BEST PRACTICES FOR BANKS

Managing The Risks of Distributed Denial-of-Service (DDoS) Attacks

(Developed by the Bankers Electronic Crimes Task Force)

INTRODUCTION

A distributed denial-of-service (DDoS) attack attempts to prevent legitimate users from accessing information or services. By targeting the computers used to operate the bank's website, email, or telephone system, an attacker may be able to prevent the bank from receiving emails sent by customers, prevent customers from accessing the bank's website (and the banking services offered on it), or prevent customers from reaching bank employees by phone.

The most common type of DDoS attack occurs when an attacker "floods" the bank website, email server, or telephone system with information. This "flood" of information varies based on what is being attacked, but fundamentally, it overloads the capacity of that service at the bank. Each system can only process a certain amount of information at once, so if an attacker overloads the system, it cannot process legitimate requests from customers who are then denied the ability to use that service.

BACKGROUND ON DDOS ATTACKS

The frequency of DDoS attacks, like all cyber-attacks, is increasing. Primary motives for launching a DDoS attack against a bank is to disrupt bank operations as a smoke screen while a different attack is being carried out, or to extort money. In late 2012 and into 2013, the largest banks in the U.S. were under persistent DDoS attacks by activists focused on embarrassing/disrupting banks. This is not typically the motive for launching an attack against a community bank. Motivations for community bank DDoS attacks are likely to mask other illegal activity, or to extort money in exchange for ending or not launching a DDoS attack. Even still, a DDoS attack against a community bank can negatively impact the bank's reputation as the public may believe their money or personal information is at risk, which can undermine the public's confidence in the financial institution or the community banking system as a whole.

As of mid-2016, the average duration of a DDoS attack was less than a day. Depending on how critical the service is that is under attack, some institutions may opt to "wait it out," but those that do must be vigilant that other illegal activities are not occurring simultaneously and have an appropriate strategy for addressing the service needs of customers. It is important to also note that while the average duration of a DDoS attack in 2016 was less than a day, the attack may certainly last much longer, potentially weeks.

PREVENTING DDOS ATTACKS

Preventing a DDoS attack from impacting access to a bank's website is a highly technical undertaking beyond the capacity of the staff at most banks, especially community banks. However, specialized firms exist that provide DDoS mitigation services to banks.

While preventing a DDoS attack from impacting bank operations requires a great deal of planning and can be costly, reducing the impact of an attack is within the range of most financial institutions. Minimizing the reputation impact of a DDoS attack is possible with good planning.

The basic process that DDoS mitigation vendors use for preventing a DDoS attack from impacting online banking services is what is commonly called scrubbing. Scrubbing involves removing the bad information "flooding" the network before it reaches the network. To do this, management must know what the "normal information traffic" looks like. Normal traffic cannot be easily determined during a DDoS attack. Therefore, if management decides to use a DDoS mitigation service, management should establish a baseline of normal traffic in advance. Additionally, if management is considering use of a DDoS mitigation service, the best time to negotiate services is before an attack occurs.

SUMMARY

While preventing a DDoS attack from impacting bank operations may be cost prohibitive for many community banks, the financial impact of an attack can be estimated. These Best Practices will assist community bankers in developing a strategy for managing risks associated with DDoS attacks. Additionally, steps can be taken to minimize the adverse reputation risk. Please note that detailing all of the technical steps for mitigating DDoS risks are beyond the scope of these Best Practices, but additional resources are listed at the end of the document.

IDENTIFY

I1 Identify the potential impact a DDoS attack could have on the bank.

I2 Identify key processes and equipment that could be targeted and that might warrant protection, such as:

- On-line banking website server(s),
- Email server,
- Telephone system, and
- ATMs.

I3 Identify/estimate the financial impact to the bank.

I4 Identify/estimate the impact on reputation if services become unavailable.

I5 If management uses DDoS mitigation services, identify baseline normal traffic. Know the normal traffic, as this can help in monitoring whether or not a DDoS attack is in process.

- Identify what makes up the bank's normal traffic.
- Identify where the traffic come from.
- Identify what time of day generates what type of traffic.

PROTECT

P1 Contact the Internet Service Provider (ISP) and the hosting company for the bank's website (on-line banking), and ask what services they have to protect against DDoS attacks.

- Review the contract for Service Level Agreements regarding availability of the website.

P2 Communicate to your customers about DDoS attacks before an attack.

- Speak at local civic organizations about cybersecurity in general, to build the bank's reputation as cybersecurity experts in the community.
- Explain that DDoS attacks do not steal money or personal information, although that could be occurring. So, if they experience a DDoS attack at their business, they should shift attention to monitoring payment systems.
- Explain that DDoS attacks do not involve hacking the bank.

P3 Develop a DDoS mitigation plan.

- Identify personnel to be involved and roles.
- Have procedures to protect the bank's payment systems, and consider increased reviews of wire transfers during an attack.

P4 Review branch connectivity to determine if there is an over reliance on Internet connections that are shared with services (website / on-line banking) that are potential targets for a DDoS attack. If so, consider protecting branch operations by using a different connection method.

DETECT

D1 Contact the hosting company for the bank's website (on-line banking) and the Internet Service Provider (ISP) to determine if they can detect DDoS attacks.

D2 Train call center personnel (or switchboard operators) to be alert for a high volume of calls regarding problems with the on-line banking website.

RESPOND

Rd1 Activate the DDoS Incident Response Plan (test plan regularly).

- Activate alternative procedures for customers to contact the bank during a DDoS attack. Having multiple methods for customers to be able to communicate is a good idea, and crucial for key large volume customers.

Rd2 Talk to both the hosting company for the bank's website (on-line banking) and to the bank's Internet Service Provider (ISP), and ask if they can reroute traffic in the event of an attack.

Rd3 Consider having an alternative website hosted on a different IP address to direct customers to so they can perform time sensitive transactions (such as payroll files).

Rd4 Provide the call center / switchboard operators with the response to provide to customers regarding the website not working. Prepare this message in advance.

Rd5 If the bank has a cyber-insurance policy, contact the insurer if the policy, especially if it provides remediation services.

RECOVER

Rr1 Restore operations to normal services.

Rr2 Document lessons learned.

- Review processes, procedures, and technology to strengthen identified weaknesses to improve response to any future incidents.

Rr3 If your bank has a cyber-insurance policy, contact the insurer if the policy provides any business interruption cost recovery.

ADDITIONAL RESOURCES

FFIEC Joint Statement
https://www.ffiec.gov/press/PDF/FFIEC%20DDoS%20Joint%20Statement.pdf

US-CERT
https://www.us-cert.gov/ncas/tips/ST04-015

Department of Justice
https://www.ic3.gov/media/2015/150731.aspx

SANS Institute
https://www.sans.org/reading-room/whitepapers/incident/preparing-withstand-ddos-attack-36412

FS-ISAC Members' Portal
FS-ISAC Threat Intelligence Committee Threat Viewpoint – Distributed Denial of Service (DDoS) Attacks

The following information is from a for-profit corporation. However, the information includes non-product specific information that can be helpful to non-customers. Some information is older, but the fundamentals are unchanged. No endorsement is implied.

The Imperva DDoS Response Playbook
https://www.imperva.com/docs/gated/WP_Incapsula_DDoS_Response_Playbook.pdf