Fake Forgetfulness Flags Fraud

By Craig Priess, Founder and VP, Guardian Analytics

Cyber criminals compromise accounts and complete fraudulent transactions in many different ways. Sophisticated schemes that use advanced malware get a lot of the press. But fraudsters continue to successfully compromise accounts and steal money with relatively simple, human-engineered attacks as well, as exemplified by the scheme described in this article.

Case Background

Criminals have access to a very large cache of information that includes account names, personal information, banking details, and much more. Cybersecurity firm Hold Security revealed recently that it discovered stolen credentials from some 360 million accounts available for sale on the underground Internet. And now fraudsters have demonstrated how they reset passwords to increase their success in using this hoard of data to access online bank accounts.

Our fraud intelligence group has tracked an ongoing series of attacks against our customers that have victimized hundreds of retail clients and a smaller number of commercial accounts at fifty or more banks and credit unions of all sizes. The attacks all include the use of the Forgotten Password feature to defeat authentication, and each institution had multiple victims signaling that once the criminals realized they could compromise one account successfully, they immediately went after more.

Generally, once they gained access to the accounts, criminals were performing online account reconnaissance where they browsed through the account, gathered information, and then logged out. In the majority of cases, they did not attempt a transaction via online banking. At least not before the financial institution was able to proactively intervene given an early indicator that the account had been compromised.

While there were no transactions attempted through online banking, financial institutions must still consider this fraud. Criminals illegally accessed the accounts and can use the information gathered in a variety of ways for their financial gain. Personal information, past deposits or payments data, signatures, and check data can be used for identity theft and offline fraud across a variety of channels. A number of our customers that were the targets of these attacks reported fraudulent transactions attempted through offline channels including faxed wire requests, transaction requests through the call center, and check fraud.

Fraud Incident Details

Criminals compromised both active accounts and dormant accounts (accounts where there are funds, but no activity). One consistent element across all attacks stood out clearly – the use of the Forgotten Password feature to complete the login process. The fraudster would enter the user name and click on the Forgotten Password button, which would present one challenge question, the answer to which the fraudster already had, and then the password could be reset.

There was a confirmation email, so ideally (from the fraudster's perspective), he would also compromise the victim's email account to intercept this notification and remove the risk of the account holder being

alerted. But the email was not necessary to confirm the new password, so even if the fraudster had not compromised the email account, he could still complete authentication and access online banking.

Once in the account, the criminals exhibited the same general pattern of behavior, clearly looking for very specific information about the account and the victim. Some of the frequently used online features used by the fraudsters were View Account Summary, Bill Pay History, and View Check Images.

The pattern and sequence of activities were unusual relative to the victim's typical online banking behavior, enabling institutions using behavioral analytics solutions, like Guardian Analytics FraudMAP, to detect the account compromise and proactively take action to prevent any losses.

Prevention Tips

1. Prioritize layers of security that protect against all of the ways that criminals compromise accounts, not just malware.
2. Look beyond the transaction and evaluate all online activity in your client accounts for unusual behavior, including the pattern noted above.
3. Check with your clients to confirm fraudulent access as quickly as you can. Taking action early will save time and money later. In our experience, clients love the proactive outreach – it is a trust and relationship building event.
4. If you find fraudulent activity, look for other accounts with similar characteristics.
5. When you confirm fraudulent online account access, place alerts on the accounts and watch for fraudulent activity in all channels, particularly faxed wire requests, fraudulent checks, and the call center.

Finally, be sure to check with the appropriate staff at your financial institution to determine if you need to provide a breach notification to your client and report the incident to credit bureaus.

About the Author
Craig Priess, Founder and Vice President, Products & Services
Priess founded Guardian Analytics in 2005, introducing the industry's first individual behavior-based fraud prevention solution. He leads the company's fraud prevention product and service innovations. He also directs the company's Fraud Intelligence and Analyst teams, producing unique insights into fraud trends and fraud prevention best practices. Priess offers expertise in threats, banking and payment systems, and layered security strategies. He is a member of the NACHA Internet Council, the Association of Financial Technology, and FS-ISAC.
www.GuardianAnalytics.com