MS-ISAC

MS-ISAC Security Primer

Telephony Denial of Service Attacks

March 2017, SP2017-0312

A Telephony Denial of Service (TDoS) attack is an attempt to make a telephone system unavailable to the intended user(s) by preventing incoming and/or outgoing calls. This is accomplished when an attacker successfully consumes all available telephone resources, so that there is no unoccupied telephone line. Hacktivists occasionally use TDoS attacks to annoy and harass a targeted agency. Malicious actors have previously used TDoS attacks as part of ransom demand by conducting a short TDoS against the targeted agency, then demanding payment to stop the TDoS. Occasionally, TDoS attacks are accidental, such as a mistake in a text message phishing (SMSishing) campaign that inadvertently directs respondents to call 9-1-1. Historically, malicious cyber actors used TDoS attacks to prevent a target from receiving notification of a pending, unauthorized financial transfer. Common targets include state, local, tribal, and territorial (SLTT) governments, high-ranking officials (e.g. mayors), law enforcement agencies, and Public Safety Answering Points (PSAPs). TDoS attacks may have a short duration or occur intermittently over several days.

RECOMMENDATIONS:

Preparing for a TDoS Attack

- Establish and maintain effective partnerships with your upstream telephony service provider and know what assistance they may be able to provide you in the event of a TDoS attack.
- Remind employees to protect themselves and the agency, by not responding to abusive statements and not providing personal information or information on internal agency functionality to the caller.
- Develop a plan to record the call information in case there is a threat or further investigation.
- Ensure you have a secondary means of communication, such as cellular telephones or radios, and notify potential affected employees of that means in advance.

During the Attack

- Limit the number of telephones that the attacked number rings on. When doing so, take into account busy and no answer roll-over functionality. If possible, limit the calls to one telephone and dedicate only one employee to answering that line. If it is a crucial line, use social media and other channels to advertise another line as being in service for that day.
- If crucial telephone numbers use the same telephone branch exchange (PBX), consider moving the crucial lines to a different, temporary PBX in case the PBX itself is targeted or overwhelmed.
- In some cases the calls may use an automated message. If that occurs and the message appears to be from a legitimate third party, contact the National Communication Center (NCC) as it may be possible the other party is also a victim and would be willing to disable the auto call functionality.
- Attempt to determine if the attack is meant as a distraction from another event, such as an unauthorized wire transfer

TDOS attacks should be documented with the local police department, the National Cybersecurity and Communications Integration Center (NCCIC) and/or the Internet Crime Complaint Center (IC3). When submitting a complaint, include keywords such as “TDOS,” “PSAP,” and "Public Safety,” and information such as call logs, date/time stamps, and originating telephone numbers.

The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation’s state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance for SLTT governments, is available at 866-787-4722, SOC@cisecurity.org, or https://msisac.cisecurity.org/. The MS-ISAC is interested in your comments - an anonymous feedback survey is available at: https://www.surveymonkey.com/r/MSISACProductEvaluation.

.