

NACHA's Risk Management Services finds it necessary from time to time to inform your organization of events regarding ACH risk that is of time-sensitive importance.

ODFIs: Keylogging Attacks

Fraudsters May Be Looking at Your Customers For a Way Into ACH

ODFIs' customers are being attacked by malicious software in which perpetrators are increasingly using rootkits (programs designed to hide or obscure the fact that a system has been compromised) to mimic the look and feel of legitimate financial institution websites. Users provide their credentials, without knowing that it is the perpetrator behind the website.

Some of the malicious software, also known as malware, infects computers by keystroke logging or keylogging. This allows the criminal to obtain user ID and password, which leads them to information about account balances, activity and potential victim accounts. Other viruses are more robust by logging user ID and password, alerting the perpetrator when the legitimate user has provided those credentials. The perpetrator then fools the user into thinking the system is down, or not responding, when the workstation is actually sending unauthorized transactions in the user's name. Once the user's credentials are logged, the perpetrator has access and can review the account details of the business, including account activity and ACH origination parameters (such as Standard Entry Class (SEC) Codes used and file limits).

Increasingly, perpetrators are targeting the corporate accounts themselves and the malware they use allows them to look just as if they were the legitimate user - originating wire transfers and ACH batches. The perpetrator creates an ACH file with CCD debits to the corporate victim's compromised account and sends PPD credits to the new accounts opened at one or more RDFIs. In some cases, incorrect SEC Codes are used, such as a PPD entry to a corporate account. These accounts are often established for the sole purpose of laundering the funds. The entire balances are typically withdrawn shortly after receiving the money. Ninety percent or more of these funds go overseas via wire transfer or other popular money transfer services.

In addition to e-mails with links or document attachments, malware can be downloaded to users' workstations by visiting legitimate websites - especially social networking sites - and clicking on the documents, videos or photos posted there.

Some malware is capable of passively monitoring financial websites and is virtually undetectable when in this passive state.

Malware may be present, but not launch any unauthorized transactions for months. In a recent incident, the virus had been present for over a year before any unauthorized transactions were initiated.

What should an ODFI do if it has been attacked?

- Contact appropriate law enforcement immediately.
- File a Suspicious Activity Report (SAR).
- If ACH consumer-level data has been breached, notify NACHA by completing the ACH Data Breach Notification Form at <http://www.nacha.org/DataBreach>.

What should the corporate customers do to protect themselves?

Financial Institutions can do a great deal to keep their platforms secure through the use of technology solutions, and corporate customers need to operate in a secure way as well. (cont'd on Page 2)

(cont'd from Page 1)

- One of the most effective, yet basic, controls is for corporate customers to always initiate ACH and wire transfer payments under dual control. For example, one individual initiates the payment file creation and another approves the file for release.
- The combination of dual control and the use of multiple factors to prove identity is very effective in preventing an attack. Multiple factors are more challenging to compromise. For example, the use of 1) something the person *knows* (PIN, password), and 2) something the person *has* (password-generated token, USB token) could mitigate the risk of an attack substantially.
- Limit administrative rights on users' workstations. This will help to prevent the inadvertent downloading of malware or other viruses by users.
- Ensure that the corporate customer's operating system and its components are up-to-date with current software 'patches.' For example, the use of the most current firewalls, malicious code filtering, virus protection and spyware removal software will aid in the control of network intrusion tactics.
- Corporate clients should be reconciling their bank accounts daily. Many corporate clients, particularly small business clients, may not typically reconcile their bank account on a daily basis, or use treasury management services such as debit blocks or positive pay. Therefore, the entry will post and the two-day return time will have passed before the unauthorized debit is noticed.
 - Remember return time frames for CCDs (entries to corporate accounts) have a two-day return time frame for unauthorized entries. This time frame is distinct from entries to consumer accounts, such as PPDs, which have a 60-day return time frame for unauthorized.

In addition, the Federal Financial Institutions Examination Council's (FFIEC's) guidance, *Authentication in an Internet Banking Environment* (FIL-103-2005), addresses why financial institutions should conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing Internet-based financial services. Go to www.ffiec.gov for more information.

MALWARE is malicious software designed to infiltrate or damage a computer system without the owner's informed consent. The damage can be any form of a variety of hostile, intrusive, or annoying software or program code. Malware includes computer viruses, worms, trojans, most rootkits, spyware, and other malicious or unwanted software. Many trojans now have remote administration capabilities that allow the perpetrator to control the victim's computer.

ROOTKIT is a program or combination of several programs designed to hide or obscure the fact that a system has been compromised. A fraudster may use a rootkit to replace system executables, which may then be used to hide processes and files that the fraudster has installed.

SPYWARE is software that is installed surreptitiously on a computer to intercept or take partial control over the user's interaction with the computer without the user's informed consent. While the term spyware suggests software that secretly monitors the user's behavior, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information, but can also interfere with user control of the computer in other ways, such as installing additional software, or redirecting web browser activity.

TROJANS are programs that appear to have some useful purpose, but in actuality contain malicious functionality. Trojan software hides its destructive portion during installation and program execution, often preventing anti-malware from recognizing it.

NACHA Risk Management Alert

is a publication of
NACHA—The Electronic
Payments Association
13450 Sunrise Valley Drive
Suite 100
Herndon, VA 20171
Phone: 703-561-1100
Fax: 703-787-0996

Editor
Jeanette A. Fox, AAP

© 2009 National Automated
Clearing House Association
All rights reserved.