

April 2022: Digital Spillovers of War, Oscars Slapping Fiasco, and Tax Season Frenzy

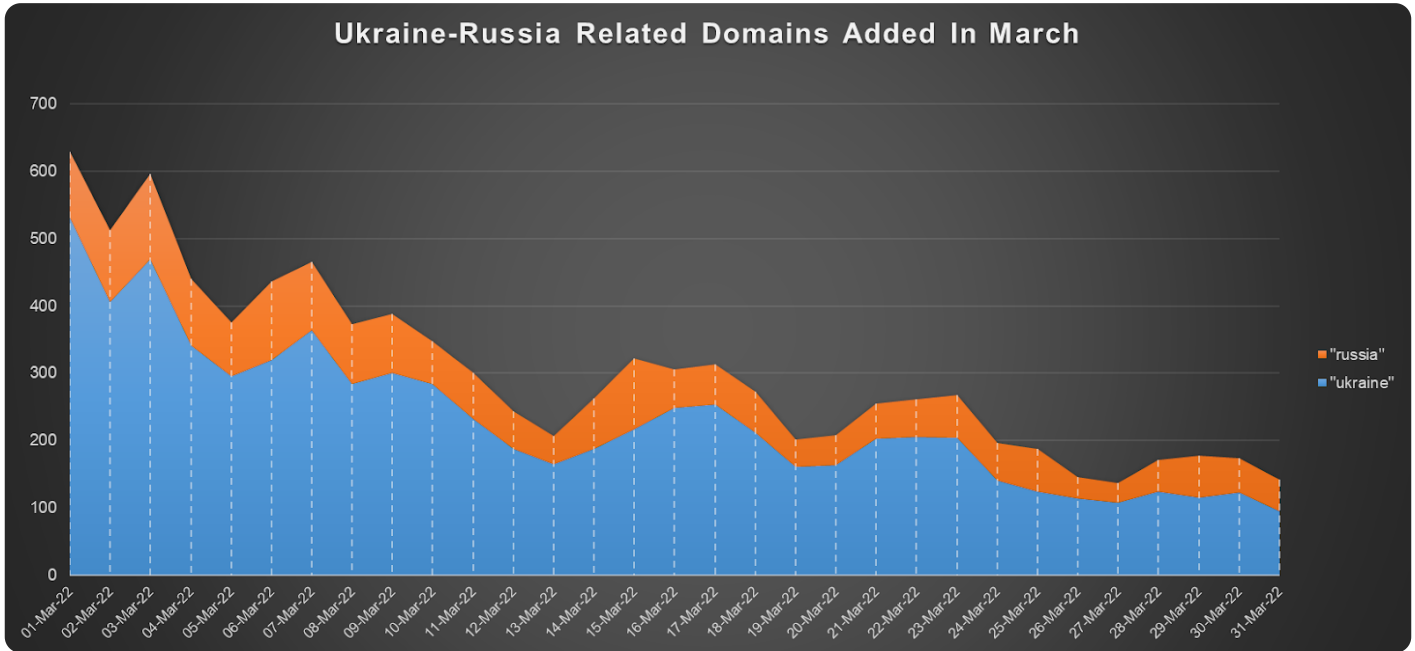
Posted on April 21, 2022

Here are some of the top events in March 2022 for which we detected significant connected domain and DNS activity. See below for an overview, and feel free to download the dedicated threat reports where available.

1. Digital Spillovers of the Russia-Ukraine War

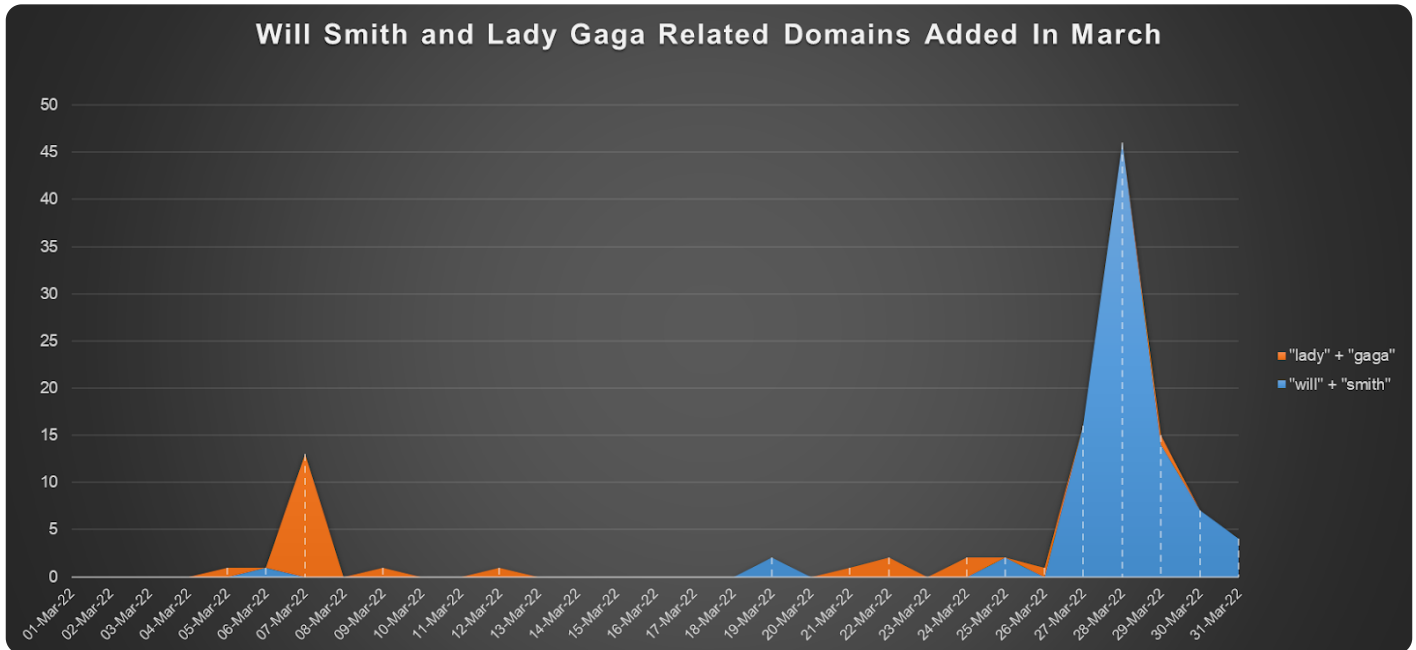
We started monitoring the DNS for domains and subdomains related to the Russia-Ukraine war on 24 February 2022. In the two weeks that followed, we found close to 4,000 newly registered domains (NRDs), several of which were found active and have been flagged as malicious. Details of our findings and analysis can be found and downloaded from our report [Digital Spillovers of Russia's Invasion of Ukraine](#).

By the end of March, this number more than doubled, with 9,316 potentially harmful domains added on 1–31 March 2022 and containing “Ukraine” and “Russia” as strings.



The most common text strings used in the domains are shown in the word cloud below.

Chris Rock incident, related domain registrations started peaking on the day the Oscars was broadcast. You can see this from the chart below.



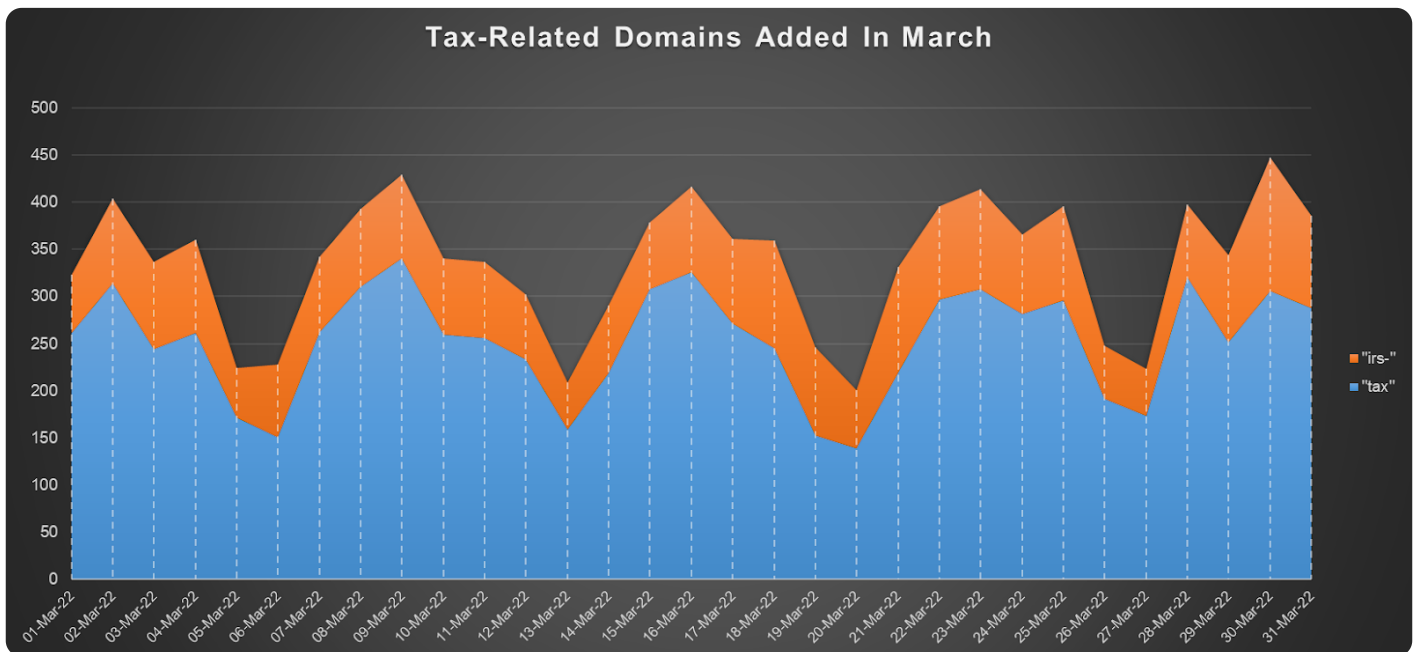
Other text strings used alongside “Lady Gaga” and “Will Smith” can be seen in the following word cloud.



3. Tax Season Frenzy

Tax- and Internal Revenue Service (IRS)-related domains can be vehicles for phishing, tax fraud, and other criminal activities. In fact, 12% of the tax-related resources added from 1 January to 23 March 2022 were already flagged as malicious at the time of analysis. Find out more about these resources and other relevant data points and analysis from our report [Be Wary of Bogus Web Properties This Tax Season](#).

In particular, 10,427 domains containing the text strings “tax” and “IRS” were registered within the month of March.



The text strings that repeatedly appeared alongside “tax” and “IRS” can be seen below.

