# Nation State Recruiting via Fraudulent LinkedIn Profiles

Threat Bulletins | Oct 14, 2020, 11:00 AM

Health-ISAC members report the increased frequency of LinkedIn being leveraged as a social engineering attack vector by nation-state adversaries. Attacks are becoming more sophisticated, escalating from basic phishing emails to whaling via LinkedIn. Nation-state threat actors are developing convincing LinkedIn profiles shortly before launching their attack campaigns. These profiles appear as legitimate LinkedIn users complete with endorsements and hundreds of connections. Executives, VPs, and Research and Development (R&D) teams have been targeted, including those working on COVID-19 vaccine and therapy programs.

The threat actors adopt the use of fluent business terminology, sector knowledge, personal references and spoofed profiles to make whaling attacks difficult for even a cautious eye to identify. The adversary uses highly targeted content combined with several other methods which executives, VPs, and R&D teams should be aware of to reduce their chances of falling victim to a whaling attack. Recent whaling attacks have used on suppliers or partners to construct whaling communications which appear credible.

**Analysis:**
Fake Job Offers: The nation state attacks outlined in this bulletin are unique in that they first make use of LinkedIn as an attack vector as opposed to the most observed tactic of email phishing. The adversary delivers well-crafted job offer letters to unsuspecting but targeted recipients who are made to believe the offer originates from an authorized colleague based on the well-developed fraudulent LinkedIn profile delivering the offer letter.

Other:
In addition to LinkedIn, the adversary is utilizing WhatsApp and Skype as additional methods to communicate with their victims. Once initial communication is established, the adversary either sends directly or provides a link to a Microsoft Word document which contains malicious macros. The adversary can also request personally identifiable information (PII), later using the PII in identity fraud attacks and further social engineering schemes. The adversary is additionally using critical language and themes to invoke urgency, creating a rapid, unsecure process to transmit PII and open malicious documents.

## Recommendations:

Health-ISAC previously reported on LinkedIn whaling in our September Cyber Threat Level published here including resources with additional guidance and training on common adversary campaigns.

Member organizations should leverage tools that provide visibility into authorized social media platforms, including LinkedIn and are encouraged to focus on social media phishing training and awareness for all employees. If an organization advertises partners such as charities, law firms, or academic institutions, they should be aware that they may receive LinkedIn messages from malicious actors masquerading as those trusted partners. LinkedIn provides guidance for recognizing and reporting scams here.

- Do not accept LinkedIn connection requests from people you do not know.
- Do not respond to unsolicited messages received via LinkedIn or any other social media accounts.
- Be very careful with unsolicited job offers as they are increasingly used as lures.
- Do not give out your phone number to unknown or unverified parties.

- Consider it a red flag when asked to switch conversations to other platforms such as WhatsApp or Skype. These platforms often do not have the protections provided by corporate networks and email systems.
- Do not follow instructions to click on links or download files to your PC.
- Recognize that fraudsters commonly use urgency as a tactic to get you to open files or click on links.
- If you have received this request or one similar, even using different names or company affiliations, stop! Do not engage in the communication further until you can independently verify the person seeking to engage with you is legitimate.
- Report all suspicious communications over email, text message, social media, phone call, or in person.

### Sources:

Recognizing and Reporting Linkedin Scams
CISO MAG - Operation North Star: A New Phishing Campaign Disguised as Job Posting
PDF - ClearSky Cyber Security - Operation 'Dream Job'
KnowB4 - Scam Of The Week: Massive LinkedIn Spam Steals Passwords
NK News - North Korea-linked hackers fake prestigious job listings to target victims


**Get access to the new H-ISAC Intelligence Portal:** Enhance your personalized information-sharing community with improved threat visibility, new notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.
**For Questions or Comments:** Please email us at toc@h-isac.org