Client Alert

May 2013

OpUSA: Criminal Hackers Planning Cyber Attacks Against Bank Websites

The hacker group Anonymous announced that it, in concert with Middle East- and North Africa-based criminal hackers and cyber actors, will conduct a coordinated online attack labeled "OpUSA" against banking and government websites today, May 7. Anonymous stated that OpUSA will be a distributed denial of service (DDoS) in which websites may be defaced and legitimate users may be unable to access websites.

Although a DDoS attack does not involve penetration of a bank's systems, it can nevertheless affect a business or other institution in a number of ways. Some of those impacts are:

- IT resources: Internal IT departments must devote time and resources to respond to the attacks, prevent further attacks, and help to address concerns from internal sources, business partners, and customers. Such incidents also may require substantial capital expenditures to protect against future incidents, *e.g.*, upgrades and patch management.
- Transaction reconciliation: Resources must be assigned to reconcile business activities that occurred during the attack, such as those involving online transactions.
- Lost business/customers: Present customers may cease transacting business with the DDoS target because of the incident and attendant inconvenience, at least until they are reassured about the safety and integrity of the system.
- Loss of potential business: This is largely unknowable, but potential customers may take business elsewhere as a result of the attack, perceived ineffective response to the attack, and/or resulting negative publicity.
- Reputational damage: There may be a reputational impact with the public, regulators, and/or customers.
- Extraordinary expenses: Internal costs, as well as fees and expenses of outside professionals and contractors retained to assist in responding to the attack and its aftermath.

Also, a highly publicized DDoS attack would be good cover for a related -- or even an unrelated -- criminal organization seeking to infiltrate the network. A DDoS attack may be seen as an opportunity to infiltrate the network because resources and focus would be diverted from where they are normally employed.

If you recognize that your bank is under attack we recommend that you take the following steps. As the IT department works to counter the attack and restore normal functions, it is best to call in professionals and investigate the situation in a privileged manner to determine the nature of the event. A bank should quickly evaluate the security of its online transaction platform. This assessment should be coupled with a process to reconcile all transactions including all ACH and wire transfer requests. The bank will also need to advise its regulator about the attack. Once the situation is normalized, a bank should do a post-

mortem and begin preparation for another attack, including technical contingencies to handle such increased traffic and consider the possibility of offensive litigation.

Contacts

Lawrence J. Bracken, II
lbracken@hunton.com

John J. Delionado
jdelionado@hunton.com

Corey Lee
leec@hunton.com

Peter Weinstock
pweinstock@hunton.com