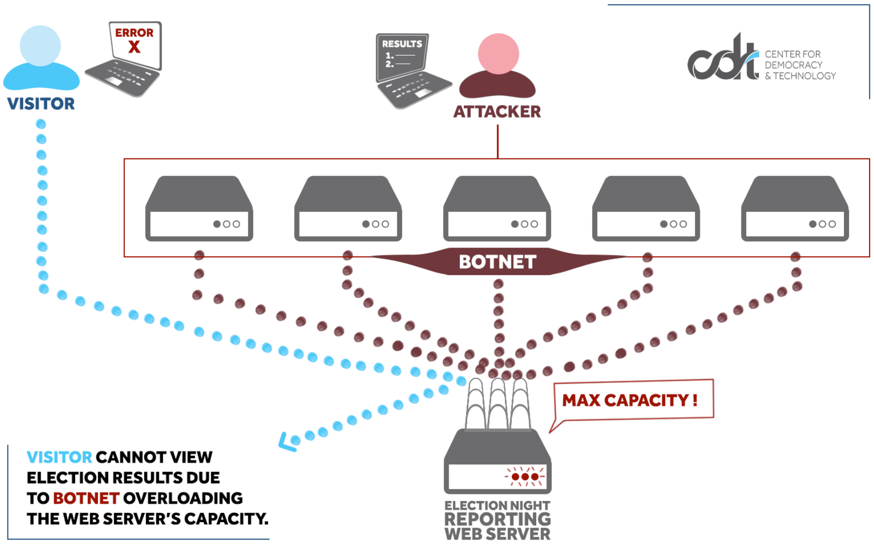
CENTER FOR
DEMOCRACY
& TECHNOLOGY

ELECTIONS
Short, simple, usable guides to help election administrators and staff better understand key concepts in cybersecurity.
VOL 3

DDoS

[Keeping Your Website Available Online]

- ➢ The greatest benefit of making certain parts of the election process available online is efficiency: it makes it faster and easier to register to vote, verify the status of a mail-in ballot, and check results on election night. Unfortunately, connecting those systems to the Internet also makes them targets for malicious actors looking to disrupt the election process by blocking access to election-related websites. A very effective method to block access to a website is to overwhelm the website's server with requests from fake visitors. When too many requests are sent to the website server other requests from legitimate visitors are turned away (or denied). **It is the digital equivalent of crowds of shoppers trying to rush into a retail store the day after Thanksgiving** – there are only so many doors into the store and that prevents everyone from entering at the same time. When this happens maliciously it is known as a Denial-of-Service (DoS) attack.


VISITOR
ERROR X
RESULTS 1. 2.
ATTACKER
CENTER FOR DEMOCRACY & TECHNOLOGY
BOTNET
MAX CAPACITY !
ELECTION NIGHT REPORTING WEB SERVER

VISITOR CANNOT VIEW ELECTION RESULTS DUE TO BOTNET OVERLOADING THE WEB SERVER'S CAPACITY.

- ➢ Generating enough requests to simulate traffic that is thousands of times larger than normal requires a lot of computers. When a malicious actor controls a large number of computers (a botnet) making repeated requests it is called a Distributed Denial-of-Service (DDoS) attack. A **DDoS Mitigation service can act as a shield and a filter** to block the large number of malicious requests while still allowing legitimate visitors to access your website normally.

- ➢ This kind of attack happened to Knox County, TN in their 2018 primary when its election night results reporting website was overwhelmed by both legitimate and malicious traffic due to interest in a popular mayoral race. No votes were changed but the **perception that the "election system was down" raised concerns** in voters locally and nationally that a larger attack was underway.

[Why DDoS Mitigation is Important]

- ➢ DDoS attacks will remain a critical threat to public-facing election systems for the foreseeable future because the attacks are **easy to start and very difficult (sometimes impossible) to withstand** for more than a few hours or a couple days, given the very large amount of traffic they can generate. Malicious actors can infect insecure computers and IoT devices (such as security cameras and DVRs) in order to control and direct them to attack a target. Improving DDoS defenses is the only practical way slow the effectiveness of this kind of attack until computers and IoT devices become more secure by default.

- ➢ Having DDoS Mitigation in-place before an attack helps establish a baseline for normal activity so that spikes in traffic or requests from unusual locations can be identified. Passing along that technical data through **information sharing coalitions** like the MS-ISAC or EI-ISAC can give other jurisdictions a heads-up about suspicious activity, and give them precious information and time for their own response.

[What Are Your Options]

- **Cloudflare: Project Athenian**
  - Web Application Firewall (WAF) uses continuous monitoring to block malicious traffic
  - Available for free to officials who run a state, county, or municipal election website
  - Access to “Under Attack” emergency support engineer and 24/7/365 phone/email/chat support
- **Jigsaw: Project Shield**
  - Blocks malicious traffic and redirects visitors to a copy of the website saved onto Google’s servers
  - Available for free to news websites, human rights websites, political organizations, and elections monitoring websites with a Google account
  - Jigsaw is part of Google’s parent company, Alphabet
- **Akamai: Enterprise Threat Protector**
  - DDoS protection using a recursive DNS-based solution that proactively identifies, blocks, and mitigates targeted threats including malware, ransomware, phishing, and data exfiltration
  - Available to electoral bodies at no cost throughout the 2018 election cycle
- **Netscout: Arbor Cloud**
  - Cloud-based protection against low-volume / high-volume attacks from single or multiple attackers
  - Available to select elections officials through the November election

[The Best Option]

- There are no bad options. Choosing a service depends on your jurisdiction's location, infrastructure responsibility, and technical capacity to integrate with a particular vendor. Some are as easy as changing your DNS records while others require adding special equipment onto your network.
- Contact your system administrator, web server vendor, and ISP to verify compatibility with the services
- Long-term IT security and service delivery strategies also need to be considered to ensure that products are compatible and to avoid vendor-specific lock-in. Ask them what their plans are for support after the election.

[What’s Next]

- Nation-states are not the only malicious actors interested in disrupting Internet-connected election systems. Activist groups, criminal enterprises, and pranksters with limited technical abilities can actual rent DDoS service for as little as $20/hour. The attack can be sustained or intermittent at the whim of the attacker.
- Millions of computers and billions of IoT devices are already online, and more are being connected to the Internet everyday. These devices typically have little to no security and can be corralled into a botnet numbering in excess of 300,000.

[More Information]

- How a DDoS attack works: https://www.youtube.com/watch?v=J25XjTfthL8
- Cloudflare: https://www.cloudflare.com/athenian/
- Jigsaw: https://projectshield.withgoogle.com/public/
- Akamai: https://content.akamai.com/us-en-PG11022-elections-protection-etp.html
- Netscout: https://www.netscout.com/news/blog/cybersecurity-and-elections
- Install MS-ISAC Albert sensors to monitor & share network data: https://www.cisecurity.org/services/albert/
- Join for EI-ISAC to share election-specific security information: https://www.cisecurity.org/ei-isac/

For more info, please contact Maurice Turner, CDT Senior Technologist, at maurice@cdt.org, and Joseph Lorenzo Hall, CDT Chief Technologist, at joe@cdt.org. Additional election security resources: http://bit.ly/CDTelectsec.