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

Status Unchanged - On October 17, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google, Adobe, 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

25 October 2019

In The News This Week

City of Johannesburg and several banks under Ransomware attack.

The City of Johannesburg in South Africa reported a breach of its network on Thursday night 24 October 2019 and shut down its website and all e-services, hours after receiving a bitcoin ransom note from a group called the Shadow Kill Hackers. The hack occurred at the same time that several banks also reported internet problems believed to be related to cyber-attacks.

In a message on Twitter posted just after 11pm the city said it had "detected a network breach which resulted in an unauthorised access to our information systems".

"The incident is currently being investigated by City of Joburg cyber security experts, who have taken immediate and appropriate action to reinforce security measures to mitigate any potential impacts. As a result several customer facing systems — including the city's website, e-services and billing systems — have been shut down as a precaution." Customers will not be able to transact on e-services nor log queries via the call centre. The note on Twitter came after several city employees received the ransom note, which reads: "All your servers and data have been hacked. We have dozens of back doors inside your city. We have control of everything in your city. We also compromised all passwords and sensitive data such as finance and personal population information." The hackers then demanded the payment of 4.0 bitcoins by October 28 at 5pm failing which they will upload all the data onto the internet.

Both Standard Bank and Absa informed customers on Thursday of the internet problem, but at least five banks are believed to be affected.

Read the story here: BussinessLive

A Texas man found guilty of hacking the Los Angeles Superior Court (LASC) computer system and used it to send out phishing emails.

A Texas man, Oriyomi Sadiq Aloba (33), was found guilty of hacking the Los Angeles Superior Court (LASC) computer system and abusing it to send out roughly 2 million phishing messages. The phishing campaign aimed at obtaining the victims' credit card numbers. The man was sentenced by United States District Judge R. Gary Klausner to 145 months in federal jails, the judge also ordered him to pay $47,479 in restitution. Read the full article here: SecurityAffairs

US stopped using floppy disks to manage nuclear weapons arsenal.

US Air Force switches to secure solid-state-based solution to replace antiquated floppy disks in SACCS nuclear weapons management system.

The US Air Force has quietly replaced the infamous floppy disks it was using to manage the country's nuclear arsenal with what sources described as a "highly-secure solid-state digital storage solution."

The switch reportedly took place in June this year, according to defence news site C4ISRNET, citing Lt. Col. Jason Rossi, commander of the Air Force's 595th Strategic Communications Squadron.

Lt. Col. Rossi's unit is in charge of maintaining the US Strategic Automated Command and Control System (SACCS). SACCS is the communications system the US uses to relay messages and keep tabs on its nuclear capabilities, such as nuclear bombers, nuclear submarines, and nuclear depos housing intercontinental ballistic missiles.

Read the story here: ZDNet Article

Traveling a lot? Using Hotel and Airport free Wi-Fi services? Is it Safe?

When traveling, your main concern used to be keeping your passport and credit cards safe and also keeping your laptop, tablet or wallet from being stolen. What about using public Wi-Fi mostly offered for free at airports, hotel rooms, coffee shops and so forth?

As security measures on the web improved quite significantly over the last few years with SSL\TLS encryption that became the norm on most websites you traverse, still, if you are using public Wi-Fi, know that if it is for free, it generally means that your friendly host didn't spend too much on sophisticated firewalls and other perimeter defence mechanisms.
Kaspersky stated that in a recent survey, 70% of tablet owners and 53% of smartphone / mobile phone owners stated that they use public Wi-Fi hotspots. It is so convenient isn't it.

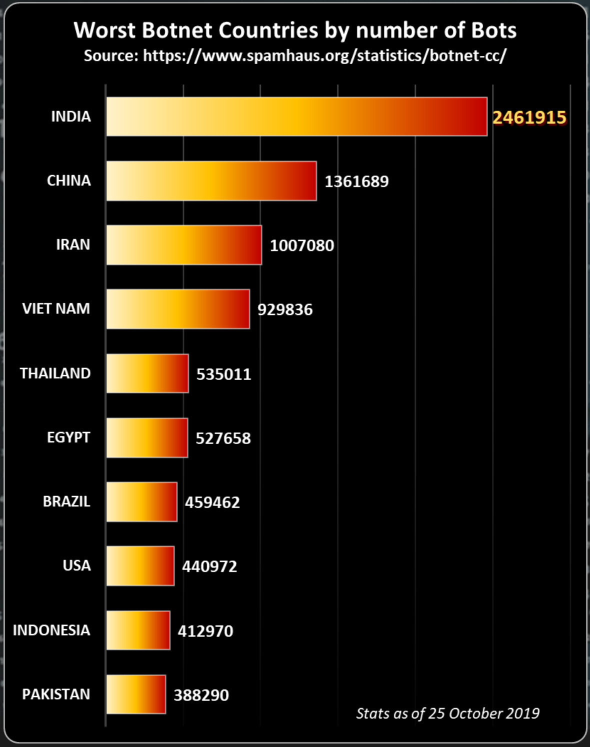
For the traveller, Hotel Wi-Fi networks are often completely open, requiring only a room number, code, or click-through to access the Internet. This lack of real encryption means your Internet usage is vulnerable to snooping from others sharing the network. If you are a mom that have to spend hours on end in supervised toddler play areas using their free Wi-Fi, these areas also became quite a target for cyber stalkers.

Remember, many hackers' ultimate objective is to get connected to an open network where multiple users are already connected, making public Wi-Fi networks a prime target. Once in, the hacker can use various tactics and methods to take control of all the communications traversing over this network.

Now, what can we do to protect ourselves when we are using public Wi-Fi or hotspots.

Let's explore some measures you can take to minimise the chances to fall victim to cyber crooks that wants your money, your credentials or even scarier your kids.

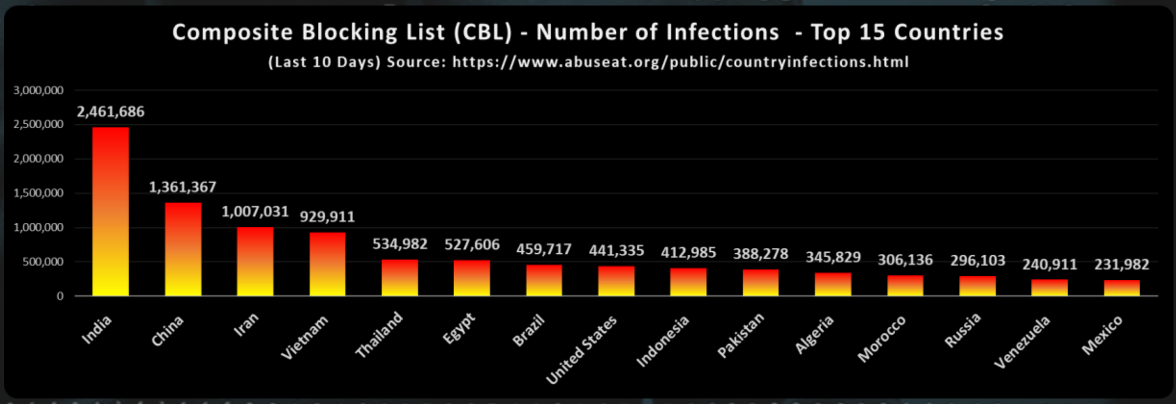
1. The first thing you have to look at is when connection to the hotspot or Wi-Fi, is to check if the connection is secured. Click on the little W-Fi icon 📶, normally in the bottom right-hand corner. In the dialog box that open, if you see a little shield with an exclamation mark in side next to the network you are connected to, it means that the connection is unencrypted and open. Your activities are traversing through the network in plain text. If there is no shield and it says "Secured" it generally means that the network has at least the basic security measures in place and data traverse encrypted.
2. Don't tick the "Automatic connection" option when connecting to the network, rather go through the pain and enter the PIN or password very time you connect.
3. If you are using a laptop or PC, turn off file sharing when you use a public Wi-Fi. On windows you can manage it from the Control Panel where you click on "Network Status and Tasks" and then on "Advanced sharing settings" Consult your system help guide for other operating systems.
4. Use a VPN - A VPN (Virtual Private Network) is the most secure option to surf on public networks. It is one of the most useful tools to help people keep their information secure when logged on to public networks. There is several free VPN's available, but it is probably better to acquire or subscribe to a VPN from a reputable vendor, it is mostly inexpensive for individual private users.
5. Use HTTPS - Whether you have access to a VPN or not, make sure you are only visiting SSL encrypted sites. Look for a small little padlock on either the left or right side of the URL address input window depending on the browser you use. If the full URL address line is displayed, it should start with "https://"If you see this it means it is encrypted.
6. Make sure the local firewall on your device is switched on and updated.
7. Make sure you have a reputable Anti-Virus program installed and make sure it is up-to-date
8. Once you leave the establishment that offered the Wi-Fi, tick the "Forget the network" option.
9. Now the most important of all, USE YOUR COMMONSENSE, if it looks to good to be true, it normally is. Be mindful of any "funny" items, pop-ups, links etc. that suddenly appear, it is normally a sign to get off that network as soon as possible.


Worst Botnet Countries by number of Bots
Source: https://www.spamhaus.org/statistics/botnet-cc/

Stats as of 25 October 2019

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

According to Radicati There are **3.9 billion** active email users, more than half of the global population vs. **3.5 billion** social media users as per a post by we are social


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