



TEXAS BANKERS ELECTRONIC CRIMES TASK FORCE



Bulletin 2012-1

April 5, 2012

The following is a recent action or issuance to be considered in the risk management practices for reducing the risks of Corporate Account Takeovers through the Protect, Detect, and Respond framework.

Cyber Thieves Launch Distributed Denial of Service Attack

A variation of Zeus malware has been used in Texas that permits thieves to launch a distributed denial of service (DDOS) attack against a bank's Internet banking website immediately after they have hijacked a customer's account and sent instructions to transfer the money. This is done to prevent customers from checking their balance (and noticing the theft) and as a distraction to the bank, in hopes that the fraudulent transaction leaves the bank before it is detected.

Recommended Action:

Update your Incident Response plan so your staff will immediately notify your fraud response committee's central point of contact (See R1 of Best Practices) if Internet banking problems begin to occur, especially late in the day and/or the last business day of the week. The fraud response committee will want to notify appropriate departments that a Corporate Account Takeover theft might be in progress and they should carefully monitor all outgoing transactions.

Even if you haven't seen suspicious transactions come through, you should closely scrutinize transactions. Additionally, be aware that thieves might block communications to the customer's telephone line or email.

Notify customers of this new development. Depending on your number of corporate customers and the capacity of your call center (or switchboard staff), consider advising your corporate customers to call the bank if they are unable to connect to the bank's website to check their balances. Notify your call center (or switchboard) of what action to take if calls begin to arrive.