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 – Cyber Criminals Targeting Financial Institution Employee Credentials to Conduct Wire Transfer Fraud

17 September 2012

Recent FBI reporting indicates a new trend in which cyber criminal actors are using spam and phishing e-mails, keystroke loggers, and Remote Access Trojans (RAT) to compromise financial institution networks and obtain employee login credentials. The stolen credentials were used to initiate unauthorized wire transfers overseas. The wire transfer amounts have varied between $400,000 and $900,000, and, in at least one case, the actor(s) raised the wire transfer limit on the customer's account to allow for a larger transfer. In most of the identified wire transfer failures, the actor(s) were only unsuccessful because they entered the intended account information incorrectly.

Tradecraft

The actor(s) primarily used spam and phishing e-mails to target their victims. Once compromised, keyloggers and RATs installed on the financial institution employee's computer provided the actor(s) with complete access to internal networks and logins to third party systems. Variants of ZeuS malware were used to steal the employee's credentials in a few reported incidents.

In some instances, the actor(s) stole multiple employee credentials or administrative credentials to third party services and were able to circumvent authentication methods used by the financial institution(s) to deter fraudulent activity. This allowed the intruders to handle all aspects of a wire transaction, including the approval.

The unauthorized transactions were preceded by unauthorized logins that occurred outside of normal business hours using the stolen financial institution employees' credentials. These logins allowed the actor(s) to obtain account transaction history, modify or learn institution specific

wire transfer settings, and read manuals providing information and training on the use of US payments systems.

In at least one instance, actor(s) browsed through multiple accounts, apparently selecting the accounts with the largest balance.

Victims

Small-to-medium sized banks or credit unions have been targeted in most of the reported incidents, however, a few large banks have also been affected.

Denial of Service Attacks

In some of the incidents, before and after unauthorized transactions occurred, the bank or credit union suffered a distributed denial of service (DDoS) attack against their public Web site(s) and/or Internet Banking URL. The DDoS attacks were likely used as a distraction for bank personnel to prevent them from immediately identifying a fraudulent transaction, which in most cases is necessary to stop the wire transfer. One botnet that has been used for this type of distraction is the Dirtjumper botnet. Dirtjumper is a commercial crimeware kit that can be bought and sold on criminal forums for approximately $200.

Recommendations to Financial Institutions:

- Educate employees on the dangers associated with opening attachments or clicking on links in unsolicited e-mails
- Do not allow employees to access personal or work e-mails on the same computers used to initiate payments
- Do not allow employees to access the Internet freely on the same computers used to initiate payments
- Do not allow employees to access administrative accounts from home computers or laptops connected to home networks
- Ensure employees do not leave USB tokens in computers used to connect to payment systems
- Review anti-malware defenses and ensure the use of reputation based content and website access filters
- Ensure that workstations utilize host-based IPS technology and/or application white-listing to prevent the execution of unauthorized programs
- Monitor employee logins that occur outside of normal business hours
- Consider implementing time-of-day login restrictions for the employee accounts with access to payment systems
- Restrict access to wire transfer limit settings
- Reduce employee wire limits in automated wire systems to require a second employee to approve larger wire transfers.

- If wire transfer anomaly detection systems are used, consider changing "rules" to detect this type of attack and, if possible, create alerts to notify bank administrators if wire transfer limits are modified
- Secure and/or store manuals offline or restrict access to the training system manuals with further security, such as enhanced access controls and/or segregation from the payment systems themselves
- Monitor for spikes in website traffic that may indicate the beginning of a DDoS and implement a plan to ensure that when potential DDoS activity is detected, the appropriate authorities handling wire transfers are notified so wire transfer requests will be more closely scrutinized
- Strongly consider implementing an out of band authorization prior to allowing wire transfers to execute
- Limit systems from which credentials used for wire authorization can be utilized
- Review intrusion detection and incident response procedures and consider conducting a mock scenario testing exercise to ensure familiarity with the plan

Incident Reporting

1. 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.

2. The FS-ISAC encourages member institutions to report any observed fraudulent activity through the FS-ISAC submission process and login at http://www.fsisac.com/. This can be done with attribution or anonymously and will assist other members and their customers to prevent, detect, and respond to similar attacks

3. Financial institutions' compliance or anti-money laundering team(s) should submit a Suspicious Activity Report (SAR) utilizing the Account Takeover guidance issued by the Financial Crimes Enforcement Network (FinCEN).