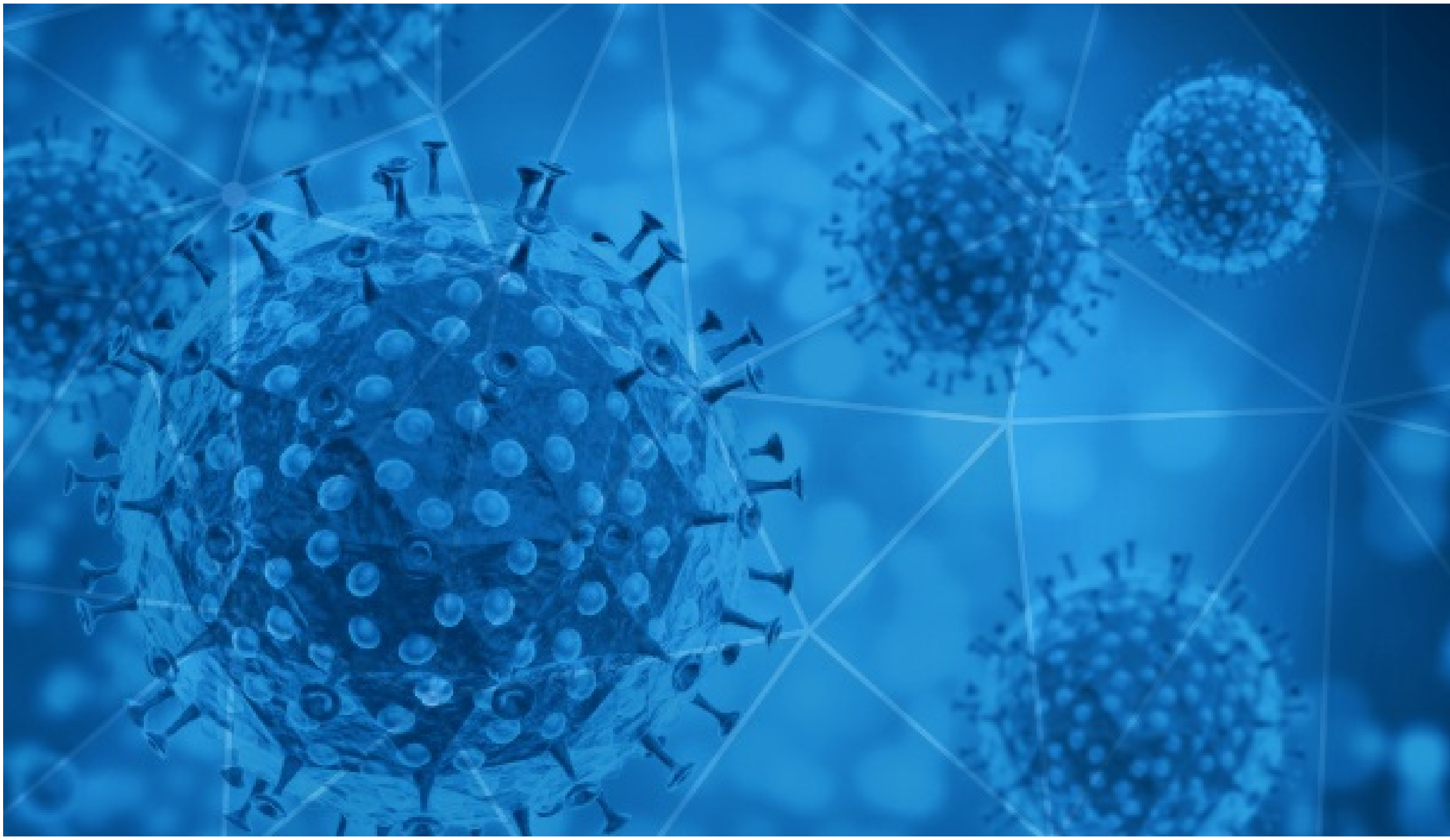
RiskIQ i3:

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

2020-12-10



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 2020-12-09 to 2020-12-10. During this period, RiskIQ analyzed 35,429 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,348 unique subject lines observed during the reporting period. The spam emails originated from 2,140 unique sending email domains and 4,553 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

Ingresaron TEST COVID19 de deteccion rapida	6358
The post-Thanksgiving surge is here, Biden's COVID-19 plan for his first 100 days, and more from Apple News	3870
The Corona Letter: Did denialism hamper India's pandemic response?	3545
Fwd: Comunicacion Urgente - COVID-19	1467
COVID-19 Relief Support.	1251
Puricador y Sanitizador de Aire, Estirilizacion contra Coronavirus	1124
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	1020
Benefício Liberado - COVID 19	646
Re: Defeat Coronavirus, non contact fever alarm device	603
Respuestas gerenciales para el post Covid19	561
Contactless infrared body temperature thermometer defeat Coronavirus	544
testy na covid-19	435
Re: Corona virus Protection Pills.Order confirmation	394
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	358
Puricador y Sanitizador de Aire, Estirilización contra Coronavirus	316
::: REG-#Season greetings [REDACTED_DOMAIN] #COVID-19*Relief Funds_From "WHO"::::	281
Corona virus (Covid19) Bailout Fund	259
Feedback on Impact of RBI COVID 19 measures on Home Loan	221
[CND Español - 4290]. #CNDEscucha conversa con Antonio Carricarte Corona	209
LIVE Executive Fireside Chat: Adapting to the Accelerated Demand for Data & Cloud in a Post-COVID World	186
Safety measures to stay protected against COVID-19	185
COVID-19 results in 15 minutes	183
Protégez-vous du Covid avec SOLUGERM France	163
Let’s fight together to get through the COVID-19	143
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove...etc.	140

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

grupolylsalud.com	6358
insideapple.apple.com	3879
timesofindia.com	3551
mscbs.gob.es	1467
hotmail.com	1343
keyable.net	1147
trendingtopic.cl	1124
gmail.com	782
ourvaluedcustomer2pjdrewardsrready.com	681
pactoeml.com.br	600

Top-15 IPs Sending COVID Spam

181.239.232.96	6350
82.85.174.28	1247
113.116.205.232	1057
201.48.13.68	600
51.83.246.187	591
51.83.246.186	433
67.219.150.138	394
139.99.122.199	281
201.231.6.107	270
177.11.0.13	259

Top-15 Countries Sending COVID Spam

US	10673
AR	7009
IN	4382
CN	2101
FR	1868
IT	1681
UA	1471
BR	1091
GB	882
PL	587

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

Herramientas tecnológicas serán fundamentales para una distribución eficiente de la vacuna contra el Covid-19	3
NUEVA FORMACION COVID PARA EMPRESAS	3
Nota stampa - IL NATALE DEGLI ITALIANI AI TEMPI DEL COVID, MERITATI “AUTO-REGALI” E IL PIACERE RITROVATO DI STARE CON AMICI E PARENTI: ECCO L’ANTIDOTO AL 2020	2
CCS /10809 Implementa GOAN política común contra COVID en 9 estados	2
CCS /10812 Reporte COVID-19: 41,215 casos acumulados y 3,826 personas fallecidas en el estado	2
Registro online per SIBONO LUCA - Avviso - Comunicazione _70G - Informativa Covid19 classe III SSIG	1
Nota: Mesa Covid-19 de Arica y Parinacota prepara plan de mitigación ante Navidad y Año Nuevo	1
RE: REPORTE COVID PEDREGAL	1
LCL Realty: Covid 19 New Office Regulations	1
COVID-19 Situational Awareness	1

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: 135,567
Domains with Potential Mail Servers: 2,610
Email-Capable Domains and Hosts: 51,645
Live Hosts and Domains Not Parked: 44,867

Mobile Apps

Apps in Official Stores: 482

by Store

Apple	243
Google	224
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,869

by Store Type:

Hybrid	968
Secondary	842
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1