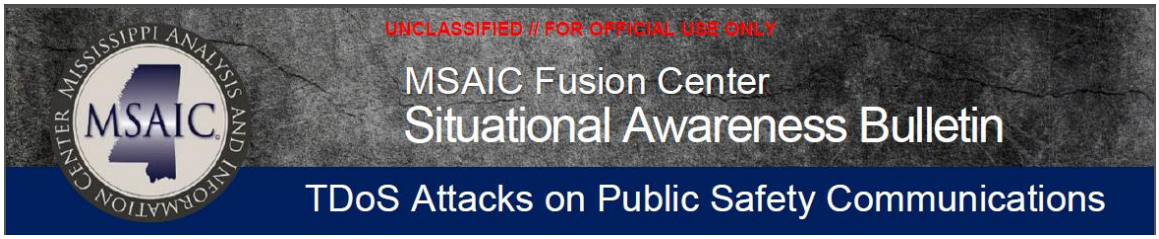
SAU
SITUATIONAL AWARENESS UPDATE
COOK COUNTY DEPARTMENT OF HOMELAND SECURITY & EMERGENCY MANAGEMENT
69 West Washington - Suite 2630 Chicago, IL 60602 V. 312.603.8180
Toni Preckwinkle, President - Cook County Board of Commissioners
Michael G. Masters, Executive Director

Date: 16 March 2013
No.01
LEO Sensitive

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail: DUTY.DESK@cookcountyil.gov or phone: (312) 603 – 8180 or (312) 603-8185.

This information is being passed through as a courtesy to the originating agency. DHSEM had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Do not advise individuals contained therein of this alert. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact DHSEM at 312-603-8185 if you have any questions or need additional information.



The Department of Homeland Security (DHS) NCCIC - National Coordinating Center for Communications – the DHS-Office of Emergency Communications, DHS - Office of Infrastructure Protection, Federal Communications Commission, the National Cyber and Forensics Training Alliance, the FBI-National Cyber Investigative Joint Task Force working in coordination with the Association of Public Safety Communications Officials (APCO) International, the National Emergency Numbers Association (NENA), Louisiana Fusion Center, Mansfield Police Department and telecommunications service providers to identify and mitigate the effects of a criminal Telephony Denial of Service (TDoS) against public safety communications, hospitals and ambulance services. **This is for immediate dissemination to public safety answering points (PSAPs) and emergency communications centers and personnel.**

Background: Information received from multiple jurisdictions indicates the possibility of attacks targeting the telephone systems of public sector entities. Dozens of such attacks have targeted the administrative PSAP lines (not the 911 emergency line), The perpetrators of the attack have launched high volume of calls against the target network, tying up the system from receiving legitimate calls. This type of attack is referred to as a TDoS or Telephony Denial of Service attack. These attacks are ongoing. Many similar attacks have occurred targeting various businesses and public entities, including the financial sector and other public emergency operations interests, including air ambulance, ambulance and hospital communications.

Scheme: These recent TDoS attacks are part of an extortion scheme. This scheme starts with a phone call to an organization from an individual claiming to represent a collections company for payday loans. The caller usually has a strong accent of some sort and asks to speak with a current or former employee concerning an outstanding debt. Failing to get payment from an individual or organization, the perpetrator launches a TDoS attack. The organization will be inundated with a continuous stream of calls for an unspecified, but lengthy period of time. The attack can prevent both incoming and/or outgoing calls from being completed. It is speculated that government offices/emergency services are being "targeted" because of the necessity of functional phone lines.

What we know:

- The attacks resulted in enough volume to cause a roll over to the alternate facility.
- The attacks last for intermittent time periods over several hours. They may stop for several hours, then resume. Once attacked, the attacks can start randomly over weeks or months.
- The attacks followed a person with a heavy accent demanding payment of $5,000 from the company because of default by an employee who either no longer works at the PSAP or never did.

What we need from victims:

- Additional insight into the scope and impact of the event- specifically how many communications centers have been attacked is critical to identifying the true scope of this occurrence.
- In order to ensure situational awareness with our members and member agencies, it is critical that this information be disseminated to emergency communications centers, PSAP's, government IT departments, and any related government agency with a vested interest in emergency communications continuity of operations.

Recommend the following:

- Targeted organizations should not pay the blackmail.
- Report all attacks to the FBI by logging onto the website www.ic3.gov

    o Ensure in the title of the report you use the keyword TDoS
    o Ensure that you identify yourself as a PSAP or Public Safety organization capture as much details as possible

- Calls logs from "collection" call and TDoS
- Time, date, originating phone number, traffic characteristics.
- Call back number to the "collections" company or requesting organization.
- Method of payment and account number where "collection" company requests debt to be paid.
- ANY information you can obtain about the caller, or his/her organization will be of tremendous assistance in this investigation and in preventing further attacks.

- Contact your telephone service provider; they may be able to assist by blocking portions of the attack.

Should you have any questions please contact the National Coordinating Center for Communications at NCC@hq.dhs.gov or 703-235-5080

This information should be considered UNCLASSIFIED//FOR OFFICIAL USE ONLY. Further distribution of this document **is restricted to public safety, first responder, emergency management agencies and those with a valid need to know** unless prior approval from the Mississippi Analysis and Information Center is obtained. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. It contains information that may be exempt from public release under the Freedom of Information Act (5 USC 552).

Any request for disclosure of this document or the information contained herein should be referred to the Mississippi Analysis & Information Center: (601) 933-7200 or msaic@dps.ms.gov.

1. 1759	2.

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency.
Dissemination of FOUO is restricted to persons with "need-to-know." Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties.
Typical FOUO requirements include:
1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.
2. The holder of the information will comply with access and dissemination restrictions.
3. Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.