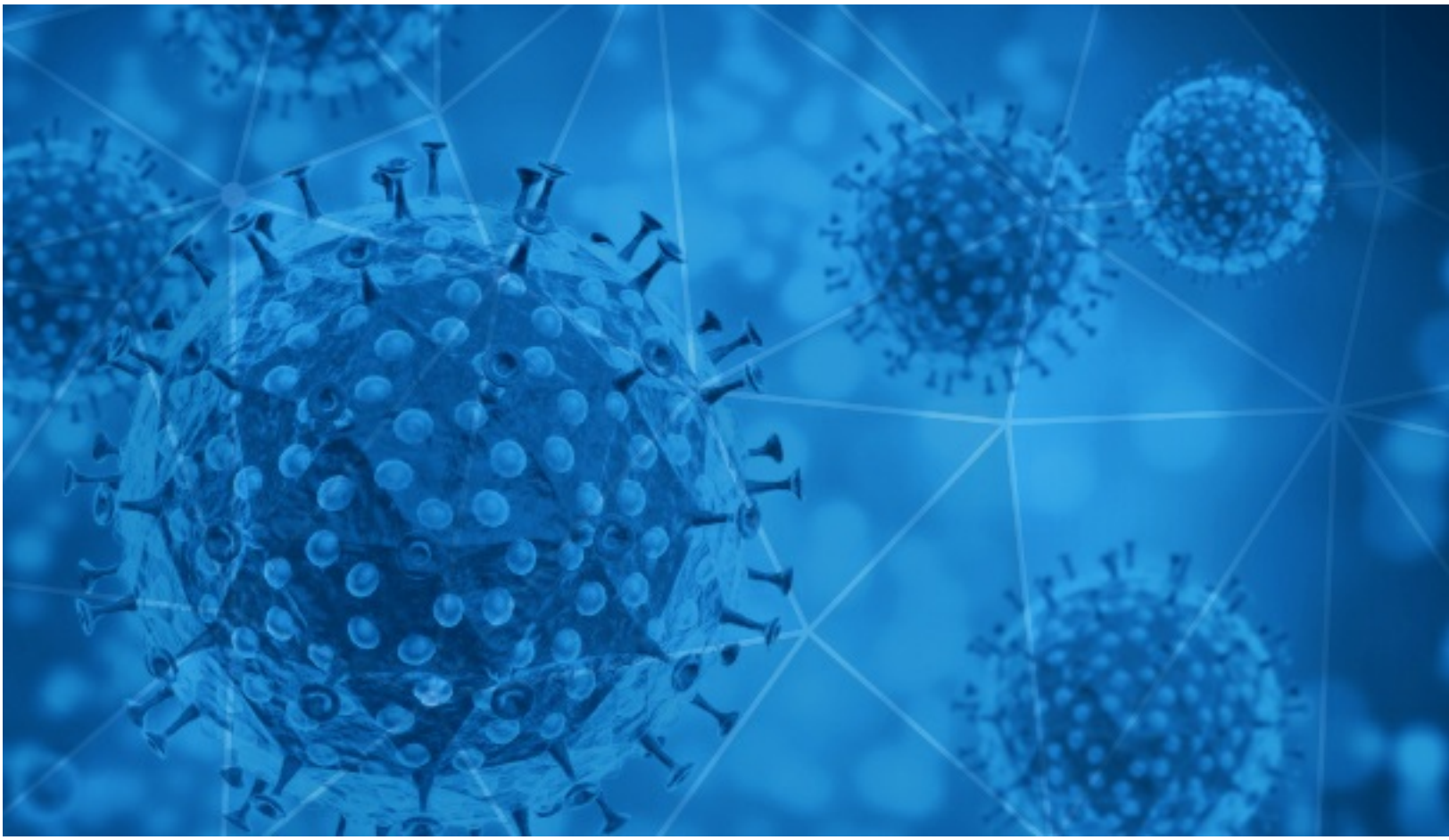
RiskIQ i3:

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

2020-08-18



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 2020-08-17 to 2020-08-18. During this period, RiskIQ analyzed 51,229 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,150 unique subject lines observed during the reporting period. The spam emails originated from 1,813 unique sending email domains and 4,129 unique SMTP IP Addresses. Analysts identified 2 emails which sent an executable file for Windows machines.

Top-25 Subjects

The latest on the Postal Service, CDC gives new coronavirus guidance for kids, and more from Apple News	4489
Fighting against COVID-19,	3982
The 3 plants you need to throw in your shopping cart to fight coronavirus	3063
The Corona Letter: Lockdown's perverse effect on child marriage	2067
COVID-19 : Protectores Faciales	2036
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	1825
Help the world's response to Covid-19 with the most protective mask on the market.	1399
Wearing a KN95 mask is your best defense against coronavirus	1380
COVID-19 And Your Credit Health	1343
Protect Scores During Coronavirus	1308
Will COVID-19 Impact Your Credit Scores?	1297
Novo pesadelo do coronavírus?!	1034
Cuidate del COVID19 con nuestros productos	752
Re:Covid 19 Loan Relief	677
(covid19) outbreak compensation	611
Soluciones para la prevencion del covid19	478
Cabinas para la prevencion del coronavirus?	473
August 2020 Edition - COVID19 Safety Essential Equipment	472
Como volver a la actividad post coronavirus?	470
Totem Covid-19 Test Rápido, Mascarillas, Guantes e Insumos	423
Correcting the Revised Form 941: Form 941X COVID-19 Edition	408
Re: keep away from Covid-19	386
COVID-19 Compensation/Relief Funds.	373
Re: Protective products related to COVID-19.	369
Re: Defeat Coronavirus, non contact fever alarm device	331

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	6888
insideapple.apple.com	4489
mallgene.guru	3063
trendingtopic.cl	2118
timesofindia.com	2070
expowe.icu	1997
climpuright.icu	1951
web4youonline.xyz	1825
deferts.casa	1786
countermail.com	1755

Top-15 IPs Sending COVID Spam

95.211.208.41	3982
170.130.165.109	3057
23.231.110.254	1997
23.231.110.253	1950
198.199.68.131	1821
23.231.110.247	1779
23.231.110.248	990
201.231.5.28	922
211.241.209.104	682
113.116.207.219	649

Top-15 Countries Sending COVID Spam

US	25875
NL	4249
IN	3517
CN	2825
AR	2577
FR	2494
DE	1394
PL	826
KR	823
GB	774

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

MT CORONET - CALLING AT PARADIP PORT - COVID -19 - HEALTH CLEARANCE	1

Top-15 Subjects Containing doc/xlsx Files

BHP w dobie Covid19 / Profesjonalny sekretariat w dobie pracy zdalnej	9
Taxation, Payroll Reconciliation and Impact of Covid 19 on your Payroll Function Course 2020	5
PANTALLAS PROTECTORAS COVID19	3
PHHS 8 17 2020 End of Day COVID 19 Report	3
ENVIAR PRESUPUESTO ELABORACION PLAN COVID 19	2
[Zone7] FW: [Zonechairs] COVID Club Support - Quick Survey	2
Corona_Meldung eingeschränkter Regelbetrieb_Bereich FBBE.xlsx	2
Re: COVID-19 Bhutanese respond survey	2
COVID-19 ECONOMIC IMPACT PAYMENT	2
Press Release : ICSI awards Corona Warriors	2

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: 119,789
Domains with Potential Mail Servers: 2,917
Email-Capable Domains and Hosts: 44,432
Live Hosts and Domains Not Parked: 69,479

Mobile Apps

Apps in Official Stores: 392

by Store

Apple	204
Google	177
WindowsPhone	10
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,132

by Store Type:

Hybrid	693
Secondary	392
Affiliate	47

Blacklisted Mobile Apps: 26

by Store Type:

Secondary	23
Official	2
Hybrid	1