Beauty and the Beast: Are These Domains Possible Vehicles for Cosmetic Product Counterfeiting?

Table of Contents

Executive Report

Months after TikTok launched its marketplace in September 2021, several users have raised concerns about the authenticity of the products they purchased. The complaints mainly pertain to beauty products, such as sunscreens, lip glosses, and makeup brushes. Aside from being ripped off, consumers may be exposed to more danger.

The City of London Police, through Cosmetics Business, cited that counterfeit beauty products may contain banned or restricted substances harmful to people.

The issue isn't only happening on the social media platform. For years, counterfeiters have used fake websites that impersonate cosmetic brands. In line with this, WhoisXML API researchers monitored the Domain Name System (DNS) for activities related to some of the top cosmetic brands. Our findings include:

- 1,900+ digital properties added from 1 June to 18 July 2022 that use the names of popular beauty brands, including Avon, Clinique, L'Oréal, Nivea, and The Body Shop
- These recently-added properties are part of a larger data set of 11,000 brand-targeted cybersquatting resources added since the beginning of the year
- About 1% of these domains have figured in malicious campaigns, some of which are still actively resolving to six unique IP addresses
- The content of some domains reveals they are selling beauty products

We further explore these findings below.

Potential Cybersquatting Properties Targeting Famous Beauty Brands

Since the start of the year, more than 11,000 cyber resources containing the names of the brands in the study have been added to the DNS. However, our data sample comprises properties added from 1 June to 18 July 2022 to make insights more time-sensitive.

The study also centers on 16 cosmetic brands, as seen in the chart below.

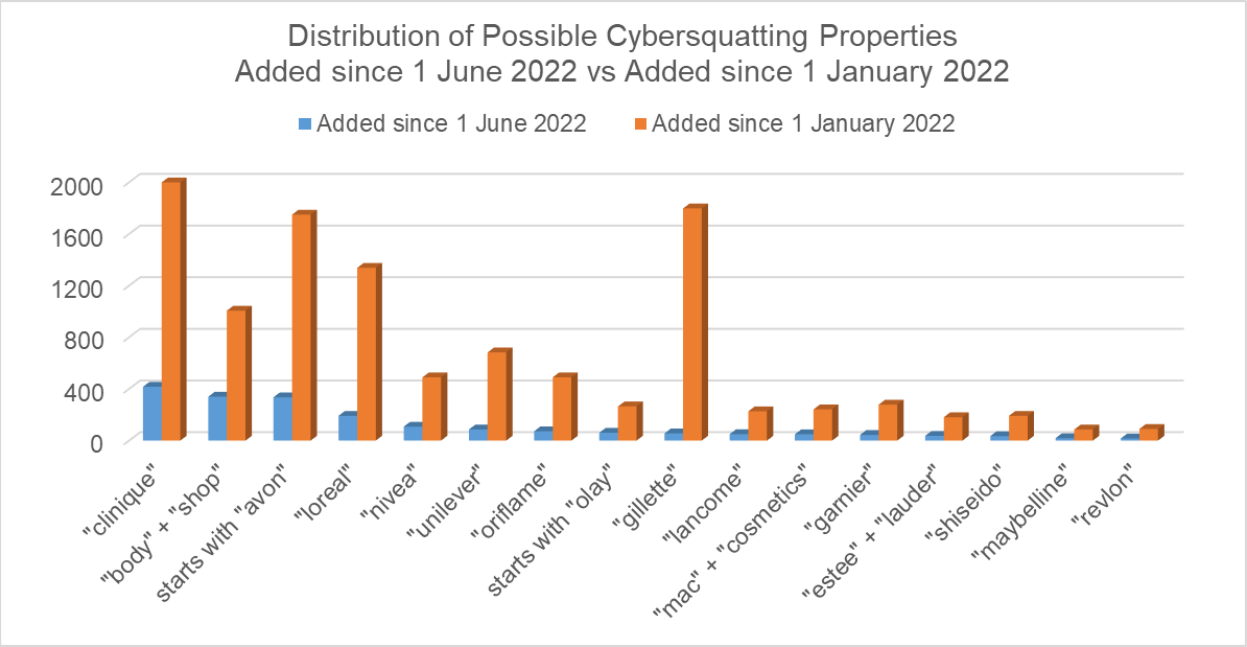
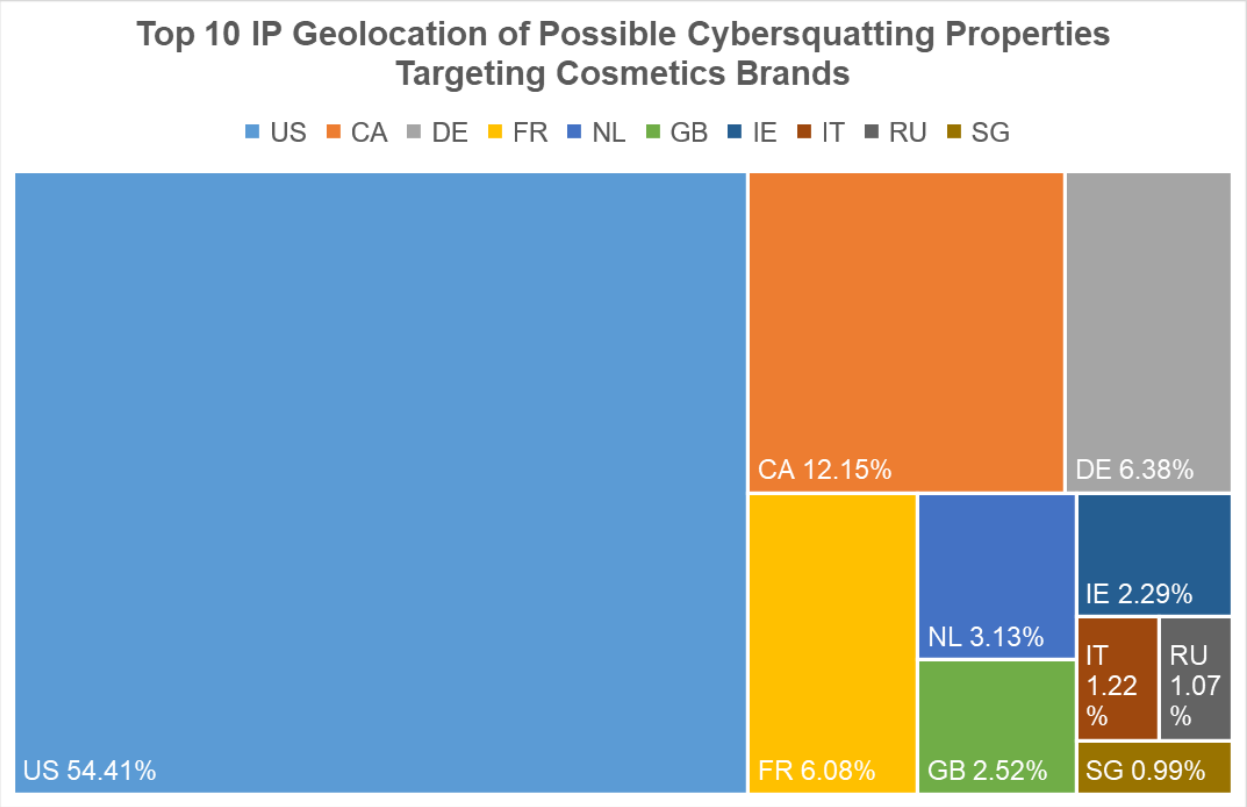


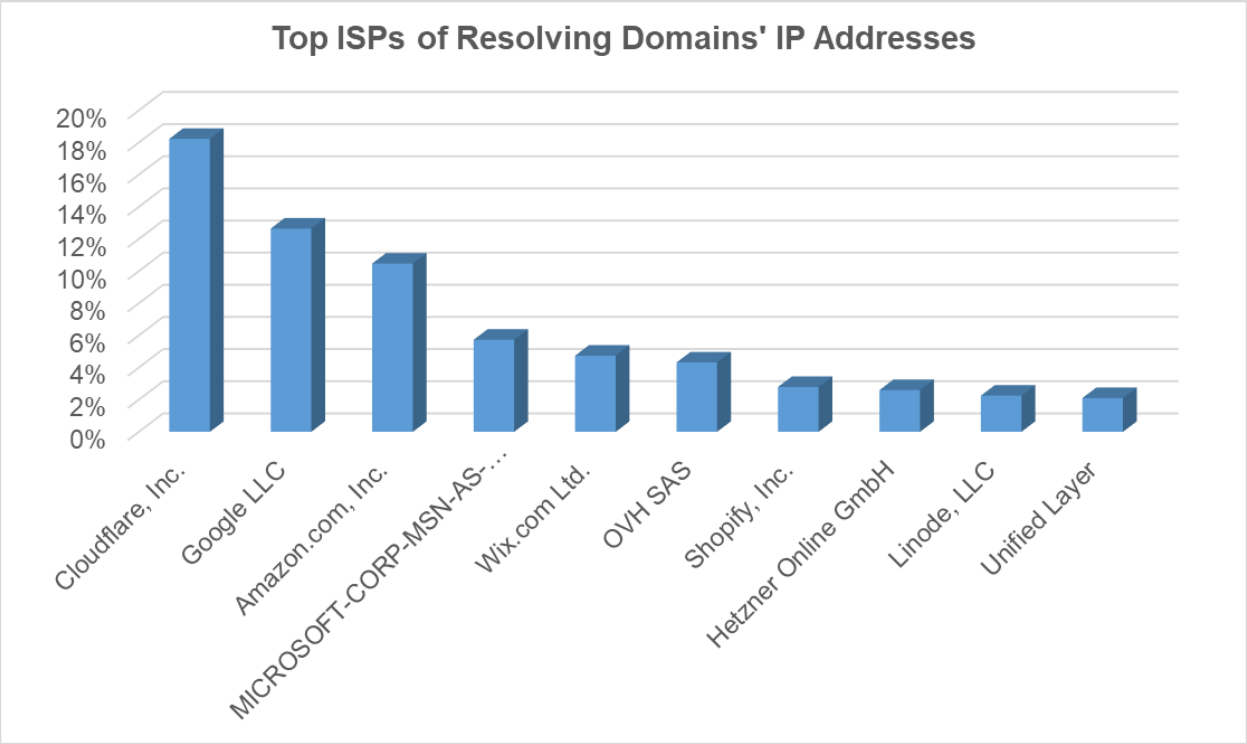
Chart 1: *Distribution of domains and subdomains containing the names of 16 cosmetic brands added from 1 June to 18 July 2022 and 1 January to 18 July 2022*

Adding Context to the Properties

To learn more about the cosmetic-themed domains and subdomains, we ran them on Bulk IP Lookup. About 88% of the domains actively resolve to 1,415 different IP addresses. Most of these are geolocated in North America, with 54.41% in the U.S. and 12.15% in Canada. The rest of the top 10 geolocations pointed mostly to Europe, while two did to Asia. The rest of the resolutions were spread out across 45 other territories.

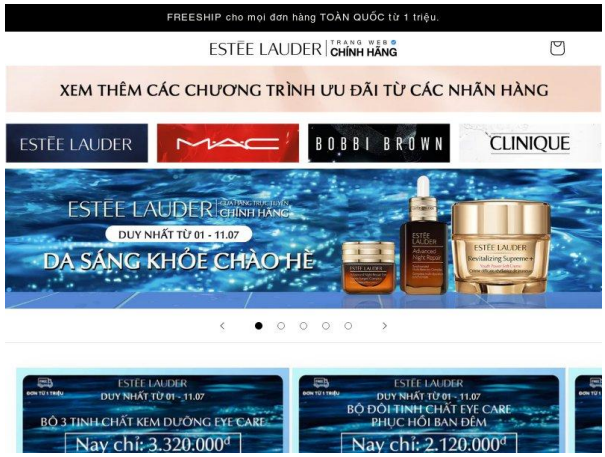


We also took note of the digital resources' Internet service providers (ISPs) and found that Cloudflare accounted for the greatest number of connected IP addresses at 18.23%. Google followed with 12.65%, Amazon with 10.47%, Microsoft with 5.73%, and Wix with 4.74%. The rest of the leading ISPs can be seen in the chart below.

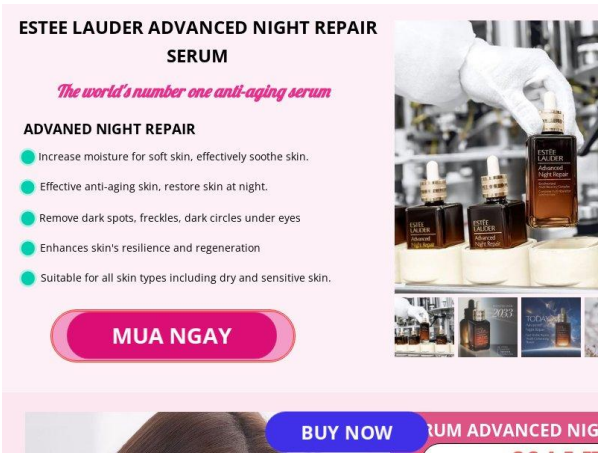


Are These Domains Selling Counterfeit Products?

We performed a screenshot analysis of the resolving properties with the help of Screenshot API. While several domains were parked or resolved to index and 404 pages, some sold beauty products, although their WHOIS records could not be attributed to the legitimate brands.



Screenshot of esteelaudercompaniesvn[.]com and esteelaudervn[.]asia



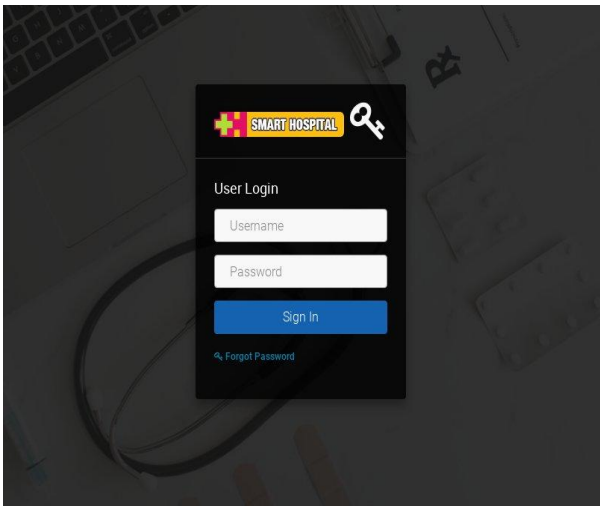
Screenshot of esteelaudermalaysia[.]pw, esteelauderph[.]makeup, esteelauderpromotion[.]com, and esteelaudershop[.]shop

These contents were replicated across other cybersquatting domains, as seen in above. All domains didn't have enough metadata to be classified under the Beauty and Style & Fashion categories, some of the official Estée Lauder domain classifications.

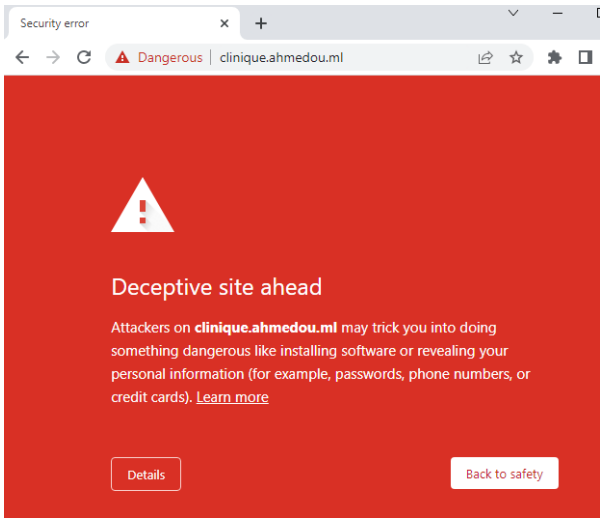
Malicious Usage

Aside from counterfeit products, we also looked out for properties used in phishing, spamming, malware distribution, impersonation, and other malicious activities. About 1% have been reported as malicious, despite having made their way into the DNS only in June.

Five of these properties still resolved to IP hosts. Alarmingly, the malicious subdomains clinique[.]ahmedou[.]ml continued to host a login page.



Screenshot lookup result of clinique[.]ahmedou[.]ml



Live screenshot of clinique[.]ahmedou[.]ml

—

Fake cosmetics can be detrimental to people's health. At the same time, fake sites can negatively affect the reputation of the impersonated brands. Preventing counterfeiting involves monitoring the DNS for possible vehicles like those featured in this study.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.

Appendix: Sample Domains

Sample Domains Added From1 June to 18 July 2022

- 150th-shiseido-event[.]com
- 180studios-gillettecorner[.]co[.]uk
- 24oriflame[.]pl
- 260sgillette[.]com
- 360bodyshop[.]net
- 3rrrautobodyshop[.]com
- abdulaidiallorealty[.]com
- acqueflореali[.]it
- aestheticclinique[.]vg
- alejadybodyshop[.]com
- allcolorsbodyshop[.]com
- allloreal[.]com
- allmaybelline[.]com
- almajedsantepolyclinique[.]com
- altanerabodypiercing[.]shop
- amazonbodyshop[.]com[.]br
- ambabody[.]shop
- amelioclinique[.]com
- amgiloreale[.]cf
- amigosbodyshop[.]repair
- amymolorealty[.]com
- anastosbodyshop[.]com
- anhelorealty[.]com
- anhelorealty[.]info
- anhelorealty[.]net
- anybodylove[.]shop
- apexbodyshop[.]co[.]uk
- appellorealestate[.]ws
- aram-clinique-tunisie[.]com
- aromacosmetics[.]cz
- arroyograndebodyshop[.]com
- artigianifloreali[.]it
- artisan-menuisier-garnier[.]com
- asistentevirtualesteelauder[.]com
- atlantabody[.]shop
- auonlinesupportthebodyshop[.]com
- autobodyshopanderson[.]com
- autobodyshopcranston[.]com
- autobodyshoplubbock[.]ws
- autobodyshops[.]us
- autobodyshoptruganina[.]com
- automotionbodyshop[.]com
- autotowingbodyshopcentraltx[.]ws
- avclinique[.]com
- avon[.]icu
- avon8[.]com
- avonab[.]ga
- avon-admin[.]africa
- avon-admin[.]durban
- avonaero[.]site
- avonagile[.]com
- avonali[.]com
- avonalinvestment[.]com
- avonandaomersetpas[.]co[.]uk
- avonandsomersetpas[.]uk
- avonandsomerstepas[.]co[.]uk
- avonandsomsersetpas[.]co[.]uk
- avonandsomsetpas[.]co[.]uk
- avonandsoomersetpas[.]co[.]uk
- avonanglicans[.]org[.]au
- avon-asm[.]ru
- avon-asm[.]store
- avonavi[.]pt
- avonaw[.]net
- avon-ax[.]ru
- avonbekescsaba[.]hu
- avonbend[.]com
- avonboosting[.]site
- avonbraefs[.]co[.]uk
- avonbrae-fs[.]co[.]uk
- avonbrochureonline[.]com
- avonbuildcon[.]com

- avonbylauramolina[.]com
- avonc[.]com[.]br
- avoncapacita[.]com
- avoncateringequipment[.]com
- avoncateringquipment[.]co[.]uk
- avoncbt[.]co[.]uk
- avon-center[.]kz
- avon-city[.]store
- avonclothing[.]shop
- avoncoating[.]com
- avoncomlashonwilliasm[.]online
- avoncomlashonwilliasm[.]website
- avon-creative[.]co[.]uk
- avoncycling[.]co[.]uk
- avondale[.]realty
- avondale-38960-kilimanjaro[.]com
- avondaleappliancesmobile[.]com
- avondaleartificialturf[.]com
- avondalebyspectronate[.]com
- avondalecitynews[.]com
- avondaledodg[.]com
- avondalehouseandforestpark[.]ie
- avondalemortage[.]com
- avondalenissa[.]com
- avondalerentalunit[.]online
- avondaleridgefarm[.]com
- avondaleridgefarms[.]com
- avondale-services[.]com

Sample Subdomains Added From 1 June to 18 July 2022

- 0001-unilever[.]reckon[.]ai
- 0004-unilever[.]reckon[.]ai
- 0010-unilever[.]reckon[.]ai
- 9tzbs7j7gh33tt3[.]blog[.]bodyshopbusines[.]smattermost[.]com
- advocaloreal[.]inet[.]studio
- aloreal[.]vochithanh[.]com
- ann-douglass-candle-and-body-shoppe[.]myshopify[.]com
- api[.]clinique-minimes[.]bivouac[.]io
- api[.]internal[.]sandbox[.]loreal[.]fluentcommerce[.]com
- api[.]loreal[.]bloomflow[.]com
- api[.]loreal-staging[.]bloomflow[.]com
- api[.]production[.]loreal[.]fluentcommerce[.]com
- api[.]unilever[.]bloomflow[.]com
- aram-clinique-tunisie-com[.]azurewebsites[.]net
- arroyoelblancomexico[.]bigthings[.]com
- artwork-bodyshop[.]myshopify[.]com
- atelieraestheticcliniqueclone[.]gogroth[.]com
- auto-body-repair-shops-reviews[.]bayareapaintlessdentrepair[.]com
- auto-body-shop-express[.]bayareapaintlessdentremoval[.]com
- autobodyshops[.]co[.]com
- auto-body-shops-near-me[.]bayareapaintlessdentremoval[.]com
- avon[.]adobomall[.]com
- avon[.]apps-bundles-rc[.]makebecool[.]com
- avon[.]berletroofing[.]com
- avon[.]citydeals[.]live
- avon[.]cloudjiffy[.]net
- avon[.]is-a[.]dev
- avon[.]juvenatemedia[.]co[.]uk
- avon[.]kosmetic[.]store
- avon[.]koverin[.]site
- avon[.]kyiv[.]ua
- avon[.]maquillagei[.]biz

- avon[.]mercyitcorp[.]com
- avon[.]mersuq[.]com
- avon[.]parol-group[.]com
- avon[.]polytechit[.]com
- avon[.]udpsa[.]com
- avon[.]votresite[.]ws
- avon7008[.]zendesk[.]com
- avon9448[.]zendesk[.]com
- avonaescapes[.]graffiti-graphics[.]online
- avonandsomerset[.]instantcloud[.]cn
- avonandsomerset[.]soc[.]srcf[.]net
- avonapi[.]mercyitcorp[.]com
- avonatechnologies[.]ez-backup[.]net
- avonbeauty[.]fashion[.]blog
- avonber[.]jupyter[.]ssc[.]dev
- avonbiela[.]myshopify[.]com
- avonbkp01-tdgr24o76yrorucb[.]dattoweb[.]com
- avonboating[.]ticknovate[.]com
- avoncadastro[.]yolasite[.]com
- avonchina[.]rackmaze[.]com
- avonchina[.]se[.]net
- avon-city[.]ruwww[.]inmusicbrands[.]com
- avoncms[.]bettertech[.]sa
- avoncustomerportal[.]azurewebsites[.]net
- avond4daagse-borgwal[.]marcelmombarg[.]nl
- avondale[.]1kapp[.]com
- avondale[.]mycloud[.]by
- avondale[.]square7[.]ch
- avondale[.]virtual-user[.]de
- avondalekitchens[.]direct[.]quickconnect[.]to
- avondanceandmartialart[.]smattermost[.]com
- avondbhanp[.]v2-prober[.]v2q[.]certsbridge[.]com
- avondbloem[.]hicam[.]net
- avondbloem[.]ngrok[.]io
- avon-dev[.]globalpreviews[.]net
- avondgebed[.]clemenspoort[.]be
- avondhubroadband[.]roniartwebdesign[.]com
- avondrood[.]zaaksysteem[.]net
- avondschool-downloads[.]hogent[.]be
- avonealunu[.]ctn[.]gts[.]multisan[.]st[.]ap[.]gtr-dev[.]certsbridge[.]com
- avonecommerce[.]srbrand[.]es
- avonelena[.]za[.]com
- avon-fe-web[.]accuhit[.]com[.]tw
- avon-fe-web-vue1[.]pages[.]dev
- avonfitnessmachines[.]smartlifefitness[.]com
- avonics[.]myshopify[.]com
- avonin[.]maps[.]arcgis[.]com
- avoniorla[.]za[.]com
- avonis-faouzi-ksentini-fmjfuea-kzowckj7hb3ey[.]eu[.]platform[.]sh
- avonis-lars-3ujejhy-qupdrrnfkc5zo[.]eu-4[.]platformsh[.]site
- avonis-mail-fix-7wkxl5q-zavkswewwaofo[.]eu-2[.]platformsh[.]site
- avonis-mb-yxivhey-qupdrrnfkc5zo[.]eu-4[.]platformsh[.]site
- avonis-michellev2-5ykjv4a-2myn6huoracs6[.]de-2[.]platformsh[.]site
- avonis-michelle-xsb4oui-qupdrrnfkc5zo[.]eu-4[.]platformsh[.]site
- avonkosmetika[.]ososba[.]cz
- avonleashea[.]blogspot[.]com
- avonleasparling[.]mrjamesedu[.]net
- avonlee[.]avonleehygiene[.]ie
- avonline[.]duckdns[.]org
- avonline[.]go[.]pw
- avonline[.]net[.]ws
- avonline[.]panel[.]gg

- avon-matus-escalante[.]myshopify[.]com
- avonmobile[.]bluefile[.]cz
- avon-moldova-link[.]net[.]ws
- avonmore[.]crd[.]co
- avonmore[.]gitpage[.]si
- avonmouth[.]gr[.]com

Sample Malicious Properties Flagged during the Malware Check Dated 19 July 2022

- nivea[.]cfd
- nivea[.]in[.]ua
- dovenivea[.]uno
- nivea-dove[.]xyz
- nivea-dove[.]fun
- dove-nivea[.]site
- dove-nivea[.]website
- bucklelancome[.]com
- bucklelancome[.]site
- dove-lancome[.]store
- lancome-dove[.]store
- lancome-golos[.]online
- shopinstylebodyoil[.]com
- nivea[.]dreamworkscdc[.]com
- clinique[.]ahmedou[.]ml
- www[.]clinique[.]ahmedou[.]ml