FACT SHEET

A Portrait of a Digital Disinformation Campaign

Attack Scenario

Disruptive Disinformation vs. Changing Votes

A lot of cybersecurity research and media coverage has focused on whether a well-orchestrated nation-state attack could compromise physical voting machines and related reporting systems to change election vote counts.

But malicious actors such as nation-state and cybercriminal hackers always seek to achieve their objectives with the least effort and fewest resources. While it is certainly possible that such actors could hack into local voting systems and change vote counts in the battleground states, such a hacking campaign would require a herculean effort of orchestration across hundreds of counties and thousands of voting precincts.

Alternatively, a digital disinformation campaign seeking to suppress or otherwise disrupt voting behavior would be less complicated to execute and therefore more likely to be attempted than efforts to change vote counts. If executed successfully at scale in critical counties and states, this disruption could accomplish the same goals of a hacking campaign with a fraction of the resources.

A well-crafted campaign could focus on specific battleground state counties and work to introduce process barriers or bogus voting process instructions to reduce voter turnout, either in total, or within specific subsets of the population. An example could be voters in rural or urban parts of a district which generally have a strong correlation to Republican and Democrat voting tendencies respectively.

The malicious actors would set up dozens of bogus website domains claiming to belong to county governments and use those bogus domains to launch bulk email campaigns intended to feed incorrect election information to the email recipients. Additionally, the emails and social media promotions could be used to drive voters to the bogus websites and feed them more false information about when, where, and how to vote.

Given the fact that voter data can be purchased or even freely obtained due to numerous recent data breaches, a very specific and targeted campaign would be trivial and inexpensive to orchestrate. After all, many millions of bulk email campaigns operate every day.

The attack plays on the fact that there are multiple challenges for a typical voter trying to identify legitimate from fraudulent sites, and this issue is further complicated by legitimate sites that often lack the most basic validation or security hygiene.

Connect With Us

Why the Counties?

McAfee has looked at how voters get information from their election boards at the county level. County websites are typically the first place a citizen would go to look up information on the upcoming local elections. Such information might include voter eligibility requirements, early voting schedules, deadlines to register, voting hours, and other critical information needed to make a citizen's vote count.

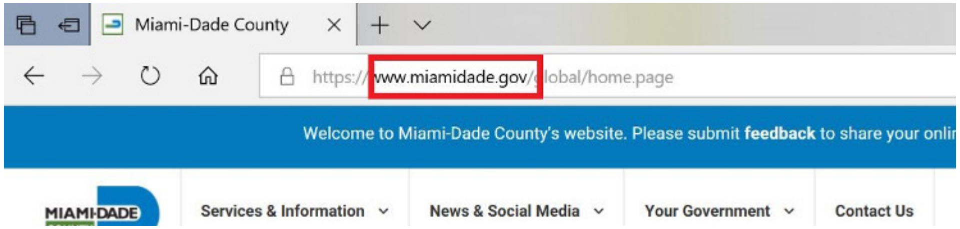
Unlike state-level websites, county websites are more obviously accessible to local citizens seeking election information, and less likely to have government validation and security measures to ensure that they are genuine, safe websites for citizens to visit.

Election 2020 prognosticators have identified key counties in states where the 2016 presidential election was decided by as few as tens of thousands of votes. For 2020, these prognosticators argue that counties such as Arizona's Maricopa County, Florida's Miami Dade County, Georgia's Cobb and Gwinnett Counties, Pennsylvania's Philadelphia and Beaver County, and others could decide which party wins the states. Their caveat is that voters turn out and vote in the numbers that are possible in those counties.

Therefore, any manipulation of voter turnout in different county precincts could impact the election results there. The weak validation and security of the website domains in these counties is a weak election security link that presents an inviting target for any malicious actors seeking to shape the election results in their favor.

.GOV: What's in a Website Name?

Our first disturbing survey revelation was that there's no consistency as to how counties validate that their websites are legitimate sites actually belonging to genuine county governments. McAfee found that significant majorities of county government websites use web addresses that do not use the .gov top level domain (TLD) naming system.

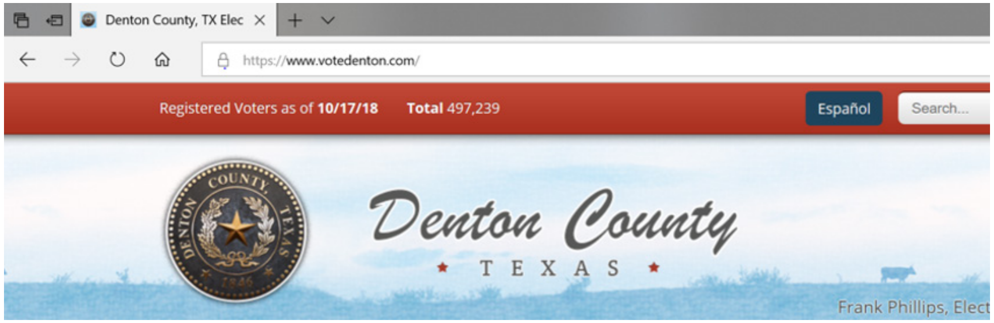


Miami-Dade County

https://www.miamidade.gov/global/home.page

Welcome to Miami-Dade County's website. Please submit **feedback** to share your onli

McAfee CTO Steve Grobman initially became concerned about this .gov issue because he lives in Denton County Texas, where the election administration site is www.votedenton.com (see below). When he saw the website name, he was a little perplexed because the county uses a website address with a .com domain name rather than a name using .gov.



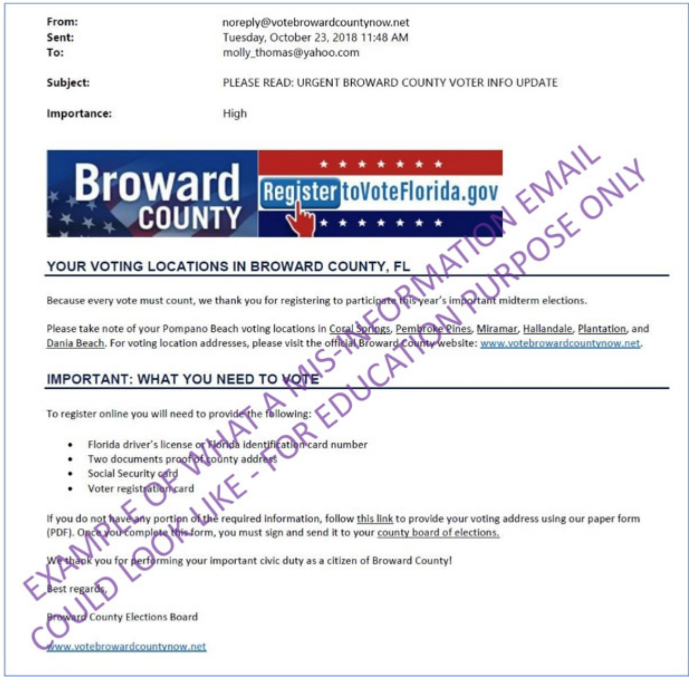
Denton County, TX Elec

https://www.votedenton.com/

Registered Voters as of **10/17/18** **Total** 497,239

A malicious party could easily purchase non-.gov website addresses using any combination of words such as “denton”, “denton county”, “tx”, “vote”, “election”, and others to create websites posing as the legitimate Denton County election administration website. That party could then send hundreds of thousands of disinformation emails to voters directing them to those bogus websites.

Following is an example of what a fraudulent email might look like if such a bad actor was trying to manipulate voters in Broward County Florida, one of the three counties that were the focus of controversy during the 2000 U.S. presidential election:



From: noreply@votebrowardcountynow.net
Sent: Tuesday, October 23, 2018 11:48 AM
To: molly_thomas@yahoo.com

Subject: PLEASE READ: URGENT BROWARD COUNTY VOTER INFO UPDATE

Importance: High

YOUR VOTING LOCATIONS IN BROWARD COUNTY, FL

Because every vote must count, we thank you for registering to participate this year’s important midterm elections.

Please take note of your Pompano Beach voting locations in Coral Springs, Pembroke Pines, Miramar, Hallandale, Plantation, and Dania Beach. For voting location addresses, please visit the official Broward County website: www.votebrowardcountynow.net.

IMPORTANT: WHAT YOU NEED TO VOTE

To register online you will need to provide the following:

- Florida driver’s license or Florida identification card number
- Two documents proof of county address
- Social Security card
- Voter registration card

If you do not have any portion of the required information, follow this link to provide your voting address using our paper form (PDF). Once you complete this form, you must sign and send it to your county board of elections.

We thank you for performing your important civic duty as a citizen of Broward County!

Best regards,

Broward County Elections Board

www.votebrowardcountynow.net

This use of .com by Mr. Grobman’s own county raised the question in his mind of how extensive the use of non-.gov website names was on Texas county election websites and similar websites across pivotal battleground states across the country.

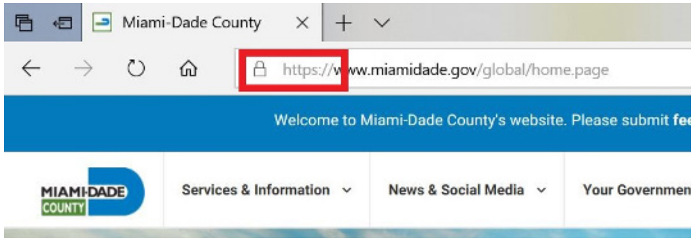
McAfee’s recent survey of county websites did indeed find significant majorities of them using .com, .net, .org, and .us rather than the government validated .gov in their web addresses.

This means that there is presently no official U.S. governing body validating whether the overwhelming majority of county and county election administration websites are legitimately owned by actual county government entities.

HTTPS: Protecting Website Visitors' Sessions

McAfee's website survey also found that significant majorities of county sites do not enforce the use of "https" or Secure Sockets Layer (SSL) certificates to secure citizens' access and exchange of personal information to those county entities.

While SSL is a technical a term, voters can easily recognize that the website they are visiting is protected by this security technology by the "https" at the beginning of website addresses. Web browsers have made recognition even easier for us by using a "lock" symbol in the address bar:



Welcome to Miami-Dade County's website. Please submit fee

When voters see https and the lock signal in their address bar, they can rest assured that their connection or session with a website is protected, meaning that any personal information they might share while registering to vote is encrypted and cannot be intercepted and stolen by a bad actor.

Perhaps more relevant to the digital disinformation campaigns, the technology's second core capability is that bad actors can't redirect site visitors to fraudulent sites that might feed them false election information.

In the same way that .gov is basic validation of government websites, https is one of the most basic forms of cyber-hygiene that McAfee expects all websites requiring confidentiality or data integrity to possess.

On the Eve of Deception

If you think about a close election race with rural or urban county or district elements to it, a malicious actor could simply send emails to hundreds of thousands of voters in rural or urban parts of the municipality and direct voters to the wrong voting locations. Such an actor would essentially be suppressing, misdirecting, and otherwise disrupting voter turnout with false information.

No voting systems would be taken offline, no voter records need be stolen, no voting machines need be damaged. In fact, it is likely that no one would even notice the digital disinformation campaign until Election Day when angry voters show up to the wrong voting stations, or to the correct sites without having registered to vote.

To avoid early detection, it is most likely that a coordinated attack would take place just 12 to 24 hours before votes are cast. The threat actors would want to provide enough time to reach a critical mass of voters for election disruption, but too little enough time for their efforts to be detected and remediated by county and state officials.

As mentioned, influencing the electorate through false communications is more practical and efficient than attempting to successfully hack into hundreds of thousands of voting machines. Such a scenario is much easier to execute than tampering with voting machines themselves, and it scales to achieve the broad election objective any malicious actors would desire.

Just Cause for Frustration

The fact that so many county and county election websites or webpages are lacking in the absolute basics of cyber hygiene is troubling. It is particularly troubling given that these external lax security and validation measures could be an indication of these governments' inattention to internal measures for protecting voter registration, vote county reporting systems, and other functions critical to elections.

Perhaps most frustrating is the realization that implementing .gov and https is affordable and very easy compared to the investments being made to protect other areas of the nation's election infrastructure.

What Voters Can Do to Strengthen Election Internet Security

What Governments Can Do to Strengthen Election Website Security

McAfee
2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com