

Major Financial Services Firms Call Online Banking Dangerous

Avivah Litan, Richard Hunter

FS ISAC has warned its members that online business banking is not safe. Its alert highlights the lack of regulatory protections for business accounts and the danger posed by sophisticated criminal hacking capabilities.

NEWS ANALYSIS

Event

On 24 August 2009, the Washington Post's Security Fix blog reported that the Financial Services Information Sharing and Analysis Center (FS ISAC) — an industry group created by a U.S. presidential order to share data about critical threats to the financial sector — had issued a confidential alert to its members, which include the Federal Reserve, the New York Stock Exchange, Citigroup, Morgan Stanley and Goldman Sachs. The FS ISAC alert urged business bank customers to "carry out all online banking activity from a stand-alone, hardened, and locked-down computer from which e-mail and Web browsing is not possible." The FS ISAC issued its alert in response to reports from financial institutions, security companies, the media and law enforcement agencies of "a significant increase in funds transfer fraud involving the exploitation of valid banking credentials belonging to small and medium sized businesses."

Analysis

The FS-ISAC warning calls into question the safety of online banking for business account holders, and confirms that criminals are winning the cyber war against financial institution account holders.

Criminals frequently target business bank accounts that cash managers handle on behalf of small businesses, school districts, county governments and other similar organizations. Criminals raid these accounts for millions of dollars (no estimates are available for the total amount of money stolen, but Gartner believes it could be very large) by planting trojans on user desktops to steal account credentials and transfer money to criminals' accounts. Especially problematic aspects of these incidents include:

- Lack of disclosure by banks to shareholders and account holders, who must learn about these incidents from media reports
- Criminals' practice of targeting business accounts, which are typically larger but enjoy less protection under the law than consumer accounts.
- Lack of protection afforded by current antivirus and anti-malware software running on users' PCs, and users' failure to keep their protection software updated.
- Criminals' ability to circumvent strong user authentication, which includes using dedicated one-time password tokens issued by the bank to business users.
- The new level of sophistication in reconnaissance, asset acquisition and exploitation demonstrated by these attacks, raising the possibility that ex-intelligence, paramilitary and military personnel are working with traditional organized crime groups.

These multistage attacks do more harm to customers than large, well-publicized credit card breaches. When cards are stolen, regulations typically require reimbursement of customers for unauthorized charges. In money transfer attacks, business users are unlikely to recover the bulk of their stolen funds.

RECOMMENDATIONS

Financial services companies and other firms with accounts that are subject to criminal takeover:

- Use a three-pronged, layered security approach that includes strong user authentication, fraud detection and out-of-band transaction verification. Don't rely solely on the strength of user authentication if the authentication is communicated through a PC browser.
- Consider offering your customers on-demand desktop and session protection tools that safeguard the user's session by creating a virtual locked environment that will not allow malware or viruses to touch that session, even if malware has been installed on the PC. A few banks have successfully used such tools to stop trojans from inflicting damage on enrolled users. Products that provide, in part, anti-malware protection include Trusteer, Verdasys and Prevyx. Also consider implementing a locked-down browser offered by a company such as Authentium.

RECOMMENDED READING

- "Childhood Ends: The Signs Are Clearer" —The path to regulation of IT products and services is unfolding on schedule, as Gartner predicted in mid-2006. **By Richard Hunter and others**
- "Magic Quadrant for Web Fraud Detection" — In a weakened global economy, the increase in cyberattacks is driving high sales growth rates for Web fraud detection vendors. **By Avivah Litan**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509