Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

13 June 2018

PIN Number
20180613-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

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

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

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: GREEN**: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

APT Actors Likely to Target US Cleared Defense Contractors

Summary

APT actors in the near future likely intend to target US Cleared Defense Contractors (CDC) via spear phishing campaigns or network infrastructure compromises, according to recent intelligence. Common spear phish targets may include individuals featured on internet-facing CDC Web sites and high-ranking CDC executives.

FBI has observed APT actors over the past two years precede spear phishing campaigns with open source research of targeted US company websites, particularly sections containing contact information for company officials which include names, titles, telephone numbers, and email addresses. In one case, an APT actor sent spear phishing emails within one-to-two weeks after researching the targeted US company.

Historically, APT actors have a strong desire to collect US defense and scientific intelligence to further their interests and advance strategic goals. As a result, US CDCs and research facilities may likely be targets for cyber adversaries due to their involvement in national security and their close relationship with the US Government.

Most companies publicly share their contact information and high-level management names on their corporate Web pages. Some corporate employees share other forms of personally identifiable information on various social media platforms. Adversaries may use this publicly-posted information to target individuals with the end goal of infecting a corporate network for intelligence collection.

Common techniques used by APT actors include sending well-crafted spear phishing messages tailored to the professional interests of the target, the use of watering holes to redirect visitors to malicious Web sites, and the use of stolen or weak user credentials to exploit a network vulnerability. After a successful compromise, APT actors attempt to expand their access in the network to multiple systems to facilitate information theft.

APT actors have increased their activity over the last several years. Cyber attacks such as WannaCry and NotPetya in the spring and summer of 2017 are examples of increasing APT activity. While WannaCry and NotPetya were not directed at the United States, both had inadvertent negative effects on US systems. The FBI advises companies to be mindful that similar attacks may likely occur in the near future. Previous attacks have coincided with national holidays of cyber targets, such as Constitution Day in Ukraine on 28 June.

For recent guidance on mitigation strategies against spear phishing and network infrastructure targeting, please refer to the following joint technical alerts:

https://www.us-cert.gov/ncas/alerts/TA18-074A

https://www.us-cert.gov/ncas/alerts/TA18-106A

Recommendations:

The FBI recommends providers implement the preventative measures listed below to help secure their systems from attacks:

- Ensure anti-virus software and firmware is up-to-date

- Monitor employee logins outside normal business hours and other anomalous activity
- Close unused ports
- Monitor employee logins outside normal business hours and other anomalous activity
- Provide regular training to employees regarding current social engineering threats, scrutinizing e-mail links and attachments, and pop-ups from attachments requesting enabling certain functions (i.e., macros)
- Brief executives at your company to be extra vigilant and report any suspicious email messages
- Apply extra scrutiny to e-mail messages with links or attachments directed toward executives

This product is marked **TLP:GREEN**. 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.

For comments or questions related to the content or dissemination of this product, contact CyWatch.

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