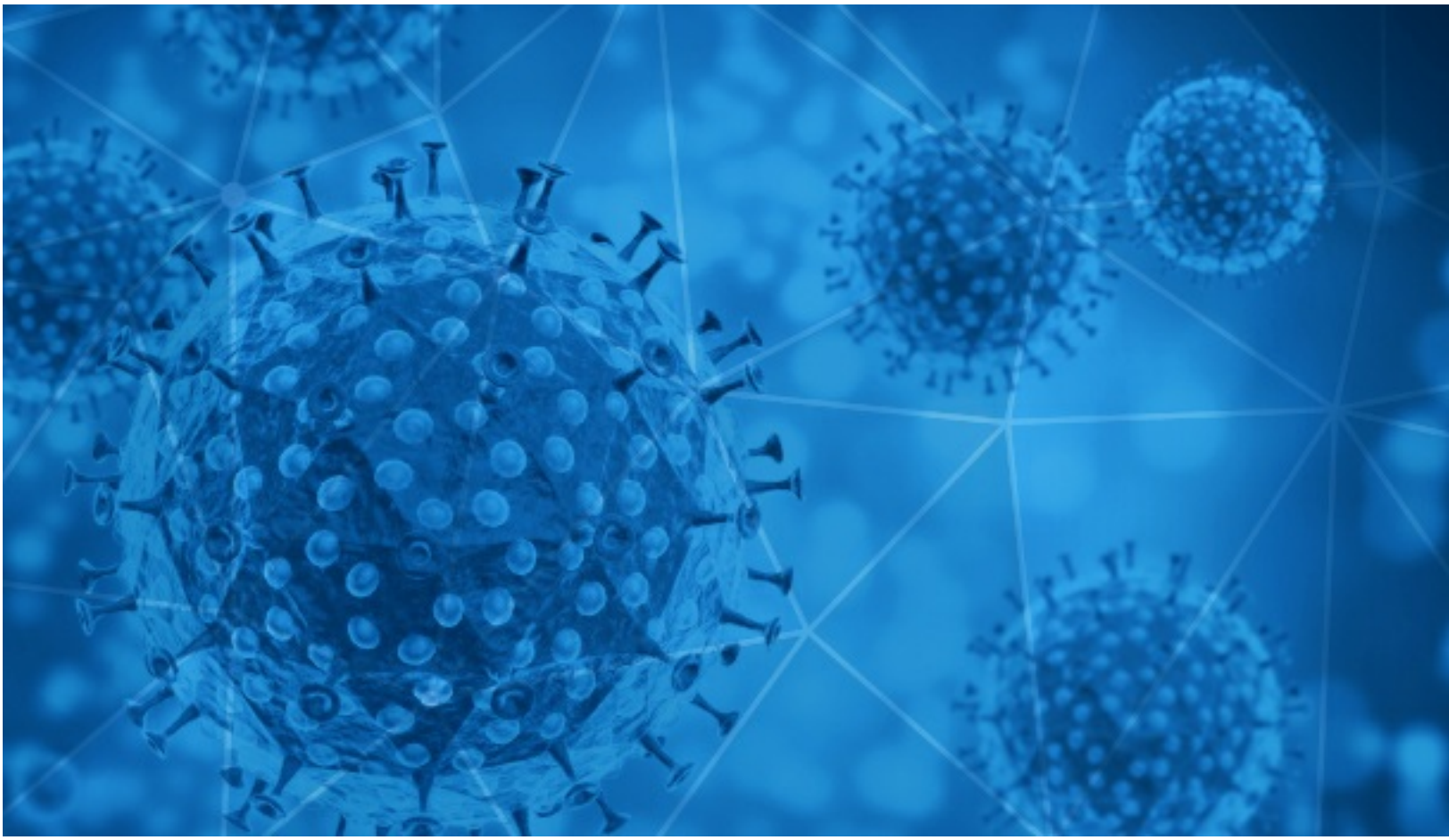
RiskIQ i3:

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

2020-09-29



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 2020-09-28 to 2020-09-29. During this period, RiskIQ analyzed 26,780 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,996 unique subject lines observed during the reporting period. The spam emails originated from 1,614 unique sending email domains and 3,469 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Why kids are left relatively untouched	3918
COVID-19 KILLED ANTHONY	1298
My COVID-19 Donation	1264
Limpieza y desinfeccion COVID 19	995
Reife Frauen zu Corona-Zeiten treffen	792
La cláusula rebus sic stantibus como remedio frente a los incumplimientos derivados del COVID-19	768
Test de deteccion rapida COVID19	684
Coronavirus (COVID-19) Funds Support.	603
Test Rápido Covid-19 Segunda Generación - 10.000 Un Entrega Inmediata	448
Beware of Malicious COVID-19 Phishing	403
Protégete RESPONSABLEMENTE Contra el Covid -19 / Los Mejores Precios	317
La mascarillas FFP2 y KN95, la mejor arma contra el COVID y los más de 10.000 contagios diarios, ¿tienes las tuyas?	292
Re: Corona virus Protection Pills.Order confirmation	287
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	252
VENETO: operativo il Fondo Anticrisi attività produttive, per la concessione di finanziamenti agevolati alle imprese coinvolte nella crisi da COVID-19, per iniziative finalizzate alla realizzazione di investimenti e interventi di supporto finanziario	252
How Etihad is using Covid-19 to make flying safer than ever | How Tata Steel is maximizing its IT investments	236
Let’s fight together to get through the COVID-19	227
Re: Your Covid-19 Relief Fund®	219
Mamparas de proteccion contra el coronavirus	211
COVID Antibody IgG + IgM test appointment time available at Just Rs.750, confirm before it expires.	203
Mamparas de proteccion COVID19	203
COVID-19 KILLED ANTHONY	197
Ref: COVIDï¿½19ï¿½2020ï¿½02	196
Register Now | Skills to learn for career growth amid COVID-19	190
Good morning, SA | Allegations mount against KwaSizabantu, how Ramaphosa reprimanded Mapisa-Nqakula, SA edges toward 700 000 Covid-19 cases	182

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	3918
gmail.com	2523
countermail.com	2094
hotmail.com	1415
sepin.es	845
126.com	795
data2web.de	792
yeah.net	712
solidarityfund.gov	622
updates.sba.gov	565

Top-15 IPs Sending COVID Spam

43.239.110.184	1263
112.49.34.2	1239
217.116.11.179	842
46.20.37.30	792
203.196.19.25	603
201.231.27.7	532
201.231.83.168	405
201.231.27.23	322
85.25.14.81	292
104.168.213.115	287

Top-15 Countries Sending COVID Spam

IN	5703
US	5450
CN	3846
AR	2148
DE	1763
ES	1265
BE	705
JP	671
FR	644
--	626

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

CORONA FLOR SRL	1

Top-15 Subjects Containing doc/xlsx Files

PHHS 9 28 2020 End of Day COVID 19 Report	7
COVID-19 Licenziamento del dirigente: specialità, soluzioni alternative, contenzioso Roma 18/11/20	6
=?ISO-8859-1?Q?El_uso_de_Radar_COVID_creci=F3_el_=FAltimo_mes_un_103%!? (MISSING)=	4
[Confed-ITA] CONFED-COVID SCHEME UPDATES	3
covid 19 health payment	3
PRODUCTOS COVID PARA EMPRESAS	2
[Arabic Press Release] تستضيف HWPL ندوة عبر الإنترنت لتعليم السلام من خلال ربط دول جنوب آسيا أثناء أزمة COVID-19	2
NdP PaynoPain: El pago contactless destrona al pago en efectivo en la era pos-COVID.	2
Urgent Covid information	1
corona; hoogrisico	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: 127,126
Domains with Potential Mail Servers: 2,895
Email-Capable Domains and Hosts: 48,087
Live Hosts and Domains Not Parked: 71,091

Mobile Apps

Apps in Official Stores: 435

by Store

Apple	220
Google	200
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,480

by Store Type:

Hybrid	816
Secondary	609
Affiliate	55

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1