Cyber Threat Intelligence in Action: Malicious COVID Footprint Enrichment, Expansion, and Infrastructure Analysis

Posted on June 22, 2020

We have been monitoring COVID-19 cyber threats for several months now. More recently, we partnered with GeoGuard to enrich a dataset of coronavirus-themed URLs and IP addresses with WHOIS data and domain reputation scoring, followed by a passive DNS analysis to enlarge the malicious footprint under the study. The three sections in this post discuss the results of our research in greater depth.

## Part 1: WHOIS Footprint Enrichment

We ran the WHOIS enrichment analysis by using Bulk WHOIS API for all of the obtained 1,098 domains, the oldest of which was registered on 2 June 1986. If you are wondering why the term "coronavirus" already appeared in a domain name in 1986, it's likely because its origins can be traced back to 1968.

Coronavirus does not just pertain to COVID-19 but also to the Severe Acute Respiratory Syndrome (SARS) identified in 2003 and the Middle East Respiratory Syndrome (MERS) seen in 2012. In the years leading up to 2020, it was therefore not surprising to see very few connected domain registrations.

Domain Registration Growth
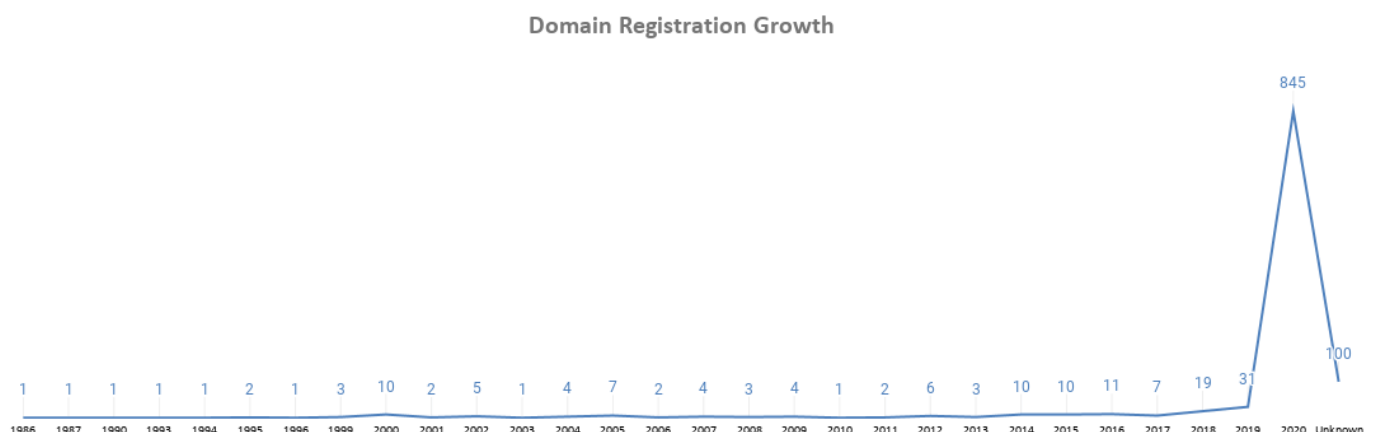
Over the past few months, however, we have seen the volume of associated domain registrations

in the dataset rise significantly from 13 December 2019 to 7 April 2020.

Registration Growth
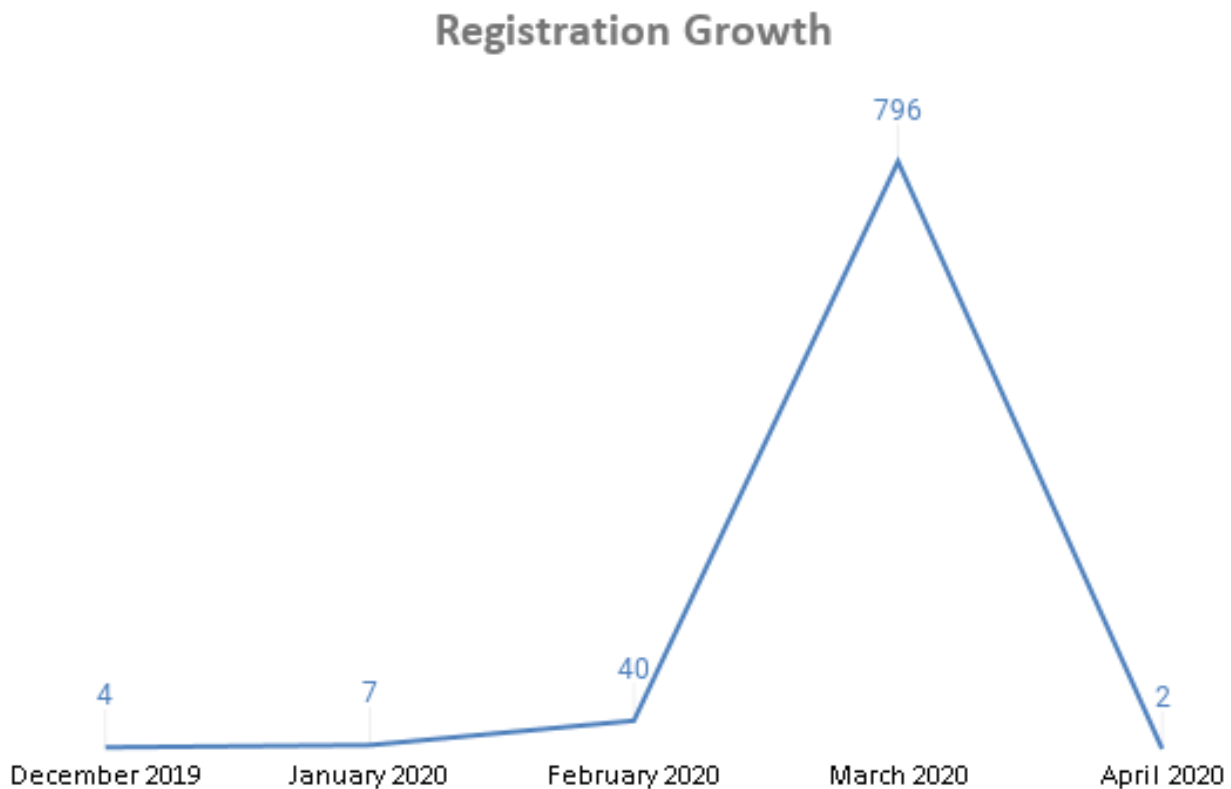
In line with the increasing domain registration trend, we published several analyses of coronavirus- or COVID-19-related threats that include but are not limited to:

- Phishing attacks, business email compromise (BEC) scams, and data stealers

- Fake donation drives and treatments

- Typosquatting

Top-Level Domains Used

A significant share (47%) of the 1,098 domains sported the .com generic top-level domain (gTLD).

Top 10 TLDs

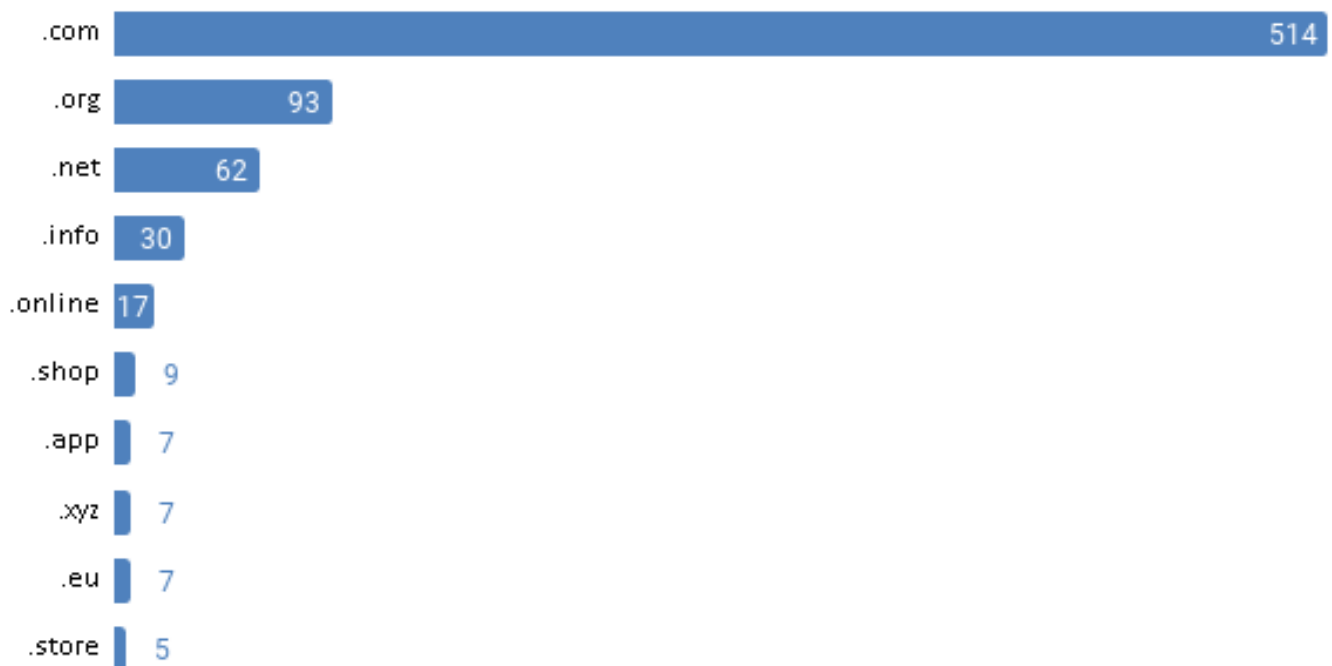| TLD	Count
.com	514
.org	93
.net	62
.info	30
.de	22
.ru	21
.it	18
.uk	17
.online	17
.es	14

Other gTLDs included:

- .site (5)

- .live and .today (4 each)

- .club, .guru, .industries, and .world (3 each)

- .edu, .biz, .asia, .cloud, .tech, .technology, .network, .delivery, .exposed, and .nrw (2 each)

Among the total number that used gTLD extensions (829), 62% were .com domains. That is not

surprising given that potential victims might be more prone to clicking on .com domains than those using new gTLD extensions.
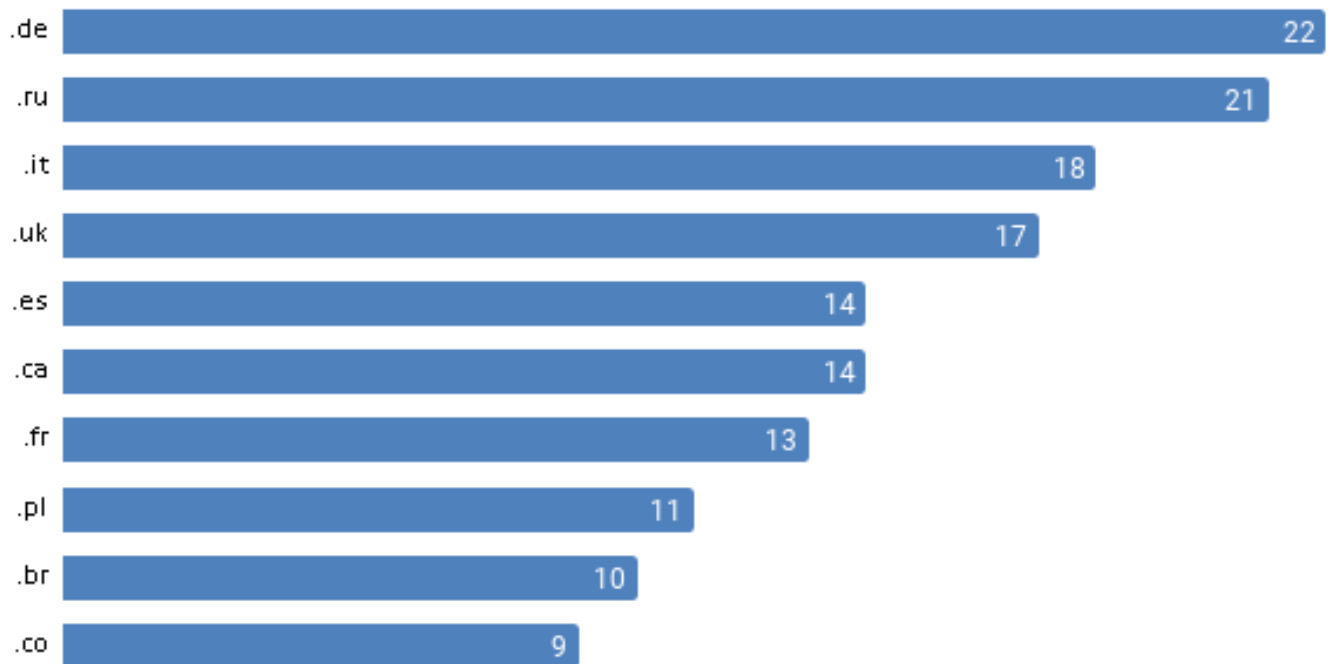
Top 10 gTLDs

gTLD	Count
.com	514
.org	93
.net	62
.info	30
.online	17
.shop	9
.app	7
.xyz	7
.eu	7
.store	5

Out of the total volume that used country-code TLD (ccTLD) extensions (269), 8% were .de domains.

Top 10 ccTLDs

ccTLD	Count
.de	22
.ru	21
.it	18
.uk	17
.es	14
.ca	14
.fr	13
.pl	11
.br	10
.co	9

Domain Registrars

Among the 1,098 domains, 18% were handled by GoDaddy.com Inc. followed by Name.com LLC and Tucows Domains Inc. with shares of 11% and 8%, respectively.

Top 10 Registrars

Registrar	Count
GoDaddy.com Inc.	203
Name.com LLC	122
Tucows Domains Inc.	92
Namecheap, Inc.	79
Google LLC	57
PDR Ltd.	27
FastDomain Inc.	19
OVH	19
REG.RU LLC	19
Enom, Inc.	17
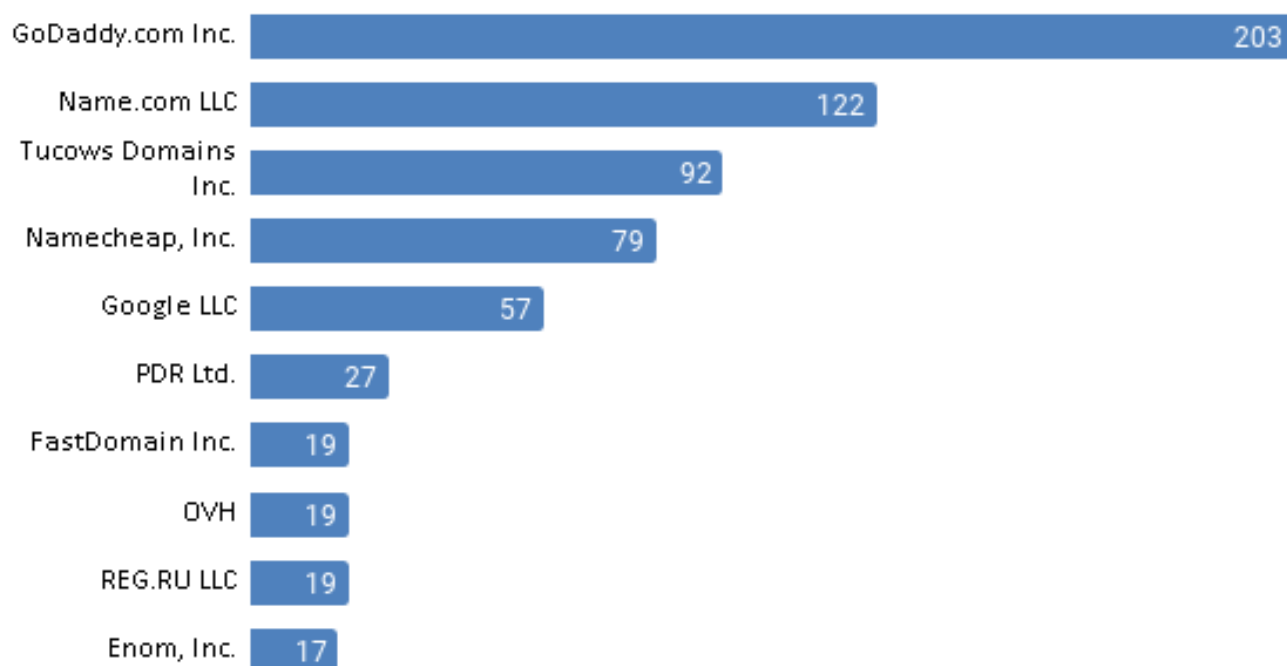
Other registrars include:

- 1&1 IONOS SE (16)

- Gandi SAS (14)

- Wix.com Ltd. (13)

- Network Solutions LLC (12)

- Beget LLC and Domain.com, LLC (11 each)

- Amazon Registrar, Inc. (10)

- Automattic Inc. and NameSilo, LLC (9 each)

- 1API GmbH; Dynadot LLC; Key-Systems GmbH; and MarkMonitor, Inc. (7 each)

- DonDominio (SCIP); Launchpad, Inc. (HostGator); Ligne Web Services - LWS; Porkbun LLC; and Wild West Domains, LLC (6 each)

- 10DENCEHISPAHARD, S.L. and TLD Registrar Solutions Ltd. (5 each)

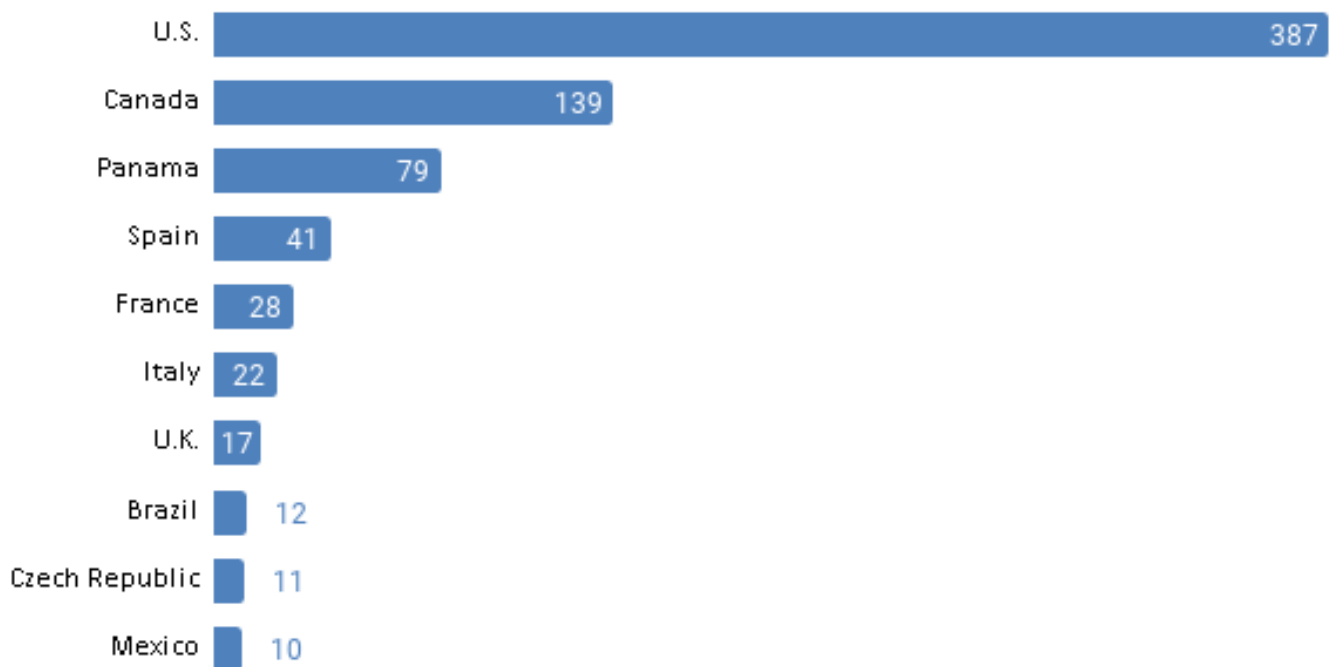From the above, it's interesting to note that the majority of coronavirus-themed registrations were made through well-known registrars, many of which are based in the U.S.

Domain Registrant Countries

More than a third of the domains (35%) were registered in the U.S. followed by Canada (12%), Panama (7%), Spain (4%), and France (2.5%). These top registrant countries are among those most hit by the pandemic, even though Panama is a popular choice for private domain registrations (and so the country might figure in the list for that reason). Also, out of 1,098, 19% (214) had redacted country information, likely because registrants wanted to remain anonymous.

Top 10 Registrant Countries

| Country	Count
U.S.	387
Canada	139
Panama	79
Spain	41
France	28
Italy	22
U.K.	17
Brazil	12
Czech Republic	11
Mexico	10

Other registrant countries include:

- India (9)

- Germany (8)

- Japan, Netherlands, and Portugal (7 each)

- Russia (6)

- Australia, Colombia, and Romania (5 each)

- China, Hong Kong, Luxembourg, Poland, and Turkey (4 each)

Domain Reputation Scores

We subjected all of the 1,098 domains to reputation checks and found that the majority had low scores, which indicates that access is better avoided (at least without proper screening). While we do not expect all of the low-scoring domains to be immediate threats, we still found 55% of them appearing on one or more blacklists. This is a clear indication of the overall maliciousness of the footprint under study.

Domain Reputation Scores

Score Range	Count
31-40	15
41-50	8
51-60	151
61-70	550
71-80	141
81-90	173
91-100	52
Unknown	8
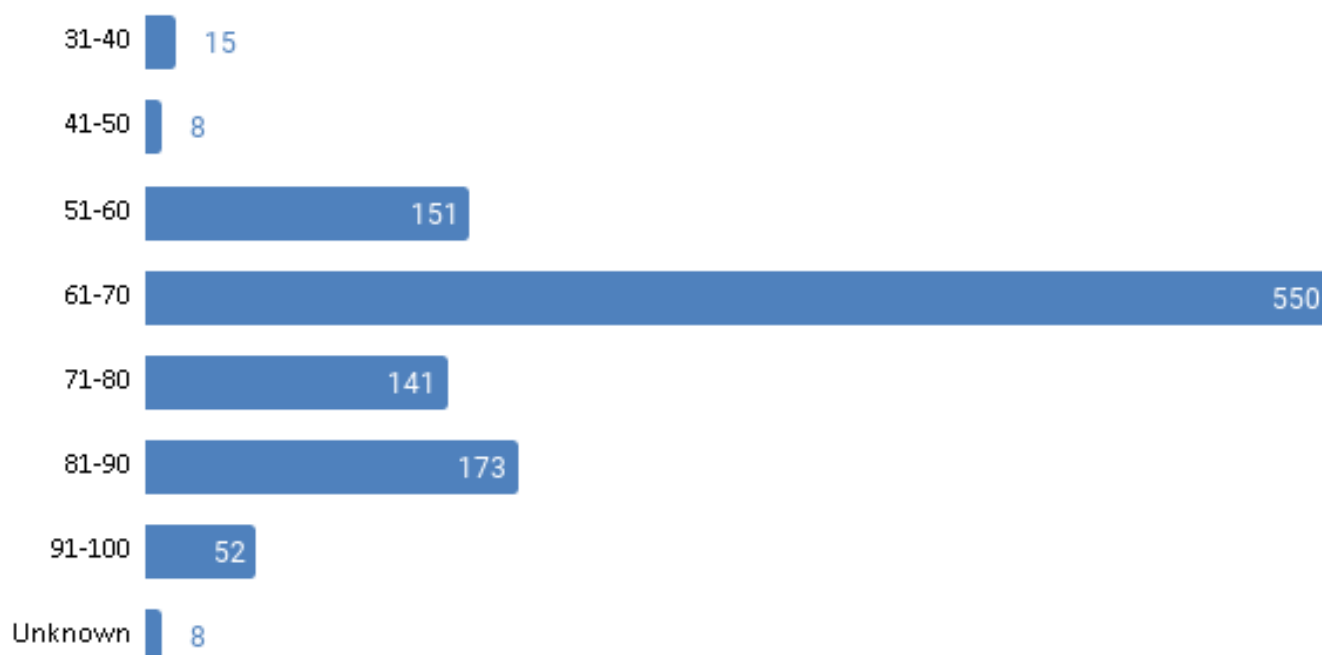
Part 2: Passive DNS Footprint Expansion

Are there other domain names connected to the malicious footprint? We aim to answer this

question in this part of our research.

We looked up the IP addresses from our datasets on our passive DNS database to identify all resolving domain names. That allowed us to identify thousands of new domains, many of which did not seem related to the pandemic judging by their name.

So, we proceeded by filtering only those connected domains that contained some variations of the terms "coronavirus" or "covid" in them. That gave us an additional 1,018 domains that shared 604 unique IP addresses. Those IP addresses were shared by between a minimum of 2 domains and a maximum of 280 from 4 January 2019 to 28 March 2020.

Top 10 IP Addresses in Terms of Domain Resolution
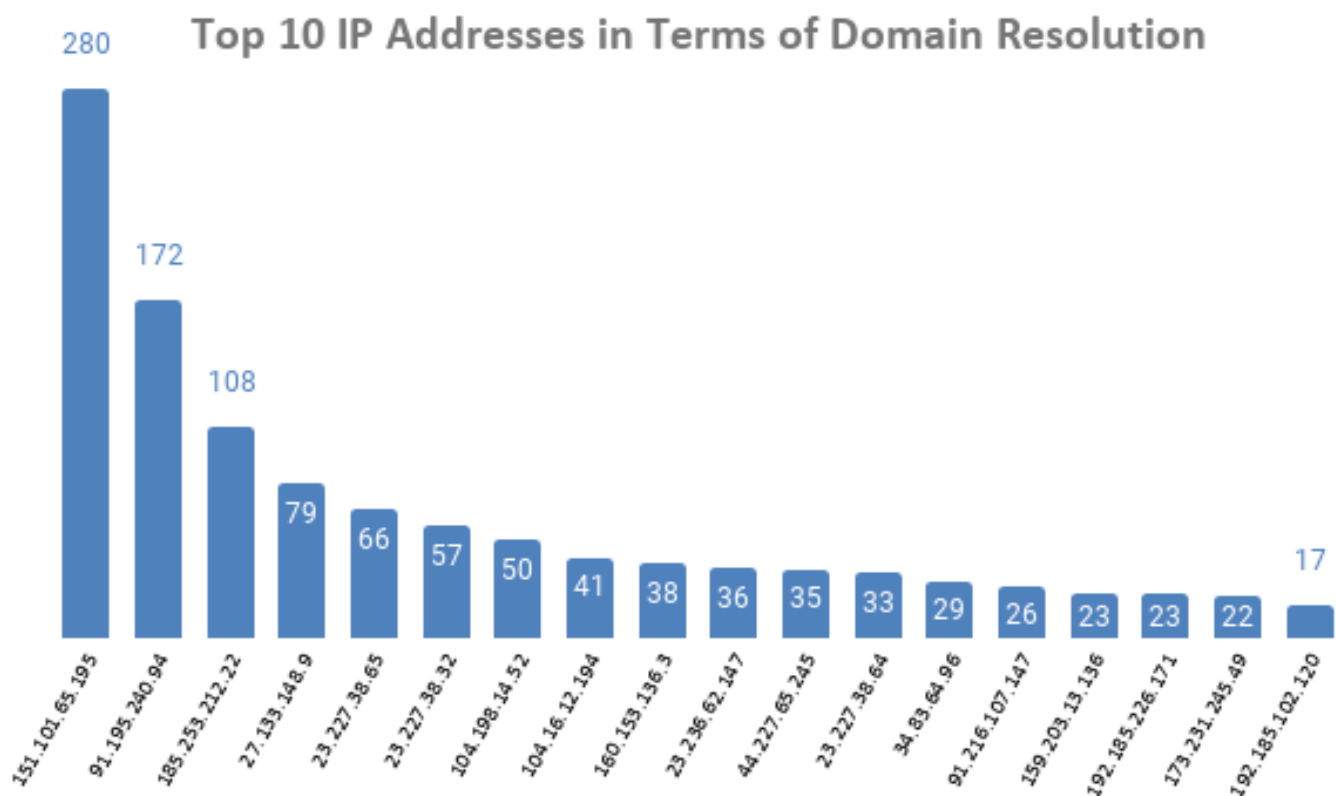
- **151[.]101[.]65[.]195:** Used by 280 domains, including covid-19[.]direct, covid-19[.]kucza[.]xyz, and covid-19[.]london.

- **91[.]195[.]240[.]94:** Used by 172 domains, including acoronaviruscure[.]com, covid19testemunhos[.]pt, and mail[.]acercacovid-19[.]pt.

- **185[.]253[.]212[.]22:** Used by 108 domains, including coronavirus-sklep[.]pl, covid-19[.]london, and covid-19[.]luasoftware[.]com.

The above representation tells us that some IP addresses did resolve to a lot of coronavirus-themed domain names at some point. A possible reason for this is bulk registration, where a given hosting provider just allocated the same IP address out of operational convenience (likely because a significant share of these domains were registered on the same date by the same person).

Part 3: Infrastructure Analysis Using Reverse IP/DNS Intelligence

What more can be said about the infrastructure of some of the above-mentioned domain names? This section shows what kind of insights can be gathered from reverse IP/DNS intelligence.

Reverse IP/DNS

Reverse IP/DNS API gives users a complete list of all the domains hosted on an IP address. In this particular scenario, ties to any of the malicious or suspicious coronavirus- or COVID-19-themed domains can be a reason for blacklisting.

We chose the domain corona-virus101[.]com from the dataset as an example. According to its WHOIS record, corona-virus101[.]com was created on 12 March 2020 by a U.S.-based registrant with GoDaddy.com Inc. To obtain its corresponding IP address, we ran corona-virus101[.]com on DNS Lookup API.

We found in our earlier analysis that corona-virus101[.]com is suspected of malicious ties. A TIP search for its corresponding IP address also flagged 184[.]168[.]221[.]32 for malicious activity. That said, organizations like those in the list of co-users of the IP address obtained via Reverse IP/DNS API will most likely be affected if security operations centers (SOCs) and managed

security service providers (MSSPs) block threat sources at the IP level.

Reverse MX

Many organizations also share mail servers with others. Our TIP analysis for
coronavirusrapidtest[.]com showed that it is also suspected of malicious ties. From the same

report, we know that the domain is connected to five mail servers with their corresponding IP addresses shown below.

Mail exchanger (MX) records ⓘ

Preference	Exchange	IPv4	IPv6	TTL
20	eforward5.registrar-servers.com	162.255.118.62	?	1800
15	eforward4.registrar-servers.com	162.255.118.61	?	1800
10	eforward1.registrar-servers.com	162.255.118.51	?	1800
10	eforward2.registrar-servers.com	162.255.118.52	?	1800
10	eforward3.registrar-servers.com	162.255.118.51	?	1800

Additional TIP queries for each mail server's IP address showed that 162[.]255[.]118[.]62 and 162[.]255[.]118[.]61 were also suspected of malicious connections. We retrieved a list of domains that shared these two mail servers that may be affected should the IP addresses be blacklisted. The owners of the domains in our Reverse MX API results would do well to shift mail servers to avoid unwanted repercussions.

eforward5.registrar-servers.com

Search by Mail server address   The demo is limited to 300 records

```
{}  0: Object                          Total records: 300
    66  name: "guidesfordomino.com",
    66  first_seen: "1551664081",
    66  last_visit: "1577563897"

{}  1: Object
    66  name: "grasswaves.bid",
    66  first_seen: "1551663985",
    66  last_visit: "1554688030"

{}  2: Object
    66  name: "govcorruption.com",
    66  first_seen: "1551663726",
    66  last_visit: "1577563720"
```

Decoded format

Reverse NS

Like mail servers, sharing a nameserver with a suspected cybercriminal does not bode well for domain owners. According to a TIP analysis, the domain coronavirusalerts[.]net is also suspected of malicious ties. The same report tells us that it has two nameservers that resolve to the IP addresses shown below.

NS records ⑦

NS records successfully fetched from the parent name server: a.gtld-servers.net.

NS server	IPv4	IPv6	TTL
ns1.md-92.webhostbox.net	162.215.253.14	?	172800
ns2.md-92.webhostbox.net	162.215.253.14	?	172800

Additional TIP queries for the nameserver IP address showed that 162[.]215[.]253[.]14 is malicious. That said, domains that share the nameserver, obtainable via Reverse NS API, may be affected by IP-level blocking as well.

As our analyses above show, malicious footprint enrichment and expansion in addition to analyzing connected infrastructure is possible with different sources of cyber threat intelligence such as Bulk WHOIS API, Domain Reputation API, and Reverse IP/DNS API, Reverse NS API, and Reverse MX API. Integrating these sources into existing solutions and systems can help platform owners, MSSPs, and SOCs build a better defense against coronavirus-related and other

malicious domains and IP addresses.