36
CRIME

Barristers | Mediators | Arbitrators
+ 44 (0)20 742 8007
4 Field Court, Grays Inn, London, WC1R 5EF

"THE DEVIL FINDS WORK FOR IDLE HANDS"
COVID-19's UNWANTED CYBER SIDE EFFECT

Sarah Gaunt – Cybercrime Specialist
https://36group.co.uk/members/sg

Cyber-crime is, at the best of times an evolving topic, in these exceptional times it is extremely fluid, as the ingenuity of the cybercriminal finds fertile ground upon which to prosper. We have in the recent past (literally) applauded the many positive actions that have emanated from this time extraordinary hardship and loss. Sadly, the recipe of "The devil finds work for idle hands" combined with the concept that the exceptional provides opportunity, cybercriminal ingenuity and a general state of latent fear, provides a meal of unrivalled opportunity for those with malevolent intent. The phrase "stay safe" is now of common occurrence. We need to be saying "stay safe" and "stay cyber safe" in these extraordinarily turbulent times.

At the date of writing (21st April 2020), GCHQ/NCSC (National Cyber Security Centre) has made a public appeal for particular cyber vigilance. This is of little surprise to those who have been monitoring the recent International and domestic statistics within this area of criminality. It is of note that the concern is such that GCHQ/NCSC have today made a specific public request to report cybercrime during the Corona-COVID-19 era to report@phishing.gov.uk. This is the culmination of world-wide concern at the general growth of cyber-crime during this crisis and the growth of Corona-COVID-19 cyber-crime in particular. This darkly emerging cyber phenomenon, like the internet, is world-wide. The variety of cybercrime that has erupted from the current pandemic is extensive and increasingly diverse and extends across the realm of the cyber offending repertoire. The position can be exemplified by looking at the World Health Organisation (WHO) itself, who had to publish a

cybercrime warning on its site in the recent past, due to the substantial use of its name (and/or individuals within or purporting to come from its organisation) within the cybercrime world. This warning seems to have been adopted within individual countrywide warnings since the initial post. The WHO requested the reporting of such events to its organisation, where its name/identity was used so that it could monitor the situation.

In the US, the FBI Deputy Assistant Director Tonya Ugoretz suggested at the recent US Aspen Institute seminar "Fight back: How to Stop Cyber Criminals During the Pandemic", that reporting of general cybercrime in the US had increased almost four fold since the commencement of the pandemic, once again note is taken of the Corona-COVID-19 specific cybercrime that has flourished[1]. The European Union's Institutions have also expressed concerns regarding cybercrime at this time. On 24th March 2020 Ursula von der Leyen (President of the European Commission) also gave a warning that cybercrime in the EU had increased due to the Corona Virus outbreak. As von der Leyen stated "They [cybercriminals] follow us online and exploit our concerns about the coronavirus. Our fear becomes their business opportunity". Interpol has published a corresponding advisory regarding the situation.

On 8th April 2020, The NCSC (used for disseminating current National cybercrime related advice), issued a joint advisory with the United States Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) dealing specifically with the cyber-crime exploitation of the Covid-19 pandemic ("The Joint Advisory Document"). It is noted within the Joint Advisory Document that "both the NCSC and CISA are seeing a growing use of COVID-19 related themes by malicious cyber actors". It is to be noted that cybercriminals are seen to be targeting all, including individuals; small, medium and large companies, and National/International Infrastructures. In the UK, of particular note, there was an increase in UK Government branded scams relating to Covid-19.The Joint Advisory Document provides examples of realistic, purportedly Government sent, communications (email AND SMS/text (there have elsewhere also been mention of malicious WhatsApp communication)), e.g. offering assistance during this crisis sent with the malicious purpose of harvesting addresses, names and banking information from the unsuspecting recipient. Other

[1] Aspeninstitute.org.

features seen in very recent times include using Corona/COVID-19 wording within the URL[2] of an email address; increased phishing[3] to steal user credentials using the Corona/COVID-19 nametags/details and phishing for malware[4] deployment (an example of using a communication where the name of a WHO individual is given) are all cited within the document. The exploitation of the new and increased use of the home working infrastructure is also contained within the Joint Advisory Document. Specific mention is made of video/telephone conferencing facilities, including less well known as well as the more popular communications platforms (such as Zoom or Microsoft Teams). Examples cited are e.g. where phishing emails, in the name of teleconferencing, are being sent and where teleconferences are being hijacked. This comes on the back of an acceptance in very early April 2020 by Eric Yuan (CEO of Zoom) that they had "fallen short" in respect of cyber security on the site which the company would rectify (reported in The Guardian). In addition to the above, the Government has, itself, posted an additional warning on 17th April 2020 entitled "Coronavirus (COVID-19): increased risk of fraud and cybercrime against charities", as stated, and as elaborated on below, no institution of sector is safe from the current cybercrime attention.

As with all aspects of this pandemic the UK is not alone, this is worldwide. Apart from WHO (that, as stated, has had its own identity issues in cybercrime), other institutions that are dealing in these adverse circumstances with treatment and prevention of the Coronavirus-COVID-19 have also reported as being under attack. There have been several reports of attempts to attack the internet infrastructure of hospitals and/or potential vaccine producing institutions, in e.g. America, Germany and the UK[5]. The wish of cybercriminals to take advantage of a stretched and vulnerable NHS/healthcare system (already the subject of relatively recent breaches), to obtain patient/sensitive data or to obtain the aspects of detailed research into a "holy grail" vaccine (with the presumed ambition of distributing ransomware[6] or similar) is not without note. The NCSC has today declared that it intends to protect legitimate Government, NHS and other essential public organisation internet

[2] URL:- The address of a World Wide Web Page.
[3] Phishing:- A fraudulent attempt to gain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.
[4] Malware:- Normally a malicious software which executes unauthorised actions on the victims system(s).
[5] See for example reported breaches in the paper produced by Elena Sanchez NICOLAS at https://euobserver.com/coronavirus/147869 and the "Fight back: How to Stop Cyber Criminals During the Pandemic" produced by the Aspen institute seminar aspeninstitute.org.
[6] Ransomware:- A type of malware from cryptovirology that threatens to publish the victims data or perpetually block access to it unless a ransom is paid.

infrastructure from attack. In these unusual times, it is however impetrative, that all of us follow the advice given by this and other like institutions, in order to attempt to protect our aspect of Internet use and where we are breached to report the breach as required, so that cybercriminals can hopefully be tracked and caught for the greater good.

To give a small indication of where we are at the current date, within the UK the NCSC has reported that so far during the Coron-COVID-19 crisis, the following has been reported:- 471 fake online shops; the existence of 555 malware distribution sites and 200 phishing sites, and 832 advance-fee frauds have been committed[7]. Action Fraud reports that last week 18.5% of all fraudulent emails were directly linked to the COVID-19 crisis. This may, of course, simply be the tip of the iceberg given an anticipated current lack of reporting. It is of note that the Interim CPS Charging Protocol – Covid-19 crisis response states (at point 10) "All Covid-19 related cases will be dealt with as Immediate cases for the purpose of obtaining a charging decision, whether they are custody or subsequently on bail", which provides an indication of the seriousness with which the prosecution authorities are viewing Covid-19 related attacks upon us at this vulnerable time.

On a more positive note, being aware of the existence of a problem means that actions can be taken to mitigate the risk and knowledge means that increased vigilance can be requested and applied. As stated, and to reiterate, anything suspicious should be reported to report@phishing.co.uk and/or to Actionfraud.police.uk. Updates and further advice can be found by visiting the NCSC site at ncsc.gov.uk. Further information can be obtained by following @Actionfrauduk and @CyberProtectUK.

More specific current national and international advice can be found at

NCSC guidance for the public to help them spot, understand and deal with suspicious messages and emails: https://www.ncsc.gov.uk/guidance/suspicious-email-actions

NCSC phishing guidance for organisations and cyber security professionals: https://www.ncsc.gov.uk/guidance/phishing

NCSC guidance on mitigating malware and ransomware attacks: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

NCSC guidance on home working: https://www.ncsc.gov.uk/guidance/home-working

CISA guidance for defending against COVID-19 cyber scams: https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams

[7] See the Guardian, BBC and other public reports of 21/04/2020.

CISA Insights: Risk Management for Novel Coronavirus (COVID-19), provides guidance for executives regarding physical, supply chain, and cybersecurity issues relating to COVID-19: https://www.cisa.gov/sites/default/files/publications/20_0318_cisa_insights_coronavirus.pdf

CISA Alert (AA20-073A) on enterprise VPN security: https://www.us-cert.gov/ncas/alerts/aa20-073a

In these extraordinary times the goal is surely first of all to “Stay safe” but secondly to “Stay cyber safe”, particularly as, during these exceptional times, the internet is providing so many of us with our access to the world and/or the avenue through which our businesses can hope to survive. In summary, where we haven’t done so, we need to take action, remain vigilant and to restrain the latent fear that so many cybercriminals use to such great effect. Stay safe, stay cybersafe.

Sarah Gaunt, Barrister

36 Cybercrime