Title: **Valimail research demonstrates that email remains a weak link in U.S. election infrastructure**

Author: Seth Blank, director of industry initiatives, Valimail

As we head into the 2020 election season in the United States, a key component of the U.S. election infrastructure remains vulnerable to attack. **Only 5% of the country's largest counties are protecting their election officials from impersonation**, according to an analysis by Valimail. The rest are vulnerable to impersonation, meaning their domains could become the unwitting vectors for cyberattacks and misinformation campaigns.

This is a problem because the overwhelming majority of cyberattacks can be traced to impersonation-based phishing emails. In the corporate world, these cyberattacks result in the loss of funds or proprietary data. But when it comes to elections, the bedrock of democracy -- free and fair elections -- is at stake.

An August 2019 report from Valimail noted that most presidential candidates' campaigns are not protected from email impersonation. And our earlier report found a similar situation across the thousands of domains used by state and local governments. The new report takes a closer look at those domains specifically used by the largest counties for election matters.

The relevance of email to election infrastructure

About 90% of all cyberattacks involve phishing, according to the Verizon Breach Report and multiple other sources. And 89% of phishing involves impersonation, according to a recent study by Barracuda. While these stats come from analyses of primarily private-sector domains, we know that the election infrastructure is also vulnerable to phishing. For instance, spear phishing played a major role in the 2016 election, as it was the vector by which the Democratic National Committee's email system was compromised. And spear-phishing attacks targeted multiple election officials in Florida during the 2018 election season, although there was no indication that these attacks had an effect on the elections.

We're not just talking about voting machines being vulnerable. While most voting machines are isolated from the Internet (they are often air-gapped for security), the same cannot be said for other elements of the election process. The electronic pollbooks that voters use to sign in on election day and the machines that tabulate votes may be connected to the Internet for software updates or to receive or transmit voting information. This makes them potential targets for email-based attacks aimed at other users of the same networks.

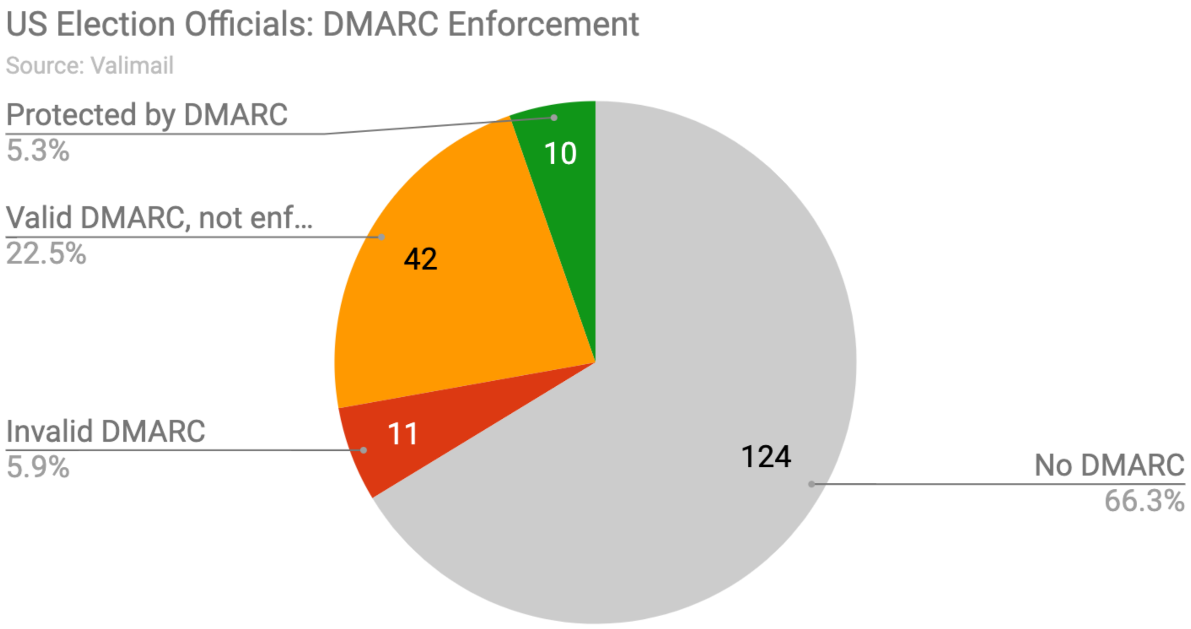
For example, an attacker might send an email to an election official that spoofed the identity of a voting machine vendor and posing as an “urgent software update” that they needed to install. Or malware could be delivered via spear-phishing emails that, if clicked on, would shut down the county’s network and disrupt the smooth functioning of an election.

These are not theoretical examples. Earlier this month the Louisiana state government’s computers were taken offline during an election week by a ransomware attack that most likely originated with a spear-phishing email message.

Apart from the voting infrastructure itself, there are other vulnerabilities susceptible to email attacks. Voting officials (county auditors, clerks, or boards of elections) must be able to communicate with the public via email. Email is often used to transmit running totals of the election results to the media. And media outlets also use email to deliver election news to the public via newsletters.

While email is not the only threat vector that election officials need to take seriously, our report shows that it is being significantly overlooked.

Specific email vulnerabilities identified



Valimail analyzed the 187 domains used by election officials in the three largest counties (or parishes) for every state in the U.S. Our analysis examined the SPF (Sender Policy Framework) and DMARC (Domain-based Message Authentication, Reporting & Conformance) status for each of these domains, enabling us to determine whether each domain is protected from impersonation attacks by a correctly configured DMARC record with a policy of enforcement (p=quarantine or p=reject). A DMARC enforcement policy prevents unauthorized senders from using the domain in the "From" field of their messages, cutting off one of the most devious impersonation vectors used by attackers.

Our analysis revealed that 124 of these domains (66%) have no DMARC records, while 34% (63 domains) do have DMARC. Of those with DMARC, 11 domains (6% of the overall total) are incorrectly configured, 42 domains (23%) are correctly configured but not at enforcement, and **just 10 domains (5%) are correctly configured and at enforcement.** It is only those last 10 that are protected from exact-domain impersonation attacks.

The ten domains that are protected from impersonation are as follows:

- St. Louis County County, Missouri — p=reject
- Jefferson County, Colorado — p=reject
- Clackamas County, Oregon — p=reject
- Hartford County, Connecticut — p=quarantine
- Lyon County, Nevada — p=quarantine

- Kanawha County, West Virginia — p=reject
- Mecklenburg County, North Carolina — p=reject
- Clackamas County, Oregon — p=reject
- Hamilton County, Ohio — p=quarantine
- Washington County, Rhode Island — p=reject

Six swing states, as identified by electoralvotemap.com, have a complete lack of protection among their three largest counties:

- Arizona – no protection
- Florida – no protection
- North Carolina – no protection
- Pennsylvania – no protection
- Michigan – no protection
- Wisconsin – no protection

Why this matters

The lack of DMARC enforcement at the state and local levels is of course not the only vulnerability in U.S. election infrastructure. However, it is a very serious one. While there are other types of impersonation, exact-domain impersonation (putting the exact domain of a spoofed organization into the "From" field of a phishing email) is particularly difficult for email recipients to detect and often go uncaught even by many email security solutions. Only DMARC offers definitive protection against this kind of attack, and only when correctly configured and set to an enforcement policy.

It does not require a stretch to imagine attackers impersonating election officials via spoofed domains in order to spread disinformation, conduct voter misdirection or vote-suppression campaigns, or even to inject malware into government networks.

For this reason, Valimail urges all state and local election officials to configure their domains with DMARC at enforcement. This step is both feasible and effective. For instance, the U.S. Department of Homeland Security issued a directive in late 2017 (BOD 18-01), mandating that civilian executive branch agencies use DMARC at enforcement on all of their domains by early 2019. As a result, nearly 80% of the federal government’s domains are now protected from impersonation, according to Valimail’s latest quarterly research.

Funding exists to help state and local governments with securing their election infrastructure, thanks to the Help America Vote Act (HAVA). Unfortunately, while HAVA disbursed nearly $400 million in 2018, it has not been used to improve email security. The email domains evaluated in the four states receiving the largest grants under HAVA — California, Texas, Florida, and New York, which each received more than $20M — are not protected.

DMARC at enforcement is a crucial best practice for stopping the largest attack vector into any organization. The low rates of state and local deployment of this open standard is a clear warning sign that best practices to protect democracy are missing in many key places. It is time to direct funding toward implementing such best practices, with DMARC at the top of the list, across state and local infrastructure. Election infrastructure needs to meet the same level of security as the federal government. The playbook on how to achieve that is well known, and funding is available. It’s time to get it done.

Note: Seth Blank is the co-chair of the Election Security Special Interest Group within M3AAWG, the industry’s leading vendor-neutral working group working to stop abuse of public message infrastructure, including email.

More information on Valimail’s solutions for government and Valimail’s offer to protect U.S. election campaigns at no charge.