3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446 • http://www.ffiec.gov

Joint Statement

Distributed Denial-of-Service (DDoS) Cyber-Attacks, Risk Mitigation, and Additional Resources

PURPOSE

The Federal Financial Institutions Examination Council (FFIEC) members[1] ("members") are issuing this statement to notify financial institutions of the risks associated with the continued distributed denial-of-service (DDoS) attacks on public websites. The statement also outlines the steps that institutions are expected to take to address these attacks, and provides resources to help institutions mitigate the risks posed by such attacks.

BACKGROUND

In the latter half of 2012, an increased number of DDoS attacks were launched against financial institutions by politically motivated groups. These DDoS attacks continued periodically and increased in sophistication and intensity. These attacks caused slow website response times, intermittently prevented customers from accessing institutions' public websites, and adversely affected back-office operations. In other cases, DDoS attacks served as a diversionary tactic by criminals attempting to commit fraud using stolen customer or bank employee credentials to initiate fraudulent wire or automated clearinghouse transfers.

RISKS

Financial institutions of all sizes that experience DDoS attacks may face a variety of risks, including operational risks and reputation risks. If the attack is coupled with attempted fraud, a financial institution may also experience fraud losses as well as liquidity and capital risks.

RISK MITIGATION

The members expect each financial institution to address DDoS readiness as part of ongoing information security and incident response plans. In accordance with regulatory requirements[2],

[1] The FFIEC is comprised of the principals of the following: The Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee.

[2] 12 C.F.R. Part 30, Appendix B (Office of the Comptroller of the Currency); 12 C.F.R. Part 208, Appendix D-2, and Part 225, Appendix F (Federal Reserve); 12 C.F.R. Part 364, Appendix B (Federal Deposit Insurance Corporation); 12 C.F.R. Part 748, Appendix A and B (National Credit Union Administration).

and the *FFIEC Information Technology (IT) Handbook on Business Continuity Planning*[3] and *Information Security*[4] booklets, the members expect institutions to take the following steps, as appropriate:

1. Maintain an ongoing program to assess information security risk that identifies, prioritizes, and assesses the risk to critical systems, including threats to external websites and online accounts;
2. Monitor Internet traffic to the institution's website to detect attacks;
3. Activate incident response plans and notify service providers, including Internet service providers (ISPs), as appropriate, if the institution suspects that a DDoS attack is occurring. Response plans should include appropriate communication strategies with customers concerning the safety of their accounts;
4. Ensure sufficient staffing for the duration of the DDoS attack and consider hiring pre-contracted third-party servicers, as appropriate, that can assist in managing the Internet-based traffic flow. Identify how the institution's ISP can assist in responding to and mitigating an attack;
5. Consider sharing information with organizations, such as the Financial Services Information Sharing and Analysis Center and law enforcement because attacks can change rapidly and sharing the information can help institutions to identify and mitigate new threats and tactics; and
6. Evaluate any gaps in the institution's response following attacks and in its ongoing risk assessments, and adjust risk management controls accordingly.

ADDITIONAL RESOURCES

In addition to the FFIEC guidance, several other publications are available to help organizations mitigate the risks from DDoS attacks. The Department of Homeland Security's National Cybersecurity and Communications Integration Center published a *DDoS Quick Guide* on January 29, 2014. This *Quick Guide* provides useful information on attack possibilities and traffic types and should be shared with an institution's IT department and the institution's online banking service provider, if applicable. The *Quick Guide* is available at www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf .

Additionally, publications such as National Institute of Standards and Technology Special Publication 800-61, *Computer Security Incident Handling Guide*, (http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf), offer specific instructions for IT staff members to help implement incident response plans. The following are additional reference materials:

- Office of the Comptroller of the Currency - Distributed Denial of Service Attacks and Customer Account Fraud, December 21, 2012; http://www.occ.gov/news-issuances/alerts/2012/alert-2012-16.html

[3] http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx

[4] http://ithandbook.ffiec.gov/it-booklets/information-security.aspx

- National Credit Union Administration - Mitigating Distributed Denial-of-Service Attacks, February 2013; http://www.ncua.gov/Resources/Pages/RSK2013-01.aspx
- US-CERT - Security Tip, Understanding Denial-of-Service Attacks, November 4, 2009; http://www.us-cert.gov/ncas/tips/ST04-015