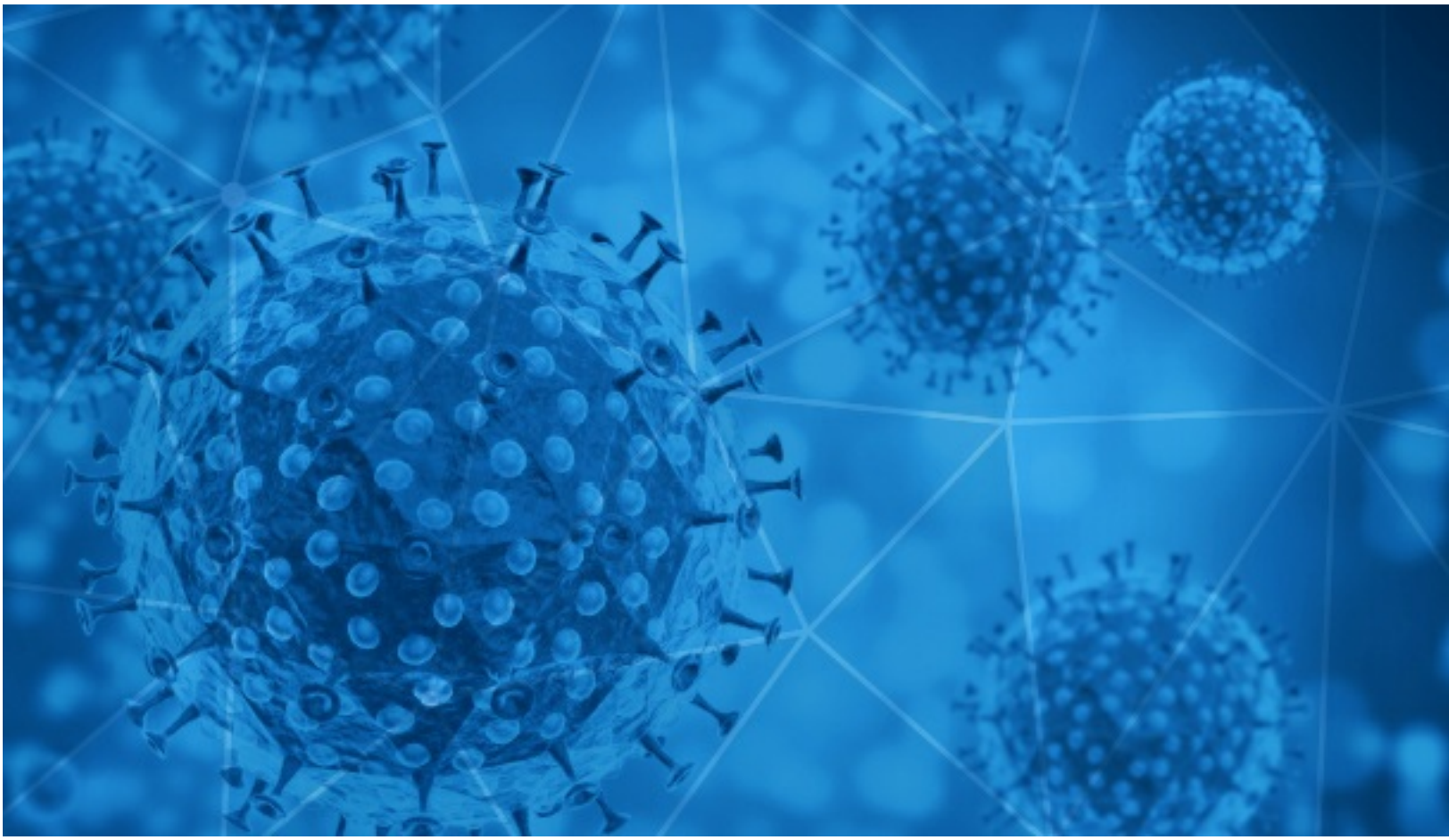
RiskIQ i3:

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

2020-12-17



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 2020-12-16 to 2020-12-17. During this period, RiskIQ analyzed 54,559 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 4,343 unique subject lines observed during the reporting period. The spam emails originated from 2,353 unique sending email domains and 4,611 unique SMTP IP Addresses. Analysts identified 4 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	18803
COVID FUNDS	6524
The Corona Letter: Preparing for a vaccine's adverse fallout	3919
VA releases COVID-19 vaccine distribution plan, vaccinations began this week	1416
Ingresaron TEST COVID19 de deteccion rapida	1125
Agevolazione Flyingmailers per l'Emergenza COVID-19 | Fai sapere che ci sei!	1039
Re: Covid-19 Donations..	857
Respuestas gerenciales para el post Covid19	784
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	769
Oportunidad de Cumplimiento de Ley de SST y Plan COVID-19	651
Gran Venta Outlet - Productos Covid 19	447
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	439
ABBOTT PANBIOâ¢: Recoleccion de muestra nasofaringea COVID-19	421
IMF COVID19 PAYMENT	418
have you received your 1 million euro Covid-19 Relief Fund? email us now to get it	334
Get your Corona-virus Mask while supplies last!	302
Traveling soon, wear this mask to fight chances of getting Corona-virus	296
Reduce your risk of Corona-virus with this Mask	293
New Corona-virus Mask!	291
UNITED NATIONS COVID19 RELIEVE SCHEME	272
Reserve Your Seat. Building a career in IT in the post-Covid world	268
4 Ways to Grow Your Beauty Business During COVID-19	263
Re: Defeat Coronavirus, non contact fever alarm device	254
Contactless infrared body temperature thermometer defeat Coronavirus	238
Let’s fight together to get through the COVID-19	226

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	18803
gmail.com	7366
timesofindia.com	3926
messages.va.gov	1450
zohomail.eu	1275
clrvisor.com	1182
grupolylsalud.com	1125
flyingmailers.com	1039
hdfcbank.net	982
walla.co.il	784

Top-15 IPs Sending COVID Spam

103.99.1.130	6524
187.63.183.27	1191
69.94.152.246	1181
181.239.232.123	1122
85.17.15.45	1038
103.225.55.82	670
103.225.52.143	582
103.225.52.183	558
107.158.43.22	553
103.225.53.252	440

Top-15 Countries Sending COVID Spam

JP	18942
US	10676
VN	6539
IN	5320
AR	2045
BR	1652
CN	1581
NL	1478
GB	981
IT	848

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Pfizer-BioNTech Covid-19 Vaccines First Interim	3

Top-15 Subjects Containing doc/xlsx Files

Ocena ryzyka zawodowego (aktualizacja pod względem COVID -19) / ZUS w praktyce	4
Two Positive Cases of COVID-19	3
KPMG. Informe Energías Renovables y COVID-19. Dic 2020	2
AISLAMIENTO DE PERSONAL POLICIAL POR COVID-19.	2
CCS/10880 Urge Alianza Federalista al Presidente una estrategia nacional eficaz e incluyente en vacunación contra COVID-19	2
Reduced Pricing on 3 Ply Masks, KN95 Masks, Sanitizer and other COVID related items REDUCED AT MSC	2
Fwd: Informe Covid vitamina D	2
COMUNICAZIONE SU COVID	2
Tres de cada diez españoles han cambiado de vivienda o tienen previsto hacerlo por la COVID-19	2
Buletin de presa 16.12.2020 + comunicat actiune COVID	2

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: 136,539
Domains with Potential Mail Servers: 2,620
Email-Capable Domains and Hosts: 51,972
Live Hosts and Domains Not Parked: 45,706

Mobile Apps

Apps in Official Stores: 490

by Store

Apple	245
Google	230
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,901

by Store Type:

Hybrid	977
Secondary	865
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1