Networking: Is that bank's URL legitimate?

May 1 2006

Computer-security professionals at the weekend were working on what is being described as a just-emerging IT problem -- the kind which, if the pros are correct, potentially could imperil all e-commerce across the globe. Hackers have apparently compromised the computer server of a Russian bank and set up a fake subsite to "phish" for credit-card information and other personal financial details, experts tell UPI's Networking.

This is a new kind of phishing scam, as computer criminals usually set up sites that simply look and feel similar to the site they are attacking. But in this instance, the phishers replicated the Moscow-based KS Bank

site itself, www.ks-bank.ru, and not just an image of it, and created a page that used its exact URL, a subsite of that URL, www.ks-bank.ru/.x/hvfcu. This new tactic raises a horrid specter for online banking consumers -- the grinding fear of whether one's e-commerce site is what it purports to be or is actually a criminal enterprise.

"This appears to be a phishing page hosted on the domain of a legitimate Russian bank," a spokesman for Cyveillance, an Arlington, Va.-based IT security firm that works with Fortune 500 firms, told Networking. "Could be a compromised server. Could be the bank's IT department employees."

Whatever the case may be, as of Monday morning the legitimate bank's site was off the Internet, and the fake subsite was as well. "The attacked credit union appealed to Cyveillance to take the phishing site down off the Internet," said the spokesman.

Experts said that the Bank of Russia confirmed that the KS Bank was housed at the address listed on its home page -- and had been in business since 1992 and was not entirely a figment of the imagination of the criminal hacking underworld.

What is more, Cyveillance notes that the "domain dossier" at CentralOps.net indicates that the KS Bank URL has been registered to the bank for some time; and a Google search found 145 pages of archives for the bank, dating back for years.

One of the more aggressive tactics used by cyber-sleuths is to work with Internet service providers and take down the phishing site as soon as possible. New technology -- like the Application-Level Behavior Blocking software by Finjan software -- is supposed to help companies keep ahead of the crooks, and stay online, even during an attack, a spokesman told Networking.

According to Lucinda Borovick, director of data-center networks for market-research firm IDC, there is an increasing market demand for products that control Web communications. "The secure content and application delivery market is a key component as customers begin to build an application aware network," she said.

The phishing attack on the Russian bank started like all phishing attacks do -- by e-mail sent over the unregulated Internet.

"Most of the bad things that happen on the Internet happen over e-mail," Tom Gillis, senior vice president of marketing and sales at IronPort, a San Francisco-based IT security firm that works with the White House and the U.S. Navy, told Networking. "Fraud and spam are rampant on e-mail. Even spyware is propagating by e-mail, with a 200 percent increase in e-mail bourne spyware in the last six months."

Experts at New York City-based MessageLabs, a provider of messaging security software, said that very targeted attack trend by phishers started in 2005. Overall, there was a decrease in the number of phishing attacks last month -- by 0.5 percent. But phishing attacks constitute 15.6 percent of all e-mail sent online. A new tactic, called spear-phishing, is expected to climb in usage in the coming months, MessageLabs reports in its April survey, released last Thursday to national reporters. "We're continuing to see it gain momentum and also increase in sophistication," said Mark Sunner, chief technology officer of MessageLabs. "Cyber criminals are becoming more adept at drawing less attention to themselves by sending out highly targeted virus and phishing attacks in smaller numbers, running smaller botnets and ultimately finding new ways to make money from victims around the world."