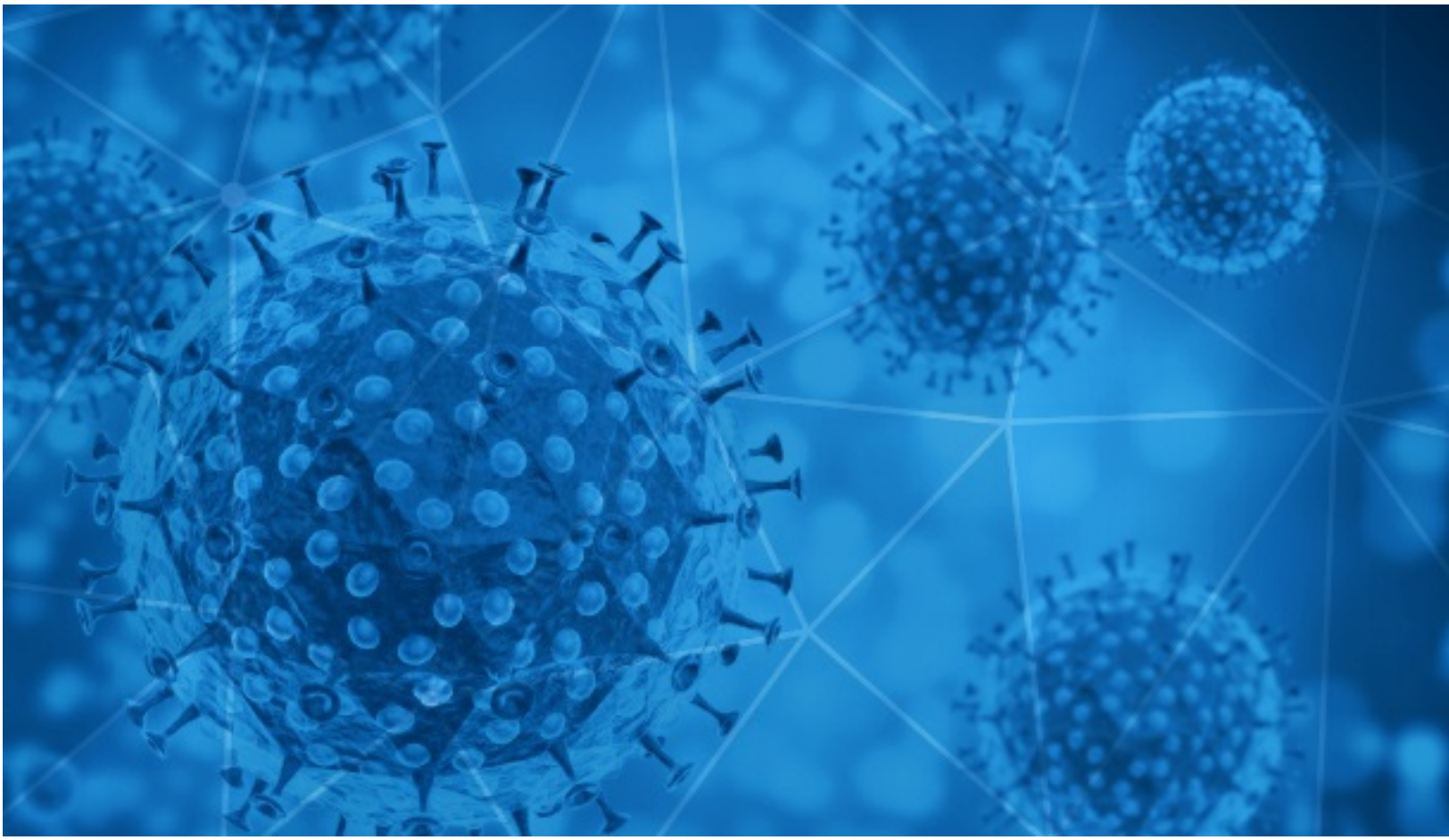
RiskIQ i3:

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

2020-07-17



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 2020-07-16 to 2020-07-17. During this period, RiskIQ analyzed 57,527 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,170 unique subject lines observed during the reporting period. The spam emails originated from 2,072 unique sending email domains and 4,316 unique SMTP IP Addresses. Analysts identified 3 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	25202
Trump, Pence Warn us About COVID-19 Hysteria	3833
The Corona Letter: Should India be worried as summer ends?	2595
CURSO BONIFICABLE (COVID-19 Prevención en el ámbito laboral)	1474
COVID-19 - Mobile App Development/ PHP, Magento, Drupal, E-Commerce -etc [REDACTED_DOMAIN]	1425
WOW!!! CONGRATULATIONS!!! You Won COVID19 PALLIATIVE ($1.5M)	1417
□□□□□□□□□□□□□□□JAL□□□□□□□□□□□□□□□□□/JAL Mileage Bank's Special Response to the Spread of COVID-19	1296
Second Wave of Covid-19	815
Insumos para Contingencia ANTI COVID-19	669
Re: How do we purchase after the COVID-19?	599
PyMEs contra el COVID19	549
COVID 19 SURVIVAL COMPENSATIONS	446
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	436
Beneficios Tributarios y Fiscalización SUNAT en tiempos Covid-19	352
Test Rapido Covid-19 Individual	341
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO ANTE EL COVID19	338
Control de Acceso y Temperatura Covid	330
Test Rapido COVID 19	301
Productos de Sanitizacion y prevencion Covid-19	284
Re: covid-19 protect products we can provide	278
Get Cover For Coronavirus	277
Let’s fight together to get through the COVID-19	246
Implacable contra el COVID-19 AMONIOX	237
Re: Against Coronavirus devices,should you interest?	230
Re: keep away from Covid-19	228

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	25205
surviving.buzz	3833
gmail.com	3050
timesofindia.com	2595
163.com	1786
aol.com	1514
foescof.es	1494
126.com	1369
jal.com	1298
trendingtopic.cl	1032

Top-15 IPs Sending COVID Spam

50.2.214.49	3833
146.255.98.204	1504
45.137.22.86	1417
185.24.233.65	790
157.119.122.136	614
103.225.53.70	543
103.225.55.52	516
103.225.55.181	496
103.225.55.222	480
103.225.55.126	465

Top-15 Countries Sending COVID Spam

JP	26637
US	5996
IN	4724
DE	4495
CN	3553
FR	1853
ES	1817
--	1521
AR	1256
IE	829

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Fw: Authorization for landing and departure of a chartered flight and exemption from Covid-19 test	1
Apresentação Ambipombal - Gestão de resíduos Hospitalares Grupo III e IV e COVID19 - Tabela de preços	1

Top-15 Subjects Containing doc/xlsx Files

Re:Covid-19 PO/882/18-19 DD 171218	53
Обучение педагогических работников по COVID-19	8
COVID-19 RELIEF FUNDING	3
Sinistra per Ravenna, Articolo Uno: il covid19 è un'opportunità per ripensare la sanità, una piattaforma per la ricostruzione del Sistema Sanitario Nazionale nelle sue articolazioni regionale e comunale	3
Anagha - information on Corona rakshak policy and request for approval	2
CORONA LETTER	2
Geldsparen beim Bus- und Bahnfahren & Engagement in Corona Zeiten & Sommerschule	2
La crisi legata al coronavirus non ha cambiato in modo permanente l'attitudine allo sport	2
TOWN OF OYSTER BAY COVID-19 FORM	2
DORO DONA 150 DISPOSITIVI AGLI ANZIANI GUARITI DA COVID-19 E DIMESSI DALL'OSPEDALE SACCO	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: 114,874
Domains with Potential Mail Servers: 2,811
Email-Capable Domains and Hosts: 43,501
Live Hosts and Domains Not Parked: 65,658

Mobile Apps

Apps in Official Stores: 348

by Store

Apple	187
Google	152
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 890

by Store Type:

Hybrid	565
Secondary	287
Affiliate	38

Blacklisted Mobile Apps: 22

by Store Type:

Secondary	19
Official	2
Hybrid	1