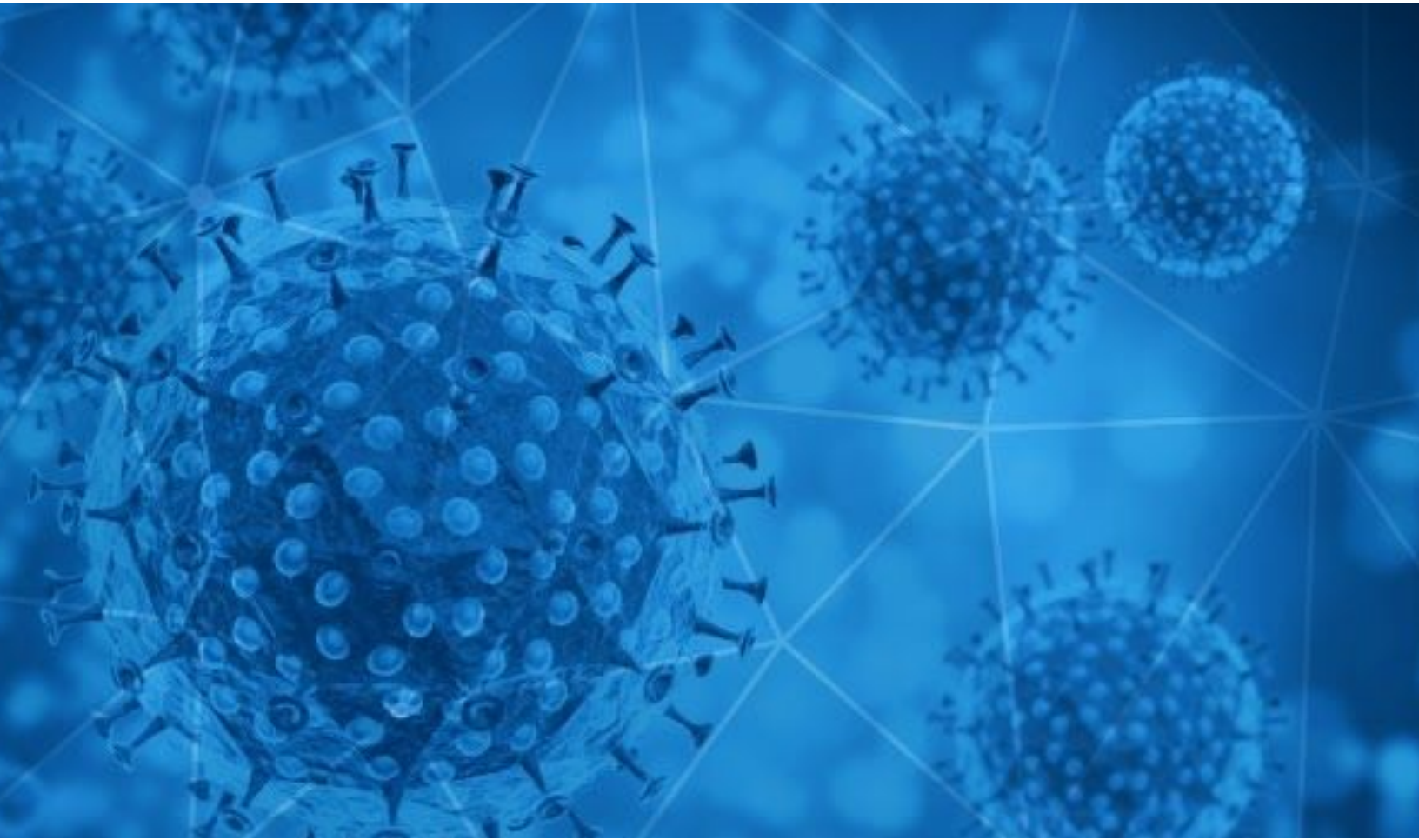
RISKIQ®

RiskIQ i3:

COVID-19 Daily Update

04/11/2020



RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

Table of Contents

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

Methodology

The information provided in this report is limited to open source and publicly available data discovered through standard, commonly known browsing techniques and keyword searches. To provide efficient results, RiskIQ may use websites that require payment in exchange for aggregation of data that is otherwise publicly available without payment and could be obtained by anyone accessing the correct sites or engaging the correct third parties to obtain the information. Information presented in this report is cross-checked against multiple sources for full verification; however, some assessments and conclusions are based on incomplete information and represent the RiskIQ analyst's judgment based on patterns and data available.

Disclaimer

The information provided in this report is "as-is" and Customer acknowledges and agrees that RiskIQ makes no representation or warranty, express or implied, as to the accuracy or completeness of the information. Customer agrees that RiskIQ shall not have any liability resulting from Customer's use of this information.

Digital Exploitation

Adapting the new economic realities from COVID-19, cybercriminals are offering steep discounts on their services, tools, and stolen data. According to research by Group-IB and Gemini Advisory, dark web vendors began dropping prices anywhere from 20-40% at the end of February/early March to drive sales at least through April 2020.

On 10 April 2020 KrebsOnSecurity warned that the new Internal Revenue Service (IRS) site for Economic Impact Payments could make it easy for thieves to intercept some stimulus payments. Because millions of U.S. residents aren't required to file a tax return, the IRS is asking these "non-filers" to use the new website to provide their bank account information to receive stimulus payments. However, the loose identification requirements, as well as the availability of Personally Identifiable Information (PII) online, will likely cause an increase in fraudulent applications.

According to research by Chainalysis, cryptocurrency scammers' incomes fell 30% during March 2020, despite attempts to leverage COVID-19. Though they appear to be reaching similar numbers of victims, the cryptocurrency price drops spurred by the pandemic have drastically reduced the revenue of Ponzi schemes and investment scams that make up most cryptocurrency scamming.

New Blacklist Data

hxxp://kfc-covid-19[.]com/

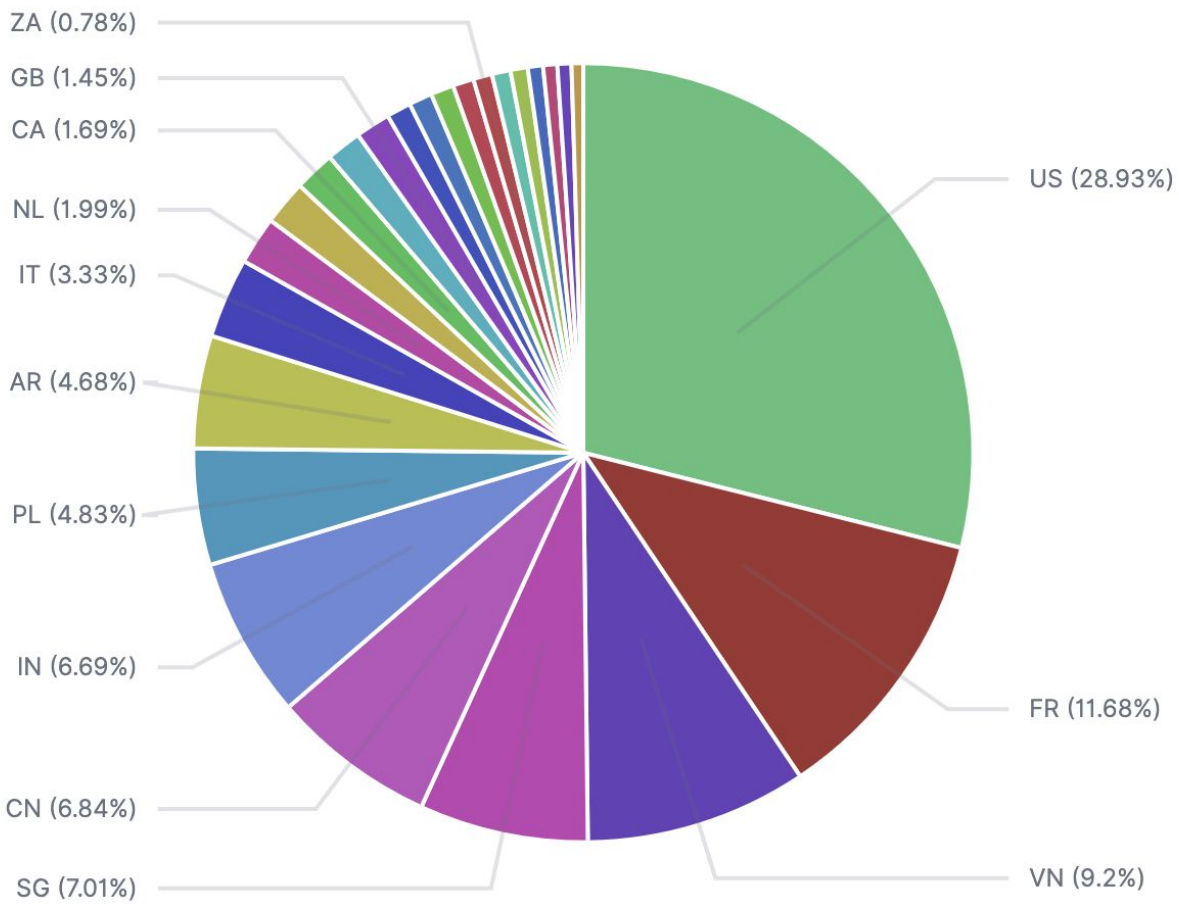
hxxps://covid-19-test-org-uk[.]myshopify[.]com/

hxxps://covid19normalityrelief[.]com/

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 04/10/2020-04/11/2020. During this period, RiskIQ analyzed 149,333 spam emails containing either “*corona*” or “*covid*” in the subject line. There were 15,552 unique subject lines observed during the reporting period. The spam emails originated from 7,076 unique sending email domains and 11,152 unique SMTP IP Addresses. Analysts identified 1,718 emails which sent an executable file for Windows machines.



Spam emails by country of origin

Top 25 Subjects

1. 9,313 - Re: UN COVID-19 Stimulus
2. 9,041 - WEBINAR: Business Survival Now & After COVID-19
3. 4,892 - CDC HEALTH emergency coronavirus (COVID-19) Pandemic
4. 4,311 - The Mask that can prevent Coronavirus now
5. 4,274 - Ethical Pandemic Coronavirus Supplies
6. 4,145 - (Quick delivery/Today's quotation) Protective mask and Diagnostic kit for COVID-19, goggles, infrared thermometer, protective clothing
7. 4,031 - CORONAVIRUS ALERT: FREE Breathing Masks For USA
8. 3,070 - The Corona Letter: India's food supply is on the edge
9. 2,949 - COVID19 Offer -85%
10. 2,534 - coronavirus.mascarilla de proteccion facial
11. 2,291 - COVID-19: Developers with skills in old programming languages see a huge demand | Average salary of software testing engineers in top IT companies
12. 2,233 - Coronavirus is spreading, this specialized mask can control it
13. 1,682 - Newster COVID-19 treatment references
14. 1,639 - Oracle offers free access to cloud courses and certification till May 15 | Indian IT firms confirm to honour job offers amid Coronavirus outbreak
15. 1,633 - SUPPORT NEEDED FOR LESS PREVILEGED COVID-19 AFFECTED PEOPLE AND AREAS
16. 1,615 - Latest Corona Virus Update: (Urgent)
17. 1,384 - CORONAVIRUS ALERT:Breathing Mask
18. 1,203 - Let our unemployment guide help you take on the COVID19.
19. 1,197 - Let our unemployment guide help you take on the coronavirus.
20. 1,193 - Be prepared. Use our unemployment guide to help during the coronavirus crisis

21. 1,192 - Welche Maske sollten Sie gegen das Coronavirus tragen? Hier die Informationen und alles Wissenswerte
22. 1,166 - Need Unemployment information because of the coronavirus?
23. 1,159 - Don't let the coronavirus stop you. Learn free information about unemployment assistance.
24. 1,141 - Are you prepared for a potential job loss due to COVID19?
25. 1,139 - Worried you might lose your job because of COVID19?

Top Subjects Containing Attachments with Executable Files for Windows Machines (PE/EXEs)

1. 1,712 - Newster COVID-19 treatment references
2. 3 - RE: Re: Re:(EMAIL ref. 767/19)/COVID-19/Order 20% discount
3. 2 - RE: Re: Re:(EMAIL ref. 767/19)/COVID-19/Order 20%!d(MISSING)iscount
4. 1 - RE: Re: Re:(EMAIL ref. 767/19)/COVID-19/Order 20% discount

Top Countries Sending SPAM - Covid?/Coronavirus Contained in Subjects (by Geolocation on SMTP IP Address)

1. 38,453 US
2. 15,526 FR
3. 12,232 VN
4. 9,312 SG
5. 9,086 CN
6. 8,894 IN
7. 6,419 PL
8. 6,224 AR
9. 4,423 IT
10. 2,644 NL
11. 2,467 DE
12. 2,244 CA
13. 1,955 BR
14. 1,922 GB
15. 1,352 RU
16. 1,285 TH
17. 1,272 HU
18. 1,155 HK
19. 1,041 ZA
20. 1,021 JP
21. 953 MY
22. 840 BE
23. 778 ID
24. 772 IE
25. 642 ES

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

COVID-19 Host, Domain, and Mobile App Tracking

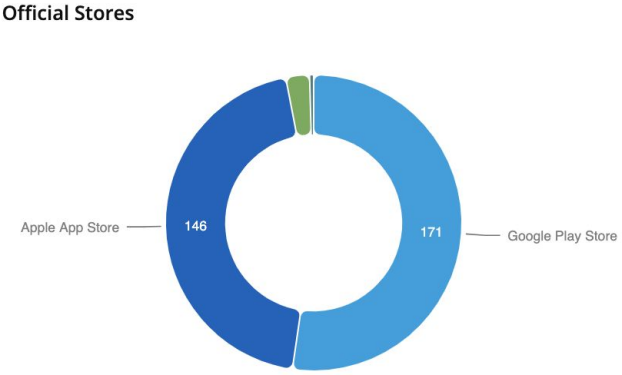
RiskIQ gathers data relating to newly-observed hosts and domains containing COVID-19, COVID19, or Coronavirus in the host or domain name and mobile apps containing COVID-19, COVID19, or Coronavirus in the title or description. A summary of data collected is contained in this section.

Domains and Hosts

Domains: 57,559
Hosts: 65,815
Hosts and Domains with Potential Mail Servers: 267
Email-Capable Domains and Hosts: 21,280
Live Hosts and Domains Not Parked: 26,353

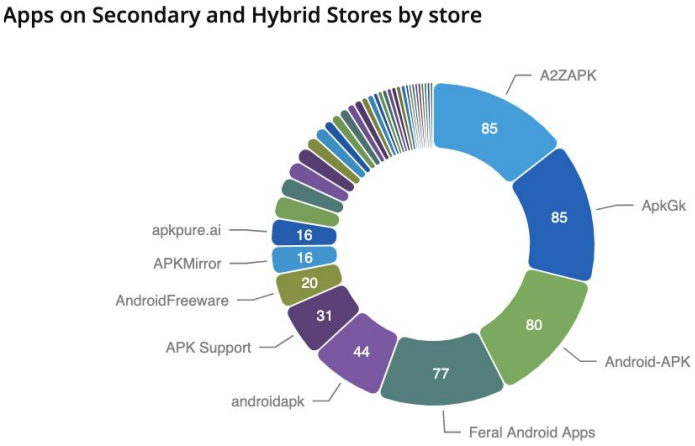
Mobile Apps

1. Apps in Official Stores: 326 (See Graph)
    a. Google Play Store: 171
    b. Apple App Store: 146
    c. Windows Phone: 8
    d. Amazon: 1



2. Apps in Secondary/Hybrid Stores: 563 (See Graph)

3. Blacklisted Mobile Apps by Store Type:
    a. Secondary: 23
    b. Hybrid: 1
    c. Official: 1



RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

End Report