

Organized Cyber Crime and Corporate Bank Account Takeovers

By Dave Tripier, CMO at IronKey

Over the last eighteen months, the global banking system has been faced with new huge security challenges. Both financial institutions and businesses alike have been battling the poor economy in hopes of recovering from the recession but are now faced with a new threat of thieves stealing clients' funds and affecting reputations. Through large scale phishing attacks, global cyber crime organizations have been successfully stealing millions from consumers. This usually involves many, sometimes even thousands of, low value transactions. However high tech criminal gangs are shifting focus and targeting the more lucrative corporate bank accounts of public and private sector organizations. Crimes that many estimate could tally over \$1 billion this year.

The Ponemon Institute's 2010 Business Banking Trust survey recently disclosed that 80 percent of banks did not pick up on fraud until after funds had already been transferred out of their institution. Even more distressing is that 57 percent of businesses that have faced fraud attacks did not receive full compensation for their bank's error. It's reported that small to medium sized businesses lose between \$100,000 - \$200,000 (even as high as \$3 million) during a single commercial account takeover. The following article provides an overview of how organized cyber crime rings are now targeting corporate banking transactions and provides valuable information on helping banks and businesses confront this new threat.

del.icio.us

Discuss in Forums {mos_smf_discuss:/root}

Gartner warns that the increasing attacks on online banking transactions is merely the tip of the cyber crime iceberg, as the banking industry is faced with a threat that could cripple confidence in the corporate online banking system. Without a change in direction, legislative or regulatory action could introduce more rules and security requirements for banks. Now more than ever, banking clients are in need of protection for their online accounts to stem the tide of losses, for both clients and banks, from account takeovers.

The Evolving Threat of Online Account Takeover

To penetrate a few large transfers from a handful of corporate bank accounts is far more profitable than to attempt thousands of consumer fraud attacks. As a result, cyber crime rings have changed their tactics.

Criminals are now using commercial online banking malware. Customizable Trojan frameworks, such as Zeus, can attack computers transparently. These malware attacks are undetected and are capable of defeating new multi-factor authentication systems positioned as authorized and requested by the FFIEC rules. Malware does not only steal banking authentication credentials but also performs automatic fraudulent transactions directly from a victim's personal computer. Bill Nelson, Executive Director of the FS-ISAC, states that "90 percent of his audience claimed to have experienced incidents of corporate account takeover."

Malware and Reputation

There is no doubt that the threat of criminal activity can shake clients' trust and confidence in institutions. The Ponemon Institute study revealed that 40 percent of businesses move their banking activities elsewhere after a fraud incident. The study also found that 11 percent of firms that have experienced fraud claimed that they have terminated their banking relationship following the attacks. An additional 29 per cent said that they did not fully terminate their relationship but moved their primary cash management services to another institution.

Negative publicity is damaging enough, but banks are also now facing lawsuits from clients. Unrecovered funds or failed reimbursement from an institution leads to clients suing banks for inadequate and lack of security. The Electronic Funds Act (EFT) of 1978, or Regulation E, does cover losses for retail banking but does not protect commercial banking.

Institutions can only withstand so much, before their clients lose confidence as well as trust and create irreplaceable damage. After the global banking crisis of 2009, financial institutions cannot afford more damage.

NACHA and FBI Guidelines for Safe Banking

To address this mounting threat, NACHA, the Electronic Payments Association, and the FBI developed guidelines to help protect banking clients from financial malware. Core to these recommendations is reducing the opportunity for financial malware to infect client computers. NACHA and FBI recommendations can be summarized by five guidelines:

- Dedicated computer: Use a dedicated computer
- Banking only: Only perform banking transactions—do not use email, office applications, or visit non-banking websites
- Malware protection: Protect the computer with anti-malware software

- Automatic updates: Keep the computer update with the latest software updates

- Strong authentication: Use strong, two-factor authentication for gaining access to bank accounts according to FFIEC rules

These guidelines are an important step in moving to a safer online banking environment. Virtually all of the known account takeovers due to financial malware could have been avoided with this approach.

Implementing NACHA and FBI Guidelines

At first, the guidelines for safe banking from the NACHA and FBI may seem unrealistic. Bank clients expect the convenience of online banking without having to buy and use a separate, dedicated computer. Instead, banks can use new technology to create the environment for safe banking put forward by NACHA and FBI.

Technologies that will help institutions protect their clients include:

- 1) A secure environment that's tamper-proof, portable, and easy to use for all types of commercial banking clients
- 2) A secure web browser that isolates banking sessions from the rest of the computer to prevent malware from taking control
- 3) Two-factor authentication to increase the assurance that the user is authorized to access online commercial banking
- 4) Anti-malware to scan the user's computer before launching a secure environment to eliminate as many possible threats as possible
- 5) Automatic updates to keep systems updated with the latest threat protection
- 6) Analytics to provide updates on client usage and the threats observed to drive anti-fraud and risk management decisions

Self-Defense

Institutions need to begin taking advantage of the guidelines created by NACHA and the FBI to defend against cyber criminal attacks. Criminals have just begun focusing on commercial online banking and, over time, their attacks will continue to become more sophisticated and developed.

The technology solutions that combine virtualization, portable security devices, and analytics currently are marketed towards banks to protect their clients and business relationships. Banks adopting these measures will be prepared to safely secure and defend their clients' business while avoiding the financial attack of this money hungry threat.

Follow-Up Questions from the Editor

1) Do you feel that PCI, HIPAA, SOX or compliance with any other gov't regulations are actually stemming the tide of cyber attacks?

There's no doubt that government and industry regulation play a part in helping to reduce the impact of cyber attacks and fraud. For example, many readers of The Ethical Hacker Network are likely involved in PCI DSS compliance scans and penetration tests. Compliance programs help raise organizational awareness and attention. However, regulatory compliance is not a substitute for a security strategy. Only by taking the offensive against cyber crime and proactively protect systems, data, and users will profits from cyber attacks be reduced and in turn help stem the tide of cyber attacks.

With one metric, cyber fraud from commercial banking fraud skyrocketing past \$1 billion this year, it's clear there is still a lot of work to do.

2) Are there any specific technologies (WAFs, white-listing, email spam prevention services, etc.) that you feel would be helpful, are underutilized or just flat out useless?

Preventing cyber crime requires a multi-layered offensive approach. There's no single silver bullet. Putting all your cyber crime fighting eggs in just one basket is a quick ticket to disaster.

For online banking fraud, institutions need to combine analytics and authentication technologies used today with new technology to protect the client computing environments. Increasingly, it's not the bank infrastructure that's under attack but the client computers of small and medium businesses. 90 percent of banks belonging to FS-ISAC (Financial Services - Information Sharing and Analysis Center) have already encountered online account takeovers initiated from their

clients' PCs.

With over 70,000 new Zeus malware variants being detected each year (and growing), it's impossible for bank clients to keep up. Instead by isolating the online banking environment and locking it down within a virtualized, write-protected environment, banks can keep financial malware from embedding itself in web browsers and performing fraudulent transactions.

3) Since many of our readers are penetration testers, do you feel as if taking an offensive look at one's own security is an effective way of finding and eventually plugging holes in organizations systems and processes?

Taking the offensive and actively looking for weaknesses is most certainly part of an effective security program to combat cyber crime. Security through obscurity, or even worse ignorance, is no longer an option. Active penetration testing is something that IronKey believes strongly in. We engage in ongoing penetration testing of our products and services. There's no doubt this improves our customer experience, and it's something we recommend all of our clients engage in too.

About the Author

Dave Tripier is CMO at IronKey, a leading provider of secure and managed portable computing solutions. Tripier is an 18-year security industry veteran. He holds a B.S. in engineering from Drexel University and performed his graduate work at the LeBow College of Business and Executive Education from the Harvard Business School.