



This product was created as part of a joint effort between the Federal Bureau of Investigation, the Financial Services Information Sharing and Analysis Center (FS-ISAC), and the Internet Crime Complaint Center (IC3).

Fraud Alert Involving Unauthorized Wire Transfers to China

26 April 2011

The FBI has observed a trend in which cyber criminals — using the compromised online banking credentials of U.S. businesses — sent unauthorized wire transfers to Chinese economic and trade companies located near the Russian border.

Between March 2010 and April 2011, the FBI identified twenty incidents in which the online banking credentials of small-to-medium sized U.S. businesses were compromised and used to initiate wire transfers to Chinese economic and trade companies. As of April 2011, the total attempted fraud amounts to approximately \$20 million; the actual victim losses are \$11 million.

In a typical scenario, the computer of a person within a company who can initiate funds transfers on behalf of the U.S. business is compromised by either a phishing e-mail or by visiting a malicious Web site. The malware harvests the user's corporate online banking credentials. When the authorized user attempts to log in to the user's bank Web site, the user is typically redirected to another Web page stating the bank Web site is under maintenance or is unable to access the accounts. While the user is experiencing logon issues, malicious actors initiate the unauthorized transfers to commercial accounts held at intermediary banks typically located in New York. Account funds are then transferred to the Chinese economic and trade company bank account.

Victims

Like most account takeover fraud, the victims tend to be small-to-medium sized businesses and public institutions that have accounts at local community banks and credit unions, some of which use third-party service providers for online banking services.

Recipients

The intended recipients of the international wire transfers are economic and trade companies located in the Heilongjiang province in the People's Republic of China. The companies are registered in port cities that are located near the Russia-China border.

The FBI has identified multiple companies that were used for more than one unauthorized wire transfer. However, in these cases the transfers were a few days apart and never used again. Generally, the malicious actors use different companies to receive the transfers. The companies used for this fraud include the name of a Chinese port city in their official name. These cities include: Raohe, Fuyuan, Jixi City, Xunke, Tongjiang, and Dongning. The official name of the companies also include the words “economic and trade,” “trade,” and “LTD.”

The economic and trade companies appear to be registered as legitimate businesses and typically hold bank accounts with the Agricultural Bank of China, the Industrial and Commercial Bank of China, and the Bank of China.

At this time, it is unknown who is behind these unauthorized transfers, if the Chinese accounts were the final transfer destination or if the funds were transferred elsewhere, or why the legitimate companies received the unauthorized funds. Money transfers to companies that contain these described characteristics should be closely scrutinized.

Unauthorized Wire Transfers

The unauthorized wire transfers range from \$50,000 to \$985,000. In most cases, they tend to be above \$900,000, but the malicious actors have been more successful in receiving the funds when the unauthorized wire transfers were under \$500,000. When the transfers went through successfully, the money was immediately withdrawn from or transferred out of the recipients’ accounts.

In addition to the large wire transfers, the malicious actors also sent domestic ACH and wire transfers to money mules in the United States within minutes of conducting the overseas transfers. The domestic wire transfers range from \$200 to \$200,000. The intended recipients are money mules, individuals who the victim company has done business with in the past, and in one instance, a utility company located in another U.S. state. The additional ACH transfers initiated using compromised accounts range from \$222,500 to \$1,275,000.

Malware

The type of malware has not been determined in every case but some of the cases involve Zeus, Backdoor.bot, and Spybot. In addition, one victim reported that the hard drive of the compromised computer that was infected was erased remotely before the IT department could investigate.

- Zeus — malware that has the capability to steal multifactor authentication tokens, allowing the criminal(s) to log in to victims’ bank accounts with the user name, password, and token ID. This can occur during a legitimate user log-in session.
- Backdoor.bot — malware that has worm, downloader, keylogger, and spy ability. The malware allows for the criminal(s) to access the infected computer remotely and further infect computers by downloading additional threats from a remote server.

- Spybot — an IRC backdoor Trojan which runs in the background as a service process and allows unauthorized remote access to the victim computer.

Recommendation to Financial Institutions

- Banks should notify their business customers of any suspicious wire activity going to the following Chinese cities: Raohe, Fuyuan, Jixi City, Xunke, Tongjiang, and Dongning.
- Wire activity destined for the Chinese cities of Raohe, Fuyuan, Jixi City, Xunke, Tongjiang, and Dongning should be heavily scrutinized, especially for clients that have no prior transaction history with companies in the Heilongjiang province.

For recommendations on how businesses can Protect, Detect, and Respond to Corporate Account Takeovers such as this, please refer to the “Fraud Advisory for Businesses: Corporate Account Take Over” available at <http://www.fsisac.com/files/public/db/p265.pdf>.

Incident Reporting

The FBI encourages victims of cyber crime to contact their local FBI field office, <http://www.fbi.gov/contact/fo/fo.htm>, or file a complaint online at www.IC3.gov.