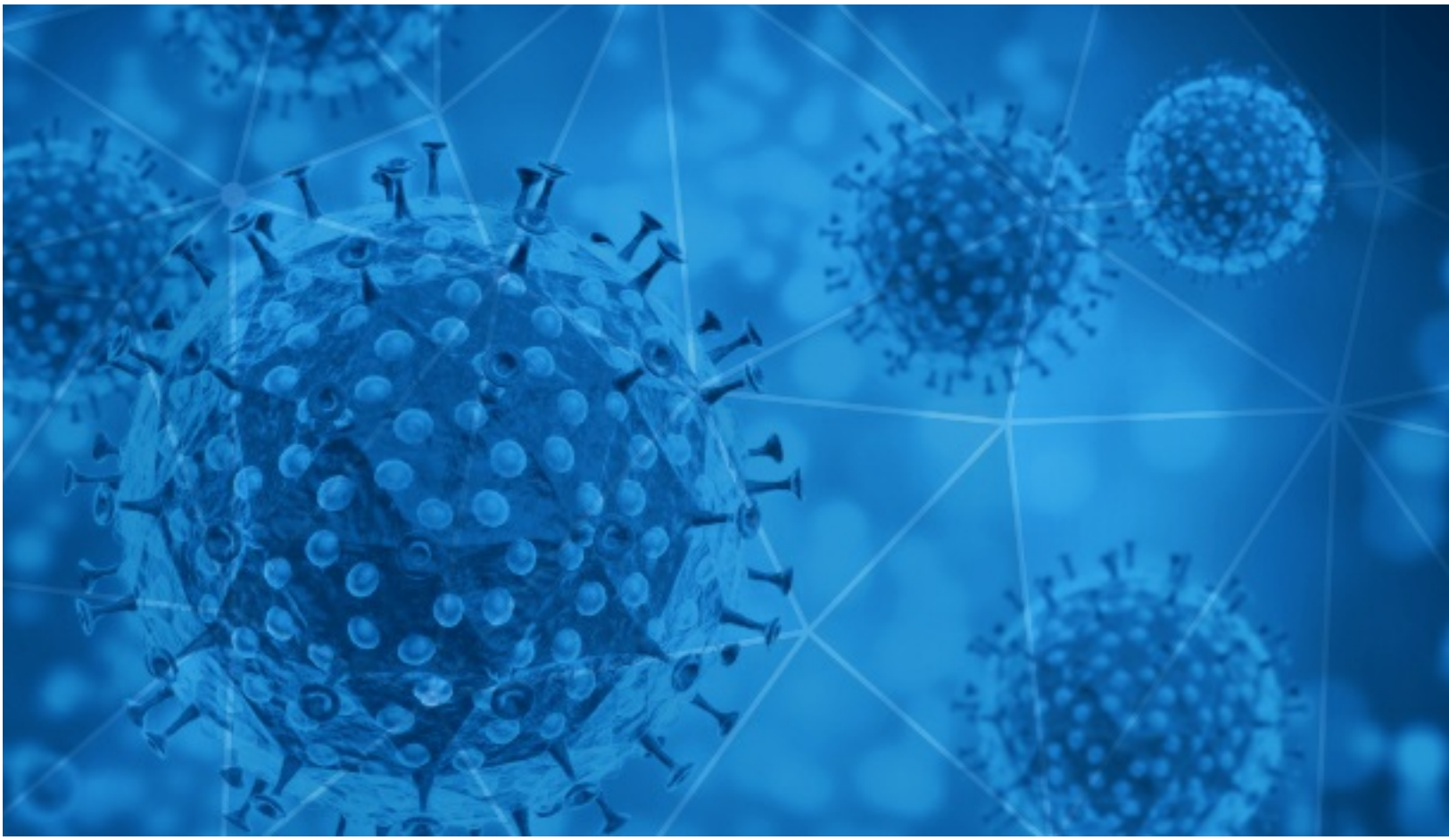
RiskIQ i3:

Finished Intelligence Indicator of Compromise (IOC) COVID-19 Report

2020-08-14



RiskIQ
22 Battery St., 10th Flr
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. The customer agrees that RiskIQ shall not have any liability resulting from their use of this information.

Notice

As of 05/15/2020 RiskIQ changed the format and frequency of the COVID-19 Daily Update. Each Friday, RiskIQ will compile the week's major stories in the Notable Events, Facts and Figures at a Glance, Stay-At-Home/Shelter-In-Place Orders, and Governmental Guidance sections of the report.

The Digital Exploitation data will continue to be delivered daily with the COVID-19 Email Spam Statistics, COVID-19 Host, Domain, and Mobile App Tracking, and COVID-themed Blacklisted Domains included.

RiskIQ has established a microsite for COVID-19 coverage, located at https://www.riskiq.com/covid19-cybersecurity/.

Thank you for your continued readership!

Daily Blacklisted Hosts Feed

RiskIQ is making a blacklisted host feed from its COVID-themed scanning available to the public. Blacklisted hosts listed in the feed have been observed serving scammy/fraudulent content, phish, malware, or malicious code. This data is delivered "AS-IS".

https://covid-public-domains.s3-us-west-1.amazonaws.com/covid19_blacklist.html

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 2020-08-13 to 2020-08-14. During this period, RiskIQ analyzed 47,761 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,485 unique subject lines observed during the reporting period. The spam emails originated from 2,028 unique sending email domains and 4,616 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Are your call details pandemic data?	2094
20,500.00 GBP COVID-19 PANDEMIC ASSISTED FUND	1597
Corona-Hilfskredite	1585
Protect Scores During Coronavirus	1560
COVID-19 And Your Credit Health	1479
Will COVID-19 Impact Your Credit Scores?	1466
Managing Yourself and COVID-19 Stress	1253
Precios Imbatibles / Productos COVID 19	969
De Radiación UV-C Led para Eliminar el CoronaVirus	876
covid-19 and children - how does it affect them?	834
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	790
Wearing a KN95 mask is your best defense against coronavirus	789
Help the world's response to Covid-19 with the most protective mask on the market.	786
ATALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ KHUẨN PHÒNG CHỐNG COVID -19	724
COVID-19 - Send Requirements + SEO (Results Guaranteed) [REDACTED_DOMAIN]	693
Covid 19 Wohltätigkeitsfonds	683
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	664
Nueva línea de atención exclusiva COVID19	537
Desinfeccion Preventiva Covid19	507
Desinfectamos su ambiente de coronavirus	489
Desinfeccion covid19 mediante termoniebla	482
Oferta Imperdible !! Test Rapido Covid-19	480
Covid-19: Quality IT Projects | SEO (Results Guaranteed) - [REDACTED_DOMAIN]	478
RE :Covid-19 / Vanity upon Vanity (Covid-19 is real. Stay Safe!)	466
Protocolos de Salud Ocupacional en tiempos de Covid-19	448

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmail.com	4142
wethosted.cyou	2724
timesofindia.com	2094
emailmarketingservices.us	2087
countermail.com	1860
126.com	1847
wethosted.icu	1781
aol.com	1700
yahoo.com	1617
waysus.cyou	1037

Top-15 IPs Sending COVID Spam

23.231.110.177	2721
23.231.110.178	1780
2.229.106.8	1597
88.198.1.109	1565
23.231.110.172	1037
181.46.136.168	790
190.247.255.193	783
113.89.41.103	561
157.119.122.38	559
190.247.240.13	552

Top-15 Countries Sending COVID Spam

US	15295
DE	6045
CN	4017
IN	3576
AR	3461
--	2892
IT	1730
FR	1577
CL	1519
ES	1190

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Fwd: Covid 19 - Circulaire préfectorale du 13 août 2020	1

Top-15 Subjects Containing doc/xlsx Files

COVID-19 RELIEF FUNDING	12
Plan primene preventivnih mera - Covid (Ministarstvo zdravlja Srbije)	9
COVID-19 Focus OIC Principi Contabili Nazionali: novità normative contabili e fiscali Milano 20/10/2020	8
BHP w dobie Covid19 / Audyt wewnętrzny warsztat kompetencyjny	6
Covid-19 compensation fund	4
Taxation, Payroll Reconciliation and Impact of Covid 19 on your Payroll Function Course 2020	3
COVID 19 - Rientri da Spagna, Croazia, Malta e Grecia. Comunicato stampa	3
[NEW] [ATTACK] [ACTION] ATTACKERS SPOOF COVID-19 LOAN RELIEF WEBPAGE	3
ŘECKO – aktuální vstupní podmínky - CK Alexandria zákazníkům povinný test na COVID-19 zaplatí!	3
Fwd: SEGURO DE SALUD COVID19	2

RiskIQ
22 Battery St., 10th Flr
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.

Domain Stats

Domains: 119,235
Domains with Potential Mail Servers: 2,898
Email-Capable Domains and Hosts: 44,178
Live Hosts and Domains Not Parked: 66,228

Mobile Apps

Apps in Official Stores: 385

by Store

Apple	202
Google	174
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,057

by Store Type:

Hybrid	658
Secondary	355
Affiliate	44

Blacklisted Mobile Apps: 25

by Store Type:

Secondary	22
Official	2
Hybrid	1