TLP: GREEN

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

9 June 2021

PIN Number

20210609-001

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-offices

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 actors. This PIN has been coordinated with DHS-CISA.

This PIN has been released **TLP: GREEN**: Recipients may share **TLP:GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

Cyber Actors Impersonating Construction Companies to Conduct Business Email Compromises

Summary

The FBI has observed cyber actors exploiting pre-existing business relationships between construction companies and clients to conduct Business Email Compromises (BECs). The targeted entities include construction companies who have contracts with a variety of public and private sector customers. According to the US Census Bureau in 2017, there are roughly 700,000 construction companies in the United States with construction projects totaling an annual revenue of roughly $1.9 trillion, which makes construction companies a lucrative target for cyber actors. The 50 largest firms account for 10% of the total revenue for the construction industry, narrowing down which companies are the most profitable for cyber actors to target.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Threat Overview

As recent as March 2021, the FBI has observed cyber actors impersonating construction companies to conduct BECs to defraud entities across multiple critical infrastructure sectors[a] with whom the construction companies have ongoing, completed, or awarded large scale[b] projects. These BECs have cost victims hundreds of thousands to millions of dollars. Cyber actors use a variety of free or subscription-based online services to collect information on construction companies and the public or private entities with whom they are doing business. This includes online budget data portals belonging to local and state governments, as well as commercial data aggregators for the construction industry. The information collected from these various sources includes project costs, bidder information, and contact information for involved parties, allowing the actors to tailor their fraudulent messages specifically to each victim-contractor relationship.

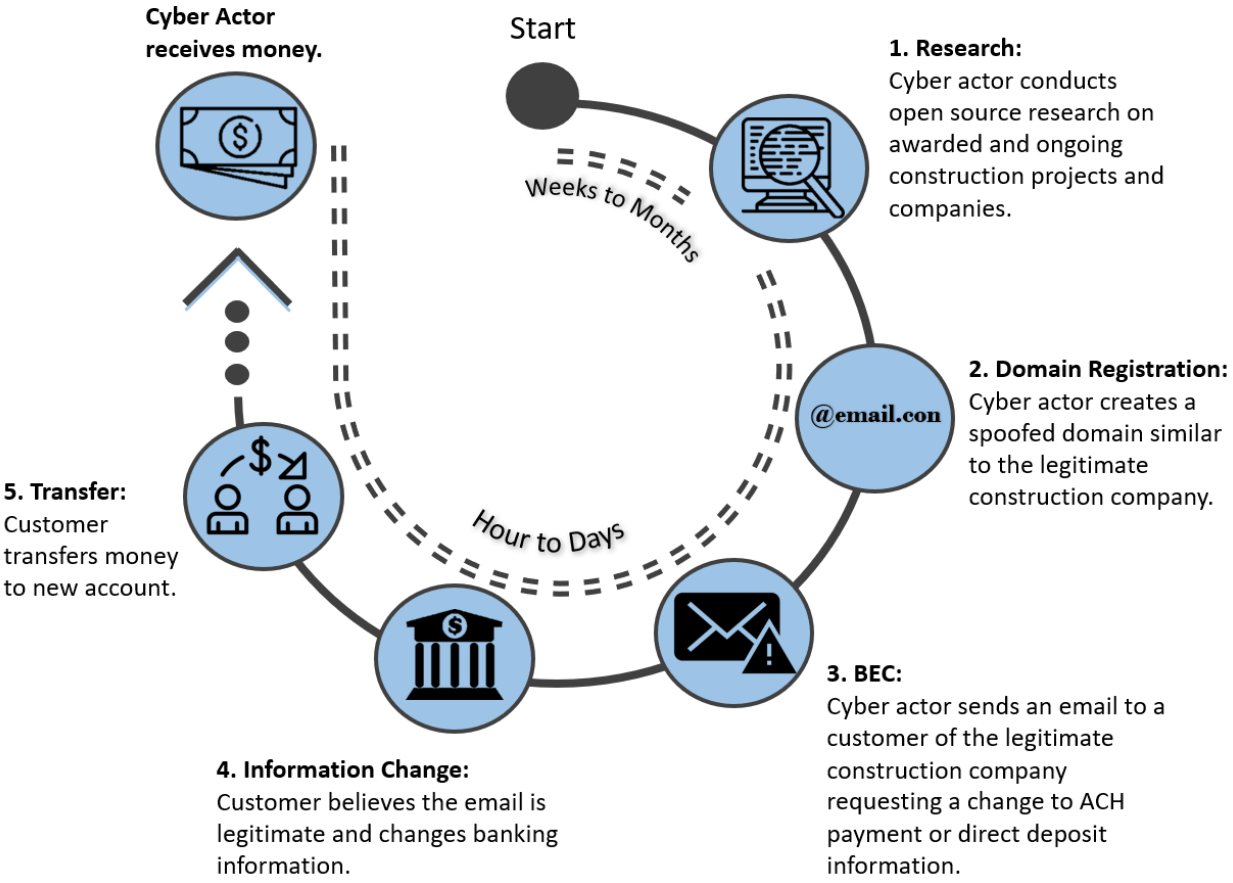
Using the information they compile, the cyber actors register domains that closely resemble the legitimate construction company's domain (e.g. domain spoofing) by using naming variations (e.g. adding the word Group or Inc.), using an acronym instead of the full company name, or adding or changing a character. These spoofed domains are used to create email accounts from which the actors send the fraudulent emails, instructing the targeted entity to update automated clearing house (ACH) or direct deposit account information. These emails contain the legitimate construction company's logo and signature line. The use of the detailed information to impersonate legitimate construction companies and exploit existing business relationships makes it difficult for victims to identify these fraudulent requests. Days or weeks may pass before the victim

[a] Presidential Directive 21 defined the 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the US that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination. The 16 sectors include: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste systems; transportation systems; and water and waste water.

[b] Large scale construction projects are defined in this product as $500,000 or more.

is aware of the fraud until the legitimate construction company contacts them regarding the missed payment.

In some cases, the cyber actors will send an initial email to acquire information on the victim company's ACH process. After receiving the information, the cyber actors tailor the ACH or direct deposit form to the victim, the information is updated, and funds can be transferred to a cyber-actor-specified account. Often times, the cyber actors' payment request amount resembles what has been advertised on the online portals.



Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Recent Activity

- In March 2021, a technical institute received a fraudulent email which appeared to be from a construction contractor, requesting an update to their ACH banking information. In response to the fraudulent request, an employee at the institution's accounts payable office made changes to the ACH without following department policy, resulting in multiple fraudulent transactions worth $1.5 million. The FBI' Recovery Asset Team (RAT) was notified and was able to recover some of the funds for the victim.

- In August 2020, a US school district received an email with an attached invoice from a cyber actor claiming to be an employee of a construction company contracted to build outdoor sports fields for the district. The email provided instructions to wire $356,000 to a specific account. The school district sent the money to the specified account and became aware of the BEC only after the legitimate construction company contacted them requesting the overdue payment. The FBI RAT was able to recover some of the funds wired to the cyber actors.

- In October 2019, cyber actors impersonated a US construction company and sent an email to a US school district requesting an update to a specified bank account for an upcoming invoice. The district made the requested changes and sent approximately $840,000 to the cyber actor-specified account. After notification from the legitimate construction company of missed payment, the school district realized the BEC scheme and were able to recover approximately $5,000.

- In July 2019, a natural gas company received a fraudulent email appearing to be from a US construction company, requesting an update to ACH bank account information. The natural gas company changed the ACH and sent a $31,000 payment for services to the cyber actor-specified account. It was not until the legitimate construction company reached out requesting payment that the

natural gas company became aware of the BEC. The FBI was contacted, but was unable to recover the funds due to amount of time that passed between the payment and notification of the BEC.

Recommended Mitigations

- Verify all payment changes and transactions in-person or via a known, established telephone number. Continue to ensure contact information is current and updated accordingly.
- Carefully check email addresses for slight changes that can make fraudulent addresses appear legitimate and resemble actual companies' names.
- Implement robust approval procedures for vetting account change requests to prevent monetary losses.
- Prohibit automatic forwarding of email to external addresses.
- Add an email banner to messages coming from outside your organization.
- Enable security features that block malicious emails, such as anti-phishing and anti-spoofing policies.
- 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.
- Prohibit legacy email protocols such as POP, IMAP, and SMTP that can be used to circumvent multi-factor authentication.
- Create an email rule to flag email communications where the "reply" email address is different from the "from" email address shown.
- Configure Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication Reporting and Conformance (DMARC) to prevent spoofing and to validate email.
- Encourage the use of domain protection services to notify your organization when similar domains to your company's domain have been registered to prevent domain spoofing.

- Educate employees on BEC scams, including preventative strategies such as how to identify phishing emails and how to respond to suspected compromises.
- Notify customers about BEC threats and mitigation methods your company is taking, such as notifying customers of internal processes for changing or updating ACH banking information.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

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.

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