On January 31, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in PHP, Apple, and Magento 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

07 February 2020

In The News This Week

Microsoft says it detects 77,000 active web shells on a daily basis

In a blog post promoting the capabilities of its commercial security platform -- the Microsoft Defender ATP - Microsoft said that on a daily basis the company's security team detects and tracks on average around 77,000 active web shells, spread across 46,000 infected servers. But while the Microsoft blog post goes on to promote Defender ATP's industry-recognized detection capabilities, the nugget in Microsoft's recent marketing material is the 77,000 and 46,000 daily statistics. These two numbers are staggering in terms of size, and especially the 77,000 figure, which is far, far larger than any previous reports about web shell prevalence. For example, earlier this month GoDaddy's Sucuri reported on cleaning around 3,600 web shells from hacked websites during all last year, in 2019, a number dwarfed by Microsoft's daily detection count. If you are not familiar with what a "Web Shell" is, read the full story with an explanation by Catalin Cimpanu here: ZDNet Article

Google admits it sent private videos in Google Photos to strangers

Google is alerting some users of its Google Photos service that they've had their private videos sent to strangers by the search giant. Google's Takeout service, that lets people download their data, was affected by a "technical issue" between November 21st and November 25th last year. It resulted in a small number of users receiving private videos that didn't belong to them.

Google's nonchalant email alerting users doesn't provide any details on how many people were affected, nor the number of individual videos that were distributed incorrectly per account. Google fixed the issue after five days, and 9to5Google reports that less than 0.01 percent of Google Photos users who used Takeout were affected. Google Photos has over 1 billion users, so even a small percentage will impact a significant number of people. Google has apologized "for any inconvenience this may have caused."

Read the full story by Tom Warren here: TheVerge

Tracker, a South African vehicle tracking company, fell victim to a cybercrime attack this weekend

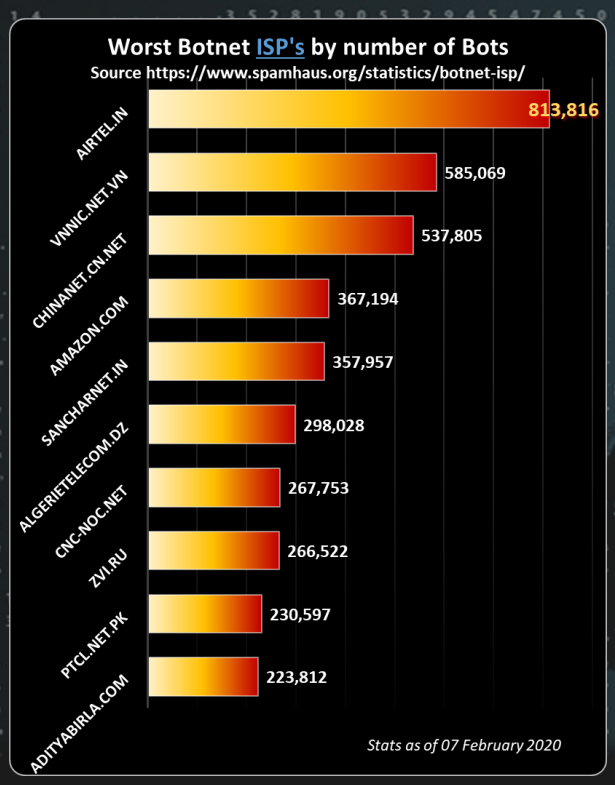
In a statement on their website the company said "Tracker has been targeted by a cybercrime attack in the form of ransomware that encrypted information on some systems, disrupting customer access to its services. However, while customers may not be able to access the Tracker system, the company said that it is continuing to successfully recover vehicles".

The company said that on detecting the malware, it immediately took its systems offline as a temporary precautionary measure, stopping the spread to other areas of its system. Tracker also deployed its IT and cyber security teams and is working closely with global and local third-party experts to resolve the matter. By Sunday morning, good progress had already been made to recover and restore some of the affected systems. At this time, there is no indication that any customer data has been compromised or accessed.

Read the company statement here: Tracker

Craziest IoT Device Hacks: Hackable sex toys

Last year, researchers from a tech firm SEC Consult announced that the private sex life of at least 50,000 users had been exposed by a sex toy 'Vibratissimo Panty Buster.' Multiple vulnerabilities put at risk not only the privacy and data but also the physical safety of the owners. All customers' data was accessible via the internet in such a way that explicit images, chat logs, sexual orientation, email addresses, and passwords were visible in clear text. But it's not the worst part. The 'Panty Buster' toys could be hacked to remotely inflict sexual pleasure on victims without their consent. Find more crazy hacks here: Finance Monthly



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

Google Maps Hack: The lighter side of things ☺

It was reported this week that a prankster, Simon Weckert, tricked Google Maps, the most popular navigation app in the world, into reporting a traffic jam on an otherwise quiet street.

Simon Weckert, a Berlin-based artist, loaded 99 second hand smartphones in to a red kiddies trolley cart with Google maps location open on all of them. He then picked a virtually empty street somewhere in Berlin and started walking up and down the street. The slow pace of the trolley cart and the fact that a whole bunch of phones were used caused Google Maps to believe that there were a lot of vehicles using a street that was actually empty. Apparently, he also did it in the street right outside Google's office in Berlin.

A video Weckert posted on YouTube, went viral which prompted Google to respond at least in a light-hearted manner. See the video here: Weckert

Weckert's hack prompted me to explore how Google Maps does it, how can it be so accurate and how can they give us near real-time traffic information? Below is an article on Gadgets360 by Ravi Sharma, explaining how it works.
(Thanks again to my good friend Yazan Shapsugh who pointed me to this story)

How Google Maps Gets Its Remarkably Accurate Real-Time Traffic Data

Google Maps is one of the most popular apps in the world, with well **over a billion users**. Google collects its mapping data from a wide variety of sources including road sensors, user contributions via Map Maker, and local transport departments, among several others.

Hidden away in Google Maps settings is the option to view traffic data for any location in real time. But how does Google collect this information, which is accurate to the last minute on most occasions?

Officially, Google says, "The traffic data comes from a variety of sources, including government departments of transportation and private data providers," among other sources. But there's more to it than just that. When it comes to traffic data and associated predictions, Google Maps users also help it out, **without even knowing they are doing so**.

Ever noticed that when you are using Google Maps navigation to reach your destination, it gives you alternate routes, or informs you of some unexpected traffic? This is because the Google Maps app on Android and iOS constantly send back real-time traffic data to Google. The data received from any particular smartphone is then compared to data received from other smartphones in the same area, and the higher the number of Google Maps users in an area, the more accurate the traffic prediction.

Another source of traffic data are users of Waze app, which Google acquired in 2013 for $1 billion; Waze users feed information like accidents and traffic jams on their routes into the app, which Google can use to make your navigation experience more accurate.

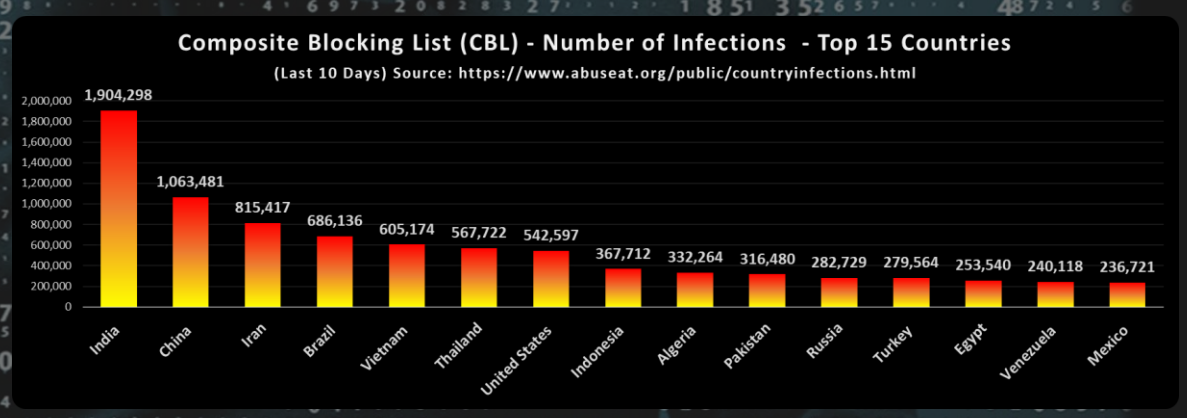
Since launch, Google has collected enough data to be able to predict the kind of traffic users can expect on any road at any time of the day. So for example, Google would know that traffic would be at a peak in the morning and evening, but not on holidays.

Using the historical data it has compiled over the years and traffic data from mobile devices using the Google Maps app, the company is able to create models for traffic predictions for different periods. For example, the modelling techniques would be able to predict that certain roads would experience more traffic during rains than other times of the year. Google also takes traffic reports from transportation departments, road sensors, and private data providers to keep its information up to date.

Amanda Leicht Moore, the Group Product Manager for Google Maps, told Tech Insider that the historical data allows it to inform Google Maps users if traffic on their route is better or worse than it typically is, and how much they will be slowed down by accidents of slowdowns.

And in cases where traffic is causing slowdowns on the road, but the route still remains the only way (or the fastest way) to a user's destination, the Google Maps sends alerts detailing the reasons behind the delay as well as informing the user that this is still the fastest route they can take.

But the accuracy of location data is unmatched only because of its users, since the billion Google Maps users on the road act as sensors for the app, which make the service as precise as possible. Of course, you can opt out of it by turning off Location Services for Google Maps in Privacy on your iPhone or turning off Google Location History under Location in the Google Settings option.



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