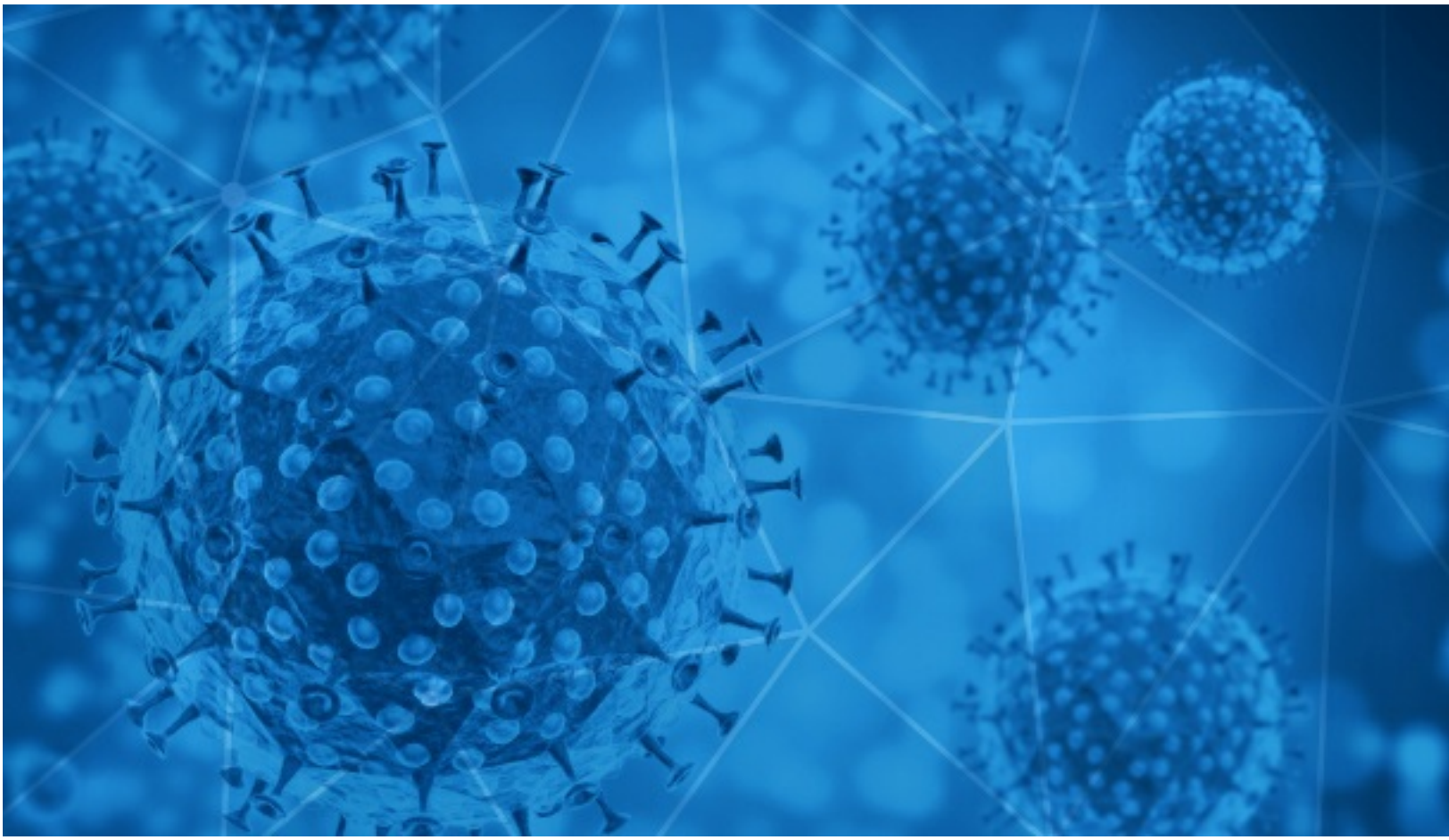
RiskIQ i3:

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

2021-02-18



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 2021-02-17 to 2021-02-18. During this period, RiskIQ analyzed 37,789 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 7,986 unique subject lines observed during the reporting period. The spam emails originated from 2,089 unique sending email domains and 4,319 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

What to know about the extreme winter weather, why U.S. coronavirus cases are dropping, and more from Apple News	6472
The Corona Letter: Vaccine rollout needs a course-correction	3823
Traveling soon, wear this mask to fight chances of getting Corona-virus	1329
New Corona-virus Mask!	1277
Reduce your risk of Corona-virus with this Mask	1249
Get your Corona-virus Mask while supplies last!	1246
NOVITA' TEST SALIVARE semplice, economico, testato per la ricerca del COVID-19 "ANTIGEN SPITTEST PCL"	1239
Últimas medidas Laborales en el entorno Covid	1016
Covid-19 Outbreak Donation	599
Gran Venta Outlet - Productos Covid 19	390
COVID LOANS FROM UNITED NATIONS	387
Home Loan Relief, COVID-19 Q&A, Free Family Reading Resources	365
TermoScanner e strumenti DPI Anti-Covid in pronta consegna con sconti oltre il 70% e prezzi a partire da Euro 39,00 + spedizione gratuita. Non Abbassiamo la guardia!!!	355
Your COVID-19 Test Results	332
LJC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation	297
Pruebas Antígenas para Descarte de COVID-19, Envíos a todo Perú.	264
COVID-19	213
Tell Congress: Expand and protect health care in the COVID relief bill!	212
Voorspellingen over corona waren nog nooit zo moeilijk als nu - Europa bekroont 17-jarige die fake webshop tegen partnergeweld opzette - Wanneer word ik gevaccineerd en hoe werkt oproepingsbrief? - Ideologische clash tussen Vlaamse en federale…	198
[QC] ATALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ KHUẨN PHÒNG CHỐNG COVID -19	193
Doctors warn FDA about covid vaccines causing autoimmune attacks in the heart and brain	188
Tax Software in the COVID-19 Environment	184
Covid19 Relief Fund	182
En vivo: Mitos y verdades sobre las vacunas COVID-19.	180
\nPREPARAR ahora la Post Covid	172

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

insideapple.apple.com	6472
clervisor.net	5101
hospiramedical.co.uk	3948
timesofindia.com	3835
gmail.com	1801
sicurezzanews.it	1239
winsonsoloads.com	641
starlingbnk.org	599
messages.va.gov	478
villakusum.com	376

Top-15 IPs Sending COVID Spam

63.81.84.42	5100
172.245.93.102	1455
107.174.142.107	1302
192.227.217.243	1191
82.135.19.131	659
51.79.156.102	599
82.135.19.130	579
198.20.248.178	572
185.221.173.42	373
169.54.168.106	301

Top-15 Countries Sending COVID Spam

US	22912
IN	4011
DE	2491
FR	1654
IT	913
--	535
BE	516
GB	498
CN	434
VN	337

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

17-02-21 - Fiche de gestion des cas COVID-19 mise à jour et infographie	1

Top-15 Subjects Containing doc/xlsx Files

IMPORTANT: COVID-19 Test by LabDX for Events	3
Fwd: CV 58 vv cho học sinh tạm dừng đến trường, tổ chức dạy học qua Internet nhằm đảm bảo công tác phòng, chống dịch bệnh Covid-19 và chương trình, kế hoạch dạy học	2
Báo cáo PCDB COVID-19, NGÀY 17/2/2021	2
Ndp_España, el país europeo más a favor de que la vacunación contra la Covid sea obligatoria	2
WEBINAR COVID 19 bilancio IAS/IFRS: equilibrio finanziario, aspetti contabili rilevanti e novità fiscali - 4 CFP Odcec - 25/2/21	2
UN Covid 19 Relief fund.	2
Gloria Krenik negative for covid	2
DIPUTACION DE ALICANTE- Nota Pleno extraordinario ayudas Covid	1
Revised COVID-19 Secure Construction RA & Guidance	1
AJUTS EXTRAORDINARIS PER A PERSONES TREBALLADORES AMB INGRESSOS BAIXOS, AFECTADES PER ERTO DERIVAT DE COVID	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: 144,514
Domains with Potential Mail Servers: 2,573
Email-Capable Domains and Hosts: 52,546
Live Hosts and Domains Not Parked: 44,113

Mobile Apps

Apps in Official Stores: 514

by Store

Apple	255
Google	242
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,100

by Store Type:

Hybrid	1072
Secondary	961
Affiliate	67

Blacklisted Mobile Apps: 29

by Store Type:

Secondary	26
Official	2
Hybrid	1