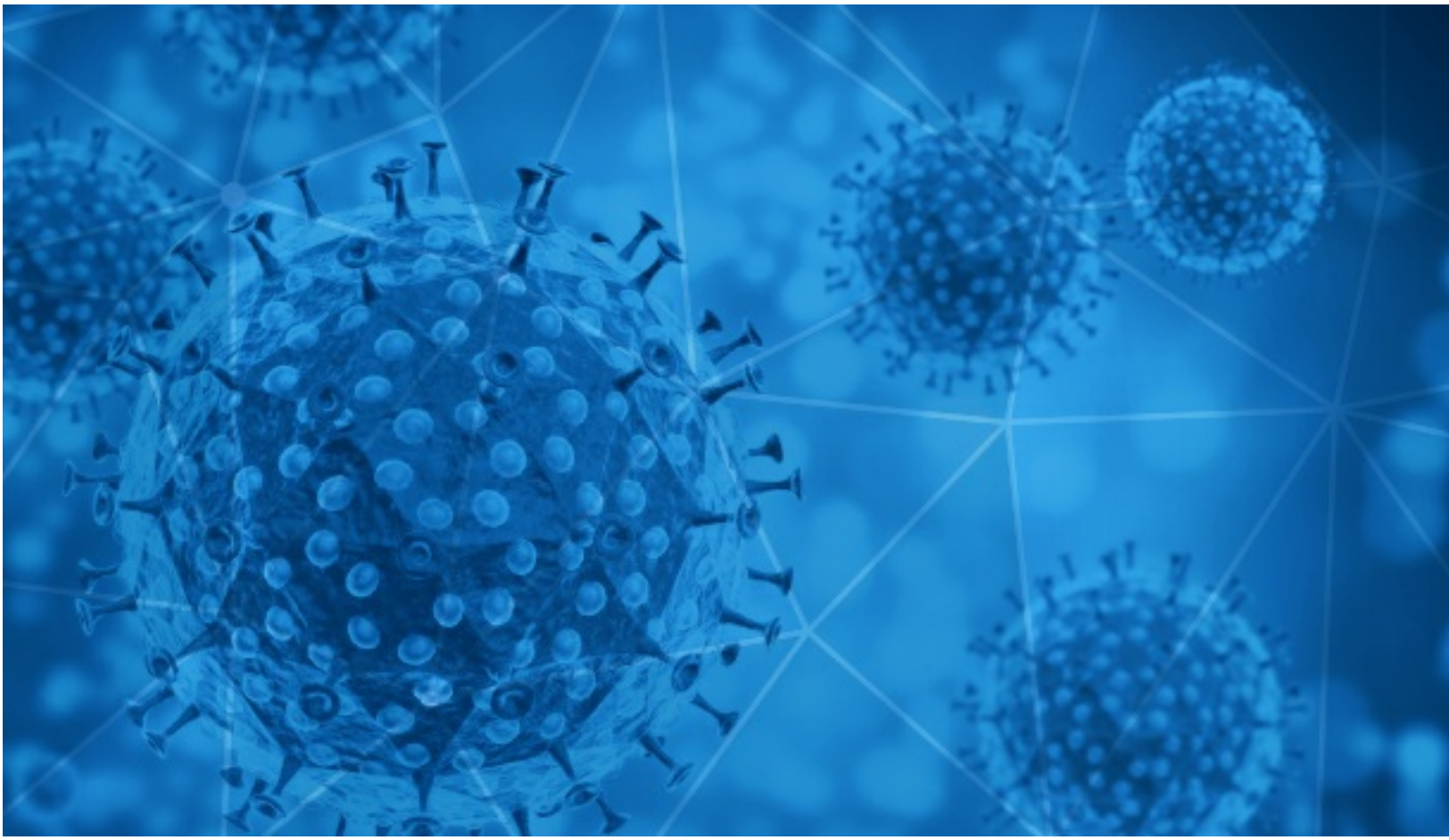
RISKIQ®

RiskIQ i3:

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

2020-11-25



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 2020-11-24 to 2020-11-25. During this period, RiskIQ analyzed 39,837 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,836 unique subject lines observed during the reporting period. The spam emails originated from 2,246 unique sending email domains and 4,962 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	11390
The presidential transition officially begins, inside Sweden's controversial COVID-19 strategy, and more from Apple News	5445
The Corona Letter: A vaccine's efficacy vs its effectiveness	2585
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	1138
[OL] After Covid-19 is defeated, things will still need to be Done!	925
Safety measures to stay protected against COVID-19	607
Haben Sie Ihre € 1.500.000,0 für eine Coronavirus-Spende erhalten, senden Sie uns jetzt eine E-Mail	525
**Re: COVID-19 - Projects| Website	Mobile Application	E-Commerce	SEO (Results Guaranteed) [REDACTED_DOMAIN]**	461
All New Testing For COVID-19, Pulse Oximeter 50%!O(MISSING)ff The Device	429
COVID Numbers Are Rising- Test For COVID-19 At Home In Seconds	417
¿Qué nos espera económicamente luego del Covid-19?	410
Testing For COVID Easy And At Home, All New Pulse Oximeter	406
Descuentos sobre descuentos en productos Covid !!!	349
Descuentos Sobre Descuentos en Productos Covid!	339
- $850,000.00 USD COVID-19 GRANT :	333
Fight COVID-19□ With $100 Gift Card!	300
Lampy sterylizujace UV-C jako dobry sposób walki z koronawirusem (covid-19)	289
Test Rápido Covid-19 Segunda Generación	267
Re: Digital signage solution for Covid-19	258
COVID-19	245
Important – deadlines you need to be aware of for the Coronavirus Job Retention Scheme	230
Re: Corona virus Protection Pills.Order confirmation	212
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove...etc.	193
Re: COVID-19 RESPONSE FUND	186
The mad dash for a coronavirus vaccine	182

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	11392
insideapple.apple.com	5449
timesofindia.com	2585
gmail.com	1762
wisdomwomensisterhood.com	979
1treebridge.com	928
icicliprulife.com	607
126.com	593
163.com	466
rtspogresonlreimmkhadkhodar.com	441

Top-15 IPs Sending COVID Spam

194.146.26.51	970
65.175.68.7	928
194.143.231.172	525
103.225.55.53	446
129.157.116.44	410
103.225.53.243	401
177.101.127.174	333
103.225.54.215	322
212.227.254.175	311
103.225.55.215	303

Top-15 Countries Sending COVID Spam

US	13447
JP	11694
IN	3846
--	1424
CN	1388
DE	1176
FR	809
GB	781
HU	537
BR	431

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

COVID 19 WEB DIR STREAMING CYBERSECURITY, PAGAMENTI DIGITALI, GDPR: perimetro nazionale sicurezza (in vigore dal 5/11) 15/12/20	13
Media Alert Avast: 2020: El año de las fake news, las estafas relacionadas con la Covid-19 y los ataques de ransomware	2
Reminder - Covid-19 Testing at Bishop Hedley High School	2
Urgent job opening :: Project Manager (AWS Migration) // Trevose, PA (present remote till covid) // 4 month contract most likely to extend	2
2963 - 8 - Preparação do Texto – "COVID-19, SAÚDE & INTERDISCIPLINARIDADE"	2
[External] Data of Death Claims related to COVID-19 - Reporting format	2
REUNIONS EXCEPTIONNELLES CME - COVID	2
information covid	2
Biserica Sf. Gheorghe Toronto- program in timpul postului Craciunului conditionat de Covid-19	1
A1 продължава дарителската си кампания за справяне с COVID-19 с предоставяне на 1000 бързи антигенни теста на УМБАЛ „Света Екатерина“	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: 133,634
Domains with Potential Mail Servers: 2,625
Email-Capable Domains and Hosts: 50,872
Live Hosts and Domains Not Parked: 46,031

Mobile Apps

Apps in Official Stores: 473

by Store

Apple	238
Google	220
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,796

by Store Type:

Hybrid	929
Secondary	808
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1