BITS
FINANCIAL SERVICES ROUNDTABLE

Cyber Attacks: Strategies for Response

October 19, 2012

Since late September 2012, 14 large financial institutions have been the subject of (or threatened to be the subject of) attacks intended to disrupt the availability of their websites. A group that calls itself the Cyber Fighters of Izz ad-din Al Qassam has claimed credit for these attacks. As there is a likelihood these attacks will continue, all financial institutions should review their preparations for dealing with such an attack.

The Financial Services Roundtable and BITS are collaborating with member companies and the Financial Services Information Sharing and Analysis Center (FS-ISAC). Below are strategies for banks and their customers to protect themselves online.

Financial institutions can prepare by doing the following:

1. Review strategies for patching IT systems and current patch status, scanning networks and managing bandwidth to minimize the number of non-attack related issues.

2. Coordinate with Internet Service Providers and other service providers to implement controls (e.g., scrubbing, rate limiting, source blocking).

3. Assess critical external-facing assets and applications to provide end-to-end protection and assess the capabilities of vendors in providing protection services or expanding bandwidth.

4. Review communications strategies to include, incident notification for both internal and external parties (e.g., senior management, key service providers, and customers) if and when the attack begins.

5. Participate in the FS-ISAC and share actionable information to protect other institutions.

6. Inform your primary regulator of attacks and seek assistance from the US Treasury Department and other agencies for assistance if attacked or threatened with attack.

7. If attacked, consider using the following consumer messages:

What's happening?

- The Web sites at some banks are being intentionally flooded with an extremely high volume of electronic traffic from thousands of locations around the world. This flood of

traffic, called "a distributed denial of service (DDoS) attack" crowds out legitimate customers trying to use the bank's Web sites.

- Customers of those banks may experience a slower than usual connection or delayed connection when logging into Web site or making transactions online.
- The slowdowns do NOT involve a data breach or hacking
- The flood of electronic traffic is intended to slow down or disable the bank's Web site.
- The traffic is not designed – and has not resulted in – hacking which involves penetration of the banks' internal systems or exposure of sensitive personal information.

Who Is Behind the Attacks?

- A group that calls itself the Cyber Fighters of Izz ad-din Al Qassam has claimed credit for the recent bank attacks.

What You Should Know

- The attacks have not resulted in unauthorized access to customer information.
- Bank employees are working hard to ensure you have access to normal, safe and consistent online financial services. In addition, you can access your accounts through alternative means, including your bank's branch offices, mobile applications and call centers.
- Banks use sophisticated online security strategies to protect customer accounts.
- Banks are working with telecommunications providers to increase capacity and invest in technology to defend attacks. There are limits to the capacity and services available from telecommunications providers.
- Banks continue to invest in technology to defend against potential attacks.
- Banks are collaborating with other banks, federal regulators, law enforcement officials, other government agencies, Internet Service Providers, and Internet security experts to fully analyze and deflect online attacks and deliver safe and consistent online service.
- Banks collaborate with the Financial Services Information Sharing and Analysis Center (FS-ISAC) which is an industry forum for collaboration on critical security threats facing the financial services sector.

What You Can Do

- Install on your computer—and keep updated—anti-virus software, firewall and anti-spyware software.
- Set your computer's operating system and browser to "automatic download" to ensure your operating system and browser include the latest security updates.
- Don't get hooked by phishing. Do not respond to unsolicited emails requesting personal information and do not download attachments on unsolicited emails.

- Use strong passwords and change them regularly. The best passwords are long—a minimum of 8 characters—and complex. Not your birthday or the name of a child or pet. Use a combination of numbers, symbols and letter; something meaningful to you like an acronym or batting averages, but not easily guessed.

Please contact John Carlson (john@fsround.org or 202-589-2432) if you have any questions or if BITS and the Roundtable can assist you. Thanks.