REPORT

U.S. Elections

Evaluating the security and data protection risks present in candidate websites

March 2020

THE MEDIA TRUST

We know digital security.

Executive Summary

The fallout of the 2016 U.S. Presidential election raised questions regarding voting fraud and distribution of misinformation. From fake accounts and exploited digital platforms to bots and foreign influence, today's election process is riddled with vulnerabilities. The 2020 federal election promises more of the same with Iran blamed for targeting candidates, journalists covering politics, and government officials.[1] Iran was also blamed for the emergence of politically-oriented malware campaigns targeting consumers.[2] The FBI discovered potential targeting of voter information and registration websites to launch Distributed Denial of Services (DDoS) attacks to disrupt their operation.[3] In addition, the Senate Intelligence Committee warned that Russia-based bad actors are gathering data to target the 2020 event.[4]

81% executing code is from digital third-party vendors

In preparation, several candidates declared digital reform as part of their platform and others hired security professionals to their teams.[5] However, the teams were short-lived and there's little evidence that candidates understand how to protect their consumer-facing digital assets.[6] Instead of looking at digital advertising spend, physical voting issues, website spoofing or general security posture, this report evaluates the extent to which candidates' digital properties (websites) provide a safe and secure user experience to consumers.

In September and December 2019, The Media Trust scanned the primary campaign websites of the incumbent U.S. President and 10 leading Presidential candidates to capture and analyze the code involved in rendering the consumer experience. Candidates were chosen according to who qualified for the third round of debates held in September. The goal was to discover how well the candidates' campaign websites met industry best practices for security and data privacy.

Specifically, the research evaluated:

- How much the individual websites rely on unmanaged technology to support their outreach efforts.
- Extent to which website visitor information is collected, especially the data leakage/breach risks third-party code (3PC) suppliers introduce to candidate websites
- Data collection activity as individuals they make donations
- Security risks of allowing unauthorized code from largely unknown suppliers to run on their websites and execute on consumer devices
- How much candidates rely on the broader digital ecosystem to target audiences and communicate their message

KEY FINDINGS

Continuous client-side monitoring of the campaign websites during September and December revealed:

- 81% executing code is from digital third-party vendors, which are entities unmanaged by (and frequently unknown to) the website operator, i.e., candidate teams
- 6% of all executing domains, on average, pose an unmitigated risk to consumers due to presence of malicious and/or suspect activity
- Klobuchar's digital footprint and cookie use is almost 3 times larger than the next closest candidate website
- 1 website directed consumers to media websites that served adware
- 11 candidate websites (all) allow tracking of consumers for at least 2 years, 6 candidates track consumers for at least 20 years
- 71% of executing code on a payment page has zero relevance to the purchase transaction, leaving the door open for compromise. 95% of executing code on Booker's donation page is not relevant to payment processing.
- 56 distinct data tracking technologies execute on Warren's donation page. These entities could gain access to consumer payment information.
- Campaign websites continue to collect consumer information even after the candidate dropped out of the race.
- As campaign spend increases so does data tracking

Introduction

Presidential campaigns rely on the digital ecosystem to help test, communicate, and propagate their messages. While the platforms take steps to control political advertising, the campaigns are charging ahead with their digital promotions, a more economical channel than print or television.[7] From social media postings to advertising, campaigns are expected to spend $1.6B this federal election cycle.[8]

This next presidential election is placing an emphasis on election security, from voting processes to campaign information exchange restrictions[9]. In fact, several candidate platforms address security, with Buttigieg hiring a CISO for a limited period of time.[10] But their cybersecurity readiness has been called into question by several groups, notably the Internet Society's Online Trust Alliance[11]

The research aims to evaluate how seriously the candidates understand digital risks and the level of effort they put forth to protect consumers when visiting their websites. It digs deeper into their website

security posture by analyzing the domains and cookies to evaluate the consumer experience—the code that renders when a consumer accesses and/or donates via the following campaign websites:

1. Joe Biden – joebiden.com
2. Cory Booker – corybooker.com
3. Pete Buttigieg – peteforamerica.com
4. Julian Castro – julianforthefuture.com
5. Kamala Harris – kamalaharris.org
6. Amy Klobuchar – amyklobuchar.com
7. Beto O'Rourke – betoorourke.com[12]
8. Bernie Sanders – berniesanders.com
9. Elizabeth Warren – elizabethwarren.com
10. Andrew Yang – yang2020.com
11. Donald Trump – donaldjtrump.com

While many have ceased their candidacy, most campaign websites are still active, drawing traffic and soliciting visitor information. It is assumed these websites will revert to their previous operating status with updated messaging upon a candidate's next election cycle—federal, state or local.

Research Results

THIRD-PARTY CODE SUPPLIERS DOMINATE

Most of the technology that powers the digital experiences consumers crave isn't developed by in-house teams. Consider the CRM systems, shopping carts, online chat tools, video delivery platforms, social sharing apps, and more that make up just a few clicks on today's digital properties. Presidential candidates can't operate without this useful functionality, but few understand the scope of what executes when a voter accesses their website.

Beyond GitHub and JavaScript libraries, organizations increasingly rely on third-party code to provide the infrastructure and functionality to deliver the features today's consumers expect: dynamic content, personalization, and seamless engagement. This third-party code operates outside the scope of the enterprise technology operations; App Sec practices don't even call for it to be reviewed as part of basic security measures. As a result, third-party code is not monitored and, therefore, there is no warning when it is compromised or used for unauthorized activity, such as re-targeting to spread misinformation.

Learn more about Third-party code

- When not properly managed, third-party code:
- Leaks personal data to hackers or other candidates to re-target with alternative messaging
- Enables the spread of misinformation via purposeful targeting
- Causes data privacy and compliance issues that flout industry best practices and regulations
- Hijacks the consumer experience during browsing and redirects to other candidate pages
- Delivers malware to unsuspecting consumers during their site visits

GENERAL WEBSITE EXPERIENCE IS DYNAMIC

To support everyday function, websites rely on a host of technologies, many unknown to the visitor or the website operator. When websites are accessed, these technologies are dynamically pulled into the website via a url or domain. This domain then enables execution of the technologies' services or function.

As expected, candidates incorporate tools to support basic website operation such as content management systems, content delivery networks, and hosting. The candidates each have a financial platform to solicit and collect donations and use analytics to measure the digital performance.

What's not readily visible to the visitor's eye are the various Advertising and Marketing technologies, which come in the form of ad servers, ad networks, affiliate marketing, targeting, third-party data platforms, and more. By combining these data sources, candidates create a complete social graph of their constituents. This third-party code is used to not only learn more about consumers when they visit candidate websites, but also to target additional messaging when consumers visit other websites in order to continue pushing their message.

EXAMPLES of 3PC

Ad Server
Affiliate Marketing Platform
Analytics
Consent Management Platform
Content Delivery Network
Content Management System
Content Recommendation Engine
Customer Identification
Data Management Platform
Demand Side Platform
Marketing Automation Platform
Online Chat
Shopping Cart
Social Widgets
Supply Side Platform
Tag Manager

Vendors and domains vary during each website execution

Candidate websites use more third-party code as their campaigns ramp up spend to reach more consumers

The first step to understanding the risks presented to consumers is to analyze the candidate's digital footprint by identifying the vendors and associated domains executed every time a visitor accesses their website. On average, the candidates use 54 domains from 89 vendors. What's interesting is how these numbers increase from September to December: 66 to 111 domains and 38 to 70 vendors respectively. Almost every candidate uses social platforms— Facebook, Google, and Twitter. Interesting exception: Trump did not have Twitter executing on his candidacy website during the scanning periods.

As expected, the candidates used more technology vendors as their campaigns ramped up from September to December. Klobuchar's campaign website is a clear outlier, with almost 3 times more executing domains than Biden' website, the next closest. The Klobuchar digital footprint is large, signifying purposeful use of digital operations. However, it also means there is more unmanaged code executing on consumer devices—a risk.

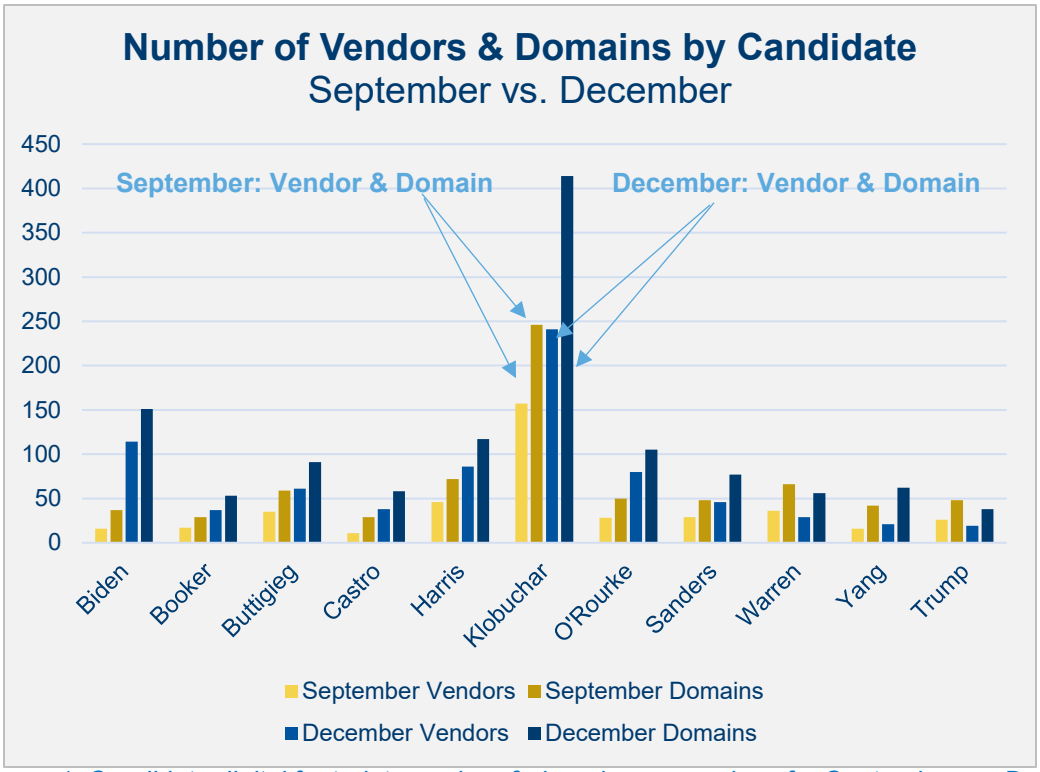


Figure 1: Candidate digital footprint, vendors & domains comparison for September vs. December

Domain classification reveals extent of third-party code

Majority of executing code on candidate websites are advertising and marketing technologies.

Domains can be classified into 4 high-level categories to provide a more comprehensive view of the candidates' digital environments:

- **Ad/MarTech:** advertising or marketing technology stack used to power the digital experience, i.e., ad server, analytics, data management platform, etc.
- **Candidate**: owned and/or operated code directly managed by the candidates' teams, i.e., their own website promotions, donation platform, etc.
- **Core Tech**: general technology services required to run any website, i.e., content delivery network, hosting, content management system, etc.
- **Warning:** code with malicious or unverified relevance to the website's execution, i.e., malware, anomalous activity, masked ownership, etc.

Together, Ad/MarTech, Core Tech and Warning represent third-party code—very little code is developed by the candidates' teams. In all, an average 81% of code that executes the consumer experience is from digital third-party vendors (77% in September vs 85% in December).

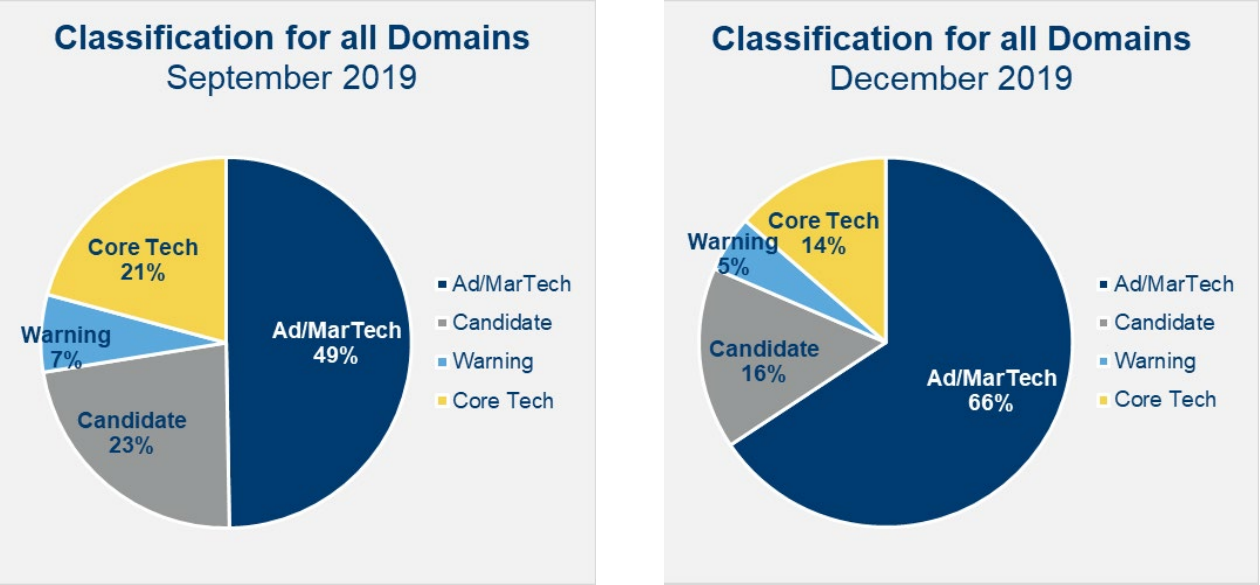


Figure 2: Collective domain classifications for all candidate websites

Even more alarming is the use of malicious domains, captured under the Warning classification. Every candidate website executed a suspicious domain when accessed by a consumer; these domains could have a history of suspicious activity, mask their ownership, or be overtly malicious. Inability to verify domain ownership is a red flag. This type of obfuscation is basic tactic adopted by bad actors, as legitimate enterprises associate their brand and legal entity to their digital properties. In addition, several of these domains were traced to legal entities based in China—a major election security concern when it comes to misinformation. The Warning activity threatens a website's security posture, the consumers who visit these websites, and the health of the broader digital ecosystem.

Domain Classification by Candidate Website

	Candidate	Ad/MarTech	CoreTech	Warning	3PC (%)
Biden	8	14	14	1	78%
Booker	9	12	7	1	69%
Buttigieg	13	31	11	4	78%
Casto	6	9	11	3	79%
Harris	16	43	10	3	78%
Klobuchar	41	161	27	17	83%
O'Rourke	14	21	14	1	72%
Sanders	13	19	11	5	73%
Warren	14	23	24	5	79%
Yang	16	12	10	4	62%
Trump	15	16	12	5	69%

Figure 3: Third-party code presence on candidate websites

In comparison to the other websites, the Klobuchar website uses the most third-party code (83%). The larger digital footprint also yields a corresponding increase in domains with a Warning classification. The next five sites rely on 78% or 79% third-party code, but they have comparatively smaller digital footprints and less Warning domains.

Every candidate website executed a “Warning” domain during the evaluation period

Domain with potential security and brand damaging incidents

Campaign unknowingly redirected visitors to a website serving adware, typically unwanted content

During the analysis, consumers were exposed to unwanted, potentially malicious activity. In each incident (most recently detected in February 2020), the Klobuchar website linked to a news story hosted on two different media websites. The media websites delivered adware programs. These programs negatively impact the user experience and automatically install on the device additional programs, many of which may contain malicious software. This includes invasive toolbars and ads that obstruct or interfere with web browsing, deliver pop-up and pop-under ads, override search engines and home pages, and alter search engine results. While the incidents were only detected a few times via the Klobuchar website, one has been affecting other digital properties for more than 9 months.

Cookies enable tracking of consumers

To enable continuous messaging, candidate websites use cookies to consistently target consumers when they are on other websites.

Ubiquitous across the digital ecosystem, cookies are small text files used by websites and third-party entities to learn more about the user. During a consumer’s website visit, the website’s server sends a cookie to the consumer’s browser where it is stored on the visitor’s device for a predetermined length of time—anywhere from the specific session up to thousands of years. Cookies enable website functionality (preferences, analytics, page history/back button, region-specific data, i.e., weather) and also track the user’s digital history or online behavior. Left unchecked, cookies can capture copious amounts of user data which is then re-used (typically sold) by others in the digital ecosystem to target users with specific messaging. Not only can this activity irritate consumers with poorly timed messaging, but it can also violate data protection regulations emerging across more than 40 states.

Third-party cookies are created by domains *other* than the one currently being visited, often without the website’s knowledge. In many instances, third-party cookies are generated by advertising and marketing firms, and each candidate website drops cookies from these entities.

Each candidate uses cookies to learn more about their constituents and to help deliver continuous messaging while these individuals access other unrelated websites, i.e., news, weather, ecommerce, etc. On average, website visitors are exposed to 146 cookies every time they access a candidate's website, (126 in September, 166 in December). The number of cookies deployed ranged from 24 (Biden) to 482 (Klobuchar) in September and the range increased in December, 48 (Trump) up to 701 (Klobuchar).

Cookie Total

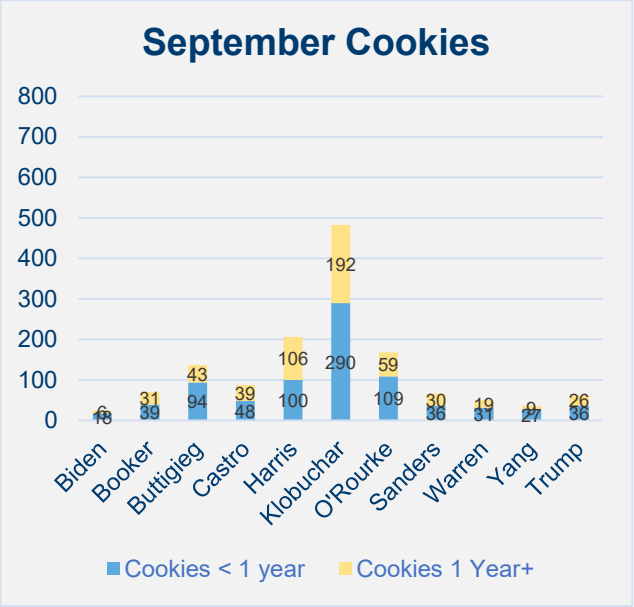
	September	December	Change
Biden	24	298	1142%
Booker	70	58	-17%
Buttigieg	137	138	1%
Castro	87	67	-23%
Harris	206	132	-36%
Klobuchar	482	701	45%
O'Rourke	168	172	2%
Sanders	66	96	45%
Warren	50	62	24%
Yang	36	49	36%
Trump	62	48	-23%

Figure 4: Total cookie count change during period

The change in cookie count indicates a ramp up in campaign outreach activity. The candidate is widening their target base and using more tracking capabilities to ensure their message repeatedly is placed in front of the right individuals.

More than 40% of those cookies have a lifespan greater than 1 year in both periods, with almost every candidate dropping cookies with a 20-year lifespan in both September and December. This means that the candidates (and a few third-party vendors) can actively collect information on the consumer's digital behavior for the next 20 years. Even more extreme, Biden and Klobuchar use cookies with lifespans of 68 and 99 years.

Cookies help candidates continuously target and deliver their messaging to voters when these individuals access other websites and mobile apps.



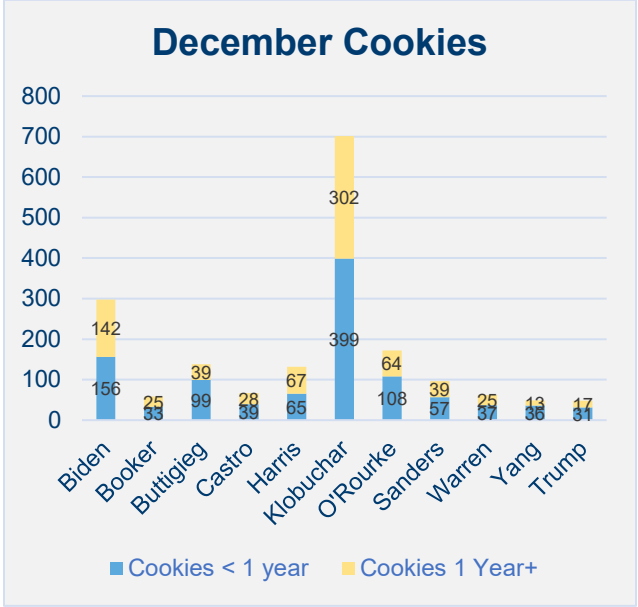


Figure 5: Cookies by lifespan in September versus December

CCPA – an emerging data protection regulation in 2020

Consumers have more choice when it comes to collection of their data and how it is used to target them with customized messaging and advertisements as they browse the broader digital ecosystem

In the absence of a national consumer privacy law, the California Consumer Privacy Act (CCPA) made waves in June 2018 when it was passed with an expected January 2020 effective date. Often referred to as a mini-GDPR or GDPR-lite, CCPA expands consumer protections for California residents, including those temporarily outside the state.[13] The protections grant more control of personal data—from what is collected, by whom, and how it's used to also mandating the honor of deletion requests and opt-out rights.

Candidate websites and mobile apps need to comply with CCPA. They collect data during each user session, including data from individuals with California-based devices. In addition, the website needs to provide consumers with a process to easily access, request deletion or opt out of the sale of their personal information–something not readily visible for the Harris or Yang websites, candidates from California. Assuming they meet the threshold (one criterion is $25 million or more in annual gross revenue), candidate inability to prove CCPA compliance exposes the campaign to financial penalties ranging from $2,500-$7,500 per incident. While the financial penalty isn't onerous, the brand damage is significant, especially if consumers exercise their right to bring lawsuits against a candidate.

Representing 55 electoral votes, California residents are important voting targets

DONATION EXPERIENCE IS RIPE FOR COMPROMISE

Presidential campaigns use their websites as a fundraising tool, providing options for individuals to purchase campaign promotional items or to make direct donations. In this regard, campaign websites function as ecommerce operations. The candidates rely on one of two different platforms: BigCommerce, an Australian entity, and Shopify, a Canadian entity.

Evaluation of a typical donation journey involved analysis of executing code of the relevant page at each stage of the process: home/main, donation/buy now, payment/pay now, and confirmation/thank you for your order. The amount of executing code varies throughout the donation journey.

PCI Compliance is inadequate for securing website transactions

Industry-driven standard fails to protect consumers during the donation process

As ecommerce operations, candidate websites need to follow PCI Data Security Standards (PCI DSS) in order to accept credit card payments. Credit card associations established PCI Security Standards Council to govern and enhance the understanding of security standards for payment account security. They developed the PCI DSS standards for any entity that stores, processes or transmits cardholder data. Among other things, PCI DSS requires protection of cardholder information, defense against hacking/malware and regular review of security processes (i.e., quarterly vulnerability scan).

The websites' ability to collect consumer personal and financial information without knowing who has access to that information points to the ineffectiveness of the standard.

Domain variability creates an ideal attack surface for bad actors

The amount of changing code highlights a lack of control over what executes on consumer devices when they access the candidate websites

As the individual moves through the donation journey the amount of code executing on their browser changes. Each page in the journey has its own vendors and data collection activity, and sometimes neither is warranted.

In general, individuals will be exposed to 9 to 56 different vendors when they make a purchase or donation via a campaign website. The Klobuchar campaign presents a more controlled digital footprint compared to the other candidates because the overall number of domains is low, and it does not fluctuate as much from one page to another. In contrast, the Warren campaign uses almost double the number of domains as other campaigns and four times higher than Klobuchar, averaging 44 domains across all pages. In fact, at almost every stage Warren uses the most code, presenting a large digital footprint that requires more oversight. (Figure 6)

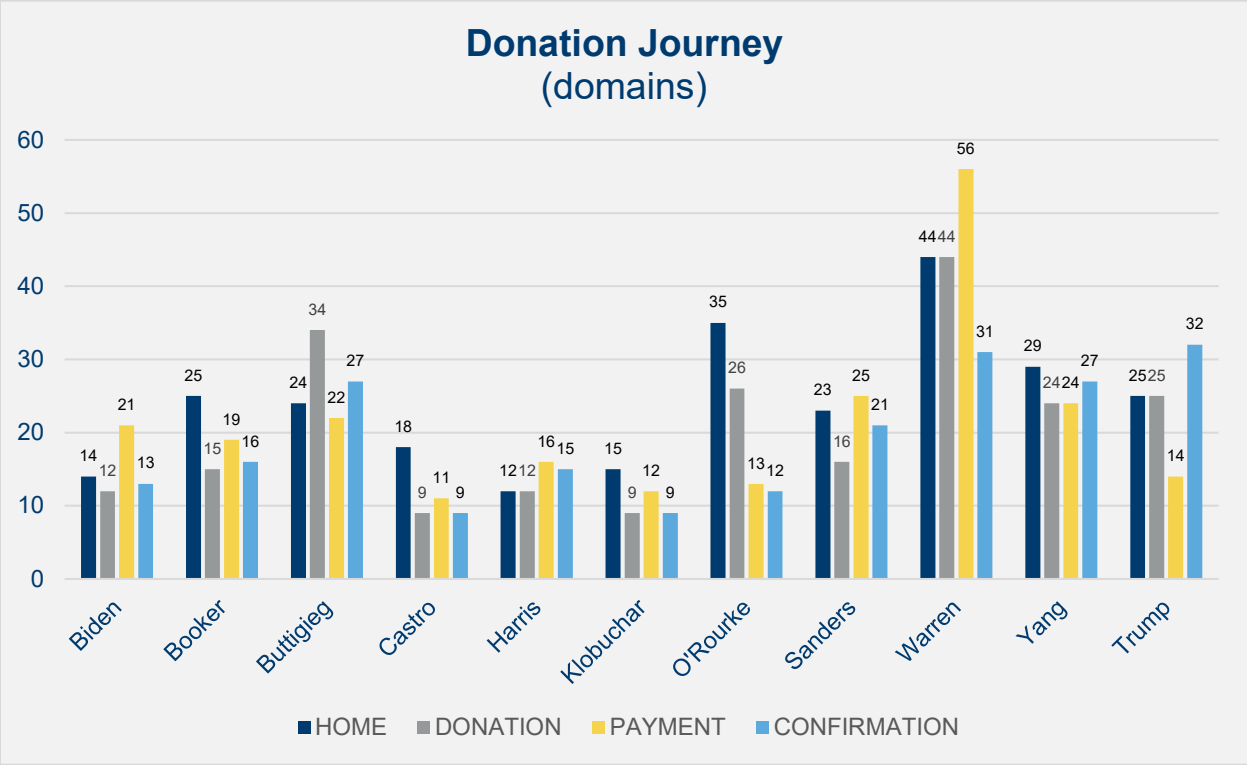


Figure 6: Domains executing during a consumer's Donation Journey

As a matter of best practice, campaigns should be vigilant to what executes on their candidate websites. That does not appear to be the case. In several campaign websites, the number of executing domains increases on the payment page with little relevance to the actual transaction. The Biden, Harris, Sanders and Warren websites have more domains on the purchase page than any other page.

A closer look reveals that more than 71% of executing code on each candidate payment page has zero relevance to the transaction, with the Booker campaign exhibiting more than 95% of unnecessary code. The mere presence of these third parties is both a security and data privacy risk as unnecessary code bloats a website, creating vulnerabilities to be exploited.

Donation Page
(non-payment processing domains)

Biden	71%	O'Rourke	92%
Booker	95%	Sanders	72%
Buttigieg	77%	Warren	93%
Castro	73%	Yang	75%
Harris	81%	Trump	79%
Klobuchar	75%		

Figure 7: Domains executing on donation pages that do not facilitate payment processing

Cookies track consumers throughout the donation journey

While more limited than general website browsing, cookies dropped during the donation journey can still surreptitiously collect consumer information

When donating to or purchasing a promotional item from a candidate website, individuals are subjected to at least 23 cookies. Unsurprisingly, the large number of domains on Warren's payment page corresponds to a large number of cookies on the same page. The significant number of cookies on the home and donation pages for Buttigieg, Warren, and, to some degree, O'Rourke serve an interesting purpose. These cookies allow the candidates to learn more about their visitors, especially those who are investigating a possible donation. The candidates use the cookies to target the users throughout the digital ecosystem, re-iterate their messaging, and, hopefully, drive the user to a donation in the future—regardless if they've already made a donation.

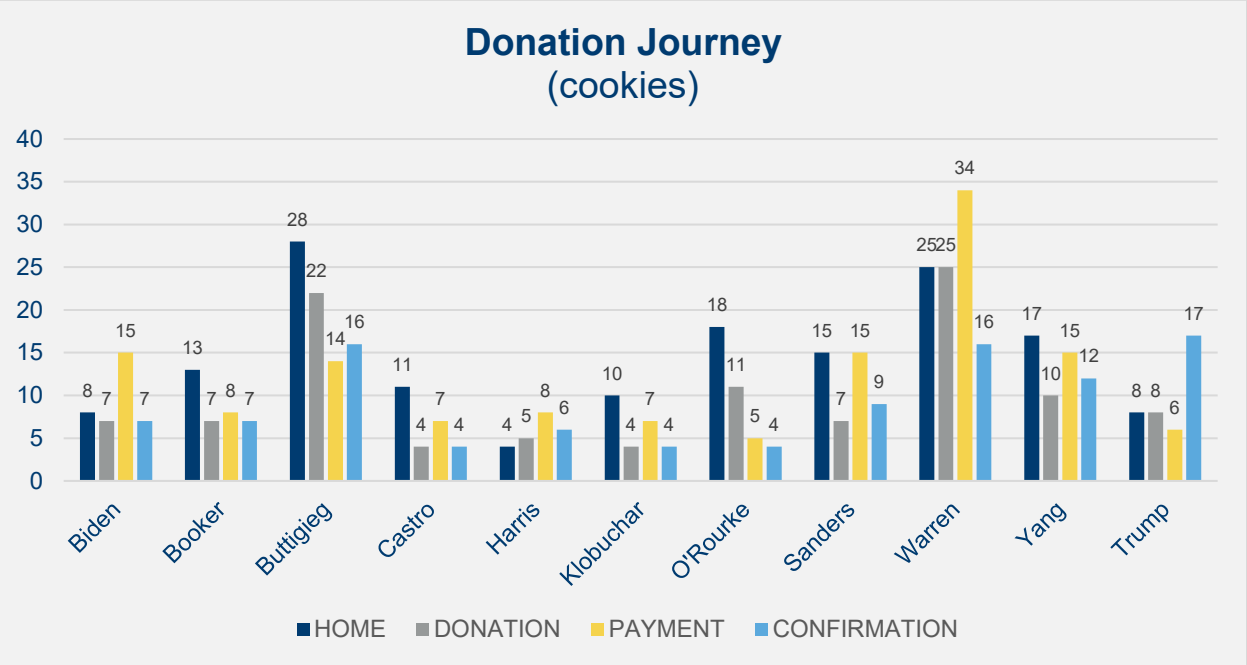


Figure 8: Cookies dropped during the consumer's Donation Journey

Conclusion: Digital Risk Is Evident

Candidates—like enterprises—are responsible for the code their websites and mobile apps put on consumer devices. Regardless if this code is malicious or collecting personal data, the presence of unmanaged third-party code demonstrates vulnerabilities in candidate websites. This third-party code can be used to surreptitiously collect consumer information to target individuals with misinformation or distribute malware and bots for future attacks.

The digital environment is dynamic. To defend against attacks and the misuse of consumer information, campaigns need to pay more attention their websites or mobile apps. Specifically, they should:

- Continuously monitor the website from the consumer's point of view to capture the entire code base involved in rendering each page accessed
- Understand the provenance of all executing code; digital vendors may have multiple domains performing different functions
- Analyze the necessity for all code accessing consumer devices to minimize unnecessary data collection, and, as a bonus, realize improved page speed
- Document, communicate and enforce operational policies with digital vendors to evaluate their compatibility and compliance with your requirements
- Hire qualified Security teams with authority, tools and resources so they can more effectively safeguard digital assets
- Publicize their IT or Security lead to enable threat sharing among candidate teams and streamline complaint reporting for consumers

Today's headlines are clear: compromise of digital third-party code remains a significant threat to candidate websites and the consumers who access them. To minimize the attack surface, candidate websites need to manage their digital vendors and limit data tracking.

Methodology

The Media Trust carried out client-side scans of 11 presidential candidate websites in two phases: (1) continuous during the months of September and December, and (2) a one-time donation journey during the third week of September. The Media Trust leverages its proprietary website, mobile app and ad tag SaaS-based service to scan these public-facing websites on a continuous, 24/7 basis using a series of user profiles to replicate a true visitor experience. This client-side monitoring identifies all vendors—third, fourth and sometimes fifth parties—executing on the website, assesses for security vulnerabilities, analyzes data collection activities and detects performance issues.

The information contained in this report was collected during the stated time frame using a generic scanning algorithm and basic desktop-only user profiles primarily based in McLean, Virginia USA. It does not address mobile or gaming devices, targeted user behavior profiles, geographies or any advertising or revenue-generating tags on the websites.

About The Media Trust

The Media Trust is on a mission to fix the digital ecosystem. Through continuous monitoring of websites and mobile apps, we provide transparency into the complex relationships delivering the consumer experience. More than 600 premium enterprises, media publishers, ad networks/ exchanges, and agencies—including 40 of comScore's AdFocus Top 50 websites—rely on The Media Trust to identify and remediate security, data protection, and quality risks which can lead to regulatory fines, depressed inventory value, revenue loss and brand damage. For more information, visit www.mediatrust.com.

[1] https://www.darkreading.com/endpoint/iran-caught-targeting-us-presidential-campaign-accounts/d/d-id/1336007
[2] https://www.infosecurity-magazine.com/news/researchers-lift-lid-politically/
[3] https://www.cisomag.com/fbi-warns-of-ddos-attacks-on-state-level-voter-websites/
[4] https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf
[5] https://www.law.com/legaltechnews/2020/01/23/experts-presidential-hopefuls-cant-afford-to-skim-on-ciso-role/
[6] https://www.cyberscoop.com/2020-elections-cybersecurity-threats-mick-baccio-political-campaigns-struggle-information-sharing/
[7] https://www.cnbc.com/2019/11/03/google-is-silent-on-political-ads-amid-facebook-twitter-spat.html
[8] https://www.mediapost.com/publications/article/346935/us-political-ad-spending-to-approach-7-billion.html and https://www.emarketer.com/content/political-ad-spend-to-reach-6-billion-for-2020-election?ECID=SOC1001
[9] https://www.washingtonpost.com/politics/democrats-push-election-security-bill-amid-impeachment/2019/10/08/bf9b2632-e9ef-11e9-a329-7378fbfa1b63_story.html
[10] https://techcrunch.com/2020/01/15/buttigiegs-ciso-resigns-leaving-no-known-cybersecurity-chiefs-among-the-2020-candidates/
[11] https://www.usnews.com/news/best-countries/articles/2019-10-11/internet-group-says-most-us-presidential-candidates-have-cybersecurity-flaws
[12] The website now redirects to a grass roots volunteer effort, “Powered by People”
[13] CCPA Infographic: https://mediatrust.com/resources/infographic-california-consumer-privacy-act