# Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

19 August 2022

PIN Number

LD20220819-001

*The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS/CISA.*

*This PIN has been released* **TLP: AMBER**

**Please contact the FBI with any questions related to this Private Industry Notification via your local FBI Cyber Squad.**

www.fbi.gov/contact-us/field-offices | **E-Mail:** cywatch@fbi.gov | **Phone: 1-855-292-3937**

# Update: Telephony Denial of Service Attacks Can Disrupt Emergency Communications Center Operations

## Summary

The FBI is providing information regarding tactics used in Telephony Denial of Service (TDoS) attacks directed at Emergency Communication Centers (ECCs) across the United States, which include public safety answering points (PSAPs), public safety communication centers (PSCCs), emergency operations centers (EOCs), and other PSCCs. This information is an update to a previously released Private Industry Notification (PIN). Actors direct these attacks at both 9-1-1 lines and 10-digit administrative/non-emergency lines used by the public to request aid from local first responders.

## Threat

A TDoS attack is an attempt to make a telephone system unavailable to intended user(s) by preventing incoming and/or outgoing calls. Actors use various TDoS methods to disrupt ECC operations. By keeping the distraction calls active for as long as possible, the victim telephone system may be overwhelmed, delaying or blocking legitimate calls for service.

As of June 2022, ECCs have observed the following TDoS tactics affecting both administrative lines and the 9-1-1 lines:

- Continuously calling 9-1-1 or the 10-digit numbers of a specific ECC, sometimes for hours at a time.
- Calling multiple ECCs—often in different states—simultaneously and conferencing these ECCs together. This can cause confusion, occupy ECC personnel, and potentially prevent the public from accessing emergency services during crises.
- Verbally threatening ECC personnel during a TDoS attack.

**Administrative Lines**

ECCs typically integrate the publicly-listed 10-digit phone numbers for their agency (administrative lines) into the 9-1-1 call-handling equipment, allowing the same personnel to answer emergency and non-emergency calls. As a result, TDoS attacks against administrative lines can impair 9-1-1 operators' ability to handle both administrative and 9-1-1 calls. TDoS attacks against administrative lines are easier to carry out because TDoS actors can dial an ECC's publicly-listed 10-digit number from any location, including from other countries.

**9-1-1 Lines**

Due to the nature of a 9-1-1 network's ability to connect any caller to an ECC serving their geographic location, an ECC should only receive 9-1-1 calls that originate locally.

The FBI has received reports of TDoS actors employing the following methods to call 9-1-1 lines from areas outside of the ECC's jurisdiction:

- *Direct dial:* Actors obtain the unlisted 10-digit phone numbers associated with an ECC's 9-1-1 lines and dial them remotely, bypassing the location-based routing of the 9-1-1 system.
- *Business phone systems*: Actors hack into a business phone system located in a specific jurisdiction and use the hacked phone system to repeatedly dial 9-1-1; actors have used hospital phone systems in this manner. Actors sometimes connect multiple victims via a conference bridge during a TDoS attack where ECC staff answering 9-1-1 lines sometimes find themselves connected to other ECCs, often in other states.
- *Voice over Internet Protocol (VoIP) lines:* VoIP lines allow users to manually change their listed physical address in the VoIP service provider's database. This address is used for routing 9-1-1 calls. TDoS actors use this feature to attack an ECC remotely by listing their physical address as a valid address within the ECC's jurisdiction.

## Recommendations

In addition to the recommendations presented in *20210217-001 TLP: WHITE, Telephony Denial of Service Attacks Can Disrupt Emergency Call Center Operations*, ECCs should consider the following:

**Technical Recommendations for Administrative/Non-Emergency Lines**

- Consider installing a voice firewall product on administrative lines. Voice firewalls can be configured to mitigate TDoS attacks by identifying calls occurring beyond a reasonable frequency (e.g., blocking calls from a phone number that calls more than 20 times in 30 seconds). Voice firewalls also allow the ECC to manually block any number and can block known spam and robocall phone numbers, preventing them from entering the ECC call queue. Voice firewalls may also offer a call authentication service to identify "spoofed" phone numbers, sometimes used by actors during TDoS, "swatting," and other fraudulent calls. Voice firewalls can create alerts to notify ECC personnel when any action is taken, such as each time an incoming TDoS call is identified or blocked.

**Technical Recommendations for 9-1-1 Systems**

- Work with the 9-1-1 call-handling vendor to configure an Interactive Voice Response (IVR) for activation during a TDoS attack. The IVR would require a human response, such as 'Please dial 1 to continue.'
- Work with the 9-1-1 call handling vendor to allow the ability to route incoming wireline and VoIP calls to separate terminals. Because TDoS attacks often employ only wireline or VoIP, routing each call type to a separate terminal can prevent the attack from affecting all 9-1-1 call takers/telecommunicators.
- ECCs using legacy 9-1-1 systems should contact their 9-1-1 service provider and ensure their 9-1-1 lines are configured to block calls coming in from someone directly dialing the unlisted 10-digit number.
- ECCs using Next Generation 9-1-1 (NG911) systems should ask their NG911 service provider about availability of a planned feature to allow ECC personnel to use the 911 call taker/telecommunicator dashboard to specify phone numbers to be blocked.

**Preparedness Recommendations for both Administrative Lines and 9-1-1 Systems**

- Discuss TDoS risks and countermeasures with other ECCs. Share information on threats, countermeasures, and best practices.
- Conduct cybersecurity assessments of 9-1-1 systems and networks to help identify threats. The Cybersecurity and Infrastructure Security Agency (CISA) offers a range of

no-cost cybersecurity assessments to federal, state, local, tribal, and territorial governments, critical infrastructure, and federal agency partners to help identify cybersecurity threats and vulnerabilities. Additional information may be found at: *Cyber Resiliency Resources for Public Safety Fact Sheet*.

- Consider transitioning to NG911 where the Emergency Service Internet Protocol Network (ESInet) may offer separate alternate routes to ECC call handling and enhanced authentication capabilities.
- Contact service providers to discuss their communication systems and how best to respond to a TDoS attack, including technical solutions and recovery options. Ensure 9-1-1 call takers/telecommunicators and their supervisors have the direct contact information for the service provider personnel designated to respond to a public safety agency during a TDoS attack.

**What To Do If You Are Under Attack**

ECCs should:

1. Immediately contact your telecommunications service providers for assistance.
2. Notify the public and share alternative methods for contacting the ECC (e.g., text-to-9-1-1, social media page, alternative telephone numbers).
3. File a report with your local FBI field office or via the Internet Crime Complaint Center.
4. Contact CISA for incident response and mitigation guidance.

## Resources

- *Cyber Risks to 911: TDoS Fact Sheet*
- *SAFECOM Transition to NG911 Webpage*
- *Public Safety Communications and Cyber Resiliency Toolkit*
- *Cyber Resiliency Resources for Public Safety Fact Sheet*

## Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or by submitting a complaint via the Internet Crime Complaint Center, the FBI's 24/7 Cyber Watch (CyWatch), or eGuardian (available via LEEP). Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. CyWatch can be contacted by phone at 855-292-3937 or by e-mail at CyWatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

## Administrative Note

This product is marked **TLP: AMBER**. The information in this product may be shared with members of your organization, and with clients and customers who need to know the information to protect themselves or prevent future harm. This document should be distributed to all US ECCs but should not be posted to any portal where individuals outside the Emergency Services Sector can access it.