

Uncovering Potential Black Friday and Thanksgiving Threats with DNS Data

Table of Contents

1. [Executive Report](#)
2. [Appendix: Sample Artifacts](#)

Executive Report

Thanksgiving is right around the corner. With it, of course, come celebrations with family and friends and the biggest Black Friday sales. All seems well and good but that's not always the case, isn't it? Because cyber threat actors always take advantage of the biggest holidays and sales to lure more victims to their eagerly waiting traps—malicious domains and subdomains.

The WhoisXML API research team is always on the lookout for current and potential threat sources in a bid to make the Internet a safer place for all. That said, we recently took a DNS deep dive in search of domains and subdomains that could serve as attack vectors for Thanksgiving- and Black Friday-themed cyber attacks.

Our in-depth investigation led to the discovery of:

- 318 email-connected domains, one of which turned out to be malicious
- 786 IP addresses, 635 of which turned out to be malicious
- 1,975 IP-connected domains, two of which turned out to be malicious
- 3,521 string-connected subdomains

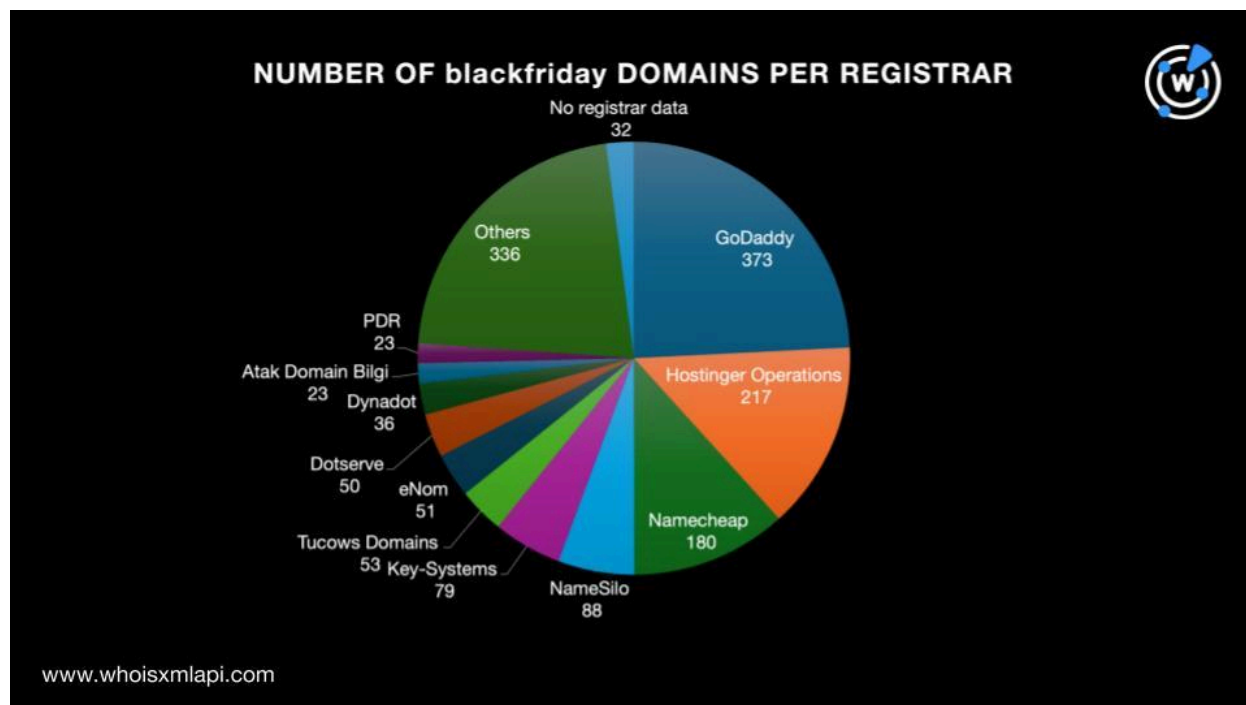
A Look at Suspicious Black Friday and Thanksgiving Domains

For this study, we obtained our datasets for expansion analysis from our [First Watch Malicious Domains Data Feed](#). We specifically searched for domains containing the text strings **blackfriday** and **thanksgiving** and uncovered a sample of 2,091 and 233 domains, respectively, as of 13 November 2024.

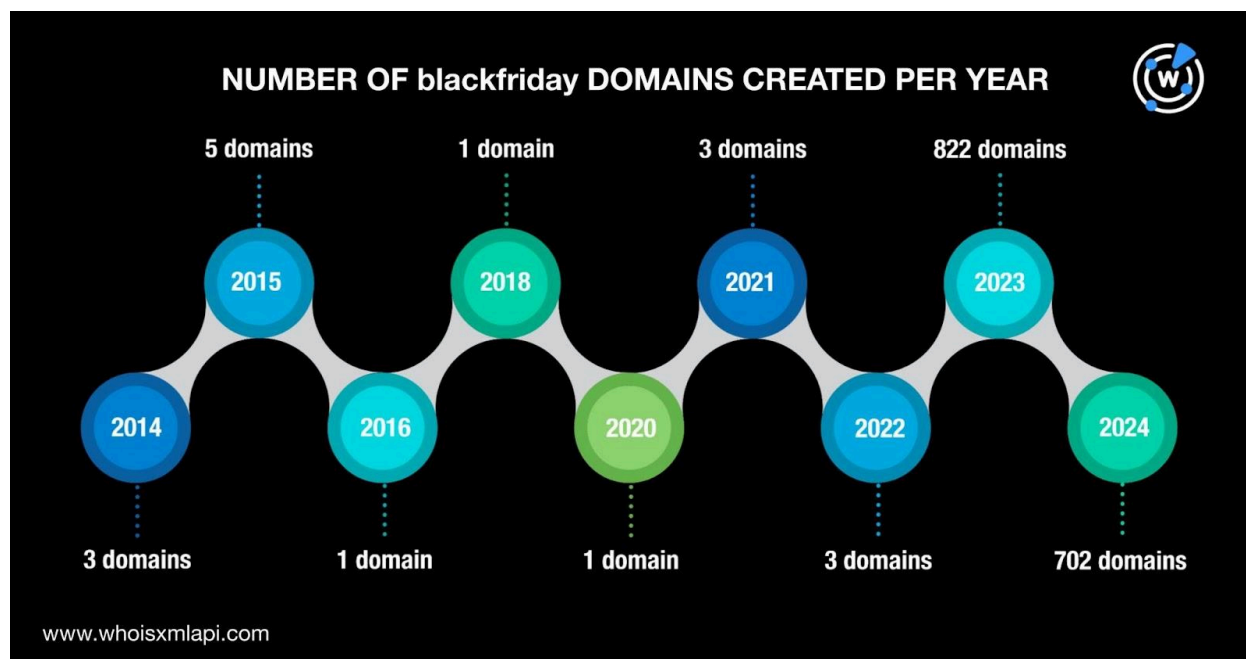
A [bulk WHOIS lookup](#) query for the 2,091 **blackfriday** domains showed that only 1,541 had current WHOIS records. The results for the 1,541 domains showed that:



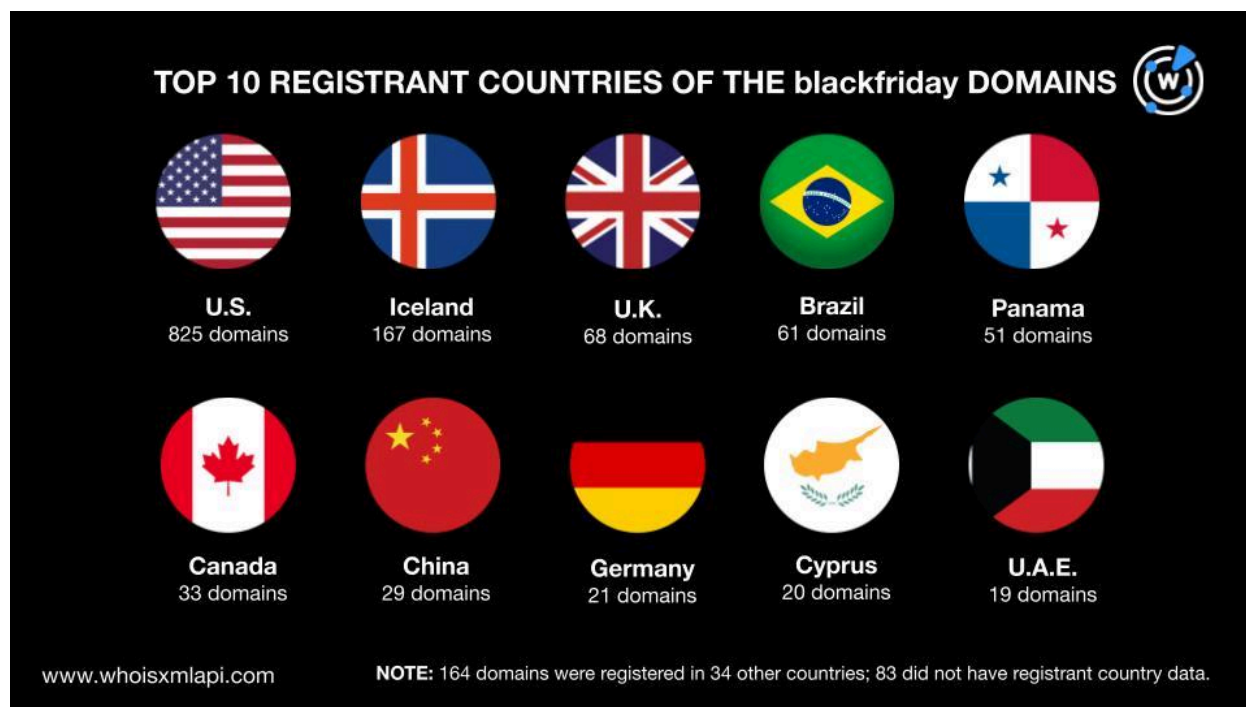
- They were administered by 104 different registrars led by GoDaddy, which accounted for 373 domains. The registrars that completed the top 10 were Hostinger Operations with 217 domains, Namecheap with 180, NameSilo with 88, Key-Systems with 79, Tucows Domains with 53, eNom with 51, Dotserve with 50, Dynadot with 36, and Atak Domain Bilgi with and PDR with 23 each. The remaining 94 registrars accounted for 12% of the total domain volume. Finally, 7% of the domains did not have registrar data in their current WHOIS records.



- They were created between 2014 and 2024. A majority, 99% to be exact, were fairly new, created from 2023 onward. Five domains were created in 2015; three each in 2014, 2021, and 2022; and one each in 2016, 2018, and 2020.

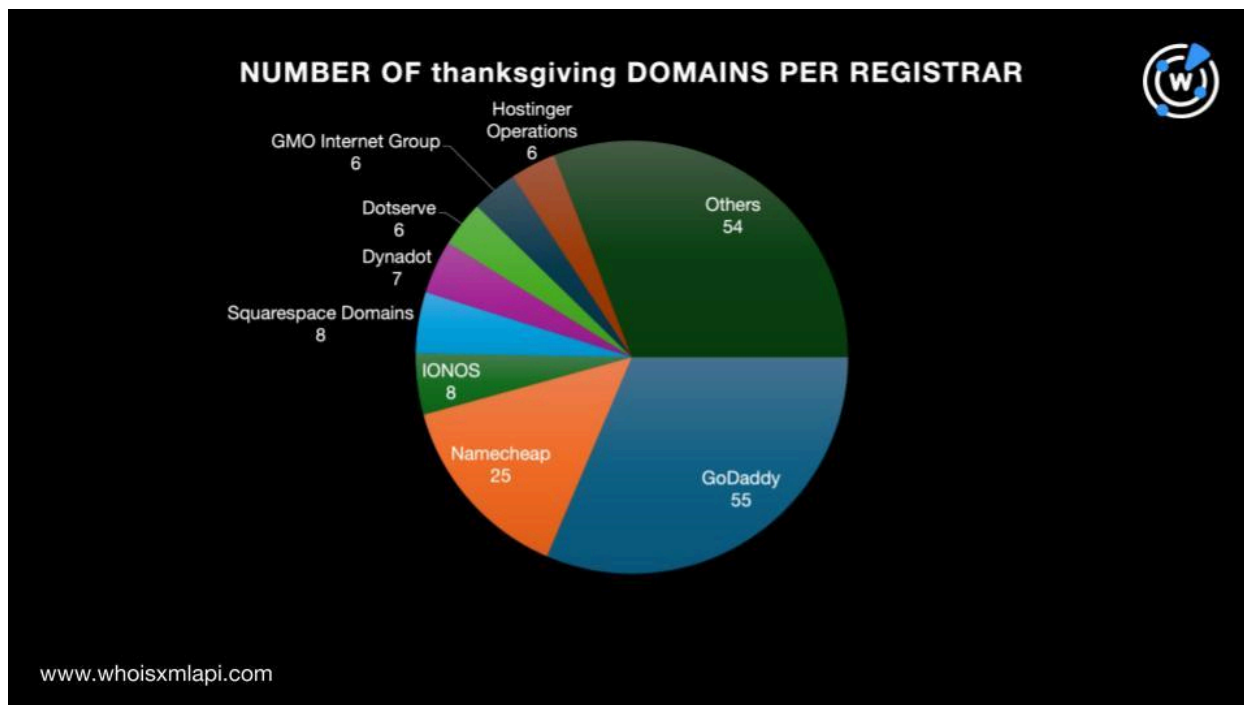


- They were registered in 44 different countries led by the U.S., which accounted for 825 domains. The rest of the top 10 registrant countries were Iceland with 167 domains, the U.K. with 68, Brazil with 61, Panama with 51, Canada with 33, China with 29, Germany with 21, Cyprus with 20, and the U.A.E. with 19. The remaining 34 countries accounted for 11% of the total domain volume. Finally, about 5% of the domains did not have registrant country data in their current WHOIS records.

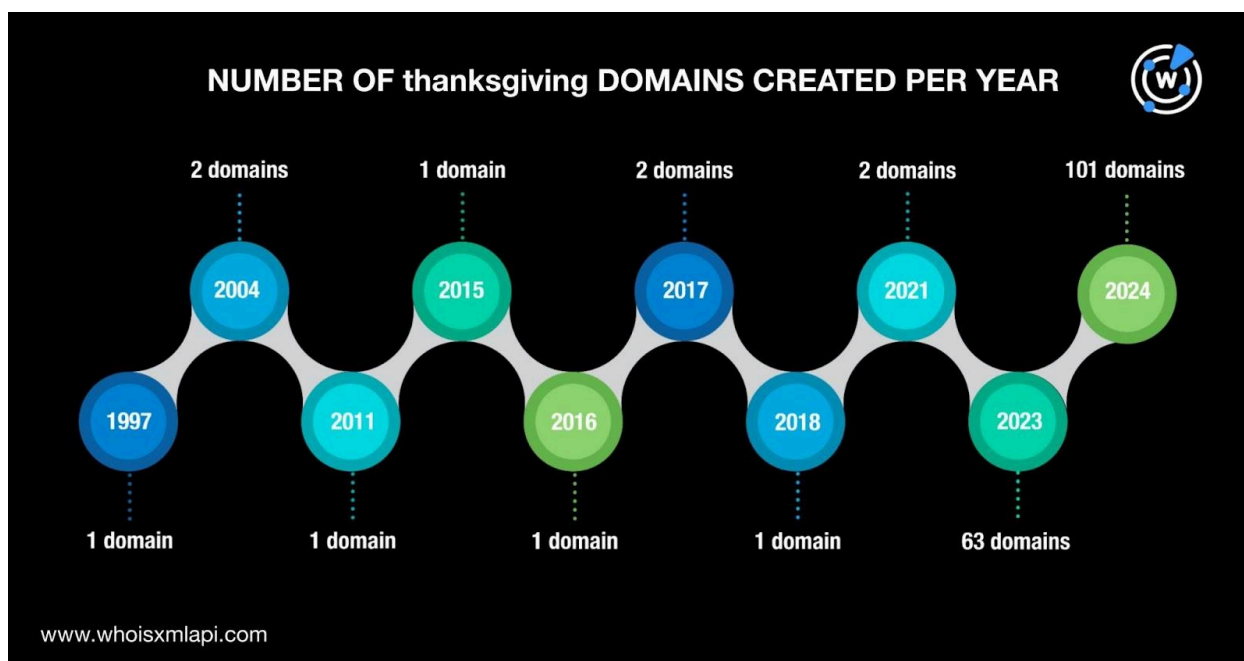


Meanwhile, a bulk WHOIS lookup query for the 233 **thanksgiving** domains revealed that only 175 had current WHOIS records. The results for the 175 domains showed that:

- They were administered by 44 different registrars led by GoDaddy, which accounted for 55 domains. The nine other registrars on the top 5 were Namecheap with 25 domains; IONOS and Squarespace Domains with eight each; Dynadot with seven; and Dotserve, GMO Internet Group, and Hostinger Operations with six each. The remaining 39 registrars accounted for 31% of the total domain volume.

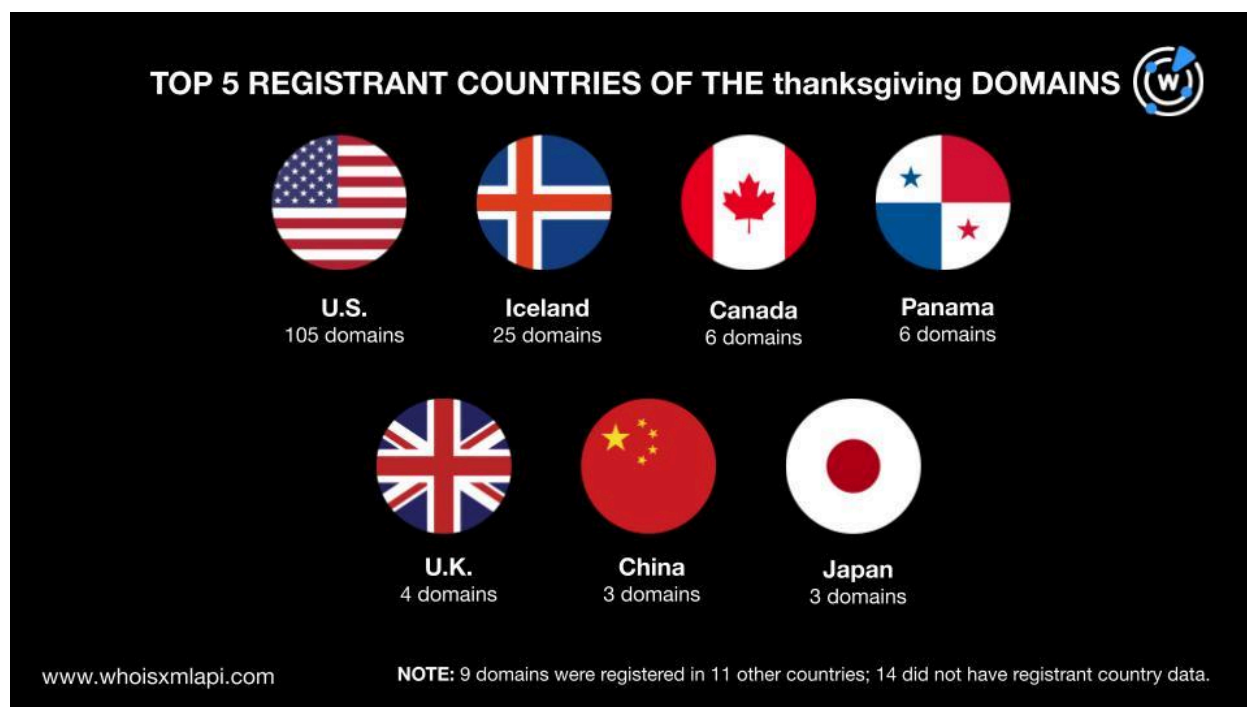


- They were created between 1997 and 2024. As with the **blackfriday** domains, most of the **thanksgiving** domains, 94% to be exact, were also relatively new, created from 2023 onward. Two domains each were created in 2004, 2017, and 2021, while one each were created in 1997, 2011, 2015, 2016, and 2018.





- They were registered in 16 different countries led by the U.S., which accounted for 105 domains. The other countries that made it to the top 5 were Iceland with 25 domains, Canada and Panama with six each, the U.K. with four, and China and Japan with three each. The 11 remaining countries accounted for 5% of the total domain volume. Finally, 8% of the countries did not have registrant country data in their current WHOIS records.



Next, we combined all the **blackfriday** and **thanksgiving** domains, with or without current WHOIS records, ending up with a total of 2,324 domains. We queried them on [Threat Intelligence API](#) and found that four of them were associated with various threats. An example is `blackfriday-best-deals[.]com`, which has already been tagged as an indicator of compromise (IoC) for generic threats and phishing.

Expansion Analysis Findings

The bulk WHOIS lookups we performed earlier for the **blackfriday** and **thanksgiving** domains uncovered 219 email addresses from their current WHOIS records after duplicates were filtered out. Upon closer scrutiny, we determined that 32 of these email addresses were public.

Querying the 32 public email addresses on [Reverse WHOIS API](#) resulted in the discovery of 318 email-connected domains after duplicates and the original domains were removed. Threat Intelligence API showed that one of them—`feiraochevro[.]com`—was associated with a cyber attack.



[DNS lookups](#) for the 2,324 original domains with current WHOIS records revealed that they resolved to 1,250 unique IP addresses—464 IPv6 addresses and 786 IPv4 addresses. We focused on the 786 IPv4 addresses for the rest of our analysis.

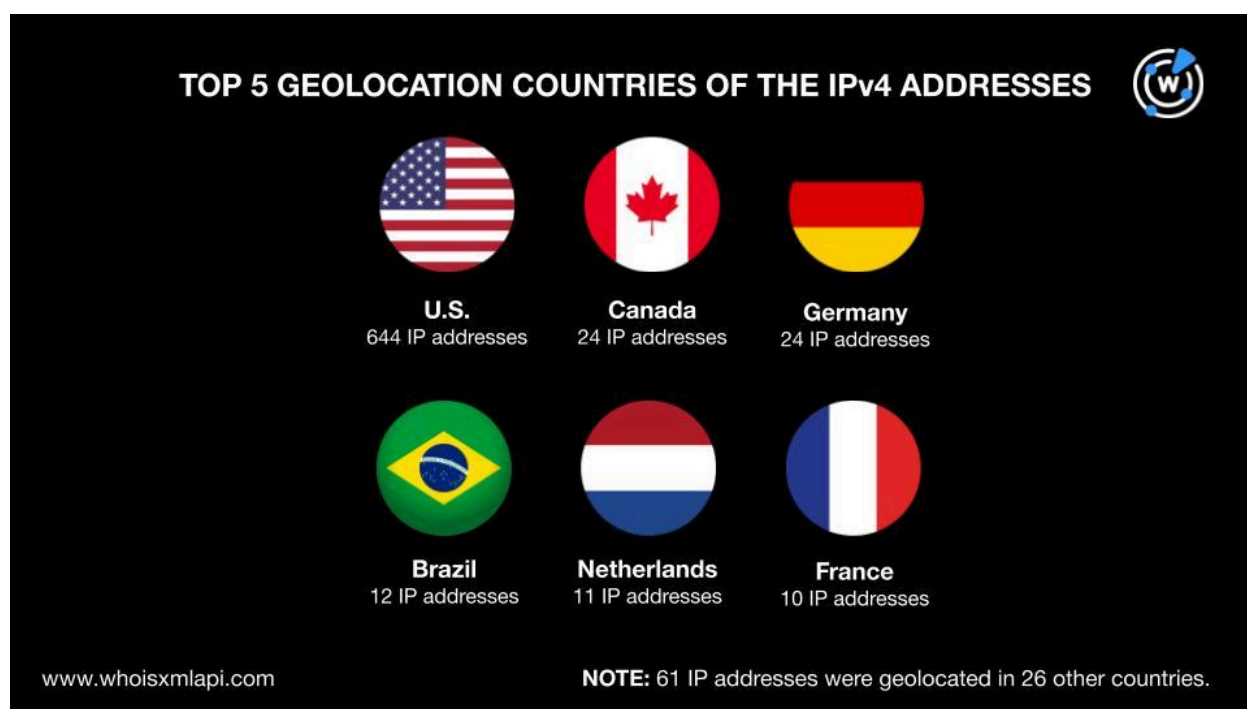
Threat Intelligence API queries for the 786 IP addresses showed that 635 were associated with various threats. Take a look at five examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREATS
103[.]169[.]142[.]0	Attack Command and control (C&C) Generic Malware Phishing Suspicious
216[.]239[.]32[.]21	Attack C&C Generic Malware Phishing Spam Suspicious
3[.]13[.]222[.]255	Generic Malware Phishing
44[.]227[.]65[.]245	Attack C&C Generic Malware Phishing Suspicious
51[.]91[.]236[.]255	Attack C&C Generic Malware Phishing Spam Suspicious

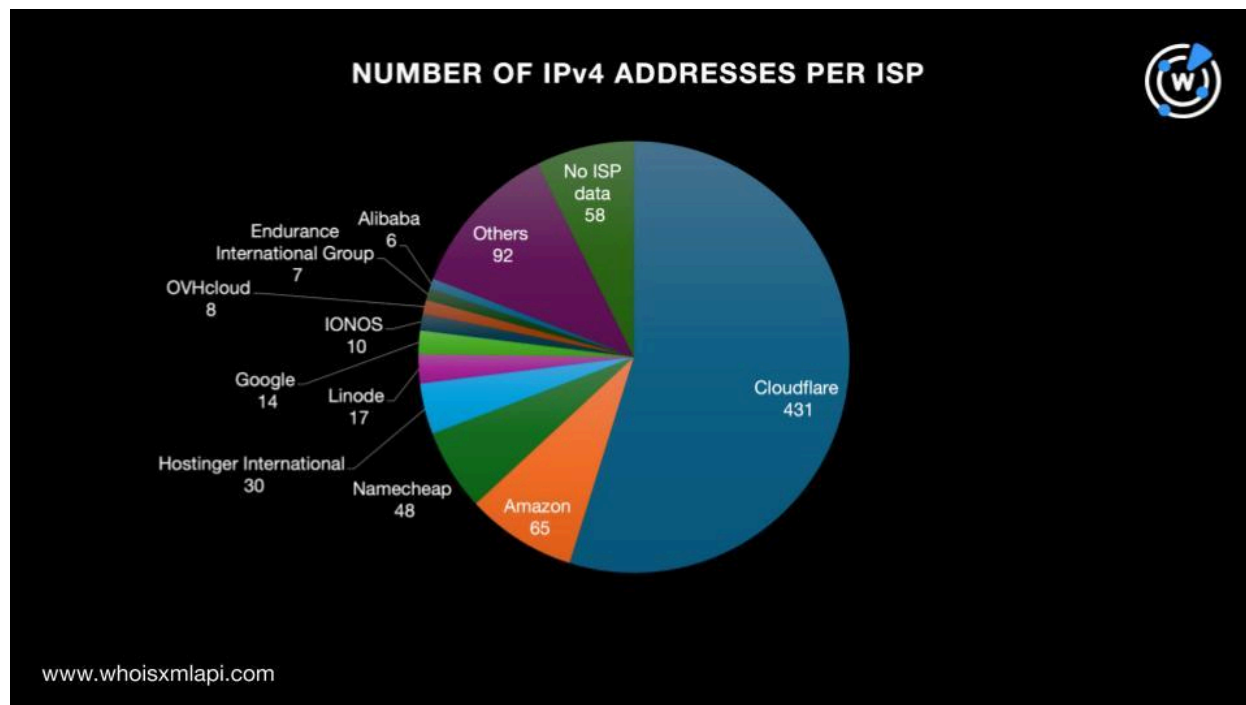


A [bulk IP geolocation lookup](#) for the 786 IP addresses showed that:

- They were geolocated in 32 different countries led by the U.S., which accounted for 644 IP addresses. Canada and Germany with 24 IP addresses each, Brazil with 12, the Netherlands with 11, and France with 10 completed the top 5 geolocation countries list. The remaining 27 countries accounted for 8% of the total IP address volume.



- They were administered by 76 different ISPs led by Cloudflare, which accounted for 431 IP addresses. The rest of the top 10 geolocation countries were Amazon with 65 IP addresses, Namecheap with 48, Hostinger International with 30, Linode with 17, Google with 14, IONOS with 10, OVHcloud with eight, Endurance International Group with seven, and Alibaba with six. The remaining 66 ISPs accounted for 12% of the total IP address volume. Finally, 7% of the IP addresses did not have ISP data.






After that, we queried the 786 IP addresses on [Reverse IP API](#) and found that 69 of them could be dedicated hosts. Altogether, these 69 shortlisted IP addresses hosted 2,975 domains after duplicates and the original and email-connected domains were filtered out.

Our Threat Intelligence API queries for the 2,975 IP-connected domains showed that two of them were associated with various threats. The domain `limitdiscountz[.]com`, for instance, was tagged as an IoC for phishing and generic threats.

Next, we trooped to [Domains & Subdomains Discovery](#) to look for subdomains that contained **blackfriday** and **thanksgiving** and ended with **.blackfriday** created on 1 January 2024 onward. We uncovered 3,521 subdomains in total.

Throughout our analysis, we discovered that seven of the domains (i.e., four from the original list of **blackfriday** and **thanksgiving** domains, one email-connected domain, and two IP-connected domains) were malicious. [Screenshot API](#) queries for them showed that several remained accessible to date. Take a look at sample screenshots below.



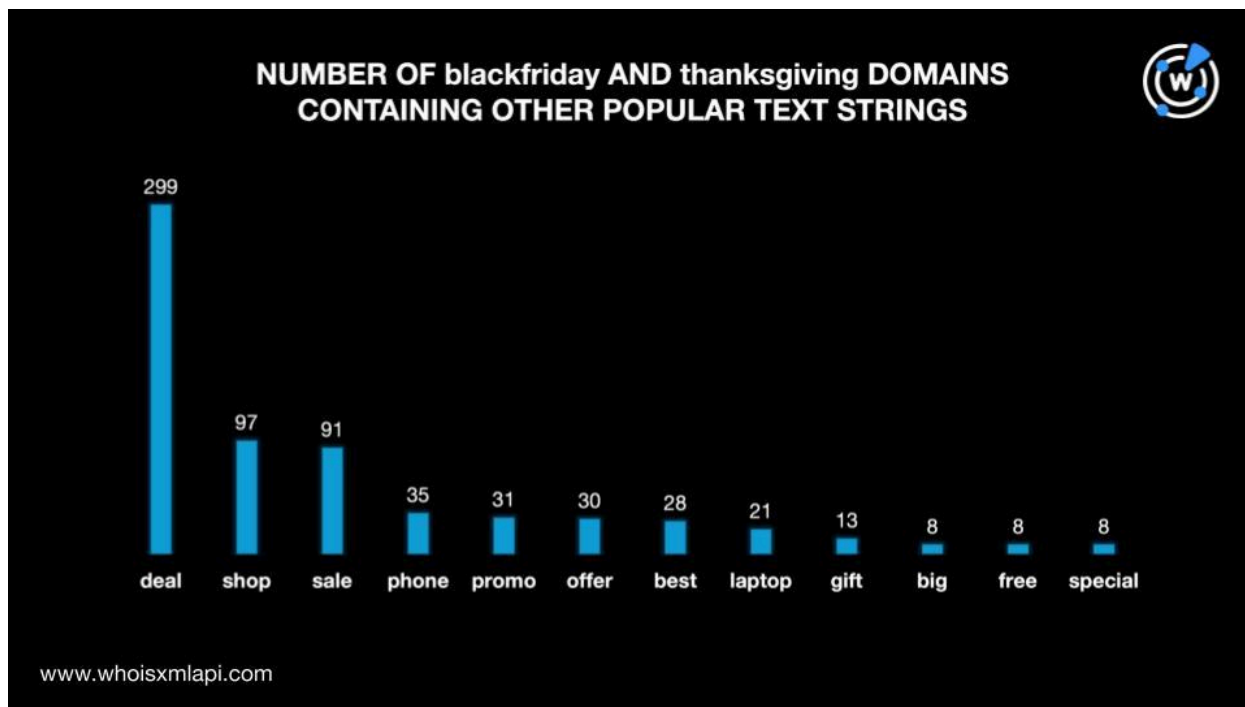
 <p>Malicious domain from the dataset blackfriday-best-deals[.]com</p>	 <p>Malicious IP-connected domain hocakoisanvuon[.]com</p>
<p>Error 1001 <small>Ray ID: 8e44dd5e8b5349</small> 2024-11-18 02:34:59 UTC DNS resolution error</p> <p>What happened? You've requested a page on a website (limitdiscountz.com) that is on the Cloudflare network. Cloudflare is currently unable to resolve your requested domain. (limitdiscountz.com). There are two potential causes of this:</p> <ul style="list-style-type: none"> • Most likely: If the owner just signed up for Cloudflare it can take a few minutes for the website's information to be distributed to our global network. • Less likely: something is wrong with this site's configuration. Usually this happens when accounts have been signed up with a <p>Malicious IP-connected domain limitdiscountz[.]com</p>	 <p>Malicious domain from the dataset staplesblackfriday[.]com</p>

We further scrutinized the 2,324 domains we obtained from First Watch Malicious Domains Data Feed to spot text strings in combination with **blackfriday** and **thanksgiving** that could figure in malicious campaigns. We identified 30 strings commonly found among them, namely:

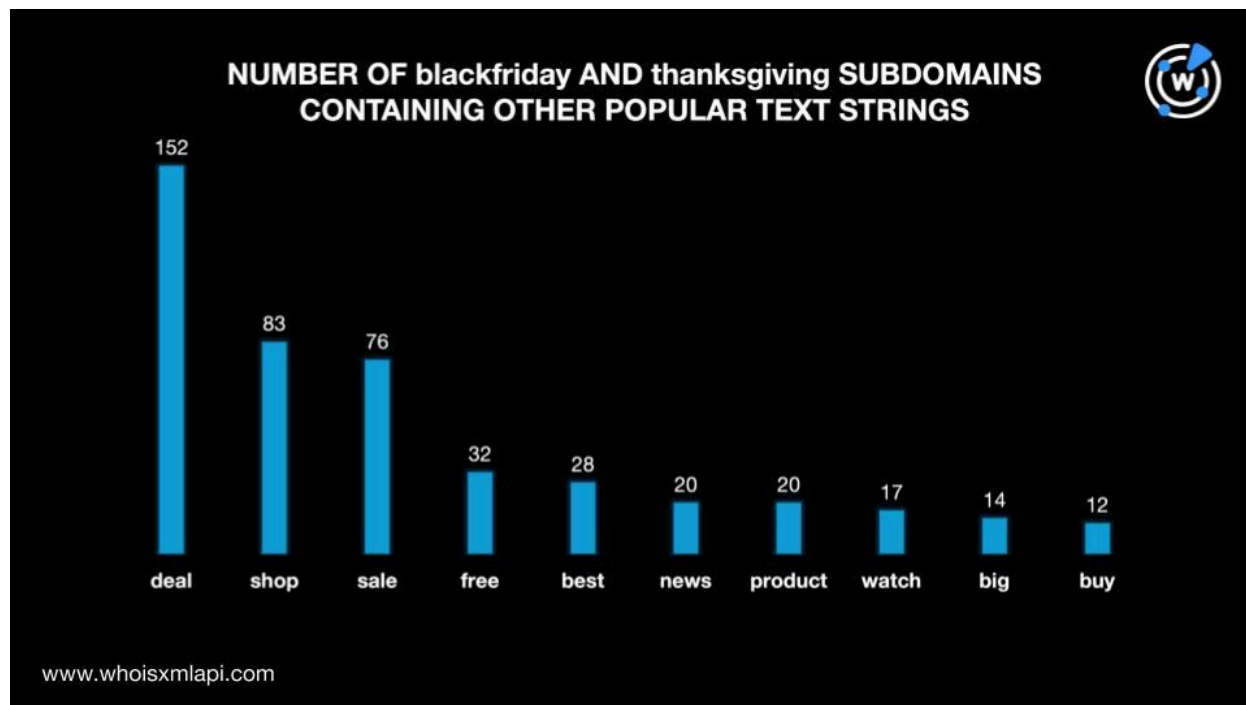
- appliance
- bag
- best
- big
- buy
- clearance
- clothing
- coupon
- deal
- discount
- electronics
- free
- furniture
- gift
- giveaway
- laptop
- market
- news
- offer
- outlet
- party
- phone
- product
- promo
- recipe
- sale
- savings
- shop
- special
- watch



Note that any of the text strings could appear simultaneously in the domains. An example would be **best** and **deal** in the domain best-black-friday-deals[.]xyz. The following chart shows how many times each string appeared in the domains.



We then looked more closely at the 3,521 subdomains to see if the text strings commonly found among the domains also appeared in them. The subdomain results differed somewhat from those for the domains.



While **deal**, **shop**, and **sale** kept their places. The top domain text strings **phone**, **promo**, **offer**, **laptop**, **gift**, and **special** were ousted by **news**, **product**, **watch**, and **buy** for the subdomains.

—

Our DNS deep dive into 2,324 Black Friday- and Thanksgiving-themed domains led to the discovery of 6,600 artifacts comprising 318 email-connected domains, 786 IP addresses, 1,975 IP-connected domains, and 3,521 string-connected subdomains. A total of 638 of these artifacts have already been weaponized for various malicious campaigns.

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 Domains from the First Watch Malicious Domains Data Feed

- 0xblackfriday[.]com
- 0xblackfriday[.]xyz
- 101domain[.]blackfriday
- 101domains[.]blackfriday
- 1stblackfriday[.]com
- 1xbetblackfriday[.]top
- 2021blackfriday[.]us
- 2023blackfridaysale[.]com
- 2024blackfriday[.]sale
- 2024blackfridaydeals[.]com
- 2025blackfriday[.]sale
- 2035blackfriday[.]com
- 247blackfriday[.]com
- 25blackfriday[.]com
- 26blackfriday[.]com
- 27blackfriday[.]com
- 29blackfriday[.]com
- 365blackfridays[.]com
- 54d-blackfriday[.]com
- 54dblackfriday[.]com
- 5starblackfriday[.]com
- 6figureblackfriday[.]com
- 7nowblackfriday[.]com
- 8filles[.]blackfriday
- 99blackfriday-us[.]shop
- a-blackfriday[.]top
- adr18kjoiasblackfriday[.]site
- ads-blackfriday[.]com
- adsblackfriday[.]com
- afterblackfriday[.]com
- ahrefsblackfri[.]day
- ai-blackfriday-bot[.]website
- aiblackfriday[.]xyz
- airwrapblackfriday[.]today
- alisonrosenneedsablackfriend[.]org
- all-black-friday[.]xyz
- allblackfridaynews[.]click
- allstarblackfriday[.]com
- alphaleteblackfriday[.]com
- alphaleteblackfridaysale[.]com
- amazingblackfriday[.]com
- amazingblackfridaydealsstereo[.]today
- amazonblackfriday[.]online
- amazonblackfridaydealz[.]com
- americanasblackfriday[.]com
- anapromoblackfriday[.]online
- andy-blackfriday[.]de
- annualblackfridaytrouttournament[.]com
- anotherblackfriday[.]com
- antecipablackfriday[.]site
- 12daysofthanksgiving[.]com
- 34856thanksgivingtrl[.]com
- aihappythanksgiving[.]com
- alcarbonvathanksgiving[.]com
- americastanksgivingtopdog[.]com
- andthanksgivingforall[.]com
- athanksgivingwebsiteforianandkylesthanksgivingparty[.]com
- bestviewthanksgivingparade[.]com
- better-than-thanksgiving[.]com
- blessedhandsgivingbackinc[.]com
- bozemancranksgiving[.]com
- buyamericanforthanksgiving[.]org
- cardthanksgiving[.]com
- charolivethanksgiving90[.]fun
- childrensthanksgivingstickhorserodeo[.]com
- chonglegalgrouthanksgiving[.]click
- communitythanksgiving[.]org
- communitythanksgivingdinner[.]org



- daddybrucethanksgiving[.]org
- dailypraiseandthanksgiving[.]com
- dayafterthanksgiving[.]store
- daysuntilthanksgiving[.]com
- denverthanksgiving2024[.]com
- devoutthanksgiving[.]com
- dfxsecurecloud[.]net
- edmondthanksgiving[.]com
- edmondthanksgivingdinner[.]com
- edmondthanksgivingdinnerorg[.]com
- edmontjanksgiving[.]org
- everythingthanksgiving[.]com
- everythingthanksgiving[.]net
- exclusivethanksgiving[.]cyou
- faithandgiving[.]info
- familythanksgiving2024[.]com
- fidothanksgiving[.]com
- freedom-thanksgiving50[.]com
- freethanksgivinggift[.]com
- freethanksgivingpie[.]com
- freethanksgivingprintables[.]com
- giftforthanksgiving[.]online
- giftforthanksgiving[.]store
- globalthanksgiving[.]net
- globalthanksgivingfoundation[.]com
- gourmiathanksgiving[.]com
- gpctthanksgiving[.]com
- greysveganthanksgiving[.]com
- hamtramckthanksgiving[.]org
- hanukkahthanksgiving2013[.]org
- happy-danksgiving[.]xyz
- happythanksgiving[.]xyz

Sample Email-Connected Domains

- 1rbcmange-royalbanksecure[.]com
- 1rbcroyal-bank-secure[.]com
- 1royalbankverif-loginteam[.]com
- 90secondtour[.]com
- 90secondtours[.]com
- adestramentothorecharlotte[.]com
- aeon-24htv[.]jpp
- aeon-chushikoku[.]com
- aeon-hoken-slot[.]com
- aeon-kyushu-recruit[.]com
- aeon-minami-ns[.]com
- aeon-minami-shop[.]com
- aeon-myhomecenter[.]com
- aeon-photo[.]com
- aeon-reform-naisou-simulator[.]com
- aeon-reform[.]com
- aeon-yanaizu[.]com
- aeon1p-sakubun[.]jpp
- aeondelight-lp[.]net
- aeonentertainment[.]jpp
- aeonkitaurawa[.]com
- aeonnextdelivery[.]net
- ame-promo-semanal[.]com
- amourdeschats[.]com
- ardarocresale[.]com
- ardarocresales[.]com
- ardaroctimeshareresale[.]com
- ardaroctimeshareresales[.]com
- ardatimeshareresale[.]com
- ardatimeshareresales[.]com
- ausin[.]properties
- ausincoin[.]com
- ausincrypto[.]com
- balsamhillioutlet[.]com
- beautysupplystore[.]us
- bestairfryer[.]us
- bestlaptops[.]us
- bestpapershredder2024[.]com
- bigdealslots[.]com
- biglotsdiscount[.]com
- biglotsdiscountsale[.]com
- biglotsdiscountstore[.]com



- biglotsof[.]com
- biglotssaves[.]com
- blackfridaydeals[.]us
- blockchainlockdown[.]com
- canadapost-verifynotification[.]com
- canadapostverify-securenotif[.]com
- cauldronstudio[.]net
- cauldroncheats[.]com

Sample IP Addresses

- 103[.]154[.]102[.]26
- 103[.]169[.]142[.]0
- 103[.]205[.]0[.]152
- 103[.]224[.]182[.]240
- 103[.]224[.]182[.]241
- 103[.]224[.]182[.]242
- 103[.]224[.]182[.]253
- 103[.]224[.]212[.]212
- 103[.]224[.]212[.]213
- 103[.]224[.]212[.]214
- 103[.]224[.]212[.]215
- 103[.]224[.]212[.]216
- 103[.]224[.]212[.]217
- 103[.]42[.]108[.]46
- 104[.]131[.]71[.]238
- 104[.]16[.]12[.]194
- 104[.]16[.]13[.]194
- 104[.]16[.]14[.]194
- 104[.]16[.]15[.]194
- 104[.]16[.]16[.]194
- 104[.]16[.]198[.]133
- 104[.]166[.]69[.]151
- 104[.]17[.]157[.]1
- 104[.]17[.]158[.]1
- 104[.]17[.]232[.]29
- 104[.]18[.]187[.]223
- 104[.]18[.]188[.]223
- 104[.]18[.]20[.]248
- 104[.]18[.]24[.]121
- 104[.]18[.]30[.]185
- 104[.]18[.]31[.]185
- 104[.]18[.]73[.]116
- 104[.]19[.]221[.]20
- 104[.]19[.]222[.]20
- 104[.]21[.]0[.]117
- 104[.]21[.]0[.]165
- 104[.]21[.]1[.]225
- 104[.]21[.]11[.]202
- 104[.]21[.]11[.]247
- 104[.]21[.]11[.]249
- 104[.]21[.]13[.]153
- 104[.]21[.]13[.]178
- 104[.]21[.]13[.]57
- 104[.]21[.]14[.]135
- 104[.]21[.]14[.]211
- 104[.]21[.]14[.]3
- 104[.]21[.]14[.]52
- 104[.]21[.]14[.]74
- 104[.]21[.]14[.]96
- 104[.]21[.]15[.]203

Sample IP-Connected Domains

- 10kweeklywin[.]com[.]au
- 119[.]118[.]214[.]35[.]bc[.]googleusercontent[.]com
- 123appsstudio[.]com
- 1399park[.]com
- 19216811[.]jing
- 1921681254[.]kim
- 1yearold[.]co[.]uk
- 22me[.]vn
- 24hkoreanmart[.]com
- 24horasparavender[.]site
- 26558hb[.]com



- 2edigital[.]co
- 30daysgiveaways[.]com[.]au
- 38453d46-c067-4af9-893b-a069442cd5c3[.]clouding[.]host
- 3dbarat[.]fr
- 3star[.]online
- 4seasonrealestate[.]com
- 505handyman[.]com
- 7brewsecretmenu[.]com
- 7brewsecretmenu[.]org
- 8002yl[.]com
- 920sb[.]com
- a2nadogados[.]com
- a3vbs[.]com
- aaaiosr23[.]shop
- abbasteries[.]com
- abdo[.]net
- abogadosrye[.]com
- abuahmed[.]me
- ac-arqs[.]com
- accioncannaben[.]com
- acciontosfaes[.]com
- accionvitanatur[.]com
- acheterleproduit[.]site
- acofarmaimpulsatufarmacia[.]com
- acousticuprisingfilm[.]com
- action-scoots[.]com
- activeoffer[.]site
- activeoffer[.]store
- acupunturaflorianopolis[.]com[.]br
- acurac[.]net
- adagro[.]com[.]br
- adegawinepremium[.]com
- adgainpartners[.]com
- adpersonam[.]com[.]au
- advisor-sherif-center[.]com
- aegonteregala[.]com
- afeim1[.]com
- affordable-reservations[.]com
- afiliaadosdasorte[.]online

Sample String-Connected Subdomains

- 14-pro-thanksgiving-deals[.]jrk-fasanenhof[.]de
- 14-pro-thanksgiving-deals[.]relaton[.]eu
- 14-pro-thanksgiving[.]antytrendy[.]pl
- 14-pro-thanksgiving[.]relaton[.]eu
- 2012blackfridayads[.]wall[.]fm
- 2012blackfridayblog[.]blog[.]com
- 2012blackfridaygoprohddhero2deals[.]blogspot[.]com
- 2014blackfridayamazon[.]blogspot[.]com[.]es
- 24-hour-fitness-thanksgiving-hours[.]panini-dino[.]de
- a-initially-thanksgiving-too[.]trycloudflare[.]com
- abekablackfridaysale[.]sv-fischingen[.]de
- academyblackfriday[.]relaton[.]eu
- academyblackfridayad[.]applerefurbi shed[.]eu
- academyblackfridayad[.]l-zebra[.]pl
- affiliate-disputes-thanksgiving-sword[.]trycloudflare[.]com
- aloblackfriday[.]billard-index[.]de
- aloblackfriday[.]postweg[.]eu
- alphaleteblackfriday[.]bvwwagenfeld[.]de
- alphaleteblackfriday[.]kbo-su[.]de
- alphaleteblackfriday[.]qualcosadibueno[.]eu
- alwaysthanksgiving-com[.]mail[.]protection[.]outlook[.]com



- amazonblackfriday[.]online[.]buysell offerup[.]com
- amazonblackfriday[.]unaux[.]com
- amm-blackfridaygeneral[.]netspacel ease[.]com
- andhomeblackfriday[.]young-acade my[.]de
- animated-happy-thanksgiving-gifs[.] wiegeschnittenbrot[.]de
- anonymous-thanksgiving[.]glitch[.]m e
- app[.]cash-wise-thanksgiving-hours[.]wiegeschnittenbrot[.]de
- app[.]is-rite-aid-open-on-thanksgivi ng-2022[.]wiegeschnittenbrot[.]de
- applock-theme-thanksgiving[.]ar[.]u ptodown[.]com
- applock-theme-thanksgiving[.]en[.]u ptodown[.]com
- applock-theme-thanksgiving[.]haber erciyes[.]com
- applock-theme-thanksgiving[.]uptod own[.]com
- archive-lloyd-hats-thanksgiving[.]try cloudflare[.]com
- ark-thanksgiving-event-2022[.]badm intongwb[.]de
- ark-thanksgiving-event-2022[.]post weg[.]eu
- ark-thanksgiving-event[.]liquishot[.]e u
- arkthanksgivingevent2022[.]yunpan[.]de
- ashleyfurnitureblackfriday2018[.]app spot[.]com
- associations-thanksgiving-providing -remedy[.]trycloudflare[.]com
- asu-thanksgiving-break-2023[.]youn g-academy[.]de
- asu-thanksgiving-break[.]antytrendy[.]pl
- asuthanksgivingbreak[.]antytrendy[.] pl
- auth[.]app[.]cash-wise-thanksgiving- hours[.]wiegeschnittenbrot[.]de
- authentication-thanksgiving-academ y-adobe[.]trycloudflare[.]com
- auto-parts-thanksgiving[.]cookie-ninj a[.]de
- auto-parts-thanksgiving[.]relaton[.]e u
- autoconfig[.]blackfriday[.]mavinapps[.]tech
- autodiscover[.]blackfriday[.]hotelmor ada[.]com[.]br
- autodiscover[.]thanksgiving[.]season alholidaycrafts[.]com