OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

HEALTHCARE & PUBLIC HEALTH SECTOR

30 April 2020

LIR 200430-007

Collection Through Professional Social Networking Sites Highlight Operational Security Vulnerabilities

References in this LIR to any specific commercial product, process or service or the use of any corporate name herein is for informational purposes only and does not constitute an endorsement, recommendation or disparagement of that product, process, service or corporation on behalf of the FBI.

The FBI Newark Field Office and the New Jersey Office of Homeland Security and Preparedness, in coordination with the FBI Office of Private Sector (OPS), prepared this Liaison Information Report (LIR) to inform industry of operational security concerns on professional social networking sites. Nation-state actors, particularly foreign threat country governments, are leveraging publicly available information on professional networking sites to spot, assess, develop, and recruit individuals to steal intellectual and propriety data as well as classified government information. The threat from foreign adversaries presents significant risks to the pharmaceutical industry, which relies on employees to keep intellectual and proprietary data confidential.

Professional social networking sites provides a rich hunting ground for foreign adversaries. Predominantly, white-collar subscribers use it to make connections, advertise their expertise, seek employment, or engage with peers in expert-based discussion groups. To bolster their credentials, users—even current and former U.S. national security officials—post detailed resumes and recommendations from their colleagues. Information available on can include a photograph of the user, contact information, the user's network (i.e., friends), current location, current/former places of employment, universities attended and majors, skills/endorsements (i.e., security clearance, certifications held, knowledge of specific research methods/tools), recommendations, accomplishments, and interests. This information could be used to craft targeted attacks.

Many employees within the pharmaceutical industry maintain profiles on this site for professional and networking purposes. Nation-state actors exploit the professional networking's open platform through the elicitation of personal and professional information from targets to gauge their value. With their most promising targets, they may offer all-expense-paid trips, employment offers, opportunities to make presentations, or joint research opportunities. China primarily has attempted to recruit individuals in the fields of aerospace, biotechnology, pharmaceutical, clean energy, deep-sea technology, information, and manufacturing fields. Its strategic goals for collection include leveraging non-traditional collectors, joint ventures, and other avenues of approach to collect necessary information, both unclassified and classified, from current and former employees.

- In June 2019, Iran-linked threat actors used the professional networking site to conduct a phishing campaign that asked victims to join their social network, according to FireEye. The adversaries masqueraded as a Cambridge University lecturer, including setting up a fake professional networking site page, to gain victims' trust. From there, the attackers asked their "friends" to open

malicious documents. FireEye noted APT34 actors used a mix of public and nonpublic tools to collect strategic information that would benefit nation-state interests pertaining to geopolitical and economic needs.

- In a June 2018 felony complaint accusing a former Defense Intelligence Agency (DIA) case officer of spying on behalf of the Chinese, the FBI noted that "printed information from a professional networking site related to several former and current DIA case officers" ahead of a trip to China in 2015. The individual was arrested in 2018 at a Seattle airport as he prepared to board a flight to China with secret US military information, according to the Justice Department. In 2019, the individual pleaded guilty and was sentenced to 10 years in federal prison.

- In October 2018, the Justice Department charged Yanjun Xu, an intelligence officer with China's Ministry of State Security, with economic espionage after he recruited a General Electric aviation engineer in a relationship that began on a professional social networking site, according to the indictment. The indictment alleges that, from around December 2013 until his arrest in April 2018, Xu recruited employees from major aerospace companies and convinced them to travel to China on the pretext of giving a presentation at a university, prosecutors said. Ultimately, Xu sought to steal trade secrets and other sensitive information from multiple American aerospace companies.

- In December 2017, Germany announced the results of a nine-month study where it discovered more than 10,000 Chinese intelligence connection attempts on a particular professional networking site via fake accounts. The fake account holders posed as recruiters and the heads of consulting firms or think tanks, and they reached out to a variety of targets within the German government.

Recommended Risk Mitigation Strategies

The pharmaceutical industry can take various steps to protect itself and employees from nation-state attempts to elicit intellectual and propriety data. This includes:

- Limit the amount of information on your professional social networking site profile
- Do not accept professional networking connections from people you do not know
- Ensure that the professional social networking site profile really belongs to the person it says it does. Check to see if you have mutual connections on the professional networking site and, if you do, reach out to those individuals to verify
- Check periodically to make sure no one has opened an account in your name or in a common variant of your name
- Question all-expense-paid trips, employment offers, opportunities to make presentations, or joint research opportunities
- Educate and regularly train employees on security policies and protocols

- Establish protocols for internal suspicious activity reporting
- Ensure proprietary information is carefully protected and monitored
- Report any suspicious professional, social networking site activity to the FBI Public Access Line (PAL)

To report any information potentially related to this matter, contact your FBI Private Sector Coordinator at your local FBI Field Office.

This LIR was disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices

OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP:RED  Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.