Father's Day: Bad Guys' Activities

Table of Contents

Executive Report

Threat actors don't rest. Their malicious campaigns operate 24/7, especially when special occasions are approaching. Last May, we discovered over a thousand web properties related to Mother's Day, many of which either hosted questionable content or have been flagged as malicious.

In this report, we looked at domain registrations that could be related to Father's Day and analyzed them using DNS intelligence. Among our findings are:

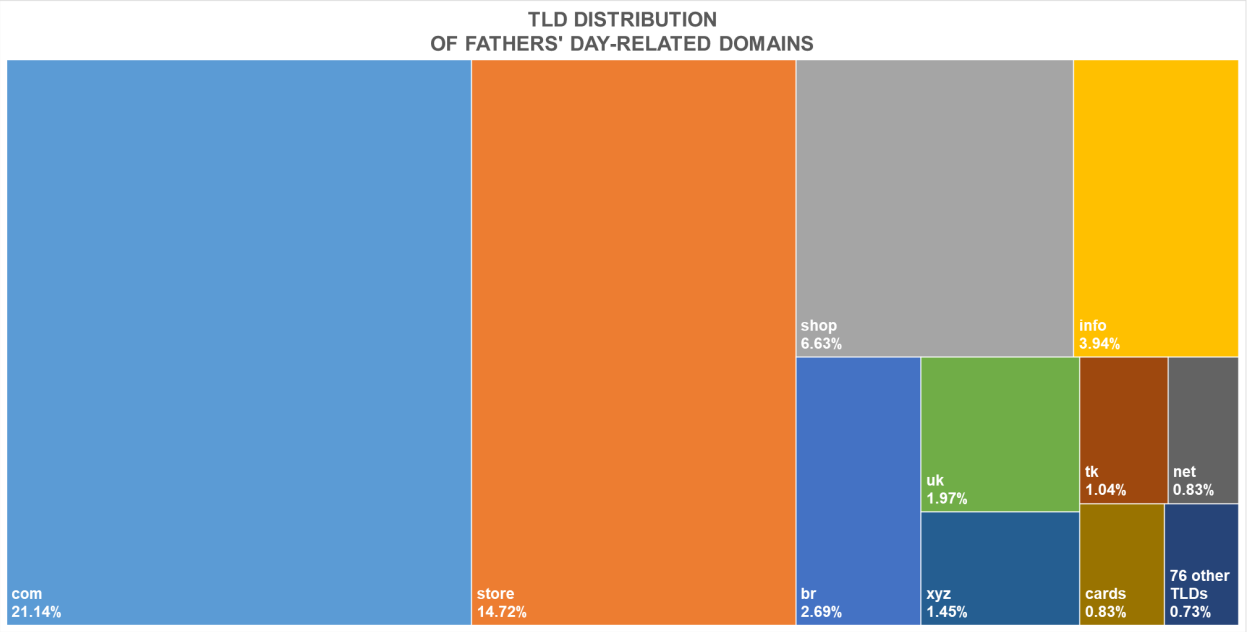
- 1,700+ domains and subdomains containing potential Father's Day-related text strings, such as "father" and "dad," alongside "gift," "game," "shop," "store," "card," and "gift"
- About 85% of the cyber resources actively resolved to 1,600+ IP addresses
- Questionable content was hosted on several properties, including login and look-alike pages, giveaways, and news sites
- Over a dozen properties have been reported as malicious by various malware engines

Analysis of Father's Day-Related Cyber Resources

TLD Distribution

About 21% of the domains we uncovered fell under the .com generic top-level domain (gTLD), followed by two e-commerce-related new gTLDs (ngTLDs), .store and .shop, with 15% and 7% shares, respectively. Other mostly used gTLDs include .info, .xyz, .net, and .cards.

There were also country-code TLDs (ccTLDs) in the top 10, including .br, .uk, and .tk. The rest of the domains were distributed across 76 other TLDs. The chart below shows the breakdown.



While large TLDs, such as .com, .info, .uk, and .net are expected to be seen since most of the legitimate websites use them, we can't say the same for other TLDs. We would specifically be wary of free TLDs, such as .tk and those named by Spamhaus as the most abused TLDs.

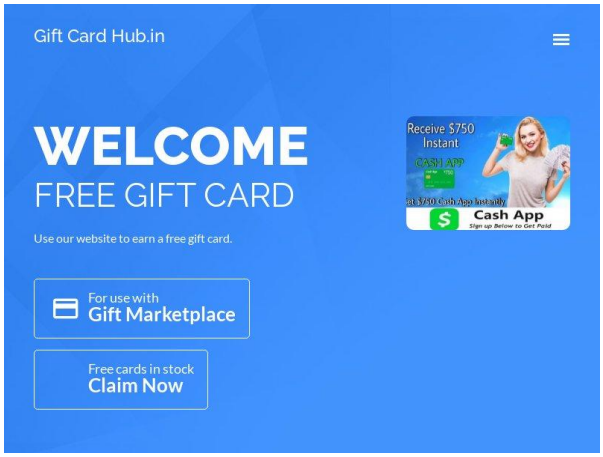
Screenshot Analysis

While hundreds of the cyber resources in the study were parked, others hosted live content. Some could be legitimate, such as the online shops of small businesses. However, some are suspicious and we will provide examples via website screenshots taken with Screenshot API in the succeeding sections.

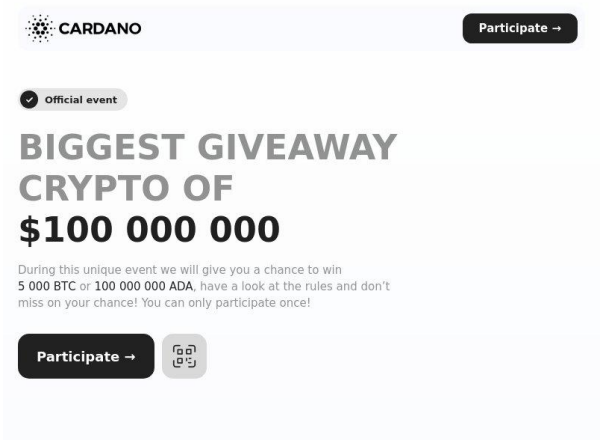
Giveaway Lures

Many Father's Day-related properties hosted content offering huge discounts and giving away gift cards or cryptocurrencies. These web pages could be used in financial scams that lure victims by promising prizes and giveaways. Below are some examples.

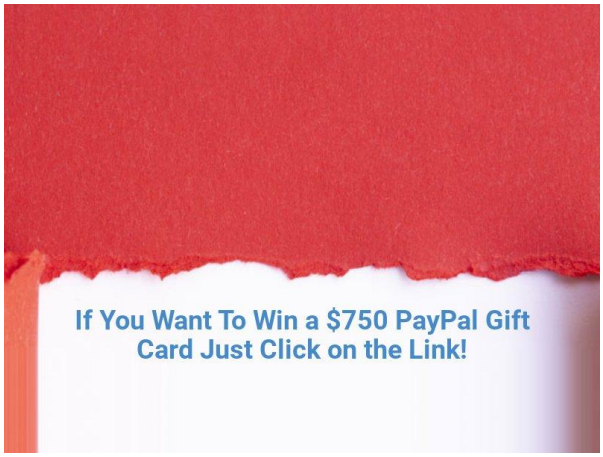
Screenshot of auspostgiftcards[.]com[.]au



Screenshot of buygiftcard[.]top



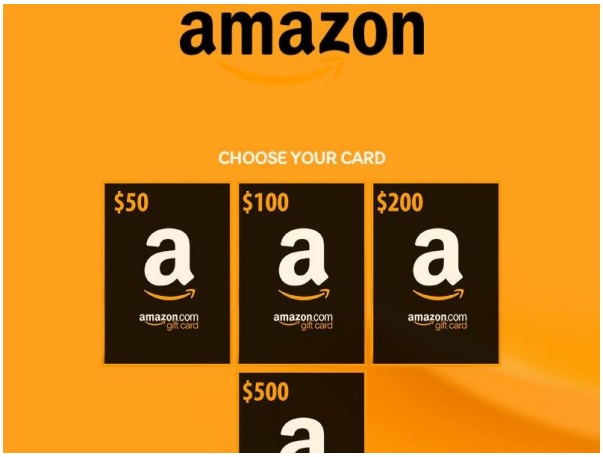
Screenshot of cardanogift[.]net



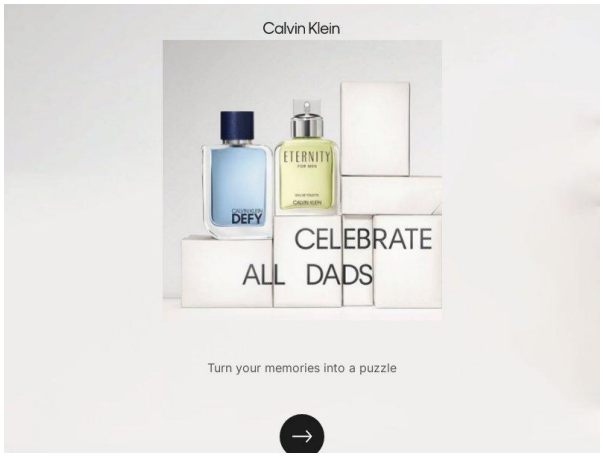
Screenshot of paypalgiftcard[.]099[.]ro

Counterfeiting and Cybersquatting Domains

Similarly, some domains imitated the pages of famous brands like Amazon and Calvin Klein, as shown by the website screenshots below. These and other similar imitation websites may be used in selling counterfeit products or phishing campaigns.



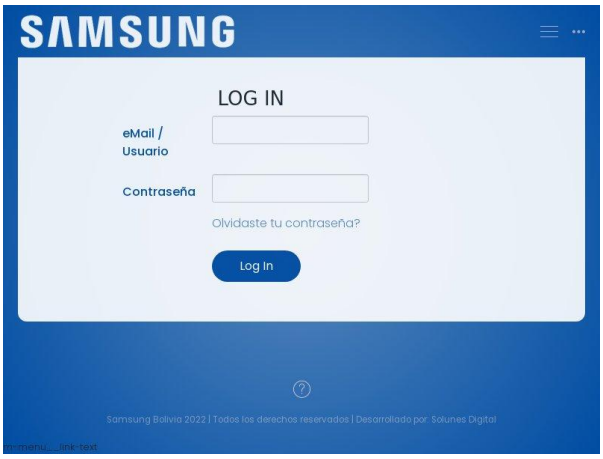
Screenshot of amzangiftcard[.]xyz



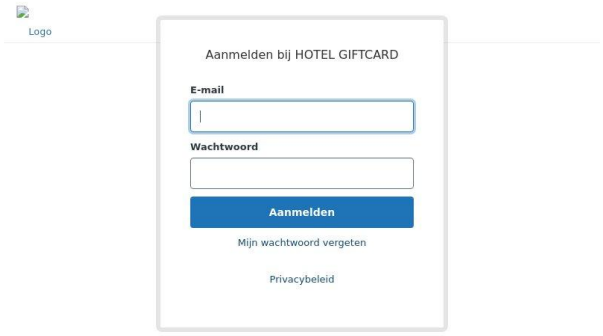
Screenshot of ckfathersday[.]vercel[.]app

Potential Credential Theft Fronts

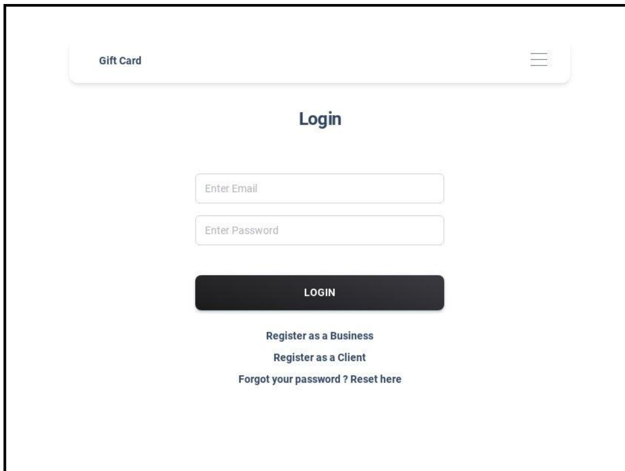
Another suspicious type of content comprises login pages that ask visitors for their usernames and passwords. People looking for Fathers' Day gifts may be redirected to these pages and enticed to enter their sensitive information.



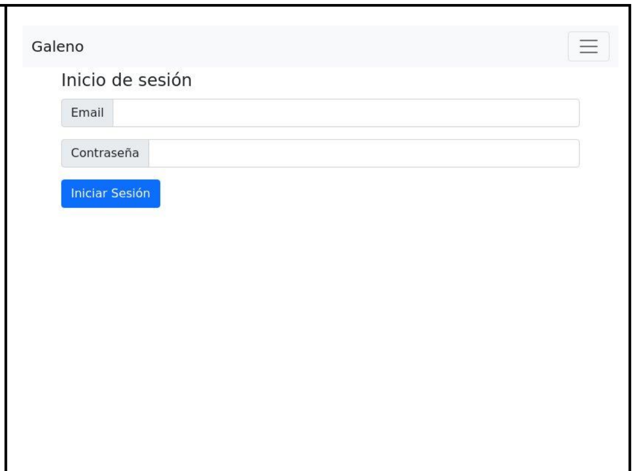
Screenshot of giftcards.samsungplus[.]com[.]bo



Screenshot of hotelgiftcard[.]zendesk[.]com



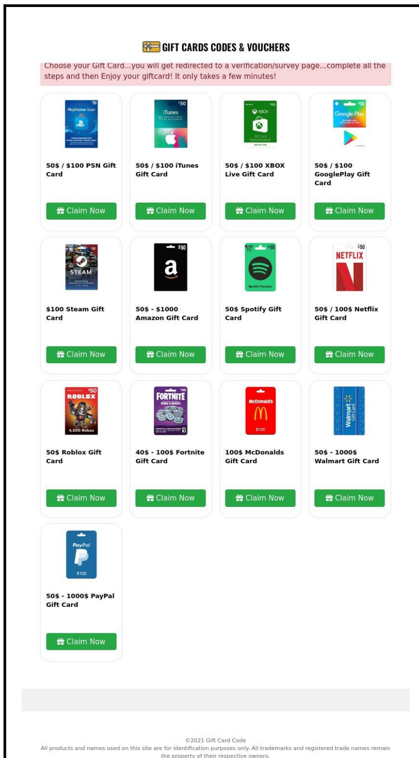
Screenshot of www[.]giftcard[.]prosolpk[.]com



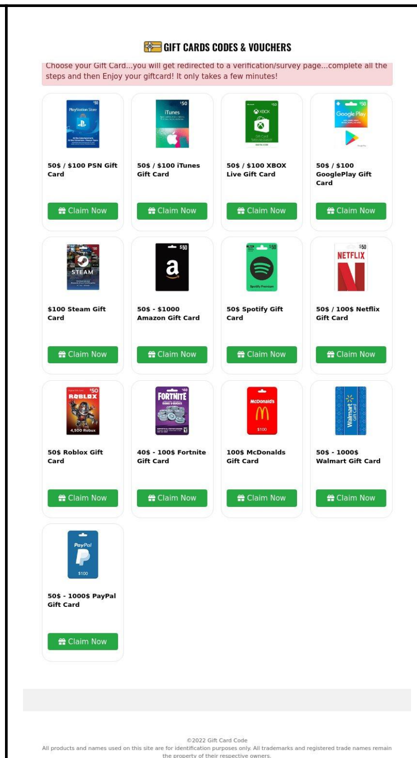
Screenshot of www[.]giftcards[.]farmaciasgaleno[.]cl

Malicious Fathers' Day Domains and Subdomains

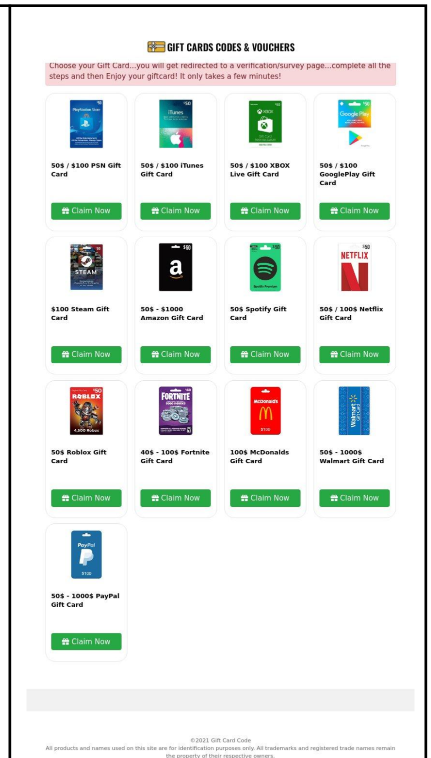
As of 10 June 2022, only 14 properties have been flagged as malicious, many of which still hosted live content. While our browser security prevented us from visiting some of them, we obtained some screenshots. Three malicious domains hosted precisely the same page, as shown below.



Screenshot of



Screenshot of



Screenshot of

gogiftcard[.]club	*giftcardhubs[.]net*	*giftcardzone[.]top*

—

Special occasions like Father's Day may increase malicious activities, as threat actors take advantage of people's interest in gifts. If you notice, most of the screenshots provided above showed pages offering gift cards. These could be used for other holidays and special events as vehicles for fraud and malware-enabled attacks.

If you wish to perform a similar investigation or research, please don't hesitate to contact us. We're always on the lookout for potential research collaborations.

Appendix: Sample Father's Day-Related Domains and Subdomains

Sample Domains Related to Father's Day Added from 1 May to 10 June 2022

- fatherlessfathersday[.]com
- fatherzzday[.]com
- fatherlessonfathersday[.]com
- fatheringday[.]org
- winfathersday[.]com
- fathersdayiseverday[.]com
- fathersdayiseverday[.]net
- fatherdaystore[.]com
- fathersdaynfts[.]com
- giftfatherday[.]shop
- fathersday2022[.]com
- everydayisfathersday[.]net
- fatherdayconvos[.]com
- fathersdaystyles[.]com
- worxfathersday[.]co[.]za
- fathersdaysurvey[.]com
- fathersdayadvice[.]com
- fathersdaysummit[.]com
- fathers-daygifts[.]com
- fathersdaybundle[.]com
- fathersdaywatches[.]com
- pgfathersdaysweeps[.]com
- coop-fathers-day[.]co[.]uk
- homedepotfathersday[.]com
- fathersdaypopupshop[.]com
- fathersdaygiftsclub[.]com
- fathersdaygiftsidea[.]com
- fatherdayshirtcenter[.]com
- fathersdaywedgucation[.]com
- personalizedfathersday[.]com
- thanks-fathers-day2022[.]com
- perfect-fathersdaygifts[.]com
- shopritefathersdaysweep[.]com
- shopritefatherdaysweeps[.]com
- shopritefathersdaysweeps[.]com
- fitterfathersdaychallenge[.]com
- shopritefathersdayssweeps[.]com
- ck-fragrances-fathers-day[.]com
- shoprightfathersdaysweeps[.]com
- michultracofathersdaysweeps[.]com
- shopritefathersdaysweepstakes[.]com

- fathersdaystainlesssteelwallet[.]com
- dadadot[.]day
- sdad[.]today
- adaday[.]xyz
- pxdadayi[.]cn
- daddies[.]day
- sundaday[.]com
- tongdaday[.]com
- buildaday[.]app
- tongdaday[.]xyz
- agoodaday[.]com
- vitosdaday[.]cf
- bagdadday[.]com
- dadagaga[.]today
- adamandaday[.]com
- magandadayi[.]com
- madrugadaday[.]com
- dadayfansipan[.]vn
- dadaykhoemanh[.]cf
- godaddytoday[.]com
- apostcardaday[.]ws
- presentdaydad[.]co
- dadaytaybac[.]live
- trungtamdaday[.]tk
- dadaycurcumin[.]vn
- yearsandaday[.]com
- todaysdadjoke[.]fun
- callmedaddy[.]today
- anightandaday[.]com
- secondaday[.]online
- acessibilidade[.]day
- deadbeatdads[.]today
- fuaidadayaofang[.]cn
- michaeldadayan[.]com
- blackfridaydad[.]com
- dadaycurcumin[.]click
- htxtaybacdaday[.]site
- ultimatedadsday[.]com
- dadiqiusenlin[.]today
- dayddadsigvisica[.]tk
- idaddaymeganbest[.]tk
- dadaycurcumin[.]online
- poundadayfatloss[.]com
- dadaythaoduoc[.]online
- knightoncanadaday[.]ca
- canadadaysaskatoon[.]ca
- foreverandaday[.]studio
- kanadadayenihayat[.]com
- oportunidadenet[.]today
- knightoncanadaday[.]com
- deadbeatdadstoday[.]com
- dadoomsdaybackpack[.]com
- funfloridadaytrips[.]com
- dingdongdaddydayton[.]com
- whosyourdaddyforday[.]com
- dadanhidayatulloh[.]my[.]id
- vienquanydieutridaday[.]xyz
- chualonghuongdaday[.]online
- acessibilidadedigital[.]day

Sample Subdomains Related to Father's Day Added from 1 May to 10 June 2022

- fathersday[.]stellaartois[.]com[.]mx
- fathersday[.]poweruptoys[.]com
- fathersday[.]harpercollins[.]com
- fathersday[.]wd40[.]co[.]uk
- fathersday[.]interactivedigital[.]com[.]gh
- fathers-day[.]straal[.]com
- fathersday1[.]blackdragonma[.]com
- fatherdayddd[.]blogspot[.]com
- 14fathersday[.]blogspot[.]in
- ckfathersday[.]vercel[.]app

- qa[.]fathersday[.]stellaartois[.]com[.]mx
- api[.]fathersday[.]stellaartois[.]com[.]mx
- dev[.]fathersday[.]stellaartois[.]com[.]mx
- fathersday-biz[.]myshopify[.]com
- www[.]fathersday[.]fundootimes[.]com
- fathersday2022[.]ruggedoutdoorsman[.]com
- www[.]fathersday[.]interactivedigital[.]com[.]gh
- fathersdayezine[.]trnd[.]ly
- fathersdayadmin[.]1kapp[.]com
- ww17[.]fathersday[.]festtoday[.]com
- hlagrofathersday[.]trnd[.]ly
- stage[.]fathersday[.]stellaartois[.]com[.]mx
- fathers-day-2022[.]novabase[.]stream
- fathers-day-poems[.]lookera[.]net
- amplifyfathersday[.]trnd[.]ly
- www[.]fathersday2022[.]ruggedoutdoorsman[.]com
- fathers-day-with-adr[.]pinedaphotos[.]com
- happyfathersday-cards[.]blogspot[.]com
- fathers-day-store-2022[.]myshopify[.]com
- 2022fatherday[.]fhc-event[.]memoriki[.]com
- www[.]fathers-day-with-adr[.]pinedaphotos[.]com
- fathers-day-gifts-2017-2[.]creator-spring[.]com
- fathersday-fishing-event[.]braveskies[.]info
- www[.]personalizedfathersday[.]metahealthsupplements[.]com
- happyfathersdayimagesquotes[.]bangla-sms[.]xyz
- fathers-day-poems-and-quotes[.]lookera[.]net
- fathers-day-quotes-and-sayings[.]lookera[.]net
- feature-father-day-tc-axpylpq-gaumfkxcdovp4[.]us-2[.]platformsh[.]site
- www[.]feature-father-day-tc-axpylpq-gaumfkxcdovp4[.]us-2[.]platformsh[.]site
- edit[.]feature-father-day-tc-axpylpq-gaumfkxcdovp4[.]us-2[.]platformsh[.]site
- daday[.]vuikhoesong[.]com
- daday[.]taoxoandaiviet[.]fun
- daday[.]kiemthaoduoc[.]com
- dadaypt[.]web99[.]xyz
- dadaychub[.]vppharm[.]vn
- dadaykhoe[.]yenvivuong[.]com
- spendaday[.]revverdigital[.]com
- www[.]adaday[.]axoneday[.]xyz
- savedadaymx[.]wixsite[.]com
- canadaday22[.]jelijo[.]ca
- dadsbirthday[.]carrd[.]co
- dayandadream[.]chinesefoodsite[.]com
- apostcardaday[.]now[.]sh
- apostcardaday[.]homesecuritymac[.]com
- canadadaytext[.]pagespeedmobilizer[.]com
- apostcardaday[.]gnula[.]se
- www[.]canadaday22[.]jelijo[.]ca
- daddayafternoon[.]biz[.]at
- www[.]amandadayman[.]amtamembers[.]com
- www[.]apostcardaday[.]gnula[.]se

- daddy-everyday-inc[.]square[.]site
- dichavidayfelicidad[.]blogspot[.]com
- feteducanadaday[.]phh1[.]lebleu[.]co
- comunidadaymaralynch[.]blogspot[.]com
- foreverandaday-studio[.]ellischaplin[.]co[.]uk
- www[.]foreverandaday-studio[.]ellischaplin[.]co[.]uk
- www[.]feteducanadaday[.]phh1[.]lebleu[.]co
- universidaddaysprin9bjcd[.]samp-rp[.]su
- www[.]universidaddaysprin9bjcd[.]samp-rp[.]su
- christmasbirthdaygiftsfordad[.]webstarts[.]com
- gowday5fdadrxil542ba6bqvxu[.]us-west-2[.]es[.]amazonaws[.]com
- o6bex7vhq23xeyedadr4hg7day[.]ca-central-1[.]es[.]amazonaws[.]com
- bestgiftformumdad[.]blogspot[.]com
- giftedadvisorycouncil[.]ch2v[.]com
- www[.]www[.]daddyogiftvoucher[.]phonesites[.]com
- fatherslegacy2022[.]gomezportraits[.]com
- my-father-app-02-05-2022[.]herokuapp[.]com
- xcsdadfr2022[.]dray-dns[.]de
- dadvisors2022[.]wixsite[.]com
- ciudadreal2022[.]blogspot[.]com
- godaddy20220430[.]workers[.]dev
- kai2022[.]catdadi[.]webredirect[.]org
- www[.]xcsdadfr2022[.]dray-dns[.]de
- monikadadyan2022[.]leifandersenphotography[.]com
- odade-ket-new2022[.]ru[.]com
- exposeguridad2022[.]axxonsoft[.]com
- exedadietbook2022[.]ru[.]com
- eledadietbook2022[.]ru[.]com
- adadoxdiettdim2022[.]ru[.]com
- dev-fedadmision2022[.]futuraschools[.]edu[.]pe
- bksaudades31mar2022[.]aloj[.]pt
- www[.]monikadadyan2022[.]leifandersenphotography[.]com
- feijoadadesjorge2022[.]tucaboclojundiara[.]com[.]br
- lasavesdemiciudad2022[.]blogspot[.]com
- akedadimslimketoo2022[.]ru[.]com
- exodadimslimketoo2022[.]ru[.]com
- www[.]bksaudades31mar2022[.]aloj[.]pt
- www[.]feijoadadesjorge2022[.]tucaboclojundiara[.]com[.]br
- www[.]oportunidade2022[.]fun[.]oportunidadeunica2021[.]com[.]br
- liquidadminbackup2022[.]direct[.]quickconnect[.]to

Malicious Properties Flagged during the Malware Check Dated 10 June 2022

- father-attached-iii-shopper[.]trycloudflare[.]com
- giftcards[.]com-com[.]biz
- www[.]giftcards[.]com-com[.]biz
- adaday[.]xyz
- godads[.]shop
- mdadqdf[.]shop
- seguridadcol[.]shop
- schoolfathergame[.]xyz
- dscardgift[.]xyz
- gogiftcard[.]club
- giftcardzone[.]top

- giftcardhubs[.]net
- giftgamescard[.]xyz
- googlegiftcards[.]tk