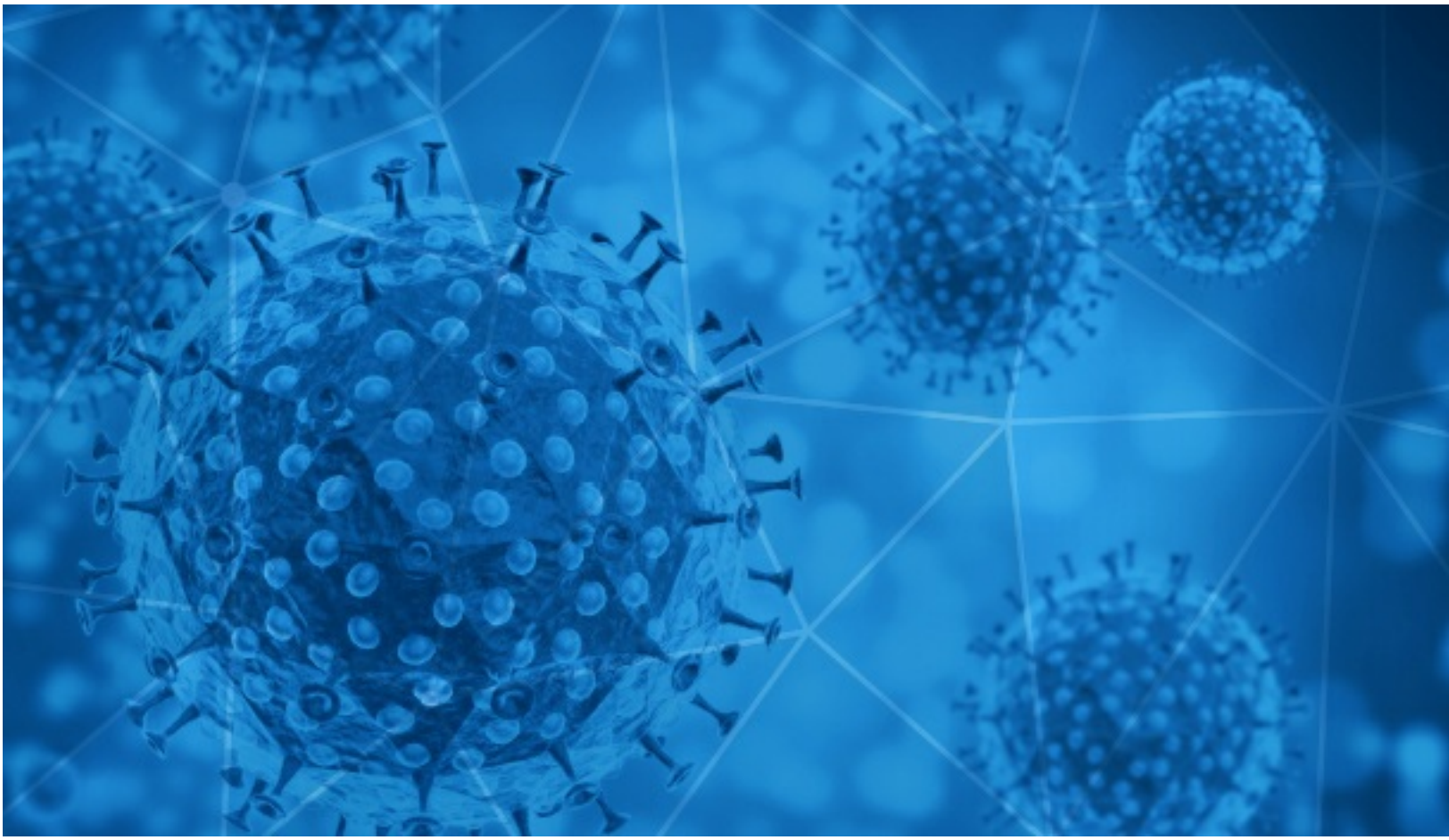
RiskIQ i3:

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

2020-11-03



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 2020-11-02 to 2020-11-03. During this period, RiskIQ analyzed 42,249 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,726 unique subject lines observed during the reporting period. The spam emails originated from 2,407 unique sending email domains and 4,538 unique SMTP IP Addresses. Analysts identified 3 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	9596
The Corona Letter: Going back to school could be tough	3536
Test rapido para la deteccion del Coronavirus	2106
TermoScanner Anti-Covid in pronta consegna. Prezzi dimezzati e modelli a partire da soli Euro 499,00. Non Abbassiamo la guardia!!!	1303
Proteja su negocio de covid y ofrezca seguridad a sus clientes	1008
Corona Schnelltest	741
Proteja su negocio de COVID19 y ofrezca seguridad a sus clientes	668
Triple test para COVID19 de deteccion rapida	565
Gestión de riesgos y auditoría en tiempos de covid19	542
Ingresaron TEST COVID19 de deteccion rapida	508
Triple test para covid de deteccion rapida	508
Test rapidos de covid aprobados por anmat	492
Precio test covid	467
Ingresaron test de covid de deteccion rapida	456
[UK BBB] When the dust [covid-19] settles training gives the best ROI of all.	444
Evite el coronavirus en su negocio	412
[UK 1] When the dust [covid-19] settles training gives the best ROI of all.	406
Coronavirus (Covid19) Bailout Fund	367
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	361
Precio test covid19	354
Test rapidos de covid19 aprobados por ANMAT	313
COVID-19 Asesoramiento contable para tu empresa	293
ATENCION COVID-19 Estudio Contable, Legal e Impositivo para tu negocio	293
ATALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ KHUẨN PHÒNG CHỐNG COVID -19	263
Mi seguro insumos covid 19 protege a tu familia	247

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	9596
walla.co.il	8636
timesofindia.com	3536
livejob.it	1303
gmail.com	912
126.com	884
bizuk01.com	850
usab2bmail.com	818
covid-19-schnelltests-24.de	741
yeah.net	732

Top-15 IPs Sending COVID Spam

190.247.240.182	3320
201.231.19.96	1730
185.221.173.42	1303
201.231.10.149	967
216.15.151.42	850
184.175.86.164	818
190.247.240.54	620
190.247.240.39	511
113.116.205.85	458
181.239.232.96	418

Top-15 Countries Sending COVID Spam

JP	9697
AR	9110
US	7038
IN	3987
CN	3237
IT	1960
DE	1246
FR	923
--	882
GB	698

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

UMIH 71 : Prolongation de la Subvention « PréventionCOVID » : Jusqu'à 50% de subvention pour l'achat d'équipements de protection	1
Tr : Coronavirus - point de situation dans le Nord - 30 octobre	1

Top-15 Subjects Containing doc/xlsx Files

COVID19 WEB DIRETTA STREAMING Licenziamento DIRIGENTE: liceità, giustificatezza, soluzioni non traumatiche, contenzioso 18/11/20	24
COVID 19 WEB DIRETTA STREAMING DIGITALIZZAZIONE, DEMATERIALIZZAZIONE, A.I. e GDPR: presidi, processi e disciplina 1/12/20	21
Oferta na środki ochrony indywidualnej przed Covid-19	7
Online Michaelmas Term: Covid-19 Update from Cambridge Union	4
Mueren 1.500 enfermeras por COVID-19 en 44 países	3
QIDA ¡Importante! Formación prevención covid19 Recibidos	3
Precizări de presă privind infectarea cu COVID-19 a trei persoane din cadrul Centralei Ministerului Afacerilor Externe și a unei persoane din Serviciul Exterior	3
COVID-19 Testing Letter	3
Doing business in China during the "COVID Second Wave"	2
[Ehealth] Онлайн конференція з теми "Протоколи лікування хворих на COVID-19". Що потрібно робити та чого робити не можна. Аналіз помилок при наданні допомоги на первинній ланці	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: 131,402
Domains with Potential Mail Servers: 2,668
Email-Capable Domains and Hosts: 49,939
Live Hosts and Domains Not Parked: 46,087

Mobile Apps

Apps in Official Stores: 468

by Store

Apple	235
Google	218
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,681

by Store Type:

Hybrid	884
Secondary	738
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1