TITLE Chinese Influencing Cambodian Election Campaign
Date: August 30, 2018

Disclaimer: this briefing note contains the encapsulation of views presented throughout the evening and does not exclusively represent the views of the speaker or the Canadian Association for Security and Intelligence Studies.

KEY EVENTS

FireEye researchers spot the TEMP.Periscope, a Chinese cyberespionage group, targeting Cambodian entities ahead of the Cambodian elections scheduled for July 2018. Targeting appears to have consisted of spear phishing emails to Monovithya Kem, Deputy Director-General, Public Affairs, Cambodia National Rescue Party (CNRP), and the daughter of imprisoned Cambodian opposition party leader Kem Sokha. The suspected phishing emails consisted of a malicious document, purportedly coming from LICADHO a non-governmental organization [NGO] in Cambodia established in 1992 to promote human rights, containing AIRBREAK malware.

NATURE OF DISCUSSION

Cambodia has been a reliable supporter of China's South China Sea position. To ensure a win, the Cambodian People's Party (CPP), one of the longest-ruling parties of the world (1979 – present) initiated violent suppressions of opposition party members and media outlets, and had the Cambodian Supreme Court dissolve the Cambodian National Rescue Party (CNRP).

BACKGROUND

Two points to consider: 1) China's influencing the Cambodian election may be related to Malaysia's 2018 elections which resulted in the 60-year ruling party being defeated. China does not want to lose another allie. 2) Malaysia was the first to normalize relationships with China and has balanced the need for economic ties against the need to manage China's ability to interfere with Malaysia's internal affairs and threat to security (such as the South China Sea policy). However, the new party is not supportive of Chinese investments, which may also occur in Cambodia if a new party wins.

© CASIS, 2018

KEY POINTS OF DISCUSSION AND WEST COAST PERSPECTIVES

Three Points Relevant to Canada:

1. Large Chinese population in Canada, some with known connections to suspected money laundering in BC Casinos. Could China be interested in influencing Canadian elections at the city, municipal, provincial, and national levels? Rationale for influencing elections linked to ensuring favorable election of individuals who support foreign investment, and relaxing migration controls.
   Specific Canadian example: Chinese corporation Anbang Insurance Group purchase of Retirement Concepts. The company, Anbang, has now been seized by Chinese Government and control of the company is with a Chinese Government designate. Does this give China's Government control of retirement resources in Canada, and access to residents of the retirement homes medical data?

2. Chinese Organized Crime alleged connections to BC Casinos.
   Specific Canadian examples: Paul King JIN's money laundering operation involving Chinese mainland whales (gambling term) at a BC casino. In a separate file CFSEU is conducting an ongoing investigation and laying of charges on Xing WEI possession of money which a "sniffer dog reacted "positive" to drug residue on the C$140,000 found in Wei's car . CFSEU notes "Mr Wei did not have sufficient legitimate income to have acquired the money ... [he] obtained the money by participating in the unlawful activity,"

3. LICADHO (Cambodian League for the Promotion and Defense of Human Rights) and McGill University Faculty of Law in Montreal Canada.
   Specific Canadian Threat Vector: Three organizations and their relationship with each other create a information technology pathway for China to potentially access Canadian Armed Forces. The pathway is China's compromising phishing attack using LICADHO emails, McGill's connection to Canadian Armed Forces via the Steinberg Centre for Simulation and interactive Learning, and McGill Faculty of Law. LICADHO and McGill Faculty of Law have internship partner agreement for legal education, McGill Faculty of Law and McGill Faculty of Medicine's Steinberg Centre for Simulation and Interactive Learning are connected as academic centres at McGill. McGill's Steinberg Centre is collaborating with Canadian Armed Forces (CAF) medical personnel who CAF conduct operational, peacekeeping, and humanitarian missions. Should McGill University explore this potential information technology pathway which may share common IT connectivity and may be vulnerable to a cyber kill chain sequence for TEMP.Periscope?

© CASIS, 2018