PROTECT YOUR ECC FROM TDOS

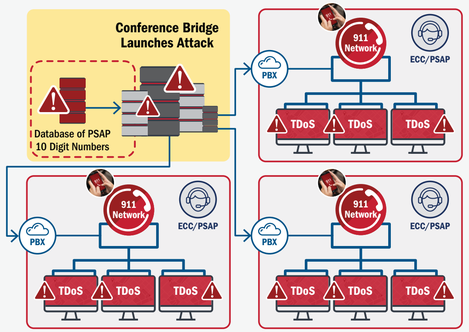
IOWA DEPARTMENT OF HOMELAND SECURITY AND EMERGENCY MANAGEMENT

TDOS: WHAT IS IT?

Telephony Denial of Service (TDoS) attacks occur when a large volume of telephone calls overloads a communications network element—overwhelming call capacity and disrupting communications.[1] At a glance, TDoS may appear to have no connection with cybersecurity. In reality, threat actors behind TDoS attacks rely on services such as mobile botnets[2] and Voice over Internet Protocol (VoIP)[3] to escalate the attacks through automated calling and caller identification spoofing. Many TDoS attacks also use social networks to encourage malicious calling campaigns.[4]

Across the US, emergency communications centers (ECCs) and public safety answering points (PSAPs) experience TDoS attacks of varying severity. Some attacks have lasted for days, others for only short periods of time. While initially focused only on administrative lines, the attackers have now managed to identify vulnerabilities that allow them direct access to 911. Such attacks intend to keep the distraction calls active as long as possible, which may delay or block legitimate calls for service. Delays due to TDoS attacks could lead to increases in emergency services response times and result in potentially dire consequences, including loss of life.[5]

WHAT DOES A TDOS ATTACK LOOK LIKE?



ADMINISTRATIVE LINES

The 10-digit phone number for your agency is usually available on a public-facing website. These numbers can be dialed from any locations globally.

ATTACK SCENARIOS:

Single Center Attack: Actors call the publicly available 10-digit number repeatedly, sometimes thousands of times. In some cases, the call volume is large enough to impact the public's ability to reach the targeted public safety agency.

Use of a Conference Bridge: The 10-digit number of numerous centers (sometimes in different states) are dialed simultaneously and the calls are placed in a conference bridge. This can cause confusion, as each answering center believes that the other agencies on the conference bridge have called them. The volume of calls can impact center operations.

911 LINES

911 is designed to be jurisdictional, meaning that in order to reach a specific 911 center, you should be physically within their jurisdictional boundaries.

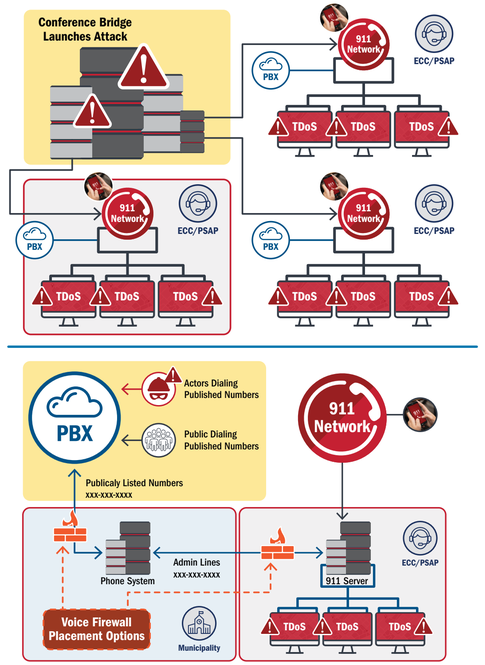
ATTACK SCENARIOS:

Hacked Business Phone System: Any business phone system that has minimal security is a potential target. After gaining control of the business phone system, hackers direct the compromised system to repeatedly call 911 via a conference bridge. When call takers answer, they find themselves on a conference call with numerous centers, often in other states. There are numerous reports of hackers gaining control of hospital phone systems to dial 911.

Directly Dialing 911 Lines: In certain areas where multiple centers share the same Telecommunications Central Office Switch (selective router),[6] 911 lines can be directly accessed by calling a 10-digit number. This configuration—the "dialable" function—allows centers to transfer calls to each other.

- The major vulnerability here is that these 10-digit numbers can be dialed from anywhere. Earlier this year, a Western state experienced a 911 attack against multiple centers, all bridged together, using this model. Depending on the volume of 911 calls generated, this could dramatically impact the public.

Using Voice over Internet Protocol (VoIP) Manual Address Feature: Hackers obtain a number of VoIP lines and then manually input a business address located within the jurisdiction of the targeted center. They can then dial 911 remotely. Once a specific TDoS attack is finished, the hackers modify the manual address feature to a different area code and launch another attack.



PROTECTING YOUR CENTER[7]

WORK WITHIN YOUR CENTER:

- ☐ Maintain call overflow reserve, adding additional call capacity on an as-needed basis to compensate for increased call volume
- ☐ Implement the National Institute of Standards and Technology Cybersecurity Framework (www.nist.gov/cyberframework) to improve cybersecurity posture
- ☐ Conduct cybersecurity assessments (e.g., CISA's Cyber Security Evaluation Tool www.cisa.gov/uscert/ics/Assessments), identify cybersecurity gaps and vulnerabilities, and determine appropriate cybersecurity standards

WORK WITH YOUR PARTNERS:

- ☐ Establish continuity of operations agreements with other ECCs/PSAPs to provide backup call capabilities during TDoS disruptions
- ☐ Engage with community partners to maintain and secure devices, as well as share inventory of programmed landlines with other ECCs/PSAPs
- ☐ Coordinate with private sector partners, such as telecommunications service providers, to prepare for TDoS events, including identifying technical solutions and recovery activities
- ☐ Work with telecommunications providers to ensure that the organization's 911 trunk lines are non-dialable

CONSIDER EXTERNAL RESOURCES:

- ☐ Consider deployment of a TDoS mitigation solution, such as a voice firewall, which can detect and mitigate call overload on administrative telephone lines; this device has the ability either to manually block calls or, using a defined threshold, block a specific number if it calls repeatedly within a defined timeframe[8]
- ☐ Plan for transition to Next Generation 911 (NG911), where the Emergency Service IP Network (ESInet) offers separate alternate routes to ECC/PSAP call handling and may offer additional authentication capabilities, thus enabling operations continuity during natural and man-made disasters like TDoS

IF YOU BELIEVE YOUR CENTER IS UNDER A TDOS ATTACK

- ☐ Contact your telecommunications service provider and report the 10-digit number(s) involved in the attack; request the specific steps required to have these calls blocked
- ☐ If the volume of TDoS calls impacts center operations, alert the public and share alternative assistance methods (e.g., text-to-911)
- ☐ If the TDoS attack is affecting 911 lines, notify any neighboring ECCs/PSAPs that provide backup to your center and direct your telecommunications provider to disable 911 call overflow; this will prevent other centers from being affected

IMPORTANT CONTACTS

Call takers may notice bizarre circumstances, and these may be the first indications of a TDoS attack. To report these activities, please contact your state and federal authorities:

STATE OF IOWA

- **Office of the Chief Information Officer (OCIO) Information Security Officer**
  855-442-4357 and 515-725-1296
- **Iowa 911 Program**
  515-725-3231
  (Ask for the Duty Officer or 911 Program Manager)

FEDERAL PARTNERS

- **FBI Omaha Field Office:**
  (402) 493-8688
- **FBI Cyber Task Forces: http://www.fbi.gov/contact-us/field**
- **FBI Internet Crime Compliant Center (IC3): www.ic3.gov**
- **Cybersecurity and Infrastructure Security Agency (CISA):**
  (888) 282-0870 www.cisa.gov

This product was supported by DHS CISA through the Interoperable Communications Technical Assistance Program.

FOOTNOTES:

1. Cybersecurity and Infrastructure Security Agency (CISA), "Cyber Risks to 911: Telephony Denial of Service," June 4, 2020, cisa.gov/publication/next-generation-911.
2. Networks of compromised devices remotely controlled by malicious software. cisa.gov/publication/next-generation-911
3. Internet Protocol-enabled service that allows for calls to be dialed via internet connection instead of an analog phone line. fcc.gov/general/voice-over-internet-protocol-voip
4. Federal Bureau of Investigation, "Public Service Announcement – Telephony Denial of Service Attacks Can Disrupt Emergency Call Center Operations," February 17, 2021, ic3.gov/Media/Y2021/PSA210217.
5. FBI, ibid.
6. Selective routing and "Selective Router" refer to the routing and equipment used to route a 911 call to the proper ECC/PSAP based on the number and location of the caller. Selective routing is derived from the Electronic Serial Number "burned" in the cellular telephone by the manufacturer. Routing relies on the Emergency Service Number (ESN) for the location of the access line from which the 911 call was placed.
7. CISA, ibid.
8. In addition to these capabilities, a voice firewall can offer services that keep a current database of known 'bad numbers,' preventing future calls from the same numbers from entering the center. The firewall could also provide an option to utilize "STIR/SHAKEN" protocol to authenticate calls. The authentication is especially useful when an ECC/PSAP receives a swatting call as call takers could inform responding law enforcement of the fact that the swatting report may not be real. Fake swatting calls are typically placed via administrative lines. For more on call authentication, see fcc.gov/call-authentication.