FARM CREDIT

FRAUD PROTECTION AWARENESS SERIES

Case Study: Account Takeover Issues Wire Transactions in the Millions

Please note that this case study represents an aggregation of actual scenarios brought to CoBank's attention, though company names have been changed.

Situation

Able Company experienced a cyber-account takeover committed through malicious software installed on their computers when the perpetrator hijacked the customer's online banking system session. The malicious software was able to obtain session credentials for creating and approving templates and wires, because the same computer was used by two separate users to approve both the template and the transaction. During the hijacked session the perpetrator created several wire templates and originated multiple wire transactions totaling millions of dollars.

Discovery and Resolution

The fraud was discovered through Able Company's financial institution's fraud protocols, which contacted Able Company to validate one of the wires for a large dollar amount that created fraud alerts. During the conversation, the financial institution validated that Able Company had not originated the wire and it was subsequently cancelled. Due to fraud protocols, the financial institution reviewed additional wire activity for Able Company and discovered that several other wires were originated on the same day. Able Company confirmed that all of the wires were fraudulent and not originated by any of their employees. The financial institution advised Able Company to immediately disconnect the computer(s) used for online banking access and to run anti-malware software to identify and remove any malware that may have infected them.

The financial institution's internal investigation discovered that the account logs used for the fraudulent wire transactions had originating IP addresses in the United Kingdom and Canada. It reported the incident to the local FBI Field Office and requested that Able Company report the fraud incident to the FBI's Internet Crimes & Complaint Center at https://www.IC3.gov.

How it Happened

During the fraud investigation, Able Company discovered that the day prior to the fraudulent wires being originated, an employee received a suspicious email that appeared to come from a colleague. The email contained a URL link that the employee followed. The employee noted that the computer then began running much slower and was inundated by a number of pop-up windows. The employee did not think anything of the occurrence and continued with daily duties, which included logging into the company's online banking to initiate legitimate wire requests.

Watch for These Red Flags

- ✓ **E-mail appears to come from a colleague.**
  Think: would a colleague send this type of e-mail?

- ✓ **The email contained a URL which the employee clicked.**
  Don't click on a URL from unknown source!

- ✓ **The computer began running much slower and was inundated by pop-up windows**
  Disconnect computer from network and have security team diagnose the computer.

- ✓ **When logging into the company's online banking, ensure you log out when your business is finished.**

- ✓ **Credentials for creating and approving templates and wires used on the same computer.**
  Design security protocols restricting creating and approving wire templates and initiating wire transactions on the same computer.