COVID-19: CYBERCRIMINALS CAPITALIZE ON GLOBAL FEARS

4 March 2020 | **Kareena Teh, Catherine Wong**

As COVID-19 continues to spread, cybercriminals have used a variety of tactics to exploit the widespread fear of infection and hunger for news and/or protective merchandise

Cyberfraud is prevalent and will only increase as more and more business is conducted online. Billions are lost each year as a consequence. As an international finance and banking center and one of the world's most open and free economies, a substantial volume of funds, including defrauded funds, flow through Hong Kong each day. In 2018 alone, there were 2,717 cases of online business fraud, with losses of HK$56 million (about US$7.2 million), and 894 email scams, of which 887 cases were corporate scams, with losses of HK$1.17 billion (about US$150.3 million). The majority of the corporate scams involved victimized organizations with no connection with Hong Kong sending money to scammers through Hong Kong bank accounts[1]. Millions can be lost in each scam. In the last two years, a South American organization and a US organization were reported as having been respectively duped into transferring US$18 million[2] and US$3 million[3] into Hong Kong bank accounts.

Email scammers typically use information obtained through cybercrime (e.g., hacking, phishing and/or use of malware) or through data leakage (e.g., from online sources and/or unsecure Wi-Fi connections) to target organizations. They impersonate executives, clients or business partners of the targeted organizations and request money transfers, often on an urgent basis. Two common types of such frauds are the CEO Fraud and the Mandate Fraud. In both, staff within the targeted organizations' account departments receive emails from spoofed email addresses (i.e., those that have been altered to appear as if they have been sent by someone other than the actual sender) requesting payment to be made. The former includes requests from purported senior executives of the organizations for payments for an ongoing business transaction or a confidential new deal, while the latter includes requests from purported clients or business partners for payment for products or services to a new bank account.

[1] https://www.info.gov.hk/gia/general/201901/29/P2019012900879.htm
[2] https://www.scmp.com/news/hong-kong/law-and-crime/article/3021505/hong-kong-anti-fraud-squad-intercepts-nearly-hk13
[3] https://www.scmp.com/news/hong-kong/law-crime/article/2140453/us-company-duped-sending-us3-million-hong-kong-account

COVID-19 cyberfraud tactics

As fears about COVID-19 continue to spread, cybercriminals have used a variety of tactics that exploit the widespread hunger for news about the coronavirus outbreak, using them as a phishing lure to gain access to information directly or through the use of implanted malware. We set out below some of the tactics employed.

Fake domains

Some phishing campaigns have incorporated fake domains designated to look like world health organizations. For example, cybercriminals have been sending out phishing emails that contain domain names similar to those used by the Center for Disease Control ("**CDC**"). While the actual centers for disease control domain is "*cdc.gov*", the attackers have incorporated the domain *"cdc-gov.org"* within their phishing emails. These CDC-themed phishing emails encourage recipients to click on a link that contains details about new cases of coronavirus around their neighborhood. The link, portrayed as steering recipients to the CDC website, instead redirects victims to a fake website which looks like an email account login page, where targets are asked to enter their username and password.[4]

A security firm also published a report about a sharp increase in the number of domains being registered related to coronavirus. An example of such a website is "*vaccinecovid-19.com*", first created on 11 February 2020 and registered in Russia. The website is insecure and offers to sell "*the best and fastest test for coronavirus detection at the fantastic price of 19,000 Russian rubles (about US$300).*"[5]

Phishing emails

Other cybercriminals have been sending out phishing emails that use concerns over coronavirus-related disruptions to entice victims to open an attached document that installs the AZORult information stealer, which assists users to ensure owner anonymity and to make it difficult to block the command-and-control server. Emotet contained in phishing emails has also been used to install malicious code on endpoints it has infected, as well as giving it the ability to scrape victims' computers for contact information. In addition, some attackers have increasingly rented Emotet botnets to install other malware, including Trickbot and various strains of ransomeware. Once the malware is downloaded, Emotet uses the infected system to send out additional phishing emails and spam with a view to growing the botnet.

In late January 2020, IBM X-Force researchers discovered a first wave of phishing scams that targeted some regions in Japan to spread the Emotet Trojan, as well as other malware, by using malicious messages that appear to contain information about COVID-19.[6] Each of these phishing emails also contains an attached document, which is portrayed as offering updates of health information. In many cases, the analysts found cybercriminals attempting to deploy a number of Trojans to victims' devices. If the file attachment is opened and Office 365 macros are enabled, an obfuscated VBA macro script begins running in the background, which then installs a Powershell script and downloads the Emotet Trojan.[7] In one email, the attackers stated that the

[4] https://www.bankinfosecurity.com/more-phishing-campaigns-tied-to-coronavirus-fears-a-13709
[5] https://www.bankinfosecurity.com/phishing-campaigns-tied-to-coronavirus-persist-a-13741
[6] https://www.bankinfosecurity.com/more-phishing-campaigns-tied-to-coronavirus-fears-a-13709
[7] https://www.govinfosecurity.com/fake-coronavirus-messages-spreading-emotet-infections-a-13675

coronavirus had been detected in Osaka, while another mentioned the Gifu region of Japan. It appears that the attackers use specifically tailored warnings and language to scare inhabitants in those areas, making them more likely to click on the attachment. The emails also end with a footer that mentions a legitimate postal address as well as a fax and phone number.[8]

In another campaign, cybercriminals were sending out phishing emails that appeared to originate from the World Health Organization (the "**WHO**"). The emails urged the victims to click on a button to download a *"document on safety measures regarding the spreading of corona virus"*. By clicking on the link in the email, victims are led to a webpage that looks similar to the WHO website but contains a popup screen asking users to submit the username and password associated with their email address. If someone enters their credentials, the information is sent to the attackers.[9]

Other cybercriminals have taken a different tactic, zeroing in on concerns around the potential effects that COVID-19 may have on global shipping. In phishing emails that Proofpoint found, the messages contain the subject line "*Coronavirus – Brief note for the shipping industry*". The document attached to the email contains malicious code that then attempts to install the AZORult malware.[10]

Implications and recommendations for businesses

While these campaigns may not appear to be targeting businesses organizations per se, they nonetheless pose a significant risk to organizations because they prey on the fear of individuals anxious for updates about COVID-19 and/or sourcing protective merchandise (such as masks and hand sanitizers). Many of these individuals may be employees of organizations, and some may even be working remotely due to the COVID-19 containment measures rolled out by governments and/or the organizations themselves.

We recommend that businesses stay vigilant and take proactive steps to:

- ensure a proper understanding of the business' cybersecurity risks and vulnerabilities, including those created by COVID-19 outlined above;
- ensure there are appropriate and properly implemented systems and procedures in place to address these risks and vulnerabilities. Ideally, these systems and procedures should have:
    - an effective reporting system to ensure timely reporting and escalation of new and/or additional risks identified and/or breaches detected;
    - a designated incident response plan and team, with relevant personnel having a proper understanding of their role and responsibility. The plan should include a communications protocol to ensure prompt notification to the paying and receiving banks and demand for repayment of the defrauded funds, timely reporting to authorities and notification of relevant stakeholders. It is also important to have professional experts, such as lawyers, forensic investigators and cybersecurity experts with relevant expertise and experience lined up and ready to respond as the

[8] https://www.govinfosecurity.com/fake-coronavirus-messages-spreading-emotet-infections-a-13675

[9] https://www.bankinfosecurity.com/more-phishing-campaigns-tied-to-coronavirus-fears-a-13709

[10] https://www.proofpoint.com/us/corporate-blog/post/coronavirus-themed-attacks-target-global-shipping-concerns

    speed of the response can often be the difference between recovery and loss of the funds; and

    - cybersecurity policies and procedures, supported by advanced hardware and software protection (e.g., antivirus, email spam/phishing detection) that is updated frequently to ensure effectiveness. Some important policy and procedural initiatives include (i) instructions to staff to be vigilant of phishing emails, to run regular spoof tests, particularly where emails appear to be suspicious, to ignore requests to click suspicious links that may lead to unsecured websites or malware, not to use public and/or free Wi-Fi connections or hot spots, and to report and delete suspicious emails; (ii) two-step approval/verification for payments, including from senior executives of the organization and established business partners, particularly when requiring a change of payment details; and (iii) multi-level or two-factor authentication for operation of bank accounts;

- ensure there are effective internal controls, including proper "*KYC*" or due diligence checks of new business partners (e.g., suppliers/vendors/customers) and verification of payment instructions. In setting up new business partner accounts, it is important to obtain details of the bank account where payment is to be made and ensure that the payee details are those of the business partner. If there is a mismatch, ensure proper understanding of the reasons and obtain clearance from compliance. If subsequent payment instructions deviate from the payment details originally provided, especially in cross-border transactions, verify with business partner, preferably by calling them at their usual office phone number or by using a fresh email unconnected to the emails providing the changed payment details. See also two-step approval/verification for payments and multi-level or two-factor authentication for operation of bank accounts referred to above;
- ensure staff are properly trained, understand and are responsive to the organization's policies and procedures, and are consistently educated about new cybersecurity risks and vulnerabilities, including those that are linked to and/or driven by major events, such as COVID-19. Consider and if appropriate, issue an alert of the COVID-19 risks and vulnerabilities outlined above so that staff will be aware of and vigilant against the tactics employed; and
- in the event of a breach, trigger the designated incident response plan and seek independent professional advice, including from (i) lawyers as to the urgent and immediate steps that need to be taken to report the breach to the authorities, freeze, trace and recover funds stolen, (ii) forensic investigators to back up, image and collect evidence; and (iii) cybersecurity experts to identify the cause(s) of the breach and remediate the compromised areas.

KEY CONTACTS

Kareena Teh
Partner
Kareena.Teh@eylaw.com.hk
+852 2629 3207

Catherine Wong
Associate
Catherine.KY.Wong@eylaw.com.hk
+852 2675 2173

Contact us

LC Lawyers LLP *in Association with* Chen & Co. Law Firm
Suite 3106, 31/F, One Taikoo Place
979 King's Road, Quarry Bay
Hong Kong
Tel: +852 2629 3200
Fax: +852 2956 1980

https://www.eylaw.com.hk/en_hk

Follow us on WeChat

This material has been prepared for general informational purposes only and is not intended to be relied upon as professional advice. Please contact us for specific advice.