For Immediate Release:
30 September 2020

Contact: (301) 243-0408 (NCSC)
(202) 324-3691 (FBI)

FBI and NCSC Release New Movie to Increase Awareness of Foreign Intelligence Threats On Professional Networking Sites and Other Social Media Platforms

The FBI and the National Counterintelligence and Security Center (NCSC) today released a new movie to increase awareness of how foreign intelligence entities use fake profiles and other forms of deception on social media platforms to target individuals in government, business and academic communities for recruitment and information gathering.

Inspired by true events, the 30-minute movie, called "The Nevernight Connection," details the fictional account of a former U.S. Intelligence Community official who was targeted by a foreign intelligence service via a fake profile on a professional networking site and recruited to turn over classified information. The movie can be accessed at: www.fbi.gov/nevernight.

Last month, NCSC disseminated this movie and other resources to the U.S. Intelligence Community to help employees recognize fake online profiles, realize the threat they pose, report these suspicious approaches to appropriate authorities, and take steps to avoid being targeted in the first place.

The NCSC and FBI are making the movie public today, as National Insider Threat Awareness Month comes to a close and as Cybersecurity Awareness Month begins tomorrow, to help the private sector, academic community, and other government agencies guard against this threat. Current and former government clearance holders who believe they have been targeted in this way are asked to contact their local FBI office.

"Social media deception continues to be a popular technique for foreign intelligence services and other hostile actors to glean valuable information from unsuspecting Americans," said NCSC Director William Evanina. "Through this movie and other resources, we hope to raise awareness among Americans so they can guard against online approaches from unknown parties that could put them, their organization and even national security at risk."

Alan E. Kohler, assistant director of the FBI's Counterintelligence Division, said: "As this movie highlights, foreign intelligence services are posing as headhunters and consultants on professional networking sites to aggressively target Americans. We believe it's critically important to educate the public in order to neutralize this threat from foreign intelligence services. We also believe it's important to send a strong message to hostile intelligence services, as we did in 2018 when a Chinese intelligence officer was arrested in Belgium and extradited to the United States for attempting to steal trade secrets from an American targeted on LinkedIn."

The Threat:
Using professional networking sites and other social media platforms, foreign intelligence services and other hostile actors often pose online as headhunters, interested employers, people with a shared interest, or others with enticing career opportunities in an effort to connect and develop relationships with individuals who have access to valuable and sensitive information.

Over time, these actors often attempt to elicit information about their targets, their work, and their contacts. In some cases, promising targets are offered all-expense-paid trips overseas for meetings or presentations, where they are pressured to turn over additional information. Some foreign intelligence services, including those from China, are doing this on a mass scale, targeting thousands globally via social media to obtain information they want.

Current and former government employees are not the only ones at risk from these schemes. Individuals in the private sector and academic and research communities are also being targeted this way by hostile foreign actors seeking to acquire trade secrets, proprietary data, and information on cutting-edge research and technology. Foreign intelligence services are looking to target anyone with access to the information they want, whether classified or unclassified.

Recent Examples:

Dickson Yeo (Facebook)

On July 24, 2020, Singaporean national Dickson Yeo pleaded guilty to acting within the U.S. as an illegal agent of China without first notifying the Attorney General. Posing as a consultant, Yeo used a professional networking site to target and recruit U.S. officials at the direction of Chinese intelligence. According to court documents, after Yeo contacted potential targets online, "the professional networking website began to suggest additional potential targets." According to Yeo, "the website's algorithm was relentless" and "it felt almost like an addiction." Among those who provided Yeo with information was a clearance holder working with the U.S. Air Force on the F-35B military aircraft program and a State Department employee who confided to Yeo he was dissatisfied at work and having financial troubles, and later wrote a report for Yeo about a then-serving U.S. Cabinet Member for money.

Kevin Mallory (Alexandria Sheriff's Office)

On May 17, 2019, former CIA officer Kevin Mallory was sentenced to 20 years in prison for conspiracy to transmit national defense information to China. Mallory was first approached by Chinese intelligence via a fake profile on a professional networking site. Fluent in Mandarin, Mallory worked for CIA, DIA, Department of State, and the U.S. Army. After leaving CIA in 2012, Mallory launched a consulting business, resulting in little success and mounting financial debt. In 2017, Chinese intelligence officers initiated contact with Mallory by having an operative posing online as a corporate headhunter send him a message on a professional networking site. Mallory travelled twice to China, where he was met by a Chinese intelligence officer and paid $25,000. On his second trip, he was provided with a covert communications device to transmit classified information to Chinese intelligence. A subsequent search of Mallory's covert communications device by the FBI revealed classified document remnants.

Mitigating Risk:

At a minimum, the FBI and NCSC encourage the public to practice basic cyber hygiene when receiving an invitation to connect via social media. Never accept an invitation to connect from someone you do not know, even if they are a friend of a friend. If possible, validate invitation requests through other means before accepting them. Report suspicious online approaches to appropriate authorities. And most importantly, be careful what you post on social media platforms about yourself and your job, as it could draw unwanted attention from adversaries and criminals.

International Actions:

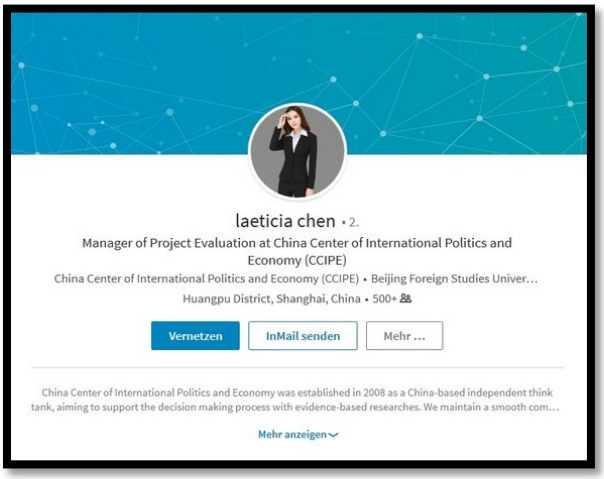
The NCSC and FBI are working with international partners to raise awareness of this threat. Earlier this year, the United Kingdom's (U.K) Centre for the Protection of National Infrastructure (CPNI) released to

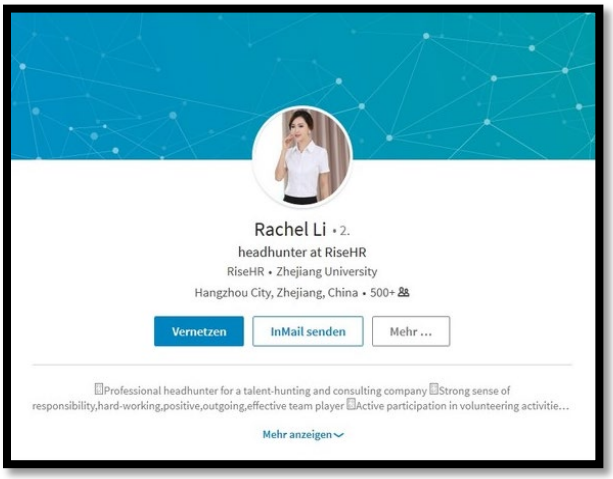
the public a set of “Think before you link” videos and awareness materials to help U.K. government and industry sectors address this threat. CPNI’s “Think before you link” materials can be found here. A direct link to CPNI’s two-minute video “Glitch” can be found here.

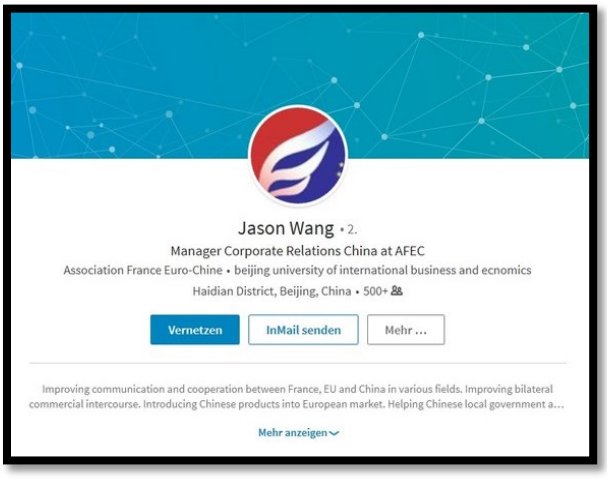
In a 2020 National Security Threat Assessment, the Lithuanian Ministry of National Defence and the State Security Department noted that “hostile foreign intelligence services increasingly use online social networks to find and recruit sources abroad. Chinese intelligence services are particularly aggressive in this area and they mainly use the opportunities provided by the social network LinkedIn.”

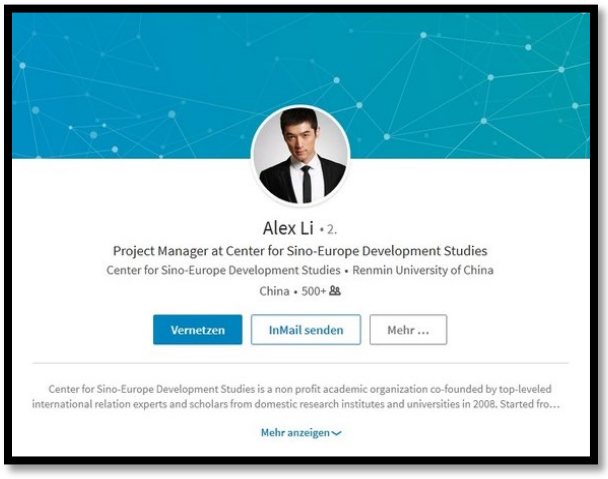
In 2019, the Australian Security Intelligence Organization noted that it had warned business and government partners about “how hostile intelligence services use LinkedIn and other social media platforms to target people in positions that could fulfill a wide range of intelligence objectives.”

In 2017, Germany’s domestic intelligence agency, Bundesamt fur Verfassungsschutz (BfV) issued a public report accusing China’s intelligence services of using fake profiles on social media platforms to target more than 10,000 German citizens, including members of parliament, ministries, and government agencies, over a nine-month period. The BfV report included screen shots (below) of some the fake profiles used for recruitment purposes, which have since been closed down.









# # #