Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

7 November 2019

PIN Number
20191107-001

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:WHITE**: 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.

Cyber Actors Leverage Subscription-based Commercial Databases to Conduct Business Email Compromise Fraud against Construction Companies

Summary

The FBI has observed cyber actors leveraging commercial databases to obtain victim targeting information to perpetuate Business Email Compromise (BEC) fraud against construction companies and their vendors.

Threat

Since December 2016, cyber actors have used subscription-based commercial databases to obtain intelligence on commercial construction projects across North America. These databases enable BEC actors to learn specifics about

tens of thousands of construction projects including key contact information, project costs, bidder lists, plan holder lists, project specifications, and agendas.

BEC actors use this intelligence to register domains similar to construction companies who have won bids and are engaged in ongoing projects. The fraudsters then send an email to the victim company, which includes an attached direct deposit form and instructions to change previously submitted banking information to a new account controlled by the actor. The victim company then processes the banking information change, and any future invoice payments are made to the altered account.

Recommendations

- Confirm requests for transfers of funds by using phone verification as part of a two-factor authentication, and verify/use previously known phone numbers.
- Carefully scrutinize all email requests for transfer of funds.
- Verify changes in vendor payment location by adding additional two-factor authentication, such as having secondary sign-off by company personnel.
- Color code correspondence emails from employee/internal accounts and non-employee/external accounts using distinct colors, or adjust settings on the email client to attach warning labels to emails originating from outside the organization.
- Create an email rule to flag email communications where the “reply” email address is different from the “from” email address shown.
- Create intrusion detection system (IDS) rules that flag emails containing extensions similar to the victim company. For example, if the legitimate email is *abc_company.com*, the IDS rules would flag fraudulent emails for *abc-company.com*.

Victim Reporting

The FBI encourages recipients to report suspicious activity to their local FBI field office, located at https://www.fbi.gov/contact-us/field-offices, or to file a complaint online at https://www.ic3.gov/complaint/splash.aspx.

Administrative Note

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

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