Telephony Denial of Service Attacks: Lessons Learned from a Public Safety Answering Point

Background

TDoS attacks occur when a large volume of telephone calls overloads a communications network element – overwhelming call capacity and disrupting communications.[1]

Throughout 2020 and 2021, a local public safety answering point (PSAP) responded to daily telephony denial of service (TDoS) attacks impacting operations. To date, these attacks have only impacted the agency's ten-digit non-emergency lines. These numbers are often provided to other agencies, alarm companies, and the public to report non-emergencies.

This case study document highlights the impacts, response, long-term recovery, and the lessons learned from one PSAP's experience with a TDoS attack.

Impacts

These attacks occur upwards of 12 times per day and are believed to be conducted by foreign actors. The time and number of occurrences vary day-to-day and consume valuable resources, including underlying technology resources and sometimes up to six personnel. During these TDoS attacks, the perpetrator engages a telecommunicator while simultaneously conferencing in additional telecommunicators, resulting in a confusing situation where multiple personnel are on the same call. During these incidents, the telecommunicator often hears ringing or a pre-recorded message. In some instances, the telecommunicator hears audio of a person talking or background noise, making it appear as if the call is from a real person. It is believed that the perpetrator sometimes conferences in other agencies as well. The audio is unclear forcing the telecommunicator to ask questions and stay on the line. During these incidents, multiple telecommunicators are conferenced in on the same call and recognize their co-workers' voices alerting them to the malicious nature of the call.

Response

Initially, the problem was reported to the agency's system administrator. The system administrator quickly contacted the agency's service provider for voice security to help mitigate the TDoS attacks. The attacks were then reported to the director of the agency, the county's security office, and the information technology (IT) department. Additionally, the PSAP director notified the county's IT department, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and surrounding jurisdictions for awareness. The PSAP also engaged with their

[1] CISA.gov, *Cyber Risks to 911: Telephony Denial of Service*, last accessed December 7, 2021.

Commercial Mobile Radio Service providers to get information on the call characteristics; however, they were unable to track the call or provide additional details.

The PSAP implemented a call authentication system appliance from a network security provider for primary and alternate devices in the path of the ten-digit ingress calls. Incoming primary rate interface circuits come into the building from a demarcation point, and from there, connect to the call handling equipment. The PSAP installed this TDoS mitigation appliance in "front" of the call handling equipment and established rules that inspect ingress calls. When certain characteristics of past attacks are met, the appliance addresses the call and keeps it from being passed into the call handling system so that personnel resources do not need to handle the call.

The PSAP does not have formal cybersecurity training for staff; however, the systems administrator engages with staff and supervisors to make them aware of the call characteristics and security capabilities to mitigate TDoS attacks.

Long-Term Recovery

The PSAP has not been able to trace the calls but continues to record TDoS incidents to help gather information about call patterns. Additionally, data collection is also assisted by e-mail notifications sent by the service provider to the systems administrator when the mitigation function is enacted.

Lessons Learned

Review policies and procedures on handling nuisance calls

Telecommunicators may be first to notice nuisance calls. However, they may be reluctant to disconnect from a 911 call for fear of consequences. Emergency communication centers (ECCs)/PSAPs should review policies and procedures to ensure they address nuisance calls. Agencies should also establish temporary standard operating procedures or guidance for responding to TDoS events. Finally, ECCs/PSAPs should ensure staff are familiar with policies and procedures for addressing nuisance calls.

Engage with service providers

ECCs/PSAPs should engage with service providers regularly. Service providers may be able to identify signs of an attack and mitigate the damage quickly while ECC/PSAP staff make other notifications and changes to their operations. Additionally, providers may be able to validate authenticity using call information.

Collaborate with neighboring jurisdictions to establish continuity of operations agreements with other ECCs/PSAPs to provide backup call capabilities during TDoS disruptions

ECCs/PSAPs should build relationships and engage with neighboring agencies to develop agreements and protocols to maintain operations in the event of a TDoS attack where service is disrupted. Larger ECCs/PSAPs may require mutual aid from centers of comparable size for backup call-handling assistance. ECCs/PSAPs should develop agreements and notification protocols with

neighboring jurisdictions to respond to service interruptions and establishing steps for notifying each other of an event to help mitigate consequences. ECCs/PSAPs should also develop plans to notify the public on how to request service in the event of a 911 outage.

Keep a detailed record of the attacks

ECCs/PSAPs should keep detailed records of attacks or attempts, including dates and times, the frequency, and a summary of the attack. This information can help establish call patterns, which may be valuable for service providers. This may also be helpful for investigative purposes and engaging with federal partners, such as the FBI and CISA.

Include ten-digit lines when implementing Next Generation 911 systems and security capabilities

TDoS attacks can occur on an agency's ten-digit non-emergency lines and implementing rules for blocking harassing calls may be necessary. ECCs/PSAPs should consider non-emergency lines, in addition to emergency lines, when implementing security capabilities.

Implement call authentication tools

ECCs/PSAPs should consider call authentication tools or services to screen calls for their validity. These tools can assist with call data verification to avoid overwhelming networks with nefarious calls.

For more information on this and other cybersecurity initiatives, contact ng911wg@cisa.dhs.gov. To learn more about TDoS, visit cisa.gov/publication/next-generation-911 or review the FBI's Private Industry Notice.