Dragon Advance Tech

Suite 701-702, 7/F, Shun Feng International Centre, No. 182 Queen's Road East, Wanchai, Hong Kong
Phone +852 2868 6182 Email: admin@dragonadvancetech.com

Cybersecurity Alert

TLP:GREEN

Business Email Compromise (BEC), sometimes known as CEO scam, has been an effective way used by attackers to deceive money from victims.
Attackers usually begin by researching the LinkedIn profiles of the victim's organizations executives,
followed by sending spear-phishing emails to trick the recipients into remitting funds to money-mules overseas.
Even though crime prevention tips are published,
there is still a significant increase in the number of similar incidents. We propose corporate's Cybersecurity team to set up monitoring solutions to detect and set alerts of such spear-phishing emails.

CEO scam bas been around for many years and people usually have the impression that after moving their email service to Office 365, G Suite, or some other popular email service providers, the spam email issues will be gone. We joined the DMARC[1] and DNS projects after attending a DMARC talk at the FIRST Symposium – Taichung/Taiwan in 2018, and we thought that phishing or targeted email attacks will not be a major security vulnerability for organizations anymore, as there are plenty of technology solutions out there to handle this legacy email security issues, and that it has been well addressed by most of the organizations in Hong Kong. However, a news article from SCMP[2] on January 6, 2019 alerted us:

> *"More than US$195.3 million [or HK$1.5 billon] defrauded from companies in Hong Kong and overseas in first 10 months of 2018. [This] figure is a 100 per cent increase on the previous year and affected more than 740 companies. The biggest amount swindled was more than HK$100 million, which an electronics company in Spain was defrauded of. Figures show Hong Kong police handled 741 cases of commercial email fraud involving total losses of HK$1.53 billion (US$195.3 million) in the first 10 months of 2018."*

The BEC attackers used traditional social engineering technique to deceive highly educated executives into authorizing wire transfer to foreign bank accounts controlled by money mules. As these Man-in-the-Email scams incidents are increasing in Hong Kong, the Anti-Deception Coordination Center (ADCC) of the Hong Kong Police Force also issued CEO Email Scam crime prevention tips[3] to the public and advised company management to impose guidelines on the verification of the email senders' identities before making fund transfers.

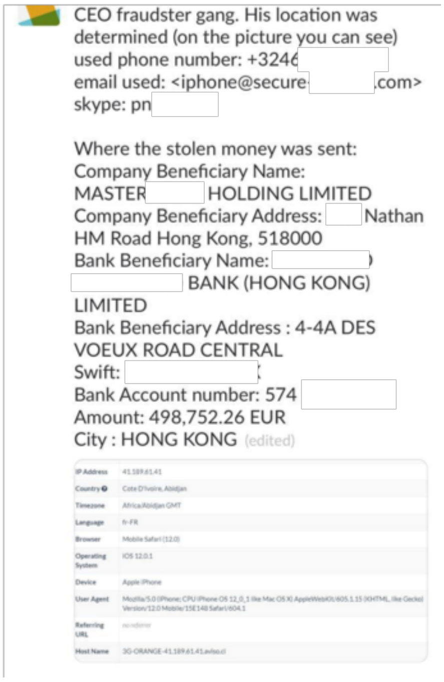
According to a BEC threat intelligence discussion list, there is a case where an international organization had sent EUR 498,752.26 to a Hong Kong bank account, which belongs to a newly

[1] https://dmarc.org

[2] https://www.scmp.com/news/hong-kong/law-and-crime/article/2180879/more-us1953-million-defrauded-companies-hong-kong-and

[3] https://www.police.gov.hk/ppp_en/04_crime_matters/ccb/fst.php?msg_id=cct_30

registered limited company in Hong Kong (the company was registered on Feb 20, 2018). (See Fig. 1 & Fig. 2)

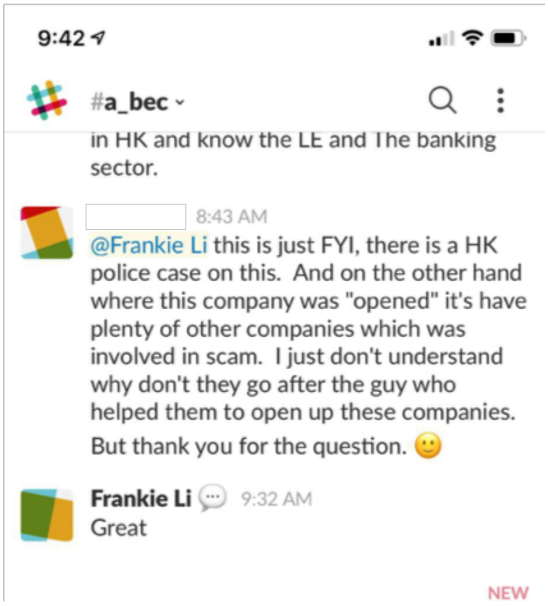


CEO fraudster gang. His location was determined (on the picture you can see)
used phone number: +3246[redacted]
email used: <iphone@secure[redacted].com>
skype: pn[redacted]

Where the stolen money was sent:
Company Beneficiary Name:
MASTER[redacted]HOLDING LIMITED
Company Beneficiary Address: [redacted] Nathan HM Road Hong Kong, 518000
Bank Beneficiary Name: [redacted]
[redacted] BANK (HONG KONG) LIMITED
Bank Beneficiary Address : 4-4A DES VOEUX ROAD CENTRAL
Swift: [redacted]
Bank Account number: 574 [redacted]
Amount: 498,752.26 EUR
City : HONG KONG (edited)

IP Address	41.189.61.41
Country	Cote D'Ivoire, Abidjan
Timezone	Africa/Abidjan GMT
Language	fr-FR
Browser	Mobile Safari (12.0)
Operating System	iOS 12.0.1
Device	Apple iPhone
User Agent	Mozilla/5.0 (iPhone; CPU iPhone OS 12_0_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0 Mobile/15E148 Safari/604.1
Referring URL	no referrer
Host Name	3G-ORANGE-41.189.61.41.aviso.ci

Fig 1 – a BEC incident published from a threat-intel list that indicates the stolen money was sent to a bank account in Hong Kong



in HK and know the LE and The banking sector.

[redacted] 8:43 AM
@Frankie Li this is just FYI, there is a HK police case on this. And on the other hand where this company was "opened" it's have plenty of other companies which was involved in scam. I just don't understand why don't they go after the guy who helped them to open up these companies.
But thank you for the question. 🙂

Frankie Li 9:32 AM
Great

Fig 2 – The case was supposed to be handled by law enforcement

We, as cyber security experts, should deploy reasonable and effective security solutions to protect our network, systems, as well as human resource. We received a lot of complaints from practitioners saying that it is very hard to train their executives to defend such social engineering attacks. Although we can deliver more security awareness training courses, such as the guidelines recommended by the SANS Institution[4] or from HKCERT[5], we should also locate some security and technological controls to detect such attack. However, it is difficult to identify an effective solution that can fit the budget for most of the organizations in Hong Kong.

If the organization has Security Information and Event Management (SIEM) solutions or has established a Security Operation Center (SOC) environment, one can configure them to look for internal/external emails domains from email headers, embedded URLs or even SWIFT codes in the email body, etc and match them with some known bad sources for identifying possible attacks. To accomplish this, the SIEM needs to collect logs from endpoints, run tailor-made scripts (or by way of API calls), together with network monitoring. There are no magic silver-bullets for defending or monitoring such attack, but we suggest the SIEM plus network monitoring solution as it causes less impact to the existing IT infrastructure in a production environment.

[4] https://www.sans.org/security-awareness-training/ouch-newsletter/2016/ceo-fraud
[5] https://www.hkcert.org/mobile_url/en/guideline/18040602

We recommend Cybersecurity teams to deploy network sensors, mirror STMP traffics, and/or examine SMTP contents by setting up direct connections to the email servers for crafting out communication of phishing attacks, click-through malware, or BEC etc and to defend ourselves from these email fraud scams via technical means.

“IT CAN HAPPEN TO ANYONE AND IT MAY HAPPEN AGAIN”