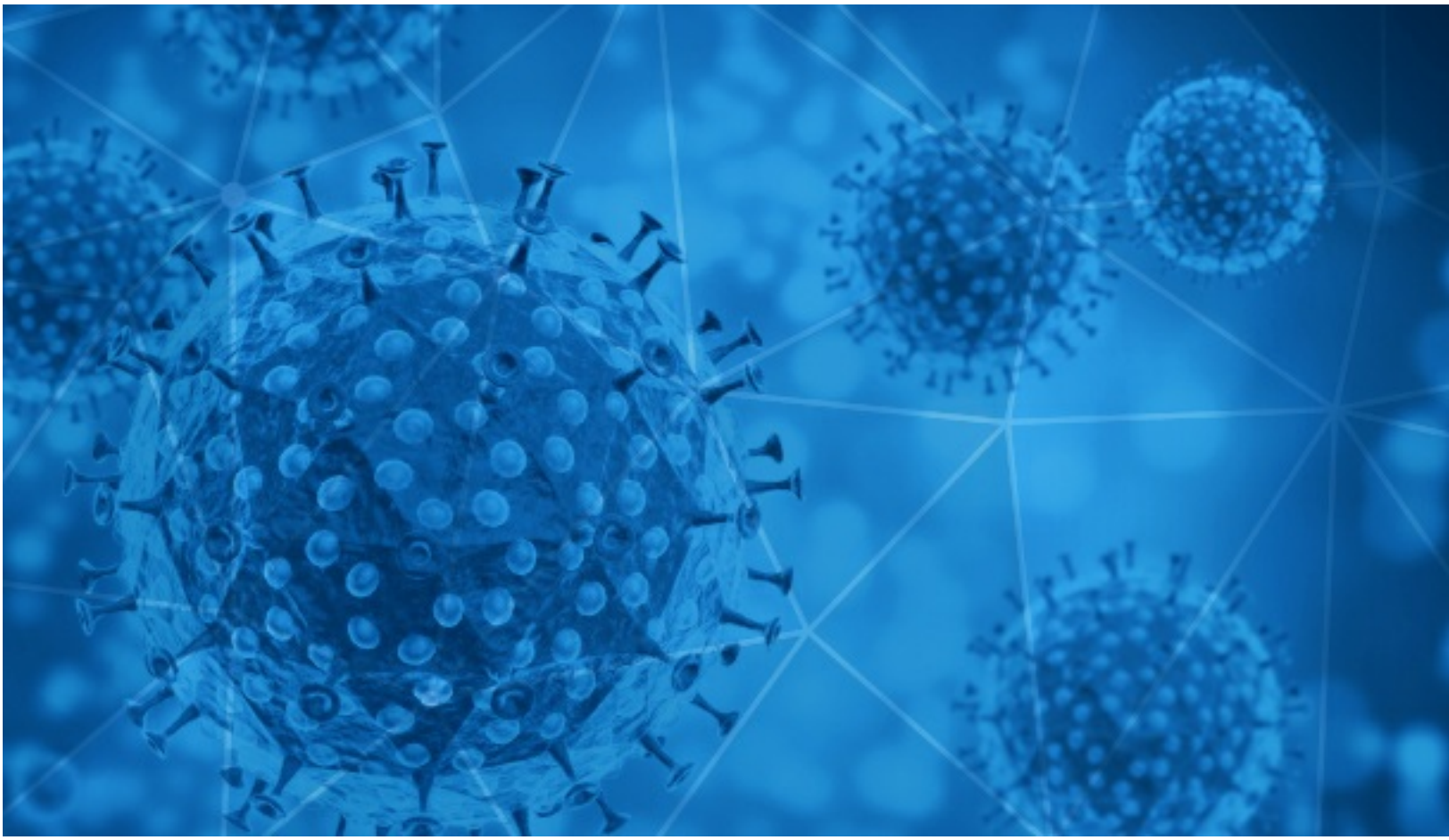
RiskIQ i3:

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

2020-06-02



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 2020-06-01 to 2020-06-02. During this period, RiskIQ analyzed 47,072 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 4,615 unique subject lines observed during the reporting period. The spam emails originated from 3,794 unique sending email domains and 6,684 unique SMTP IP Addresses. Analysts identified 158 emails which sent an executable file for Windows machines.

Top-25 Subjects

Test Rapido Covid 19	6440
The Corona Letter: India seeks to lower a drug's price	3152
CORONAVIRUS RELIEF FUND (CRF) 2020	2033
Covid19- Fund Compensation Notice./Paying Center	1278
Front Sight's Response to Nevada's Current COVID-19 Restrictions…	998
Products for COVID-19	954
Protejase del Covid-19, Productos Certificados	689
□□□□□□□□□□□□□□□□JAL□□□□□□□□□□ / JAL Groups' Latest Response to Covid-19	659
Re: Price Offer and Request for Quotation-Urgent (Stay Safe COVID-19)	616
Thank God we are save from Covid19	614
Re: COVID-19 Financial Relief Funds for you	595
Covid-19 Relief Funds	520
Coronavirus Relief,	468
COVID-19 EMERGENCY DELIVERY OF YOUR CONSIGNMENT BOX TODAY.	467
Caretas Faciales anti COVID - 19	458
Seminario: Nuevas Medidas Tributarias en Tiempos de COVID-19	419
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	391
AHORRA Dinero, Emprende y Protege tus espacios contra el Covid-19 con Productos Novedosos	382
Test Rápido prueba serológica Covid-19 $ 15.000	354
COVID-19 - Custom Projects | Mobile Application | SEO !! -etc [REDACTED_DOMAIN]	352
May "COVID-19" Philanthropies	321
Coronavirus : l'essai Discovery, un énorme fiasco ?, Covid : les signes à repérer sur votre peau	295
Covid-19 Compensation Relief Funds :	288
Protege tu espacio del covid-19	287
Paneles Divisorios Anticovid-19	261

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

trendingtopic.cl	6449
gmail.com	5997
timesofindia.com	3183
outlook.com	3136
163.com	1908
126.com	1475
medicproduction.com	1112
frontsight.com	998
hotmail.com	923
focazen.com	852

Top-15 IPs Sending COVID Spam

51.77.33.39	2095
177.23.28.38	2032
51.77.33.43	1888
51.77.33.44	1694
51.38.159.218	1351
91.212.153.94	1255
209.123.15.146	997
209.58.149.66	970
156.96.157.101	616
95.216.37.176	614

Top-15 Countries Sending COVID Spam

US	11854
FR	7780
CN	5416
IN	4556
BR	2734
--	1912
DE	1567
JP	1114
RU	839
AR	835

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

COVID-19 Update	154

Top-15 Subjects Containing doc/xlsx Files

Financial Accounting Impact of COVID-19- An In-depth Look at IFRS	20
Бесконтактная антивирусная ручка для двери! Решение против COVID-19 !	13
PROTEGE A TU EMPRESA FRENTE AL COVID	4
АИКБ настоява за изработване на законодателство и алгоритъм на действие при кризи от мащаба на COVID-19	3
COVID-19 y niños: pautas para las familias en la desescalada y cómo actuar si los menores requieren atención sanitaria	3
Please join me on June 3rd at 10 AM - Implications of Covid19 – Discussion with Allianz- Peter Lefkin, Senior Vice President, Government & External Affairs	3
Coronavirus - advice for the Third Sector across Lancaster District - Updated Monday 1st June 2020	3
NdP HomeExchange revela las cinco claves que marcarán el turismo post Covid-19	3
IFEMA arranca su actividad en julio 2020 con SICUR ESPECIAL COVID	2
NOTA | Diputado Ibáñez y Core Nataly Campusano, ofician por redirección de fondos del 6% Regional para financiar las últimas políticas de gobierno por Covid en Valparaíso.	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: 101,978
Domains with Potential Mail Servers: 3,047
Email-Capable Domains and Hosts: 38,815
Live Hosts and Domains Not Parked: 41,563

Mobile Apps

Apps in Official Stores: 282

by Store

Apple	163
Google	111
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 603

by Store Type:

Hybrid	358
Secondary	217
Affiliate	28

Blacklisted Mobile Apps: 19

by Store Type:

Secondary	18
Official	1