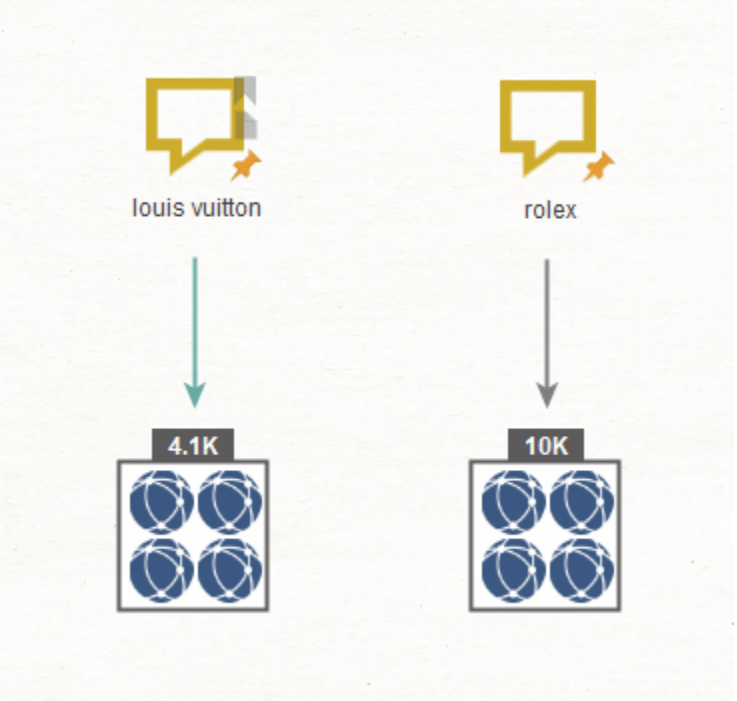
Revealing Active Counterfeiting Domain Footprints with WhoisXML API Tools and Maltego

Counterfeiting is an age-old problem that has reached unprecedented proportions following the global shift to online shopping. Let's investigate this cybercrime—particularly those targeting specific luxury brands using WHOIS, DNS, and IP intelligence gleaned through Maltego and WhoisXML API transforms.

Understanding the Extent of Online Counterfeiting

Among luxury brands' primary concerns is how massive a problem online counterfeiting or typosquatting can be. To find out, we followed these steps on Maltego using [WhoisXML transforms](#).

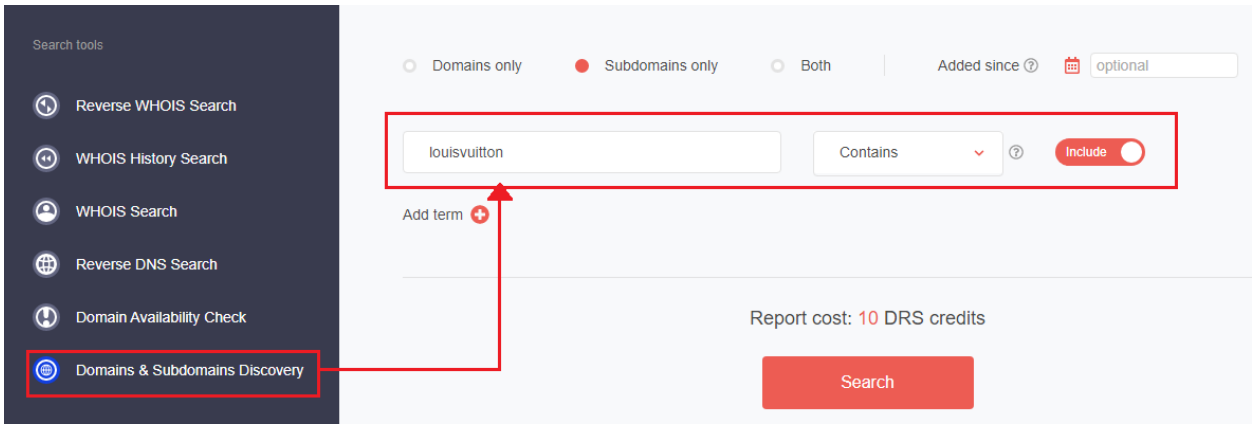
1. Add a phrase entity and type the brand name.
2. Retrieve domains containing the brand name using the "To Domains and IP Addresses (Reverse WHOIS Search) [WhoisXML]" transform.

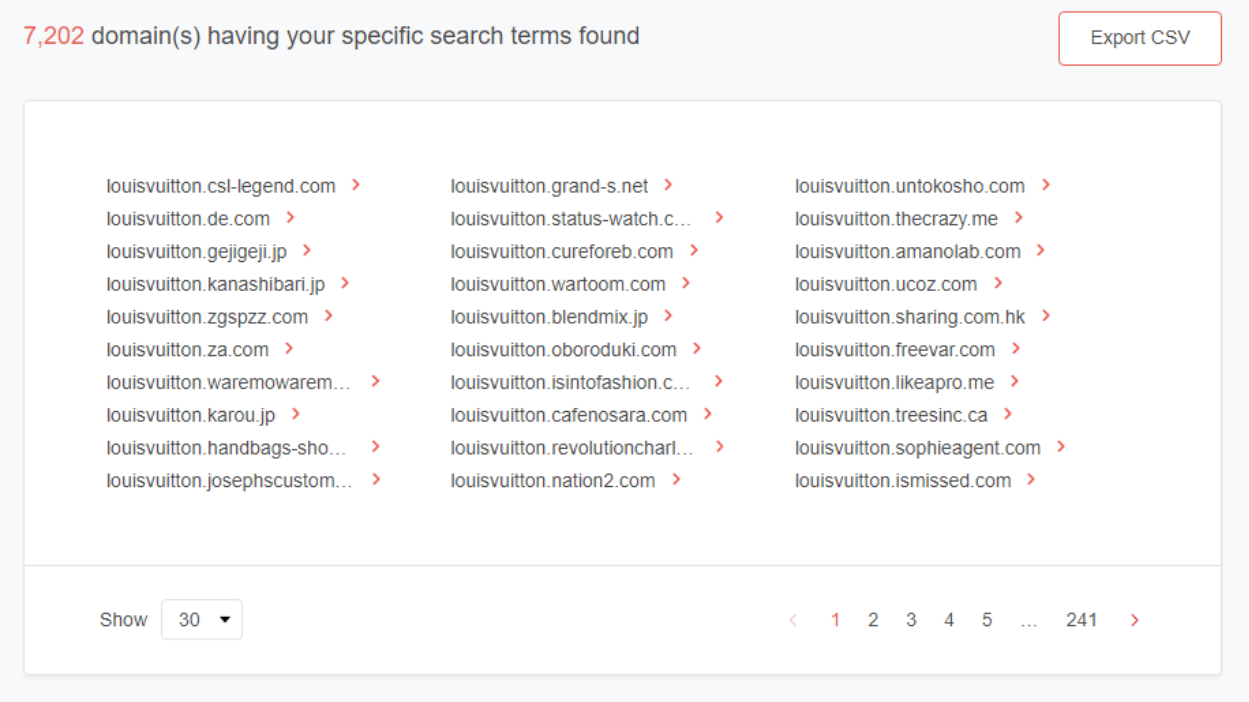


For Rolex and Louis Vuttion alone, we saw more than 14,000 domains, many of which could be associated with cybersquatting or counterfeiting.

The sample can be further expanded if we include subdomains with similar characteristics since these properties can also be used to enable additional cybercriminal practices, such as domain shadowing. We used Domains & Subdomains Discovery, which is part of the Domain Research Suite (DRS), to retrieve subdomains containing specific brand names by following these steps:

1. Go to the Domains & Subdomains Discovery window and type the brand name into the search field.
2. Make sure to set the suitable parameter. Select “Contains” if you want to retrieve all subdomains containing the brand name. Alternatively, select “Starts with” or “Ends with” if you want only subdomains that begin or end with the search string.





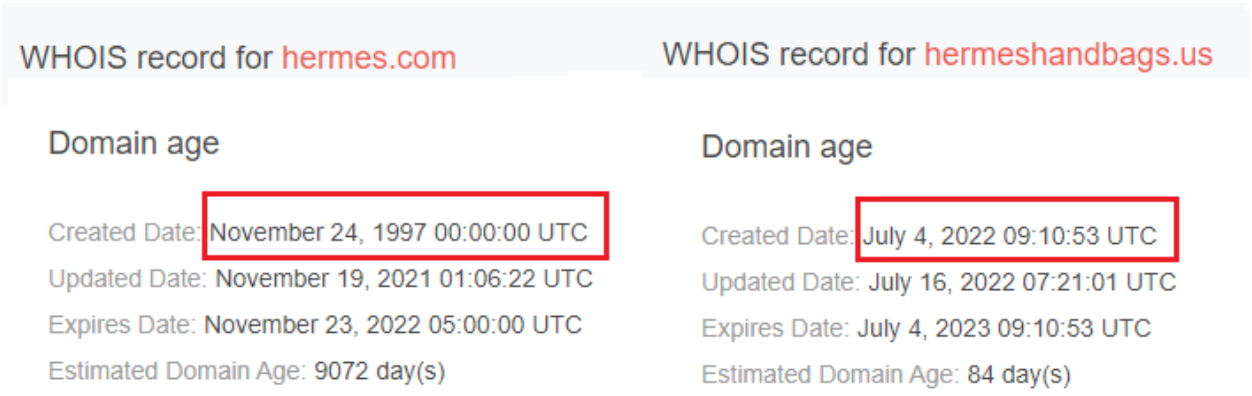
For Louis Vuitton, we found an additional 7,202 potential cybersquatting properties on top of the 4,000+ domains obtained via Maltego. Also, note that on DRS, a creation date can be defined through the “Added since” functionality if you want to narrow down results.

Techniques to Analyze and Prioritize Infringing Properties

From tens of thousands of possibly compromised or cybersquatting properties identified, false positives may be unavoidable. How do you sort which domains are possible vehicles for counterfeiting and which ones are managed by legitimate brands? Some infringing properties may also be momentarily inactive, not requiring immediate action compared to mobilized cybersquatting domains. For these, we glean insights from DNS clues.

Domain Age

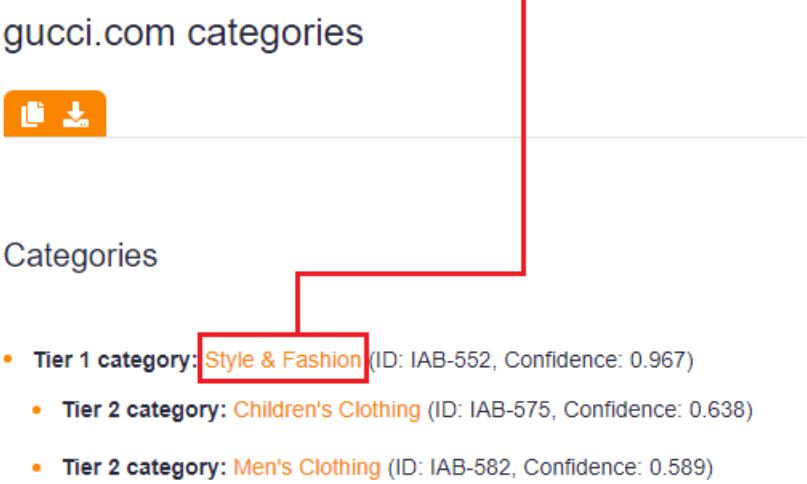
Here, we compare the creation dates of hermes[.]com and one of the cybersquatting domains targeting the brand, hermeshandbags[.]us. Hermes’s official domain has been registered since 1997, while the infringing domain was only added to the DNS in July 2022.



Website Categorization

We detected several live websites under the same categories as the imitated brands. Examples include various Gucci domains primarily categorized as Style & Fashion websites, similar to how gucci[.]com is categorized.

domainName	websit	categor	categor	categories.0.tier	categor	categor	categories.0.tier2.n	categor
guccibeltbag.com	TRUE	0.95651	IAB-552	Style & Fashion	0.678155	IAB-561	Women's Accessories	0.95651
guccibuy.ru	TRUE	0.908343	IAB-552	Style & Fashion	0.771648	IAB-561	Women's Accessories	0.908343
guccigazelle.com	TRUE	0.830674	IAB-552	Style & Fashion	0.608816	IAB-566	Women's Clothing	0.830674
guccimyr.asia	TRUE	0.927781	IAB-552	Style & Fashion	0.754809	IAB-561	Women's Accessories	0.927781
guccistore.online	TRUE	0.853368	IAB-552	Style & Fashion	0.660082	IAB-561	Women's Accessories	0.853368
tk-gucci.com	TRUE	0.941071	IAB-552	Style & Fashion	0.676373	IAB-582	Men's Clothing	0.941071



The people behind these websites went through the trouble of publishing enough content to be categorized correctly. If they can't be publicly attributed to a legitimate brand, these properties

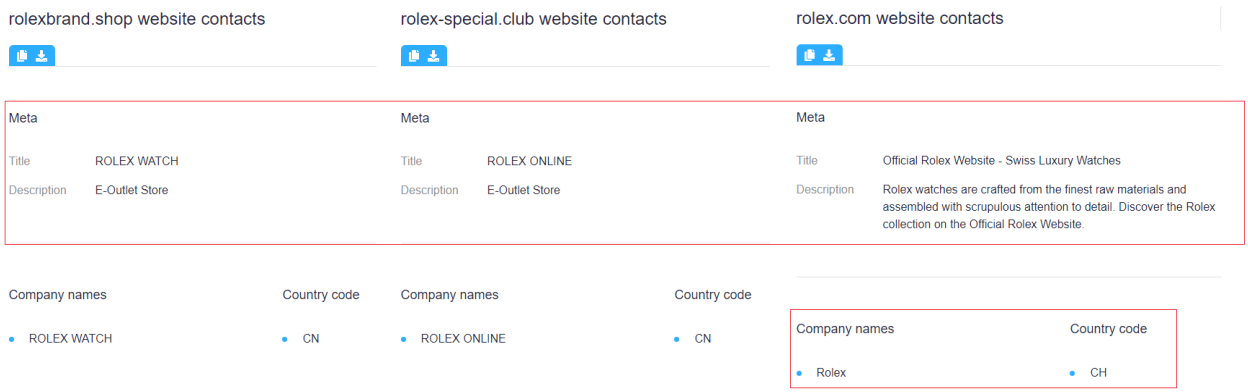
can possibly be selling counterfeit items or phishing unsuspecting users for their credit card information.

These infringing websites can be accorded more priority compared to inactive cybersquatting properties. Given a list of resolving Gucci-targeted domains below, security teams and investigators may focus first on those categorized as Style & Fashion websites compared to those with insufficient content.

domainName	websit	categor	categor	categories.0.tier1.name
guccipick1.com	TRUE	0.941626	IAB-186	Family and Relationships
gucci-8a.com	TRUE	1	CUS-5	Not enough content
gucci-jp.club	TRUE	1	CUS-5	Not enough content
gucci-jp.live	TRUE	1	CUS-5	Not enough content
gucci-jp.shop	TRUE	1	CUS-5	Not enough content
guccicon-jp.xyz	TRUE	1	CUS-5	Not enough content
guccigoshop.com	TRUE	1	CUS-5	Not enough content
gucciladyhandbags.c	TRUE	1	CUS-5	Not enough content
guccistore.shop	TRUE	1	CUS-5	Not enough content
guccitshirt.store	TRUE	1	CUS-5	Not enough content
lvguccibag.us	TRUE	1	CUS-5	Not enough content
guccishoes.co	TRUE	0.567209	IAB-441	Real Estate
guccibeltbag.com	TRUE	0.95651	IAB-552	Style & Fashion
guccibuy.ru	TRUE	0.908343	IAB-552	Style & Fashion
guccigazelle.com	TRUE	0.830674	IAB-552	Style & Fashion
guccimyr.asia	TRUE	0.927781	IAB-552	Style & Fashion
guccistore.online	TRUE	0.853368	IAB-552	Style & Fashion
tk-gucci.com	TRUE	0.941071	IAB-552	Style & Fashion
dropshopdigregoriog	TRUE	1	CUS-4	Unsupported language
lvguccibag.store	TRUE	1	CUS-4	Unsupported language

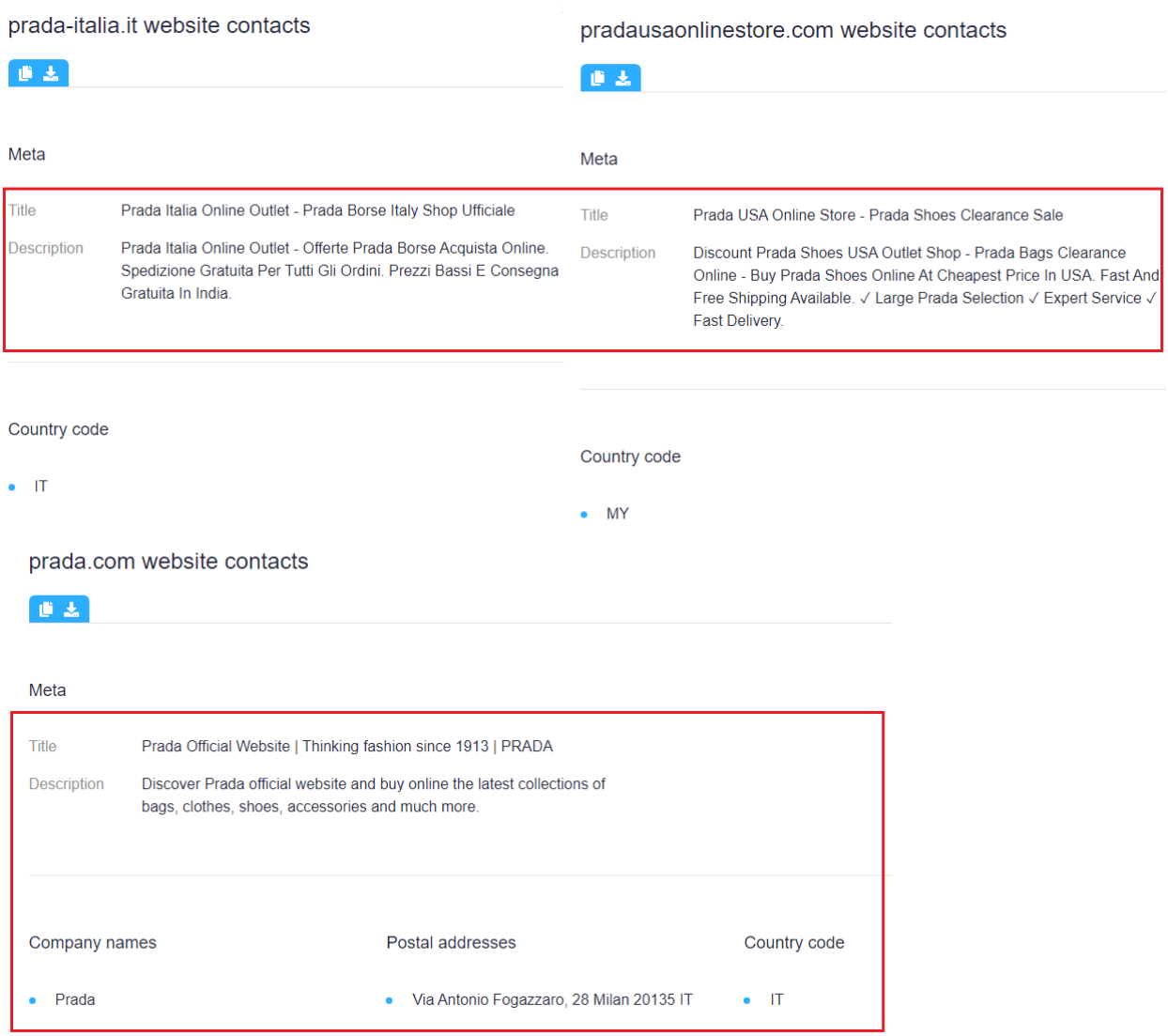
Website Contacts

Some live cybersquatting websites have meta titles and descriptions, which may be an effort to rank on search engines. Below are some Rolex cybersquatting domains with meta titles, descriptions, and contact information, alongside the official Rolex domain.



The cybersquatting domains differ in messaging compared to the official domain. While they describe themselves as outlet stores, rolex[.]com emphasizes that it is the official Rolex website. The company names and country codes also differ.

Some companies may also publish additional contact details, such as the postal address for prada[.]com.

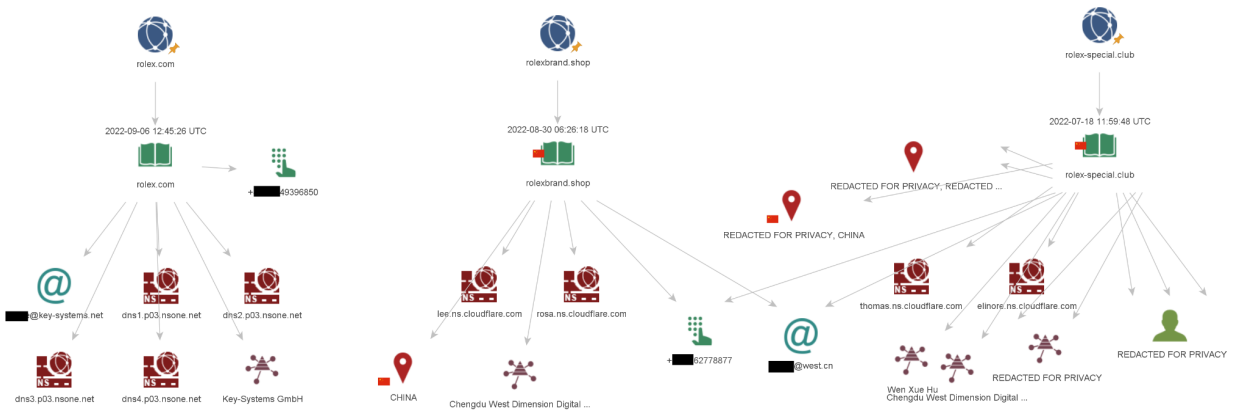


Any mismatched contact details and meta information should be noted as they can set infringing domains apart from legitimate ones.

WHOIS Registration Records

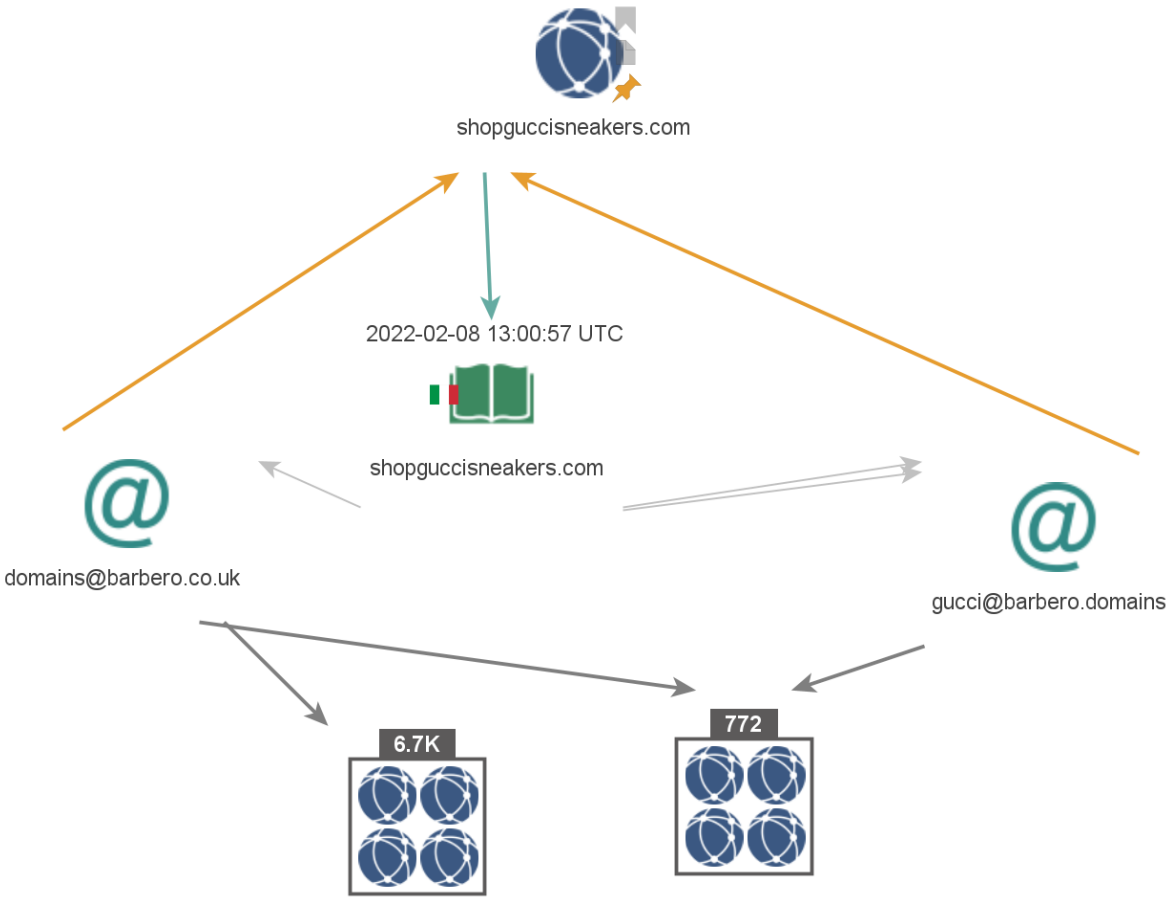
We can also check if these cybersquatting properties can be attributed to the imitated brands. We added domain entities on Maltego, the Rolex official domain and two cybersquatting resources, then ran the “To WHOIS Records [WhoisXML]” transform to extract the WHOIS records of the three domains.

The official Rolex domain is not connected to the other two domains, as visualized by the Maltego graph below. On the other hand, rolexbrand[.]shop and rolex-special[.]club share the same location and registrar details.



Evaluating Brand Protection Efforts

Current and historical WHOIS records can further be used to determine the actions taken by the legitimate brands to protect their organizations from online counterfeiting. We cite shopguccisneakers[.]com as an example. Its current WHOIS record indicates that it employs the services of a domain administrator called “Barbero & Associates.”



Based on the Maltego investigation, Barbero manages around 6,700 domains, 772 of which belong to Gucci.

The effort to seize cybersquatting domains is a never-ending pursuit. To put things in perspective, more than 10,000 domains containing “gucci” have been added throughout time. Only about 8% of them are managed by Barbero.

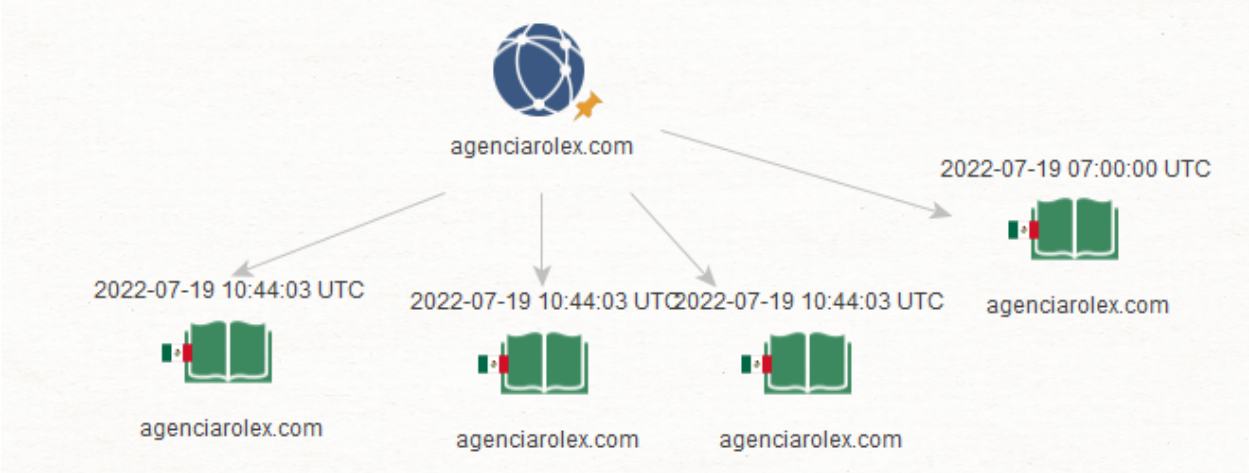
The volume added within a given period also adds to the threat. In the first half of 2022 alone, 1,216 domains containing “gucci” have been registered. Around 474 more have been added since the beginning of the second half of the year.

Providing Deeper Context

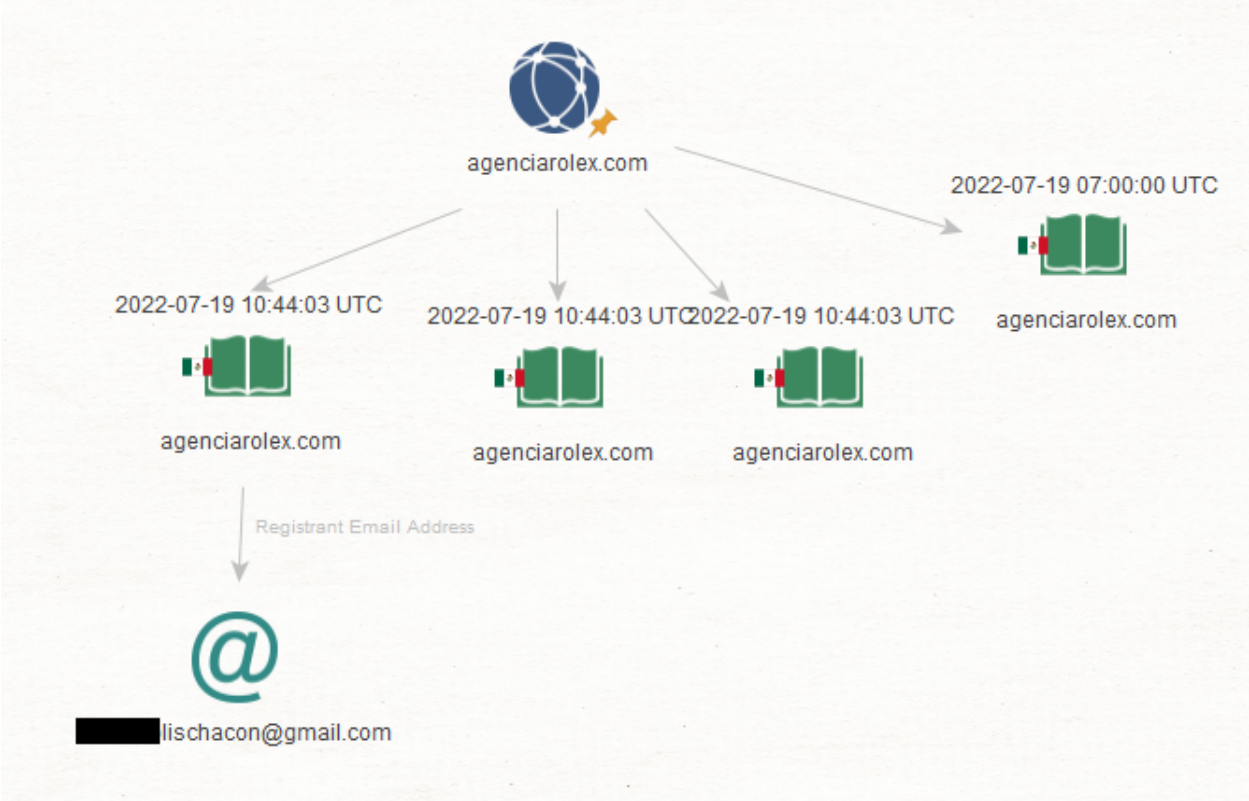
Learning more about the cybersquatting properties can help us understand threat actor behaviors and uncover more details that can bring us one step closer to catching them or mapping their infrastructure. Below are some ways Maltego and WhoisXML API can help contextualize counterfeiting domains.

Mapping Malicious Domain Infrastructures Using Historical WHOIS Data

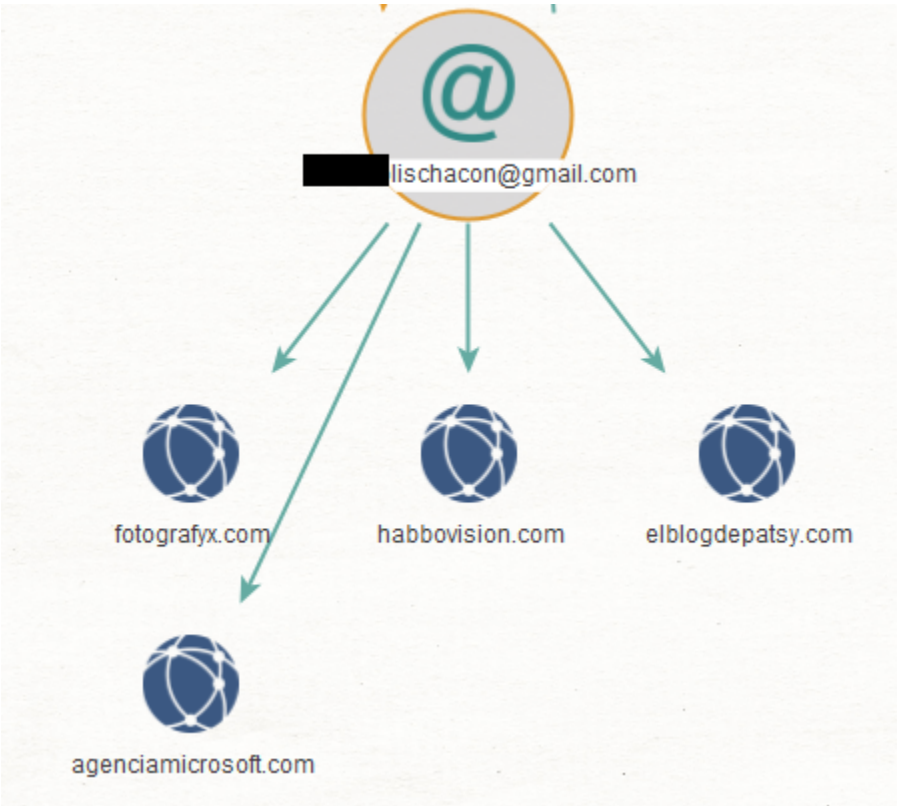
We start by adding a domain entity on Maltego and running the “To Historical WHOIS Records [WhoisXML]” transform. Four historical WHOIS records were found for agenciarolex[.]com.



In one of the records, we ran the “To Registrant Email” transform, revealing an unredacted email address.



We ran the “Historical Reverse WHOIS Search” transform to see other domains registered using the email address. This action returned four domain names.

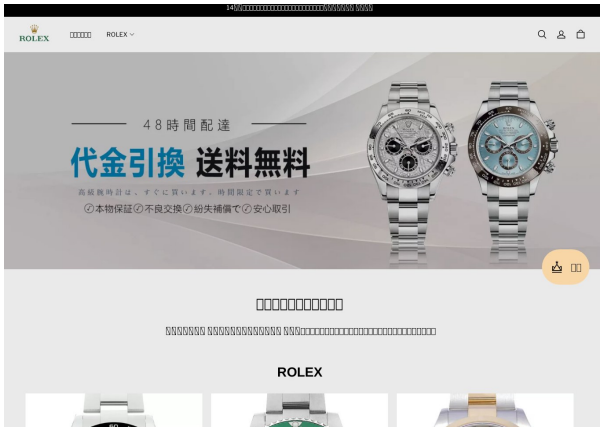


Determining the Malicious Usage of Counterfeiting Properties

We ran a bulk malware check on the luxury brand-themed cybersquatting domains added this year and found that several have been flagged as malicious. That indicates that not only are the infringing properties potential vehicles for selling counterfeit items, but they can also be used in phishing, malware distribution, scams, and other malicious activities.

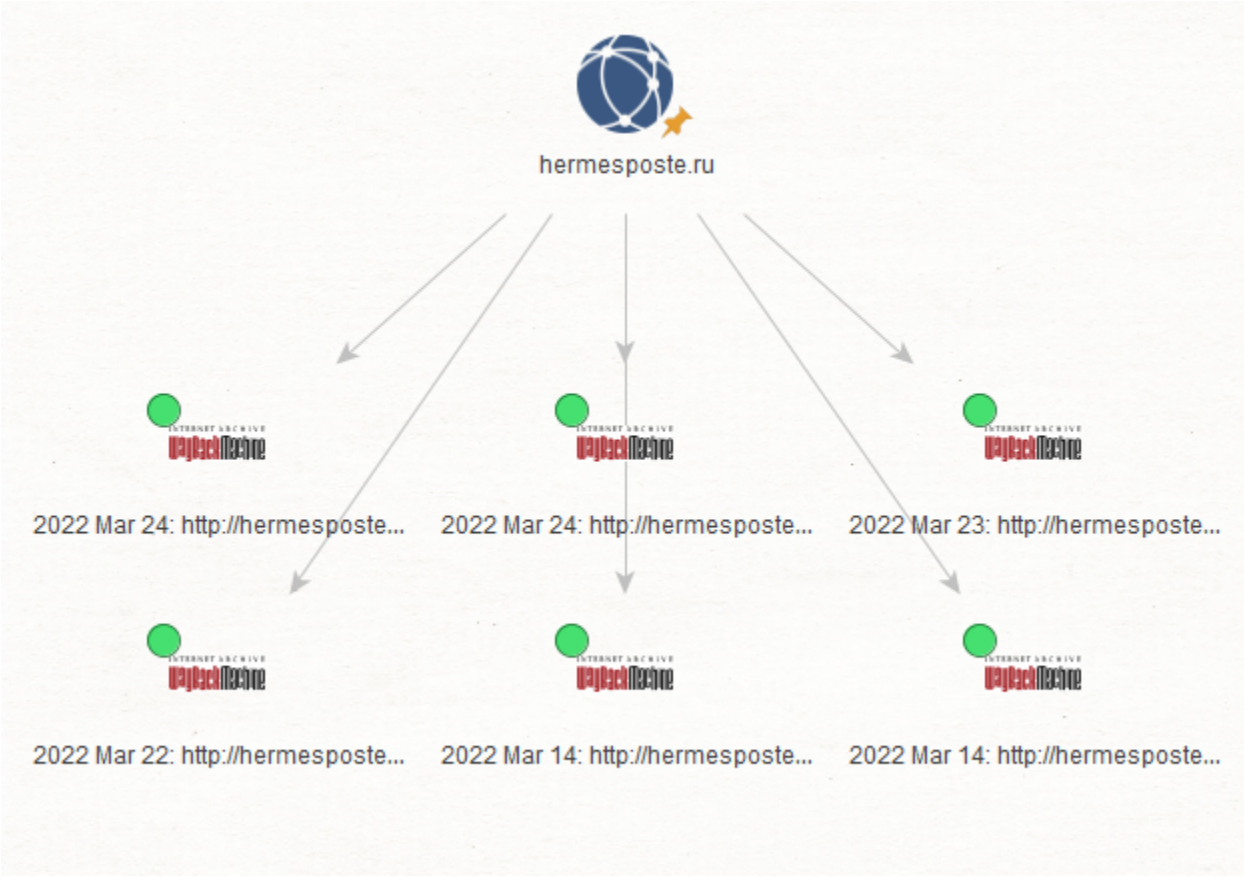
We also found that some of these properties continue to host content as of this writing. Below are a few examples.

Website screenshot of guccimyr[.]asia



Website screenshot of rolexsz[.]com

We can also see the types of content malicious properties hosted in the past using Maltego's "To Wayback Machine" transform. For hermesposte[.]com, the transform returned six snapshots.

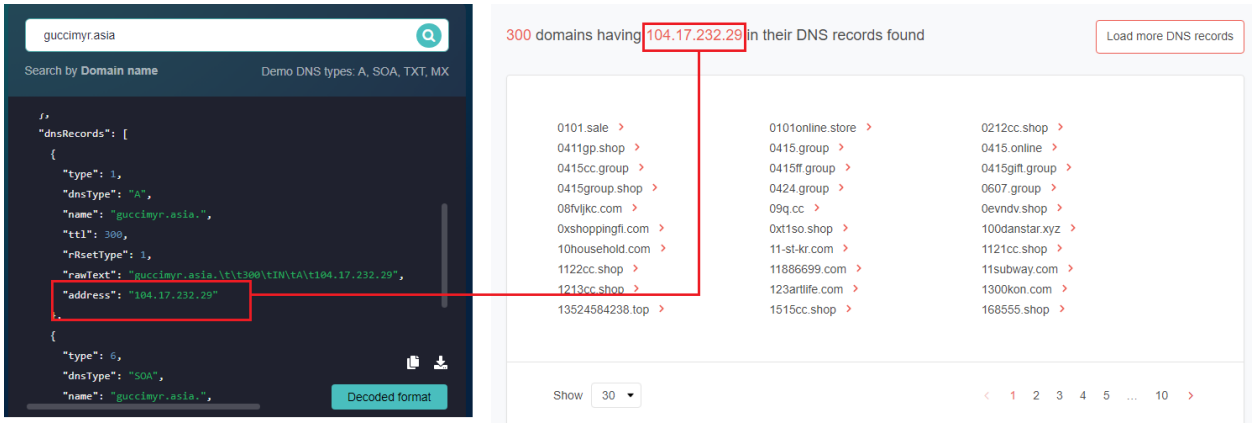


Threat Expansion

Now that we have identified malicious properties, we can examine DNS and WHOIS connections to find related domains that could be part of the malicious infrastructure.

Retrieving IP-Connected Properties

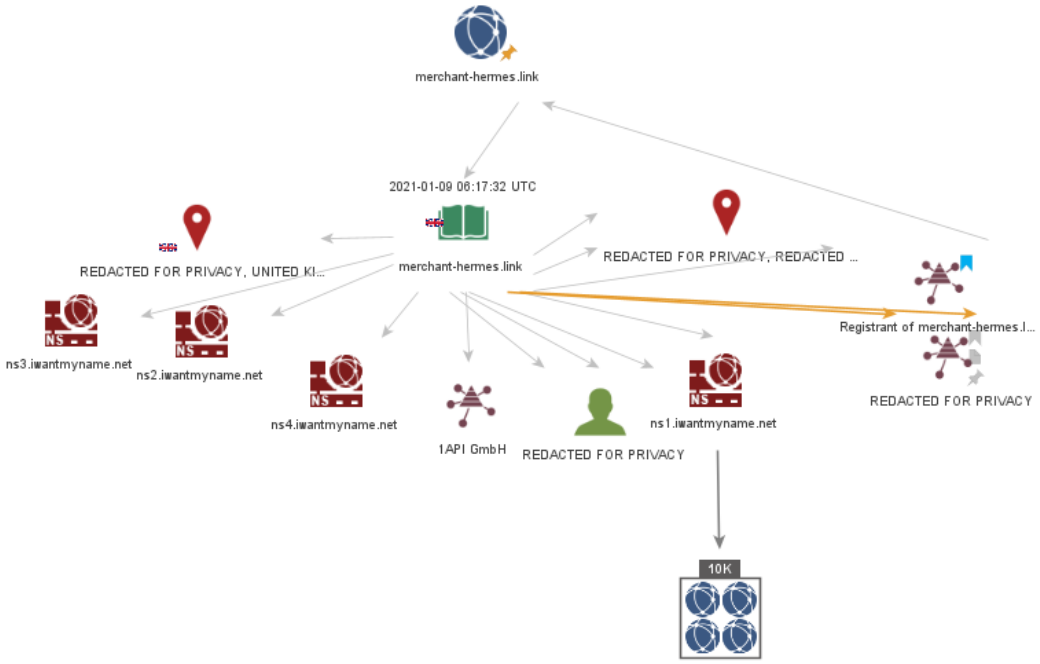
We can find more connected domains by looking at a malicious domain's IP resolutions. The DNS records of domain guccimyr[.]asia show that it resolved to 104[.]17[.]232[.]29. A reverse IP/DNS lookup on the IP address pointed to more domain names.



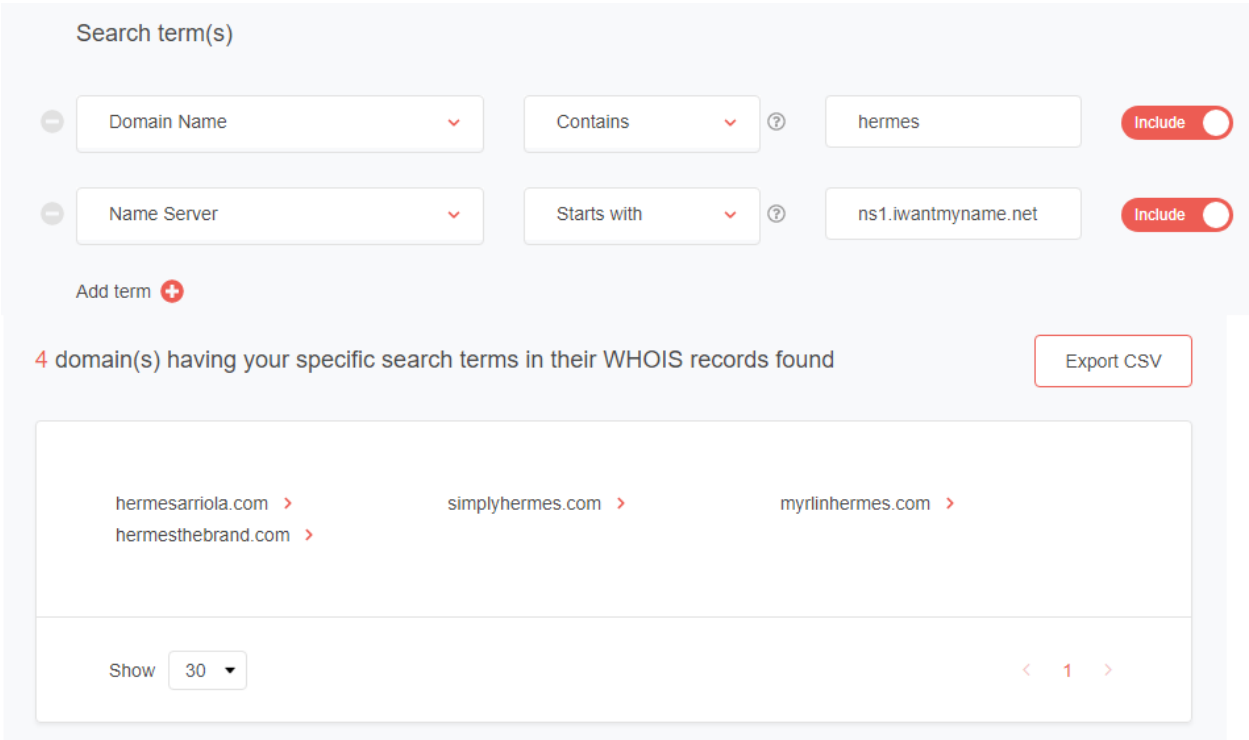
Looking for WHOIS-Connected Cyber Resources

We have previously illustrated how to use the "Historical Reverse WHOIS Search" transform on Maltego to retrieve all domains that share a registrant email address. What happens if WHOIS records are redacted?

The transform can also be used for nameservers or other WHOIS data points. To illustrate, we extracted the historical WHOIS records of malicious domain merchant-hermes[.]link and retrieved more than 10,000 domains sharing the same nameserver.



We can make the search more targeted and filtered by combining search terms on DRS. For example, we can look for Hermes cybersquatting domains that use the same nameserver as the malicious domain. We found four additional domains.



—

Throughout this investigation, we demonstrated how investigators could probe counterfeiting, beginning with determining how huge the problem is for a specific company or industry, among other threats. The investigation can be deepened using DNS, WHOIS, and IP intelligence to ensure proper threat prioritization and remediation. Moreover, additional connected domains can be uncovered by scrutinizing IP and WHOIS connections.

Are you interested in the data presented in this research? Contact us for commercial inquiries or check eligibility to join our Research and Media Collaborations program.