Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

9 April 2020

PIN Number
20200409-001

Please contact the FBI with any questions related to this Private Industry Notification.

Local Field Offices:
www.fbi.gov/contact-us/field-offices

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This PIN has been released **TLP:WHITE**.

Nation-State APTs Continue to Target US Think Tanks; Sensitive Information Remains at Risk

Summary

Nation-state Advanced Persistent Threat (APT) actors continue to target US think tanks as a means of acquiring sensitive information. These adversaries have successfully compromised the think tanks by unsophisticated social engineering tactics and exploiting common vulnerabilities in networks, highlighting a significant security gap in the protection of sensitive national security information. Nation-state APT actors have sought access to US think tank organizations – which employ former US Government (USG) personnel who continue to engage with current USG officials on political, domestic, foreign, and economic policies – as a means to collect sensitive USG information, bypassing the need to target USG networks directly.

The reasoning behind this targeting approach is two-fold: USG networks tend to be more secure and more difficult to access, and mitigation efforts within USG networks have historically been effective. As such, adversaries pursue alternate paths to collect similar information, pivoting to organizations that maintain USG connections, possess USG information and personal identifying information, and have little-to-no USG network defense oversight, which create significant security issues in the protection of sensitive information.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

History of Targeting

Nation-state APT actors have continued to target US think tanks since at least 2014 and have successfully compromised many of these same networks since that time. Adversaries have likely relied on multiple avenues for initial access - from employing low-skilled capabilities to gain access via credential harvesting and spear-phishing attacks, to leveraging advanced approaches to take advantage of unpatched and unsecured networks. In some instances, following successful mitigation and removal of adversaries from compromised networks, actors have been able to regain access shortly thereafter, continuing to exfiltrate sensitive information and put networks at risk.

Depth of Information Acquired

Information acquired by nation-state APT actors has spanned multiple subjects, many of which include sensitive topics not intended for exposure to adversaries. The information stolen by adversaries has mainly coincided with current world events, with adversary interest focused on the US position and policy perspective, presumably in support of strategic decision making by nation-state leadership. The following is a general listing of themes acquired from compromised US think tanks over the past several years:

- US Elections-Related Topics
- US Plans to Support Opposition Movements
- US Views on Arms Treaties and Missile Defense
- US Politics and Foreign Policy
- US Interests in Conflict Areas
- US Interests/Conflicts with Competing World Powers
- US Decision Making and National Security Issues
- US Energy Policy
- US Cyber Deterrence
- US Efforts to Counter Foreign Influence
- US Collaboration on Advanced Technologies
- US and NATO Interests
- US Defense Plans
- US Missile Development Plans
- US Sanctions Planning

Mitigation Guidance

The information sought by APT actors will likely continue to be a primary focus of their collection interests; however, proper network defense and adherence to information security best practices can assist in mitigating the threat and reducing the risk that endangers sensitive national security information. The following guidance may assist in developing proper network defense procedures:

- Provide training on methods to secure and transmit sensitive information
- Apply encryption to data at rest and data in transit
- Employ and support proper procedures for password security
- Require two-factor authentication for account/network access
- Provide appropriate employee training on the dangers and impact of social engineering (spear-phishing attacks and email spoofing)
- Blacklist malicious IPs, and those from unverified/obfuscated sources (TOR, unapproved VPNs, etc.)
- Routinely apply software patches and upgrades

Reporting Suspicious Activity

The FBI encourages organizations which may have been affected by nation-state APT activity to contact their local FBI field office. A list of FBI field offices is available at https://www.fbi.gov/contact-us/field-offices.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey