Information Notice

Distributed Denial of Service (DDoS) Attacks on Member Firms

June 19, 2015

Suggested Routing

- Compliance
- Legal
- Operations
- Registered Representatives
- Senior Management

Key Topics

- Cybersecurity
- Distributed Denial of Service Attack (DDoS)
- Information Technology

Cybersecurity continues to be a concern for broker-dealers and a focus of FINRA. FINRA issued a *Report on Cybersecurity Practices* on February 3, 2015, to highlight effective practices that firms should consider to strengthen their cybersecurity programs.

Within the past two weeks, several member firms have informed us that they have been subject to DDoS attacks originated by a cyber-criminal group known as DD4BC. A successful DDoS attack renders a website or network unavailable for its intended users by overwhelming the site with incoming messages. It appears that DD4BC has been targeting financial services/broker-dealer firms that have an online presence.

In these incidents, DD4BC first sends the firm an email announcing that the firm will be a target for a DDoS attack, but that the firm can avoid the attack by paying a ransom in Bitcoin. DD4BC conducts a short "demonstration" attack, typically lasting about one hour, with the threat of further attacks if the ransom is not paid. DD4BC requests payment within 24 hours to prevent further attacks.

If you receive a communication from DD4BC or experience a similar attack, please contact your local FBI and SEC offices and FINRA. In addition, ensure you have plans in place to address this type of incident. Elements of a DDoS response plan may include:

- the use of DDoS mitigation and monitoring tools (firms should consider contacting your Internet service provider (ISP) to put service-provider side traffic filters in place); and
- preparation of contingency communications plans for customers if a firm's website is unavailable.

If you are a member of FS-ISAC or other IT controls organizations please contact them as they can help with mitigation advice.

Questions concerning this *Notice* should be directed to:

- David Kelley, Surveillance Director at (816) 802-4729;
- Chris Longobucco, Regulatory Principal, IT Controls at (312) 899-4394; or
- Len Smuglin, Principal Examiner at (212) 416-1595.