FBI Cyber Division

Private Industry Notification

2 July 2014

PIN: 20140702-001

(U) Cyber Criminals Use Telephony Denial of Service (TDoS) Attacks to Extort Healthcare and Public Health Sector Employees

(U) Cyber criminals continue to conduct Telephony Denial of Service (TDoS) attacks to extort money from Healthcare and Public Health Sector employees. In one instance, the 9-1-1 Public Safety Access Point (PSAP) communications of a hospital was disabled during the attack. The cyber actors often used spoofed telephone numbers and/or assigned IP addresses making the telephone calls more difficult for law enforcement to track. Due to the ease of TDoS attacks that cyber actors carry out on vulnerable systems, as well as using tactics to evade detection, it is most likely that TDoS will be the "go-to" method that can be used on other organizations, whether government or private, that rely heavily on telephone lines.

UNCLASSIFIED

(U) Telephony Denial of Service (TDoS)

(U) Denial of service attack, which is aimed at crippling the organization's phone lines.

Source: www.securelogix.com

(U) TDoS Attacks Targeting Employees in Healthcare and Public Health Sector

(U) In March 2014, the emergency communications of a San Francisco Bay Area hospital was disabled by a TDoS attack. The attack method used was a computer to continuously redial the Emergency Room (ER) thereby crashing the hospital's telephone trunk. All ER telephone lines were busy rendering the system dead. This TDoS attack although similar to previously reported attacks was significantly different in that PSAP communications were disrupted and the hospital was unable to receive any emergency telephone calls during the attack.

(U) Beginning in April and continuing through August of 2013, another Bay Area hospital was subjected to a series of TDoS attacks. Employees in the Central Supply Department and Labor and Delivery Departments were targeted by the cyber actor in an attempt to extort money from the victims. Prior to each TDoS attack, the facility received a telephone call from an unidentified individual who requested to speak with one of the employees; the cyber actor used apparent spoofed telephone numbers to make the telephone calls. The individual stated the employee owed a debt but in order to collect the debt the individual requested the employee to provide credit card numbers and other personal identifiable information (PII). When the employee refused to provide the information requested, the individual initiated TDoS attacks on the facilities telephone network. During each attack, the hospital was unable to receive any telephone calls for a period of approximately 10 hours.

(U) Since 2013, approximately 1000 similar complaints were received by the FBI's Internet Complaint Center (www.ic3.gov) from medical centers across the country. All of the complaints include an unidentified individual, speaking with a foreign accent, calling in regards to debt collection and TDoS attacks if the information requested was not provided. At times, the individual carried out TDoS attacks on the actual emergency dispatch centers, which were unable to receive telephone calls. Most of the telephone calls appeared to be from spoofed telephone numbers belonging to other US businesses from across the country.

(U) Earlier in March 2013, the Association of Public-Safety Communication Official (APCO) International released a bulletin on TDoS attacks describing the TDoS extortion scheme, which starts with a telephone call to an organization from an individual claiming to represent a collections company for payday loans. The caller usually has a strong accent and requests to speak with a current or former employee concerning an outstanding debt. Failing to receive payment from an individual or organization, the perpetrator launches the TDoS attack, which involves a continuous stream of telephone calls for a lengthy period of time. The attack can prevent both incoming and/or outgoing telephone calls from being completed.

(U) Preventive, Response and Reporting Steps that Can Help Victims and/or Possible Future Victims of TDoS Attacks

(U) It is suggested medical/healthcare services institutions adhere to the following checklist that has been developed as a result of cooperative effort between federal authorities, public safety representatives, and commercial service providers.

(U) Preventive measures:

- (U) Discuss how to respond to a TDoS event with your service provider and 9-1-1 equipment vendors.
- (U) Ensure the Public Safety Telecomunicators and their supervisors have access to the telephone number and direct contact information for the service provider's personnel or division equipped to respond to a public safety TDoS.
- (U) Discuss with your telephone system engineers or technician possible configuration changes to isolate critical phone lines (incoming 9-1-1 calls for service). Prevent an overload of non-critical lines from rolling-over to lines answered by 9-1-1 call-takers.
- (U) Remind employees of their obligations to protect PII.

(U) During a TDoS attack:

- (U) Save the voice recording of suspects who may call before, during or after the TDoS attacks.
- (U) Record all telephone numbers and account information, if the caller is demanding payment(s) (e.g. start and stop time of the events, number of call per hour or per day, telephone numbers, any instruction on how to pay alleged debt, such as account number, call back number, etc.)
- (U) Retain all call logs and IP logs (if applicable).
- (U) Separate the affected telephone number from 9-1-1 and other critical trunks.

(U) Reporting a TDoS attack:

- (U) File a complaint with the FBI's Internet Crime Complaint Center (www.ic3.gov) and the National White Collar Crime Center (NWC3). Include the keywords *TDoS*, *PSAP*, and *Public Safety* in the description of the incident.
- (U) File a report with your local police department or sheriff's office. Law enforcement agencies can assist by coordinating with the local FBI field office and the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) at nccic@hq.dhs.gov.
- (U) Consolidate call logs and IP logs; mark for long-term retention.

(U) Reporting Notice

(U) The FBI encourages recipients of this document to report information concerning cyber activity to the FBI's 24/7 Cyber Watch (CyWatch) by telephone at 855-292-3937 or by e-mail at cywatch@ic.fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

(U) Administrative Note:

(U) This information in this product UNCLASSIFIED in its entirety, and is intended for release to the Healthcare and Public Health and Emergency Services Sector. Recommend distribution via the National Health-Information Sharing and Analysis Center (NH-ISAC) and the Emergency Management and Response-ISAC (EMR-ISAC).

(U) There is no additional information available on this topic at this time.