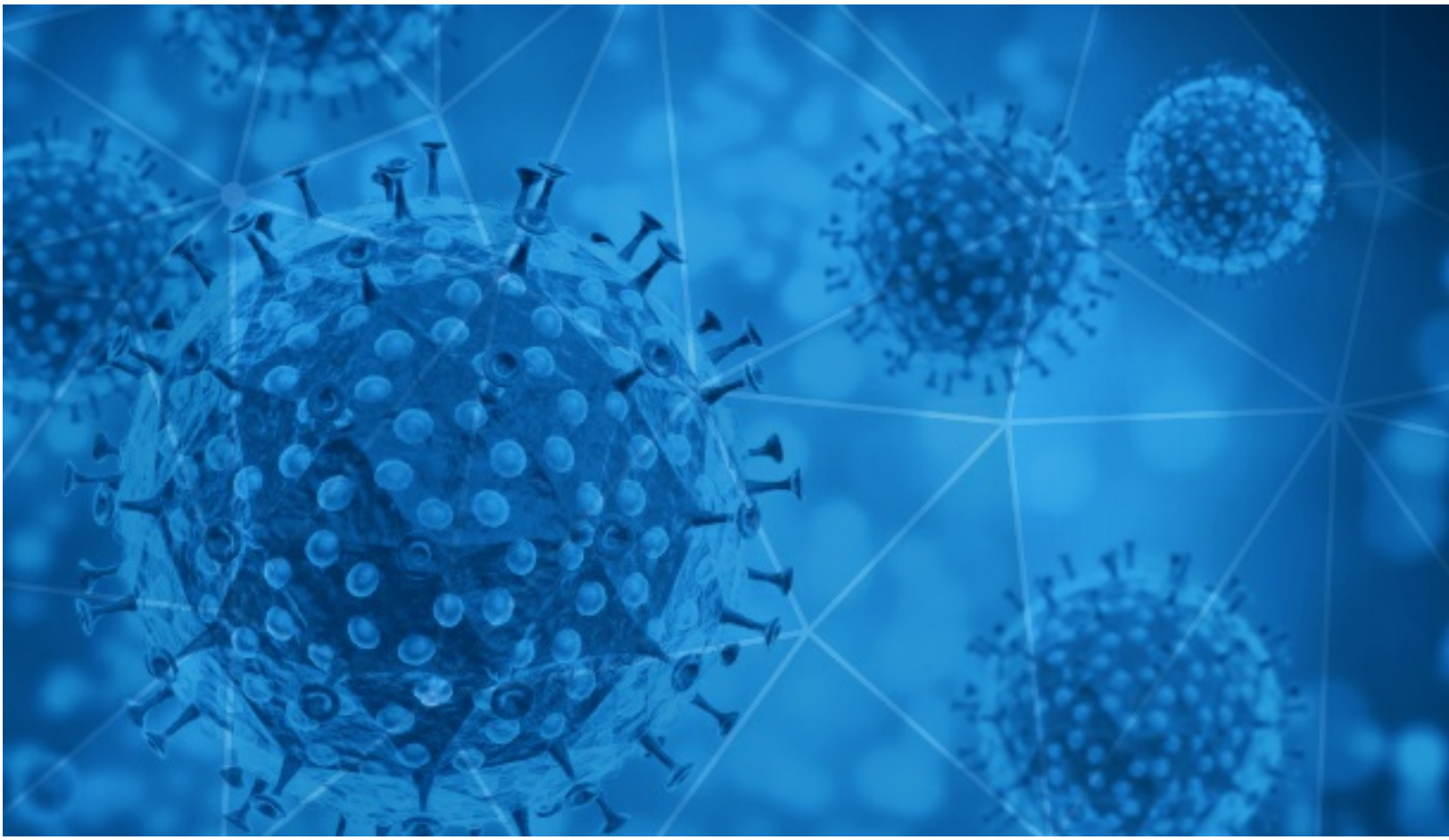
RiskIQ i3:

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

2020-12-28



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 2020-12-27 to 2020-12-28. During this period, RiskIQ analyzed 39,195 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,427 unique subject lines observed during the reporting period. The spam emails originated from 946 unique sending email domains and 2,322 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□	20147
The Corona Letter: Could a more contagious coronavirus be good news?	5200
URGENT - Apply Before NYE 2021 - Your Pre-Approval for Small Business Relief - COVID19	1680
Covid19 Pandemic Relieve Package	1053
Feeling Helpless Against Corona?	761
Trump's pardoning spree continues, COVID-19 reaches Antarctica, and more from Apple News	631
Trump issues a wave of pardons, the mysterious link between COVID-19 and sleep, and more from Apple News	598
SARDEGNA, FONDO RESISTO: prorogata al 30 dicembre 2020 la scadenza per i contributi a fondo perduto alle PMi e Grandi imprese sostenere le imprese e ilavoratori in conseguenza della sospensione o ridotta attività dovuta all'emergenza da Covid-19	459
Safety measures to stay protected against COVID-19	427
Offering N95 FACE MASK (3M 1860,1860S, Makrite 9500 N95,N95S,HARLEY, SAMPLING SWAB AND TUBE KITS,Novel Coronavirus (COVID-19) Test ,quick delivery in a couple days	417
COVID-19 - Pagamento necessario 27/12/2020	334
Let’s fight together to get through the COVID-19	315
Because of COVID-19 this year 2020 we have decided to give out £175,000.00 GBP	315
SPECIAL REPORT: How Brits Are Earning Millions From Home During Coronavirus Pandemic Thanks To Celebrity Chef Gordon Ramsay	309
Oferta de préstamo Covid-19	243
!You have won covid-19 palliative award fund €950.000,00 Euro!	208
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	204
Re: Digital signage solution for Covid-19	203
Sourcing Epidemic prevention products to Fight Against COVID-19	200
Re: covid-19 touch monitor	195
2020 was een rotjaar, maar voor hen nog iets meer - OVERZICHT. Dit verandert op 1 januari - Coronamaatregelen in voetbal missen effect niet	141
"Coronavirus and how it affects children"	137
New Covid-19 e-book and how to keep your children safe	129
COVID-19 Chinese protective products	121
United Nations 2020 Covid-19 Compensation Payment.	110

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

epc-store.com	20150
timesofindia.com	5207
batecatings.top	1678
insideapple.apple.com	1229
mail.hcancerbarretos.com.br	1053
akbtoine.maison-desmarques.fr	761
gmail.com	688
163.com	538
italiacontributi.it	459
icicipruli fe.com	427

Top-15 IPs Sending COVID Spam

63.80.89.142	1678
138.219.221.50	1053
103.225.54.79	727
103.225.55.79	591
103.225.52.179	521
46.254.37.34	459
103.225.54.92	444
103.225.55.215	438
103.225.52.69	438
103.225.52.249	429

Top-15 Countries Sending COVID Spam

JP	20180
US	6615
IN	5673
CN	1299
RU	1153
BR	1072
DE	607
IT	512
BE	322
GB	289

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

FW: «Η επιστήμη, η συνεργασία και η λογική κέρδισαν το στοίχημα» δήλωσε ο Πρόεδρος της Βουλής μετά τον εμβολιασμό του κατά του κορωνοϊού Covid-19	9
Buletin de presa 27.12.2020 + comunicat actiuni COVID19	2
CCS 10961 Reporte estatal COVID-19: 44,448 contagios y 4,199 fallecimientos	2
COVID 19 Natore(27.12.2020)	1
NP- Minsa: Ciclistas se unen a campaña 'No bajemos la guardia ante la COVID-19'	1
Fwd: CVASU COVID-19 Testing lab report on 27/12/2020	1
RV: Alcance Altas pacientes covid	1
corona sample from rajoir	1
NP- Médicos del Hospital Loayza operan a pacientes COVID-19 con estrechez de tráquea por intubaciones prolongadas	1
IMSS Boletín 860.-Trabajo Social del IMSS acerca fiestas decembrinas a pacientes con COVID-19 (LINK DE VIDEO Y FOTOS)	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: 137,673
Domains with Potential Mail Servers: 2,598
Email-Capable Domains and Hosts: 52,458
Live Hosts and Domains Not Parked: 47,975

Mobile Apps

Apps in Official Stores: 497

by Store

Apple	244
Google	237
WindowsPhone	15
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,953

by Store Type:

Hybrid	1002
Secondary	891
Affiliate	60

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1