Distributed Denial of Service Attacks Could Hinder Access to Voting Information, Would Not Prevent Voting

ic3.gov/media/2020/200930.aspx

September 30, 2020 (2020-09-30T10:00:00-04:00)

Alert Number

I-093020-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

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

The FBI and CISA are issuing this PSA as a part of a series on threats to the 2020 election to enable the American public to be prepared, patient, and participating voters.

The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) are issuing this announcement to raise awareness that Distributed Denial of Service (DDoS) attacks on election infrastructure can hinder access to voting information but would not prevent voting.

DDoSs are common cyber-attacks that can slow or render election-related public-facing websites inaccessible, which could hinder voters' ability to access voting information or voting results. A DDoS attack occurs when attackers flood a public-facing, Internet accessible server with requests, rendering the targeted server slow or inaccessible. This prevents users from accessing online resources, such as web pages and online accounts, and may disrupt business activities for a period of time.

The public should be aware that if foreign actors or cyber criminals were able to successfully conduct DDoS attacks against election infrastructure, 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 in an effort 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 a registered voter from casting a ballot, or compromised the integrity of any ballots cast.

The FBI and CISA have worked closely with election officials across the country to identify alternative channels to disseminate information to voters, such as verified social media accounts, traditional media, and other backup resources. Election officials have multiple safeguards and plans in place to limit the impact and recover from a DDoS incident with minimal disruption to the voting process.

Recommendations

- Seek out information about how to vote and polling place information prior to Election Day.
- Seek out information from trustworthy sources, verify who produced the content, and consider their intent.
- Rely on state and local government election officials for information about registering to vote, polling locations, voting by mail, and final election results.
- Determine where to vote before Election Day.
- Verify the web address of legitimate websites and manually type the address into your browser.
- Do a quick search for other reliable sources before sharing a controversial or emotionally charged article, post, tweet, or meme you read. Studies show that being well informed requires getting information from many places. If it isn't from a credible source or if you can't find a second reliable source, don't share it.

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 helps critical infrastructure owners and operators, including those in the election community, remain resilient against physical and cyber threats. The FBI and CISA provide services and information to uphold the security, integrity, and resiliency of the U.S. electoral processes.

Victim Reporting and Additional Information

The FBI encourages the public to report information concerning suspicious or criminal activity to their local field office (www.fbi.gov/contact-us/field-offices) or to the FBI's Internet Crime Complaint Center (www.ic3.gov). For additional assistance, best practices, and common terms, 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
- #Protect2020: www.cisa.gov/protect2020