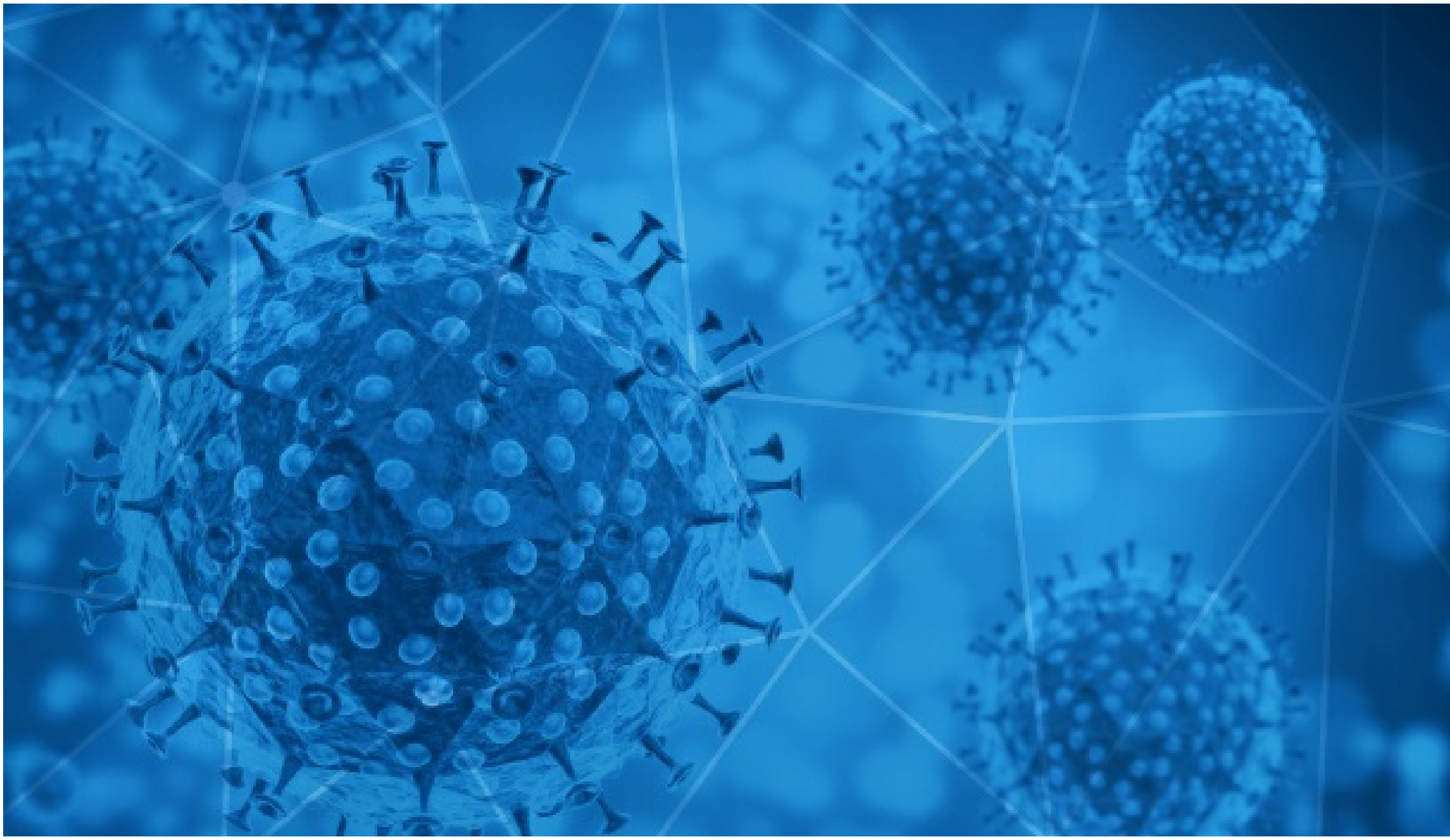
RiskIQ i3:

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

2021-01-08



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

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 2021-01-07 to 2021-01-08. During this period, RiskIQ analyzed 36,293 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,448 unique subject lines observed during the reporting period. The spam emails originated from 2,294 unique sending email domains and 4,588 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

⚠️ New Coronavirus Strain!	8021
The Corona Letter: More worry about the South African strain	3946
Covid-19 Relief F und	3744
COVID-19 Update: We are open and now offering Free Virtual Consultations	1271
Gran Venta Outlet - Productos Covid 19	1079
New Corona-virus Mask!	854
Reduce your risk of Corona-virus with this Mask	834
Traveling soon, wear this mask to fight chances of getting Corona-virus	820
Covid-19 Pandemic Relief Program	779
Get your Corona-virus Mask while supplies last!	771
Redeem Your R18,000.00 Covid-19 Relief Funds instantly	407
Let’s fight together to get through the COVID-19	406
UN COVID-19 RELIEF FUNDS APPROVED	404
Contactless infrared body temperature thermometer defeat Coronavirus	384
HERZLICHEN GLÜCKWUNSCH, CASH COVID-19 PALLIATIVEN AUS MEINEN LOTTERIEGEWINNEN	375
Re: Defeat Coronavirus, non contact fever alarm device	351
COVID-19 Financial Support/Loan Program.	321
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.	292
Good Morning, SA | Covid conspiracy headache for the ANC, business owners suffer emotional stress	176
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	170
NCJ Daily - Huffman on Locking Down Amid the Capitol Riot. 30 New COVID Cases. A New Health Order. WaPo Takes on Brius.	167
Test Covid Per Farmacie - Sierologici e Antigenici	157
Corona-Update: Wirtschaft in Not! | Mit Empathie bei der Belegschaft punkten | Die Unternehmensnachfolge richtig regeln	151
COVID-19 Vaccination Registration - Confirmation	117
PowerSurge - January 7 - Charging station anxiety, Fighting COVID 19, Predictions for 2021 and more …	107

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

printchainmarketing.co.uk	8021
timesofindia.com	3952
xcontrol.it	3744
clevisor.com	3279
gmail.com	2263
standardbank.co.za	821
akhirawahdnshaamolananjibobih.com	739
keyable.net	735
163.com	663
akhirawahdanshaamolananjibobih.com	458

Top-15 IPs Sending COVID Spam

69.94.156.43	3277
157.245.42.150	2788
193.169.212.59	2088
193.169.212.58	2046
193.169.212.61	1960
193.169.212.60	1927
159.203.20.65	956
185.43.108.196	821
113.116.207.77	614
212.118.12.44	394

Top-15 Countries Sending COVID Spam

US	12919
DE	8612
IN	4214
CN	2369
CA	1295
FR	922
GB	875
JO	777
CL	586
UA	461

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

[sjbm.premium] SFM -> Etude flash VOC-UK et CHU demande conseil scientifique COVID19	1

Top-15 Subjects Containing doc/xlsx Files

Dwudniowy kurs Kadry i płace w dobie COVID 19 - szkolenie on-line	11
Rezultate campanie donare plasma convalescenta COVID-19	5
COVID-19 Vaccination	5
Positive Cases of COVID-19: 01/06/21	4
*****NEW Rapid COVID-19 Results***COVID-19 Rapid Antigen Tests for $29 each**	3
COMUNICADO Vacunas y vacunación contra Covid-19: respuestas a algunas dudas frecuentes	2
Session follow-up materials: Nursing Home COVID-19 Network ECHO Conference 1/7/2021	2
Revue de la disponibilité des intrants de lutte contre le VIH, la Tuberculose, le Paludisme et de l'utilisation des Equipements de Protection Individuelle dans le contexte de la COVID 19	2
COMUNICADO AFADHYA - NUEVAS MEDIDAS DE RESTRICCIÓN Y POSIBLE CIERRE DE LOCALES - CORONAVIRUS	2
Press Release: COVID-19 Vaccine Logistics Chain Reliability and Compliance - Order# 52357446	2

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: 138,761
Domains with Potential Mail Servers: 2,564
Email-Capable Domains and Hosts: 52,854
Live Hosts and Domains Not Parked: 53,885

Mobile Apps

Apps in Official Stores: 496

by Store

Apple	241
Google	239
WindowsPhone	15
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,997

by Store Type:

Hybrid	1027
Secondary	909
Affiliate	61

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1