



November 10, 2008 11:50pm AEDT

Russian link in \$4500 online theft

Karen Dearne | November 11, 2008

FORENSIC investigators have traced evidence of a theft of \$4500 from a Sydney woman's online bank account to a Russian server holding many more sensitive details captured by a Trojan horse hidden on her computer.

Sandra Bridekirk's brush with cybercrime began when she noticed two unauthorised deductions - each for \$1485 - from her account with a major bank on two days last week.

When she rang the bank, she was told a third payment was programmed to occur that day. "The scary thing was that the transactions had been done with my personal access number and my password, and even my husband doesn't know those," she said.

"It was set up to keep taking money out - the sum is apparently just under our daily limit - every day until it was all gone."

Ms Bridekirk was told the payments had been made to an interstate bank account. The third transaction was stopped, but \$3000 has been frozen until her bank and police finish their investigations. A further shock awaited Ms Bridekirk when an examination of her computer revealed all of her web credentials had been stolen - including all her user names and passwords, and her email address lists.

Andreas Baumhof, chief technical officer of online transaction security firm TrustDefender, discovered that Ms Bridekirk's computer had been infected by a drive-by download on September 2.

"This means the Trojan was silently installed on her computer without her knowing when she went to a compromised website."

Mr Baumhof found it was Trojan.Spy.Banker.EGJ, which injects extra HTML (web markup language) into internet banking web pages in order to capture passwords and credit-card details.

"All log-in forms on her machine have been collected and sent to Russia," he said.

"This means all her details were compromised."

Mr Baumhof found that the Trojan was active on the PC until September 10.

"She always had antivirus running and it did protect her a few times by detecting a virus before it was executed," he said. "But there's often a lag between an infection and when the sample becomes known to antivirus vendors so they can update their software to deal with it."

AusCERT analysis and assessments manager Kathryn Kerr said a similar Trojan, known as Sinowal, Torpig or Mebroot, had become prolific in the past 12 months, mainly because its many variants could not be detected soon enough by antivirus vendors.

"The HTML injection feature is very worrying, as once your computer is infected the Trojan just sits there waiting, with a target list of sites it's looking for," Ms Kerr said.

"The next time you connect to your online banking site, the Trojan detects that a request has been made to a particular bank.

"It then allows the connection to go ahead, but it intercepts the web page in your browser, and injects web code so that it appears to be part of the legitimate website.

"But it's not. Effectively, you've got two channels occurring simultaneously - one with the legitimate bank site

and one with the attacker, which will often prompt you for additional information that then gets sent off to some remote location."

Symantec security expert Robert Pregnell said internet users should check that their antivirus software included a firewall and intrusion prevention capabilities.

"If you bought your software even two years ago, you need to check that it has these protections," he said.

"An intrusion prevention system will detect a change in the connections that have been established with a bank, and they will give you a highly visible warning."

Copyright 2008 News Limited. All times AEDT (GMT + 11).