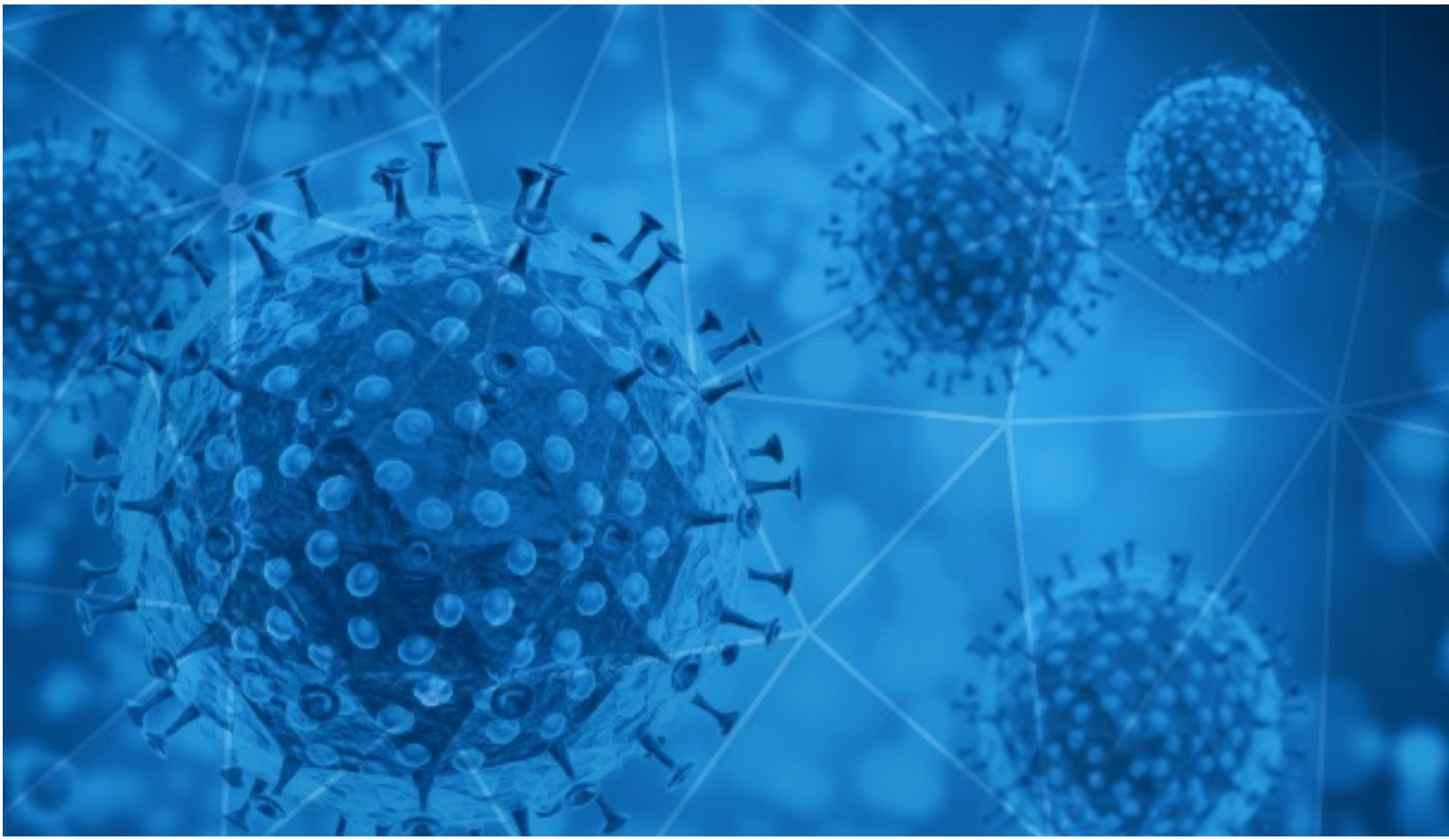
RiskIQ i3:

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

2020-12-18



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 2020-12-17 to 2020-12-18. During this period, RiskIQ analyzed 42,900 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,412 unique subject lines observed during the reporting period. The spam emails originated from 2,243 unique sending email domains and 3,991 unique SMTP IP Addresses. Analysts identified 3 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	14007
-- Ask Details For Covid-19 Relief	3586
The Corona Letter: Another case of allergic reaction to Pfizer's vaccine	3507
Agevolazione Flyingmailers per l'Emergenza COVID-19 | Fai sapere che ci sei!	1373
Respuestas gerenciales para el post Covid19	1047
Oportunidad de Cumplimiento de Ley de SST y Plan COVID-19	761
Shop Now: KN95 Masks Continues To Help Stop The Spread COVID19 Cases	626
Jeremih Details Near-Death COVID Experience {VIDEO} 4 dead in SNOW storm+ $600 Stimulus Checks added	585
Offering N95 FACE MASK (3M 1860,1860S, Makrite 9500 N95,N95S,HARLEY, SAMPLING SWAB AND TUBE KITS,Novel Coronavirus (COVID-19) Test ,quick delivery in a couple days	489
ABBOTT PANBIOâ¢: Recoleccion de muestra nasofaringea COVID-19	458
Freelancer Coronavirus Survey #4	391
Gran Venta Outlet - Productos Covid 19	293
Get Your KN95 Certified Official Masks Have Now Restocked Due To Surge In Covid19 Cases	272
With COVID Cases Rising, KN95 Masks Continue To Keep Americans Safe	261
Shop Now: Official KN95 Masks Have Been Labeled Effective In Fighting COVID19 Virus	260
Let’s fight together to get through the COVID-19	239
YOUR COVID 19 RELEF FUND HAS BEEND RELEASED TO YOU	209
Extension to the Coronavirus Job Retention Scheme – what you need to do now	209
Moeten scholen dicht tot 31 januari? - EU vaccineert vanaf 27 december - Tenerife op slot: verwarring troef - Macron besmet met coronavirus	202
Franse president Macron heeft corona, ook Michel in quarantaine - Europees Hof behoudt verbod op onverdoofd slachten - Waarom het nog niet zo’n slecht idee is om de grenzen te sluiten - Molenberghs over verlenging kerstvakantie: ‘Opletten met opbod…	196
"We are waiting for your Order corona vaccine Confirmation"	190
Urgent - Certified Salesforce Architect required for Newyork City, NY - Remote to begin and will be onsite post covid.	179
[SPAM] IMF COVID19 DSP	174
NCJ Daily - Humboldt Sees Fifth COVID Death in a Week. Fatal 299 Crash. Samoa Homicide Suspect Arrested.	171
Attn: Claim your COVID-19 Relief Funds	158

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	14007
xcontrol.it	3586
timesofindia.com	3514
flyingmailers.com	1373
walla.co.il	1047
stargoldmedics.com	1017
focazen.com	761
gmail.com	735
dudleydeboisier.com	626
pinhang.co	600

Top-15 IPs Sending COVID Spam

67.53.52.108	1685
142.93.83.242	1556
85.17.15.45	1370
172.245.93.73	1010
194.146.26.61	626
107.158.43.51	565
194.146.36.143	532
103.225.54.191	450
201.231.58.202	443
103.225.52.113	386

Top-15 Countries Sending COVID Spam

JP	14066
US	11936
IN	3721
--	1924
CA	1857
NL	1705
AR	1467
DE	880
CN	846
FR	841

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Pfizer-BioNTech Covid-19 Vaccines First Interim	3

Top-15 Subjects Containing doc/xlsx Files

NOTA DE PRENSA: AEC y SEDAR garantizan la seguridad en los quirófanos, y remarcan la importancia de poner al mismo nivel la asistencia de pacientes COVID y NO COVID en todos los hospitales españoles	16
Dwudniowy kurs Kadry i płace w dobie COVID 19 - szkolenie on-line	12
NUEVA FORMACION COVID PARA EMPRESAS	6
Presumed Positive Case of COVID-19: Ahtanum Valley	4
NdP_Nueva Zelanda: cómo sacar partida de la COVID-19 para lograr una buena reputación de 'Marca País'	4
COVID-19 Statement for 12/17/20	3
I: COVID-19, NEONATI: NO A SEPARAZIONE DALLA MADRE. STUDIO ITALIANO PUBBLICATO SU RIVISTA INTERNAZIONALE - Società Italiana di Neonatologia (SIN)	3
Covid 19-Staying Safe During the Holiday Season	2
Ndp_Los médicos están totalmente convencidos de vacunar contra el Covid	2
Carceri: Piano vaccinazioni anti-Covid-19 ricomprenda anche i detenuti - Comunicato stampa	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: 136,648
Domains with Potential Mail Servers: 2,621
Email-Capable Domains and Hosts: 51,988
Live Hosts and Domains Not Parked: 45,572

Mobile Apps

Apps in Official Stores: 491

by Store

Apple	245
Google	231
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,904

by Store Type:

Hybrid	977
Secondary	868
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1