



Print This Article

<< Return to [Silentbanker trojan dupes bank customers into sending money](#)

Silentbanker trojan dupes bank customers into sending money

[Jack Rogers](#)

January 14 2008

A researcher has warned that the Silentbanker trojan apparently is able to circumvent two-factor authorization and inject itself into the middle of ongoing banking transactions, duping bank customers into sending money to attackers while the customer proceeds with what looks like a valid transaction.

Silentbanker also can redirect users to an attack-controlled server, according to researcher Liam Omurchu, who posted the [warning](#) Monday on [Symantec's Security Response blog](#).

When the banking trojan was first reported by Symantec last month, the anti-virus company tagged it with a "very low" Risk Level 1 classification, and indicated that its capabilities were limited to recording keystrokes, capturing screen images and stealing confidential financial data.

However, according to Omurchu, recent manifestations of Silentbanker appear to indicate that the trojan is a more potent threat than originally thought.

"The scale and sophistication of this emerging banking trojan is worrying, even for someone who sees banking trojans on a daily basis," Omurchu said in his blog posting.

Omurchu said that the ability of Silentbanker to perform man-in-the-middle attacks on valid transactions is the greatest cause for concern. He said the trojan can silently change the user-entered destination bank account details to the attacker's account details in the middle of a transaction.

The user does not notice this change because the trojan presents information the user expects to see, duping the bank customer into entering a second authorization password, in effect handing the money in the account over to the attackers, Omurchu said.

The Silentbanker trojan is able to intercept authentication traffic before it is encrypted, so that even if the transaction takes place over SSL, the attack is still valid. It can authenticate certificates and cookies, if they are required, as well as user names and passwords, he said.

A particularly sinister example of the trojan's sophistication, Omurchu said, is its ability to acquire missing information from unsuspecting bank customers. If the attackers are missing a key piece of information they need to conduct a transaction, the trojan enables the attackers to add extra HTML to the authorization page asking the user for that extra information, he said.

Silentbanker also downloads a configuration file that contains the domain names of more than 400 banks throughout the world, Omurchu said.