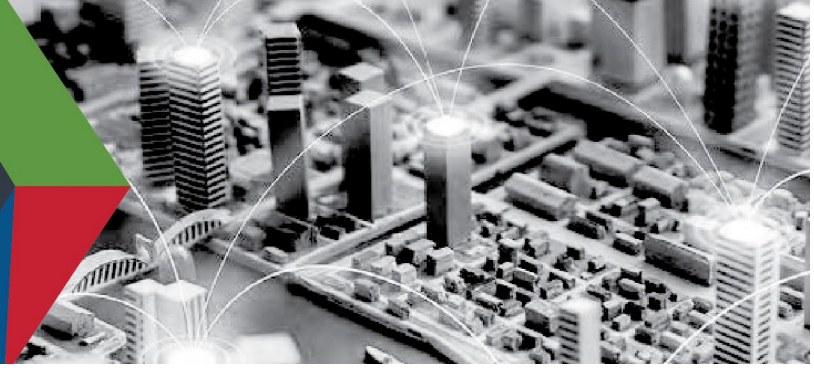
DEFEND TODAY, SECURE TOMORROW



CYBER RISKS TO 911: TELEPHONY DENIAL OF SERVICE

Telephony Denial of Service (TDoS) events occur when a large volume of telephone calls overloads a communications network element—overwhelming call capacity and disrupting communications. Congestion may occur in any part of a communications network, from the telecommunications provider infrastructure to end-user equipment. Whether malicious (e.g., cyber attack) or accidental (e.g., malfunctioning equipment), TDoS events present a unique challenge for public safety stakeholders, specifically emergency communications centers (ECCs)/public safety answering points (PSAPs). This risk, as outlined in Figure 1, can result in disruptions to call answering capabilities and severely impede a jurisdiction's ability to provide emergency response services.

Threat	Vulnerability	Consequence	Risk
Overwhelming volume of calls or sessions to a network element	Operational or technical deficiency that enables a cyber incident	Degradation or disruption of 911 call answering capabilities	Exploitation of vulnerabilities to disrupt or degrade 911 service

Figure 1: Public Safety Communications TDoS Risk

TDoS events can originate from both mobile and fixed-line voice communications systems. Malicious actors may employ a variety of tools to launch TDoS events, including mobile phones, botnets, Voice over Internet Protocol (VoIP) services, compromised private branch exchanges (PBXs), or preprogrammed landline phones. Both 911 and the 10-digit numbers served by ECC/PSAPs can suffer TDoS events. Events affecting 911 numbers originate within the PSAP service area, while events affecting the 10-digit numbers can originate from anywhere. Using this document, ECC/PSAP administrators may familiarize themselves with common TDoS events vectors and best practices to protect networks.

MOBILE PHONES AND BOTNETS

Mobile phones may facilitate TDoS events, commonly using non-subscriber phones or mobile robot networks, known as botnets. All mobile service providers must connect 911 calls, even if a phone is disconnected from cellular service (i.e. non-subscriber). Non-subscriber mobile phones may not provide detailed identifying or location information to ECCs/PSAPs, obscuring the origin of calls. Large numbers of inexpensive used or pre-paid phones can enable a TDoS events. A mobile botnet is a network of compromised devices remotely controlled by malicious software. Mobile botnets automate TDoS, enabling malicious actors to continuously dial 911 from many devices. Depending on the number of infected devices, mobile botnets can disrupt call answering capabilities in multiple geographic areas.

Arizona Mobile Botnet TDoS

In 2017, Arizona authorities sentenced an individual for instigating a TDoS event against Phoenix area ECCs/PSAPs. The individual used social media to distribute malicious software onto unsuspecting users' mobile devices. Infected devices began repeatedly calling 911 without user knowledge, disrupting call capabilities at local ECCs/PSAPs.

CONNECT WITH US
www.cisa.gov

For more information about this subject, email: PublicSafetyComms@cisa.dhs.gov

Linkedin.com/company/cybersecurity-and-infrastructure-security-agency

@cisa.gov | @cyber | @uscert_gov

Facebook.com/CISA

VOICE OVER INTERNET PROTOCOL

VoIP provides telephone service through Internet Protocol (IP) networks (e.g., the Internet). VoIP services often depend on a dedicated phone number for emergency services, providing ECCs/PSAPs with a fixed street address when dialed. The VoIP emergency phone number ensures users connect with their local first responders. Unlike a physical landline connection, VoIP customers can subscribe to phone numbers in any geographic area. A malicious actor may subscribe to phone numbers in different geographic areas to target specific ECCs/PSAPs, obscuring the origin of the event.

Malicious actors may also exploit VoIP services to spoof caller identification services. Caller identification spoofing enables perpetrators to make incoming calls appear to originate from a different number. Malicious actors may use spoofing techniques to make a large volume of incoming calls appear to originate from a trusted number, bypassing cybersecurity controls that may otherwise block suspicious traffic.

COMPROMISED PRIVATE BRANCH EXCHANGES

Private business telephone switching systems, such as PBXs, may be compromised to automatically dial local ECCs/PSAPs. PBXs may be in a business/government facility or hosted on an IP network, which increases vulnerability to physical tampering, malfunction, or cyber attack. Large PBXs in particular can place a substantial volume of concurrent calls to local ECCs/PSAPs.

PREPROGRAMMED LANDLINES

Local jurisdictions may require private and non-profit sector organizations to maintain landline phones preprogrammed to call 911 (e.g., elevators, pools). For instance, preprogrammed phones are often publicly accessible with highly variable security and maintenance standards. Malicious actors may physically or electronically tamper with these preprogrammed phones to initiate a TDoS events on a local ECC/PSAP. In addition, poorly maintained devices may malfunction and accidentally flood ECCs/PSAPs with false positive emergency calls.

Texas Preprogrammed Landline TDoS

In 2017, a preprogrammed landline phone in a Houston-area hotel elevator malfunctioned. The device continuously dialed 911 over a 10-hour period, placing thousands of calls to local ECCs/PSAPs. The large volume of calls disrupted voice communications capabilities, preventing ECCs/PSAPs from receiving legitimate emergency calls. Local public safety officials eventually used call location information to track down and repair the malfunctioning device. While ruled an accident, malicious actors may exploit unsecured devices to initiate TDoS events.

MITIGATION BEST PRACTICES

The Cybersecurity and Infrastructure Security Agency (CISA) is engaging with ECCs/PSAPs, trade associations, and private-sector partners to tailor cybersecurity solutions and best practices for public safety communications users and system administrators. CISA also partnered with SAFECOM and the National Council of Statewide Interoperability Coordinators to publish the Cyber Risks to Next Generation 911. The report provides an overview of Next Generation 911 systems and best practices, empowering public safety communications partners to improve their cybersecurity posture for 911 systems. Table 1 outlines best practices ECCs/PSAPs may consider adopting to reduce the impact of TDoS threats.

Table 1: Best Practices to Mitigate TDoS Risk

Threat	Best Practices
Mobile Phones, Botnets, VoIP, and PBX	Maintain call overflow reserve, adding additional call capacity on an as-needed basis to compensate for increased call volume
	Establish continuity of operations agreements with other ECCs/PSAPs to provide backup call capabilities during TDoS disruptions
	Consider deployment of a TDoS mitigation solution, which can detect and mitigate call overload on administrative and 911 telephone lines
	Coordinate with private-sector partners, such as telecommunications service providers, to prepare for TDoS events, including identifying technical solutions and recovery activities
	Implement the National Institute of Standards and Technology Cybersecurity Framework to improve cybersecurity posture
	Conduct cybersecurity assessments, identify capability gaps and vulnerabilities, and determine appropriate cybersecurity standards
Preprogrammed Landlines	Engage with community partners to maintain and secure devices, as well as share inventory of preprogrammed landlines with ECCs/PSAPs

REPORTING

If your organization is experiencing a TDoS event, *immediately* contact telecommunications service providers and federal partners for assistance. In addition, alert the public and share alternative assistance routes. Table 2 identifies federal organizations for assistance, depending on the incident, as well as reporting guidance for TDoS events.

Table 2: Federal Resources and Reporting TDoS

Federal Partner	Component	When to Report
CISA	CISA Central	Suspected or confirmed cyber incidents that may impact critical infrastructure and require technical response or mitigation assistance
Federal Bureau of Investigation (FBI)	FBI Field Offices	Cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity
	Cyber Task Forces	
	Law Enforcement Enterprise Portal	
United States Secret Service	Secret Service Field Offices	Cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card and other financial payment information
	Electronic Crimes Task Forces	