Two-Headed Trojan Targets Online Banks

internetnews.com/security/article.php/3846186/TwoHeaded+Trojan+Targets+Online+Banks.htm

October 29, 2009

HomeSecurity

By Larry Barrett
October 29, 2009

A new Trojan called “W32.Silon” is the latest headache for online banks and their customers, packing a one-two punch that helps it evade security tokens and steal customer log-in information at the same time.

The two-headed Trojan, according to online security software vendor Trusteer, uses a “two-pronged payload” to steal log-in information and commit financial fraud at popular online banks.

“This new Trojan illustrates how advanced malware writers have become in their ability to dynamically execute multiple, bank-specific attacks with a single piece of software,” Amit Klein, CTO and chief researcher at Trusteer, said in a statement. “The level of sophistication built into W32.Silon is concerning, as is its focus on circumventing strong authentication systems like card and PIN readers.”

W32.Silon is a new malware variant that intercepts Internet Explorer Web browser sessions and has been associated with fraud incidents at several large banks, according to Trusteer researchers.

To steal user credentials, W32.Silon performs its initial attack when a user begins a Web log-in session and enters his username and password. The malware intercepts the log-in POST request, encrypts the requested data and sends it to a command-and-control (C&C) server.

When it targets users of online banking applications that are protected by transaction authentication devices such as tokens or banking card readers, W32.Silon waits until the user has logged in and then injects dynamic HTML code into the log-in flow between the user and the bank’s Web server.

First, the malware presents authentic-looking Web pages that appear to be from the bank asking users to employ their transaction authentication device. Next, the user is asked to enter information from the device into the Web page.

This information is then used by the criminals to execute fraudulent transactions on behalf of the user, Trusteer said.

“We have put all of our banking customers on alert, and are attempting to get the word out with this advisory,” Klein said.

The sophistication of online scams has evolved to a point where watchdogs organizations such as the Anti-Phishing Working Group (APWG) have created an entirely new category for defining and quantifying attacks on financial institutions.

The group now defines “crimeware” as code designed to attack the data held by financial institutions.

“Due to evolution of attack sophistication, it is becoming increasingly difficult to separate and report on attacks that are specifically designed to steal customer banking information,” Dan Hubbard, Websense’s CTO, said earlier this month. “Additionally, attacks that only [look] for credentials from popular social networking, Webmail and gaming sites can lead to attacks for banking theft and crimeware.”

Trusteer advises online banking customers to be especially vigilant when conducting transactions online and to visit its Web site for help detecting and removing the W32.Silon Trojan.

Larry Barrett

Previous articleCalifornia Medicaid Members' Data Exposed
Next articleGoogle Chrome development slows to fix bugs