To print: **Click here** *or* Select **File** and then **Print** from your browser's menu

---
This story was printed from ZDNet News,
located at http://news.zdnet.com

By Ingrid Marson
URL: http://news.zdnet.com/2100-1009_22-5823591.html

A major identity theft ring has been discovered that affects up to 50 banks, according to Sunbelt Software, the security company that says it uncovered the operation.

The operation, which is being investigated by the FBI, is gathering personal data from "thousands of machines" using keystroke-logging software, Sunbelt said Monday. The data collected includes credit card details, Social Security numbers, usernames, passwords, instant-messaging chat sessions and search terms. Some of that data is then saved in a file hosted on a U.S.-based server that has an offshore-registered domain, according to Sunbelt.

In the two days that Sunbelt has been monitoring the file, the company has seen confidential financial details of customers of up to 50 international banks, said Eric Sites, vice president of research and development at the Clearwater, Fla.-based security software maker.

"For almost every bank that is listed (in the file), it's possible to get into the person's account," Sites said.

Along with passwords for online banking sites, information on credit cards also has been gathered. Sites said that Sunbelt had found one customer's credit card number, expiration date and security code, in addition to name and address. That information would allow anyone to use the credit card, he said.

"The types of data in this file are pretty sickening to watch," Sunbelt President Alex Eckelberry wrote in a blog posting dated Saturday. "In a number of cases, we were so disturbed by what we saw that we contacted individuals who were in direct jeopardy of losing a considerable amount of money."

Sunbelt said that the people behind the scheme have obtained access to a considerable amount of bank information, including details about one company account containing more than $380,000 and another account that has "readily accessible" funds of more than $11,000.

An FBI representative was unable to confirm whether or not an investigation was taking place.

The data theft is carried out by a Trojan horse downloaded at the same time as CoolWebSearch and a mail zombie, Sunbelt said. Patrick Jordan, a Sunbelt

employee, discovered the identity theft ring while researching a variant of CWS, which is a malicious program that hijacks Web searches and disables security settings in Microsoft's Internet Explorer Web browser.

"During the course of infecting a machine, he (Jordan) discovered that a) the machine he was testing became a spam zombie and b) he noticed a call back to a remote server. He traced back the remote server and found an incredibly sophisticated criminal identity theft ring," Eckelberry wrote in the blog posting. "We are still trying to ascertain whether or not this is directly related to CWS."

The malicious code is hosted on a Web site that mainly hosts pornography, which Sites was unwilling to name. Users of Windows XP who have not installed Service Pack 2 are particularly vulnerable, as the code could be automatically downloaded without the user's knowledge, Sites said. Sunbelt is currently investigating whether users of earlier Windows versions, such as Windows 2000 and Windows ME, are also vulnerable.

"If you have an unpatched Windows machine, when you go to the URL it will automatically download everything from the Web site, including the Trojan. All you have to do is type in the URL and you're hosed," Sites said.

The Trojan is a new variant, so antivirus and anti-spyware vendors do not yet block it, Sites said. Sunbelt plans to send information on the Trojan to security companies as soon as possible.

The activity could be the latest attempt by a criminal gang to use spyware for financial gain. In March of this year, Britain's National Hi-Tech Crime Unit foiled an attempt to steal about $390 million from the Japanese bank Sumitomo Mitsui. In that case, keyloggers were used to relay passwords and access information to the criminals who intended to transfer the funds electronically. A man in Israel was arrested after allegedly trying to transfer $25 million of the funds.

"We are aware of (Sunbelt's claims) that personal information was captured. But we can't confirm it until we can take a look at it," said an eBay spokesman. "If it is the case, we will act accordingly and appropriately."

eBay owns online payment service PayPal.

Ingrid Marson of ZDNet UK reported from London. CNET News.com's Dawn Kawamoto contributed to this report.