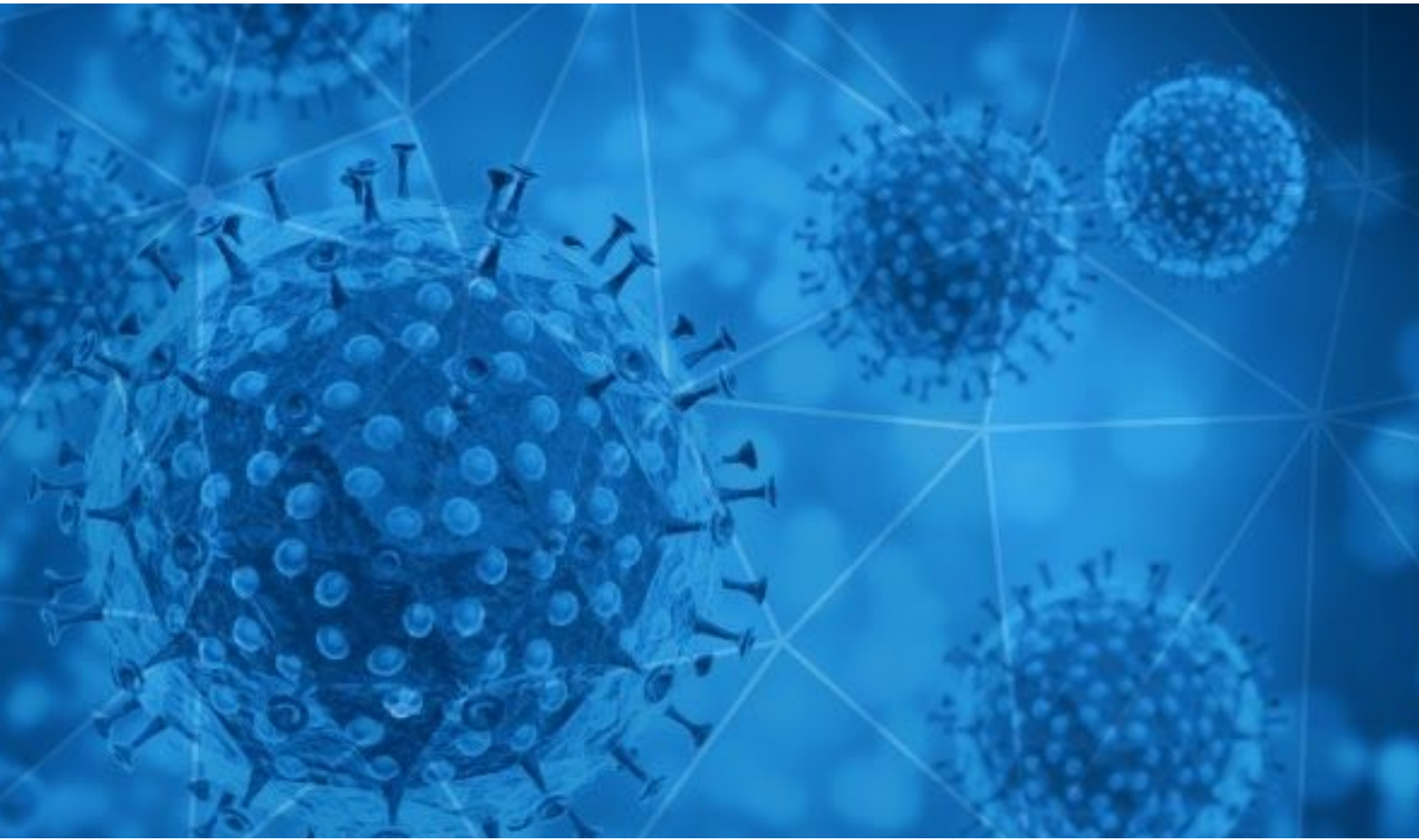
RISKIQ®

RiskIQ i3:

COVID-19 Daily Update

05/09/2020



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

Cybercriminals are exploiting the increasing number of layoffs during the ongoing pandemic to recruit new money mules to help launder money. According to research by PhishLabs, the criminals are sending phishing emails to targets in Canada and the United States with the "opportunity" to work from home for $5,000 per month. Some of the messages are generic and instruct the recipient to request more information via email while others impersonate Wells Fargo Human Resources and claim to be recruiting personal assistant positions.

Cybersecurity researchers now believe the malicious spear phishing attacks against the World Health Organization (WHO) beginning in early April were likely the work of Iranian state-sponsored hacking group Charming Kitten. Several of the messages sent to WHO were carefully designed to look like legitimate correspondence from the British Broadcasting Corporation and the American Foreign Policy Council, and they prompted recipients to click on a shortened URL that diverted to a malicious domain. The domains featured in the messages—including mobiles[.]identifier-services-session[.]site, sgnldp[.]live, and the link shortening service bitli[.]pro—were hallmarks of Charming Kitten's previous attacks, according to Clearsky Cyber Security.

Israel is preparing to launch a "cyber defense shield" for the country's health care sector amid a spike in attacks since the beginning of the global COVID-19 pandemic. As planned, the new system, to be developed by FireEye and the Israeli Health Ministry, will provide real-time protection from cyber attacks.

Online child exploitation has risen to unprecedented levels in the last few months. John Shehan, vice president of the National Center for Missing and Exploited Children (NCMEC), shared that his organization has received 4.2 million reports of child exploitation content in April--up 2 million from March and nearly 3 million from April 2019. This spike is, in part, due to the rise in children at home on internet-connected devices, which creates additional opportunities for abusers to virtually groom minors. Further, there are also more adults online reporting child abuse material. Child traffickers have evolved their operating models by moving what previously would've been face-to-face interactions online through subscription videos and images.

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

New Blacklist Data

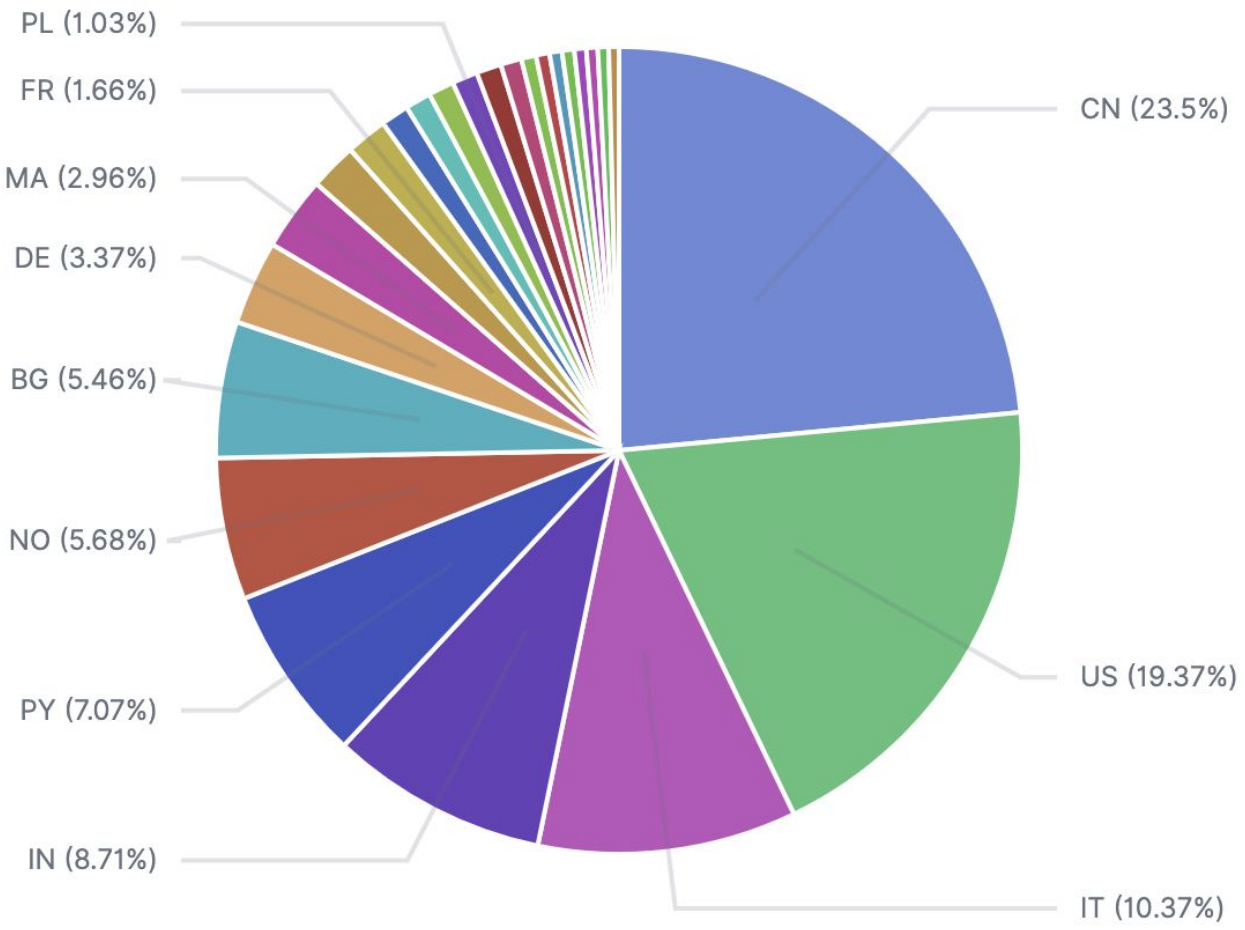
hxxps://freedatacovid-19[.]000webhostapp[.]com/

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

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

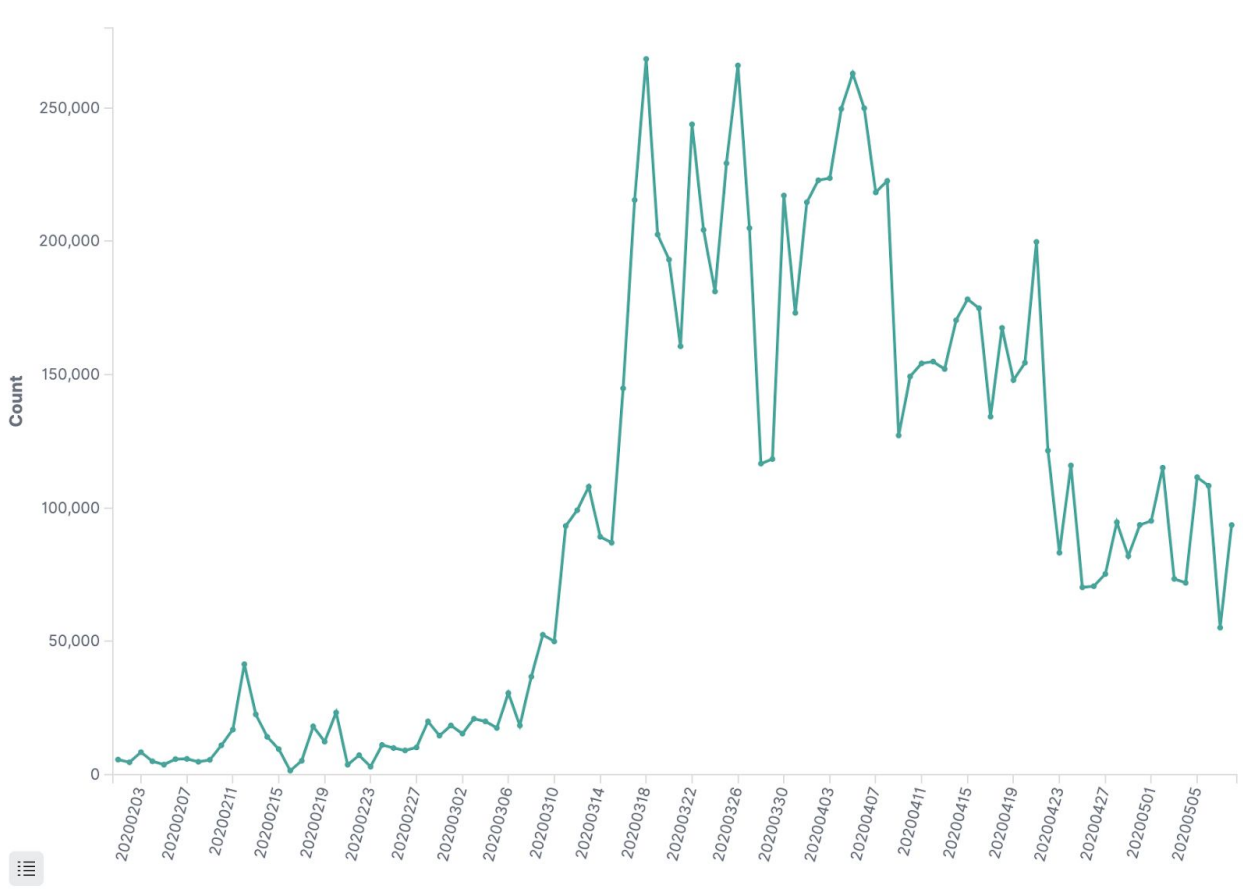
COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 05/08/2020-05/09/2020. During this period, RiskIQ analyzed 93,606 spam emails containing either “*corona*” or “*covid*” in the subject line. There were 7,519 unique subject lines observed during the reporting period. The spam emails originated from 5,598 unique sending email domains and 9,441 unique SMTP IP Addresses. Analysts identified 232 emails which sent an executable file for Windows machines.



Spam emails by country of origin

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



Spam emails by volume since February 1, 2020

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

Top 25 Subjects

1. 8,089 - COVID-19 Stimulus Package Grant Beneficiary
2. 7,843 - Covid-19: non fermiamoci adesso
3. 4,857 - COVID-19 Stimulus Package Grant Beneficairy
4. 4,318 - Working together to fight COVID-19 with immunoglobulin therapy
5. 4,253 - Donate your plasma to help develop a potential treatment for COVID-19
6. 4,248 - You survived COVID-19 YOU COULD HELP OTHERS DO THE SAME
7. 3,264 - The Corona Letter: Bigger the state, bigger the problem
8. 3,254 - COVID-19 Stimulus Package Grant(s) Beneficiary
9. 2,634 - <redacted>, Collect ""COVID-19"" Aid Now
10. 2,028 - 5 high paying coding languages you can learn for free | Indian IT firm rolls out salary hike to employees amid COVID-19
11. 1,168 - Corona Quarantine Update
12. 1,151 - UN/World Health Covid-19 Donations 134.19.178.112
13. 1,013 - COVID19 Career Guide: Start Gaining Work Experience From Home
14. 866 - Reife Frauen treffen trotz Corona
15. 799 - NYC nurse, steals coronavirus patient's cr-dit ca-d as he was on a ventilator 2 buy $60 in groceries
16. 760 - Re: Covid-19 / Vanity upon Vanity
17. 752 - Re: Defeat Coronavirus, non contact fever alarm device
18. 696 - Contactless infrared body temperature thermometer defeat Coronavirus
19. 642 - COVID19: Przyłbice ochronne z atestem CIOP-PIB
20. 642 - COVID-19 Resources for Your Small Business
21. 620 - CUIDADO DE ADULTOS MAYORES /// PROTOCOLO ANTE EL COVID19
22. 570 - COVID-19 Donation Fund
23. 511 - RE: Covid-19 protection masks have been stocked to our US warehouse

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

24. 501 - Sale Masks , Breathing machine and Corona Virus test Kit with good price.

25. 454 - Re: Covid-19 / Vanity upon Vanity

Top 10 IP Addresses

1. 6,290 - 190.211.241.74
2. 5,351 - 183.160.213.245
3. 5,052 - 82.134.25.158
4. 4,855 - 91.236.145.175
5. 3,787 - 183.160.239.121
6. 3,681 - 36.5.132.1
7. 2,634 - 81.192.231.96
8. 2,020 - 219.65.84.187
9. 1,448 - 119.123.128.149
10. 1,168 - 142.11.218.186

Top 10 Domains (RDNS)

1. 6,290 - host74[.]teisa[.]com[.]py
2. 5,052 - 158[.]82-134-25[.]bkkb[.]no
3. 2,634 - adsl-96-231-192-81[.]adsl2[.]iam[.]net[.]ma
4. 2,020 - mgw07[.]tbsl[.]in
5. 1,168 - client-142-11-218-186[.]hostwindsdns[.]com
6. 1,151 - mail[.]healthnet[.]org[.]np
7. 866 - data2web[.]de
8. 660 - svm39636[.]vps[.]tagadab[.]it
9. 641 - 5E98C5F9[.]static[.]tld[.]pl
10. 589 - cpe-181-46-136-165[.]telecentro-reversos[.]com[.]ar

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

1. 227 - URGENT NEED: U.S. Department of Health & Human Services/COVID-19 Face Mask/ Forehead thermometers

2. 5 - URGENT TENDER#675320 (covid19 kits)

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

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

1. 20,911 CN
2. 17,235 US
3. 9,231 IT
4. 7,754 IN
5. 6,290 PY
6. 5,059 NO
7. 4,858 BG
8. 2,999 DE
9. 2,637 MA
10. 1,687 NL
11. 1,477 FR
12. 999 GB
13. 924 ES
14. 916 BR
15. 913 PL
16. 890 CA
17. 748 AR
18. 527 BE
19. 481 AU
20. 445 GR
21. 435 VN
22. 425 IR
23. 403 MX
24. 387 KR
25. 365 CL

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

COVID-19 Host, Domain, and Mobile App Tracking

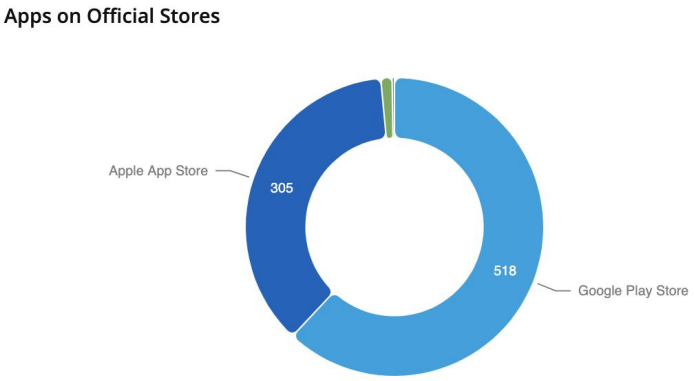
RiskIQ gathers data relating to newly-observed hosts and domains containing COVID-19, COVID19, or Coronavirus in the host or domain name and mobile apps containing COVID-19, COVID19, or Coronavirus in the title or description. A summary of data collected is contained in this section.

Domains and Hosts

Domains: 78,550
Hosts: 89,514
Hosts and Domains with Potential Mail Servers: 292
Email-Capable Domains and Hosts: 28,495
Live Hosts and Domains Not Parked: 35,774

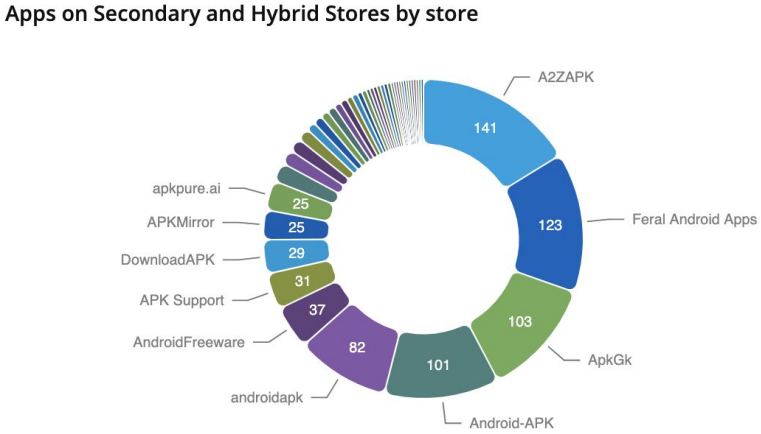
Mobile Apps

1. Apps in Official Stores: 833 (See Graph)
    a. Google Play Store: 518
    b. Apple App Store: 305
    c. Windows Phone: 9
    d. Amazon: 1



2. Apps in Secondary/Hybrid Stores: 823 (See Graph)

3. Blacklisted Mobile Apps by Store Type:
    a. Secondary: 33
    b. Hybrid: 1
    c. Official: 2



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

End Report