On August 7, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to multiple vulnerabilities in PHP.

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

16 August 2019

In The News This Week

Capital One hacker implicated on 30+ more copany breaches.

The Capital One breach is still in the news and revelations of more companies being hit by the same woman are creating waves of security concerns. Paige A. Thompson, the hacker accused of breaching US bank Capital One, is also believed to have stolen data from more than 30 other companies, US prosecutors said in new court documents filed this week. "The government's investigation over the last two weeks has revealed that Thompson's theft of Capital One's data was only one part of her criminal conduct," US officials said in a memorandum for extending Thompson's detention period.

"The servers seized from Thompson's bedroom during the search of Thompson's residence, include not only data stolen from Capital One, but also multiple terabytes of data stolen by Thompson from more than 30 other companies, educational institutions, and other entities."

US prosecutors said the "data varies significantly in both type and amount," but, based on currently available information, "much of the data appears not to be data containing personal identifying information."

US officials said the investigation is still ongoing and the FBI is still trying to identify all the companies from where Thompson stole data they found on her home server. "The government expects to add an additional charge against Thompson based upon each such theft of data, as the victims are identified and notified," prosecutors said.

The court documents don't list the names of any of the other 30+ companies that Thompson is believed to have hacked. However, according to previous media reports, this list might include companies such as Unicredit, Vodafone, Ford, Michigan State University, and the Ohio Department of Transportation.

Thompson, a former Amazon engineer, is believed to have breached AWS servers belonging to Capital One and the additional 30+ companies, from where she took proprietary information that she later stored on her home server. From Capital One alone, Thompson is believed to have taken the personal data of over 106 million Americans and Canadians.

After her arrest, Thompson told investigators that she did not sell or share any of the stolen data. In the new court documents, US officials said they haven't found any evidence to suggest that Thompson lied, which might reduce the extent of the 30+ breaches that she is accused.

As for the Capital One accusations, the US government believes it has a rock-solid case. "The evidence that Thompson committed this crime is overwhelming," officials said.

The court documents filed today, which argue for continuing to detain Thompson, also detail three stalking allegations, threats to "shoot up" a company's office, and threats to commit "suicide by cop" by pulling a fake gun on an officer and force the officer to shoot back. The US government also noted that Thompson's past behaviour appears to be related to "a significant history of mental health problems."

Read the full story here: ZDNet Article

Password tip: Use a pass phrase next time you change your password. Try something like "My dog is number 1". Remember spaces count as characters and in this example you have an 18 character password which will take a gazillion years to crack.

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

According to a 2019 survey by CyberSeek The U.S. has a total employed cybersecurity workforce consisting of nearly **715,000** people, and there are currently almost **314,000** unfilled positions

"IoT" Explained.

The Internet of Things (IoT) - IoT devices are more and more in the cyber security spotlight nowadays and was even a hot topic on the Black Hat USA 2019 conference last week. What is IoT really and why is it such a security concern? Below is an adapted simple explanation of IoT by Calum McClelland of iotforall (click to read the full article)

"How are you reading this post right now? It might be on desktop, on mobile, maybe a tablet, but whatever device you're using, it's most definitely connected to the internet. An internet connection is a wonderful thing, it gives us all sorts of benefits that just weren't possible before. Connecting things to the internet yields many amazing benefits. We've all seen these benefits with our smartphones, laptops, and tablets, but this is true for everything else too. And yes, I do mean everything.

The Internet of Things is actually a pretty simple concept, it means taking all the things in the world and connecting them to the internet. I think that confusion arises not because the concept is so narrow and tightly defined, but rather because it's so broad and loosely defined. To help clarify, I think it's important to understand the benefits of connecting things to the internet. Why would we even want to connect everything to the internet?

When something is connected to the internet, that means that it can send information or receive information, or both. This ability to send and/or receive information makes things smart, and smart is good.

Let's use smartphones (smartphones) again as an example. Right now you can listen to just about any song in the world, but it's not because your phone actually has every song in the world stored on it. It's because every song in the world is stored somewhere else, but your phone can send information (asking for that song) and then receive information (streaming that song on your phone).

To be smart, a thing doesn't need to have super storage or a super computer inside of it. All a thing has to do is connect to super storage or to a super computer. Being connected is awesome.

In the Internet of Things, all the things that are being connected to the internet can be put into three categories: (1) Things that collect information and then send it. (2) Things that receive information and then act on it. (3) Things that do both. And all three of these have enormous benefits that feed on each other.

Collecting and Sending Information - This means sensors. Sensors could be temperature sensors, motion sensors, moisture sensors, air quality sensors, light sensors, you name it. These sensors, along with a connection, allow us to automatically collect information from the environment which, in turn, allows us to make more intelligent decisions. On the farm, automatically getting information about the soil moisture can tell farmers exactly when their crops need to be watered. Just as our sight, hearing, smell, touch, and taste allow us, humans, to make sense of the world, sensors allow machines to make sense of the world.

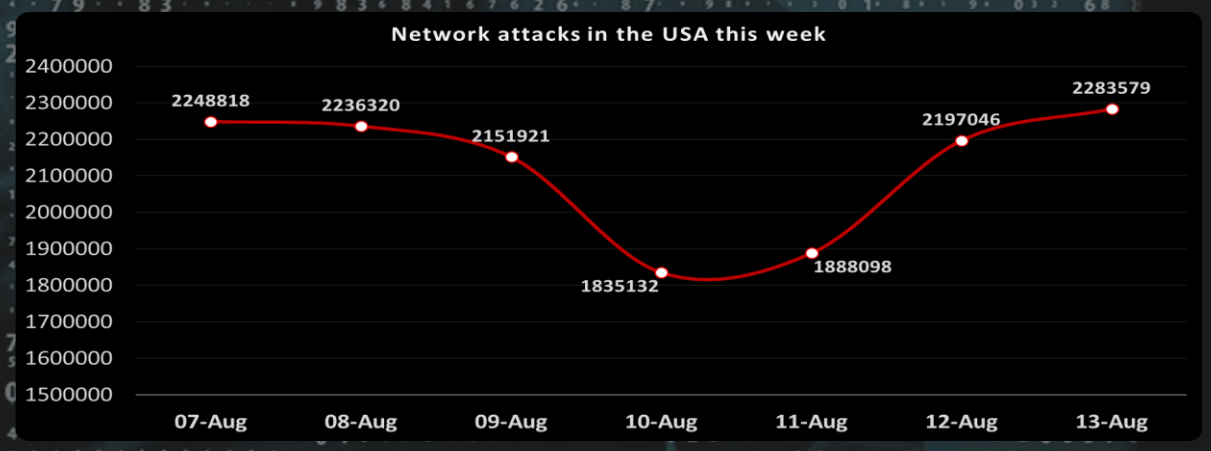
Receiving and Acting on Information - We're all very familiar with machines getting information and then acting. Your printer receives a document and it prints it. Your car receives a signal from your car keys and the doors open. The examples are endless. So what? The real power of the Internet of Things arises when things can do both of the above. Things that collect information and send it, but also receive information and act on it.

Doing Both - Let's quickly go back to the farming example. The sensors can collect information about the soil moisture to tell the farmer how much to water the crops, but you don't actually need the farmer. Instead, the irrigation system can automatically turn on as needed, based on how much moisture is in the soil. You can take it a step further too. If the irrigation system receives information about the weather from its internet connection, it can also know when it's going to rain and decide not to water the crops today because they'll be watered by the rain anyways.

The takeaway definition: The internet of Things, or "IoT" for short, is about extending the power of the internet beyond computers and smartphones to a whole range of other things, processes and environments."

The Security challenge – Many, or I'll dare to say even most of these smart IoT devices were never designed with security in mind. The fact of the matter is that if it's connected to the internet, it has an IP address, and if it is known to the internet it can be accessed. Whether it is a smart fridge, smart TV, moister sensor, security camera system or even a robot vacuum cleaner, it can be hacked and highly personal information can be gathered and used for criminal intent.

In a follow-up article I'll delve into things we could do or consider to make sure our IoT devices are secure and are not leaking information out to some dude sitting hallway across the world or as close as across the street.



AUTHOR: CHRIS BESTER
chris.bester@yahoo.com