

ID theft monitor draws RSA conferees

Deborah Gage, Chronicle Staff Writer

Friday, April 11, 2008



On a flat-screen television monitor in the basement of Moscone Center in San Francisco, thieves are buying and selling stolen identities.

To the right of the screen is a list of the hackers' nicknames - Bitzers, Blacknet, Block13 and so on. On the left are the offers of the personal information they're selling: "SSN DOB USA 4\$ BEST PRICE."

"He's guaranteed to be a victim of identity theft," said Tim Lukens, a vice president at Affinion Group, as he watched a sample name, phone number, e-mail and mother's maiden name of one unfortunate man scroll by. "He just doesn't know it yet."

The screen was capturing a live recording of an Internet Relay Chat channel, an Internet-enabled conference call where data thieves often congregate. These particular thieves were outside the country, Lukens said - "beyond the reach of U.S. law enforcement."

At the annual RSA Conference in San Francisco this week, one of the largest gatherings of security professionals in the world, the mood was sober, as the security industry struggles to figure out how to halt the rising tide of Internet crime. Although prices for stolen credit cards have been dropping due to intense competition, according to Internet security vendor Symantec, it's still a multimillion-dollar industry.

The good guys have a lot of information about how the bad guys operate, and they're sharing more and more of it.

Security consultant Ira Winkler on Tuesday demonstrated how he hacked into a power plant last year at the request of the plant's managers, who were sure it couldn't be penetrated. His audience included employees of the Department of Defense.

The plant's owners made a mistake, he said, when they tried to save money by using the same computers to control the plant that they used to run their business.

Employee access to e-mail on those computers left the plant's network open to the Internet, and all Winkler had to do was send employees an e-mail and fool them into clicking on a link, which led them to a Web site that planted malicious software code, called malware, on their computers. The attack was so successful that after a couple of hours, the plant asked to have it stopped.

"There's a major storm brewing," Winkler told his audience. "We have a weak infrastructure. We talk a lot, but there's little action."

In the next room, Ben Jun of Cryptography Research was demonstrating how to hack into iPods and other

consumer electronics.

Earlier in the day, a session on new Internet attacks held by SANS, a group of security researchers in Bethesda, Md., was so full that people were turned away.

Data thieves are growing more adept, said several people at the conference, and the tools to fight them aren't all there.

Internet service providers try to block spam, but their margins are so thin they can't afford to do as much as they should, said Joe St. Sauver, who manages Internet2 security programs at the University of Oregon. For example, some credit card companies unwittingly allow their cards to be accepted at spammer Web sites that sell goods to criminals.

Cybercrime is global, yet law enforcement agencies are bound by the geography they serve, and people whose computers get infected and taken over by hackers have nowhere to call.

St. Sauver said there are worldwide networks of compromised computers, many of them home PCs that hackers have taken over remotely. "And nobody is calling their congressman or senator and complaining when they get spam."

Some progress is being made. Greg Garcia, assistant secretary for cybersecurity at the Department of Homeland Security, pledged Wednesday to clean up federal computers as an example to the private sector, which controls most of the Internet. He also promised to share technology the government has developed that searches out vulnerabilities.

Microsoft doesn't have all the answers, said Craig Mundie, Microsoft's chief research and strategy officer. At a keynote on Tuesday he asked for a dialogue on how Microsoft can secure its products and protect privacy. The company has created a Web site for the discussion, which it calls End to End Trust.

Howard Schmidt, a former chief security officer for Microsoft who went on to advise the White House, said Europeans are watching and learning from Americans' mistakes in rushing out new technology products without considering security and privacy.

Schmidt is also affiliated with SCIPP International, a nonprofit whose founder, Winn Schwartau, proposes creating a cybercorps of teenagers, a sort of Neighborhood Watch program for the Internet.

Schwartau has founded several companies and is an expert on cyberwar. He's been studying it off and on since before 1991, when he warned Congress about the possibility of a "digital Pearl Harbor."

Sixty percent of all security breaches stem from basic mistakes made by computer users, he said, but where are they supposed to go when they have a problem? Computers - like cars - are machines, yet, he said, "You need a license to drive a car."

As for the man whose identity was probably stolen during the earlier demonstration, the Affinion Group doesn't plan to call him. It sells its chat room monitoring service to banks.

"We used to call everybody so we could sleep better at night, but we don't have the resources anymore," said

Dan Clements, the president of CardCops, which developed the monitoring technology and was acquired by Affinion last year. "We can't call thousands of people."

E-mail Deborah Gage at dgage@sfchronicle.com.

<http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/04/11/BUTQ102MFM.DTL>

This article appeared on page **C - 1** of the San Francisco Chronicle