Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

31 July 2015

Alert Number
I-073115-PSA

E-mail Extortion Campaigns Threatening Distributed Denial of Service Attacks

The Internet Crime Complaint Center (IC3) recently received an increasing number of complaints from businesses reporting extortion campaigns via e-mail. In a typical complaint, the victim business receives an e-mail threatening a Distributed Denial of Service (DDoS) attack to its Website unless it pays a ransom. Ransoms vary in price and are usually demanded in Bitcoin.

Victims that do not pay the ransom receive a subsequent threatening e-mail claiming that the ransom will significantly increase if the victim fails to pay within the time frame given. Some businesses reported implementing DDoS mitigation services as a precaution.

Businesses that experienced a DDoS attack reported the attacks consisted primarily of Simple Discovery Protocol (SSDP) and Network Time Protocol (NTP) reflection/amplification attacks, with an occasional SYN-flood and, more recently, Wordpress XML-RPC reflection/amplification attack. The attacks typically lasted one to two hours, with 30 to 35 gigabytes as the physical limit.

Based on information received at the IC3, the FBI suspects multiple individuals are involved in these extortion campaigns. The attacks are likely to expand to online industries and other targeted sectors, especially those susceptible to suffering financial losses if taken offline.

If you believe you have been a victim of this scam, you should reach out to your local FBI field office, and file a complaint with the IC3 at www.IC3.gov. Please provide any relevant information in your complaint, including the extortion e-mail with header information.

Tips to protect yourself:

- Do not open e-mail or attachments from unknown individuals.
- Do not communicate with the subject.
- If an attack occurs, utilize DDoS mitigation services.