SpyEye Malware Borrows Zeus Trick to Mask Fraud

pcworld.com/article/247252/spyeye_malware_borrows_zeus_trick_to_mask_fraud.html

By Jeremy Kirk

A powerful bank-fraud software program, SpyEye, has been seen with a feature designed to keep victims in the dark long after fraud has taken place, according to security vendor Trusteer.

SpyEye is notable for its ability to inject new fields into a Web page, a technique called HTML injection, which can ask banking customers for sensitive information they normally would not be asked. The requested data can include logins and passwords or a debit card number. It can also use HTML injection to hide fraudulent transfers of money out of an account by displaying an inaccurate bank balance.

Trusteer noticed that SpyEye also hides fraudulent transactions even after a person has logged out and logged back into their account. The latest feature is designed with the same goal of keeping users unaware of fraud. The next time users log into their bank accounts, SpyEye will check its records to see what fraudulent transactions were made with the account, then simply delete them from the Web page, said Amit Klein, Trusteer's CEO. The account balance is also altered.

It appears that SpyEye has borrowed more from Zeus, a famous piece of banking malware that is now commonly available and considered the parent of SpyEye. The two pieces of malware were competitors, but in 2010 merged. Zeus also has the capability to hide its fraudulent transactions from victims.

"Zeus uses the stored balance details to inject into the same page at a later time to persistently hide the fact that money was fraudulently transferred from the user's account," according to a September 2011 report by Ryan Sherstobitoff, an independent security researcher, in the Information Systems Security Association Journal.

Trusteer has seen the technique used when a fraudster uses SpyEye to capture a person's debit card details. When those details are obtained, the fraudster conducts a purchase over the Web or phone, and SpyEye masks the transaction, Klein said. It does not affect, however, the bank's ability to see the fraud, he said.

Send news tips and comments to jeremy_kirk@idg.com

Note: When you purchase something after clicking links in our articles, we may earn a small commission. Read our affiliate link policy for more details.

Related:

- Security

- Business