ONLINE TARGETING OF CURRENT & FORMER U.S. GOVERNMENT EMPLOYEES

Foreign intelligence entities, particularly those in China, are targeting current and former U.S. government (USG) employees for recruitment by posing as consulting firms, corporate headhunters, think tanks, and other entities on social and professional networking sites. Their deceptive online job offers, and other virtual approaches, have become more sophisticated in targeting unwitting individuals with USG backgrounds seeking new employment. Current and former federal employees should beware of these approaches and understand the potential consequences of engaging. U.S. clearance holders are reminded of their legal obligation to protect classified data even after departing USG service.

RED FLAGS

Signs of Potential Online Targeting by Malicious Actors

Online targeting may occur on social media, professional networking sites, and online job boards, as well as through direct contact via email and various messaging platforms. Recruiters may appear to be affiliated with a legitimate firm from a non-alerting country.

Too Good to Be True: Be suspicious of jobs offering remote or flexible work and a disproportionately high salary for the role advertised.

Urgency: The recruiter may be overly responsive to your messages and try to rush you off the networking platform to a more secure communication method.

Flattery: The recruiter may overly shower you with praise or refer to you as a top candidate, especially if your U.S. government affiliation is known.

Requests: The recruiter may initially request you provide written reports on innocuous topics for the job, followed by demands for reports containing non-public or sensitive information.

Scarcity: There may be an emphasis on so-called limited, one-off, or exclusive online job opportunities for quick payment.

Expedited Timelines: The job hiring and payment cycle may take only a few weeks, rather than several months.

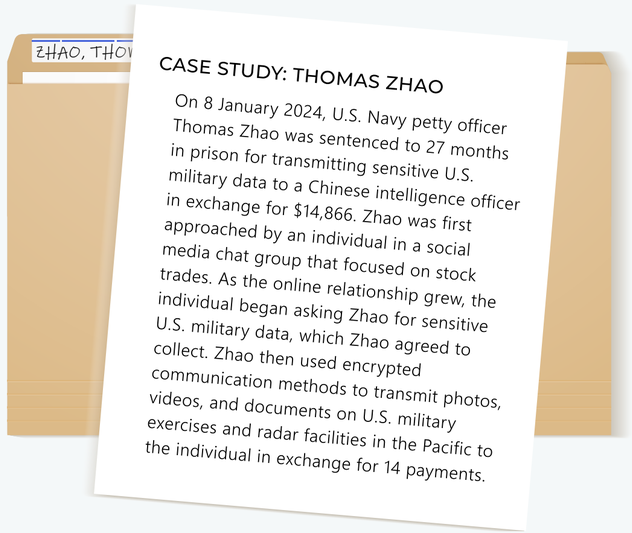
MITIGATION STRATEGIES

Employees

- **Practice good cyber hygiene** when using social and professional networking sites and other platforms.
- **Make yourself a harder target.** Be careful what you post online about your work (particularly security clearances), as it could draw unwanted attention from threat actors. Review your online account settings to control data about you that is publicly available. Current/former clearance holders must also follow their agency's prepublication review requirements.
- **Don't accept online invitations to connect with strangers** unless you can validate them first through other means.
- **Conduct rigorous due diligence** on the individual and/or entity offering the job opportunity.
- **Familiarize yourself with the outside employment requirements of your department or agency** if you are a current USG employee. Declare and obtain advance permission for all outside employment, including gig work. Protect yourself by ensuring a security officer reviews and approves any outside employment offer.

Employers

- **Train employees on cyber hygiene** and the deceptive online recruitment tactics used by foreign intelligence entities.
- **Ensure employees know** which information related to their jobs is sensitive and must be protected. Do not leave gray areas.
- **Communicate well and often** with employees to minimize confusion or frustration. Be transparent and respond to concerns with patience and empathy.
- **Coordinate** with HR, IT, Labor & Employee Relations, and personnel/physical security offices to make organized, comprehensive departure plans. Ensure employees are briefed out of any sensitive programs and remind them of their duties to protect information in perpetuity.
- **Provide easy access to support services** (mental, financial, career, etc.) for both current and departing employees. Ensure employees understand any prepublication review requirements.



CASE STUDY: THOMAS ZHAO

On 8 January 2024, U.S. Navy petty officer Thomas Zhao was sentenced to 27 months in prison for transmitting sensitive U.S. military data to a Chinese intelligence officer in exchange for $14,866. Zhao was first approached by an individual in a social media chat group that focused on stock trades. As the online relationship grew, the individual began asking Zhao for sensitive U.S. military data, which Zhao agreed to collect. Zhao then used encrypted communication methods to transmit photos, videos, and documents on U.S. military exercises and radar facilities in the Pacific to the individual in exchange for 14 payments.

Additional Resources:

- NCSC: Intelligence Threats & Social Media Deception Resources
- FBI: Clearance Holders Targeted on Social Media
- DCSA: DOD Insider Threat Management and Analysis Center (DITMAC)
- *The Nevernight Connection* Short Film
- UK National Protective Security Authority (NPSA): Think Before You Link

Reporting:

- Report suspicious online approaches to social media platforms
- If you believe that you or your personnel have been targeted, contact the nearest FBI office at: www.fbi.gov/contact-us/field-offices, submit a tip online at: tips.fbi.gov/home, or call 1-800-CALL-FBI

Additional Information:

- Unclassified NCSC products can be found at: www.ncsc.gov
- Federal Bureau of Investigation (FBI) website: www.fbi.gov
- Defense Counterintelligence and Security Agency (DCSA) website: www.dcsa.mil
- For those seeking updates and alerts about NCSC products and other news, email: NCSC_Outreach@odni.gov
- Follow NCSC on social media: @NCSCgov or National Counterintelligence and Security Center