



TEXAS BANKERS ELECTRONIC CRIMES TASK FORCE



Bulletin 2013-2

May 6, 2013

Distributed Denial of Service Attacks on the Rise: What Community Bank CEOs Should Know

Cyber thieves and hacktivist groups (hackers that disrupt online services for social causes) have been increasing their use of distributed denial of service (DDoS) attacks on the banking system. A DDoS attack in its simplest form floods a financial institution's website with incoming messages that essentially overloads the website, thereby preventing bank customers' access to online banking services. In some cases, a goal of the DDoS attack is to serve as a distraction to bank personnel to prevent them from immediately identifying a fraudulent transaction occurring during this time.

A DDoS attack is a temporary disruption. As of this date, most DDoS attacks last for several hours. However, some attacks have continued for several days. While customers will have difficulty accessing online banking services during this period, it is important to remember that there are other delivery channels through which they can conduct banking transactions.

Although this could change, currently only a few banks with less than \$5 billion in total assets have been the target of DDoS attacks. This bulletin focuses on what CEOs of banks with less than \$5 billion in total assets should know about DDoS attacks and what actions they may want to implement.

Recommended Actions:

The potential impact of DDoS attacks depends on the importance of online banking services for your bank's customers. As the importance of online banking increases for your bank, the more attention it will need in the risk management process. While all banks should educate themselves about the latest cyber threats, banks with \$1 to \$5 billion in total assets in particular need to be evaluating DDoS attacks as a potential business interruption to online banking. The bank's business impact analysis, within the business continuity plan, needs to be updated with strategies for addressing this risk. Banks larger than \$5 billion should already have continuity plans in place for DDoS interruptions.

Confirm Transactions

If your bank becomes the target of a DDoS attack, consider it a diversionary tactic by thieves to mask stealing funds. Protecting the bank's payment systems will need to be a primary focus for bank staff. Even if the attack is launched by hacktivists, which sometimes announce their attack in advance, unaffiliated cyber thieves might take advantage of the announced disruption to attempt a Corporate Account Takeover fraud through your bank.

If your institution does not already conduct full call-back procedures of all wire and ACH activity (or above some tolerable loss amount), then strongly consider implementing that process during a DDoS attack. If your bank already conducts call backs for transactions over a specific amount, consider lowering that limit during a DDoS attack.

Educate Customers

If your bank has a large number of commercial banking customers that depend on online banking services, consider talking with at least the key customers and lending officers in advance about the difference between DDoS attacks and hacking (which actually puts information and funds at risk). Plan alternative methods that can be used for conducting banking activity if a slowdown to your online banking services occurs, as well as various ways your customers can alert the bank should they discover they are the victim of a cyber-theft.

Retail consumer education is also necessary, either before or during an event. Customers may have questions about the safety of their money when they cannot access their account online. Consider having a prepared response for your customer service / call center, which will likely experience an increased volume of calls from customers trying to utilize the bank's online banking services. Also be prepared to increase the number of customer service representatives answering calls, and remind customers of any alternative methods available to them for conducting banking transactions. Whether you disclose that you are the target of a DDoS attack or simply confirm that you are experiencing network disruptions is an individual decision.

Review Network

Mitigating a DDoS attack is a technical process that usually requires the assistance of outside vendors to work with the Internet Service Provider (ISP) that provides the Internet connection to your website. Depending on your network design, DDoS attacks could slow down your internal network and email. Regardless if the bank's website hosting is outsourced or internal, institutions with greater dependence on a fast internal network should have their technical staff evaluate the network structure with the threat of DDoS attacks in mind and plan alternative measures to mitigate the impact to bank's customers.

Also refer to ECTF Bulletin 2012-1 related to DDoS attacks.