United States Secret Service [INFO]

March 8, 2019

[INFO] Information Only Alert – GIOC Reference #19-005-I
TLP Green

Emerging Business Email Compromise Scenario: Large Scale Construction and Contracting Firms

Victim reporting of successful Business Email Compromise (BEC) matters continue to increase. Although financial institutions are targeted, other industries remain vulnerable. Real estate, healthcare, human resources, and education sectors continue to be in the crosshairs. Most recently, criminal actors are targeting large-scale construction and contracting firms.

The playbook remains the same:

1) Criminal actors infiltrate the email system of a company through malware or social engineering.
2) Criminal actors register spoofed domains and email accounts that look almost exactly like the potential victims domain.
3) Criminal actors wait until a large financial transaction is imminent. Then using the spoofed email address, criminal actors send fraudulent wiring instructions to redirect wire transfers to a fraudster-controlled bank account.

Recently observed trends involve criminal actors targeting large-scale construction firms. Using spoofed domains to fool entities in the supply chain of construction companies- high dollar transactions intended for allocation in major construction projects are being stolen. The scheme is made possible because the bad actors are using privileged and contemporaneous information obtained through malware and email surveillance to deceive the customers and business partners of the construction companies to reroute their payments.

Several actions can help deter and prevent this fraud scheme:

1) Verify all changes in payment and financial information via phone or in person with a known and trusted individual.
2) Employ dual factor authentication regarding changes in client or financial information.
3) Consistently monitor IT systems for the presence malware.

[INFO] - Indicates informational or educational content.

4) Monitor and restrict the use of auto-forwarding and inbox sweep rules.
5) If email systems are not working properly i.e. missing or not received emails, investigate immediately.
6) Use a domain registration monitoring service to prevent the registration of spoofed domain names.

BEC schemes like those targeting the construction industry are preventable as long appropriate precaution and due diligence is exercised. If a BEC scheme is encountered, contact your local U.S. Secret Service office and file an IC3 complaint at www.ic3.gov/complaint.

Any questions relating to this alert can be directed to the GIOC at gioc@usss.dhs.gov or 202-406-6009.