



RiskIQ i3:

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

2020-05-29



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, phishing, malware, or malicious code. This data is delivered "AS-IS".

https://covid-public-domains.s3-us-west-1.amazonaws.com/covid19_blacklist.html

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 2020-05-28 to 2020-05-29. During this period, RiskIQ analyzed 44,456 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 5,748 unique subject lines observed during the reporting period. The spam emails originated from 4,021 unique sending email domains and 6,791 unique SMTP IP Addresses. Analysts identified 3 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Is it too early to "stop chasing the virus"?	3184
6 models of disinfection carbinet channel help you re-start bussiness and fight covid 19	2460
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	1618
Re: Vanity upon Vanity, COVID -19.cc	1419
Last Chance: COVID19 Offer -85%	1328
U.S. coronavirus deaths pass 100,000, why the virus may never go away, and more from Apple News	1212
Especial Pandemia Covid	707
Protejase del Covid-19, Productos Certificados	667
Insumos Covid por mayor compra minima \$ 1.000.000 stock permanente y precios insuperables	603
IMPORTANTE - COVID-19 (CORONA VIRUS)	559
Beneficios y facilidades Tributarias en tiempos Covid-19	500
Repuestos y servicio técnico batidoras KITCHEN AID - Bandejas de desinfección COVID-19	451
Plan de Vigilancia, Prevención y Control del Covid-19 para el reinicio de actividades	423
Test Rapido Covid 19	420
Plan de contingencia anti COVID	382
CONGRESO ONLINE EN VIVO RRHH-Covid-19, Tmec, Sindicatos, Pensiones	346
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO ANTE EL COVID19	341
Test Rápido Covid-19 IgG/IgM	337
Coronavirus Relief,	321
COVID-19	319
Mamparas de proteccion COVID19	317
Re: Defeat Coronavirus, non contact fever alarm device	312
Contactless infrared body temperature thermometer defeat Coronavirus	302
“Expertos en Prevención de Riesgos. Especialistas en Protocolos COVID-19”	282
Insumos Críticos Covid 19 Mayoristas	281

- CONFIDENTIAL -

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmail.com	4146
timesofindia.com	3184
sanlogistics.cn	2492
126.com	2436
163.com	2095
yellowpagescloud.net	1569
insideapple.apple.com	1212
outlook.com	1076
trendingtopic.cl	1061
tie.cl	618

Top-15 IPs Sending COVID Spam

203.86.233.195	2460
119.122.88.142	1618
178.62.23.243	1411
80.211.76.14	1046
181.160.218.46	618
119.123.128.111	614
80.211.174.185	524
198.211.114.182	426
51.77.33.39	342
181.46.136.165	341

Top-15 Countries Sending COVID Spam

US	11909
CN	7029
IN	4176
HK	2609
FR	2504
GB	2280
IT	2151
DE	1884
AR	1029
CL	869

- CONFIDENTIAL -

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

URGENT TENDER#675320 (covid19 kits)	2
Comunicado Covid-Epay - IMPORTANTE	1

Top-15 Subjects Containing doc/xlsx Files

Cuzco IV - NP Robots con cámaras termográficas para una vuelta al trabajo Covid Free	30
CDC and ASN issued COVID-19 guidelines for care of patients on dialysis	18
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	16
3 czerwca dr Monika Mucha: CIT 2019 rozliczenie w dobie COVID, w programie m.in.: przedłużenie terminów do przesłania informacji ORD-U i informacji IFT-2R	15
CIT 2019 rozliczenie w dobie COVID - dr Monika Mucha 3 czerwca, m.in.: możliwość odstąpienia przez małych podatników od płacenia zaliczek w formie uproszczonej	12
CIT 2019 rozliczenie w dobie COVID - dr Monika Mucha 3 czerwca, m.in.: odstąpienie od stosowania przepisów dot. złych długów wobec podatnika będącego dłużnikiem	11
CIT 2019 rozliczenie w dobie COVID 3 czerwca - dr Monika Mucha, m.in.: możliwość stosowania przy zaliczkach na podatek stawkę przewidzianą dla dochodów z kwalifikowanych praw własności intelektualnej	11
CIT 2019 rozliczenie w dobie COVID dr Monika Mucha - 3 czerwca, m.in.: wydłużenie terminu na złożenie zawiadomienia o dokonaniu zapłaty na rachunek inny niż STIR	11
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
dr Monika Mucha: 3 czerwca CIT 2019 rozliczenie w dobie COVID, w programie m.in.: wydłużenie terminów związanych z cenami transferowymi	10

- CONFIDENTIAL -

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: 100,145
Domains with Potential Mail Servers: 2,990
Email-Capable Domains and Hosts: 37,902
Live Hosts and Domains Not Parked: 40,364

Mobile Apps

Apps in Official Stores: 276

by Store

Apple	162
Google	106
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 576

by Store Type:

Hybrid	338
Secondary	212
Affiliate	26

Blacklisted Mobile Apps: 19

by Store Type:

Secondary	18
Official	1