Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

17 February 2021

PIN Number
20210217-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field-offices

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

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 has been coordinated with DHS-CISA.

This PIN has been released **TLP: WHITE**: Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Telephony Denial of Service Attacks Can Disrupt Emergency Call Center Operations

Summary

The Federal Bureau of Investigation is issuing this PIN to provide awareness regarding Telephony Denial of Service (TDoS) attacks. TDoS attacks affect the availability and readiness of 911 call centers and can undermine public trust in emergency services.

Threat Overview

What is A TDoS Attack?

A TDoS attack is an attempt to make a telephone system unavailable to the intended user(s) by preventing incoming and/or outgoing calls. The objective is to keep the distraction calls active for as long as possible to overwhelm the victim's telephone system, which may delay or block legitimate calls for service. The resulting increase in time for emergency services to respond may have dire consequences, including loss of life.

TDoS attacks have evolved from manual to automated. Manual TDoS attacks use social networks to encourage individuals to flood a particular number with a calling campaign.

An automated TDoS attack uses software applications to make tens or hundreds of calls, simultaneously or in rapid succession, to include Voice Over Internet Protocol (VOIP) and Session Initiation Protocol (SIP). Numbers and call attributes can be easily spoofed, making it difficult to differentiate legitimate calls from malicious ones. [a]

TDoS services and tools are widely available to actors with all levels of experience. The proliferation and low cost of VOIP software allows cyber actors to conduct the attacks with minimal preparation and equipment.

TDoS Attacks at Critical Call Centers

Public Safety Answering Points (PSAPs) are call centers responsible for connecting callers to emergency services, such as police, firefighting, or ambulance services. PSAPs represent key infrastructure that enables emergency responders to identify and respond to critical events affecting the public.

TDoS attacks disrupt the ability to request emergency services, posing a genuine threat to public safety, especially if used in conjunction with a physical attack. Implementing safeguards can help ensure disruptions are contained as much as possible, and emergency operations are not completely halted.

TDoS Actors' Motives

TDoS attacks can be rooted in hacktivism, financial gain or harassment. Hacktivists might use computer network exploitation to advance their political or social causes. Malicious actors may initiate a TDoS attack in order to extort municipalities for financial gain. Malicious actors may also use TDoS attacks to harass call centers and distract operators, regardless of harmful effects. These attacks may be accompanied by messaging on social media platforms to increase the severity.

[a] SIP is a signaling protocol used for initiating, maintaining, and terminating real-time sessions that include voice, video and messaging applications. VOIP is a technology that allows voice calls to be made using broadband Internet.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Recommendations

Before a TDoS Attack

- Prepare in advance: create a written Incident Response Plan for TDoS and other cyber-attacks, or other non-malicious critical infrastructure disruptions.
- Establish continuity of operations agreements with other PSAPs to provide redundancy and backup capabilities.
- Consult with your telephone systems engineer on ways to protect your system from a TDoS attack. Consider configuration changes to isolate critical phone lines (incoming 9-1-1 calls for service), and prevent an overload of non-critical lines from rolling over to lines answered by 9-1-1 call-takers.
- Conduct cybersecurity assessments, identify capability gaps and vulnerabilities, and determine appropriate cybersecurity standards.
- Consider deployment of a TDoS mitigation solution, which can detect and mitigate call overload on administration and 911 telephone lines.
- Contact your telephone service provider to discuss your communication system and how best to respond to a TDoS attack, including identifying technical solutions and recovery activities. Ensure the Public Safety Telecommunicators and their supervisors have access to the direct contact information for the service provider's personnel or division equipped to respond to a public safety TDoS.

During a TDoS Attack

- Save the voice recording of suspects who may call before, during or after the TDoS attacks.
- Record all telephone numbers and account information, and details of any demands (e.g. start and stop time of the events, number of calls per hour or per day, details of any payment demands, such as account numbers, call back numbers, etc.)
- Retain all call logs and IP logs (if applicable).
- Separate the affected telephone number from 9-1-1 and other critical trunks.

Reporting a TDoS Attack

- File a report with your local law enforcement agency, which can assist by coordinating with the FBI Field Office to report the attack.
- File a complaint with the Internet Crime Complaint Center (www.IC3.gov). When filing a complaint, be sure to use the key words TDOS, PSAP, and Public Safety in the incident description.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 CyberWatch (CyWatch). 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. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

For comments or questions related to the content or dissemination of this product, contact CyWatch.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey