

[Print](#) | [Close this window](#)

Web firm sounds alert on criminal data trove

Tue May 6, 2008 1:38pm EDT

By Mark Trevelyan, Security Correspondent

LONDON (Reuters) - A Web security firm said on Tuesday it had tipped off international banks and police after finding a huge trove of stolen business and personal data amassed on a server in the space of just three weeks.

Finjan Inc said it had notified the U.S. Federal Bureau of Investigation, police in various countries and more than 40 financial institutions in the United States, Europe and India about the discovery of the so-called "crimeserver".

"This server was running for about three weeks and within this period it managed to collect 1.4 gigabytes of data. It is indeed the largest treasure we've found in this very short time," Yuval Ben-Itzhak, chief technology officer of the California-based firm, said in a phone interview from Israel.

The stolen data consisted of 5,388 unique log files including 1,037 from Turkey, 621 from Germany, 571 from the United States, 322 from France, 308 from India and 232 from Britain.

It included company personnel files, insurance details, social security numbers, medical records, credit card details and exchanges of confidential business email, in one case including details of a pending court case.

Ben-Itzhak said it was striking that the crimeserver itself was not security-protected, meaning anyone could potentially have accessed it over the Internet.

"The server was not secure at all. It indicates that these people that are doing the crime today, they are not security experts, they are not computer science experts.

"They are people who are buying the crime toolkits ... software packages that hackers, the smart people, are selling," he told Reuters.

"The person that operated this server had no clue on security, he had no clue about how to configure a Web server. He just took a ... toolkit and started to use it and in three weeks he managed to have this fortune, this treasure on his server."

'TROJAN' SOFTWARE

The crimeserver had a 'command and control' application that enabled the user to define what types of target to infect with 'trojan' software.

"Online statistics reports are included in this command and control. They can tell you who you managed to infect; where they are coming from; if the trojan that is now installed on their machine is sending you data, how much data you're getting -- you get all these online reports as well."

The hosting server was located in Malaysia and the Web domain was registered to a Russian individual with a Moscow address. Ben-Itzhak said

this could not be validated because domains can easily be registered in false names.

He said the discovery highlighted a growing trend for criminals to target commercial data. Details of pricing, company policies and stock-sensitive earnings results were all at risk.

"It's not just individuals at home doing their online banking and someone is stealing their password...The big picture is these criminals are looking for business data."

(Editing by Robert Woodward)

© Thomson Reuters 2008. All rights reserved. Users may download and print extracts of content from this website for their own personal and non-commercial use only. Republication or redistribution of Thomson Reuters content, including by framing or similar means, is expressly prohibited without the prior written consent of Thomson Reuters. Thomson Reuters and its logo are registered trademarks or trademarks of the Thomson Reuters group of companies around the world. Thomson Reuters journalists are subject to an Editorial Handbook which requires fair presentation and disclosure of relevant interests.

Reuters journalists are subject to the Reuters Editorial Handbook which requires fair presentation and disclosure of relevant interests.