WhoisXML API Presents Global DNS Trends at Europol

On 6–7 April 2022, Europol hosted the 13th Operation In Our Sites (IOS), a recurring event that aims to foster collaboration between law enforcement agencies, the public sector, and private organizations in the fight against counterfeiting, intellectual property infringement, and online piracy. The joint effort, involving different stakeholders from 30 countries and several industries, resulted in the seizure of more than 490,000 domains in 2021.

WhoisXML API was invited to participate in the event held in Alicante, Spain, as it aligns with the company's mission to make the Internet a safer place through transparency and the sharing of data relevant to the battle against cybercrime.

In the words of our CEO Jonathan Zhang, "Early detection and, hence, protection against counterfeiting, phishing, trademark infringement, and other cybercrime are crucial in making the Internet more secure. While we gather global DNS and domain data to enable these processes, this isn't a one-company job. Boosting Internet security requires collaboration and data sharing, which Europol and Operation IOS embody."

Early Detection, Discovery, and Contextualization Techniques against Counterfeiting Domains

WhoisXML API Head of Marketing and DNS Threat Researcher Alexandre François represented the company at the event. The company's presentation looked at how a satellite view of the world's DNS could help detect, expand, and provide context to possible counterfeiting domains. The main points and investigations are shared below.

Searching for Hints of Counterfeiting in Typosquatting Groups

Individuals and entities can add several domains to their portfolio in one go through bulk domain registrations. Threat actors can also do the same to construct their malicious domain footprints.

Building on the evidence that threat actors gradually deploy bulk-registered domains, we looked at groups of domain names that are more likely to be used to sell counterfeit products. The domains in each group were registered on the same day and contained similar text strings.

Typosquatting Groups Targeting Luxury Brands

With the help of Typosquatting Data Feed, we selected 88 typosquatting domain groups linked to luxury brands, including Armani, Burberry, Cartier, Gucci, Hermes, Louis Vuitton, Prada, Rolex, and Versace. Examples of these groups are shown below.

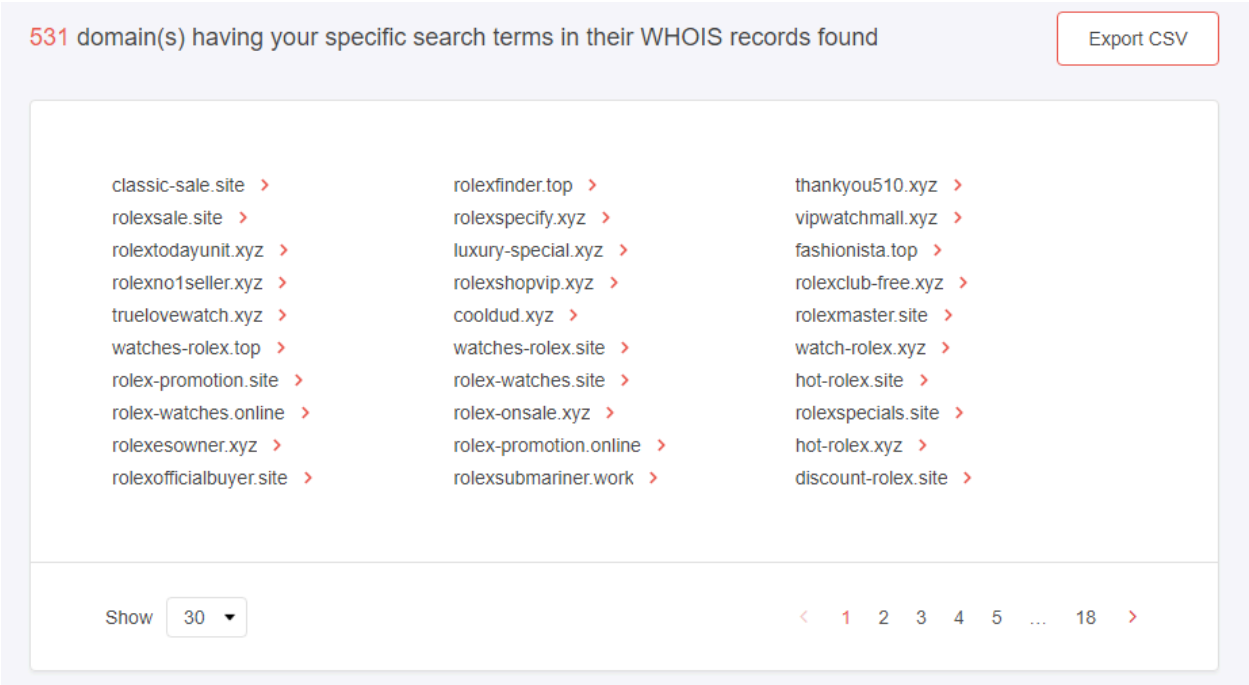
date	group_number	group_member_number	total_no_of_grp_members	domain
2021-03-29	903	2	7	sellmyrolex.boutique
2021-03-29	903	3	7	sellmyrolex.review
2021-03-29	903	4	7	sellmyrolex.guru
2021-03-29	903	5	7	sellmyrolex.shop
2021-03-29	903	6	7	sellmyrolex.store
2021-03-29	903	7	7	sellmyrolex.reviews
2021-04-04	766	1	3	jenshermes.club
2021-04-04	766	2	3	jens-hermes.club
2021-04-04	766	3	3	jens-hermes.com
2021-04-12	421	1	3	hermes-package-fees.com
2021-04-12	421	2	3	myhermes-package-fees.com
2021-04-12	421	3	3	myhermes-package-fee.com
2021-04-20	351	1	6	35casinoarmani.com
2021-04-20	351	2	6	38casinoarmani.com
2021-04-20	351	3	6	36casinoarmani.com
2021-04-20	351	4	6	37casinoarmani.com
2021-04-20	351	5	6	34casinoarmani.com
2021-04-20	351	6	6	casinoarmani.com
2021-04-23	1805	1	3	buyprada.com

Uncovering More Counterfeiting Domains

The typosquatting groups in our investigation included 540 domains in total. Enriching these domains with WHOIS information from Bulk WHOIS API enabled us to discover more. For instance, several Rolex domains were registered by an organization named “Wen Xue Hu,” as shown in the screenshot below.

domain	registrant_organization	registrant_country	registrant_state
hot-rolex.site	Wen Xue Hu	CHINA	Si Chuan
hot-rolex.shop		CHINA	Si Chuan
hot-rolex.xyz	Wen Xue Hu	CHINA	Si Chuan
watch-rolex.shop		CHINA	Si Chuan
watch-rolex.site	Wen Xue Hu	CHINA	Si Chuan
watch-rolex.xyz	Wen Xue Hu	CHINA	Si Chuan
watches-rolex.xyz	Wen Xue Hu	CHINA	Si Chuan
watches-rolex.site	Wen Xue Hu	CHINA	Si Chuan
watches-rolex.shop		CHINA	Si Chuan
watches-rolex.top	Wen Xue Hu	CHINA	

A reverse WHOIS lookup using the registrant organization as a search string revealed a much larger domain footprint—more than 500 domains, most of which also appeared to be imitating Rolex.

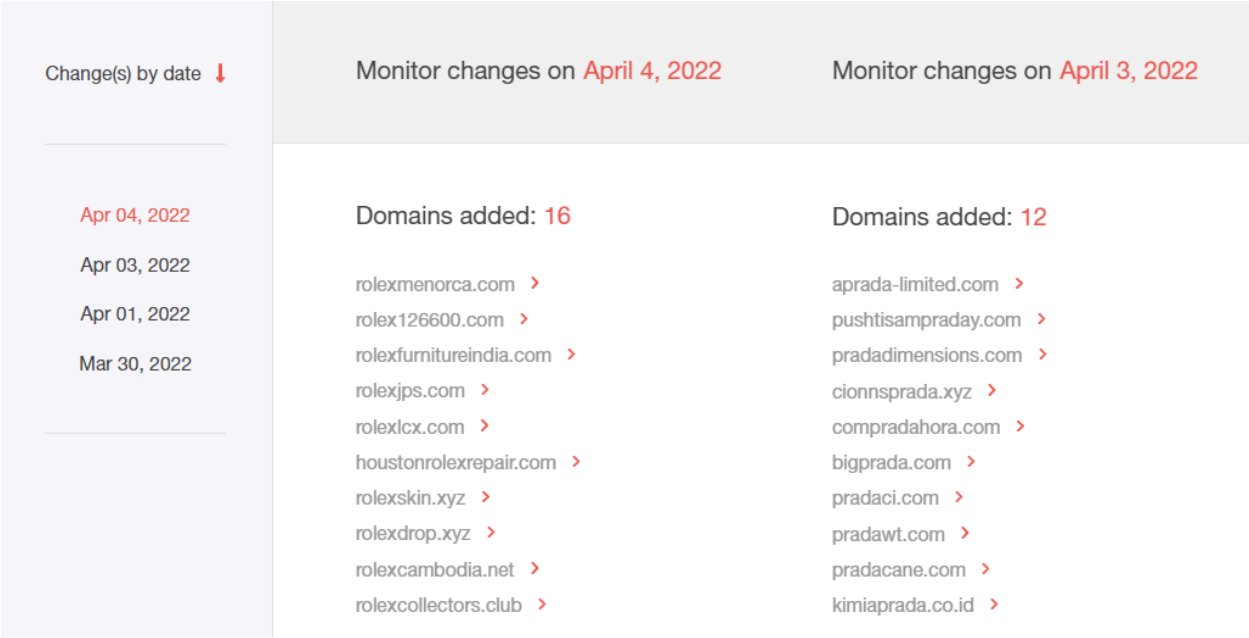


Early and Real-Time Detection of Possible Counterfeiting Domains

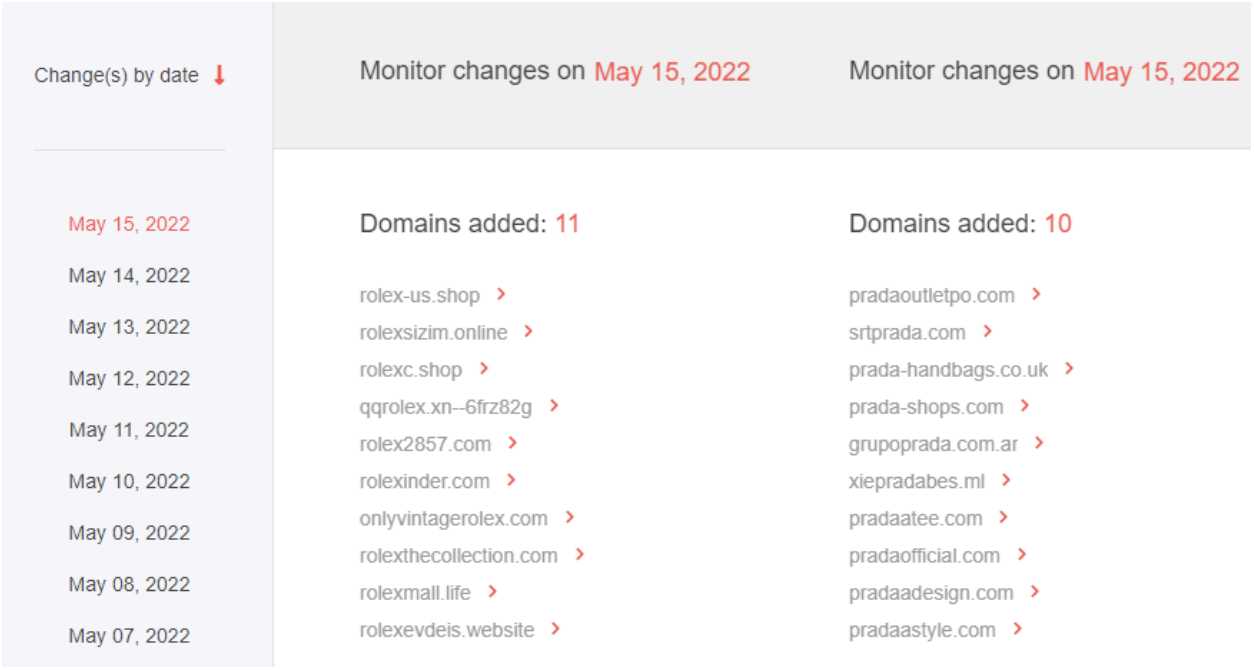
The previous technique highlighted the prevalence of bulk domain registration and how organizations can make this work for them by searching for counterfeiting clues. Another domain registration feature exploited by malicious actors is that it can be done anywhere anytime. Domains that can become possible vehicles for counterfeiting can be registered even while you sleep.

For this reason, the daily detection of suspicious domains can be an effective way to combat counterfeiting properties, possibly before they can be deployed. Brand Monitor allowed us to track the DNS activities of domains containing luxury fashion brand names.

Days before IOS, more than a dozen domains were added for each luxury brand. Below are screenshots of Prada and Rolex domains added on 3–4 April 2022.



We continued to detect the registration of similar domains each day post-IOS, including those added on 15 May 2022 below.



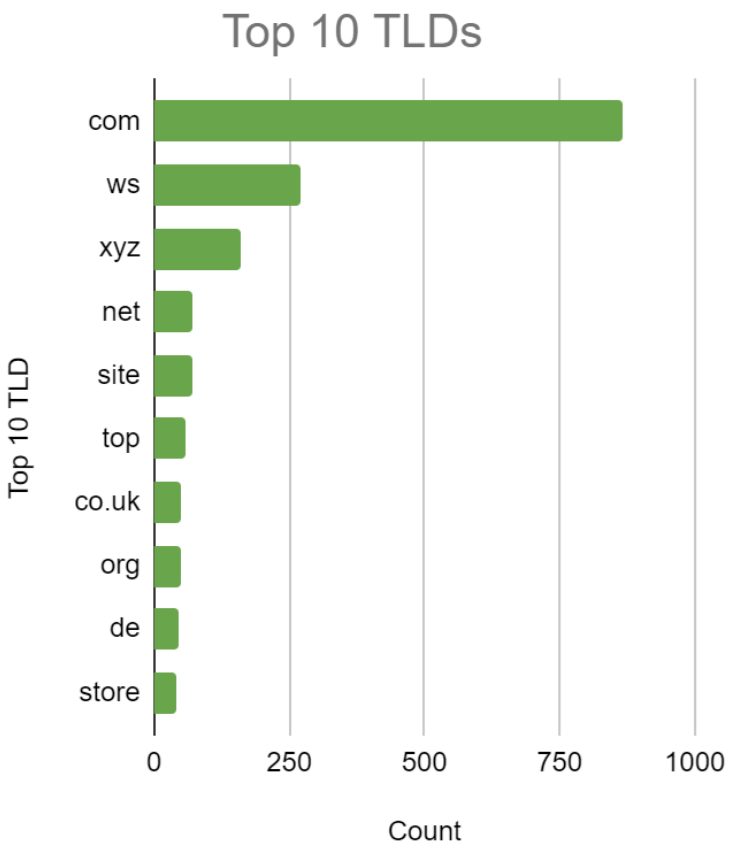
Advanced DNS Contextualization

The investigation presented during IOS XIII was further deepened by providing context gleaned from DNS intelligence.

Top-Level Domain (TLD) Analysis

The sample for this section included 2,504 domains containing the names of the above-mentioned fashion luxury brands from January to March 2022. We then identified the top 10 TLDs used in the domains, which included some of the most abused ones, namely, .ws and .top.

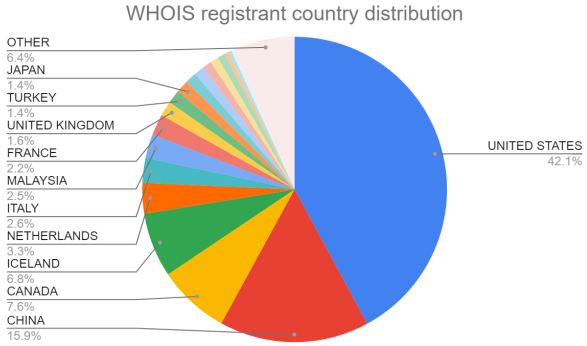
The chart below shows the TLD distribution of the domains.

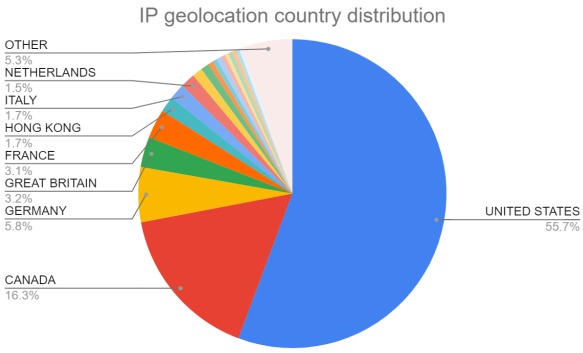


Typosquatting text strings alongside disreputable TLDs may be a suspicious combination that hints at possible counterfeiting domains.

Location Analysis

We performed two types of location analysis on the sample. One looked at the registrant countries while the other was based on the IP geolocation of the domains. The charts below show a side-by-side comparison of the WHOIS registrant country and IP geolocation distribution.



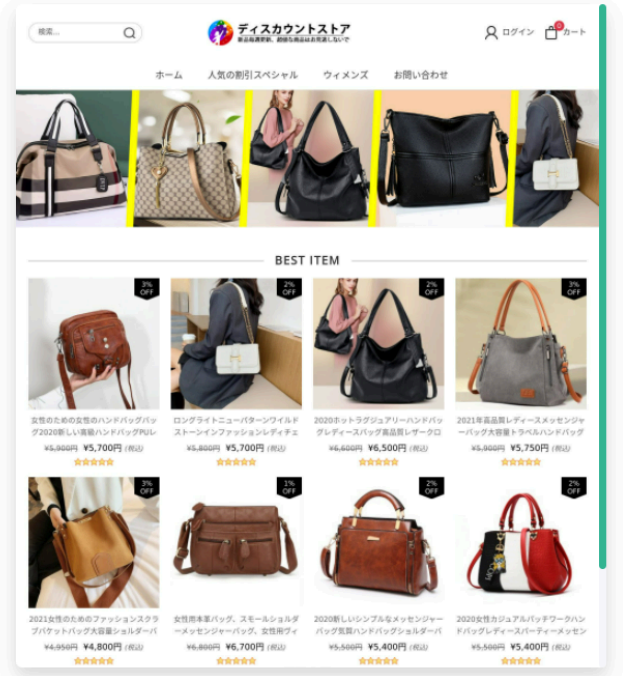


Both analyses brought us to the conclusion that although they carry European brands, most of the domains don't have European-located infrastructure.

Screenshot Analysis

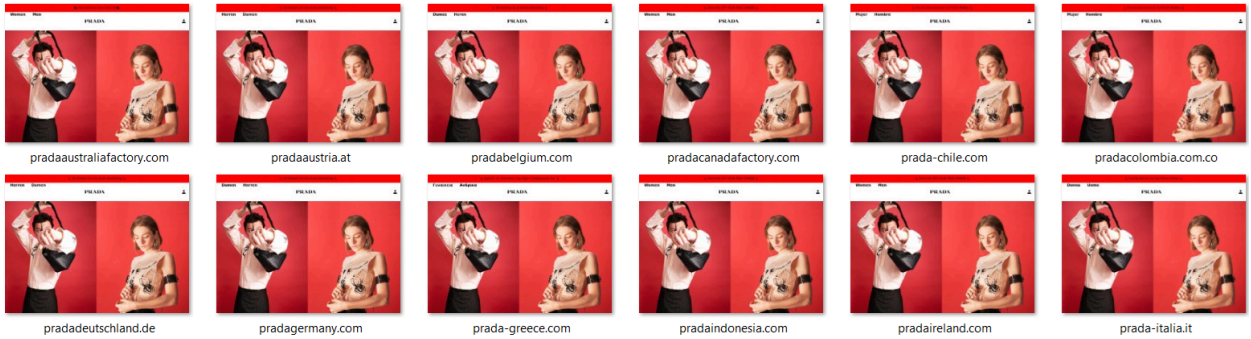
Website Screenshot API allowed us to see the content hosted by the domains. The screenshots below show a selection of bags on tokyolouisvuitton[.]com while hot-rolex[.]shop sold Rolex watches at 70% off.

tokyolouisvuitton.com website screenshot

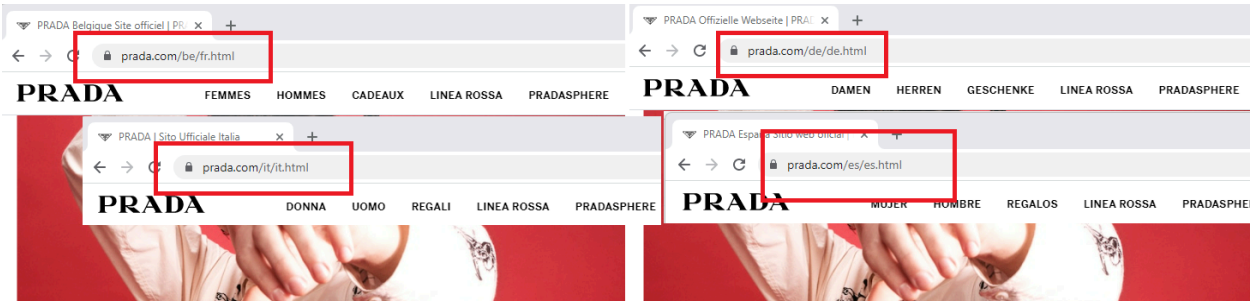


hot-rolex.shop website screenshot

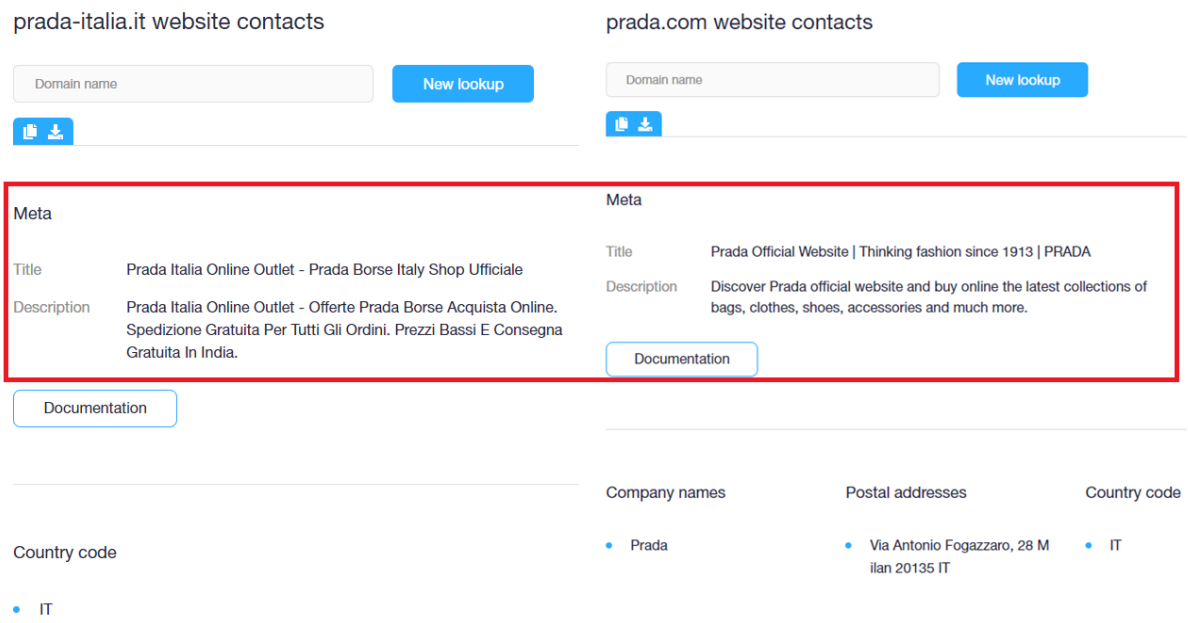
We also discovered several other web content that appeared to be imitating the luxury brands in the study. Among those that stood out was a group of Prada domains that hosted the same content as the legitimate site, as shown below.



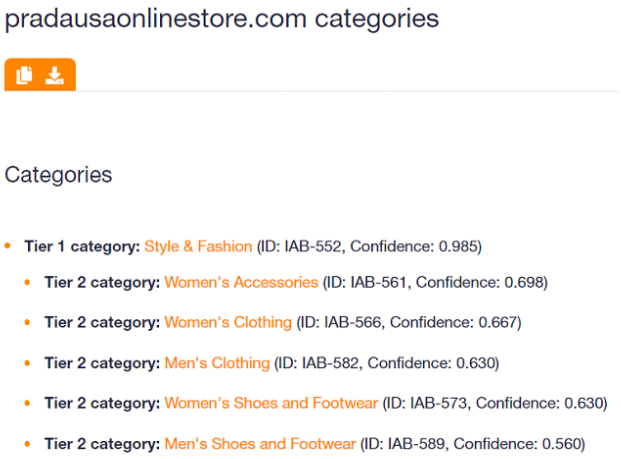
Aside from the content, these domains seemed to target different countries. They had country names as part of their second-level domain (SLD) and used geo-targeted languages.
In contrast, the legitimate Prada website uses a subdirectory structure to cater to different geographical locations.

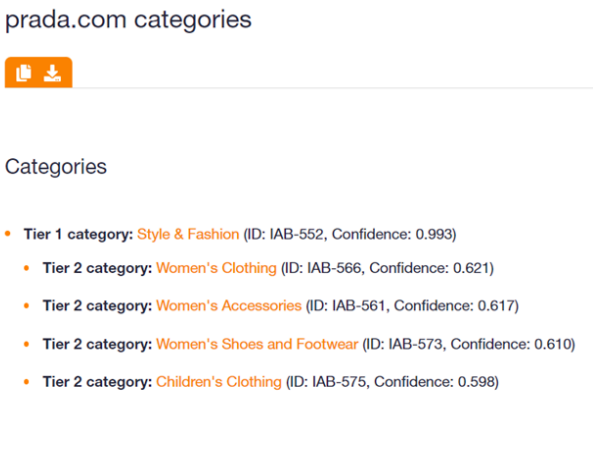


There was likely something fishy about the Prada domains identified, potentially hinting at brand squatting or a phishing campaign. Interestingly, the actors behind them went through the trouble of creating language-specific meta titles and descriptions. Website Contacts API, for instance, picked up meta tags for several Prada domains, similar to the ones shown in these images:



Also, as a result of these details and the web content, the domains were classified correctly by Website Categorization API, notably under the Style & Fashion website category.





—

Although prone to abuse and exploitation, the DNS is also full of information that enables early and real-time threat discovery and in-depth contextualization. WhoisXML API continues to explore partnership and collaboration opportunities with the public and private sectors as part of our mission to make the Internet safe through data sharing and transparency.

Please don't hesitate to contact us for inquiries and proposals for joint research and investigations or if you aim to solve business problems associated with brand squatting and counterfeiting.