DEFENDING THE 2018 MIDTERM ELECTIONS FROM FOREIGN ADVERSARIES

[presented by] = [josh kevin eli] * [franklin] + [ian weinstock]
Disclaimer

This work does not represent the opinions of our various employers. This is personal work; done on personal time. It is party agnostic.
Agenda

- History
- Methodology
- Election Infrastructure
- Campaign Results
- State Results
- Vendor Results
- Recommendations
- Conclusions
What is ElectionBuster?

- A python application, software suite, and project
- Everything we do is to protect US elections
- Our scope is large:
  - Candidates, election officials, voting system manufacturers, voting services providers
- Started with finding fake presidential sites, now:
  - Assessing campaign infrastructure
  - Assessing online state and local infrastructure
  - Identifying fake sites for candidates, PACs, and states
Project History

- Humble beginning as a 2012 GMU graduate project
- Initially a manual process to find fake domains
- Initially a single program, now a suite
- Shoutout to Robert Tarlecki and Matt Jablonski for their excellent teamwork for Shmoocon 2014 [7]
- Presented an update on the 2014 and early 2016 election findings at BsidesDC 2015 [10]

Focus on measurable impact for 2018
1. Obtain names of candidates
2. Gather lists of candidate and state election websites
3. Process candidate names and websites with ElectionBuster and other assessment tools
   Note: See [11] for the grading scale and rubric
4. Perform manual and automated data analysis
5. Disclose results to affected parties in a responsible manner
6. Party like rockstars
What Systems Are Out There?

- Controlled by election officials (examples)
  - Voting equipment (e.g., Opscan, DREs, BMDs)
  - Electronic pollbooks
  - State election websites (e.g., SoS, SBoE)
  - Voter registration systems with online interfaces

- Under candidate and party control
  - Candidate & party websites
  - Candidate & party voter information DBs

- Other control: PACs, Non-profits
2016 Election Attacks

- Phishing of campaigns, voting service providers, and election officials [2]
- Typosquatting on campaign fundraising sites and party contractor-controlled domains [6]
- Social media manipulation & (mis|dis)information [5]
- Data breaches of federal, state, & local systems [8]
  - Also candidate and campaign systems [9]
- Direct attacks on online voter registration systems and campaign infrastructure [4]
There are 1000s of candidates running in this November’s election
  ○ We’ve scanned most of them
Most campaigns are very small operations, with little to no IT expertise
Larger campaigns have sophisticated IT infrastructure
We observed campaigns being run purely from Twitter, Facebook, Instagram, and Snapchat
  ○ This might be the future...cheap and secure
2012 Findings

- Basically guessing for typosquats
- Manual data analysis
- Found very interesting typosquats
- Fake DNC and RNC site accepting donations
- Infected political action committee (PAC) sites
- Presented results at Shmoocon 2014 [7]
2014 Findings

- First iteration of ElectionBuster
- Found NRCC sites that could potentially confuse voters into donating to the wrong candidate
- Several candidate sites were actively distributing malware
- Sensitive WHOIS information
- Highlighted need to focus on data analysis
KIRKPATRICK FOR CONGRESS

A career politician and insider, Kirkpatrick was booted out of Congress by Arizonans in 2010 after she sided with Nancy Pelosi and supported ObamaCare. But in 2012, she managed to return after Pelosi’s allies came to her rescue with millions of dollars.

That probably explains why Kirkpatrick continues to be in Pelosi’s back pocket.

Kirkpatrick is a huge embarrassment to Arizona. How?

- Kirkpatrick walked out on her own town hall because she didn’t want to answer questions about voting for ObamaCare.
- After she lost the election, Kirkpatrick brought campaign staffers on the official House payroll then spent over $100,000 in taxpayer funds on salaries and bonuses for just two days of work.
- Kirkpatrick voted to keep the Grand Canyon shut down so she could protect ObamaCare.
- Kirkpatrick isn’t just liberal – she doesn’t even do her job as a representative. She missed 16 votes in just her first few days back in Congress.

DONATE

www.annkirkpatrick.com
2016 Hillary Clinton Typosquats

Day of scans:
E-Day 2016

R igraph
2016 Donald Trump Typosquats

Day of scans: E-Day 2016

R igraph

www.jeb4president.com

www.jebbush.com

www.jillstein.us

www.trumpforpresz.com

www.ted2016.org

www.donaldjtrump.com

www.teamhillary.com

www.trump2016.com

www.votetrump.com

www.presidenttedcruz.org
Date of scans: 20180715

R igraph
Success...and Failure

- We released PACScan in 2015
- Pointed it at ActBlue, one of the main fundraising platforms used by Democrats
- Recent indictments show that DNC and DCCC sites were hacked to redirect to a fake ActBlue page:
  - actblues(dot)com
- Although we detected it, we did not flag it as malicious even after investigating
May 31, 2016, YERMAKOV searched for open-source information

...and its reporting on X-Agent and X-Tunnel. On or about June

...Conspirators attempted to delete traces of their presence on the DCCC

...using the computer program CCleaner.

June 14, 2016, the Conspirators registered the domain actblues.com,

...the domain of a political fundraising platform that included a

...donations page. Shortly thereafter, the Conspirators used stolen DCCC

...modify the DCCC website and redirect visitors to the actblues.com

INPUTS = actblue, 2016, 2016

There were 27 positive results. There were

http://www.actblue.com
http://www.catblue.net
http://www.artblue.us
http://www.aceblue.com
http://www.artblue.com
http://www.actblue.org
http://www.catblue.com
http://www.ictblue.com
http://www.actblue.net
http://www.actblues.com
http://www.artblue.info
http://www.aceblue.biz
http://www.agtblue.com
ElectionBuster 2018 Updates

- Rewritten for Python3
- New variants and templates for PACs, election websites, and manufacturers
- Correlating ElectionBuster data with open source threat intelligence
- Began checking for homographic attacks via EvilURL and DNStwist
A Curious Case: Linda Coleman

- Candidate for State office in North Carolina
  - Under our radar
- Previously ran for Lt. Governor, this domain was purchased and repurposed [3]
- Code stripped from Wayback Machine to create a pharmaceutical storefront
- Ivan Gusev did not redact WHOIS information
- Assumed fake name, not politically motivated

Note that this was not originally identified by us; we independently investigated.
IT’S TIME FOR A DIFFERENT APPROACH IN RALEIGH.

I’m running for Lieutenant Governor because I want to give North Carolina’s middle class families a fighting chance again. The Republican majority running things in Raleigh continues to unravel so much of what built our great state. It’s time for a different approach. I know, working together, we can achieve this and more. Join me today by signing up below. Acheter cialis pas cher en pharmacie

Linda Coleman

www.lindafornc.com
WHOIS for lindafornc.com

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registrant</td>
<td>********** **********</td>
</tr>
<tr>
<td>Registrant Org</td>
<td>Private person</td>
</tr>
<tr>
<td>Registrant Country</td>
<td>RU</td>
</tr>
<tr>
<td>Registrar</td>
<td>GoDaddy.com, LLC</td>
</tr>
<tr>
<td>Registrar Status</td>
<td>ok</td>
</tr>
<tr>
<td>Dates</td>
<td>1,136 days old</td>
</tr>
<tr>
<td>Name Server(s)</td>
<td>NS1.DEALCOUPONSHOP.COM (has 16 domains)  NS2.DEALCOUPONSHOP.COM (has 16 domains)</td>
</tr>
<tr>
<td>Tech Contact</td>
<td>********** **********</td>
</tr>
<tr>
<td>IP Address</td>
<td>208.89.215.19 - 23 other sites hosted on this server</td>
</tr>
<tr>
<td>IP Location</td>
<td>- Washington - Seattle - Virpur</td>
</tr>
<tr>
<td>Domain Status</td>
<td>Registered And Active Website</td>
</tr>
<tr>
<td>Whois History</td>
<td>12 records have been archived since 2015-01-30</td>
</tr>
<tr>
<td>IP History</td>
<td>5 changes on 6 unique IP addresses over 3 years</td>
</tr>
<tr>
<td>Registrar History</td>
<td>1 registrar</td>
</tr>
</tbody>
</table>
ELECT COMRADE DEVIN NUNES
избранный товарищ Дьявол Нунес

www.electdevinnunes.com
Who we are & what we do

DSA is the major organization on the American left with an all-embracing moral vision, systematic social analysis, and political praxis rooted in the quest for radical democracy, social freedom, and individual liberties.

—Cornel West

www.gillibrandsucks.com
Join Carly, as we continue the fight to elect conservatives, reform Washington, and restore a citizen government to our great nation.

Meet Carly >

www.carlyfiorina.com
Job Creators Say “Enough is Enough” to Boxer

“Carly Fiorina knows firsthand the challenges facing companies across the nation that are struggling in this difficult economy, and she has consistently demonstrated her commitment to advancing policies that support the interests of businesses large and small.”

As a U.S. senator, Carly will help produce sustained economic growth and create more jobs, and we are pleased to endorse her candidacy for U.S. Senate.”-Bakersfield Chamber of Commerce President and Chief Executive Officer Debra Moreno

Cheap Non Owners Car Insurance here
Non Owners Car Insurance Auto

Read More
Congressional Site Statistics

- The following stats include everyone running for the Senate that we could identify.
- All House incumbents are included in these stats:
  - Races we deemed important were also included.
  - Too many candidates to include.
  - Skewing towards incumbents likely alters stats.
- A majority of the scans were taken during June 2018.
- Relied on Ballotpedia for pulling candidates.
Congressional Site Grades

**House**
- A+: 14 (2.7%)
- A: 287 (54.5%)
- B: 60 (11.4%)
- C: 5 (0.9%)
- T: 7 (1.3%)
- F: 1 (0.2%)
- No Grade: 153 (29.0%)

**Senate**
- A+: 2 (2.0%)
- A: 80 (80.8%)
- B: 12 (12.1%)
- C: 1 (1.0%)
- F: 4 (4.0%)
- No Grade

- □ grade
- ■ missing
Congressional TLS Implementations

<table>
<thead>
<tr>
<th></th>
<th>TLS 1.0</th>
<th>TLS 1.1</th>
<th>TLS 1.2</th>
<th>TLS 1.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>House</td>
<td>198 (37.6%)</td>
<td>118 (22.4%)</td>
<td>83 (15.7%)</td>
<td>469 (89.0%)</td>
</tr>
<tr>
<td>Senate</td>
<td>329 (62.4%)</td>
<td>409 (77.6%)</td>
<td>444 (84.3%)</td>
<td>58 (11.0%)</td>
</tr>
</tbody>
</table>

- **Enabled**
- **Disabled**
Let’s Look to the States!

- States / local jurisdictions host election sites
- Election sites provide info, report results, and register voters
- Sites may be hosted by SoS, State Board of Elections (SBoE), or 3rd party org (e.g., Cloudflare, Google)
- Overwhelming majority use a .gov TLD
  - Others use a .us or .org TLD
- About half of the VR systems move from .gov to .us or .org
REGISTER TO VOTE OR UPDATE YOUR VOTER REGISTRATION INFORMATION

WELCOME TO OHIO'S ONLINE VOTER REGISTRATION SYSTEM

This system provides a convenient and secure way to:

- Register to vote in Ohio
- Update your voter registration address

WHAT YOU NEED
American Samoa

- Unincorporated United States Territory
- Runs separate .gov and .org sites
  - Not the only state organization to do this
- Site infected via a Drupal vulnerability
- Contacted for remediation
- Responsible authorities were advised
- Often to view the infected site, you need to approach from an IP outside the US
- 1 man IT operation
Welcome to the official website of the Election Office for the Government of American Samoa.

This website is part of the Election Office's efforts to make the election process even more accessible to the public. Information about candidates, nomination process, filing of candidacy, campaign contributions and spending requirements, qualifications for electors, registration requirements, and voting by absentee ballots are some of the major topics addressed on this site. Information for candidates and electors are also available on this site.

Read more

VOTER SEARCH
Coverage From Leaked NSA Memo

The nonexistent email accounts were called “requestabsentee@americansamoaelectionoffice.org” and “r-questabsentee@americansamoaelectionoffice.org.” The analyst believes they did this to create the email accounts—although this is something they could have done directly by just registering the accounts. [19]

requestabsentee(at)americansamoaelectionoffice(dot)org

Although strange, we believe this to be coincidental.
Voter Registration Site Grades

- A+: 5 (13.5%)
- A: 21 (56.8%)
- B: 8 (21.6%)
- C: 1 (2.7%)
- F: 2 (5.4%)
Voter Registration HSTS Use

9 (24.3%)

28 (75.7%)

- Enabled
- Disabled
Voter Registration Vulnerabilities

- **Beast**
  - Included: 10 (27.03%)
  - Excluded: 27 (72.97%)

- **Heartbleed**
  - Included: 37 (100.0%)

- **Poodle**
  - Included: 37 (100.0%)

- Included
- Excluded
Election Site Vulnerabilities

- **Beast**
  - Included: 37 (49.333%)
  - Excluded: 38 (50.667%)

- **Heartbleed**
  - Included: 75 (100.0%)

- **Poodle**
  - Included: 72 (96.00%)
  - Excluded: 3 (4.00%)
Election vendors have websites too!
There are different types of vendors
The following stats include:
- Voting system manufacturers
- Voting system resellers
- Voter registration vendors
- Voting service providers
Vendor TLS Grades

- A+: 1 (7.1%)
- A: 8 (57.1%)
- B: 1 (7.1%)
- C: 1 (7.1%)
- No Grade: 3 (21.4%)
Recommendations to Campaigns

- Beware what you click
- Two factor authentication - even personal accounts
- Purchase common election domains, before someone else does - list in the appendix
- Please use a trusted digital certificate
- Use TLS 1.2+, strong cipher suites with HSTS
- Incumbents should consider EV certs
- Work with ISPs and FBI for domain takedowns
- Run security assessment tools on your own domain
Recommendations to States

- Two factor auth for all critical systems
- Purchase common domains (Register+state.com)
- Maintain a trusted certificate, consider EV cert
- Use TLS 1.2+, strong ciphers / algorithms
- Get on the HSTS pre-load list
- EI-ISAC / DHS can help with intel & remediation
- Run open source tools on your own domain
- Obtain outside assessments - vet providers
- Make it easy to contact you: security@yourstate.gov
The Aftermath

- 0 sites with SSL, 0 homographs, a lot of HTTP
- 2 VR systems with a grade of F, 1 with a grade of C
- Contacted campaigns and vendors using untrusted certificates and insecure protocols
- Contacted all, and worked with some, states affected by:
  - Likely typosquats / suspicious domains
  - Insecure, or no, TLS implementations
  - Untrusted certificates, known vulnerabilities
  - Malware actively on their site
The situation is improving, yet there’s still common sense ways to improve security

States are getting some monetary assistance from Congress

The community is responding:
- Center for Internet Security released an election focused cybersecurity handbook [16]
- Center for Democracy and Technology (CDT) & Center for Technology and Civic Life (CTCL) are working to teach election officials cybersecurity basics [18]
- Defending Digital Democracy effort focused on campaign security [15]
Conclusions

- We need to continue defending our elections
- More needs to be done, at larger scale - faster
- We assessed the bare minimum of web security
- It’s difficult to advise officials on security problems
- Responsible disclosure is SO MUCH work
- If you don’t vote, you’re helping the attackers
- Much of this can be done by ordinary citizens
- Wanna help? You need to learn: Work the polls
For a copy of the slides and data, visit: pleasego.vote

Josh: @thejoshpit
Ian: @heuristicmystic
https://github.com/thorshand/electionBuster
Appendix
References


Special Thanks To Tony Adams

- Cybersecurity expertise
- Elections expertise
- Sounding board for the entire talk
Common Templates

- Lname + Fname :: http://www.barackobama.com
- Lname + '-' + Fname :: http://www.chris-christie.com
- Fname + year :: http://lepage2014.com
- Fname + Lname + year :: http://johnwalsh2014.com
- Fname + ‘for’ + state :: http://alisonforkentucky.com
- Fname + Lname + ‘for’ + state :: http://www.edfitzgeraldforohio.com
- Lname + ‘4’ + state :: http://www.heck4nevada.com
- Fname + ‘for’ + position :: https://bryansmithforcongress.com
- Position + Fname + Lname :: http://www.congressmanbillyoung.com
- ‘team’ + Fname :: http://www.teammitch.com
- ‘vote’ + fName :: http://www.voteal.com
- ‘elect’ + Fname + Lname :: http://www.electfrench.com
- ‘team’ + ‘fName :: http://www.teammitch.com
- ‘friendsof’ + fName ::https://www.friendsofamata.com
- lName + ‘for’ +stateAbbreviation :: http://feinsteinforca.com
Attacks started as early as 2015
100s of bit.ly and other links emailed to DNC / Clinton officials [2]
  dnc.org, hillaryclinton.com
Use of fake gmail splash pages
Lead to access of emails, chats and GDrive
Information distributed to other organizations (e.g., Wikileaks)
Phishing Vendors & Officials

- Phishing emails sent to US voting system service vendors and over 100 election officials [17]
- Masqueraded as a voting technology vendor and a fake cybersecurity company
- Emails contained a Word document with a malicious payload
- The addresses used contained gmail domains such as vrsystems(at)gmail(dot)com
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.
Data Breaches

- Local: 650k voter records left on a CF card [8]
- State: Illinois VR system breached [12] as well as the Georgia KSU Center for Election Systems [20]
- Federal: Vendor information stored on US EAC certification portal [14]
- Vendor: ES&S AWS bucket leaks 1.8 million records [13]
- Campaign: Deep Root Analytics stored 1.1 TB of voter information on an unsecured server [9]
  - Over 200 million records
Homographic Attacks

- Using alternative character sets to typosquat
- Instead of creating our own tool, let’s try what’s out there:
  - DNStwist and EvilURL
- Focused on election portals
- Found new and interesting typosquats, but no homographic domains
Ron Barber is running for Congress because he is more interested in keeping his job than making sure there are jobs for you and your family.

Barber will say just about anything to get elected — even if that means just going along with what Washington special interests tell him to do.

**How out-of-touch is Ron Barber?**

- Barber voted against a balanced budget that bans taxpayer-funded first class travel for Members of Congress (Roll Call #88, 3/20/13)
- Barber voted against constructing the Keystone Pipeline (Roll Call #179, 3/22/13)
- Barber voted to allow student loan interest rates to increase (Roll Call #183, 5/23/13)
- Barber even voted against work requirements for food stamps — requirements passed under Democratic President Clinton. (Roll Call #476, 9/19/2013)

DONATE

Fed up with Ron Barber? Sign up today.

www.ronbarber2014.com
Discovering on accident
The number of hits ElectionBuster returns for a given candidate is often correlated with who wins the race
ElectionBuster hits are sometimes equal with candidates, which means a toss up
Correlation != causation
Likely even talking about this will change it
Let’s cherry pick some examples!
# Illinois Election Results

## Governor
- Pritzker: 45.2%
- Biss: 26.6%
- Kennedy: 24.3%
- Raunder: 51.4%
- Ives: 48.6%

## 4th District
- Garcia: 66.4%
- Flores: 21.6%
- Gonzalez: 12%

## 3rd District
- Lipinski: 51.2%
- Newman: 48.8%

---

Hits Per Candidate over 2016
Congress on Let's Encrypt & HSTS

Let's Encrypt
- House: 220 (35.1%)
- Let's Encrypt: 307 (49.0%)
- Other Authorities: 50 (8.0%)

HSTS
- Senate: 69 (11.0%)
- Enabled: 458 (73.2%)
- Disabled: 8 (1.3%)
- Other Authorities: 91 (14.5%)
Voter Reg TLS Implementations

- **TLS 1.0**: 10 (27.0%) Disabled
- **TLS 1.1**: 8 (21.6%) Disabled
- **TLS 1.2**: 36 (97.3%) Enabled
- **TLS 1.3**: 34 (91.9%) Enabled
Election Site TLS Implementations

<table>
<thead>
<tr>
<th>TLS Version</th>
<th>Number of Records</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS 1.0</td>
<td>44</td>
<td>58.7%</td>
</tr>
<tr>
<td></td>
<td>31</td>
<td>41.3%</td>
</tr>
<tr>
<td>TLS 1.1</td>
<td>53</td>
<td>70.7%</td>
</tr>
<tr>
<td></td>
<td>22</td>
<td>29.3%</td>
</tr>
<tr>
<td>TLS 1.2</td>
<td>64</td>
<td>85.3%</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>14.7%</td>
</tr>
<tr>
<td>TLS 1.3</td>
<td>73</td>
<td>97.3%</td>
</tr>
</tbody>
</table>

- **Enabled**
- **Disabled**
Election Site HSTS Use

- Enabled: 64 (85.3%)
- Disabled: 11 (14.7%)
Vendor TLS Implementations

<table>
<thead>
<tr>
<th>TLS</th>
<th>Enabled</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>1.1</td>
<td></td>
<td>2 (14.3%)</td>
</tr>
<tr>
<td>1.2</td>
<td></td>
<td>13 (92.9%)</td>
</tr>
<tr>
<td>1.3</td>
<td></td>
<td>13 (92.9%)</td>
</tr>
</tbody>
</table>
Vendor HSTS Use

- 9 (64.3%) Disabled
- 5 (35.7%) Enabled
Recommendations to Companies

- Advise your clients on cybersecurity issues
- Purchase common domains
- Maintain a trusted certificate, consider extended validation (EV) certificate
- Use TLS 1.2+, strong cipher suites
- Use HSTS, get on the pre-load list
- Request assistance from EI-ISAC, DHS, FBI and other organizations