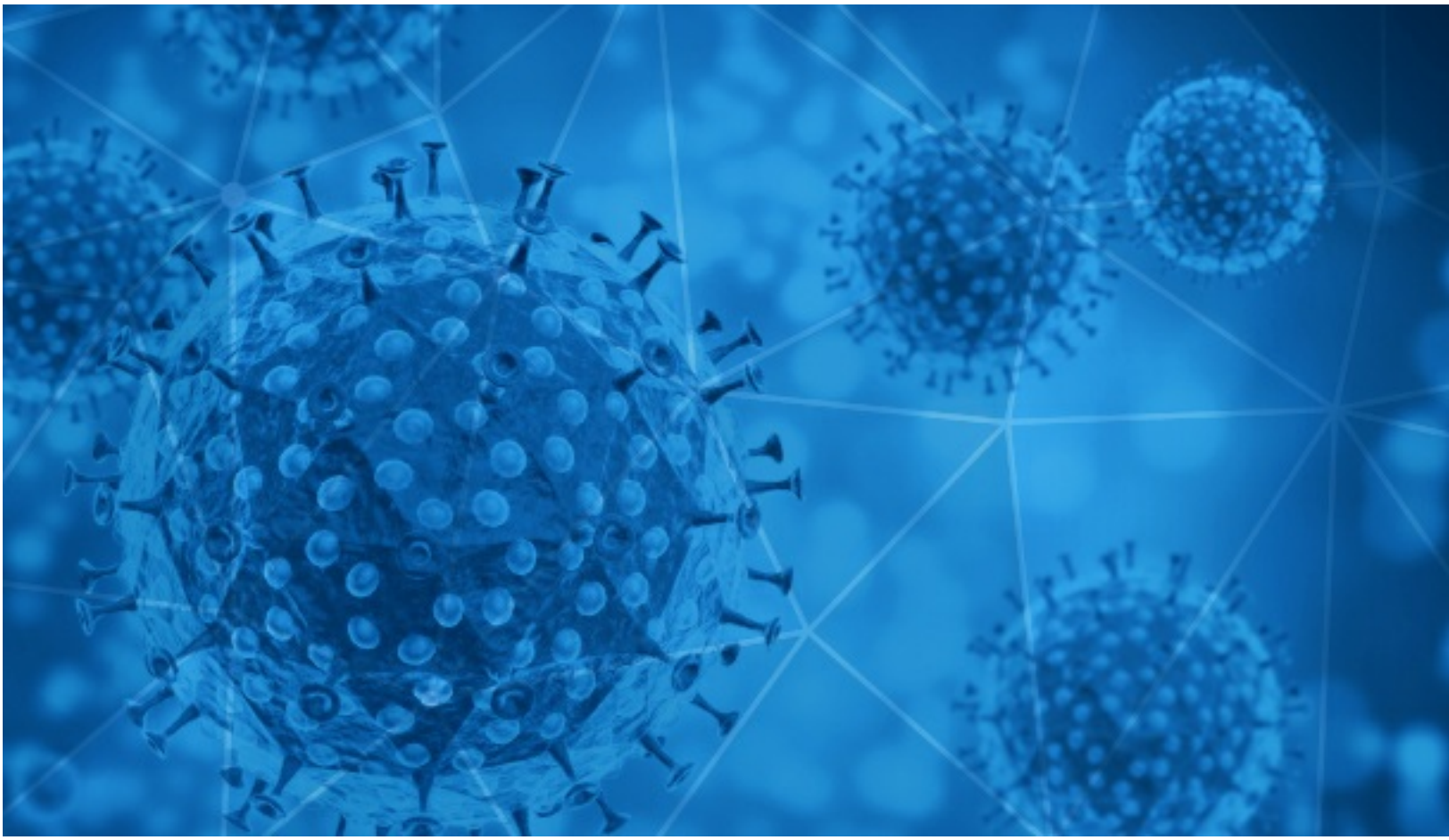
RiskIQ i3:

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

2020-08-24



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 2020-08-23 to 2020-08-24. During this period, RiskIQ analyzed 55,942 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,081 unique subject lines observed during the reporting period. The spam emails originated from 661 unique sending email domains and 2,299 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	27420
The Corona Letter: The debate over blood plasma therapy	2646
Top 10 highest-paying programming languages in 2020 | Infosys to offer promotions to its employees from September amid Corona crisis	2399
Desinfectamos su ambiente de coronavirus	1909
Desinfeccion Preventiva Covid19	1845
Desinfeccion covid19 mediante termoniebla	1837
United Nations Covid-19 Palliative/Financial Support/Congratulations.	1797
covid-19 and children - how does it affect them?	698
Re:Covid 19 Loan Relief	626
Precios Imbatibles / Productos COVID 19	615
Complete your online registration for Covid Antibody IgG test at Rs 750 only | Limited offer.	567
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	561
Re: keep away from Covid-19	560
Re: Personal & Business Funding (COVID-19 Relief)	537
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	481
Re: Defeat Coronavirus, non contact fever alarm device	450
Contactless infrared body temperature thermometer defeat Coronavirus	445
Sumptuous Siam Spread @ International Plaza - Post Covid-19 Circuit Breaker	440
Cabinas para la prevencion del coronavirus?	386
Soluciones para la prevencion del covid19	374
Como volver a la actividad post coronavirus?	369
Will COVID-19 Impact Your Credit Scores?	363
COVID-19 And Your Credit Health	361
Nitrile-Vinyl-Latex Gloves Wholesale & COVID-19 Products with Best Price - Fast Shipping - Order NOW!	361
Protect Scores During Coronavirus	328

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

toyotacarrr.com	27423
ymail.com	6433
timesofindia.com	2646
gmail.com	2480
techgig.com	2399
126.com	2240
rediffmail.com	1363
keyable.net	895
emailmarketingservices.us	698
custacin.cyou	657

Top-15 IPs Sending COVID Spam

201.231.10.6	5002
219.65.84.187	2384
194.250.22.81	1796
201.231.27.232	1269
113.89.41.139	895
23.231.110.130	649
211.241.209.104	626
103.225.55.27	611
181.46.136.168	481
103.225.55.88	480

Top-15 Countries Sending COVID Spam

JP	27514
AR	7223
IN	5235
US	3988
CN	3876
FR	2289
KR	807
--	710
GB	592
PH	537

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

ANC Weekly COVID-19 Reports	26
COVID-19 RELIEF FUNDING	12
Taxation, Payroll Reconciliation and Impact of Covid 19 on your Payroll Function Course 2020	3
Arba Minim for 2020 - The year of Covid-19	2
Re: COVID -19 DUTY SCHEDULE OF DNB/CPS RESIDENTS	2
CCS/9761 Ascienden a 1,106 los decesos por COVID-19 en Chihuahua	2
circualr 083 de 2020 - Secretario de Salud Municipal - Priorizacion de Poblacion para pruebas Covid-19	2
REMITE REPORTE COVID - 19, DE LA EESTP PNP SANTA LUCIA	2
REMITE REPORTE COVID 19 DEL PERSONAL CAS DE LA EESTP-PNP-TRUJILLO DEL DIA DOMINGO 23AGO2020.	2
Fwd: PLAN DE TRABAJO, CRONOGRAMA DE ACTIVIDADES Y PLAN PREVENTIVO COVID 19	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: 120,469
Domains with Potential Mail Servers: 2,924
Email-Capable Domains and Hosts: 45,043
Live Hosts and Domains Not Parked: 69,335

Mobile Apps

Apps in Official Stores: 403

by Store

Apple	209
Google	179
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,212

by Store Type:

Hybrid	717
Secondary	444
Affiliate	51

Blacklisted Mobile Apps: 26

by Store Type:

Secondary	23
Official	2
Hybrid	1