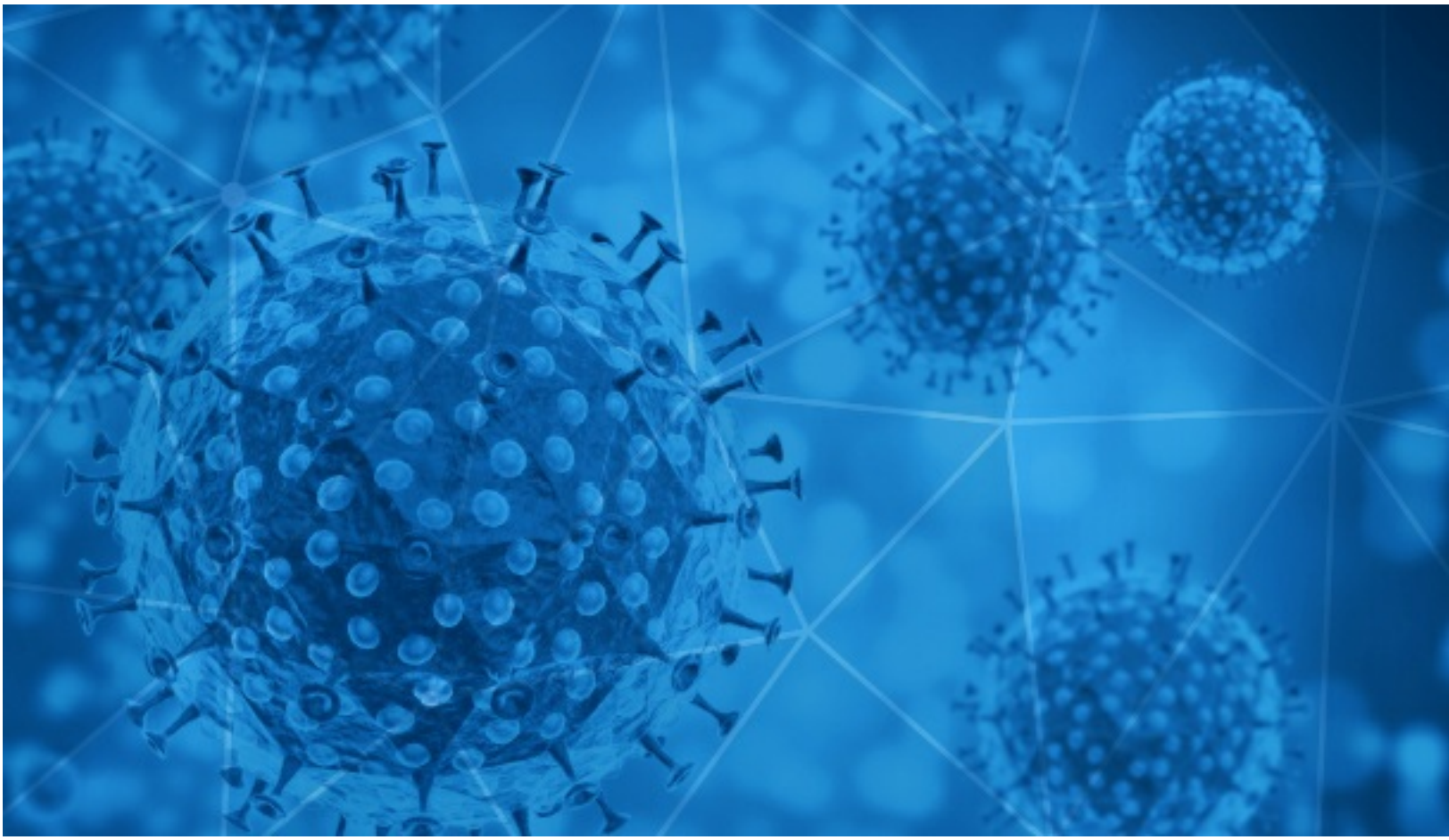
RiskIQ i3:

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

2020-12-16



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 2020-12-15 to 2020-12-16. During this period, RiskIQ analyzed 33,490 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 4,560 unique subject lines observed during the reporting period. The spam emails originated from 2,427 unique sending email domains and 4,017 unique SMTP IP Addresses. Analysts identified 3 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Should an infected person get vaccinated?	3055
Oportunidad de Cumplimiento de Ley de SST y Plan COVID-19	2079
Your Email Has Been Awarded 1 Million Pounds In 2020 Coca Cola Covid-19 Pandemic Award	1646
Respuestas gerenciales para el post Covid19	1425
Ingresaron TEST COVID19 de deteccion rapida	932
Contactless infrared body temperature thermometer defeat Coronavirus	837
ABBOTT PANBIOâ¢: Recoleccion de muestra nasofaringea COVID-19	834
Attn: Claim your COVID-19 Relief Funds	782
Re: Defeat Coronavirus, non contact fever alarm device	776
Re: Covid-19 Donations..	647
COVID 19 SPENDE	555
Wir verdoppeln Ihre Spende: Kinder brauchen Bildung – auch in Corona-Zeiten	516
HKTDC Export Index 4Q20: Exporter Sentiment Improves as Initial Covid-19 Shockwave Recedes	468
[Earn Credits] Don't lose TRAFFIC with Covid 19 (Watch Video).	459
VA releases COVID-19 vaccine distribution plan, vaccinations began this week	438
Re: COVID-19 RELIEF FUND	387
dobbiamo lavorare! ma dobbiamo difenderci!!! reso disponibile - Kit TEST SIEROLOGICO rilevamento anticorpi COVID-19	370
COVID-19 Impact on Banking and Financial Services	350
S'expatrier au Portugal. Assurance emprunteur. Modèle budget prévisionnel. Formalités douanières Brexit. TVA tests coronavirus. Plus-value immobilière. Vérification comptable. Guide CIR. Garantie jeunes. Ajustement crédit impôt 2020. Echéance IS ...	326
Covid-19 Relief Funds Award	318
__ $850,000.00 USD COVID-19 COMPENSATION GRANT :	307
Reserve Your Seat. Building a career in IT in the post-Covid world	277
Gran Venta Outlet - Productos Covid 19	273
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	259
COVID FUNDS	236

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmail.com	3697
timesofindia.com	3057
focazen.com	2079
stargoldmedics.com	1959
hotmail.com	1721
keyable.net	1613
walla.co.il	1425
grupolylsalud.com	932
soft-carpex.com	834
zohomail.eu	647

Top-15 IPs Sending COVID Spam

172.245.93.73	1821
192.3.136.7	1647
181.239.232.123	932
113.89.42.252	769
201.231.8.64	757
187.63.183.27	636
218.232.105.246	620
64.222.143.70	555
201.231.27.203	486
113.116.207.234	460

Top-15 Countries Sending COVID Spam

US	14229
IN	3588
CN	2670
AR	2467
DE	1946
BR	1166
FR	879
KR	875
NL	744
GB	629

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

TR: COVID	1

Top-15 Subjects Containing doc/xlsx Files

Five Positive Cases of COVID-19	2
Fwd: Appeal Refund for covid-19	2
Ocena ryzyka zawodowego (aktualizacja pod względem COVID -19) / ZUS w praktyce	2
Buletin de presa 15.12.2020 + comunicat actiune COVID19	2
Screening di massa anti-Covid: si è riunito il Comitato ristretto dei sindaci Asl	2
Com.St. // CORONAVIRUS, GRANA PADANO: UNA CONFEZIONE IN OMAGGIO AI DONATORI DI PLASMA IPERIMMUNE	2
NUEVA FORMACION COVID PARA EMPRESAS	2
FW: AYUSH Doctors participation in COVID19 campaigns of Public Health	1
RE: Covid - 19 Welcomers	1
CORONA : sluiting winkels tm 19 januari	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: 136,410
Domains with Potential Mail Servers: 2,618
Email-Capable Domains and Hosts: 51,939
Live Hosts and Domains Not Parked: 46,406

Mobile Apps

Apps in Official Stores: 489

by Store

Apple	245
Google	229
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,899

by Store Type:

Hybrid	976
Secondary	864
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1