In the news - THE WALL STREET JOURNAL – December 2009

FBI Probes Hack at Citibank. Russian Cyber Gang Suspected of Stealing Tens of Millions; Bank Denies Breach

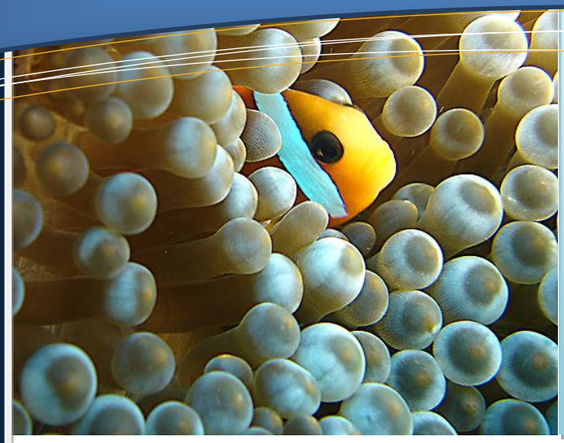
The Federal Bureau of Investigation is probing a computer-security breach targeting Citigroup Inc. that resulted in a theft of tens of millions of dollars by computer hackers who appear linked to a Russian cyber gang, according to government officials. The attack took aim at Citigroup's Citibank subsidiary, which includes its North American retail bank and other businesses. It couldn't be learned whether the thieves gained access to Citibank's systems directly or through third parties. The attack underscores the blurring of lines between criminal and national-security threats in cyber space. Hackers also assaulted two other entities, at least one of them a U.S. government agency, said people familiar with the attack on Citibank. The Citibank attack was detected over the summer, but investigators are looking into the possibility the attack may have occurred months or even a year earlier.

The FBI and the National Security Agency, along with the Department of Homeland Security and Citigroup, swapped information to counter the attack, according to a person familiar with the case. Press offices of the federal agencies declined to comment. Joe Petro, managing director of Citigroup's Security and Investigative services, said, "We had no breach of the system and there were no losses, no customer losses, no bank losses." He added later: "Any allegation that the FBI is working a case at Citigroup involving tens of millions of losses is just not true." Citigroup is currently 27%-owned by the federal government. The threat was initially detected by U.S. investigators who saw suspicious traffic coming from Internet addresses that had been used by the Russian Business Network, a Russian gang that has sold hacking tools and software for accessing U.S. government systems. The group went silent two years ago, but security experts say its alumni have re-emerged in smaller attack groups. Security officials worry that, beyond stealing money, hackers could try to manipulate or destroy data, wreaking havoc on the banking system. When intruders get into one bank, officials say, they may be able to blaze a trail into others. Last month, a federal indictment in Atlanta named eight alleged Russian and Eastern European hackers, most still at large, who prosecutors say broke into a U.S. unit of Royal Bank of Scotland in 2008 and stole $9 million from ATMs in 280 cities world-wide in a matter of hours. RBS cooperated with investigators and ensured that its customers were reimbursed. Losses to online crime of all types exceeded $260 million in the U.S. last year, the FBI estimates. Attacks on corporations are "at an epidemic level," former White House cyber-security director Melissa Hathaway said recently. U.S. banks have generally been loath to disclose computer attacks for fear of scaring off customers. In part this is an outgrowth of an experience Citibank had in 1994, when it revealed that a Russian hacker had stolen more than $10 million from customer accounts. Competitors swooped in to try to steal the bank's largest depositors. Citibank said at the time that it was able to recover most of the money and that the attack didn't put customer funds at risk.

The new attack targeting Citibank highlights the growing sophistication and threat posed by overseas criminal networks. "There were a couple of days of struggling," said one person familiar with the attack. "There were some sophisticated elements that made it hard to block." Among weapons the hackers used, according to people familiar with the case, was a small army of infected computers commanded by software called Black Energy. Hackers use Black Energy primarily to block access to Web sites. Somebody used it during Russia's brief 2008 war with Georgia to shut down Georgian government and bank Web sites. Someone also used it in 2007 to block government and bank Web sites in Estonia and to attack the Web site of a political foe of Vladimir Putin, then Russia's president and now its prime minister. Black Energy was written by a Russian hacker who goes by the name Cr4sh, said Joe Stewart, a researcher for SecureWorks, a computer-security company. The software sells online for $40, according to Jose Nazario, a manager at Arbor Networks, which analyzes computer threats. Black Energy can be upgraded to invade computer systems and snatch data. DigitalStakeout, a firm that monitors cyber attacks, found in April that Black Energy was being used with a tool that steals bank-account log-on information. The combination was being sold online for $700 as a package called the YES Exploit System, said DigitalStakeout's chief executive, Adam Mikrut. Over the summer, Mr. Stewart said, he discovered that Cr4sh had developed a new version of Black Energy with an added feature that steals banking credentials. In the Citi attack, the software included a tailor-made feature designed to attack the bank, according to two people familiar with the incursion. The thieves stole an estimated ten of millions of dollars, according to three people familiar with the matter. It remains under investigation, and whether any of the money has been recovered couldn't be learned. The migration of payments to the Internet, in combination with new bank systems that settle transactions the same day, "has enabled bank heists to occur in seconds from thousands of miles away," said Tom Kellermann, a former World Bank cyber-security official and now an executive at Core Security Technologies. Robert Blanchard, co-owner of Bridge Metal Industries, a lighting company in Mount Vernon, N.Y., can attest to that. At 3 a.m. on July 6, Mr. Blanchard tried to log on to his company's Citibank account but couldn't do so with his regular password and token code. He says he called Citibank and was told it would change his password and send him a new one by overnight mail. "I thought at that point I was safe," he says. But he still couldn't get in. By the time he called his local bank branch to sort out the problem, he says, online thieves had sent $1,007,655 to banks in Latvia and Ukraine. "Even the bank can't act as quickly as these guys," Mr. Blanchard says. It isn't clear whether the incident was part of the larger attack on Citibank. Investigators discovered that a computer at Mr. Blanchard's lighting company had been infected by a computer at another company he co-owns. That one then dragooned his lighting-company computer into a group of computers used to attack others -- the same modus operandi as Black Energy's. The software loaded on one of Mr. Blanchard's computers included a spyware program that logged the keystrokes he typed and could capture the data he used to sign on to his bank account, he says. He adds that after days of prodding, Citibank sleuths began working to help him recover $810,855 from the Latvian bank, and Citibank then gave him the remainder. Asked about the Blanchard case, Citigroup said: "While we do not discuss customer details, the individual case described was an isolated incident of fraud. Consistent with legal requirements, our customers are not liable for any unauthorized use of their accounts."

BROCHURE ON BIOMETRIC AUTHENTICATION OVER THE CLOUD

Sign-in With Your Fingertip



BioSign™

Useful User's Authentication Principles You Should Remember

The organization security team must defend all critical and valuable points internally and externally and in particular web sites, web-access points and web databases.

The attacker can choose the weakest point only.

Text-passwords are commonly the weakest point in the chains of IT security.

Secured text-passwords become cumbersome, too difficult to remember by users and expensive to organizations.

Biometrics proves to be much secured than any text-password.

Physical biometrics provides an answer to the real world of public facilities. It cannot provide the required answer for the virtual world.

Behavioral and dynamic biometrics provides the optimal answer for the virtual world of IT security, Internet and cloud computing.

The organization security team must play by the rules.

The attacker can play dirty.

The attacker can strike at will while someone is"sleeping".

Protect your web site against phishing attacks

The Problem:

Text-passwords prove to be insecure; passwords can be easily stolen by any novice hacker, exposing you to financial losses and fraud and then what? Claiming "it wasn't me... I want my money back" like many other victims. The situation of claiming "it wasn't me… I want my money back", is unforgettable to many victims that found themselves, helpless and vulnerable. What about your membership in social networks such as: Facebook, Myspace and others? Is it secured enough or it is still protected by text-passwords?

What about the potential of losing your private data and passwords over the web, publicly exposing your confidential inbox, outbox, sent mails and more to every user over the net including your family secrets re: Sara Palin incidence. You may find more information about this incident; Sarah Palin's e-mail hacked by anonymous at:

http://stupidcelebrities.net/2008/09/17/palins-email-hacked-by-anonymous-pics/ .

Massive identity theft attack, probably conducted by Phishing attack happened on Oct 5th 2009 where "Thousands of accounts on web-based e-mail system Hotmail have been compromised" software giant Microsoft has confirmed." For more details please visit: http://news.bbc.co.uk/2/hi/8291268.stm or at:

List of 20,000 More Email Accounts From Gmail, Hotmail, Yahoo, AOL And Others Posted Online.

http://cyberinsecure.com/list-of-20000-more-email-

ANB's BioSignID solution:

ANB challenges the vulnerability and the limitation of text-passwords while addressing the latest critical and harmful cyber threats such as: SSL-Strip, SSL-Sniff and Chain Certificates attack.

BioSignID offers behavioral biometric identities that are optimal for the virtual world of Internet, IT systems and cloud computing. Unlike typical authentication technologies, users don't have to remember endless passwords nor periodically change their web account's password in every different web site and/or IT system. **BioSignID** web service eliminates your web site vulnerability to phishing attacks by implementing a parallel communication channel to your mobile touch screen device. **BioSignID** protects your web identity from being stolen by Identity theft activities such as SSL-Strip, SSL-Sniff and Chain-Certificate attack. **BioSignID** improves your privacy over the web and secures your web access to your web accounts over the web. **BioSignID** Authentication web service was designed for the cloud computing environment.

How BioSignID works?

Two or three authentication factors

The BioSignID authentication web service is based on authenticating biometric identities instead of text-passwords. Each BioSignID identity is unique and represents the following authentication factors:

- Something you know (your abstract signature/ your initial)
- Something you are (the way you sign-in – your personal biometric features)
- Something you have (Optional) – BioSignID for Mobiles includes your device ID and SIM card.

The BioSignID three factors authentication web service offers the highest security level. For comparison, text-password represents only the factor of something you know.

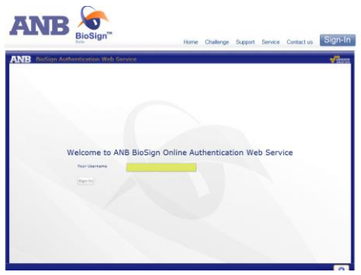
BioSignID for the cloud computing environment

ANB offers the BioSignID authentication web service for the Amazon's EC2 cloud via Amazon AWS (Amazon Web Services). For more information please visit the following URL at:
http://developer.amazonwebservices.com/connect/entry.jspa?externalID=3187

While offering the BioSignID web service in Amazon AWS, ANB launched www.biosignid.com web site (currently in beta stage) in order to build the first group of BioSignID users in the Internet environment and demonstrate how the BioSignID service can be replicated and work in private clouds.

How BioSignID authentication web service works?

Whenever the user would like to login to web site that is being protected by BioSignID web service or to web site that supports the Open-ID standard, the protected web site is browsed using one of the following Internet web browsers: Microsoft IE 6.xx/7.xx/8.xx, Apple Safari 3.xx/4.xx Firefox 2.xx/3.xx and Google Chrome. When the user clicks on the Sign-in button, a new session is established with the BioSignID server opening the BioSignID Virtual-Pad as illustrated here.



In the BioSignID Virtual-Pad page, a Microsoft Silverlight client-based application is installed on the spot enabling hardcoded endpoint-to-endpoint secured channel using SSL 128bits key encryption.

The user types his unique username (for Open-ID the system uses the user's unique Open-ID universal username) and then the Virtual-Pad signing surface is displayed waiting for the user to sign-in his biometric signature (abstract signature or his initials signature) as demonstrated in the following figure.

The BioSignID three factors authentication web service offers the highest level security model.

The user signs and then his signature is sent for verification at the BioSignID authentication server. Upon a successful verification, a unique security token is generated for the user's active cookie. For the Open-ID web site, the user browser is redirected back to the waiting session as a logged user as described in the Open-ID protocol. For more information about the Open-ID protocol, please visit the following
http://openid.net/get-an-openid/what-is-openid/

In general the Open-ID is a world leading standard for web authentication that support SSO (Single0Sign-On) where each user can have a unique and universal username for accessing third party web site that works with Open-ID provider such ANB BioSignID. Among the leading web sites you can find:

- ✓ www.facebook.com
- ✓ www.livejournal.com
- ✓ www.wordpress.com
- ✓ www.politicalmarket.cnn.com
- ✓ www.mysears.com
- ✓ www.stackoverflow.com

ANB | Security as it should be

JOIN BioSignID NOW

Visit us at: www.biosignid.com

ANB installed BioSignID authentication web service in Amazon Cloud EC2. The BioSignID is now in Beta stage in order to demonstrate its proof on concept and unique benefits in challenging anti-phishing and identity theft threats. Please don't hesitate to use ANB's BioSignID trail online version at: www.BioSiginID.com The BioSignID authentication web service is now free. You can login to your Facebook account and/or many other web sites that support the Open-ID authentication standard.

Installation

The BioSignID authentication web service can be installed in a dedicated server or in a servers cluster in order to ensure high availability with high performance to millions of users. The ANB's BioSignID solution is based on Microsoft .NET 3.5 framework, the database is installed on Microsoft SQL 2005 and the web service runs on Microsoft IIS 7. The thin client software is automatically installed in each end-user web browser using the only pre-requirement item, Microsoft Silverlight 3.5 framework. There is no need for special software distribution service or automatic versioning system.

For any further technical materials and/or additional information, please visit the BioSignID FAQ page at: http://www.biosignid.com/HelpPages/FAQ.aspx

For order and pricing information please contact ANB marketing team at one of the following ANB's offices:

ANB | Security as it should be.

HQ Office
37 Upper Brook Street
London
United Kingdom
W1K 7PR

Ph + 44 (0)20 7495 2726 Fax + 44 (0)20 7495 7775
www.anbsys.com info@anbsys.com

ANB | Security as it should be.

RnD Lab
Industrial Park,
P.O.Box 3762,
Kefar Netter,
Israel 40593

Ph +972.(0)9.885.5215 Fax +972.(0)9.865.5620
www.anbsys.com support@anbsys.com

Microsoft CERTIFIED Partner | intel Intel® Product Integrator | IBM World Partner | Ready for IBM Tivoli software | Yael Software

Important Tips!

There are many excellent sources and web sites that publish security news on daily basis. The following are a few of the more authoritative and popular ones:

Computer Emergency Response Team (CERT): www.cert.org
SANS Institute: www.sans.org
Internet Storm Center: www.incidents.org
Security Focus: www.securityfocus.com
The Register: www.theregister.com