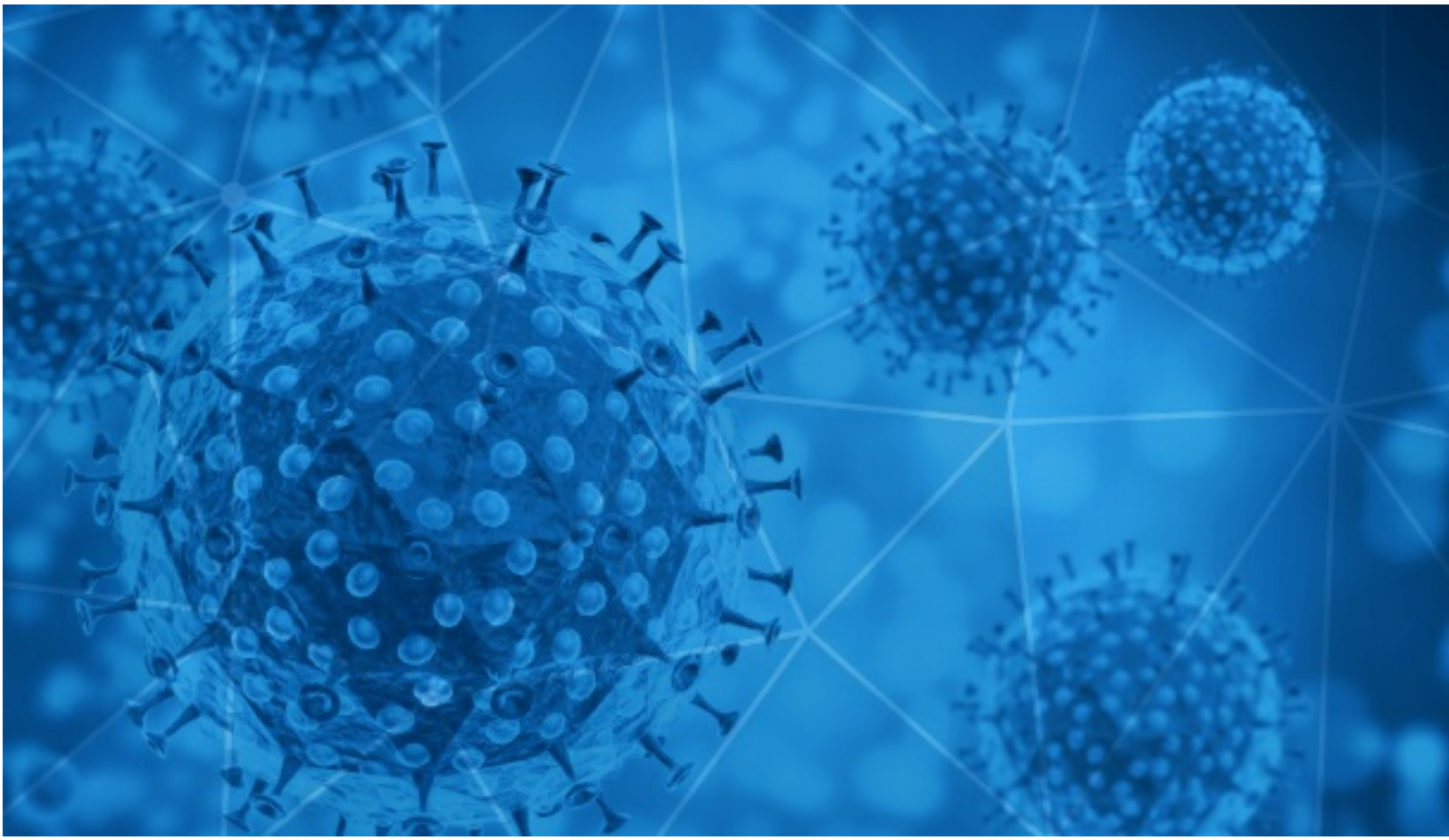
RISKIQ®

RiskIQ i3:

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

2020-12-23



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 2020-12-22 to 2020-12-23. During this period, RiskIQ analyzed 27,769 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,092 unique subject lines observed during the reporting period. The spam emails originated from 2,051 unique sending email domains and 3,588 unique SMTP IP Addresses. Analysts identified 5 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Do we need a bigger first list for vaccines?	3452
Check out "JOE BIDEN TAKES THE COVID 19 VACCINE" on Wane Enterprises	1884
Important update on COVID-19 vaccines	1580
"Coronavirus and how it affects children"	1057
Covid-19 Relief Details	994
New Covid-19 e-book and how to keep your children safe	956
Check out our new e-book about Covid-19 and how it affects your children	819
Ingresaron TEST COVID19 de deteccion rapida	538
Dieses Covid-Spezialpaket wird geliefert	497
Oportunidad de Cumplimiento de Ley de SST y Plan COVID-19	488
Beanspruchen Sie Ihr Operation Covid-Paket	447
TCS is turning Covid-19 into its biggest opportunity | India Inc bullish to take HR functions to cloud	279
Full COVID19 Protection- KN95 Masks Are Being Restocked With Virus Numbers Rising	278
COVID-19 - Earn $4.510 from home	276
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	272
LJC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation	256
COVID-19 Impact on Banking and Financial Services	227
Soy Camila Cid, representante de la marca de alcohol gel Como Te Odio Corona.	212
BREAKING NEWS: Dick Smith Reveals How to Profit from Coronavirus	198
Let’s fight together to get through the COVID-19	189
Prueba Rapida para Descarte de COVID-19 a Solo 24.90	188
COVID19 Testing Made Easier- No More Nose Swabs Or Painful Needles	184
No COVID Pain Testing- Detect C0VID19 Using This Simple Tool That Clips To Finger	180
Opportunity Knocks: How You Can Make Money From VideoTours 360 During Covid-19	180
Promoción Insumos Covid-19 Especial Para Empresas	174

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	3457
electronicemail.com	2832
waneenterprises.com	1884
subscriptions.cms.hhs.gov	1629
xcontrol.it	1000
aol.com	948
gmail.com	550
grupolylsalud.com	538
focazen.com	488
volta-investments.com	401

Top-15 IPs Sending COVID Spam

85.25.110.28	2832
69.55.59.220	931
181.239.232.123	538
165.22.75.121	492
51.79.142.8	452
194.116.229.176	278
131.0.103.220	256
194.116.229.179	227
70.32.77.141	227
219.65.85.29	216

Top-15 Countries Sending COVID Spam

US	12021
IN	3952
DE	3205
FR	1074
CN	1019
AR	873
GB	843
--	815
IT	530
NL	374

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

COVID-19 Update	1

Top-15 Subjects Containing doc/xlsx Files

Δελτίο Τύπου: Υπερψηφίστηκε η διάταξη του ΥπΑΑΤ, Μ. Βορίδη - Ακατάσχετες και αφορολόγητες εφεξής οι ενισχύσεις Covid-19 που λαμβάνουν οι Έλληνες αγρότες	3
Four Positive Cases of COVID-19:	3
Buletin de presa 22.12.2020 + comunicat actiuni COVID19	2
Fwd: Covid test report 20/12/2020_CVASU_Chittagong	2
ATORP achieves Intertek's Certification on Business Continuity Management to demonstrate its resilience amid COVID-19 pandemic	2
Bekannt aus den Medien - Livinguard Pro Mask - antivirale Gesichtsmaske mit 95% Filter - FFP2-Masken, Covid-19 Schnelltests etc.	2
Re: Covid-19 Protocols & Virtual Consultation	2
Fwd: Covid test report 22/12/2020_CVASU_Chittagong	2
CCS/10922: Agradece Chihuahua a todo el equipo que trabajó en hospitales móviles contra COVID-19	2
Seimo nario Mindaugo Puidoko pranešimas: „Seimo laikinoji darbo grupė imasi spręsti sveikatos paslaugų prieinamumo problemas per COVID-19 pandemiją“	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: 137,254
Domains with Potential Mail Servers: 2,602
Email-Capable Domains and Hosts: 52,296
Live Hosts and Domains Not Parked: 47,415

Mobile Apps

Apps in Official Stores: 493

by Store

Apple	245
Google	233
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,930

by Store Type:

Hybrid	987
Secondary	884
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1