Guardian Analytics

Chatting for Dollars

December 2012

Case Background

Fraudsters are now using financial institutions' (FIs) own processes to commit fraud, employing the FI's customer service representatives to execute fraudulent transactions. Guardian Analytics has uncovered a new attack scheme that takes advantage of the live chat feature in the FIs' online banking platform.

Guardian Analytics has identified several instances of this emerging scheme, all in short order and across multiple FIs. All of the FIs were on the same online banking platform, which suggests a possible connection that the fraudsters know which platforms offer a live chat feature. However, it's too early to say definitively that this scheme is limited to one banking platform.

Fraud Incident Details

Based on the examples seen, here's how the fraud scheme is designed to operate:

1. The fraudster logs into online banking using stolen credentials. He does so from his own computer, using his own Internet Service Provider (ISP).
2. The fraudster does some initial reconnaissance and fraud setup such as checking account balances and completing internal transfers into the checking account, sometimes from multiple accounts. But no transaction is initiated.
3. The fraudster enters into a live chat session with customer service.
4. The fraudster requests assistance with a wire transfer over chat and the customer service rep completes the wire transfer request on behalf of the fraudster.

Observations and Trends:

- In all cases the attacks were executed from locations, computers and ISPs that were unusual for the account holder.
- The attacks included internal transfers, sometimes from multiple accounts, into the checking account from which a wire transfer could be sent. Although internal transfers as an online banking activity were not unusual for the victims, the dollar amounts of the transfers were significantly larger than what was typical for the victims.
- In all cases, this was the first time that the live chat feature had been used, and in most cases the chat feature was used multiple times.
- The fraudster was taking advantage of the fact that he had already been authenticated as part of logging into online banking and knowing that the customer service rep may not ask for any further authentication.
- If all went well, this scheme could have unfolded quite quickly. However, in some cases the scheme didn't work as designed and multiple online banking sessions and multiple live chat sessions were needed, which provided additional data points for fraud analysts and opportunities to detect the scheme.
- All of the transfer amounts were under $8,000, keeping this scheme generally under the radar of most FIs.

Guardian Analytics

Chatting for Dollars

December 2012

Prevention Tips

- Proactively monitor for *any* suspicious activity online, not just transactions. The best chance to stop this type of attack is by noticing before the attack that an account has been compromised and anomalous reconnaissance or fraud setup activity has occurred.
- When suspicious or unusual activity is identified – such as chat being used for the first time, a new login location, a new ISP, or particularly large internal transfer amounts – immediately notify other departments, such as customer service, to be on alert for the account in question.
- Consider a policy to re-authenticate all transactions requested via chat, either via the chat itself or using an out-of-band channel such as by phone.
- Extend processes that are already in place for all phone-requested wire transfers to chat-initiated wire transfers. For example, if a contract is required to send wires over the phone, then the same should be in place for chat. If a PIN is required for phone wires, a PIN should be required for chat. If neither contracts nor PINs are required currently, consider adding such policies.
- Evaluate all account activity including online activity for suspicious behavior prior to releasing wire transfers, regardless of the channel through which the wire request was submitted.

About Guardian Analytics – Guardian Analytics is the leading provider of behavior-based anomaly detection solutions for preventing online, mobile, ACH and wire fraud. Over 200 financial institutions and millions of account holders are protected by FraudMAP and benefit from our Fraud Intelligence research and expertise.