



Corporate Account Takeover

WHAT IS CORPORATE ACCOUNT TAKEOVER?

“Corporate account takeover” is when cyber-thieves gain control of a business’ bank account by stealing the business’ valid online banking credentials. Although there are several methods being employed to steal credentials, the most prevalent involves malware that infects a business’ computer workstations and laptops.

A business can become infected with malware via infected documents attached to an e-mail or a link contained within an e-mail that connects to an infected web site. In addition, malware can be downloaded to users’ workstations and laptops by visiting legitimate websites - especially social networking sites - and clicking on the documents, videos or photos posted there. This malware can also spread across a business’ internal network.

The malware installs key logging software on the computer, which allows the perpetrator to capture a user’s credentials as they are entered at the financial institution’s web site. Sophisticated versions of this malware can even capture token-generated passwords, alter the display of the financial institution’s web site to the user, and/or display a fake web page indicating that the financial institution’s web site is down. In this last case, the perpetrator can access the business’ account online without the possibility that the real user will log in to the web site.

Once installed, the malware provides the information that enables the cyber-thieves to impersonate the business in online banking sessions. To the financial institution, the credentials look just like the legitimate user. The perpetrator has access to and can review the account details of the business, including account activity and patterns, and ACH and wire transfer origination parameters (such as file size and frequency limits, and Standard Entry Class (SEC) Codes).

The cyber-thieves use the sessions to initiate funds transfers, by ACH or wire transfer, to the bank accounts of associates within the U.S. These accounts may be newly opened by accomplices or unwitting “money mules” for the express purpose of receiving and laundering these funds. The accomplices or mules withdraw the entire balances shortly after receiving the money, and then send the funds overseas via over-the-counter wire transfer or other common money transfer services.

WHY ARE SMALLER BUSINESSES AND ORGANIZATIONS TARGETED?

The cyber-thieves appear to be targeting small- to medium-sized businesses, as well as smaller government agencies and non-profits, for several reasons:

1. Many small businesses and organizations have the capability to initiate funds transfers - ACH credits and wire transfers - via online banking (individual consumers generally do not have this capability except for payees set up in online bill payment systems);
 - a. This funds transfer capability is often related to a small business’ origination of payroll payments;
 - b. In corporate account takeover, the cyber-thieves may add fictitious names to a payroll file (directed to the accounts of money mules), and/or initiate payroll payments off-cycle to avoid daily origination limits;
2. Small businesses often do not have the same level of resources as larger companies to defend their information technology systems;
3. Many small businesses do not utilize additional banking services, such as password-generating tokens, and do not monitor and reconcile their accounts on a frequent or daily basis;
4. Small businesses bank with a wide variety of financial institutions with varying degrees of IT resources and sophistication. Some financial institutions may not offer or require services that would defend against corporate account takeover.

PREVENTION, DETECTION AND REPORTING FOR BUSINESS CUSTOMERS

ACCOUNT CONTROLS

1. Reconcile all banking transactions on a daily basis.
2. Initiate ACH and wire transfer payments under dual control, with a transaction originator and a separate transaction authorizer.
3. Utilize multi-factor and multi-layer authentication, for example:
4. Something a person *knows* (user ID, PIN, password);
5. Something a person *has* (password-generating token, USB token).
6. Utilize both routine and “red-flag” reporting on transactions.
7. Immediately report any suspicious transactions to the financial institution.
8. Stay in touch with other businesses and industry sources to share information regarding suspected fraud activity.

COMPUTER SECURITY TOOLS AND PRACTICES

1. Install a dedicated, actively managed firewall. A firewall limits the potential for unauthorized access to a network and computers.
2. Install commercial anti-virus software on all computer systems.
3. Ensure virus protection and security software are updated regularly.
4. Ensure computers are patched regularly, particularly operating system and key applications, with security patches.
5. Consider installing spyware detection programs.
6. 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. If you are not certain of the source, do not click any links.
7. Create strong passwords with at least 10 characters that include a combination of mixed case letters, numbers and special characters.
8. Prohibit the use of "shared" usernames and passwords for online banking systems.
9. Use a different password for each website that is accessed.
10. Change the password several times each year.
11. Never share username and password information with third-party providers.
12. Limit administrative rights on users' workstations.
13. Carry out all online banking activities from a stand-alone computer system from which e-mail and Web browsing are not possible.
14. Verify use of a secure session ("https") in the browser for all online banking.
15. Avoid using an automatic login features that save usernames and passwords for online banking.
16. Never leave a computer unattended while using any online banking or investing service.
17. 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.
18. Clear your browser cache in order to eliminate copies of web pages that have been stored on your hard drive.

RECOMMENDATIONS FOR CORPORATE ACCOUNT TAKEOVER VICTIMS

1. Immediately cease all activity from computer systems that may be compromised. Disconnect the Ethernet or other network connections to isolate the system from remote access.
2. Immediately contact your financial institution so that the following actions may be taken:
 - a. Disable online access to accounts.
 - b. Change online banking passwords.
 - c. Open new account(s) as appropriate.
 - d. Request the financial institution's agent review all recent transactions and electronic authorizations on the account.
 - e. 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.
3. Maintain a written chronology of what happened, what was lost and the steps taken 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.
4. File a police report 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.

This document is for information purposes and is not intended to provide legal advice. The guidance included is not an exhaustive list of actions, and security threats change constantly.

Sources: NACHA (www.nacha.org) and the Financial Services – Information Sharing and Analysis Center (www.fs-isac.com)

December 2, 2009