ROLL CALL RELEASE
INTELLIGENCE FOR POLICE, FIRE, EMS, AND SECURITY PERSONNEL
6 February 2014

(U//FOUO) Extortion Schemes Use Telephony-Based Denial-of-Service Attacks

UNCLASSIFIED

(U//FOUO) Since at least January 2012, criminals are using telephony-based denial-of-service (TDoS) combined with extortion scams to phone an employee's office and demand the employee repay an alleged loan. If the victim does not comply, the criminals initiate TDoS attacks against the employer's phone numbers. TDoS uses automated calling programs—similar to those used by telemarketers—to prevent victims from making or receiving calls. Recent examples include the following:

- (U//FOUO) According to DHS reporting, between 28 January and 3 March 2013, the public safety answering point for a south-central region sheriff's office received a call demanding repayment of a loan for an unknown individual. A TDoS attack followed this request, disrupting the non-emergency business lines.

- (U) The US Coast Guard (USCG) in late May 2013 reported that an individual called a USCG cutter claiming to have a legal matter to discuss with a crewmember. The subsequent TDoS attack flooded the ship's telephone network with several rounds of TDoS phone calls, completely disrupting phone service.

(U//FOUO) For more information on TDoS scams, please reference *Homeland Security Note* "(U//FOUO) Cyber Criminals Combine Tactics for Extortion;" this product is available by searching on HSIN Intel or CI Home at https://hsin.dhs.gov.

(U) **What to do During a TDoS Event:**

- (U) Do NOT make any payments, but DO record all phone numbers and payment instructions.
- (U) If practical, save the voice recordings of suspect calls—before, during, and after the TDoS events.
- (U) If the caller is demanding a payment, attempt to capture the following information: start and stop times of calls and number of calls per day; phone numbers and caller ID information; instructions regarding how to pay, such as account number or callback number.
- (U) Attempt to separate the affected phone number from other critical trunks.

(U) **Reporting Computer Security Incidents**

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us-cert.gov/report/ and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

IA-0086-14

(U) Prepared by the Office of Intelligence and Analysis (I&A) and National Protection and Programs Directorate, US Computer Emergency Readiness Team. Coordinated with Federal Bureau of Investigation. This product is intended to provide cybersecurity awareness to federal, state, local, and private sector first responders in matters that can affect personnel and network security of their respective organizations.

*(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with critical infrastructure and key resource personnel or private sector security officials without further approval from DHS.*