OUTSTACK

Outside Perspectives on Voter Registration Security

Joshua M. Franklin

Election Verification Network - 2019

March 14 & 15, 2019 – Washington, DC

Disclaimer

- This represents my work and that of my colleagues at OutStack
- Not performed under the banner of any other employer or organization
- OutStack is party agnostic

OutStack Technologies

- Public Benefit Corporation established in Washington, DC
- Focused on campaign and election infrastructure cyberdefense
- Our automated platform:
  - Detects copycat sites
  - Prevents online donation theft
  - Provides a baseline security checkup
  - Recommends related domains for defensive acquisition
  - Identifies vulnerabilities and malware in election infrastructure

Experience

- National Institute of Standards & Technology
- Election Assistance Commission
- Center for Election Systems
- Pollworker in more states than anyone I know (9)
- 15 years working with vote capture and tabulation systems
- 7 years working with candidates and campaigns

Attacks on VR Systems

- In 2016, DHS notified 21 states of potential attacks on their online voter registration systems [12]
  - Many states denied they were even scanned
  - Illinois confirmed a breach
- Beginning of a better partnership between states and federal government regarding threat intelligence sharing
- Spurred our investigation into the security of these systems

Alabama
Alaska
Arizona
California
Colorado
Connecticut
Delaware
Florida
Illinois
Iowa
Maryland
Minnesota
Ohio
Oklahoma
Oregon
North Dakota
Pennsylvania
Texas
Virginia
Washington
Wisconsin

White Hat Activities

- Created *ElectionBuster* in 2012 to identify fake candidate sites
- Scanned 2,000+ candidates in 2018 with *ElectionBuster*
  - Reported hundreds of vulnerabilities to candidates
  - Also reported malware, sensitive personal information, and fake sites
- Due to 2016 attacks, began assessing internet facing infrastructure owned by local and state governments

2012 General Election

- ✓ Presidential

2014 General Election

- ✓ Presidential
- ✓ Senate
- ✓ House
- ✓ PACs

2016 General Election

- ✓ Presidential
- ✓ Senate
- ✓ House
- ✓ PACs
- ✓ Gubernatorial

2018 General Election

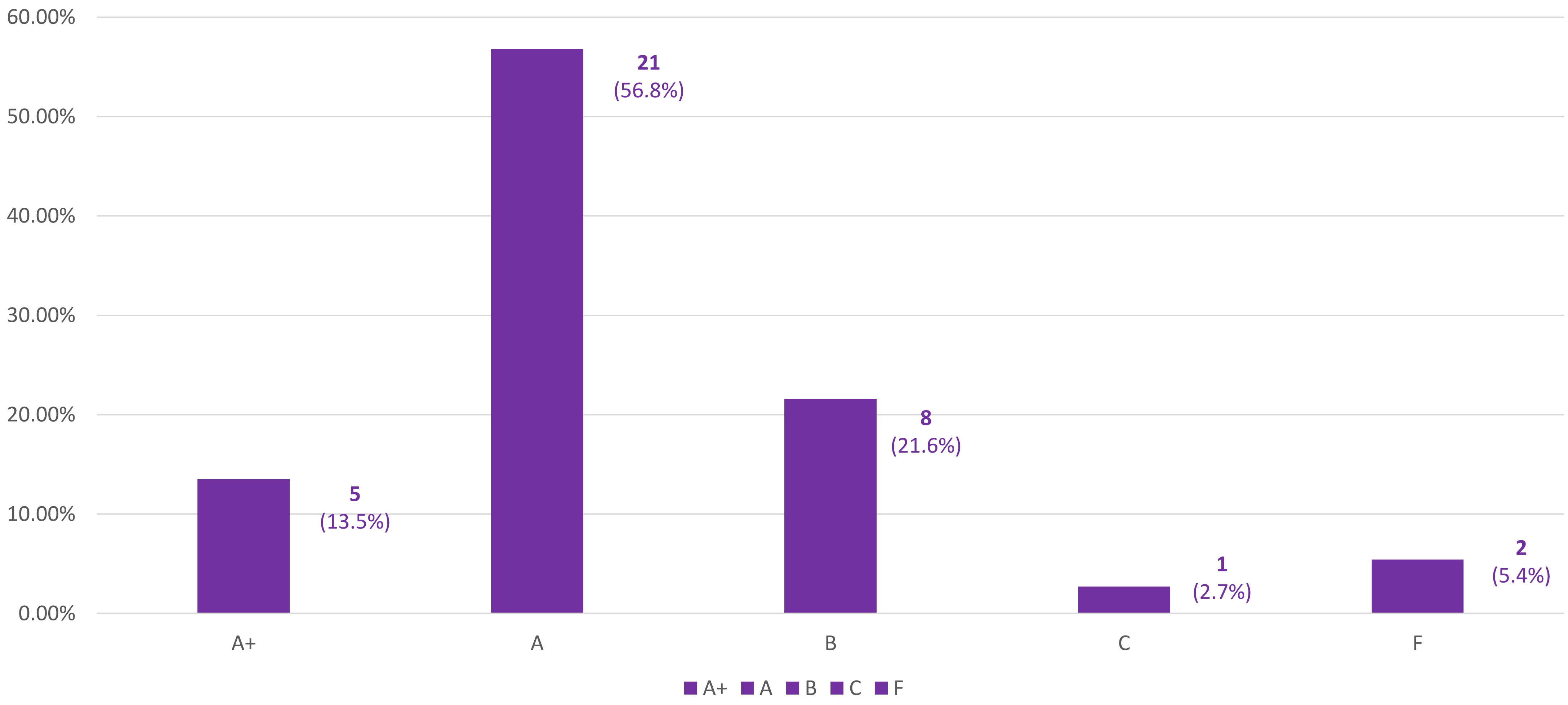
- ✓ Presidential
- ✓ Senate
- ✓ House
- ✓ PACs
- ✓ Gubernatorial
- ✓ Voter registration
- ✓ Election websites

OUTSTACK
www.outstack.vote

Internet Facing Election Tech

- Internet facing election infrastructure includes:
  - Online voter registration portals
  - State Board of Election (SBoE) / SoS homepages
  - Election Night Reporting portals
- VR systems are new, whereas SBoE / SoS sites are … around the same age as the rest of election infrastructure
- VR were much more secure than election websites
- At the time of our scans, 37 states used online VR systems
- Many states used .gov for Voter Reg, also saw .org and .us

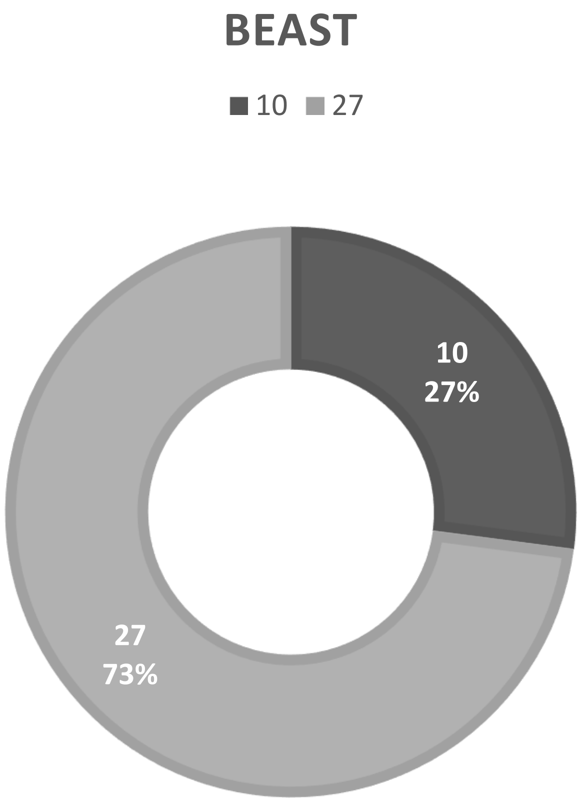
2018 Voter Registration Site Grades

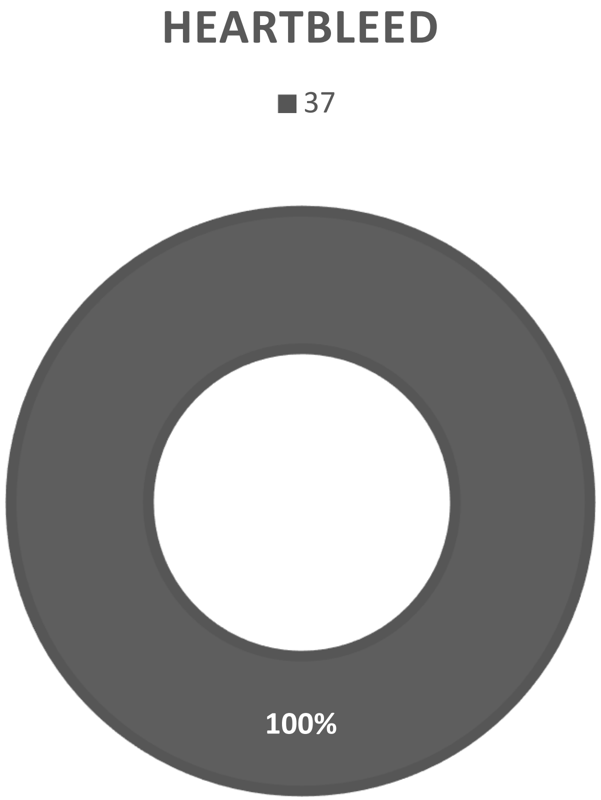


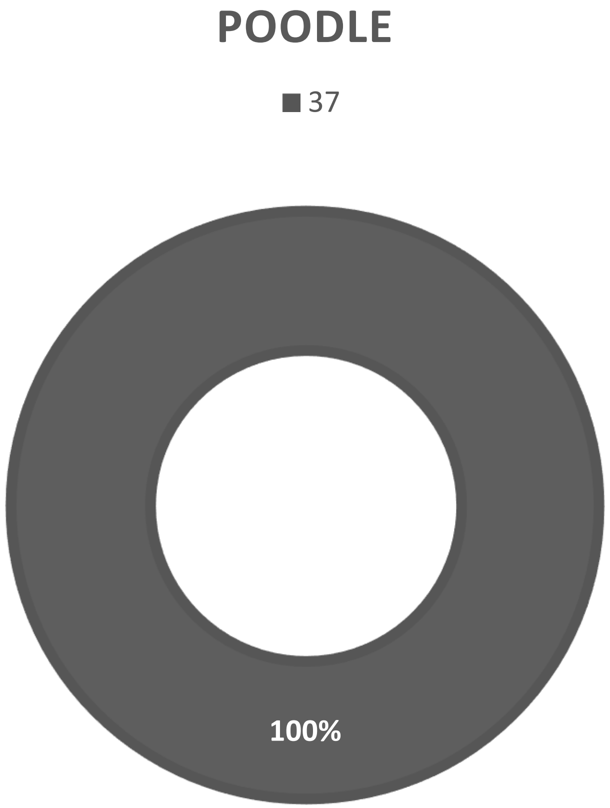
2018 VR Vulnerabilities

░ Included

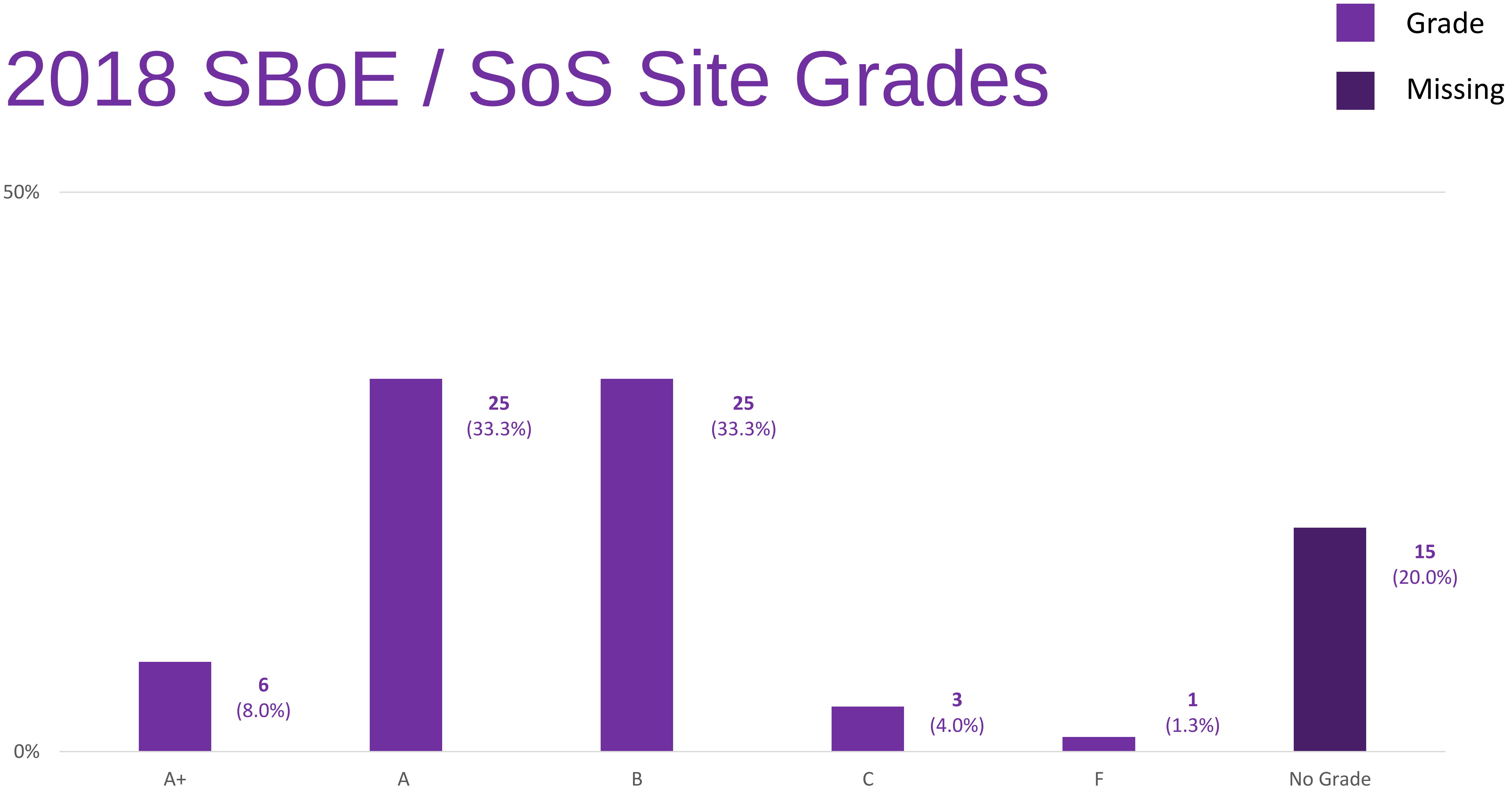
▓ Excluded







2018 SBoE / SoS Site Grades

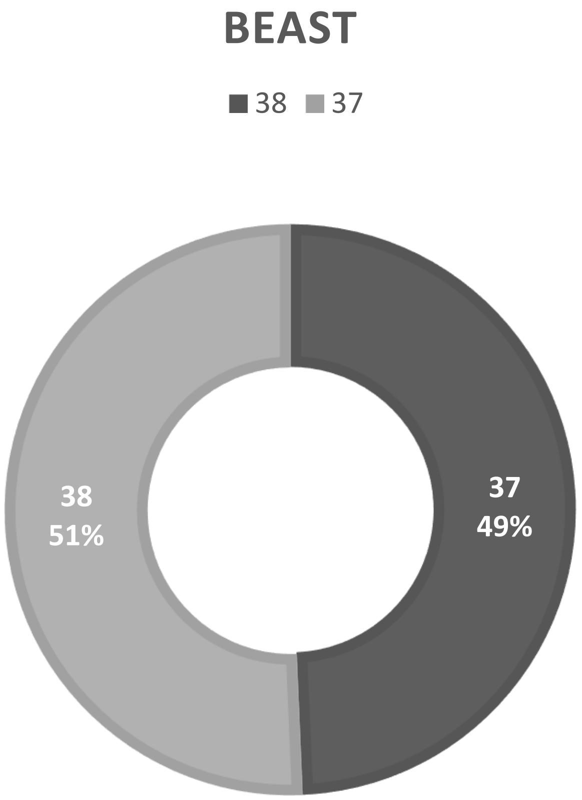


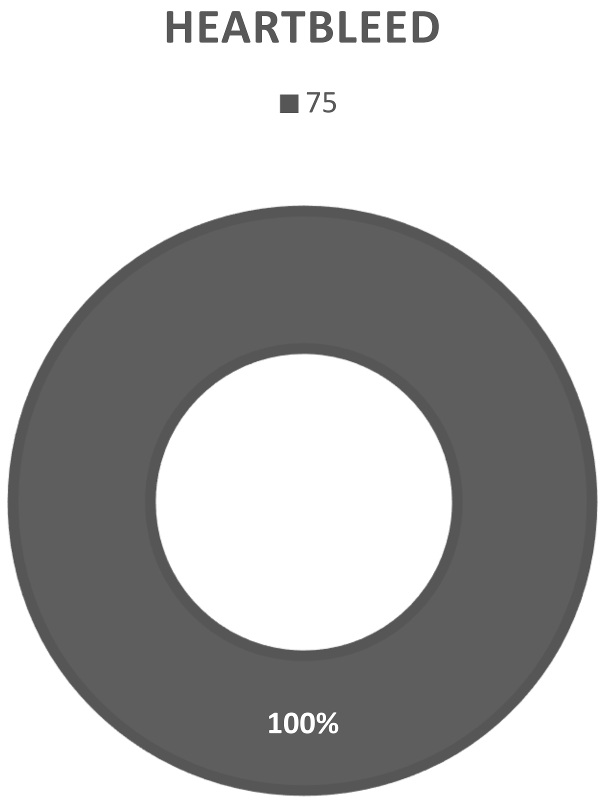
OUTSTACK
www.outstack.vote

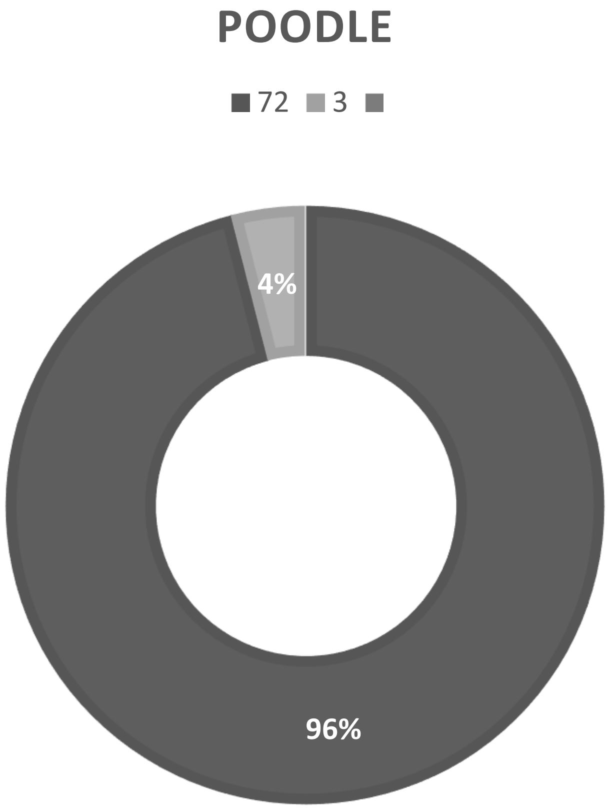
2018 SBoE / SoS Site Vulnerabilities

▨ Included

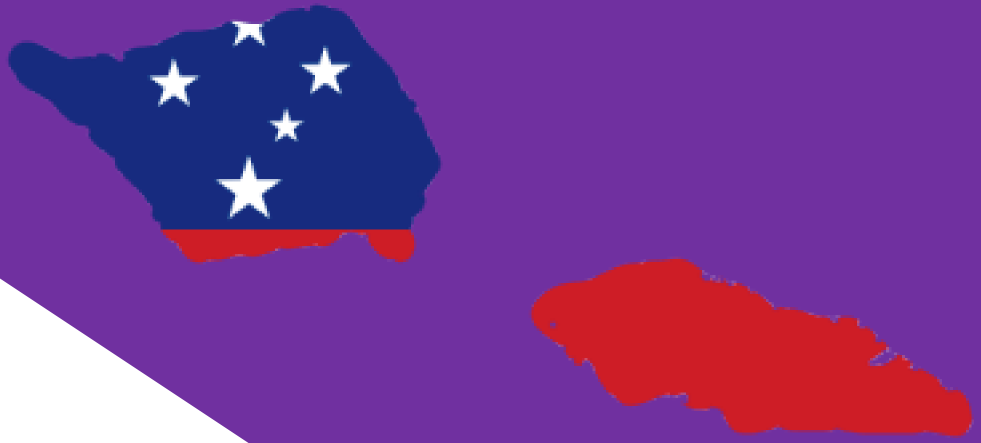
■ Excluded


BEAST


HEARTBLEED


POODLE

American Samoa



- Runs separate .gov and .org sites
  - Not the only organization to do this
- Site infected via a Drupal vulnerability
- Often to view the infected site, you need to approach from an IP outside the US
- Contacted AS for remediation and advised federal authorities and EI-ISAC

Contacting Election Officials

- Finding the right people at the states was difficult
- Often times email addresses were simply not available
  - Hackers do not want to use a contact form
- Time zones were an occasional issue
- Resorted to sending election officials DMs over Twitter
  - This worked!
- Eventually received proper contacts from many people in this room

Finishing Up

- After presenting this work at DEF CON, members of the National Guard from multiple states reached out:
  - Found them to be extremely competent
  - Independent confirmation of issues
- Officials from 4 states asked us to do county-level scans
- States not setup to work with external entities
- Given permission, more in-depth scans are possible

Recommendations

- 2FA for all critical systems
- Purchase common domains, such as the dot com version of your site (RegisterPennsyltucky.com)
- Purchase and maintain a trusted certificate
- TLS 1.2+ w/ strong algorithms & HSTS pre-load list
- EI-ISAC / DHS can help with intel and remediation
- Obtain outside assessments - vet providers
- Make it easy to contact you: security@yourstate.gov

Extended slides and data are available at:

pleasego.vote

josh@outstack.vote

OUTSTACK

Outside Perspectives on Voter Registration Security