Q2 2022: Seasonal Domain Registrations, Persistent Online Shopping Dangers, Burgeoning NFT Cybersquatting, and the Russia-Ukraine War

Posted on July 18, 2022

We rounded up some of the most significant events and trends in the second quarter of 2022 that we observed coinciding with domain registration and DNS activities. An overview of these highlights is presented below.

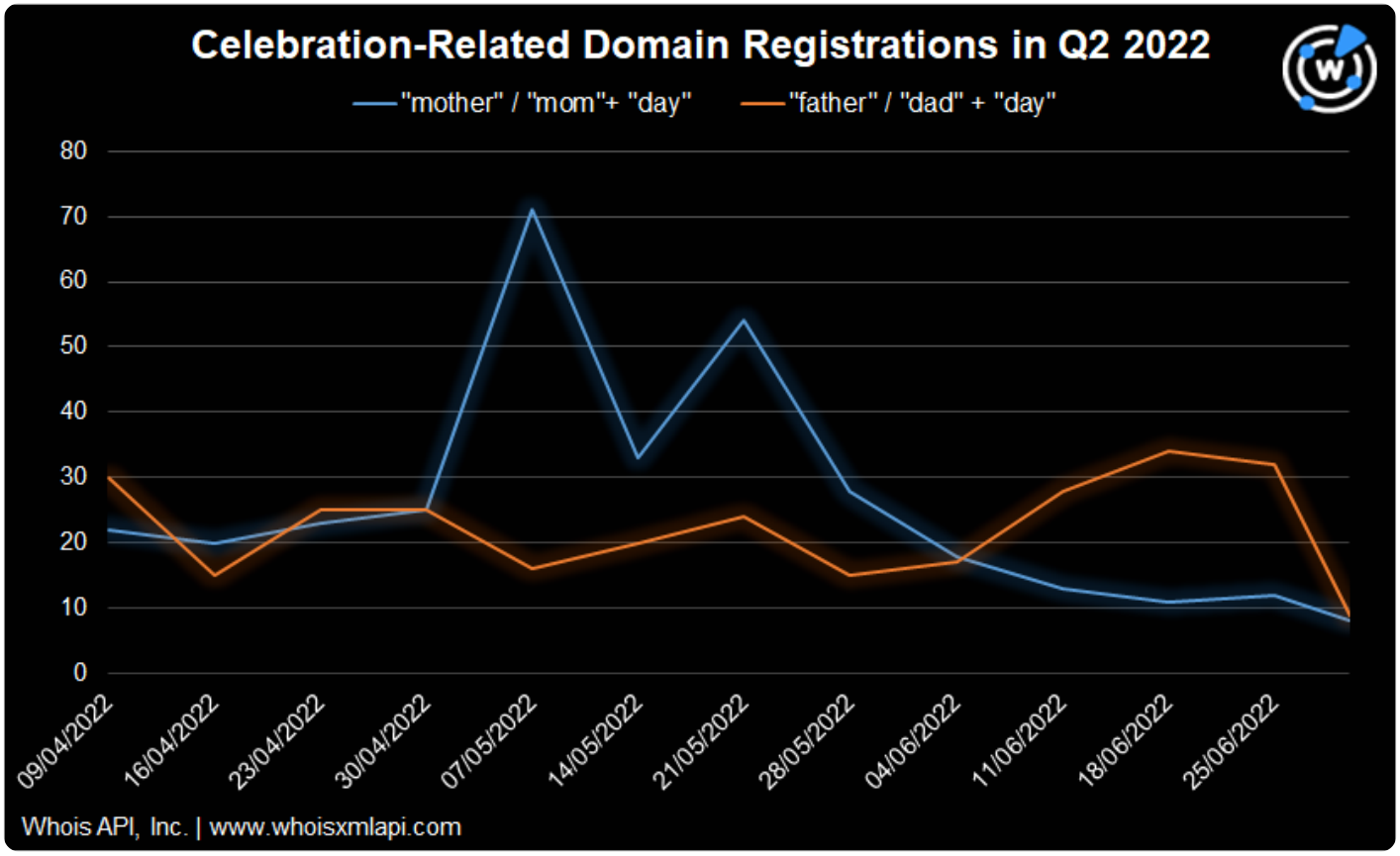
Seasonal Domain Registration Trends

In our May DNS Threat Highlights, we reported a spike in domain registrations relevant to Mother's Day in the weeks before the event. We also published a related report, where we discovered more than 1,100 Mother's Day properties and detected several as malicious.

Father's Day also led to some significant activities. Our dedicated threat report discovered 1,700+ domains and subdomains related to the event, and quite a few turned out to be malicious.

These celebration-related DNS trends are captured in the chart below. From 1 April to 30 June 2022, hundreds of domains possibly related to the two events were added. The registration volume of Mother's Day-related domains peaked a week before the Mother's Day week ending 14 May 2022, then spiked again the week after the event. After May, the registrations dwindled.

Father's Day-related domains also followed an upward registration trend in the week prior to 19 June 2022. Relevant domain registrations went up and then declined after the event.

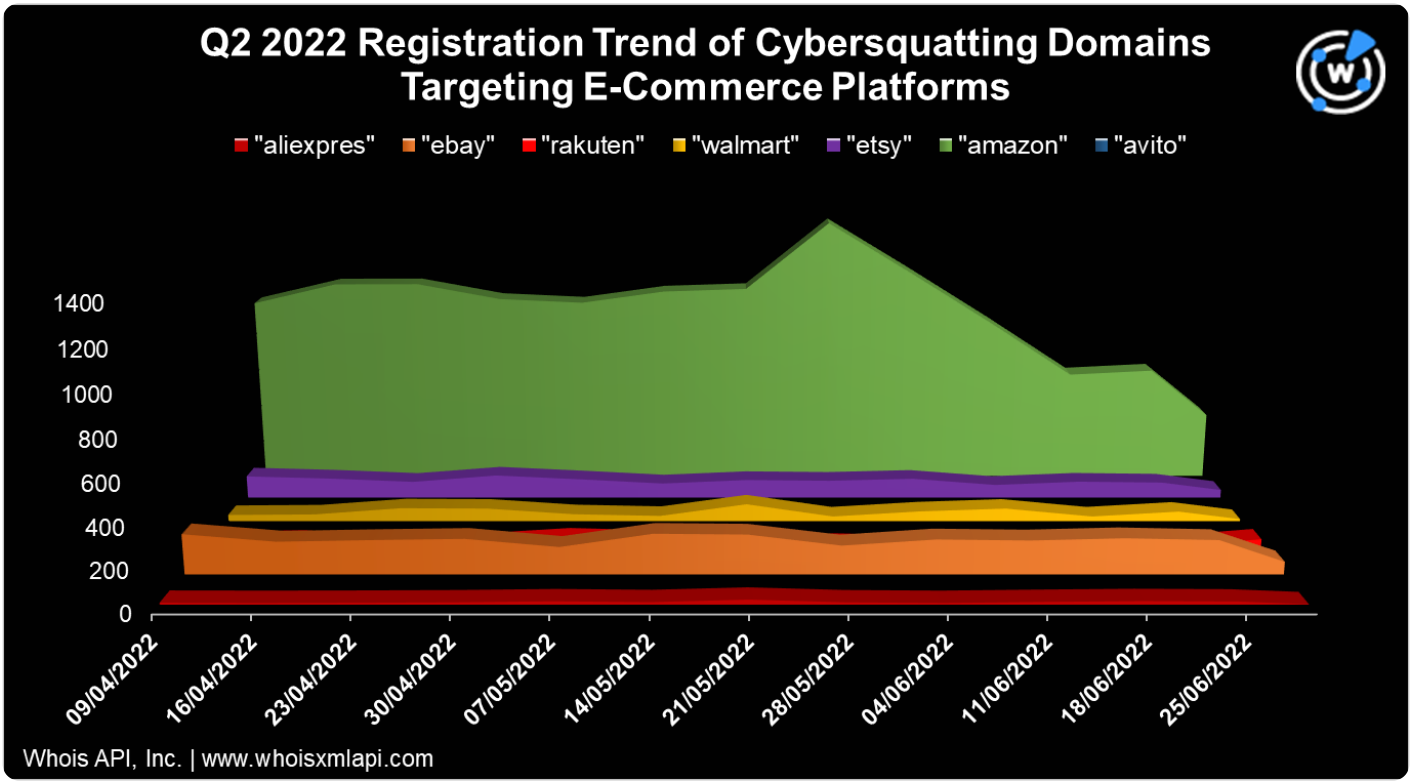


Some of the most common text strings that appeared in the event-related domains are “ideas,” “gift,” and “info.” These and other words are depicted in the word cloud below.

Online Shopping Dangers Amplified by Cybersquatting Domains

Another significant DNS activity was the continuous stream of cybersquatting properties targeting top e-commerce sites, such as AliExpress, Amazon, Etsy, and Walmart. More than 13,000 properties were added in May. Expanding this to include the whole second quarter of 2022, we discovered almost 17,000 properties using the names of seven of the top online shopping platforms.

The domain registration distribution and weekly trends are reflected in the chart below. While there were more Amazon look-alike domains, the cybersquatting activities increased around May and dwindled in the final days of June.

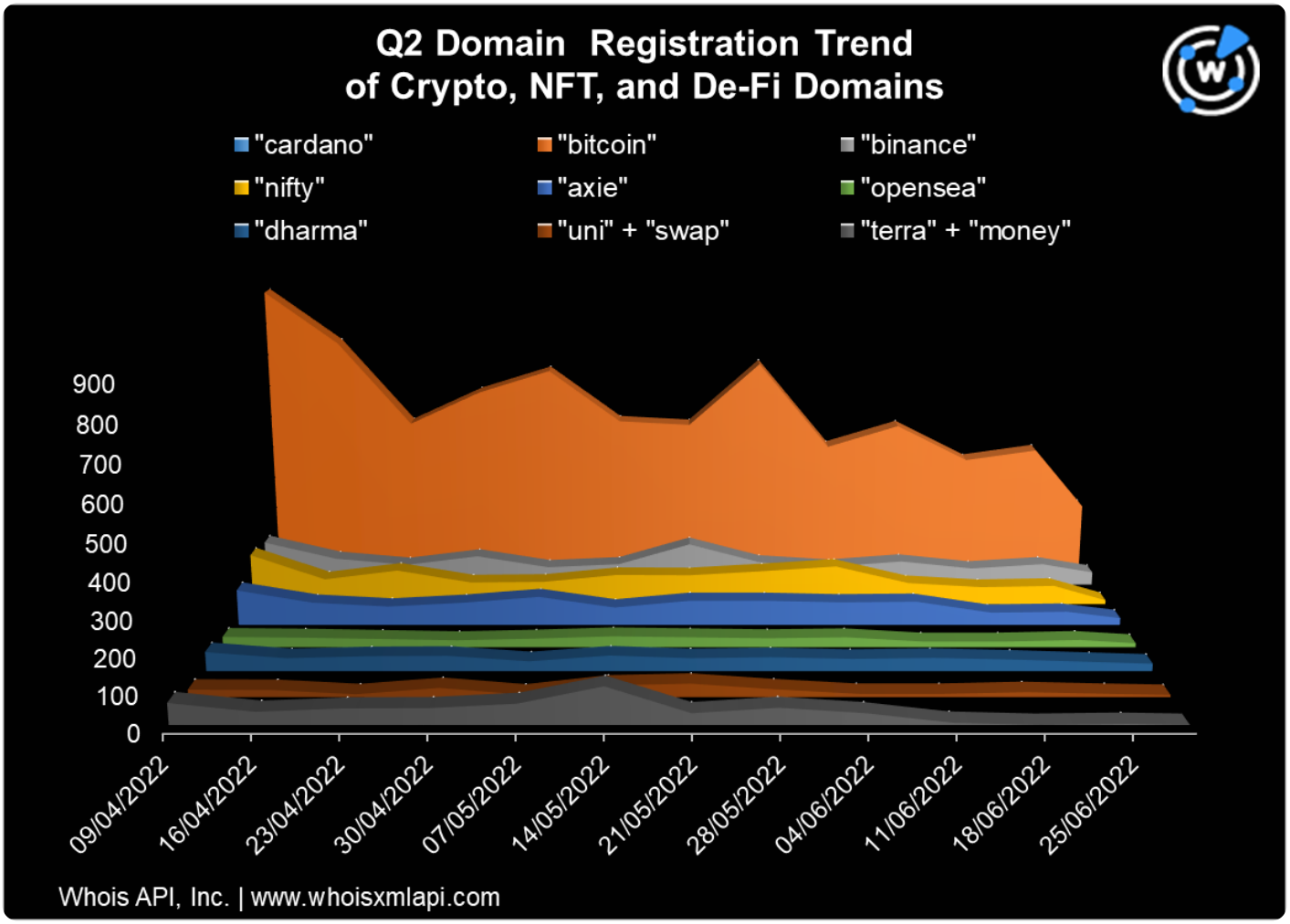


Most of the words that appeared alongside the company names were online shopping-related. Examples include “shop,” “mall,” “products,” “payment,” and “sale.”

Cryptocurrency and NFT-Related Domain Registration

Early this year, we discovered more than 65,000 domains and subdomains related to non-fungible tokens (NFTs) and analyzed them. We dived into the DNS again in our May newsletter to see how NFT-related domain registrations were going and found more than 1,600 properties.

For this Q2 2022 report, we expanded our study to include cryptocurrencies and decentralized finance platforms, yielding 11,461 properties. We plotted the trend in the chart below, showing that bitcoin-related domains accounted for most of the registrations.

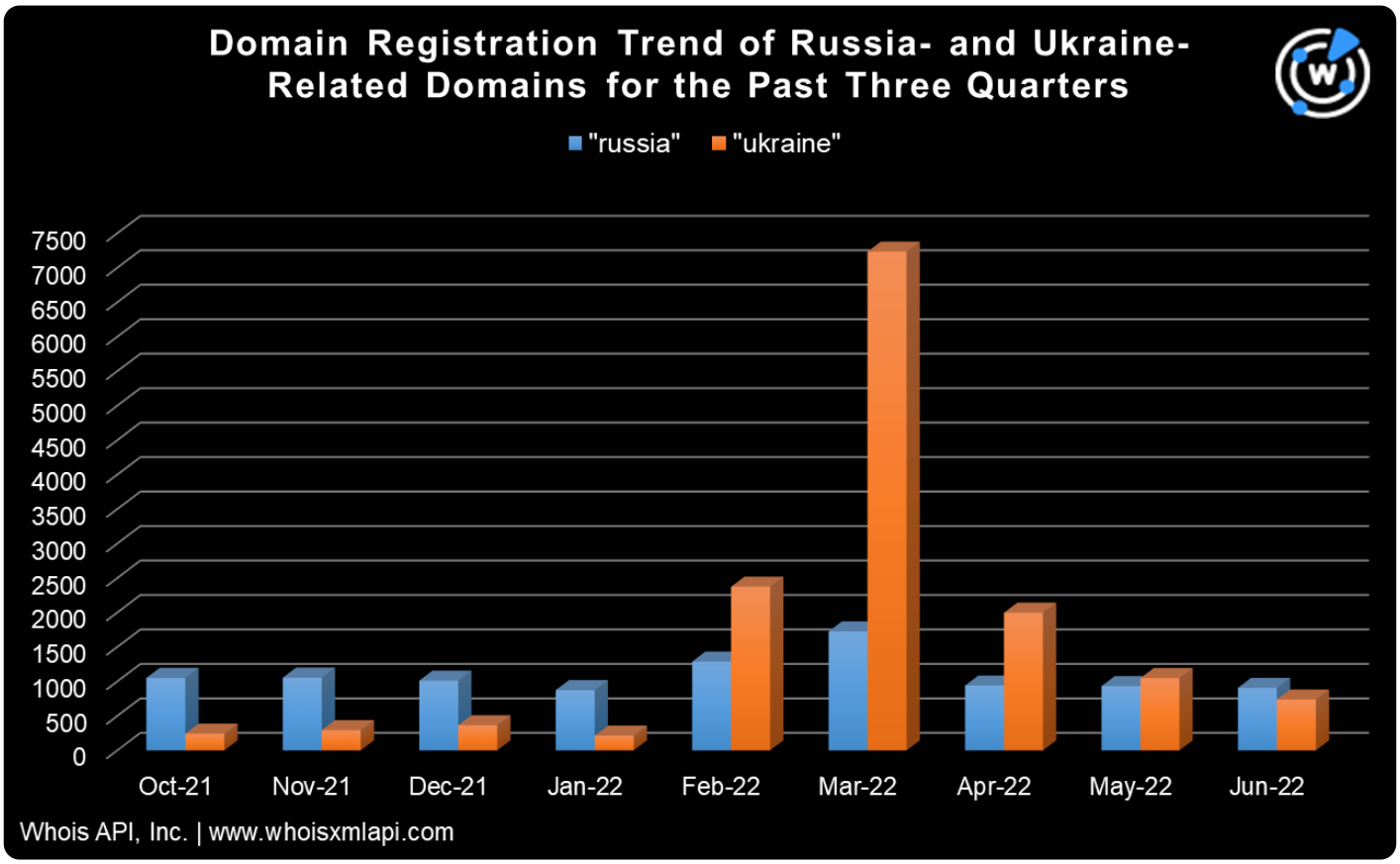


Aside from the names of top cryptocurrencies, NFTs, and De-Fi platforms, most of the strings used in the domains included “app,” “wallet,” “decode,” “mining,” and “exchange.”

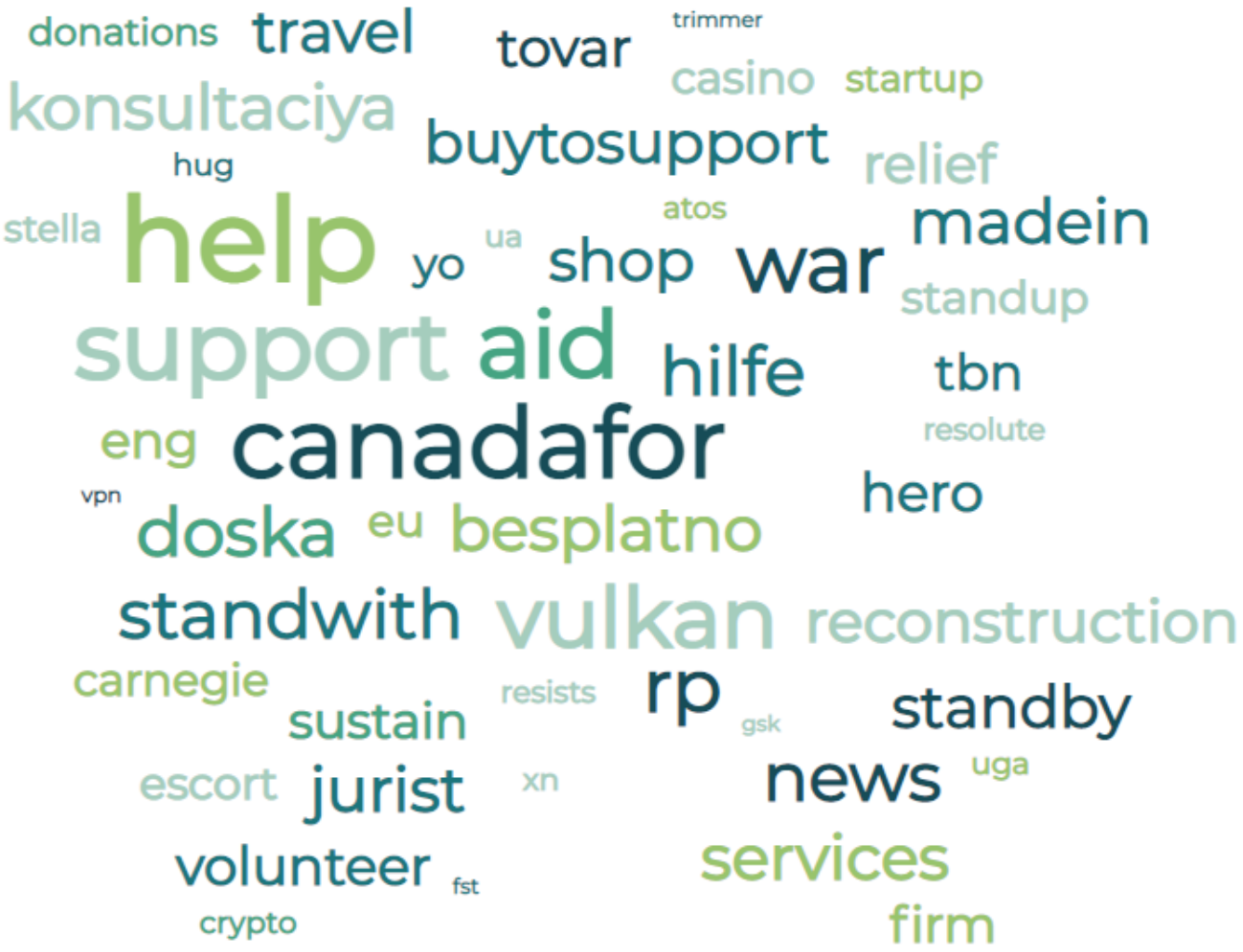
Digital Spillovers of the Russia-Ukraine War

Although the armed conflict between Russia and Ukraine began in February 2022, related domain registration activities continued to surpass pre-war levels. From the fourth quarter of 2021 to January 2022, only a little over 1,000 domains containing the names of the two countries were added per month.

But within a week of the war, we observed more than 3,900 new domains, which we analyzed in this threat report. In Q2 2022, relevant domain registrations remained relatively high, notably for domains containing “Ukraine.” The chart below shows the monthly trends from October 2021 to June 2022.



The strings that were repeatedly used in the domains included “help,” “relief,” “volunteer,” “standwith,” and “support.” These weren’t very different from the text strings used in the domains added in March. More words can be seen in the word cloud below.



—

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