Hunting for U.S. Presidential Election-Related Domain Threats in the DNS

Table of Contents

Executive Report

As if the attention surrounding the upcoming U.S. presidential elections is not enough, the WhoisXML API research team may have unveiled thousands of potential sources of disarray—election-related cybersquatting domains. These domains may be a lucrative source of income for some people. Case in point? The domain HarrisWalz[.]com was recently sold for US$15,000 at a 99.94% profit margin.

Cybersquatting domains may also be used for more nefarious purposes. For example, the same cybersquatter who sold HarrisWalz[.]com also sold ClintonKaine[.]com to an anonymous buyer back in 2016. The domain was ultimately used to publish anti-Clinton news during the election period.

Recently, Microsoft warned that nation-state attackers employ impersonation and other tactics, techniques, and procedures (TTPs) to sow discord and undermine elections. Cybersquatting domains can be among their tools.

Our study focused on domains and subdomains that contain the names of presidential candidates and other election-related strings. We discovered:

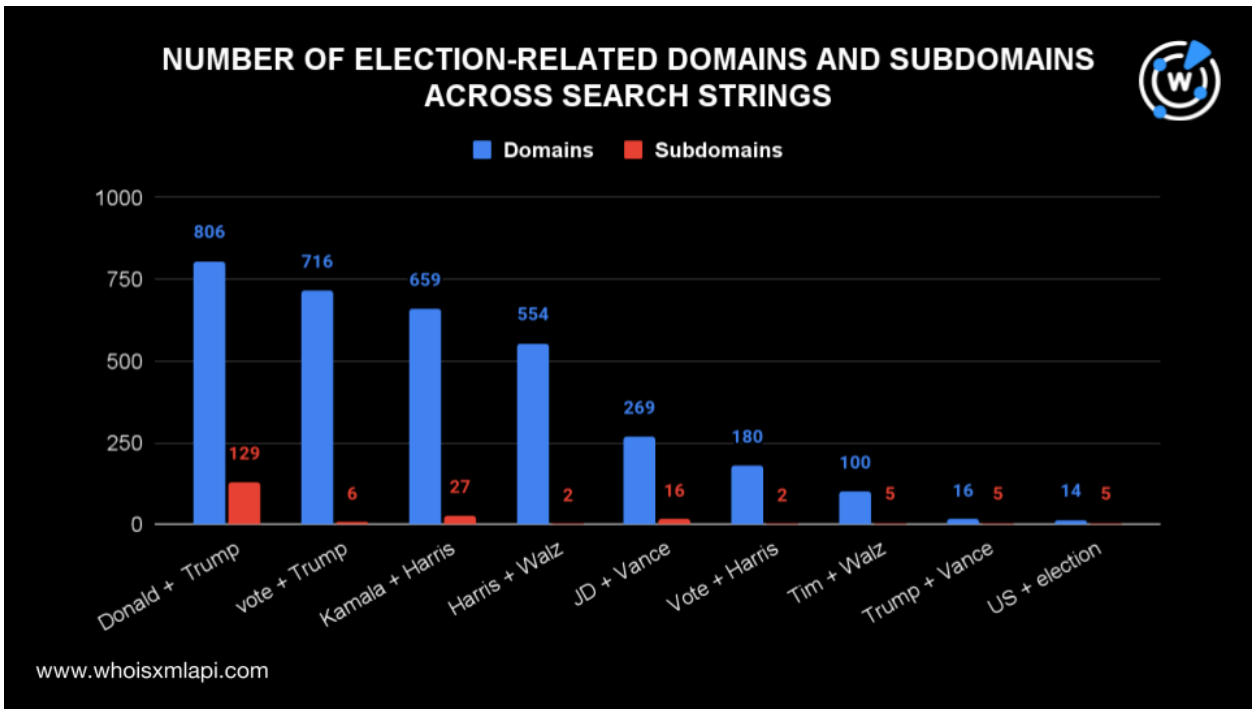
- 2,320 unattributable election-related domains
- 197 election-related subdomains (yielding 121 unattributable root domains)
- 541 email-connected domains
- 1,165 IP addresses, 775 of which were malicious

Uncovering Election-Related Cyber Resources

To begin our investigation, we used Domains & Subdomains Discovery to search for election-related web properties. Specifically, we looked for domains and subdomains added from 1 January to 15 August 2024 that contained these strings:

- **Kamala** + **Harris**
- **Tim** + **Walz**
- **Harris** + **Walz**
- **Vote** + **Harris**
- **Donald** + **Trump**
- **JD** + **Vance**
- **Trump** + **Vance**
- **vote** + **Trump**
- *Starts with* **US** + **election**

We found a total of 3,314 domains and 197 subdomains, after removing duplicates, with the distribution shown in the chart below.



Attribution of the Election-Related Domains

We then sought to determine if any of the web properties in the study were under the control of the candidates or the U.S. government. To do that, we first obtained the WHOIS record details of the relevant official domain names, namely:

- donaldjtrump[.]com
- kamalaharris[.]com

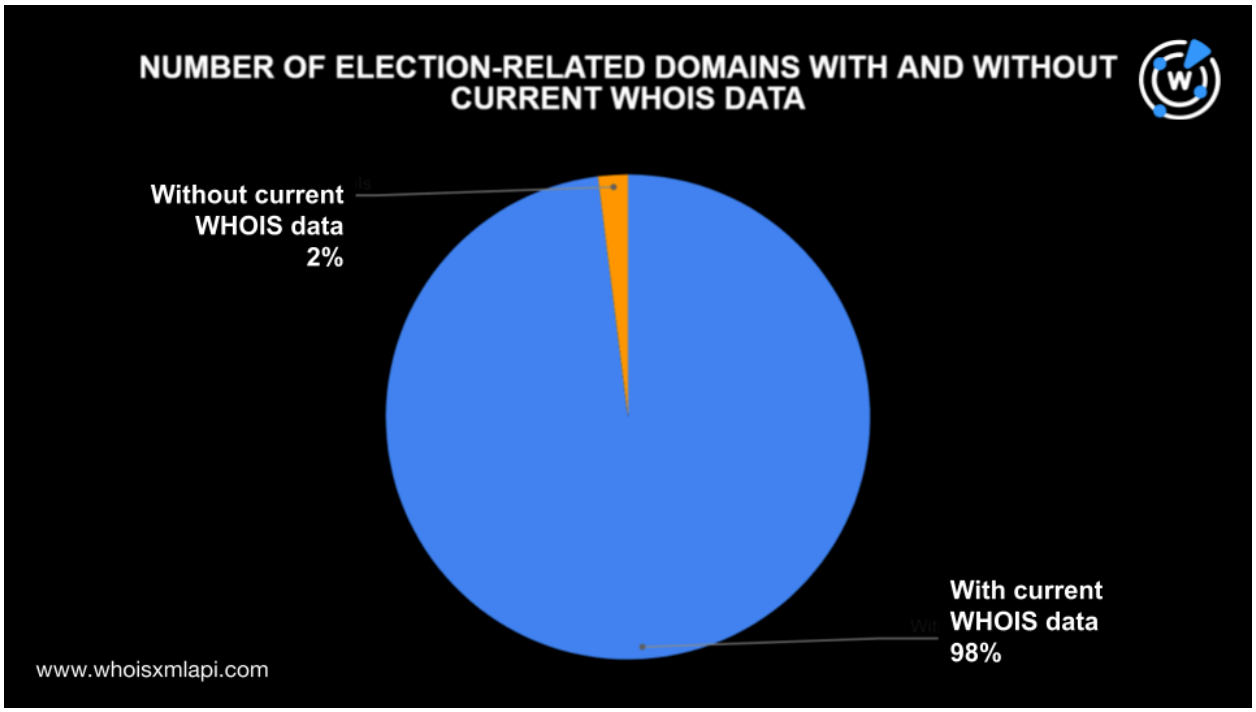
- walzflanagan[.]org
- usa[.]gov

We did not find any official domain dedicated to vice presidential candidate JD Vance. We also included usa[.]gov since it hosted the official website for the U.S. elections.

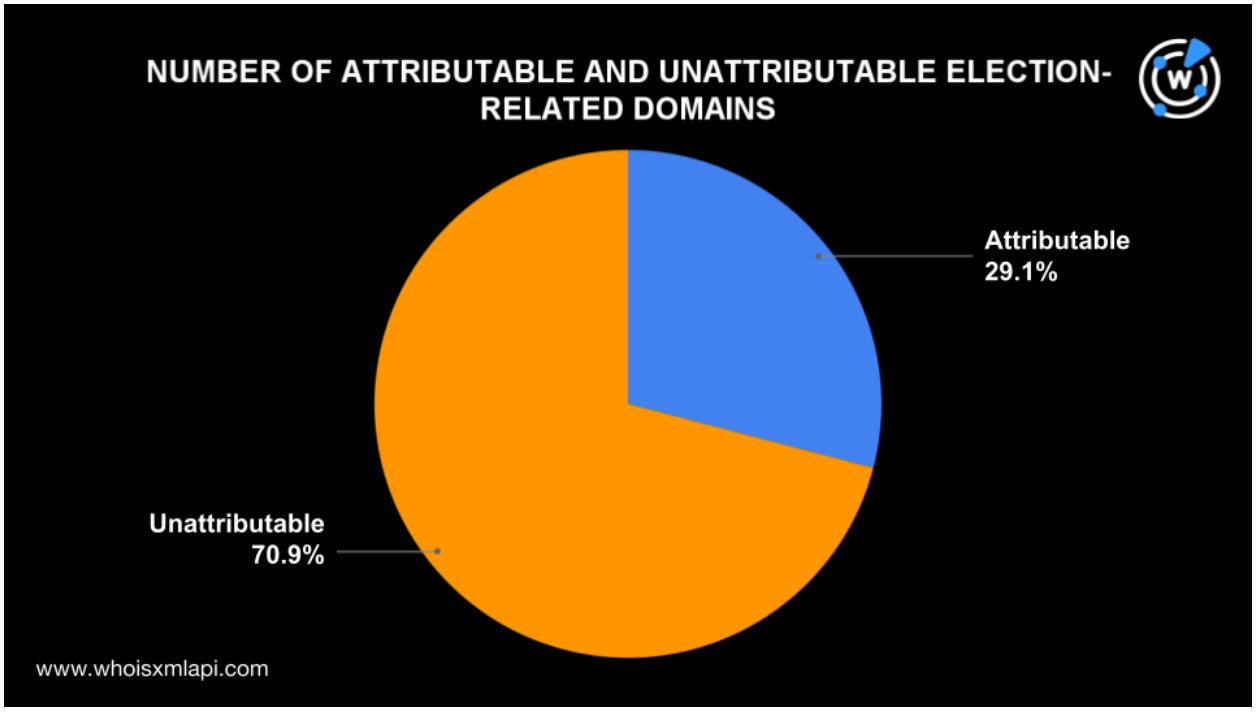
Our bulk WHOIS lookup for the four domains revealed they all had privacy-protected WHOIS information. That means we could not publicly attribute any election-related domain to the email addresses or names of the entities managing the official domains.

However, the WHOIS information includes other vital data points, such as name servers and registrant telephone numbers.

Running a bulk WHOIS lookup on 3,511 election-related domains and subdomains revealed that 70 did not have current WHOIS details.



After checking for overlaps between the WHOIS information of the four official domains and the 3,441 election-related domains with current WHOIS data, we were able to exclude 1,000 unique domains from further analysis since they shared the exact name servers of kamalaharris[.]com (i.e., seven domains) and the registrant telephone numbers of donaldjtrump[.]com (i.e., 986 domains) and kamalaharris[.]com (i.e., seven domains).

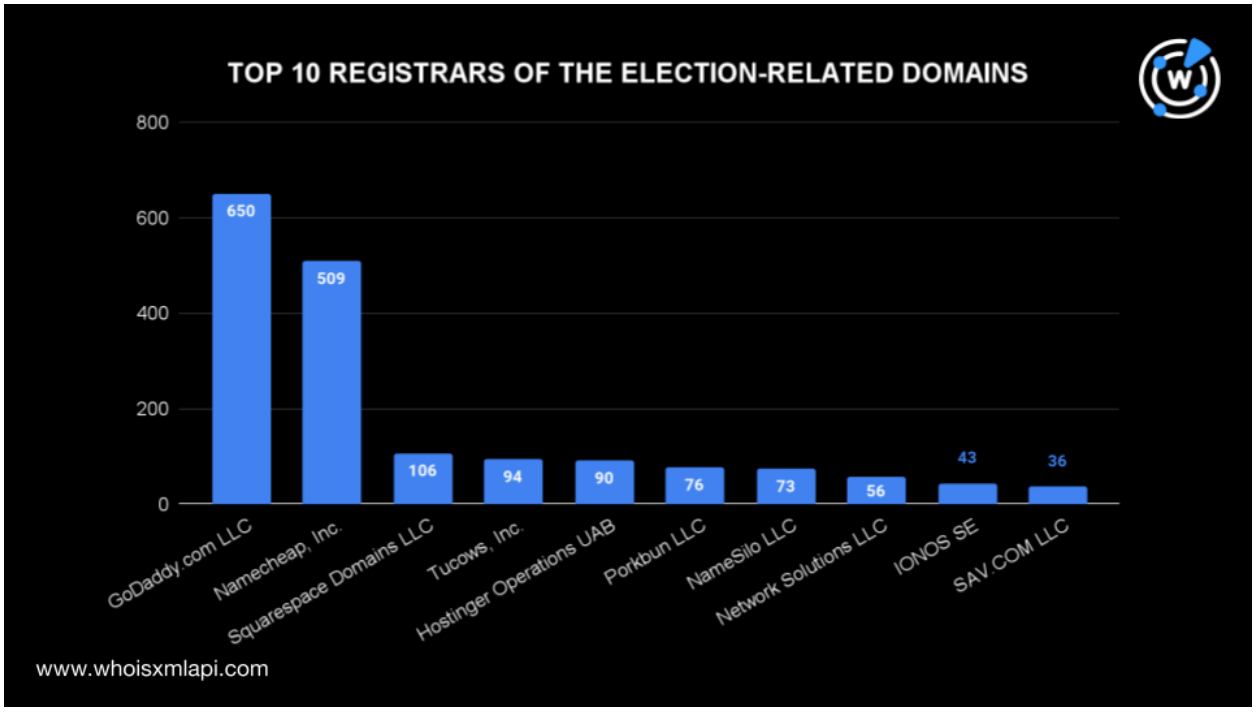


We were left with 2,441 domains comprising 2,320 election-related domains and 121 root domains of the election-related subdomains that could not be attributed with high confidence to the same entities managing the official domains. These can be potentially considered cybersquatting domains and so were subjected to further analysis.

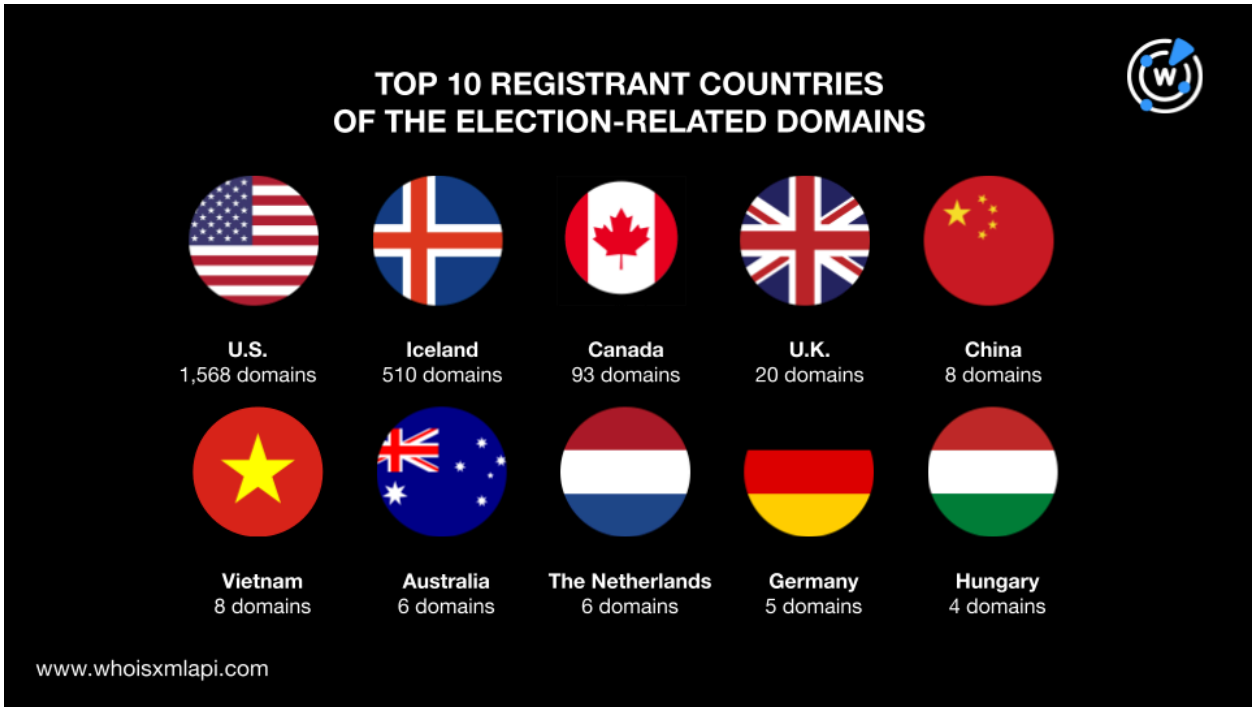
Unmasking Who's behind the Election-Related Domains

The WHOIS information of the 2,441 potentially cybersquatting domains revealed that:

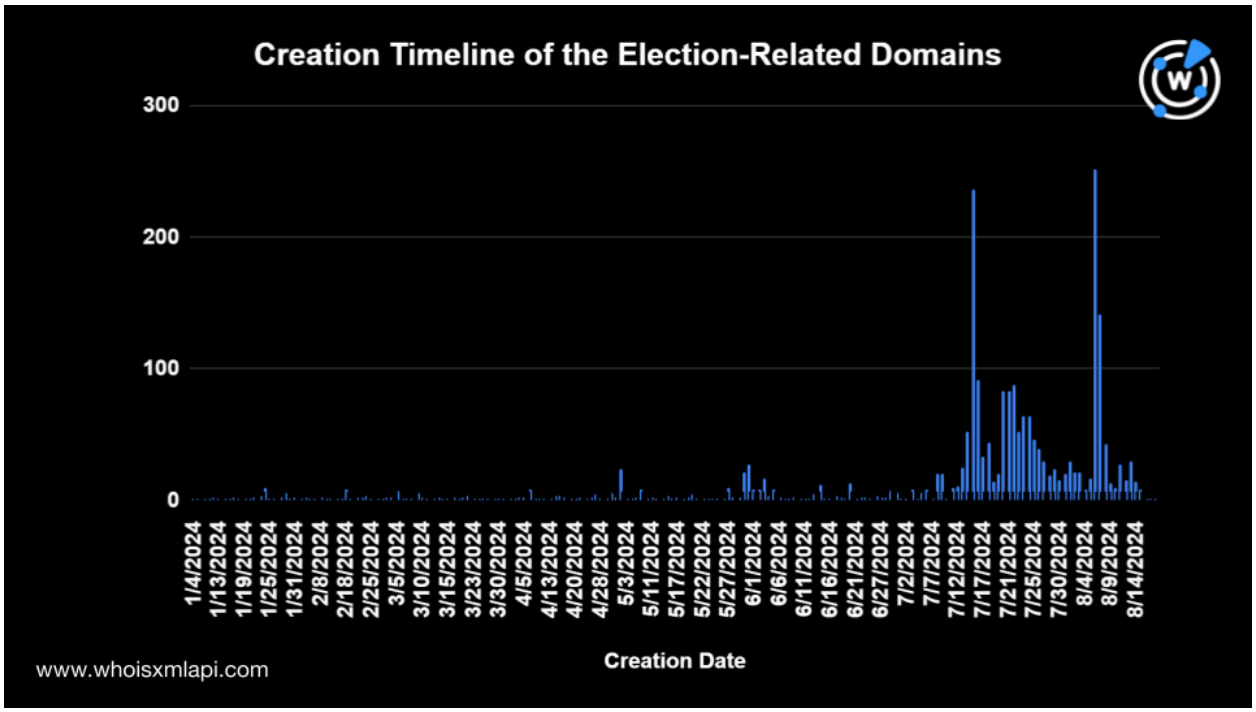
- GoDaddy.com LLC was the top registrar, administering 650 domains. It was followed by Namecheap, Inc. (509 domains); Squarespace Domains LLC (106 domains); Tucows, Inc. (94 domains); Hostinger Operations UAB (90 domains); Porkbun LLC (76 domains); NameSilo LLC (73 domains); Network Solutions LLC (56 domains); IONOS SE (43 domains); and SAV.COM LLC (36 domains). 591 domains were distributed across more than 100 registrars, while 117 did not have current registrar data.



- A majority of the domains, 1,568 to be exact, were registered in the U.S. The rest of the top 10 geolocation countries included Iceland (510 domains), Canada (93 domains), the U.K. (20 domains), China (eight domains), Vietnam (eight domains), Australia (six domains), the Netherlands (six domains), Germany (five domains), and Hungary (four domains). 56 domains were registered across 25 other countries, while 157 domains did not have current registrant country information.



- Most of the domains' WHOIS creation dates coincided with major election-related events. Registrations spiked a few days after the attempted assassination of Donald Trump on 13 July 2024. A higher uptick was detected on 6 August 2024, a day after Kamala Harris was confirmed as the Democratic presidential nominee.



Digging Up Deeper Connections of the Election-Related Domains

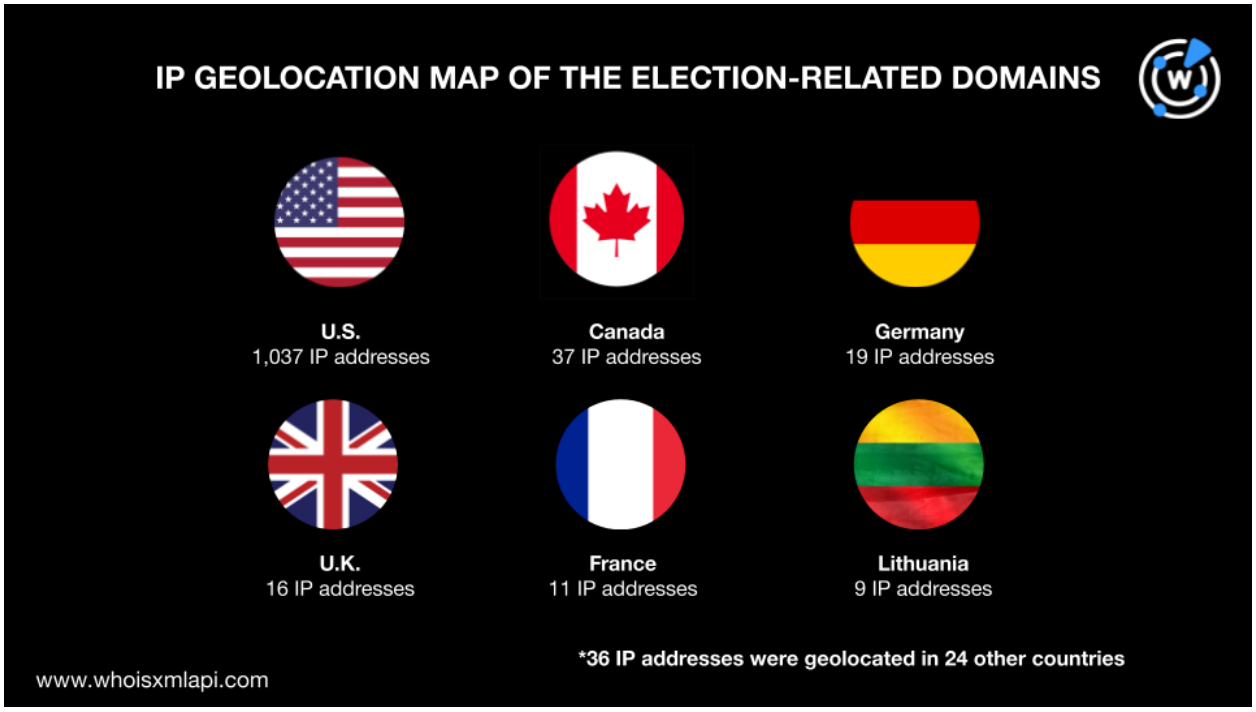
The next step was to find more web properties potentially related to the cybersquatting domains. To do that, we extracted 520 registrant email addresses from the historical WHOIS records of the 2,441 domains. Only 61 were public email addresses.

Pivoting off these email addresses using Reverse WHOIS API, we found 1,343 email-connected domains. However, since two of the email addresses were used to register more than 300 domains each, we excluded them from the list. After removing duplicates and filtering out domains found on the original list of 2,441 election-related domains, we were left with 541 additional email-connected domains. Some of these domains contained the name variations of the candidates and other famous personalities.

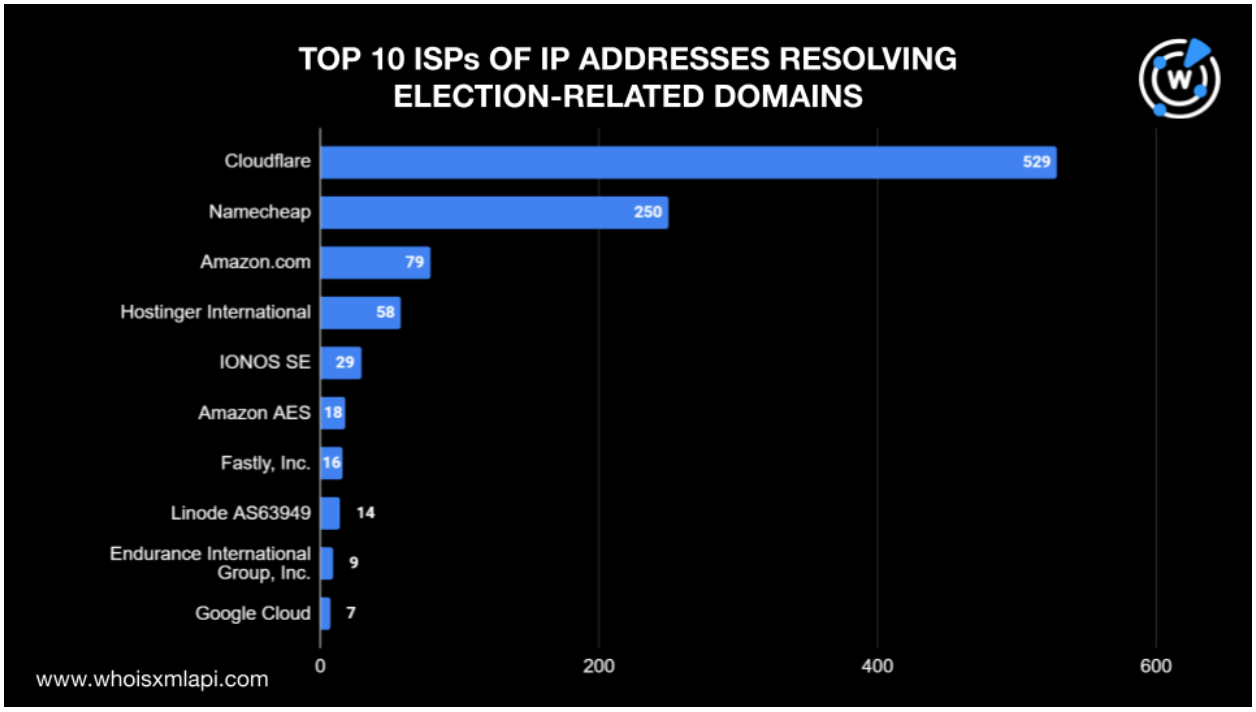
We then ran DNS lookups on the 2,441 domains, leading us to 4,072 IP resolutions involving 1,165 unique IP addresses. It's important to note that none of these IP addresses resolved the official domains.

A bulk IP geolocation lookup for the 1,165 IP addresses revealed that:

- Although a majority (1,037 IP addresses) were geolocated in the U.S., 128 IP addresses traced back to other countries, such as Canada (37 IP addresses), Germany (19 IP addresses), the U.K. (16 IP addresses), France (11 IP addresses), Lithuania (nine IP addresses), and 24 other countries all over Asia and Europe (36 IP addresses).



- Cloudflare managed almost half of the IP addresses. The rest of the top 10 ISPs included Namecheap (250 IP addresses), Amazon.com (79 IP addresses), Hostinger International (58 IP addresses), IONOS SE (29 IP addresses), Amazon AES (18 IP addresses), Fastly (16 IP addresses), Linode AS63949 (14 IP addresses), Endurance International Group (nine IP addresses), and Google Cloud (seven IP addresses).



Possible Malicious Connections of the Election-Related Domains

Looking up the IP addresses on Threat Intelligence API revealed that 775 or 66.52% have already been tagged as indicators of compromise (IoCs) in various types of cyber threats. These malicious IP addresses hosted 2,077 of the 2,441 election-related domains in the study. Some examples are shown in the table below.

MALICIOUS IP ADDRESS	ASSOCIATED THREAT TYPES	RESOLVING DOMAIN
3[.]64[.]163[.]50	Attack Command and control (C&C) Generic Malware Phishing Spam	0xdonaldjtrump[.]xyz
15[.]197[.]148[.]33	Attack C&C Generic Malware Phishing Spam	2024-harriswalz[.]org

3[.]33[.]130[.]190	Attack C&C Generic Malware Phishing Spam	2024-harriskelly[.]vote 2024donaldtrump[.]vote
96[.]126[.]123[.]244	Attack C&C Generic Malware Phishing Spam	cdndonaldjtrump[.]com harrisswalz[.]com kamalaharriscampaign[.]us trumpjdvance[.]org

Our investigation of the election-related web properties enabled us to discover 4,223 artifacts comprising 2,320 domains, 197 subdomains (yielding 121 unattributable root domains), 541 email-connected domains, and 1,165 IP addresses. Aside from being unattributable to legitimate entities managing the official domains of the imitated personalities, it's also alarming that 85.09% of the election-related web properties resolved to malicious IP addresses.

If you wish to learn more about the products used in this research, please don't hesitate to contact us.

Disclaimer: *We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.*

Appendix: Sample Artifacts

Sample Election-Related Cybersquatting Domains

- 0xdonaldjtrump[.]xyz
- 0xdonaldtrump[.]xyz
- 2024-harriswalz[.]org
- 2024-harriskelly[.]vote
- 2024donaldtrump[.]vote
- 2024donaldtrumpmypresident[.]tv
- 2024harris-beshear[.]vote
- 2024donaldtrumpmerch[.]com
- 2024harriskelly[.]vote
- 2024harriscooper[.]vote
- 2024harris-kelly[.]vote
- 2024harris-walz[.]vote
- 2024harris-cooper[.]vote
- 2024harris-buttigieg[.]vote
- 2024harriskellyvote[.]org
- 2024harriswalz[.]store

- 2024harriswalz[.]xyz
- 2024harriswalz[.]me
- 2024kamalaharris[.]store
- 2024harriswalz[.]org
- 2024harriswalz[.]us
- 2024trumpburgum[.]vote
- 2024trump[.]vote
- 2024trumpvance[.]xyz
- 2024trumpvance[.]store
- 2024trump-vance[.]vote
- 2024trumpvance[.]org
- 2024trumpvance[.]info
- 24trumpvance[.]com
- 34reasonstovotefortrump[.]com
- 45donaldjtrump48[.]com
- 24kamalaharris[.]com
- 24harriswalz[.]com
- 47kamala-harris[.]com
- 47trumpvancetransition[.]org
- 48presidentdonaldjtrump[.]com
- 4donaldtrump[.]us
- 4harriswalz[.]com
- 4trumpvance[.]com
- 4kamalaharris[.]com
- 4trumpvance[.]net
- 4trumpvance[.]org
- aikamalaharris[.]com
- 48donaldjtrump[.]org
- akasforharris[.]vote
- americafordonaldtrump[.]org
- americafordonaldtrump[.]us
- americaforkamalaharris[.]org
- aldonaldbintrump[.]xyz
- americahatesfascistslikedonaldjtrump[.]com
- americahatesfascistslikedonaldjtrump[.]net
- americahatesfascistslikedonaldjtrump[.]org
- americansagainstdonaldttrump[.]org
- americansforkamalaharris[.]org
- americanshatefascistslikedonaldjtrump[.]com
- americansforkamalaharris[.]us
- americansvotetrump[.]store
- aidonaldtrumpstore[.]com
- americanshatefascistslikedonaldjtrump[.]org
- americavotesharris[.]com
- armeniansforharriswalz[.]com
- askdonaldtrump[.]ai
- artofthesurgedonaldtrump[.]com
- assassinationattemptdonaldtrump[.]com
- assassinationattemptondonaldtrump[.]com
- auditmytrumpvote[.]com
- auntiesforkamaladeviharris[.]org
- auntiesforkamalaharris[.]org
- austinforharriswalz[.]com
- abortdonaldtrump[.]org
- armenianamericansforharriswalz[.]com
- americanshatefascistslikedonaldjtrump[.]net
- americaforkamalaharris[.]us
- alaskansforharriswalz[.]com
- banpornvotetrump[.]com
- banpornvotetrump[.]org
- beatdonaldtrump[.]us
- beatdonaldtrump[.]xyz
- believersfordonaldjtrump[.]org
- believersfordonaldjtrump[.]net
- betrumpsvote[.]com
- beatdonaldtrump[.]vote
- believersfordonaldjtrump[.]co
- believersfordonaldjtrump[.]com
- blackmenforharris-walz[.]org
- bitdonaldtrump[.]com
- bidenvotersfortrump[.]com

- blacksfortrump[.]vote
- blackvoters4trump[.]com
- blackmenforharris-walz2024[.]org
- blackvoters4harris[.]com
- blackvotersforharris[.]com
- bookofkamalaharris[.]online
- bookofdonaldtrump[.]vip
- borderczarkamalaharris[.]com
- bulletproofdonaldjtrump[.]co
- buyharriswalzmerch[.]com
- britsforharriswalz[.]com
- butler13donaldtrump[.]com
- bulletproofdonaldjtrump[.]com

Sample Election-Related Cybersquatting Subdomains

- www[.]kamalaharris[.]blue[.]kamala[.]blue
- kamalaharrissol-fun[.]pages[.]dev
- kamalaharris[.]org[.]cdn[.]bsd[.]net
- kamalaharris[.]branddive[.]com
- kamalaharriscbdoil[.]wixsite[.]com
- www[.]kamalaharris[.]votemeapp[.]com
- kamala-harris[.]fortniteskiny[.]eu
- go[.]kamalaharris[.]org[.]cdn[.]bsd[.]net
- kamala-harris-booty[.]mailforjesus[.]de
- kamala[.]harrisnis[.]not[.]black
- kamala-harris-impersonator[.]car-comfort[.]pl
- kamalaharrissol[.]github[.]io
- kamalaharris-oa[.]edge[.]targetedaction[.]net
- kamalaharrisconsultants[.]us[.]com
- when-kamala-harris-is-president[.]glitch[.]me
- kamalaharrisclaim[.]pages[.]dev
- kamalaharristoken-4m4[.]pages[.]dev
- kamala-harris-ass[.]kaawa[.]de
- kamalaharristoken[.]pages[.]dev
- kamalaharris[.]tibet[.]org
- kamalaharris[.]great-site[.]net
- kamalaharris[.]web3crypro[.]com
- kamalaharrisimpersonator[.]aupairusainfo[.]de
- kamalaharris[.]votemeapp[.]com
- www[.]kamalaharris[.]org[.]cdn[.]bsd[.]net
- kamalaharrisstore[.]myshopify[.]com
- kamala[.]harris[.]is[.]not[.]black
- walzyoyjmtimrr34[.]europe-west4[.]sourcemanager[.]dev
- vq55fwtimdfsazspuhhq-pwalze-815257678-clientnsv4-s[.]akamaihd[.]net
- vq4f4ltimewhizpwalzq-f-c5b806f68-clientnsv4-s[.]akamaihd[.]net
- tim-walzs-proud-of-you[.]glitch[.]me
- tim-walz-fixed-your-bicycle[.]glitch[.]me
- undead4harriswalz[.]pages[.]dev
- undeadharriswalz[.]workers[.]dev
- harris[.]vote[.]gkh[.]edo[.]temporary[.]site
- www[.]harris[.]vote[.]gkh[.]edo[.]temporary[.]site
- realdonaldtrump-truth-social[.]cookie-ninja[.]de
- donald-j-trump-desk[.]antytrendy[.]pl
- ildonaldo-trumpo-twitter[.]cistus-creticus[.]de
- djdonaldtrumpet[.]webflow[.]io

- realdonaldtrumptruthsocial[.]kbo-su[.]de
- iwastheonethattriedtoshootatdonaldtrumpbutmyaimsucks[.]uk[.]to
- www[.]donaldjtrump[.]ru[.]com
- donald-j-trump[.]postweg[.]eu
- donaldtrumperc[.]pages[.]dev
- donaldtrump2024[.]samuraj[.]xyz
- donaldtrump2for2[.]com[.]trife[.]xyz
- free-donald-trump-gold-bars[.]gib-8-zak[.]de
- ildonaldtrumpo[.]sweetoclock[.]de
- donald-trump-news50283[.]therainblog[.]com

Sample Email Connected Domains

- justinbieber[.]us
- vanceforpresident[.]us
- madeintheai[.]us
- whocansave[.]us
- straitjoy[.]com
- killproject2025[.]us
- virtualcollegetours[.]us
- trumpandburgum[.]us
- myconservativeclub[.]com
- harrisbeshear2024[.]us
- harriswaltz2025[.]com
- gaintab[.]com[.]ng
- trumprubio2024[.]us
- vpwalz[.]us
- vance28[.]us
- commandertrump[.]us
- dollducks[.]com
- durianpizza[.]com
- newcalicutartscollege[.]com
- donaldtrumppotus[.]us
- kidsonbikes[.]us
- fearnot[.]us
- aiupdate[.]us
- kamilafor[.]us
- moveforkamala[.]com
- alysiapriami[.]com
- djtjdv[.]us
- derbyinthecloud[.]com
- aigeeks[.]us
- trump-gaetz[.]us
- loveabbeymusic[.]info
- houstonbaptistchurch[.]com
- linkphx[.]mobi
- healdetroit[.]com
- tvvillapark[.]com
- babyshib[.]us
- ideadomains[.]com
- koshermayaroyale[.]com
- walz2032[.]us
- trumpyoungkin2024[.]us
- castleholdingsllc[.]com
- stvalhouse[.]com
- fightfight[.]us
- tarasutaria[.]net
- dodusol[.]com
- draggycoin[.]com
- makeamericasmileagain2024[.]com
- affvoice[.]com
- krishnatrussroofing[.]com
- aiupdates[.]us

Sample IP Addresses

- 3[.]64[.]163[.]50
- 15[.]197[.]148[.]33
- 3[.]33[.]130[.]190
- 76[.]223[.]54[.]146

- 13[.]248[.]169[.]48
- 192[.]64[.]119[.]144
- 172[.]67[.]213[.]185
- 104[.]21[.]86[.]8
- 2606:4700:3030::6815:5608
- 2606:4700:3031::ac43:d5b9
- 192[.]64[.]119[.]219
- 104[.]21[.]32[.]219
- 172[.]67[.]136[.]123
- 2606:4700:3035::6815:20db
- 2606:4700:3036::ac43:887b
- 162[.]255[.]119[.]206
- 162[.]255[.]119[.]152
- 107[.]161[.]23[.]204
- 209[.]141[.]38[.]71
- 198[.]251[.]81[.]30
- 192[.]64[.]119[.]92
- 162[.]255[.]119[.]170
- 103[.]169[.]142[.]0
- 192[.]64[.]119[.]80
- 162[.]255[.]119[.]237
- 162[.]255[.]119[.]26
- 192[.]64[.]119[.]109
- 23[.]227[.]38[.]71
- 2620:127:f00f:b::
- 162[.]255[.]119[.]172
- 185[.]26[.]105[.]244
- 66[.]96[.]144[.]191
- 208[.]91[.]197[.]27
- 84[.]32[.]84[.]32
- 192[.]64[.]119[.]164
- 44[.]230[.]85[.]241
- 52[.]33[.]207[.]7
- 192[.]64[.]119[.]187
- 162[.]255[.]119[.]225
- 173[.]236[.]242[.]226
- 216[.]40[.]34[.]41
- 162[.]255[.]119[.]29
- 192[.]64[.]119[.]82
- 192[.]64[.]119[.]216
- 162[.]255[.]119[.]47
- 3[.]168[.]147[.]87
- 3[.]168[.]147[.]82
- 3[.]168[.]147[.]124
- 3[.]168[.]147[.]44
- 34[.]216[.]117[.]25
- 54[.]149[.]79[.]189
- 185[.]230[.]63[.]186
- 185[.]230[.]63[.]171
- 185[.]230[.]63[.]107
- 89[.]116[.]31[.]183
- 192[.]64[.]119[.]239
- 162[.]255[.]119[.]56
- 74[.]208[.]236[.]204
- 2607:f1c0:100f:f000::200
- 217[.]70[.]184[.]38
- 192[.]64[.]119[.]226
- 192[.]64[.]119[.]183
- 192[.]64[.]119[.]60
- 198[.]185[.]159[.]145
- 198[.]49[.]23[.]144
- 192[.]64[.]119[.]28
- 198[.]49[.]23[.]145
- 198[.]185[.]159[.]144
- 162[.]255[.]119[.]223
- 162[.]255[.]119[.]21
- 192[.]64[.]119[.]7
- 162[.]255[.]119[.]78
- 192[.]64[.]119[.]93
- 162[.]255[.]119[.]96
- 162[.]255[.]119[.]214
- 162[.]255[.]119[.]22
- 192[.]64[.]119[.]75
- 192[.]64[.]119[.]224
- 192[.]0[.]78[.]25
- 192[.]0[.]78[.]24
- 192[.]252[.]151[.]17
- 45[.]79[.]19[.]196
- 173[.]255[.]194[.]134
- 72[.]14[.]178[.]174

- 96[.]126[.]123[.]244
- 45[.]33[.]23[.]183
- 45[.]33[.]20[.]235
- 45[.]33[.]2[.]79
- 45[.]56[.]79[.]23
- 45[.]33[.]30[.]197
- 72[.]14[.]185[.]43
- 45[.]33[.]18[.]44
- 198[.]58[.]118[.]167
- 192[.]64[.]119[.]72
- 104[.]21[.]2[.]246
- 172[.]67[.]129[.]229
- 2606:4700:3035::6815:2f6
- 2606:4700:3034::ac43:81e5
- 162[.]255[.]119[.]220
- 172[.]67[.]160[.]127