Financial Crime Impact: COVID-19 (Corona Virus) and Cyber and Financial Fraud Threats

March 2020

By Financial Crime Compliance (FCC)

Introduction

As the COVID-19 pandemic causes rapid and unprecedented disruption to all aspects of modern life and working practices, a wide range of criminals, both physical or online and in some cases, state sponsored, are working tirelessly to capitalise on mass public fear and confusion for financial gain and economic advantage. Financial Crime Compliance teams in Standard Chartered are also collaborating to ensure we understand what this may mean for our clients and our controls. This bulletin raises awareness of the fraud and cyber-related threats facing us as private individuals and employees, as well as to businesses, to help us navigate what the US Attorney General describes as "an unprecedented wave of cyber-attacks and cyber-enabled financial fraud".

SUMMARY

- The global uncertainty and anxiety generated by the COVID-19 pandemic has made a large volume of people more economically, psychologically and physically vulnerable to being targeted and exploited by criminals. We expect the threats posed by criminals to our clients and our employees will continue to increase in the short term, especially as disruption and associated financial pressures increase.

- Criminal campaigns and Nation state sponsored groups have closely tracked the spread of the virus and may be actively targeting home workers, to gain access to personal data and corporate systems, or potentially to spread disinformation that fosters social instability. An existing widespread potential deficiency in the security of home I.T. infrastructure, particularly among individuals not used to remote working arrangements, could exacerbate this threat.

- Cyber-enabled fraudsters and other criminals have been quick to adapt established scams and social engineering techniques to this pandemic to steal money and personal data. Intelligence shows a rise in COVID-19-related Authorised Push Payment (APP) investment fraud and other scams targeting individuals, including our clients.

- Malicious campaigns started with a focus on information theft and are moving to more disruptive attacks, using phishing emails linked to fake and malicious websites purporting to be global health regulators such as the World Health Organisation (WHO) and Centre for Disease Control (CDC). We expect this to continue in the short term.

BEWARE: CORONAVIRUS DISINFORMATION

Recent media reporting suggests increasing evidence of disinformation or 'conspiracy theory' campaigns around COVID-19 with the intention to aggravate the public health crisis. Such activity intensifies general uncertainty and may increase the number of users clicking on unsolicited links or attachments.

Phishing, Smishing, Vishing: Fraudster 'social engineering' scam **m**ethods of eliciting information from individuals, usually personal data, by email, text message or phone call. The personal data collected may be used to perpetrate further fraud, such as identity impersonation frauds, or sold on to other criminals.

COVID-19 Themed Fraud 'Clickbait' Scams Targeting Individuals

- **'Change to bonuses'** – an email purporting to be from the HR department stating that bonuses will no longer be paid in the usual manner due to coronavirus.
- **Giveaways'** – offering victims loans with a social engineering pressure stating that banks will be closing due to coronavirus.
- **'Health Alerts'** – promising official public health information seeking to harvest personal data.
- **'Cures/Preventative aids'** – adverts to businesses offering the provision of masks, survival guides or medical supplies.
- **Disruption to supply chain'** – particularly emails purporting to provide updates and alteration to shipping distribution
- **'Lists of infected people'** – an email claiming to provide a list of people affected by coronavirus in a given area (Action Fraud)
- **Front Charity websites** - As seen in past global crises and disasters, criminals pose as charities collecting donations to help in the fight against Coronavirus. Such links are shared quickly across social media platforms; we can expect this to continue as a key driver of fraudulent scam activity.

STAY VIGILANT. STAY SAFE

Protect yourself from scams:

TAKE FIVE FOR FRAUD

takefive-stopfraud.org.uk

Financial Crime Impact: COVID-19 (Corona Virus) and Cyber and Financial Fraud Threats
March 2020

Criminal Opportunities and Challenges: Bank Accounts and 'Cashing Out'

- Criminals usually need one or more bank accounts to move and ultimately benefit from the proceeds of crime. They are known to seek out individuals they can bribe dupe or coerce to become 'money mules'; either complicit or non-complicit individuals who permit criminals to use their bank accounts to move the proceeds of crime.
- The emerging economic disruption from COVID-19 is likely to increase the number of people who are financially vulnerable, and therefore more susceptible to approaches by criminals offering them money in return for the use of their banking facilities.
- This threat already impacts the most vulnerable in society disproportionately, but the sudden upsurge in both numbers and diversity of individuals being impacted for the first time could lead to a substantial increase in complicit mules as people become desperate to make ends meet. One current Instagram post is offering anyone 'extra income within 60-90 minutes' through a money mule scheme.
- As a challenge, however, criminals may struggle to cash out using ATMs where severe restrictions on movement, such as those currently imposed in Spain and Italy, include curtailing access to ATMs.

DDOS Attack: a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Increased Threat from Distributed Denial of Service (DDoS) Attacks

- Due to the heightened level of attention and activity in legitimate users trying to access online resources during periods of self-isolation and national lockdown it is likely that threat actors will continue to try to disrupt and deny these services.

Case Studies: DDoS Attacks in the US and Germany

- The US Department of Health and Human Services (HHS) experienced an attack in mid-March. Reportedly due to COVID-19 preparations, this attack did not result in service disruption but came at an unwelcome time when they were prioritising providing information to the public on how to cope with the pandemic.
- An attack was launched against a takeaway food delivery website in Germany to coincide with the increased demand resulting from social distancing recommendations. The demand to cease the attack was 2 bitcoins (~11000 USD). The website is currently operational.

Cyber Threat Targeting Remote Workers and Businesses

- People working remotely may be less secure or protected when accessing or sharing sensitive information than they would be by the office IT infrastructure provided by their employer. This is particularly acute where our clients as employers cannot offer workers access through secure servers or video/audio conferencing platforms.
- Some businesses may be forced to operate with only a highly stressed 'skeleton crew' in the office at a time when cyber criminals are stepping up their attacks, and when it is difficult for businesses to differentiate between or seek additional professional opinions on legitimate and malicious traffic caused by an increase in use of remote access.

Latest Reported Cyber Threat Campaigns

- Advanced Persistent Threat (APTs) groups have adopted 'coronavirus' or 'COVID-19' in malicious emails to deliver malware to further their objectives. Health agencies, including; the World Health Organisation (WHO), the US Centre for Disease Control, the Ukraine Ministry of Health and the Mongolian Ministry of Health have all allegedly been spoofed by nation state-sponsored groups in attempts to deliver malware.
- 'CoronaVirus' ransomware, a newly emerged version, is being distributed alongside an info-stealing trojan, with the demand for 50 USD in bitcoins to decrypt. It is possible this ransomware is a distraction to infect users with the info-stealing trojan.
- Brno University Hospital in the Czech Republic, a major coronavirus testing hub, has experienced a ransomware attack that disrupted operations, as has a US based healthcare centre.
- DopplePaymer and Maze ransomware operators have reportedly stated they will not target hospitals or emergency services during the pandemic. It is unlikely this abstinence will be enforced and even if it is, it only removes a very small percentage of criminal group-operated ransomware.
- It is likely that criminals will move towards disruption focused attacks to maximise illegitimate profits from critical services and infrastructure. Phishing emails and malicious attachments remain the primary ways criminals are deploying ransomware.