

The High Wire Act

April 2011



Case Background

Following research reinforcing that corporate account takeover and online fraud are still issues for the industry, institutions and their account holders are experiencing a new trend in online banking fraud attacks. Criminals are compromising the online accounts of small-to-medium sized US businesses (SMBs) and sending wire transfers to economic and trading companies located in the Heilongjiang province in the People's Republic of China.

On April 26, 2011 the FBI, FS-ISAC, and the Internet Crime and Complaint Center [released an alert](#) on the scheme, providing information learned from twenty incidents. The wires were all for high dollar amounts - FBI cases and Guardian Analytics investigations reveal the fraudulent wires ranged from \$50,000 to \$1,900,000. These fraud attempts have occurred as recently as March and April of this year.

Fraud Incident Details

As with the ongoing stream of commercial banking fraud incidents, victims were primarily SMBs banking with local or community banks and credit unions. Very recent cases Guardian Analytics investigated include unsuccessful wire fraud attempts to China via business accounts at two banks in the Midwest, one that experienced a \$1.9M attack, and one that experienced a \$1.8M attack.

Here is how the attacks work:

- Computers of a person within an SMB who can initiate funds transfers were compromised by email-based phishing scams or through visits to malicious websites.
- Criminals installed malware on victims' machines to capture credentials, including the one-time passwords and token IDs.
- While criminals can use malware to appear as if they are logging into online banking from the legitimate user's computer, the incidents reviewed by Guardian Analytics involved criminals logging into online banking from unusual locations, relative to the expected patterns of behavior for the account holders. (Guardian Analytics has identified an IP address associated with these attacks. For more information, please email info@guardiananalytics.com.)
- Malware blocked legitimate user sessions and posted 'maintenance' splash screen for users, allowing the criminal to successfully bypass multi-factor authentication, including tokens.
- Criminals initiated both domestic and international wire transfers with destination accounts in China. Domestic wires had the name of a US-based bank in the wire fields, but contained additional instructions in the wire itself to route funds to a company in China.
- The recipients of the fraudulent transfers all contain the name of a Chinese port. These cities include: Raohe, Fuyuan, Jixi City, Xunke, Tongjiang, or Dongning. The name of the companies receiving the funds also include the words "economic and trade," "trade," and "LTD." The cases Guardian Analytics reviewed contained recipient names of "Raohe Jiaxing Economic and Trading Company" and "Raohe Xinfei Economic and Trading Company."

The High Wire Act

April 2011



- Recipient bank accounts typically were with the Agricultural Bank of China, the Industrial and Commercial Bank of China, or the Bank of China.

Prevention Tips

As the [2011 Business Banking Trust Study](#) highlights, banks have more than financial losses at risk following a fraud attempt. Forty-three percent of businesses took their services to another institution following a fraud attack.

Institutions should be on the lookout for suspicious activity and be particularly vigilant in pinpointing wires with the combination of recipient company and bank names. With the recent breaches at RSA, Epsilon, Sony and others to come, more personal data than ever is available for criminals to use for spear phishing and other social engineering schemes.

Fraud Informer recommends taking the following actions to avoid falling victim to the schemes described above:

- **Proactively search for online wire requests** with the suspect recipient names that are destined for the Chinese cities of Raohe, Fuyuan, Jixi City, Xunke, Tongjiang, and Dongning, and to one of the following banks: Agricultural Bank of China, the Industrial and Commercial Bank of China, or the Bank of China. Be prepared to act quickly.
- **Alert your wire desk** and have them vigilantly review domestic and international transfers that contain recipient information contained in the FBI alert.
- **Inform your business account holders** of this fraud scheme, and enlist their help in monitoring account activity.

In addition, it's important to be aware that fraudsters are continually changing their attacks and to prepare accordingly. Therefore, Fraud Informer further recommends techniques that don't rely on detailed knowledge of an attack.

- **Assume all account holder end points are compromised** and continually monitor all online sessions for unusual logins, unexpected account activity and anomalous transactions relative to expected patterns of behavior for each individual user. This can help identify account takeover before any money leaves your institution.
- **Put in place fraud prevention foundations recommended by analysts** that include account and user behavior-based profiling and monitoring solutions. Taking ownership of the problem at your institution will be a strong signal to your account holders that you are investing in your relationship with them.