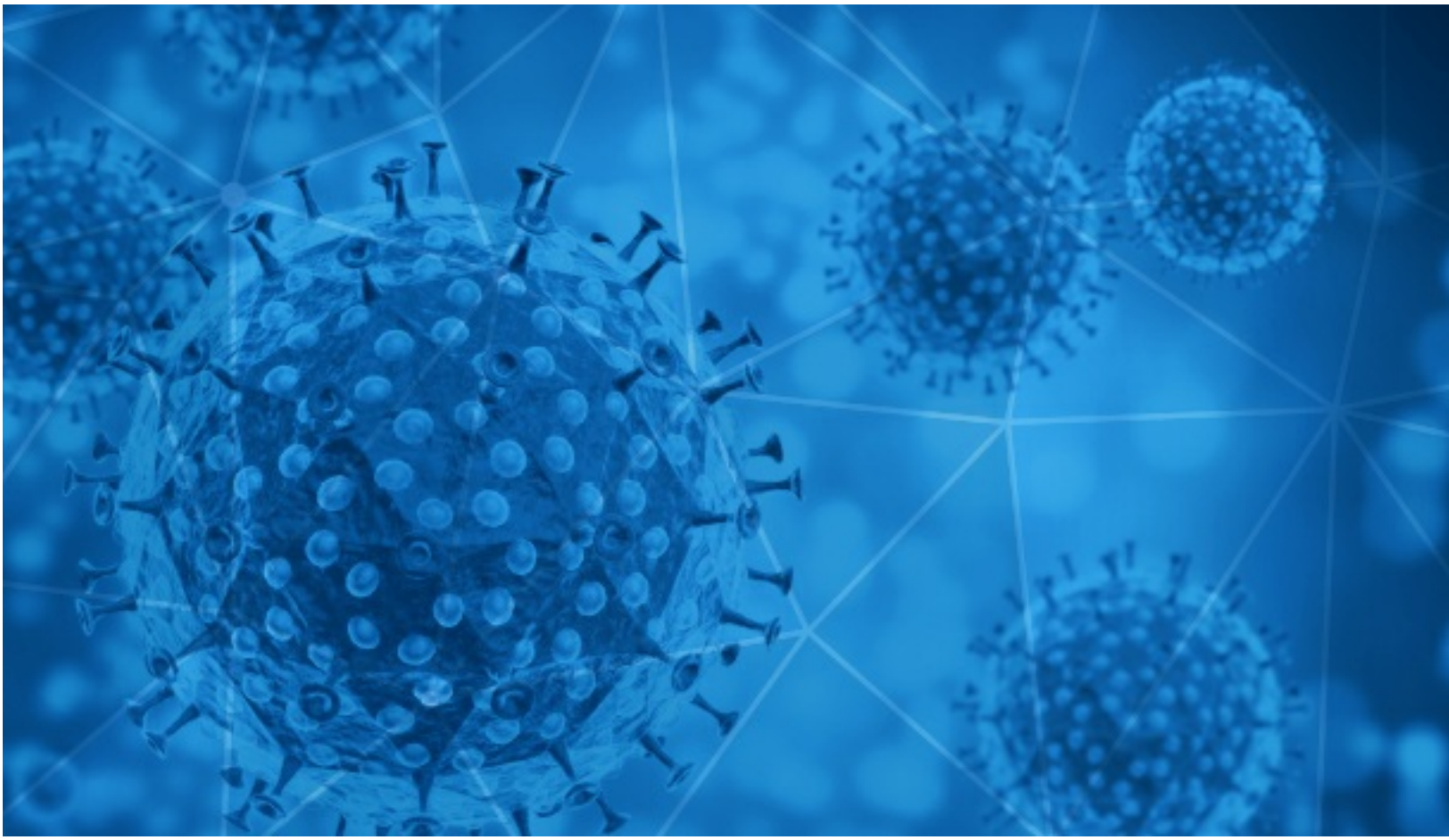
RiskIQ i3:

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

2020-12-01



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 2020-11-30 to 2020-12-01. During this period, RiskIQ analyzed 25,060 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,604 unique subject lines observed during the reporting period. The spam emails originated from 2,295 unique sending email domains and 4,162 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: A case for a shorter isolation period	2847
How Thanksgiving gatherings will affect the pandemic, a COVID-19 crisis in the NFL, and more from Apple News	2827
Ingresaron TEST COVID19 de deteccion rapida	2585
Corona virus (Covid19) Bailout Fund	865
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	780
Cuomo tells hospitals 2 recruit retired doctors NOW & warns he may reinstate lockdown as COVID soars	767
Covid test for exiting employees	578
Respuestas gerenciales para el post Covid19	534
Re: COVID-19 - Projects| Website | Mobile Application | E-Commerce | SEO (Results Guaranteed) [REDACTED_DOMAIN]	415
Contactless infrared body temperature thermometer defeat Coronavirus	356
Re: Defeat Coronavirus, non contact fever alarm device	341
Mi seguro insumos covid 19 protege a tu familia	338
Adopt These 6 New Habits & Stay Safe from COVID - 19	312
Descuentos Sobre Descuentos en Productos Covid!	301
Re: Digital signage solution for Covid-19	253
All New Portable UV Wand, Help Protect Your Family From COVID-19 50%!O(MISSING)ff Cyber Monday	239
With COVID On The Rise, Protect Yourself And Your Family With All New UV Wand	196
Managing the Remote Workforce During Covid-19: Policies, Procedures, and Practices	193
Re: COVID-19 RESPONSE FUND	191
Let’s fight together to get through the COVID-19	182
The Morning: The path of Covid deaths	180
Gran Venta Outlet - Productos Covid 19	176
Descuentos sobre descuentos en productos Covid !!!	165
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	151
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.	146

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

insideapple.apple.com	2923
timesofindia.com	2853
grupolylsalud.com	2585
gmail.com	1137
bknegaraindonesia.com	856
caribbeanfever.com	767
keyable.net	697
walla.co.il	534
163.com	467
vincentjoiner.com	437

Top-15 IPs Sending COVID Spam

181.239.232.96	2585
177.11.0.13	865
113.89.41.148	696
194.146.47.137	435
157.119.121.104	341
190.247.240.170	313
165.227.203.111	289
198.199.67.196	289
104.248.10.217	204
212.227.254.175	193

Top-15 Countries Sending COVID Spam

US	9785
IN	3474
AR	3310
CN	1719
BR	935
GB	756
DE	729
--	681
FR	633
IT	361

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

Apply For An Affordable Loan at 4% For COVID-19 support	16
Apply For An Affordable Loan at 4%!F(MISSING)or COVID-19 support	6
NOTA. FELGTB alerta de que hay diagnósticos por VIH que se están atendiendo tarde debido a la pandemia de la Covid-19	4
NUEVA FORMACION COVID PARA EMPRESAS	3
Еще 4000 человек сдали плазму крови для лечения COVID-19 в Южной Корее. Пресс-релиз, фото.	3
Notice No. 1764: Confirmed Case of COVID-19 Infection in Discovery Bay	3
6.ONLINE FORTBILDUNG Krankheitsverläufe von Corona	2
RESULTADO - COVID -19	2
RV: U071 POSITIVO COVID 19 U/O 23-27 DE NOVIEMRE 2020	1
Re: NMM COVID19 Surveillance report @ 26 Nov 2020	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: 134,389
Domains with Potential Mail Servers: 2,615
Email-Capable Domains and Hosts: 51,239
Live Hosts and Domains Not Parked: 45,681

Mobile Apps

Apps in Official Stores: 477

by Store

Apple	240
Google	222
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,823

by Store Type:

Hybrid	940
Secondary	824
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1