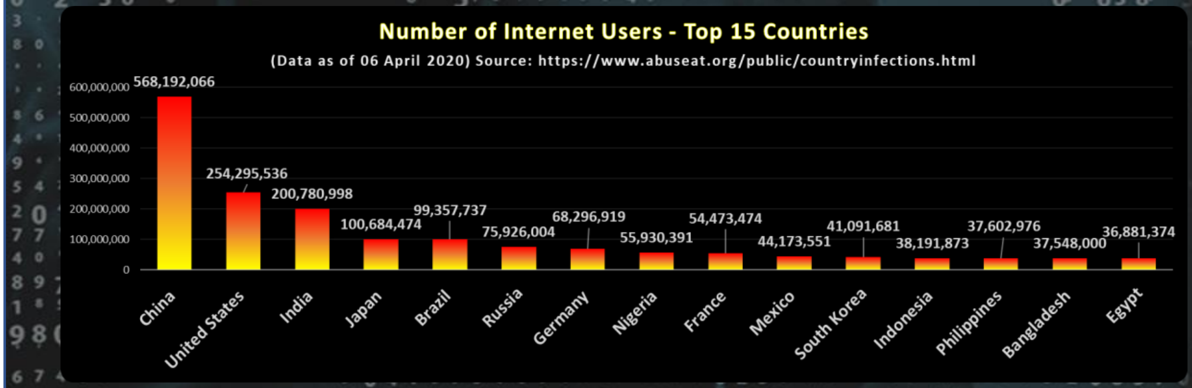
Around the same time of the article above, BBC News also reported on the subject. (Adapted version)

BBC News reported

All countries with a population of at least 250,000 are using some form of A.I. surveillance systems to monitor their citizens, says Steven Feldstein from the US think tank Carnegie. And it is China that dominates this market - accounting for 45% of the sector's global revenue. "Some autocratic governments - for example, China, Russia, Saudi Arabia - are exploiting A.I. technology for mass surveillance purposes,"

One place that offers an interesting insight into how China has rapidly become a surveillance superpower is Ecuador. The South American country bought an entire national video surveillance system from China, including 4,300 cameras.

"Of course, a country like Ecuador wouldn't necessarily have the money to pay for a system like this," says journalist Melissa Chan, who reported from Ecuador, and specialises in China's international influence. "The Chinese came with a Chinese bank ready to give them a loan. That really helps pave the way. My understanding is that Ecuador had promised oil against those loans if they couldn't pay them back." (*Melissa used to report from China, but was kicked out of the country several years ago without an explanation)*



Author: Chris Bester (CISA,CISM)
chris.bester@yahoo.com