Trojan Tricks Victims Into Transferring Funds

krebsonsecurity.com/2011/07/trojan-tricks-victims-into-transfering-funds/

It's horrifying enough when a computer crook breaks into your PC, steals your passwords and empties your bank account. Now, a new malware variant uses a devilish scheme to trick people into voluntarily transferring money from their accounts to a cyber thief's account.

The **German Federal Criminal Police** (the "Bundeskriminalamt" or BKA for short) recently warned consumers about a new Windows malware strain that waits until the victim logs in to his bank account. The malware then presents the customer with a message stating that a credit has been made to his account by mistake, and that the account has been frozen until the errant payment is transferred back.

When the unwitting user views his account balance, the malware modifies the amounts displayed in his browser; it appears that he has recently received a large transfer into his account. The victim is told to immediately make a transfer to return the funds and unlock his account. The malicious software presents an already filled-in online transfer form — with the account and routing numbers for a bank account the attacker controls.

The BKA's advisory isn't specific about the responsible strain of malware, but it is becoming increasingly common for banking Trojans to incorporate "Web injects," custom designed plug-ins that manipulate what victims see in their Web browsers.

This attack is an insidious extension of the tactic that was pioneered by the URL Zone Trojan, which specializes in manipulating the balance that victims see when they log into their (cleaned-out) bank accounts.

If you log in to your bank account and see something odd, such as a "down for maintenance" page or an alert about a wayward transfer, your best option is to pick up the phone and call your bank. Make sure you are using the bank's real phone number: Malware like the ZeuS Trojan has been known to present newly-fleeced victims with messages about problems with the bank's Web site, along with a bogus customer support phone number.