Security Software Company Discovers Possible ID-Theft Ring

By *srlinuxx*
Created *06/08/2005 - 2:17pm*
Submitted by srlinuxx on Saturday 6th of August 2005 02:17:39 PM Filed under Security [1]

A Florida security software company says it has stumbled across what may be a major identity-theft effort.

Sunbelt Software Inc., which makes software used to protect computers from spyware, says it has discovered a server holding passwords and other personal information that may have been illegally collected using keylogging software.

"One of our researchers here, while doing some research for our anti-spyware tool, came across a server that happened to have a file on it that turns out to be a log file from a keylogger that's been deployed, it looks like, all over the world," David Bove, Sunbelt's director of spyware research, said in an interview.

Bove wouldn't provide more details about how the server was found or where it's located. Sunbelt has contacted the FBI about the discovery, he says. The FBI didn't immediately return calls seeking comment.

Keyloggers, whether hardware- or software-based, are used to capture information typed into computers, typically without the knowledge of the computer user. Used by law enforcement, they're a valuable tool for obtaining passwords criminals use to encrypt incriminating information. Used by criminals, they're a valuable tool for emptying online bank accounts and perpetrating identity-theft fraud. Keylogging software is usually distributed through Trojan software, worms, or viruses.

In July 2003, Juju Jiang pleaded guilty in federal court to computer fraud charges for using a keylogging program called Invisible KeyLogger Stealth at a number of Kinko's locations in Manhattan. In March, the British Hi-Tech Crime Unit foiled an attempt to steal some $420 million from a London branch of Japanese bank Sumitomo Mitsui. The thieves reportedly hacked the bank's systems through information obtained from a keylogger.

Bove says the log file contains user IDs, passwords, and associated URLs, along with IM chat logs that have been captured and transmitted over the Internet by the keylogger. Whoever is responsible has been periodically harvesting the suspected stolen data and resetting the file size, he says. When the file was discovered a week ago, it had 22 Mbytes of data. It currently has 4 Mbytes and is growing at a rate of 200 Kbytes per hour, Bove says.

Sunbelt president Alex Eckelberry brought the discovery to light through a Sunbelt blog posting. "We're sitting upon literally thousands of pages of stolen identities that are being used right now," Eckelberry wrote Friday afternoon.

"There is a LOT of bank information in here, including one company bank account with over US$350,000 and another small company in California with over $11,000 readily accessible," Eckelberry wrote. "This list goes on and on and

on."

"We were trying to figure out if this was real or not," Bove says. "And we actually logged into those accounts. That's how we knew how much money was in there. Then we immediately attempted to contact the individuals to let them know."

By Thomas Claburn
InformationWeek

Security
