Public Service Announcement

FBI & CISA

Alert Number: I-073124-PSA

July 31, 2024

Just So You Know: DDoS Attacks Could Hinder Access to Election Information, Would Not Prevent Voting

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are issuing this announcement to raise awareness that Distributed Denial of Service (DDoS) attacks on election infrastructure, or adjacent infrastructure that support election operations, could hinder public access to election information but would not impact the security or integrity of election processes.

These low-level attacks, which are expected to continue as we approach the 2024 U.S. general election, could disrupt the availability of some election-related functions, like voter look-up tools or unofficial election night reporting, during the election cycle but will not impact voting itself. Threat actors may falsely claim that DDoS attacks are indicative of a compromise related to the elections process as they seek to undermine confidence in U.S. elections. In recent years, DDoS attacks have been a popular tactic used by hacktivists and cyber criminals seeking to advance a social, political, or ideological cause.

DDoS attacks occur when malicious cyber actors flood a public-facing, internet-accessible server with requests, rendering the targeted server slow or inaccessible. This temporarily prevents legitimate users from accessing online information or resources, such as web pages and online services, and may disrupt business activities for a period of time. Specific to elections, DDoS attacks targeting election infrastructure could prevent a voter from accessing websites containing information about where and how to vote, online election services like voter registration, or unofficial election results.

In the event that foreign actors or cyber criminals conduct DDoS attacks against election infrastructure or other infrastructure supporting election administration, the underlying data and internal systems would remain uncompromised, and anyone eligible to vote would still be able to cast a ballot. In the past, cyber actors have falsely claimed DDoS attacks have compromised the integrity of voting systems to mislead the public that their attack would prevent a voter from casting a ballot or change votes already cast. The FBI and CISA have no reporting to suggest a DDoS attack has ever prevented an eligible voter from casting a ballot, compromised the integrity of any ballots cast, or disrupted the ability to tabulate votes or transmit election results in a timely manner.

In addition to direct communication channels such as official websites, election offices across the country have identified alternative channels to disseminate information to voters, such as traditional news outlets, direct messaging to voters, and other backup resources. Election officials have multiple safeguards, backup processes, and incident response plans to limit the impact of and recover from a DDoS incident with minimal disruption to election operations.

Recommendations:

The FBI and CISA recommend voters take the following precautions:

- Seek out information from official sources, such as state and local election officials, about registering to vote, polling locations, voting by mail, and final election results.
- If the official website for your election office is unavailable contact your state or local election official.
- Remember that DDoS attacks cannot impact the security or integrity of the actual election systems.

CISA and the FBI coordinate closely with federal, state, and local election partners and provide services and information to safeguard U.S. voting processes and maintain the resilience of U.S. elections. The FBI is responsible for investigating and prosecuting election crimes, malign foreign influence operations, and malicious cyber activity targeting election infrastructure and other U.S. democratic institutions. CISA, as the Sector Risk Management Agency for Election Infrastructure, helps critical infrastructure owners and operators, including those in the election community, ensure the security and resilience of election infrastructure from physical and cyber threats.

Victim Reporting and Additional Information

The FBI and CISA encourage the public to report information concerning suspicious or criminal activity, such as DDoS attacks, to their local FBI field office (www.fbi.gov/contact-us/field-offices-offices), by calling 1-800-CALL-FBI (1-800-225-5324), or online at ic3.gov.

DDoS attacks impacting election infrastructure can also be reported to CISA by calling 1-844-Say-CISA (1-844-729-2472) or emailing report@cisa.dhs.gov. For additional assistance to include common terms and best practices, such as media literacy, please visit the following websites:

- Protected Voices: www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices;
- Election Crimes and Security: www.fbi.gov/scams-and-safety/common-scams-and-crimes/election-crimes-and-security.
- CISA #Protect2024: https://www.cisa.gov/protect2024