Account Hijacking of Corporate Customers
Recommendations for Customer Education
24 August 2009

This product was derived from a joint effort between the Federal Bureau of Investigation (FBI), the Financial Services Information Sharing and Analysis Center (FS-ISAC), NACHA - the Electronic Payments Association, and other Federal government agencies.

Background

There has been a shift in the online criminal world from primarily targeting of individuals to increased targeting of corporations. In the past 6 months financial institutions, security companies, the media and law enforcement agencies are all reporting a significant increase in funds transfer fraud involving the exploitation of valid online banking credentials belonging to small and medium sized businesses. Eastern European organized crimes groups are believed to be predominantly responsible for the activities that are also employing witting and unwitting accomplices in the United States (money mules) to receive, cash and forward payments from thousands to millions of dollars to overseas locations via popular money and wire transfer services.

Compromise of the Customer

Typically compromise of the customer is carried out via a "spear phishing" e-mail which directly names the recipient correctly and contains either an infected file or a link to an infectious Web site. The e-mail recipient is generally a person within a company who can initiate funds transfers or payments on behalf of the business. Once the user opens the attachment, or clicks the link to open the Web site, malware is installed on the user's computer which usually consists of a Trojan keystroke logger, which harvests the user's corporate online banking credentials. Many types of spear-phishing have been used by criminal groups including messages impersonating the Better Business Bureau, US Court System, and UPS to name a few. The image below shows a recent example of a fraudulent Microsoft Update web site where receivers of "spear phishing" e-mails were taken after clicking the embedded link within the e-mail.

In this example the phishing e-mail was posing as a Microsoft Critical Update, thus bringing the user to a fictitious Microsoft page.

The Fraud

The customer's online credentials are either uploaded to a website from where the fraudster can later download them, or, if the bank and customer are using two factor authentication system, the Trojan keystroke logger may detect this and immediately send an instant message to the fraudster alerting them of the secure web activity. The fraudster then accesses the financial institution through use of the captured username and password or through hijacking the secure web session.

The fraud is carried out when the fraudster creates another user account from the stolen credentials or directly initiates a funds transfer masquerading as the legitimate user. These transfers have occurred through wire or ACH that are directed to the bank accounts of willing or unwitting individuals. Often within a couple days, or even hours of recruiting money mules and opening accounts, money is deposited and the mule is directed to immediately forward a portion of the money to subjects in Eastern Europe by various means.

Recommendations for Financial Institutions

The FS-ISAC[a] and NACHA[b] observe that implementation of information security best practices and comprehensive technology solutions is increasingly important to hinder and prevent the continual ease with which these and other intrusions are conducted in order to mitigate the

---

[a] FS-ISAC, or Financial Services Information Sharing and Analysis Center, was established in 1999 by the financial services sector in response to 1998's Presidential Directive 63 which mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect US critical infrastructure.

[b] NACHA, the Electronic Payments Association, and formerly the National Automated Clearing House Association, was formed in 1974 to establish uniform operating rules for the exchange of ACH payments.

potential for longer-term loss of confidence in the financial sector. Therefore, the FS-ISAC and NACHA recommend that all financial institutions consider implementing the following controls:

- Strong Authentication – Financial Institutions should review the Federal Financial Institutions Examination Council's (FFIEC's) guidance, *Authentication in an Internet Banking Environment* (FIL-103-2005).
- Anomalous/Fraudulent Transaction Detection - Financial institutions should implement appropriate fraud detection and mi*tigation best practices including transaction ris*k profiling.
- Out-of-Band Transaction Authentication – Consider using manual or transaction authentication systems in concert with fraud detection.
- Network Defense-in-Depth - Institutions should implement a best practice, layered Defense-in-Depth[c] to their network and system infrastructure. This Defense-in-Depth should include both technical and procedural controls.

The FS-ISAC and NACHA can refer member institutions to further appropriately detailed resources on these subjects.

Recommendations to Business and Corporate Customers

Guidance from regulatory agencies has not, to date, focused on account compromise issues surrounding corporate customers. The FS-ISAC and NACHA recommend financial institutions educate corporate and small business customers on the need to operate in a secure way as well, including:

- Account Controls:
  - Educating customers proactively about account features that may protect their accounts, such as check cashing limitations and automated payment filters.
  - Recommend reconciliation of all banking transactions on a daily basis.
  - Recommend customers initiate ACH and wire transfer payments under dual control, with a transaction originator and a separate transaction authorizer.
- Recommend customers employ best practices to secure computer systems in their business including but not limited to:
  - If possible, and in particular for customers that do high value or large numbers of online transactions, recommend commercial banking customers carry out all online banking activities from a stand-alone, hardened and completely locked down computer system from which e-mail and Web browsing are not possible.
  - Be suspicious of e-mails purporting to be from a financial institution, government department or other agency requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes and similar information. Opening file attachments or clicking on web links in

---

[c] Defense-in-Depth is a layered defense strategy that includes technical, organizational, and operational controls.

3

suspicious emails could expose the system to malicious code that could hijack their computer.
  o Install a dedicated, actively managed firewall, especially if they have a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to a network and computers.
  o Create a strong password with at least 10 characters that include a combination of mixed case letters, numbers and special characters.
  o Prohibit the use of "shared" usernames and passwords for online banking systems.
  o Use a different password for each website that is accessed.
  o Change the password a few times each year.
  o Recommend customers never share username and password information for Online Services with third-party providers.
  o Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.
  o Install commercial anti-virus and desktop firewall software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.
  o Ensure virus protection and security software are updated regularly.
  o Ensure computers are patched regularly particularly operating system and key application with security patches. It may be possible to sign up for automatic updates for the operating system and many applications.
  o Consider installing spyware detection programs.
  o Recommend clearing the browser cache before starting an Online Banking session in order to eliminate copies of web pages that have been stored on the hard drive. How the cache is cleared will depend on the browser and version. This function is generally found in the browser's preferences menu.
  o Recommend customers verify use of a secure session (https not http) in the browser for all online banking.
  o Avoid using an automatic login features that save usernames and passwords for online banking.
  o Never leave a computer unattended while using any online banking or investing service.
  o Never access bank, brokerage or other financial services information at Internet cafes, public libraries, etc. Unauthorized software may have been installed to trap account number and sign on information leaving the customer vulnerable to possible fraud.
- Recommend customers familiarize themselves with the institution's account agreement and with the customer's liability for fraud under the agreement and the Uniform Commercial Code as adopted in the jurisdiction.
- Stay in touch with other businesses to share information regarding suspected fraud activity.
- Immediately escalate any suspicious transactions to the financial institution particularly, ACH or wire transfers. There is a limited recovery window for these transactions and immediate escalation may prevent further loss by the customer..

Recommendations for Online Fraud Victims

In the event the customer is a victim of fraud, there are a number of immediate recommendations they should take to help protect their financial interests. A few general suggestions include:

- Immediately cease all activity from computer systems that may be compromised. Unplug the Ethernet or cable modem connections to isolate the system from remote access.
- Immediately contact their financial institution so that the following actions may be taken as a priority to contain the incident:
    - Online access to the accounts be disabled.
    - Online Banking passwords changed.
    - New account(s) opened as appropriate.
    - Request the financial institution's agent review all recent transactions and electronic authorizations on the account.
    - Additionally, ensure that no one has requested an address change, title change, PIN change or ordered new cards, checks or other account documents be sent to another address.
- Customers can generally find customer service or fraud prevention contact telephone numbers on monthly statements. Recommending they have this information readily available will often facilitate a call.
- Always recommend customer's suffering fraud file a police report with the local police department and provide the facts and circumstances surrounding the loss. Obtain a police report number with the date, time, department, location and officer's name taking the report or involved in the subsequent investigation. Having a police report on file will often facilitate dealing with insurance companies, banks, and other establishments that may be the recipient of fraudulent activity. The police report may initiate a law enforcement investigation into the loss with the goal of identifying, arresting and prosecuting the offender and possibly recovering losses.
- Maintain a written chronology of what happened, what was lost and the steps the customer took to report the incident to the various agencies, banks and firms impacted. Be sure to record the date, time, contact telephone number, person spoken to, and any relevant report or reference number and instructions.
- Realize that if the customer carries out personal online banking from the business computer system, there are also potential identify theft aspects to the compromise. Recommend the customer review the recommendation at the Federal Trade Commission's Identity Theft website
- Dependent on law enforcement investigative and forensic considerations, recommend the customer have their network and systems reviewed by a qualified computer forensic/information security professional.

Incident Reporting

Besides having customers report the matter to local law enforcement agencies, where online fraud is identified the FS-ISAC strongly encourage 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.

FS-ISAC member institutions are requested to report suspicious activity via anonymous submission using the FS-ISAC Cyber Incident Report. Alternatively, members may contact the FS-ISAC Security Operations Center directly at 1-888-732-2812 to obtain immediate assistance. The FS-ISAC website at http://www.fsisac.com has further contact and useful information.

Incident References

Further public reporting in relation to incidents believed associated with these matters is available below:

"*Clampi/Ligats/Ilomo Trojan: One of the largest and most professional thieving operations on the Internet*," July 29, 2009, Joe Stewart, SecureWorks, Inc.
 "*Fake Microsoft "critical update" spam propagating Trojan*," June 22, 2009, Angela Moscaritolo, SC Magazine USA
"*Fraud Update: The 13 Hottest Schemes You Need to Prevent*," May 26, 2009, Linda McGlasson, Managing Editor, Bank Info Security
"*How Hackers Snatch Real-Time Security ID Numbers*," August 20, 2009, Saul Hansell, The New York Times
"*On the Backs Of Mules: An ACH Fraud Scheme*," August 2009, Craig Priess, Bank Technology News
"*The Growing Threat to Business Banking Online*," July 20, 2009, Brian Krebs, Washington Post
"*The Clampi Trojan: The Rise of Matryoshka Malware*," July 30, 2009 Brian Krebs, Washington Post