08/04/21

Thursday Thoughts – 8th April 2021

This week's Thursday Thoughts has news on new targets for the cybercriminals namely the new "rogue Netflix app" which actually takes over your WhatsApp account and sends automatic replies to your incoming messages, a LinkedIn Trojan based on your job profile, the introduction of Morse code into emails to bypass security features and new way for your Bluetooth to be used against you which is called "bluebugging". There is also some worrying advice that we are developing unhealthy internet habits, with the news that online gaming addiction is on the increase.

As well as details of how you can check if your Facebook account was part of their recent data breach I have included some detail on why businesses may want to consider moderating work tools like Slack. There is also news of a new Expedia COVID Travel Tool.

On my watch list is the potential impact of France mandating a "Decline All Cookies" Button for websites, so far just those that receive traffic from France. If you are a VMware user you will want to read about their Carbon Black Cloud Workload product update. Finally in an interesting twist in the WeLeakInfo story the cybercriminals themselves are being targeted because their personal details (including credit cards used to purchase lists of breached accounts) have been leaked on the dark web.

Blogs and Videos of the Week
Emily Overton -Deciding what HR records to scan
Debbie Reynolds/Pamela Gupta - The Privacy impact of biometric tracking in the workplace
Bjarke Ingels, John Schellnhuber - The New European Bauhaus - From Vision to Reality

Keeping your Email Safe

We are seeing an increase in the use of creative bypasses in email filters. In some cases if you highlight the text and right click it, you will find that the entire text was encoded (in some cases even using Morse code) and then translated back as text on the screen. The advice to guard against this is to always be suspicious and check that the link you have been sent is real!

Watch out for Fake Netflix Links in WhatsApp

There's another bit of malware which can be downloaded from the official Google Play Store and is propagated through WhatsApp messages. You need to keep your eyes open for a rogue "Netflix" App named "FlixOnline". The app is designed to monitor the user's WhatsApp notifications, and to send automatic replies to the user's incoming messages. To guard against this we should be wary of download links or attachments that they receive via WhatsApp or other messaging apps, even when they appear to come from trusted contacts or messaging groups.

#thursdaythoughs is a weekly summary of Cyber Security matters from Sam Alford @pppmauthor

Previous Editions can be found on https://www.pppmanagement.co.uk/blog-1

Latest Hackers Target – Your Phone (using Bluetooth)

Most of us keep our Wi-Fi and Bluetooth enabled on our devices all the time because it is so helpful. This week I heard of a new attack 'bluebugging' which I thought I'd share. It is where hackers use software to detect nearby Bluetooth devices, check which networks your device has previously connected to and try to replicate one of these trusted networks. and then bombard your device with malware, spy on you and even intercept and redirect phone calls, access bank details, send or receive files or simply watch what you are doing in real time. It is often performed in busy public places, most recently Bournemouth, and bombard the targets with messages as they walked through the city.

The recommendation is that you disable Bluetooth whenever it is not in use, disable file-sharing services like Airdrop or Fast Share unless you are sending or receiving files from a trusted friend and install an antimalware app installed on your smartphone, tablet and Bluetooth-enabled computers.

Mobile Gaming Addiction Is On The Rise

The increase in substance abuse that has come about as a result of the pandemic has been well documented. But are you aware of the other type of addiction that experts warn is on the increase- online mobile game addiction and unhealthy internet usage. According to Apple Insider there was a 10% increase in downloads from both Apple and Google App stores in the first quarter of this year and nearly 3 times as many gaming apps than non-gaming ones were downloaded in 2020. If you are one who has developed unhealthy habits or are spending too much time scrolling on the phone you may want to consider using a screen time control app or checking if your antivirus software has integrated parental control features that could help you manage screen time.

A New Spear-Phishing On LinkedIn

This is basically a weaponized job offer. The sophisticated backdoor trojan called "more eggs" uses phishing lures (malicious ZIP files) with the same name as that of the victims' job title. You know the one you have on your LinkedIn profile. In the example I saw if the LinkedIn member's job is listed as Senior Account Executive—International Freight the malicious zip file would be titled Senior Account Executive—International Freight position. When the fake job offer is opened the victim unwittingly initiates the trojan.

Is Your Account Part Of The Facebook Data Breach?

Upwards of 533 million Facebook users from 106 countries have had their personal data leaked online, including phone numbers, Facebook IDs and date of birth. If you want to check if you are part of that breach the free site that tracks data breaches "Have I Been Pwned" has been updated to include a phone number search. If you do find out that your

#thursdaythoughs is a weekly summary of Cyber Security matters from Sam Alford @pppmauthor

Previous Editions can be found on https://www.pppmanagement.co.uk/blog-1

data has been compromised the best thing to do is change the passwords of compromised sites and use two-factor authentication for additional security.

Who Is Moderating Your Remote-Work Tools

Businesses are seeing an increase in remote-work TROLLs, harassment, sexism, and racism on remote work platforms like Slack! These spaces are largely unmoderated and therefore it is up to the company to protect employees. In an unusual move Slack's help centre will also assist if an employer doesn't take action. Maybe this is the start of something from the big corporates.

Expedia Launches a new COVID Travel Tool

Expedia Group has launched a New COVID-19 Travel Advisor Tool. This provides travellers with current details about travel restrictions worldwide and hopes to simplify the experience for people who are looking for advice about prospective destinations. Following the success of the pilot phase more than 1.6 million travellers used the COVID-19 Advisor in the winter of 2020. The tool provides destination-specific information about restrictions and travel information is considered to be critical to rebuilding traveller confidence.

France take the Lead and Mandate a "Decline All Cookies" Button

As of March 31 2021 the French Data Protection Authority (CNIL) require websites to add a "Decline All" button to their cookie banner for "traffic from France". This is to allow visitors to reject all non-essential cookies quickly and easily (news media and others who try to get round the problem by making the process more complex should take note). I wonder how long it will be before other Data Protection Authorities (the ICO for example) to follow their lead.

Critical Auth Bypass Bug Found in VMware

It is reported that the administrative interface on VMware's Carbon Black Cloud Workload (data centre security product) can be manipulated to bypass authentication thereby allowing an adversary with network access to the interface to gain access to the administration API of the appliance. Armed with the access, a malicious actor can then view and alter administrative configuration settings. The company have issued an update to combat this bug.

WeLeakInfo Customer Details Leaked Online

In an interesting twist the personal information of about 24,000 WeLeakInfo customers (a website that used to sell personal data on the dark web) was recently leaked on the dark web. It included the details of anyone who has made a purchase on the site on their credit card using Stripe. It is possible that these individuals (cybercriminals who purchased illegal databases to target the unsuspecting/trusting public) are now finding themselves targeted

#thursdaythoughs is a weekly summary of Cyber Security matters from Sam Alford @pppmauthor

Previous Editions can be found on https://www.pppmanagement.co.uk/blog-1

by law enforcement agencies in affected countries or those who have the tools to connect the dots and use the information to find out what sort of person purchases stolen data.

Blogs and Videos of the Week

Emily Overton -Deciding what HR Records To Scan

This blog from Emily discusses the pros and cons of going paperless in HR. It is all a case of balancing risk against reward. It is refreshing to hear someone else say that going paperless is not something to aspire to. A completely paperless environment is just not realistic and some records you will probably never use again but may need to keep as evidence (in rare cases). So if you are contemplating your paper archives think hard about what it is you are trying to achieve, and how much it is likely to cost in time and storage. Finally check out BS10008:2020 and then get some specialist advice. https://rmgirl.co.uk/2021/02/12/part-4-deciding-what-hr-records-to-scan-for-paperless/

Debbie Reynolds/Pamela Gupta - The Privacy Impact Of Biometric Tracking In The Workplace

There are massive potential Cybersecurity and Data Privacy impacts of the introduction of of biometric tracking in the workplace. This was particularly brought into focus because of Amazon's plan to track their drivers behaviour by the use of Biometrics. In the latest Data Privacy and Cybersecurity Fix video, Debbie Reynolds and Pamela Gupta Global discuss reasons why biometric data should have special protections, what the law says and the attendant privacy or cyber risks. You can watch it here: https://www.youtube.com/watch?v=k2F_od5VneE

Bjarke Ingels, John Schellnhuber - The New European Bauhaus - From Vision to Reality

Despite popular demand there is still lots to do on climate change. In this video Bjarke and John discuss the "New Bauhaus" and how to change the future for our planet . I was really interested to hear their ideas on how we can fundamentally change our development models to include nature and treat it as a whole. Some of the examples are phenomenal especially how wood can be used to create a carbon negative building. https://www.youtube.com/watch?v=ucpBYUw6b2M&list=PLxaUSBUUlSvh5KvBrb485FSWm63kLBeBo&index=18