THURSDAY THOUGHTS

The focus this week in the cyber world has been very much on phishing scams (email and text) many of which have purported to come from "trusted" organisation such as Oxford University, HMRC, Samsung, Adobe and the Bank of America. There is therefore a continuing need for us all to be vigilant and aware of this continuing risk. Talking of which I received a TV licence phishing email myself this week titled 'YourLicence DirectDebit Support'. Following my own advice I forwarded it to the NCSC using their "Suspicious Email Reporting Service" reporting tool. This proved really easy to do. I also received a reply from the NCSC who say that since the service was launched at the end of April they have removed 1,387 malicious sites which is really good news for us all.

Of concern to many will be the vulnerabilities affecting VPN products from Pulse Secure, Fortinet and Palo Alto and within approximately 79 different Netgear routers. There has also been a ransomware attack against Conduent the IT service provider and worrying news that Aerospace and military officials are being targeted by hackers posing as HRs offering jobs but who's intent is to conduct espionage against the organisations the individual works for. News this afternoon included an update on UK COVID19 Track and Trace and Mike Ouwerkerk shared a really pithy post this week "What does malware do" which I have included just before the Blogs section as it will be a really useful way to share the information with our families and colleagues.

My "Blogs of the week"

Sara Kay - The Daily Giggle Channel… any place, anywhere, virtual laughter…
Emily Overton - How records management can help with cybersecurity
Gareth Perry (Databroker) - Cheap data will never leave you cheerful

NCSC warn of a UK wide automated, ongoing phishing campaign

The NCSC warn that the automated widespread phishing campaign which has been active since 2018 is still spreading indiscriminately across a very broad range of UK sectors. The problem starts with a user receiving a phishing email from a legitimate and known email account (which has been compromised).

Here are some things to watch out for:

- Emails where the subject line contains the compromised user's address-book entry for the recipient (the recipient's name, the email address or may just be blank)
- A black ellipsis with a grey highlighted background and a single sentence underneath containing a hyperlink. There are some slight variations in the sentence wording but the four structures currently prevalent include:
    - Notification received Open notification.
    - Notification received View notification.
    - Notification clipped Open notification.
    - Notification clipped View notification.
- Office 365 voice mails with "Message from Trusted server"
- Emails from the Bank of America
- HMRC text message about Self-Employment Income Support Scheme (SEISS)

You will find more information including a screenshot of the current phishing email on the NCSC website: https://www.ncsc.gov.uk/news/mass-credential-harvesting-phishing-campaign-active-uk

Bank of America phishing scam

On a same theme beware of Bank of America emails which may contain a link to a credential phishing page which then asks victims for their 'security challenge questions'. It is possible for the email to bypass email security controls because it doesn't follow the format of a more traditional phishing attack because it targets only a few people in the organization and therefore gets past Microsoft's email security and Secure Email Gateway. Although the sender name - Bank of America - was impersonated because the email was sent from a valid personal Yahoo account it will pass all of the security checks. You can read more here: https://www.bleepingcomputer.com/news/security/why-did-this-bank-of-america-phishing-email-bypass-spam-filters/

Hackers hijacked an Oxford University email server

Hackers have harvested Microsoft Office 365 credentials from European, Asian, and Middle Eastern targets by leveraging reputable accounts such as of Oxford University, Adobe, and Samsung. Using legitimate Oxford SMTP servers the attackers were able to create their own email addresses and sent phishing messages disguised as Office 365 voice mails which contained the words "Message from Trusted server" above the content. After a victims clicked the Listen/Download button they were redirected to a phishing landing page disguised as an Office 365 login page. You can read more here: https://www.bleepingcomputer.com/news/security/hijacked-oxford-server-used-by-hackers-for-office-365-phishing/

HMRC text message phishing scam targets self-employed

HMRC have warned of a new phishing scam related to the Self-Employment Income Support Scheme (SEISS). Generally this takes the form of a SMS that indicates the victim may be eligible for a tax refund. This redirects to a fraudulent website (that looks like the official HMRC site) where personal data is gathered including HMRC log in, bank account number, security code and expiry date so that the victim can claim a "bogus" refund. If you receive any suspicious emails or phone calls you should forward them to phishing@hmrc.gov.uk suspicious text messages should be sent to 60599.

HMRC will never send notifications of a tax rebate or ask that personal or payment information be disclosed by email or text message

The NCSC has further information on how self-employed workers, and others, can protect themselves against these scams of this type. https://www.ncsc.gov.uk/guidance/suspicious-email-actions

Using the NCSC reporting tool

I had occasion to forward a suspicious message titled 'YourLicence DirectDebit' and claiming to come from TV licencing. It was really easy to use the NCSC tool and I received an unexpected thank you email by return which have details of the 1,387 malicious sites that the NCSC has removed since they launched the Suspicious Email Reporting Service on 21st April 2020.

Conduent firm hit by ransomware attack

The European operations of Conduent, the IT services provider who deliver services on behalf of business and governments across the world, were hit by a Maze ransomware attack overnight on 29 May. The attackers apparently took advantage of a vulnerability in Citrix VPN appliances in the early hours of the morning.

Vulnerabilities affecting VPN products from Pulse Secure, Fortinet and Palo Alto

The NCSC warns that Advanced Persistent Threats continue to target both UK and international government, military, academic, business and healthcare (hundreds of UK hosts may be vulnerable). The threat actors are exploiting the known vulnerabilities in "SSL VPN" products and can retrieve files, including login credentials which are used to connect to the VPN and change configuration settings. You can read more here: https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities

79 Netgear router models vulnerable to remote attack

2 researchers have found a vulnerability in in the web server component of 758 different firmware versions used in 79 Netgear routers since 2007. If you have a Netgear router it would be best to read the zdnet article: https://www.zdnet.com/article/unpatched-vulnerability-identified-in-79-netgear-router-models/

Google Chrome to remove words like 'blacklist' and 'whitelist'

Major tech companies such as Google Chrome have decided to change their development language to adopt "blocklist" and "allowlist" rather than "blacklist" and "whitelist". These "new" terms are clearer and more descriptive and therefore easier to understand. You can read the article here: https://beebom.com/google-blacklist-whitelist-removed-code/

UK virus-tracing app switches to Apple-Google model

Following trials in the government's centralised Track and Trace app in the Isle of Wight it was found that the software registered about 75% of Android handsets but only 4% of iPhones. The UK has therefore decided to follow Germany, Italy and Denmark and move from a "centralised" approach to a "decentralised" one and will use a model based on the one being developed by Apple and Google. This will be welcomed by privacy experts as the Apple-Google design has been promoted as being more privacy-focused (it will however mean less access for epidemiologists). At the Downing Street briefing this afternoon it was announced that the google/apple product does not yet offer sufficiently accurate location tracing. Therefore the UK government will share their app development with Google/Apple to make the system better. We can expect the app in the autumn, initially for symptoms reporting and ordering tests, it will include contact tracing later. You can read more here: https://www.bbc.co.uk/news/technology-53095336

Aerospace and military officials targeted by hackers posing as HRs

A sophisticated cyber-espionage campaign has been targeting staff in the aerospace and military (in Europe and the Middle East) by posing as HRs and offering fake jobs. The primary aim of these agents was to spy on key employees of the targeted firms although some attempted to siphon money as well. The actions have been linked to the Lazarus Group (a hacking group with links to the North Korean government). You can read the article here: https://thehackernews.com/2020/06/military-aerospace-hacking.html

What does malware do

This week Mike Ouwerkerk published a pithy guide to the main malware types and what they do - it is really easy to understand:

Malware	It Says	It Does
Virus	"Ha ha I tricked you into doing that!"	It gets on your device because you did something to allow it on like opening a dodgy attachment or clicking on a dodgy link.
Worm	"Sit back and relax, you don't need to do anything!"	It looks for vulnerabilities to get in, and spreads by itself.
Spyware	"Thank you for typing in your bank account details!"	It logs what you do (e.g. keystrokes), and sends the info back to the creator.
Trojan Horse	"Please download me, I am useful!"	It poses as useful software, you install it, and it's got nastiness inside.

To guard against these we need to be cyber aware and DON'T CLICK LINKS! (I love that Mike has this in his Linked In "Headline") and install Patches and have a good "Anti malware" software.

Blogs of the week

The daily giggle channel… any place, anywhere, virtual laughter….

Have you heard of Laughter Yoga? Neither had I but when I met Sara Kay from Serious Laughter at a virtual networking event. Sara explains in her blog what laughter yoga is and how she finds that she works better when her brain is "full of oxygen from laughing". Sara has a really positive outlook which is so helpful at this time. It is still possible to access laughter via the Daily Giggle Channel on Facebook and her website where you can be guided through intentional laughter and establish a social connection away from work. You can read more and find links for free virtual sessions here: https://www.seriouslaughterwellbeing.co.uk/the-daily-giggle-channel-any-place-anywhere-virtual-laughter/

How records management can help with cybersecurity

Emily Overton's blog this week is about how records management can help in with information security. It's really important that we know what is on our systems so that we can put the most effective security in place. If something doesn't need to be kept it should be got rid of (GDPR calls this the Data Minimisation rule). But you should know why you are holding and why. Timely disposal of records means you won't spend your budget on Redundant, Obsolete or Transient records. You can read the full blog here https://rmgirl.co.uk/2020/06/15/reducing-the-attack-surface/. I recommend the video on that page for those who want to understand more about what records management is and why it is important.

In particular you should know: **what** you have, **why** you have it and **how** long you need to keep it.

Cheap data will never leave you cheerful

Businesses will always look for a good deal but the search for cheap data, especially at this time, should not be seen as the ultimate goal. Often "cheap data" is just not worth the money or hassle. Gareth Perry in his blog outlines the risks to your brand from buying cheap data, the potential consequences and why the adage "quality over quantity" should be applied to purchasing data. You can read the article here: https://www.data-broker.co.uk/insights/cheap-data-will-never-leave-you-cheerful/