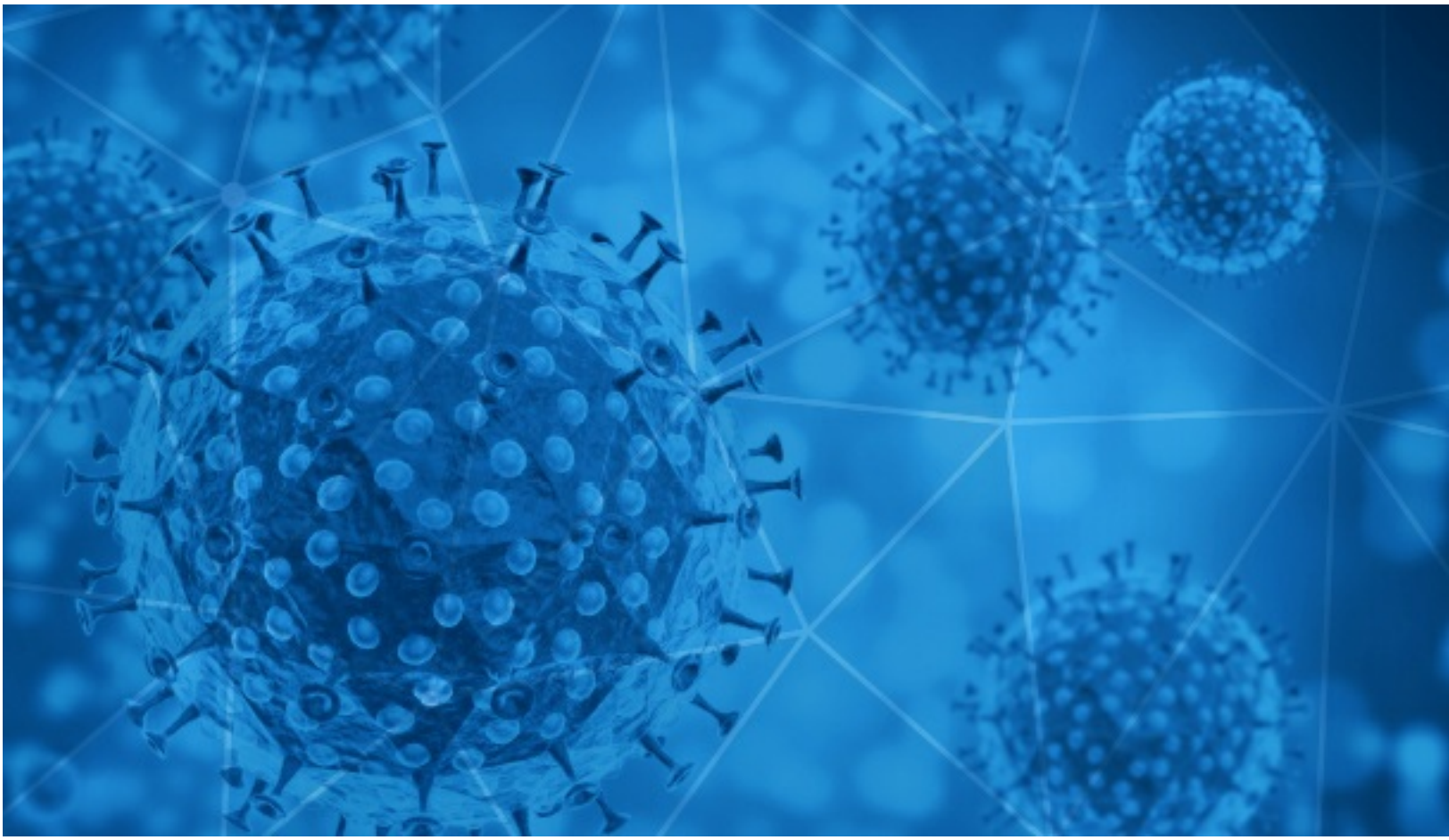
RiskIQ i3:

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

2020-07-16



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 2020-07-15 to 2020-07-16. During this period, RiskIQ analyzed 39,949 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,759 unique subject lines observed during the reporting period. The spam emails originated from 1,810 unique sending email domains and 3,915 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

COVID-19 Update: We are open and now offering Free Virtual Consultations	16150
The Corona Letter: Where cash works, cashless doesn't	1716
re: Test Rapido de Diagnostico COVID-19	1448
[REDACTED_DOMAIN] Notification: You Have (9) Pending Incoming Messages for redacted@threatwave.com (COVID-19 IS REAL!! STAY SAFE)	1208
Covid-19-Hilfsfonds	771
PyMEs contra el COVID19	719
Re: How do we purchase after the COVID-19?	577
CURSO BONIFICABLE (COVID-19 Prevención en el ámbito laboral)	461
States plead for a national coronavirus strategy, what to know about herd immunity, and more from Apple News	459
Second Wave of Covid-19	458
What to know about medical conditions and COVID-19	452
Test Rápidos Covid Entrega Inmediata	414
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	352
Test Rapidos COVID -19	345
Evita el Covid19 en tu lugar de trabajo	258
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO ANTE EL COVID19	255
Mantene tu lugar de trabajo libre de covid19	245
Test Rapido COVID 19	230
WSJ Torches COVID Hysteria Surrounding Schools	221
Re: covid-19 protect products we can provide	216
COVID-19 - Mobile App Development/ PHP, Magento, Drupal, E-Commerce -etc [REDACTED_DOMAIN]	216
Re: Against Coronavirus devices,should you interest?	209
Beneficios Tributarios y Fiscalización SUNAT en tiempos Covid-19	206
DPI linea fase3 covid-19 protezione e igiene	194
We Produce Covid-19 (Face Mask,Isolation Gown,Head/Shoe/Sleeve Cover,Vinyl Gloves ,PE Gloves,Apron)	183

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

wikimedia.org	16150
gmail.com	4404
timesofindia.com	1716
163.com	1596
countermail.com	1222
126.com	1082
trendingtopic.cl	515
foescof.es	464
insideapple.apple.com	459
gofundme.com	458

Top-15 IPs Sending COVID Spam

200.28.55.250	1448
172.93.189.66	801
202.90.240.33	699
113.118.173.77	624
146.255.98.204	470
95.211.211.232	446
185.24.233.65	442
45.137.22.86	370
68.183.25.199	353
119.122.89.21	339

Top-15 Countries Sending COVID Spam

US	10458
AU	4347
BR	3925
JP	3435
CN	3010
AR	2363
IN	2180
CL	1814
FR	1537
DE	1316

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Voluntárias que confeccionaram máscaras dão exemplos de amor na luta contra a covid-19	1

Top-15 Subjects Containing doc/xlsx Files

PPE items against Covid-19	7
Fwd: FW: Documents Required for PF Advance under COVID-19	2
NP- Los neumólogos advierten que España podría enfrentarse a un segundo brote significativo de coronavirus en un escenario muy diferente al del mes de marzo	2
Becas o aportes para capacitaciones en tiempos Covid-19 !!!!!!!	2
LEVANTAMIENTO DE CADAVER COVID 19. COM. ZARZUELA	2
COVID Test sites July 15 to 19	2
COVID-19 Task Force Meeting	2
EXISTENCIAS DEL COVID-19	2
Covid Update - Melbourne Metro and Mitchell Shire	2
Искусственный интеллект борется с Covid-19 в столичных клиниках	1

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: 114,749
Domains with Potential Mail Servers: 2,808
Email-Capable Domains and Hosts: 43,461
Live Hosts and Domains Not Parked: 66,373

Mobile Apps

Apps in Official Stores: 346

by Store

Apple	187
Google	150
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