Homeland Security | Office of Intelligence and Analysis

NOTE

(U//FOUO) Cyber Criminals Combine Tactics for Extortion

17 October 2013

(U//FOUO) Prepared by the Office of Intelligence and Analysis (I&A), Cyber Intelligence Analysis Division, Cyber Intelligence Support Branch. Coordinated with the National Cybersecurity and Communications Integration Center and the National Coordination Center for Communications.

(U) Scope

(U//FOUO) This Note describes a new combination of tactics by cyber criminals that disrupts telephone systems of targeted organizations. This information is provided to assist and inform the Department and federal, state, local, territorial, tribal, and private sector partners in mitigation efforts regarding criminal activity that could affect their operations.

*(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 authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.*

(U) Key Judgment

(U//FOUO) Criminals are combining traditional extortion scams with telephony-based denial-of-service (TDoS) attacks for financial gain. We assess this tactic could be leveraged by malicious cyber actors to disrupt communications services related to critical infrastructure.

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

(U//FOUO) Criminals since at least January 2012 have attempted to extort money from military personnel and local government offices by employing a tactic commonly referred to as a "payday loan" scam. Law enforcement and open source reporting have detailed numerous incidents where criminals have obtained personal identifying information (PII) of potential victims to execute scams. In these instances, the criminals phone the employee's office and demand that the employee repay an alleged loan; if the victim does not comply, the criminals initiate TDoS attacks against the offices or organizations of the targeted employee. TDoS differs from other telephone disruptive techniques by the number of calls generated; by occupying lines continuously with repeated automated calls, the victim is prevented from making or receiving telephone calls. Criminal actors use robocalling as a TDoS tactic designed to block all incoming and outgoing phone calls.

(U) Robocalls

(U) Robocalls are unsolicited, auto-dialed, pre-recorded calls to landline and wireless phones. Legal robocalls from telemarketers must follow strict, prescribed sets of rules, allowing for a recipient to opt out of receiving any additional calls.

- (U//FOUO) The US Coast Guard (USCG) in late May 2013 reported that an individual called a USCG cutter claiming a crewmember was late on his loan payments. The subsequent TDoS attack flooded the ship's telephone network with several rounds of phone calls, completely disrupting phone service. The calls lasted from 1 to 15 minutes in length, and each round of calls lasted from 10 minutes to 2 hours. The targeted crewmember from the cutter had recently received notice from his bank that his accounts had been hacked and his PII had been compromised.

- (U//FOUO) Between 28 January and 3 March 2013, the public safety answering point (PSAP) for a south-central region sheriff's office received a request to repay the loan of an individual, whom the caller believed was an employee of the PSAP. A TDoS attack followed this request, disrupting business lines.

- (U//FOUO) Between 14 January and 6 March 2013, a south-central region state legislative office experienced a TDoS attack in which the caller requested a former employee by name and claimed the individual owed money. The TDoS attacks began after the legislative office refused to pay. The office received approximately 100 calls per minute, completely tying up the office's business lines.

(U) Public Safety Answering Point

(U) A PSAP is a central facility focused on receiving routine as well as emergency calls. The duties vary from state to state, however. Some centers are also responsible for dispatching emergency services.

(U//FOUO) In all incidents, individuals—not organizations—were the initial extortion targets, and the caller had information identifying them as current or former employees of the attacked organizations. The victims were likely selected for extortion through the exploitation of their PII. The TDoS activity against the south-central region PSAP and state legislative office may have been conducted by the same attacker as the description of the caller's voice and the sequencing of the disruptive activities were very similar.

(U//FOUO) Old Techniques, New Spin

(U//FOUO) Neither TDoS attacks nor payday loan scams are new. Their combination, however, represents a change in tactics for malicious actors.

(U//FOUO) FBI in December 2010 released information from the Internet Crime Complaint Center (IC3) regarding extortion attempts involving payday loans. In most instances, victims—who may or may not be behind on loan payments—were contacted by malicious actors who stated the actor was in a position of authority to collect on the victims' loans. The targeted victims were told they were late on payments and must make payments to avoid legal action. Victims were instructed on how to make the payments.

(U//FOUO) TDoS is not a sophisticated technique and is similar to employing robocall capability used by telemarketers, albeit on a much larger scale.

- (U//FOUO) Companies sell legitimate telemarketing auto-dialer software for $195 to $495. This software, when combined with a Voice over Internet Protocol (VoIP) line and used by malicious actors, can create a low-cost capability for criminal activity.

- (U//FOUO) Cyber criminals also advertise TDoS attack services on underground forums, with prices ranging from $30 per hour to $20 per day based on the length of the TDoS and the call density.

(U) Outlook and Implications

(U//FOUO) We judge malicious cyber actors will continue to target organizations through possible compromised PII and, even if the extortion demands are met, the TDoS attacks probably will persist with cyber actors demanding additional funds. (See Appendix for information regarding the best practices in the event of a TDoS attack.)

(U) Appendix: Best Practices Checklist Developed by Private Sector for Telephony-Based Denial-of-Service Attacks

(U//FOUO) DISCLAIMER: The industry practices reflected in this checklist were developed by various private sector organizations in response to TDoS attacks. They are provided here, with permission, for informational purposes only and to assist other entities and organizations in developing appropriately tailored protective and support measures against such attacks. This checklist is not exhaustive. Moreover, in providing it, the Department of Homeland Security makes no warranties of any kind regarding the information and practices contained within this checklist nor endorses any entity, product, or service referenced therein.

(U) Information continues to be received from multiple jurisdictions indicating the existence of ongoing attacks targeting the telephone systems of public sector entities. Over 200 such attacks have been identified to date. The perpetrators of the attack launched numerous phone calls against the targeted telephone network, tying up the system and preventing the agency from receiving legitimate calls. This type of attack is referred to as a TDoS, or telephony denial-of-service, attack.

(U) As a result of a cooperative effort between federal authorities, Association of Public-Safety Communications Officials, National Emergency Number Association, public safety representatives, and commercial service providers, the following checklist has been developed to assist the development of a continuity of operations plan for your agency.

(U) Before a TDoS event:

» (U) Discuss how to respond to a TDoS event with the service provider. These discussions might include both telephone service providers (9-1-1 and administrative phones, if separate providers) as well as 9-1-1 equipment vendors.

» (U) Ensure the Public Safety Telecommunicators and their supervisors have access to the phone number and direct contact information for the service provider’s personnel or division equipped to respond to a public-safety TDoS attack.

» (U) Discuss with the telephone system engineer or technician possible configuration changes to isolate critical phone lines (incoming 9-1-1 calls for service) from administrative and other lines, taking into account hunt groups, busy or no-answer rollover to other lines, rollover to other PSAPs, etc.* Prevent an overload of non-critical lines from rolling over to lines answered by 9-1-1 call-takers.

* (U) Hunt Group refers to a group of extensions that are organized to process specific calls. Upon answering a call, the Private Branch Exchange (PBX) automatic call distributor may transfer the call based upon the caller's Dialed Number Identification Service or automatic number identification (ANI) or extension. Likewise caller identification information (from an interactive voice response) may be used to direct the call to a particular group of agents. The term is derived from the concept that the PBX is programmed to "hunt" for the next available agent within in a specified extension group.

- (U) Remind employees of their obligation to protect PII and how to protect themselves from identity theft (for example, see http://www.consumer.ftc.gov/features/feature-0014-identity-theft). Additionally, if an attack were to occur at the agency, reassure the targeted employee that they are not responsible for the attack. They and the agency are merely victims of a highly sophisticated criminal enterprise.

(U) During a TDoS event:

- (U) Save the voice recording of suspects who may call before, during, or after the TDoS events.

- (U) If the caller is demanding additional information or phone numbers, refrain from providing this information. This may be the primary goal and may lead to additional TDoS attacks.

- (U) Record all phone numbers and account information. If the caller is demanding payment(s), attempt to capture the following information:

  - (U) Start and stop times of the events;
  - (U) Number of calls per hour or per day;
  - (U) Phone numbers and other ANI or automatic location identification information of the incoming calls;
  - (U) IP addresses, if applicable; and
  - (U) Any instructions for how to pay, such as account number, call-back phone number, etc.

- (U) Retain all call logs and IP logs for the time period of the attacks.

- (U) Attempt to separate the affected phone number from 9-1-1 and other critical trunks; work with the PBX provider/maintainer.

(U) After the event:

- (U) File a complaint with the IC3 at www.IC3.gov—co-sponsored by the FBI and the National White Collar Crime Center. Include the keywords “TDoS,” “PSAP,” and “Public Safety” in the description of the incident.

- (U) File a report with the local police department or sheriff’s office.

  - (U) If the investigator is unsure of how to proceed, there are resources available to assist. The FBI, Federal Communications Commission, and Federal Trade Commission are all engaged in this process, and the DHS National Coordinating Center for Communications, National Cybersecurity and Communications Integration Center can help coordinate information.

  - (U) Advise local law enforcement that the Communications Assistance for Law Enforcement Act protocol can be invoked, enabling service providers to collect data on the originator of the call and provide it to law enforcement resources.

- (U) Consolidate call logs and IP logs, marking them for long-term retention.

(U) Appropriate 9-1-1 centers and PSAPs should also share this information with other public safety facilities with which they interact, including private ambulance service dispatch centers, hospitals, air ambulance dispatch centers, etc.

(U) Reporting Computer Security Incidents

(U) To report a telephone denial of service incident, contact the Internet Crime Complaint Center (IC3), at http://www.ic3.gov and complete the IC3 Incident Reporting System form. The IC3 Complaint Reporting System provides a secure, web-enabled means of reporting suspected internet crimes or incidents to IC3.

(U) I&A invites you to participate in a brief customer feedback survey regarding this product. Your feedback is extremely important to our efforts to improve the quality and impact of our products on your mission. Please see below to access the form and then follow a few simple steps to complete and submit your response. Thank you.

(U) Tracked by: HSEC-1