June 2022: Monkeypox Outbreak, Never-Ending Fashion Brand Counterfeiting, and Online Shopping Dangers

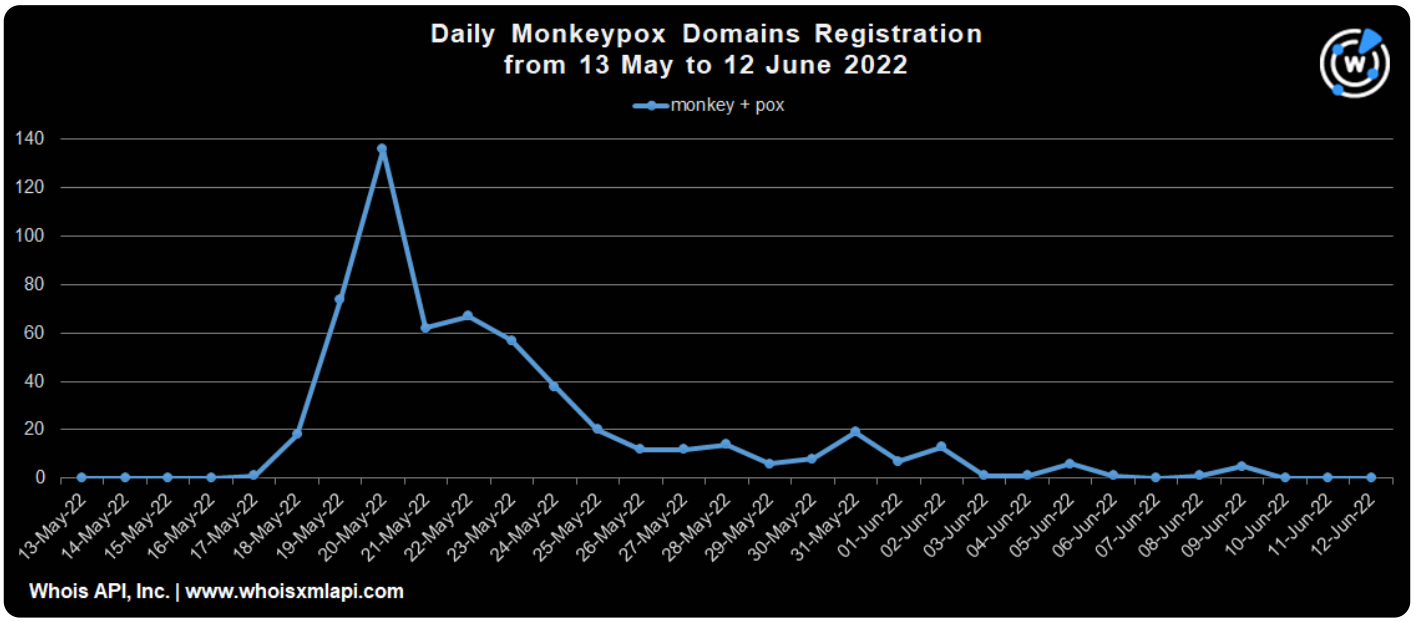
Posted on June 24, 2022

We detected noteworthy domain registration and Domain Name System (DNS) activity connected to some of the current events in May 2022, along with age-old targets of cybercriminal activities. We provided an overview for three of these items below. You may download relevant threat reports where available.

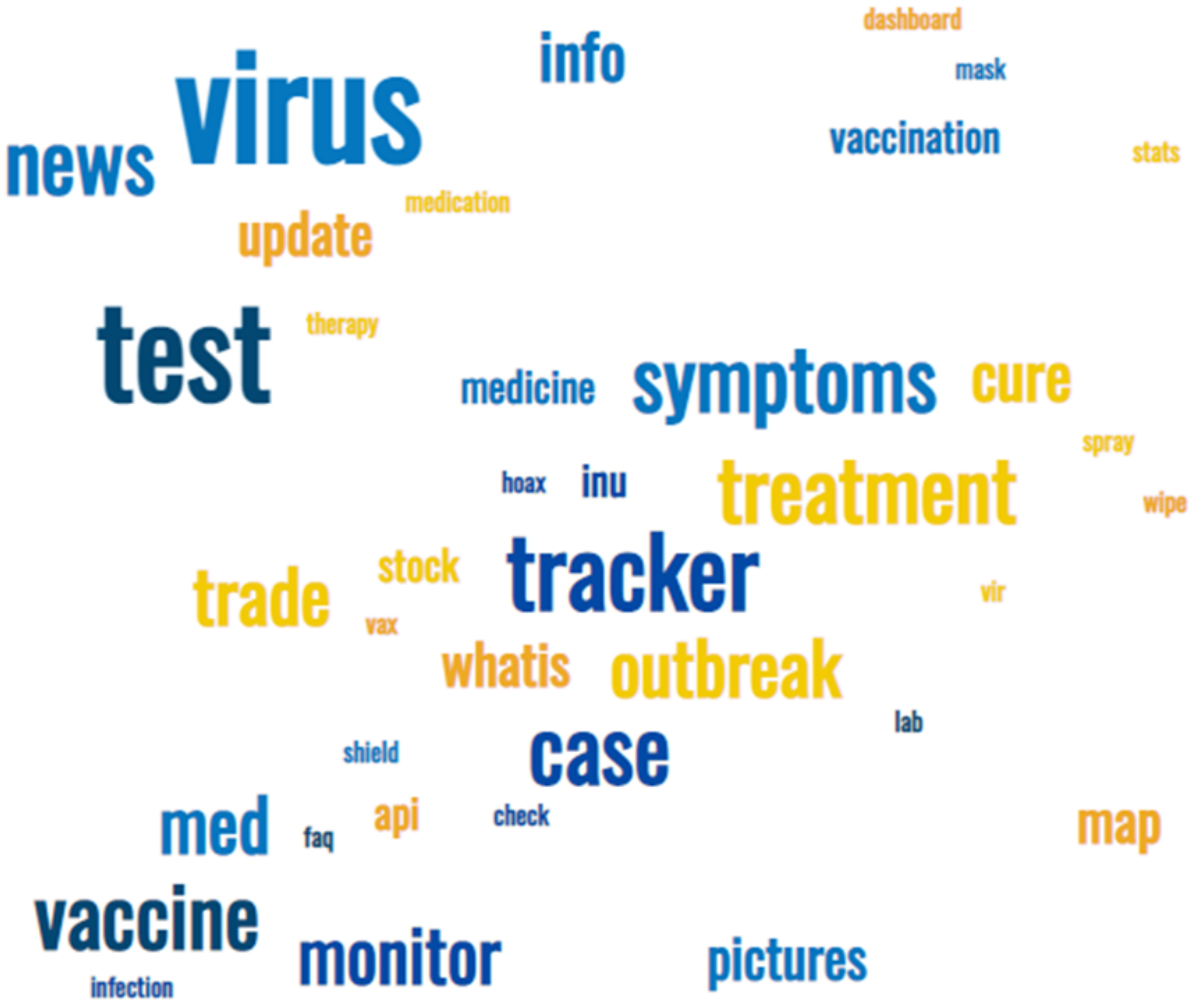
1. Monkeypox Outbreak

Confirmed cases of monkeypox were reported beginning on 13 May 2022. Five days later, the Massachusetts Department of Public Health identified the first case of monkeypox in the U.S. We decided to see how this health-related event possibly affected the DNS. While it doesn't seem as large-scale as the Coronavirus-themed domain registrations, there is still significant traction.

Within a month since the outbreak was announced, we tallied more than 500 domain names bearing the text string “monkeypox.” The chart below shows the daily registration trend. From no significant movement between 12–17 May 2022, domain registration suddenly increased the day the first U.S. case was reported. It peaked on the 20th and started dwindling on the 29th.



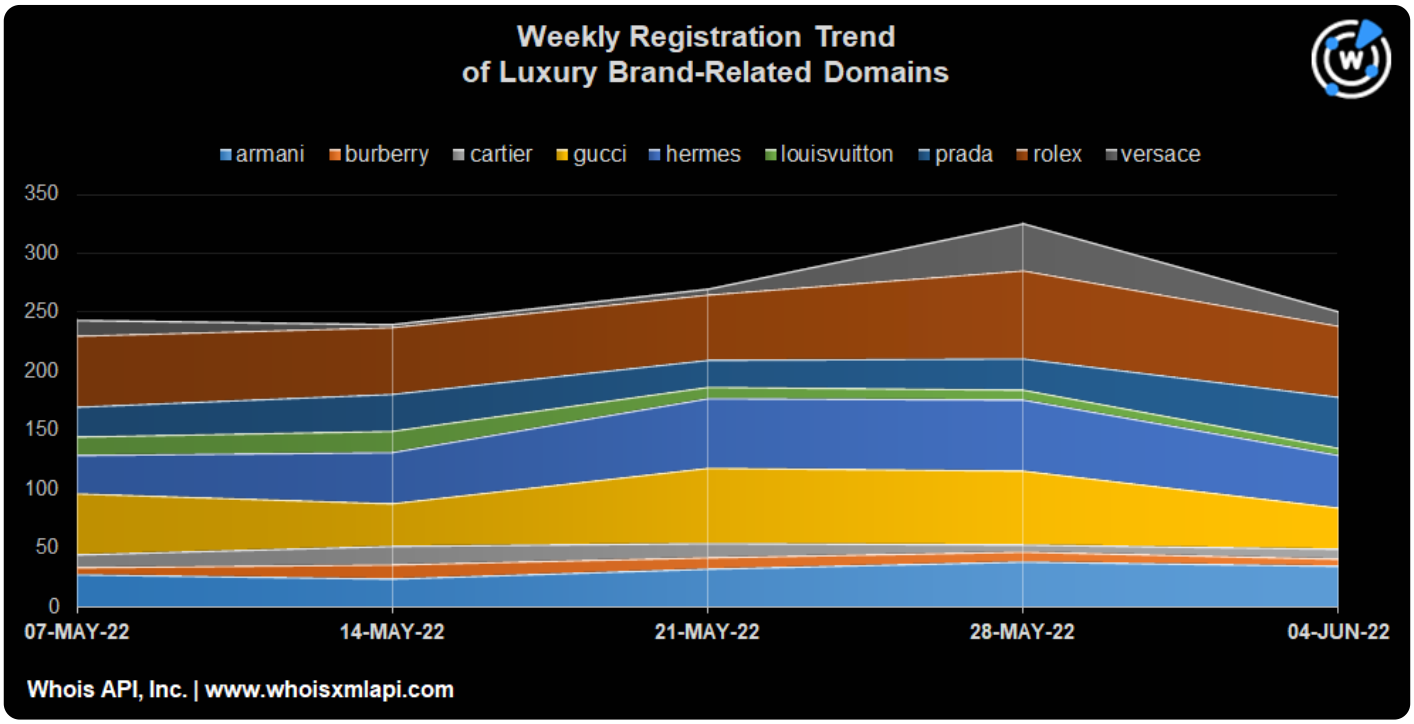
Among the most common terms that appeared alongside the Monkeypox domains are “virus,” “symptoms,” “test,” “tracker,” and “treatment.” These and other text strings can be seen in the word cloud below.



2. Nonstop Counterfeiting of Fashion Brands

As one of the favorite targets of counterfeiters and brand abusers, luxury brands are targeted all year round. In fact, we uncovered thousands of cybersquatting domains targeting Rolex, Hermes, Gucci, Prada, Armani, Louis Vuitton, Cartier, Versace, and Burberry added in the first quarter of 2022. We analyzed these properties and presented our findings at Europol's 13th Operation In Our Sites (IOS) Conference.

DNS trends relevant to these luxury brands remain outstanding, with 1,331 domains registered from 1 May to 4 June 2022. Registration peaked on the week ending 28 May 2022, as seen in the chart below.



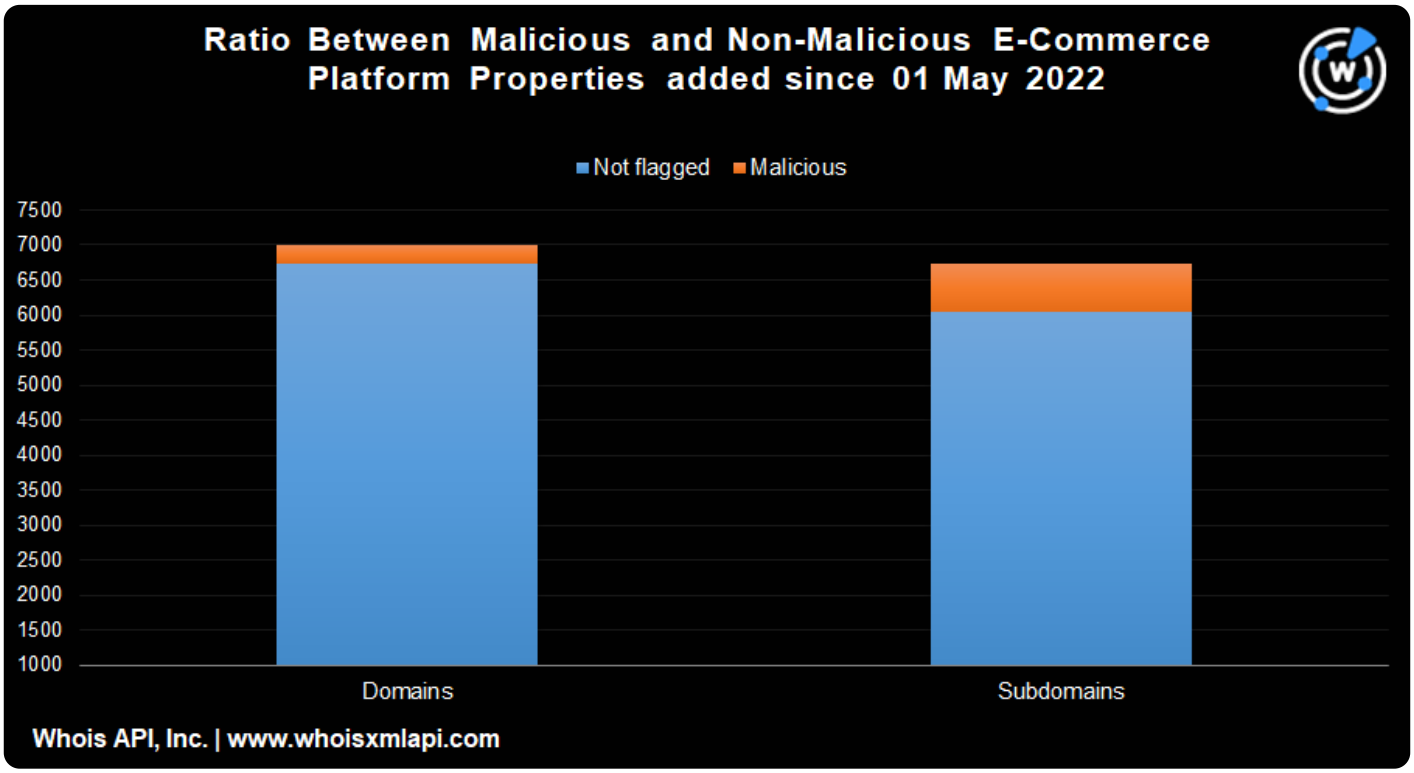
Common text strings appearing together with the luxury brand names were noted. The strings “official,” “mall,” and “outlet” may improve the legitimacy of the domains in the eyes of regular Internet users. On the other hand, “japan” and “uk” may mean that some of the domains are geographically targeted. There's also the use of urgency-inducing keywords, such as “sale,” “discount,” and “coupons,” which in some cases may raise concerns.

3. Increasing Online Shopping Dangers

We also recently looked beyond luxury brands and into the much broader spectrum of online

shopping in our threat report, Online Shopping Danger? 13K+ Cybersquatting Properties of Top E-Commerce Sites Discovered. The study focused on the digital footprint of top e-commerce platforms AliExpress, Amazon, Avito, eBay, Etsy, Rakuten, and Walmart.

About 7% of the 13,737 new domains and subdomains related to these companies have already been flagged as malicious. Notably, there are more dangerous subdomains than domains, with threat actors exploiting legitimate root domains, such as duckdns[.]org. The chart below shows the ratio between the domains and subdomains reported as malicious and those that aren't.



The study points out that cybersquatting subdomains and domains pose a threat. Even those that haven't been flagged as malicious are potentially dangerous since they host login pages made to look like the imitated websites.

Some of the recurring text strings in the digital properties we uncovered are also used in phishing URLs. These include "login," "account," "services," "support," and "notification." The word cloud below shows these and other text strings.

One term that stood out is “kleinanzeigen,” the German equivalent of “classified ads.” It repeatedly appeared alongside eBay-targeted domains. Using this German text string, we uncovered more suspicious domains.

For more information about the above-mentioned domain registration events and analyses or enterprise commercial inquiry, please do not hesitate to contact us.