On August 19, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Zoho, Apache, IBM and Google 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
21 August 2020

In The News This Week

Data breach exposes personal information of 24 million South Africans

Credit bureau **Experian** has suffered a massive data breach, exposing the personal information of as many as 24 million South Africans and almost 800 000 businesses to a "suspected fraudster". This is according to a statement by South African Banking Risk Centre (Sabric), which said Experian has reported the incident to law enforcement authorities and is working with "appropriate" regulatory authorities. "Banks have been working with Experian and Sabric to identify which of their customers may have been exposed to the breach and to protect their personal information, even as the investigation unfolds," Sabric said in the statement. "Banks and Sabric have also been co-operating with Experian in their efforts to secure the data and ensure the perpetrators are brought to book." Read the full story by Duncan McLeod here: TechCentral Also see other sources for latest updates: EWN, BussinessTech *(Thanks to my good friend Graeme Cartwright who pointed me to this story first)*

FritzFrog - New Fileless P2P Botnet Malware Targeting SSH Servers Worldwide

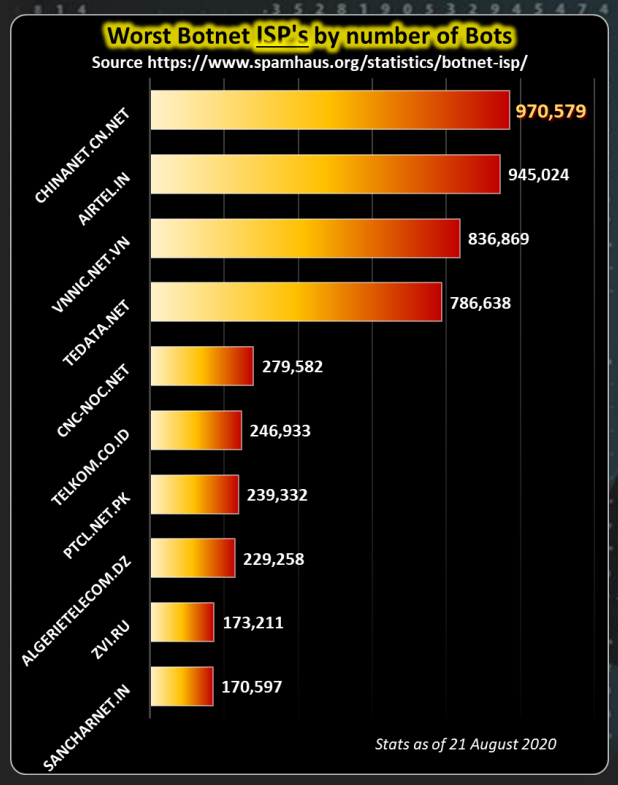
On Wednesday, cybersecurity researchers took the wraps off a sophisticated, multi-functional peer-to-peer (P2P) botnet written in Golang that has been actively targeting SSH servers since January 2020. Called "FritzFrog," the modular, multi-threaded and file-less botnet has breached more than 500 servers to date, infecting well-known universities in the US and Europe, and a railway company, according to a report released by Guardicore Labs on Wednesday. "With its decentralized infrastructure, it distributes control among all its nodes," Guardicore's Ophir Harpaz said. "In this network with no single point-of-failure, peers constantly communicate with each other to keep the network alive, resilient and up-to-date". In addition to implementing a proprietary P2P protocol that's been written from scratch, the communications are done over an encrypted channel, with the malware capable of creating a backdoor on victim systems that grants continued access for the attackers. Read the full story by Ravie Lakshmanan here: The Hacker News

Marriott faces London lawsuit over vast data breach

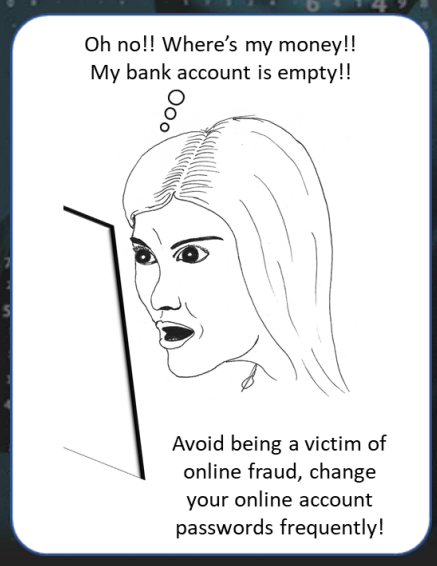
Marriott International, a leading hotel operator, is facing a London class action brought by millions of former guests demanding compensation after their personal records were hacked in one of the largest data breaches in history. Martin Bryant, founder of technology and media consultancy Big Revolution, is leading the claim for English and Welsh-domiciled guests after more than 300 million customer records from Marriott's global database, potentially including passport and credit card details, were hacked between 2014 and 2018. "I hope this case will raise awareness of the value of our personal data, result in fair compensation; and also serve notice to other data owners that they must hold our data responsibly," he said in a statement. The lawsuit, which seeks unspecified damages for loss of control of personal data, automatically includes guests who made a reservation for one of the former Starwood brand hotels - including Sheraton Hotels & Resorts and St. Regis hotels - before Sept. 10, 2018.. Read the full article here: Reuters

Hackers hijack design platform Canva to go phishing

Australian design platform Canva unwittingly provided phishing campaigns with graphics, making threat actors' schemes appear more legitimate as they pilfer credentials through social engineering trickery. Hackers hijacked the graphic design site, owned by the fast-growing company whose valuation recently grew from $3.2 billion to $6 billion, and used it to leverage other brands like SharePoint, Microsoft Office and DocuSign in their messages, according to a blog post by KnowBe4. The company's customers reported more than 4,200 malicious emails generated through Canva since mid-February, when phishing emails noticeably increased. "Businesses and their employees should be on the alert for phishing campaigns that exploit or spoof legitimate online services and brands," Eric Howes, principal researcher at KnowBe4 and author of the blog post, told SC. "This is not a new phenomenon, nor is it uncommon." Read the full story here: SC Media



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



How much of your personal data is on the Internet?

In light of all the major data breaches that made the news in recent months including the Experian breach mentioned here, I thought of highlighting what criminals are after and how much of your personal data could be available if a breach happens. In his article "The Digital Survival Blueprint" published in BankerX, Koshiek Karan dives into the topic which makes for real interesting reading. Below is a slightly adapted extract of the article but please read the full article with pictorials here: BankerX

The Digital Survival Blueprint (Extract)

1. Find out how many times you have been exposed

You have already been compromised, your data has been leaked and chances are, your entire history of cat videos you liked at 3AM is available to someone else. The weakest link in the chain of digital privacy are humans themselves. The recent Twitter breach (like the one at Experian) was thanks to an impersonated identity. Then again, some humans have been known to consume Tide Pods, set themselves alight (for fun) & blindly argue FRIENDS was a great TV show. Check out this site " ';–have i been pwned? " which will tell you when and where your data has been compromised.

Running a check on my personal email account, there was one major incident (there's most certainly more out there) where my personal details were compromised. Was it when I gave away my privacy in exchange for extra lives on Candy Crush 5 years ago? No – it was the exercise & calorie measurement app. Yet another reason not to watch what you eat. My morning pain au chocolat & double espresso habit found itself on the dark web.

Another useful site to check if any of your private accounts have been compromised is DeHashed. Ultimately, knowledge is power. You really can't solve for an unknown. Knowing the apps/ platforms that are most vulnerable helps make better choices. More importantly, it's a splash of icy water when you realize how real this is and sometimes this is the catalyst we need to be more vigilant. What can be done with your private information? "It's just an ID number, what's the worst that could happen?". The end use is endless. You could end up being married to someone you never met, end up purchasing items across the world or even have someone replace you in the world (even if you're dead). "Ghosting" isn't just when you stop replying to texts on Tinder – it's also when criminals steal the identity of dead people and take over bank accounts, apply for new credit and even file fraudulent tax returns. Personal information on the dark web is really cheap. Check out the price list: Dark Web Price Index 2020. It's actually disappointing that someone is willing to pay up to $75 for someone's Facebook account. Access to people you went to high school with selling Herbalife really isn't worth that much.

2. Find out the data your favourite apps collect from you

Every social media platform has an entire library of data on each of us. It's what makes targeted advertising work – ads which pop-up for a holiday to Bali, except you don't remember even letting Facebook know you wanted an island holiday. It's creepy, unnerving and strangely accurate. I downloaded my Facebook data & here's what I found: My entire contact list, their phone numbers & the number of times I contacted them together with a full list of advertisers who have my information on a contact list for targeted marketing. It contains a list of thousands of interests, tags & an activity log that helps target ads… It even shows my fondness for garlic bread… Every tiny little facet of you which hints at a preference, it locks it in and records it. Everything. It's forensic.

Location services meant Facebook recorded every one of my moves, every single day since joining. It gives you the GPS co-ordinates. That little wine tasting trip? It knew every detail & had it recorded.

In the folders listed are every message I have ever sent, received, read or deleted via messenger. It even has a log of every sticker used. There's a full record of every friend request you denied & every person you unfriended. It lists every picture I ever took/ was tagged in and every single FB search and every song I listened to & the time I listened to it. Every single vote I clicked on. Every like, comment, emoji, page visited, link you click, video you watch, person you tag… every click is a data entry onto your online DNA & lives forever.

Following is some useful links and Instructions on how to get hold of your personal data:

(1) Download your Facebook Data; (2) How to access all the data Twitter collects on you; (3) Request a copy of your personal data on Tinder: (4) How to download your Instagram personal data. - This is only to name a few, just Google the other social media platforms that is not mentioned, instructions are readily available.

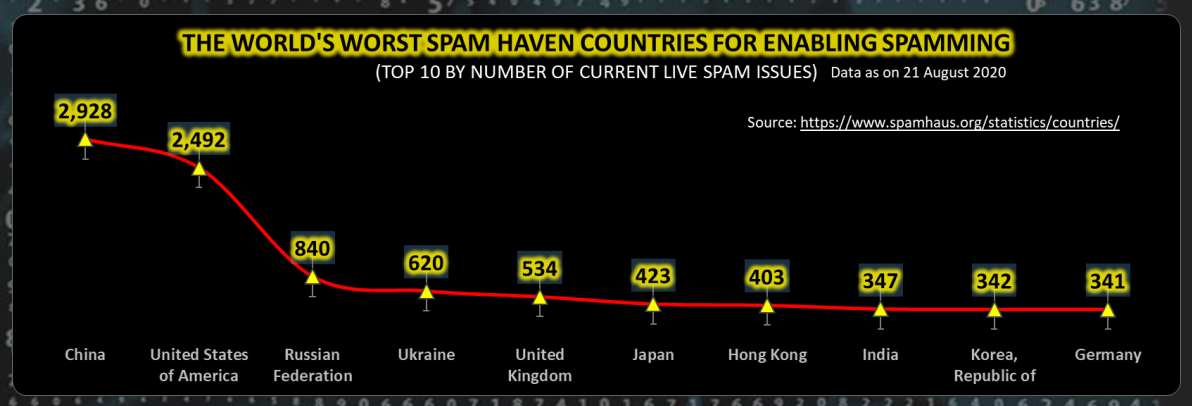
3. Protection

a) If you landed in the crossfire of the Experian breach and you live in South Africa, you can apply for free Protective Registration - The Southern African Fraud Prevention Service (SAFPS) will alert all of its members (which include all of the main local banks and credit providers) that your identity is compromised or your physical Identity document or passport is lost or stolen. Register here SAFPS, its free and anyone in SA can register. Find out if a similar service is offered in your country of residence.

b) Use common sense – e.g. The bank will never phone you up or send you an email asking for your password – ever.

c) Practice good online login hygiene - Two-factor authentication, secure devices and strong passwords are non-negotiable.

d) Get insured - Check with your insurance provider and find out about personal liability insurance that covers identity theft.



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