Domain and IP Intelligence: Tracking the Spike in Coronavirus-Themed Domain Registrations

Posted on May 14, 2020

The first cases of COVID-19 infection came to the fore in December 2019. Five months later, the world is still reeling from the disease. The numbers are overwhelming. According to the Johns Hopkins Coronavirus Resource Center, more than 4 million people worldwide have gotten infected, over 290,000 of whom have died from the disease at the time of writing. And dismayingly, these numbers are still expected to rise.

In response, governments all over the world have imposed varying degrees of social distancing strategies. People are urged to stay home, schools are closed, mass transportation in many countries is suspended, and countless small businesses have ceased operations. For the majority, one consolation of being in home quarantine is their access to the Internet and, therefore, the world. But even on the Web, people are not safe from the virus.

Using our IP and domain intelligence, we detected an increasing trend toward coronavirus-themed domain bulk registrations—some of which may have to do with the proliferation of coronavirus-themed cybercrimes taking advantage of the pandemic. Let us show you our key findings.

The Data: Coronavirus-Themed Domains

With the help of IP and domain intelligence that powers our tools such as Domain Monitor, Brand Monitor, and WHOIS Lookup, we tracked the number of domain registrations for coronavirus-themed domains. In particular, we looked for domain names that contain either of the following substrings:

- oronavir
- covid

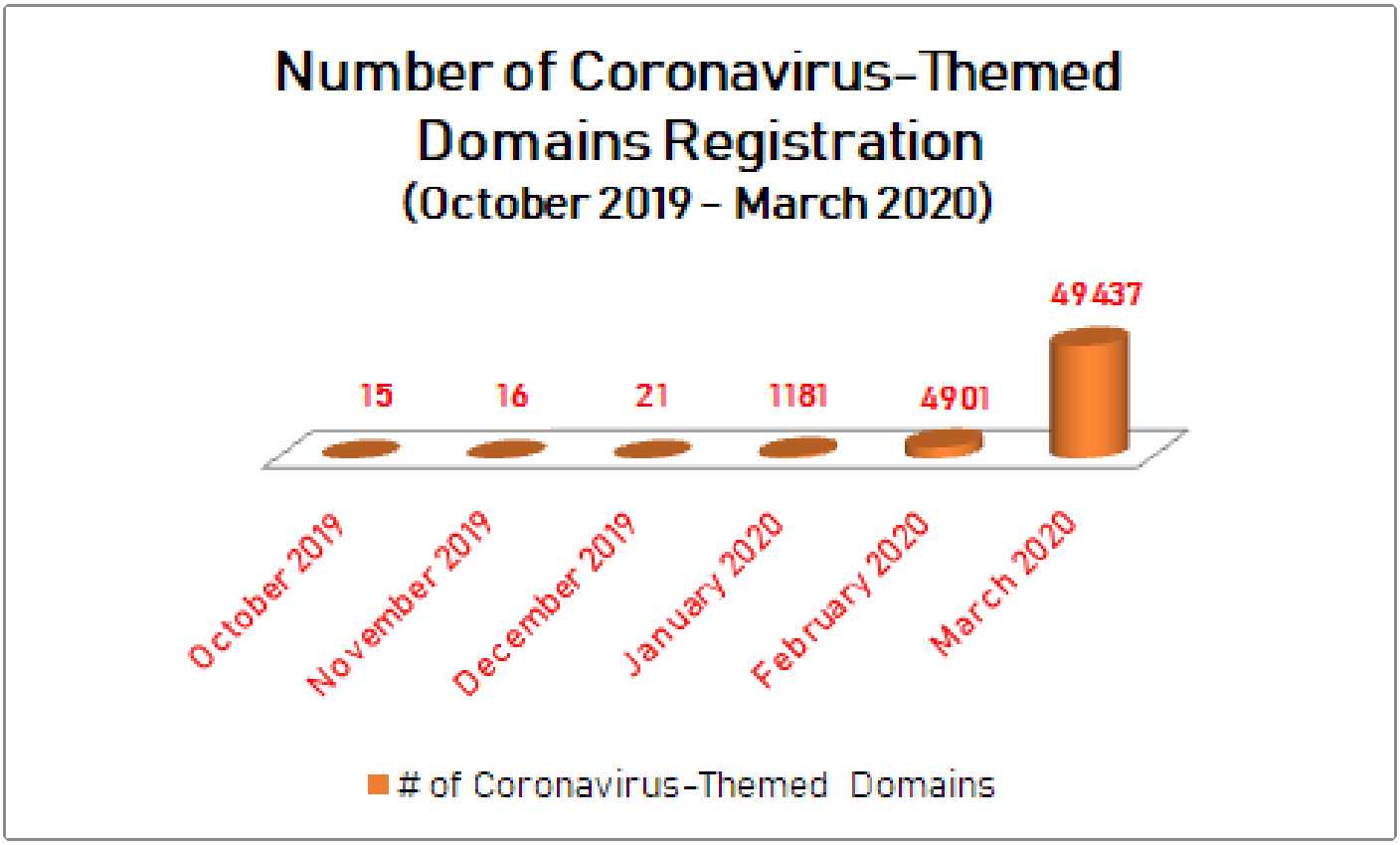
We started looking at the data from October 2019 and found 15 coronavirus-themed domains. The figure did not change much in November and December, with 16 and 21 domain names respectively added. While these domains contained either of the substrings, they do not seem related to the disease. After all, it wasn't until 11 March 2020 that the World Health Organization (WHO) declared the coronavirus a pandemic.

Below are a few examples of the domain names picked up from October to December 2019:

- marcovideochat[.]com
- nicovideo[.]news
- ecovide-environnement-lpa[.]fr
- pycovid[.]ru
- tourmexicovideos[.]com
- covideibriganti[.]com
- ricovidas[.]net
- encoviddy[.]com
- istitutomedicovidimura[.]com
- ecovida[.]website

It’s interesting to note that these are unrelated to the COVID-19 virus (unlike others which we will discuss later).

In January 2020, we saw a significant increase in the number of coronavirus-themed domain names. Specifically, 1,181 domain names contained the substrings “oronavir” or “covid.” That’s a glaring 5,523.81% increase from December 2019.



By February, the number rose to 4,901 (indicating a 314.99% increase from January). And in March, the volume of coronavirus-themed domain registrations went up to 49,437 (a 908.71% rise from the previous month). To give you a glimpse of what these domain names look like, here are some of those registered in March:

- autoimmunecovid[.]org
- autotestcovid19[.]com
- bostoncovidcleanup[.]com
- cdc-covid19[.]com

- cooronavirusnewsnow[.]com
- copingthroughcovid[.]com
- covid-19fundraising[.]com
- covid19[.]legal
- covid19relief[.]fund
- covid19smallbizfund[.]com

Unlike the domain names found in the last quarter of 2019, these show a more explicit connection to the outbreak.

Registrant Countries Versus COVID-Affected Countries

As the outside world came to a near standstill, domain parkers and possibly cybercriminals became quite busy. But where are these people located? To find the answer, we extracted the top 30 registrant countries of the coronavirus-themed domain names, as indicated in their WHOIS records.

Note that the records of several domain names were redacted for privacy, perhaps, in compliance with the General Data Protection Regulation (GDPR).

1	United States	11	Germany	21	Brazil
2	Canada	12	India	22	Portugal
3	Panama	13	Turkey	23	Austria
4	United Kingdom	14	Russia	24	Ireland
5	Spain	15	Netherlands	25	Japan
6	Italy	16	Israel	26	South Africa
7	Australia	17	Czech Republic	27	Colombia
8	France	18	Poland	28	Senegal
9	Redacted for Privacy	19	Mexico	29	Thailand
10	China	20	Switzerland	30	Singapore

Table 1: *Top 30 registrant countries of coronavirus-themed domain names*

Most of the registrants are from the U.S., Canada, Panama, the U.K., Spain, Italy, Australia, France, and China (top 10 registrant countries). Interestingly, six of these countries are also among the top 10 countries affected by the pandemic—the U.S., the U.K., Spain, Italy, France, and China.

825,306 US	43,368 Brazil	14,873 Austria	9,242 Romania
204,178 Spain	40,956 Belgium	13,942 Israel	9,125 Singapore
183,957 Italy	39,405 Canada	11,631 Saudi Arabia	7,891 Denmark
159,300 France	34,318 Netherlands	11,512 Japan	7,755 United Arab Emirates
148,453 Germany	28,063 Switzerland	10,832 Chile	7,241 Norway
130,184 United Kingdom	21,379 Portugal	10,694 Korea, South	7,135 Indonesia
95,591 Turkey	20,178 India	10,398 Ecuador	7,033 Czechia
84,802 Iran	17,837 Peru	9,856 Poland	6,723 Belarus
83,864 China	16,040 Ireland	9,749 Pakistan	6,630 Serbia
52,763 Russia	15,322 Sweden	9,501 Mexico	6,599 Philippines

Table 2: *Confirmed cases by country/region/sovereignty taken from Johns Hopkins Coronavirus Resource Center on 22 April 2020*

Also, comparing the data in Tables 1 and 2, most of those on the top 30 registrant countries of coronavirus-related domains are also in the top 30 most affected by COVID.

The suspected connection between the registrant countries and the nations severely affected by the disease raises some critical questions. Are these newly registered domain names being used to help particular countries fight against the effects of the pandemic? Or are they, perhaps, meant to take advantage of the affected countries' fears and sense of social solidarity brought about by the outbreak? After all, WHO and other authorized organizations don't need any new domain names. They can easily host their COVID-19 web pages on their official websites.

Tracking Cybercriminals' Digital Footprints: Actual Malicious Reports

Although many coronavirus-themed domains may be legitimate, some have figured in malicious activities including phishing and malware attacks. That doesn't veer off from the current

cybersecurity landscape where domain names often get weaponized. Even WHO had to issue an official warning against cybercriminals. A snippet of WHO's statement reads:

"Hackers and cyber scammers are taking advantage of the coronavirus disease (COVID-19) pandemic by sending fraudulent email and WhatsApp messages that attempt to trick you into clicking on malicious links or opening attachments."

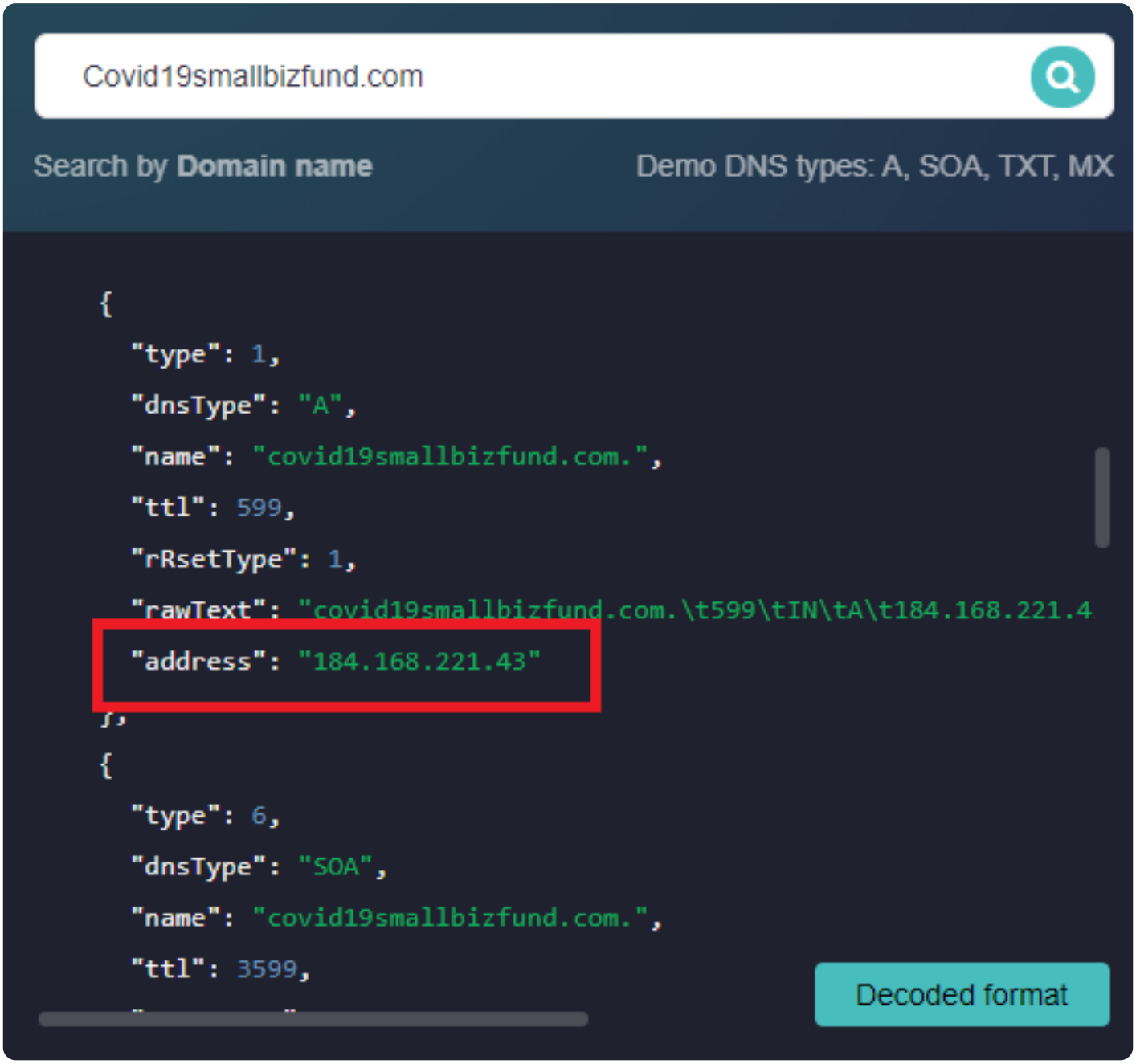
This scheme, as it turns out, is just the tip of the iceberg. Here, we tackled some of the tactics that cyber criminals employ with the aid of coronavirus-themed domain names.

Donation Drives

Some actors take advantage of the social solidarity that the pandemic brought about. Coronavirus-themed domains are used to ask for donations, which often turn out to be phishing sites or malware hosts. When a victim lands on the domain intending to donate, threat actors steal their credit card or banking details instead. Some of the domains were tagged as malware hosts on VirusTotal such as:

- cdc-covid19[.]com
- covid19relief[.]fund
- covid19[.]legal
- covid-19fundraising[.]com
- covid19smallbizfund[.]com

These domains could make victims believe that they are legitimate donation portals. Therefore, consulting a passive DNS database for IP and domain intelligence and associations may be worth looking into. The domain covid19smallbizfund[.]com, for instance, resolves to the IP address 184[.]168[.]221[.]43. Such IP intelligence came from DNS Lookup API.



The passive DNS database revealed several other domains that resolve to the same IP address (a few of them are listed below). As covid19smallbizfund[.]com is possibly tied to phishing undertakings, these domains also deserve investigation.

DOMAIN	LAST_UPI	IPS
amymuller.com	26/07/2019	184.168.221.43
draperstrends.com	26/07/2019	184.168.221.43
ethic-edit.com	26/07/2019	184.168.221.43
staatsdesigns.com	26/07/2019	184.168.221.43
take2americainc.net	26/07/2019	184.168.221.43

Coronavirus Treatments

Threat actors have also begun targeting the healthcare sector by sending emails about COVID-19 treatment. Victims who clicked on the embedded links or downloaded attached files unwittingly infected their devices with the HawkEye malware, a notorious Trojan and keylogger. In one campaign, even the WHO Director General was impersonated in a phishing email.

Source: IBM X-Force Exchange

Some domains that could lure victims into believing that the alleged cure for the coronavirus is

legitimate include:

- autoimmunecovid[.]org
- autotestcovid19[.]com
- bostoncovidcleanup[.]com
- copingthroughcovid[.]com

Key Takeaways

The tremendous spike in the number of coronavirus-themed domain name registrations proved once again that domain names are among the most used attack vectors. From only a couple of dozen domains registered from October to December 2019, the number has risen to more than 50,000 in March 2020.

The correlation between the top registrant countries and the nations affected by the pandemic, although not absolute, also sparks concern. Are domain parkers and cybercriminals aiming to profit off their countrymen?

Regardless of the answer, it's clear that coronavirus-related computer infections are increasing as threat actors continue to weaponize domain names while capitalizing on the pandemic. From donation drives, surveys, extortion, and even treatment lures, anyone could fall victim to coronavirus-themed phishing and malware attacks.

However, cybersecurity teams can use IP and domain intelligence to fight off not only pandemic-themed attacks but also other cyber threats.