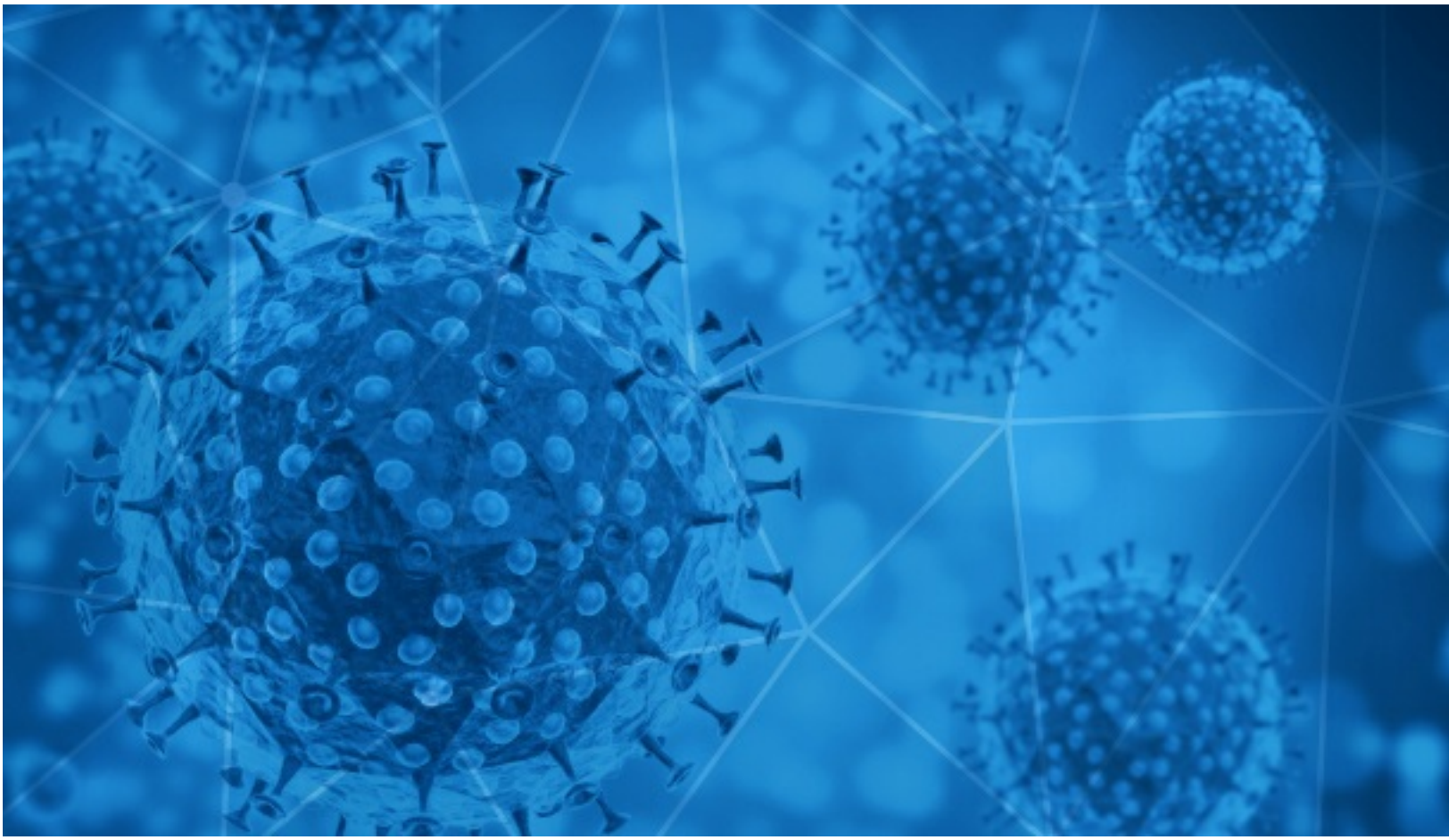
RiskIQ i3:

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

2020-05-28



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 2020-05-27 to 2020-05-28. During this period, RiskIQ analyzed 57,348 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 5,825 unique subject lines observed during the reporting period. The spam emails originated from 3,666 unique sending email domains and 6,738 unique SMTP IP Addresses. Analysts identified 2 emails which sent an executable file for Windows machines.

Top-25 Subjects

Introducing Zero Fee Money Transfers Amidst COVID-19 Outbreak	4822
Protejase del Covid-19, Productos Certificados	3607
The Corona Letter: The case of missing migrants	3181
Covid19- GRANT RELIEF FOR CORONAVIRUS PANDEMIC	3161
IRS COVID-19 Relief Fund	1952
COVID-19: UN	1687
Products for COVID-19	1263
COVID19 Offer -85%	1239
6 models of disinfection carbinet channel help you re-start bussiness and fight covid 19	889
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	832
Re: Vanity upon Vanity, COVID -19.cc	799
COVID-19 EMERGENCY DELIVERY OF YOUR CONSIGNMENT BOX TODAY.	584
COVID-19 CHARITY RELIEF AMOUNT	512
Catalogo articulos prevencion Covid-19	498
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	456
5 ways to improve your job search using social media amid COVID-19	393
IMPORTANTE - COVID-19 (CORONA VIRUS)	375
Fight Corona-virus with this…	374
It that helps fight Corona-virus!	366
Señaletica de Seguridad - Prevención del COVID-19	364
Beneficios y facilidades Tributarias en tiempos Covid-19	358
This will save you from Corona-virus !!!	354
COVID-19 - Custom Projects | Mobile Application | SEO !! -etc [REDACTED_DOMAIN]	343
Re: FWD: Re: Confirm Purchase Order product of covid 19	342
Coronavirus Relief,	315

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	5523
bookmyforex.com	4822
outlook.com	4574
trendingtopic.cl	3937
timesofindia.com	3181
163.com	2051
irs-gov.com	1952
126.com	1858
yellowpagescloud.net	1479
medicproduction.com	1263

Top-15 IPs Sending COVID Spam

161.35.128.139	4822
91.143.80.127	3161
211.68.68.5	1687
209.58.149.66	1263
51.38.157.47	1185
51.77.33.39	1061
51.77.33.43	947
203.86.233.195	889
119.122.88.142	830
46.101.3.131	796

Top-15 Countries Sending COVID Spam

US	18820
CN	7358
FR	5350
IN	4628
DE	4584
IT	2156
GB	1853
CA	1686
HK	1247
AR	1137

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

TR: 27-05-2020 - EPIDEMIE COVID 19 - CORONAVIRUS - NOTE 30	1

Top-15 Subjects Containing doc/xlsx Files

dr Monika Mucha 3 czerwca CIT 2019 rozliczenie w dobie COVID, w programie m.in.: możliwość odstąpienia przez małych podatników od płacenia zaliczek w formie uproszczonej	13
NP_Patrocina un Deportista y catorce deportistas se suman a #ObjetivoVacuna para seguir captando fondos para encontrar una vacuna contra el Covid19	12
Financial Accounting Impact of COVID-19- An In-depth Look at IFRS	12
dr Monika Mucha: 3 czerwca CIT 2019 rozliczenie w dobie COVID, w programie m.in.: wydłużenie terminów związanych z cenami transferowymi	12
COVID-19 Survey for Review	10
dr Monika Mucha: 3 czerwca CIT 2019 rozliczenie w dobie COVID, w programie m.in.: jednorazowa amortyzacja ŚT nabytych w celu produkcji towarów związanych z przeciwdziałaniem COVID-19	10
CIT 2019 rozliczenie w dobie COVID - dr Monika Mucha 3 czerwca, m.in.: odstąpienie od stosowania przepisów dot. złych długów wobec podatnika będącego dłużnikiem	10
3 czerwca dr Monika Mucha: CIT 2019 rozliczenie w dobie COVID, w programie m.in.: przesunięcie zapłaty podatku od przychodów z budynku za miesiące marzec – maj 2020	8
3 czerwca CIT 2019 rozliczenie w dobie COVID dr Monika Mucha, m.in.:odliczenie od dochodu kosztów poniesionych na działalność badawczo – rozwojową celem opracowania produktów związanych z przeciwdziałaniem COVID-19	8
3 czerwca dr Monika Mucha: CIT 2019 rozliczenie w dobie COVID, w programie m.in.:utrzymanie statusu podatnika CIT przez podatkową grupę kapitałową w przypadku poniesienia negatywnych konsekwencji ekonomicznych z powodu COVID -19	7

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: 99,590
Domains with Potential Mail Servers: 2,980
Email-Capable Domains and Hosts: 37,587
Live Hosts and Domains Not Parked: 40,115

Mobile Apps

Apps in Official Stores: 274

by Store

Apple	161
Google	105
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 569

by Store Type:

Hybrid	332
Secondary	211
Affiliate	26

Blacklisted Mobile Apps: 19

by Store Type:

Secondary	18
Official	1