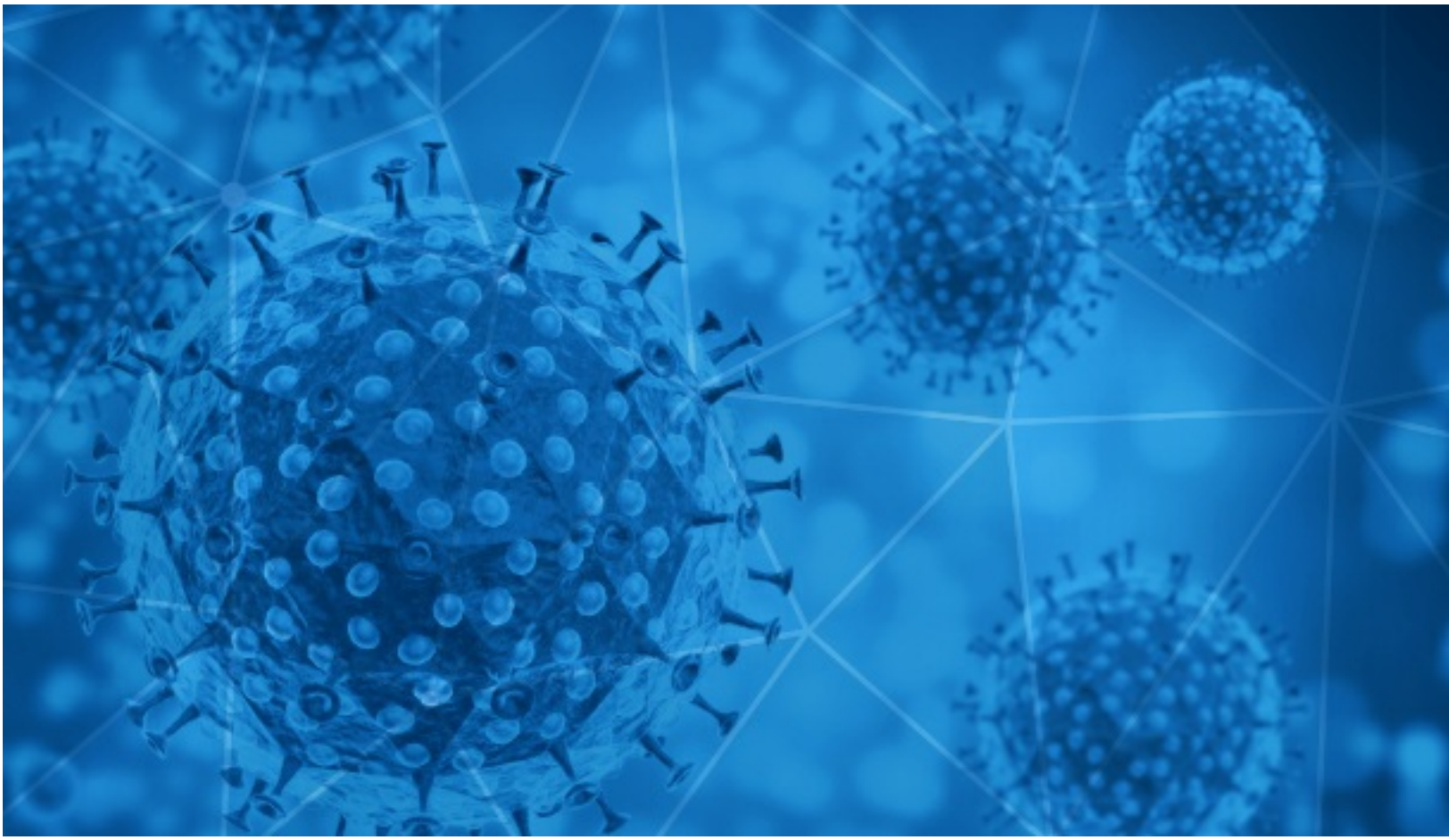
RiskIQ i3:

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

2020-07-27



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 2020-07-26 to 2020-07-27. During this period, RiskIQ analyzed 19,131 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,466 unique subject lines observed during the reporting period. The spam emails originated from 717 unique sending email domains and 1,780 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: When antigen and RT-PCR test results differ	2786
Covid Victims Compensation	1046
MICROSOFT COVID-19 RELIEF FUND - GLOBALGIVING	1026
PyMEs contra el COVID19	932
Please Notice: -Free provision of COVID-19 plasma -	610
247.. RECENT INFORMATION ABOUT COVID 19	567
Notice:4000 free provision of COVID-19 plasma in Korea	465
Protect Scores During Coronavirus	396
Credito para Capital de Trabajo FOGAPE COVID-19 - Conoce sus Historias	373
COVID-19 And Your Credit Health	360
Will COVID-19 Impact Your Credit Scores?	352
Incontri online in Italia (no corona)	314
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	292
BEST way to manifest money in a post-corona world	288
Como volver a la actividad post coronavirus?	278
Making money during the covid!	272
Secret Corona Cash Manifestation Formula	271
Cabinas para la prevencion del coronavirus?	268
Soluciones para la prevencion del covid19	244
China Supply Chain of COVID-19	227
Chinese protective products of COVID-19	212
Test Rapido COVID 19	208
Korea Trend News-COVID19(V5)	204
Re: coronavirus civil mask / Chinese qualified manufacturer	193
COVID-19 Lastest News	189

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

timesofindia.com	2786
gmail.com	2003
countermail.com	1722
alizathly.icu	1108
163.com	1084
microphilanthropies.com	1026
citromail.hu	685
126.com	615
mkldlhfkdh.work	610
manifsmagic.com	559

Top-15 IPs Sending COVID Spam

170.130.213.130	1108
201.231.10.183	1051
153.122.116.244	1046
164.163.167.2	1026
202.172.28.146	641
223.74.106.137	617
150.95.12.105	610
191.37.0.247	567
69.94.156.16	559
201.231.4.13	397

Top-15 Countries Sending COVID Spam

US	4132
IN	2854
JP	2332
AR	2026
CN	1963
BR	1849
DE	649
FR	554
KR	470
UA	369

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

MT CORONET CALLING AT PARADIP PORT - COVID -19 - HEALTH CLEARANCE	1

Top-15 Subjects Containing doc/xlsx Files

ANC Weekly COVID-19 Reports	9
Safety, Security at Work Training(Post Covid 19 Preparedness Course)	3
COVID-19 RELIEF FUNDING	3
COVID -19 DUTY SCHEDULE OF DNB/CPS RESIDENTS	2
info coronavirus	2
Gulf Coast Village Covid-19 Update	1
COVID Update July 26	1
REMITE REPORTE COVID 19 PERSONAL CAS DE LA EESTP-PNP-TRUJILLO DEL DOMINGO 26JULIO2020.	1
Fwd: COVID-19 Update - July 26	1
CONSOLIDADO DE LLAMADA CASO COVID-19	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: 116,375
Domains with Potential Mail Servers: 2,849
Email-Capable Domains and Hosts: 43,968
Live Hosts and Domains Not Parked: 65,781

Mobile Apps

Apps in Official Stores: 358

by Store

Apple	190
Google	159
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 922

by Store Type:

Hybrid	590
Secondary	293
Affiliate	39

Blacklisted Mobile Apps: 23

by Store Type:

Secondary	20
Official	2
Hybrid	1