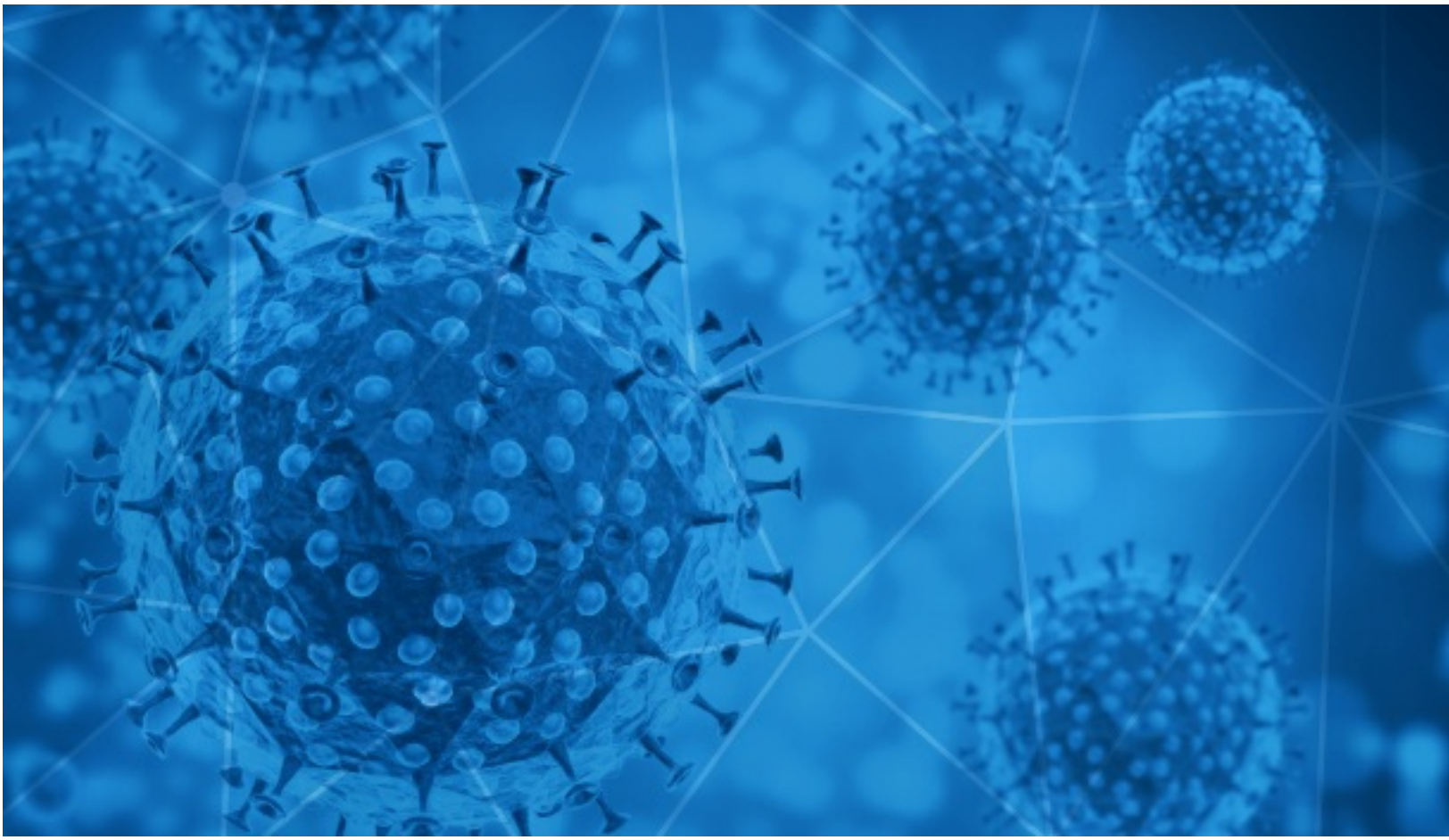
RiskIQ i3:

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

2020-10-19



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 2020-10-18 to 2020-10-19. During this period, RiskIQ analyzed 32,445 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,872 unique subject lines observed during the reporting period. The spam emails originated from 1,057 unique sending email domains and 2,709 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

Limpieza y desinfeccion COVID 19	6012
The Corona Letter: Do frequent sero surveys really help?	4927
Test rapido para la deteccion del Coronavirus	2091
Test de deteccion rapida COVID19	2078
WORLD HEALTH ORGANIZATION $500,000 GRANT CONFIRMATION FOR CORONA VIRUS	1674
Proteccion Covid Totem de Control	945
Your COVID-19 Test Results	784
COVID-19 Products | Gloves & Face Mask | High Quality and Low Prices | Discounts - PROMO CODE#:523730848	726
Evite el coronavirus en su negocio	657
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	540
Equipos de Protección y Prevención del COVID-19	519
COVID -19 RELEIF FUND	454
Mamparas de proteccion COVID19	413
Mamparas de proteccion contra el coronavirus	401
Let's fight COVID with 5x Immunity Booster	369
COVID-19 COMPENSATION UNIT. Send all Replies to benduke111@aol.com	313
Salve sua família! Iniciativa Covid19	271
Covid-19 anti body(IgG+IgM) test is confirmed at Rs.750, Book your slot.	267
COVID-19 Protection Products	266
Save your family! Covid19 initiative	197
Re:Against Covid-19, Direct factory Skymed,V Gloves, Superior ,SUPERLEUR GB, Kichyglove brand NITRILE GLOVES	185
Re:□coronavirus civil mask / Chinese qualified manufacturer	184
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products).	183
protective supplies for corona	179
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products).	160

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

tutanota.com	11652
timesofindia.com	4936
gmail.com	2376
yeah.net	1333
trendingtopic.cl	945
sp-myucbpharma.com	849
dhs.wisconsin.gov	782
126.com	723
focazen.com	519
163.com	478

Top-15 IPs Sending COVID Spam

201.231.19.42	5825
190.247.227.226	2266
201.231.115.28	2125
201.231.6.56	860
61.142.80.33	726
190.247.227.64	573
117.54.4.204	454
98.152.200.190	432
118.67.248.39	316
219.65.85.11	296

Top-15 Countries Sending COVID Spam

AR	11731
IN	5421
CN	4442
US	4170
FR	1789
ID	802
DE	622
CA	426
--	375
GB	328

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

ANC Weekly COVID-19 Reports	34
10 17 2020 CuraScript SD Newsletter Covid and Shortage Products In Stock	3
COVID19 Notice - HISD 2020-2021 Edison MS 10.18.2020	3
Invitation for Webinar on Navigating the Impact of COVID-19 on the Agriculture Supply Chain in India	2
Fwd: FW: [EXT] covid-19 Rangpur Division	2
COVID-19 Site Impact Monitoring (Tableau)	2
Comunicado Ayuntamiento de Almonaster. Coronavirus	1
Rita Carter's COVID Form	1
REMITE REPORTE COVID 19 DEL PERSONAL CAS DE LA EESTP-PNP-TRUJILLO DEL DIA 18OCT2020.	1
FW: Copy of Working covid_pos_neuro_dx_codes and PD_20200505 PA -Copy V3 (002).xlsx	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: 129,768
Domains with Potential Mail Servers: 2,744
Email-Capable Domains and Hosts: 48,994
Live Hosts and Domains Not Parked: 46,694

Mobile Apps

Apps in Official Stores: 464

by Store

Apple	237
Google	212
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,595

by Store Type:

Hybrid	859
Secondary	679
Affiliate	57

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1