Thursday Thoughts – 15th April 2021

This week's Thursday Thoughts comes amid news of sanctions for Russia because of amongst other things interference in the US election and for being behind a the SolarWinds attack there is a new malware "Saintbot" that steals your passwords and is designed to not execute in Romania or CIS countries, now who could be behind that we ask!

There is more on the LinkedIn Trojan circulating which is based on your job profile, and an advisory from the NCSC because it is so concerned that many organisations in the UK have not yet downloaded the patch for the Fortinet VPN vulnerability and their credentials may have been shared on the dark web. There are new vulnerabilities to be aware of in Chrome, and an increase in the old faithful "this is Microsoft" phone call harassing the vulnerable. You may also be missing out on some useful security enhancements if you haven't updated your Zoom recently. The blurred background would have been so useful for the Estate agent who exposed his client's personal data in the 3D tour of his house. It is so important to think what it is you are sharing on line – you only have to think about journalists telephoto lenses capturing government documents to realise the importance.

Blogs and Videos of the Week

Karen Watson (My Life Digital) - Rebuilding Consumer Trust After Cambridge Analytica
Luke Robert Mason, Debra J Farber, Alexander Hanff - Breaching Clubhouse

Spoof Job offers for LinkedIn Users

You may have missed this last week so it's worth repeating there have been a spate of spoof jobs offered to LinkedIn users. Experts are warning that criminals are taking the job title on an individual's profile and creating a malicious zip file with the job title as the position offered. When an individual opens the fake job offer a trojan is downloaded onto their device which contains that allows malicious software to be downloaded as well as harmful plugins. These may even give the criminals access to the victim's computer without their knowledge.

In the UK you can report this sort of incident to Action Fraud or direct to the NCSC. Emails can simply be forwarded to report@phishing.gov.uk texts can be forward to 7726.

The NCSC will then investigate all reports received. Since April 2020 more than 5,500,000 reports have resulted in the removal of more than 41,000 scams and 81,000 URLs.

NCSC issue an advisory about Fortinet VPN

The NCSC is so concerned that organisations in the UK have not yet downloaded the patch for the Fortinet VPN vulnerability CVE-2018-13379 that it has issued an advisory on the matter. In November 2020 it was discovered that credentials for 50,000 vulnerable Fortinet VPNs worldwide were stolen and subsequently shared on a criminal forum.

In addition to stealing credentials, criminals have also stolen and published the session IPs of over 600 IPs located in the UK. The advice from the NCSC is that if you have not installed the updates yet you should now assume that you have been compromised and to begin incident management procedures. Users should check whether the 2019 updates have been installed. If not then remove affected device from service, returned it to a factory default and reconfigure it before it returns to service.

HMRC and Microsoft "cyber scams" on the increase

Once again, I hear news of the vulnerable being targeted with HMRC, COVID Vaccination, Television Licence or Microsoft Scams. Last week another cold call was made to an elderly family member claiming to be from Microsoft and wanting to talk about their computer. There isn't even a computer in the house! It is concerning how frequent these calls come and how troubling the vulnerable find them.

While it is impossible to list all the scams however, this is a brief outline of the types of scams that are being seen and how to guard against them. The key message is to remain vigilant and take steps to protect yourself. The cyber security agencies continue to work with law enforcement and industry partners to disrupt or prevent cybercrime activities.

Threats at the moment include:

- Phishing, using Linked in Profiles or HMRC Grants
- Distribution of malware with a coronavirus/COVID-19 theme
- New domain names being registered with coronavirus related titles
- An increase in SMS and phone a on the vulnerable
- Scams which pretend to come from "UK government" or a trusted organisation.

What should you watch out for?

- Authority - Is the sender claiming to be from someone official?
- Urgency - Are you told you have a limited time to respond?
- Emotion - Does the message make you panic, fearful, hopeful or curious?
- Scarcity - Is the message offering something in short supply?

If you receive a Phishing email you can report it to Crime Stoppers or forward it to the NCSC.

Zoom

When was the last time you updated your Zoom software? You may find that until you do your Zoom does not work quite like other peoples does. Some of the most recent updates are blurring of backgrounds and security settings for meeting hosts. Also, I find it better to log into Zoom rather than just follow a link. It seems that way you can share screen more easily etc.

Promoting privacy and data protection in Ukraine and CIS countries

There is news this week of Privacy Hub an NGO who are eager to create a community of privacy professionals to raise privacy awareness in Ukraine and CIS countries. The NGO, with the UNDP are creating educational series to build awareness of the need to protect personal data and a project to help Ukrainian companies assess their compliance with Ukrainian data protection legislation and the GDPR.

New Flaw in Chrome, Opera, and Brave Browsers

News of yet another flaw in Google Chrome, Microsoft Edge, Opera, and Brave. This time in the V8 JavaScript that powers the web browsers. Google has addressed the issue in the latest version of V8 but it hasn't made its way into mainstream yet so browsers could still remain vulnerable to attacks.

A New Malware that Steals your Passwords

Theres a new malware out that is being called "Saint Bot" which uses a wide variety of techniques and starts with a phishing email that claims to be a bitcoin wallet but actually contains an embedded ZIP file ("bitcoin.zip"). Clicking on the zip file then downloads the next stage malware, a WindowsUpdate.exe executable, which, in turn, disables Windows Defender and connects the computer to a command-and-control (C2). The malware is designed to not execute in Romania and select countries within CIS – no prizes for guessing where it was developed then!

Crypto-related traffic increases

Business interest in cryptocurrency is currently on the increase with reports that it has increased 7fold since the beginning of the year. This is driving interest in underlying platforms. You can read more here: https://research.g2.com/insights/blockchain-investment-drives-cryptocurrency-market-growth

What can Be Seen on Your Virtual House Tour?

A UK estate agent was in trouble this week when it emerged that the 3D tour of a house that he was marketing had a large amount of personal information visible in the

background. Shockingly this included financial paperwork in the study which could be read by

New ICO guidance on the Relationship between PECR and the UK GDPR

The ICO has released new guidance on the relationship between PECR, the Data Protection Act 2018 (DPA) and the UK GDPR. In particular where the PECR rules apply. Did you know that if you are setting cookies then you should consider PECR compliance **before** you look to the UK GDPR. There are exceptions and if your cookie meets one of the exemptions, then the requirement to have consent to set it doesn't apply but it is really quite complex and I would recommend you check out the ICO website link below (you will find Figure 1 very helpful as it includes a flow chart for consent for cookies. https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-the-cookie-rules-relate-to-the-gdpr/

Blogs and Videos of the Week

Karen Watson (My Life Digital - Rebuilding Consumer Trust After Cambridge Analytica
In my life digital's ThrowbackThursday blog this week, Karen discusses how Cambridge Analytica and Facebook could rebuild relationships in the aftermath of the #DeleteFacebook campaign. This story illustrates that customers have a large part to play in challenging the behaviour of big tech businesses. Some would say that their reach is greater than the regulatory authorities "Organisations need to be seen to be using data with respect, not in ways that create suspicion and mistrust, causing customers to untick all the boxes, refuse cookies and shroud themselves in anonymity." You can read the blog here: https://mylifedigital.co.uk/rebuilding-consumer-trust-after-cambridge-analytica-2/

Luke Robert Mason, Debra J Farber, Alexander Hanff - Breaching Clubhouse
Many of us are increasingly cautious with our online privacy online and this conversation looks at the latest issues discussing illegal profiling, data processing, the need to read the privacy polities before signing up to something on line. The unlawful privacy violations of Clubhouse come under scrutiny in this discussion and it is quite worrying the potential fines businesses who have signed up and shared their contacts with the platform may face. An interesting watch: https://vimeo.com/525620622/ad5114f7d8