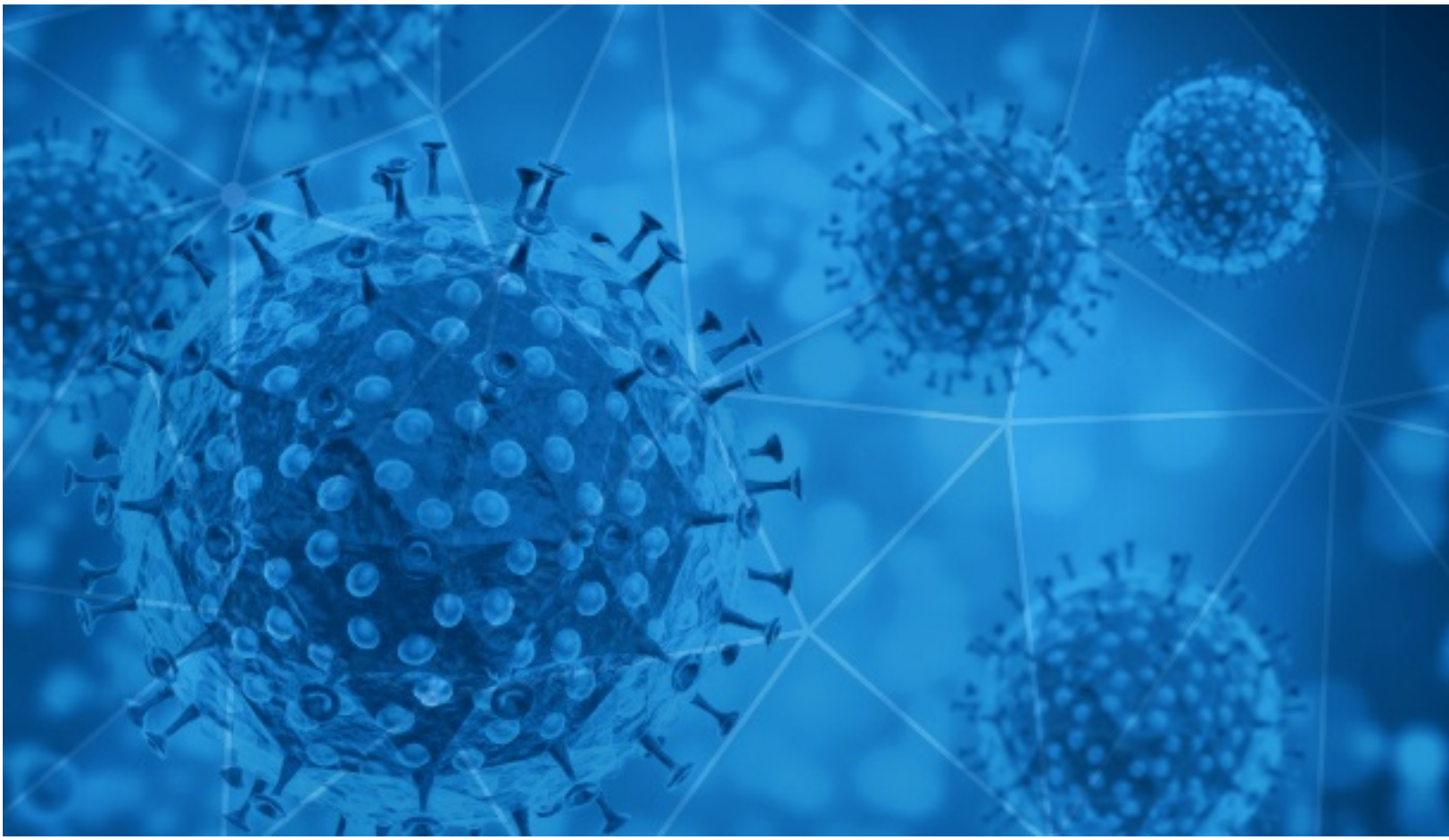
RiskIQ i3:

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

2020-10-27



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 2020-10-26 to 2020-10-27. During this period, RiskIQ analyzed 46,637 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,316 unique subject lines observed during the reporting period. The spam emails originated from 2,161 unique sending email domains and 4,382 unique SMTP IP Addresses. Analysts identified 2 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	11494
New COVID-19 cases reach record highs, signs of life on Venus might be a fluke, and more from Apple News	4924
Urgente - Informacion CORONAVIRUS	3896
The Corona Letter: The elderly may have a shot at beating Covid	3521
Urgente - COVID19	3101
KEEP SCHOOLS OPEN SAFELY...COVID OR NOT!	1314
DPICOVID ritornati con disponibiltà limitata … verifica subito le tua necessità.	858
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	505
COVID-19 Compensation Claim	495
ICO Covid Inversión	485
Avoid COVID with this "touchless" infrared thermometer	380
Evite el coronavirus en su negocio	355
Test rapido para la deteccion del Coronavirus	324
The future of PE/VC Investment in India post-Covid. Join the experts. Register now!	293
ATTN: FBI COVID-19 PANDEMIC COMPENSATION FUND!!!	234
Mi seguro insumos covid 19 protege a tu familia	234
Fortify Your Digital Assets in the Post COVID-19 Era I Sync Up With Top CISOs @ ETCISO Decrypt I 6 Nov	220
How Did COVID-19 Benefit Cybersecurity?	216
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	215
ATTN: FBI COVID 19 PANDEMIC COMPENSATION FUND!	208
Let’s fight together to get through the COVID-19	196
United Nations Covid-19 Disbursements.!!!	182
Llegaron los Test COVID19 de deteccion rapida	182
WORLD HEALTH ORGANIZATION $500,000 GRANT CONFIRMATION FOR CORONA VIRUS	181
3 Unexpected Ways the COVID-19 Pandemicic is Impacting the Job Market	177

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

epc-store.com	11495
mscbs.gob.es	6997
insideapple.apple.com	4925
timesofindia.com	3527
gmail.com	1374
innovativetechholdings.com	1314
tutanota.com	1058
sicurezzanews.it	858
yeah.net	757
126.com	688

Top-15 IPs Sending COVID Spam

192.241.142.175	1314
190.247.227.222	799
45.81.224.99	786
195.123.222.141	769
195.123.222.140	716
45.137.67.35	654
195.123.222.144	572
45.82.179.103	538
195.123.222.138	531
195.123.222.142	513

Top-15 Countries Sending COVID Spam

JP	11620
US	10820
IN	4548
--	3943
NL	3365
CN	2207
AR	2031
DE	1452
ES	891
IT	642

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

aide covid- filière équine - dossier avant le 3 novembre	1
TR: Demande de paiement dossier AT COVID 19	1

Top-15 Subjects Containing doc/xlsx Files

***IMPORTANT* Bulk Quote Request-Covid19**	74
NOTA DE PRENSA: El 19% de los españoles no controla su tensión y no sabe si es persona de riesgo frente al coronavirus	18
Ocena ryzyka zawodowego (aktualizacja pod względem COVID -19)	7
COVID-19 WEBINAR DIRETTA STREAMING Anticorruzione e Trasparenza P.A. e Società Pubbliche: RPCT e PNA 2019-2021 26/11/20	6
COVID-19 VENDITA REGISTRAZIONE + ATTI APPALTI e L. 120/20 Semplificazioni: cosa cambia per procedure e affidamenti 13/10/20	4
Statement Concerning Governor Pritzker's COVID Restrictions	2
NP Doctoralia_Los daños colaterales del Covid-19: Dientes desgastados, astillados e incluso rotos, principal motivo de consulta al dentista	2
FW: [Final] Notification of COVID-19 close contacts	2
Fw: Humble Request for Important COVID Survey: Prof Dr. Vitull K. Gupta	1
Kind Attention || Saifee Hospital Commits To Tighter Sterilization Protocols Under International Guidelines For COVID-19 And Other Patients	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: 130,535
Domains with Potential Mail Servers: 2,671
Email-Capable Domains and Hosts: 49,376
Live Hosts and Domains Not Parked: 46,540

Mobile Apps

Apps in Official Stores: 466

by Store

Apple	235
Google	216
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,650

by Store Type:

Hybrid	869
Secondary	723
Affiliate	58

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1