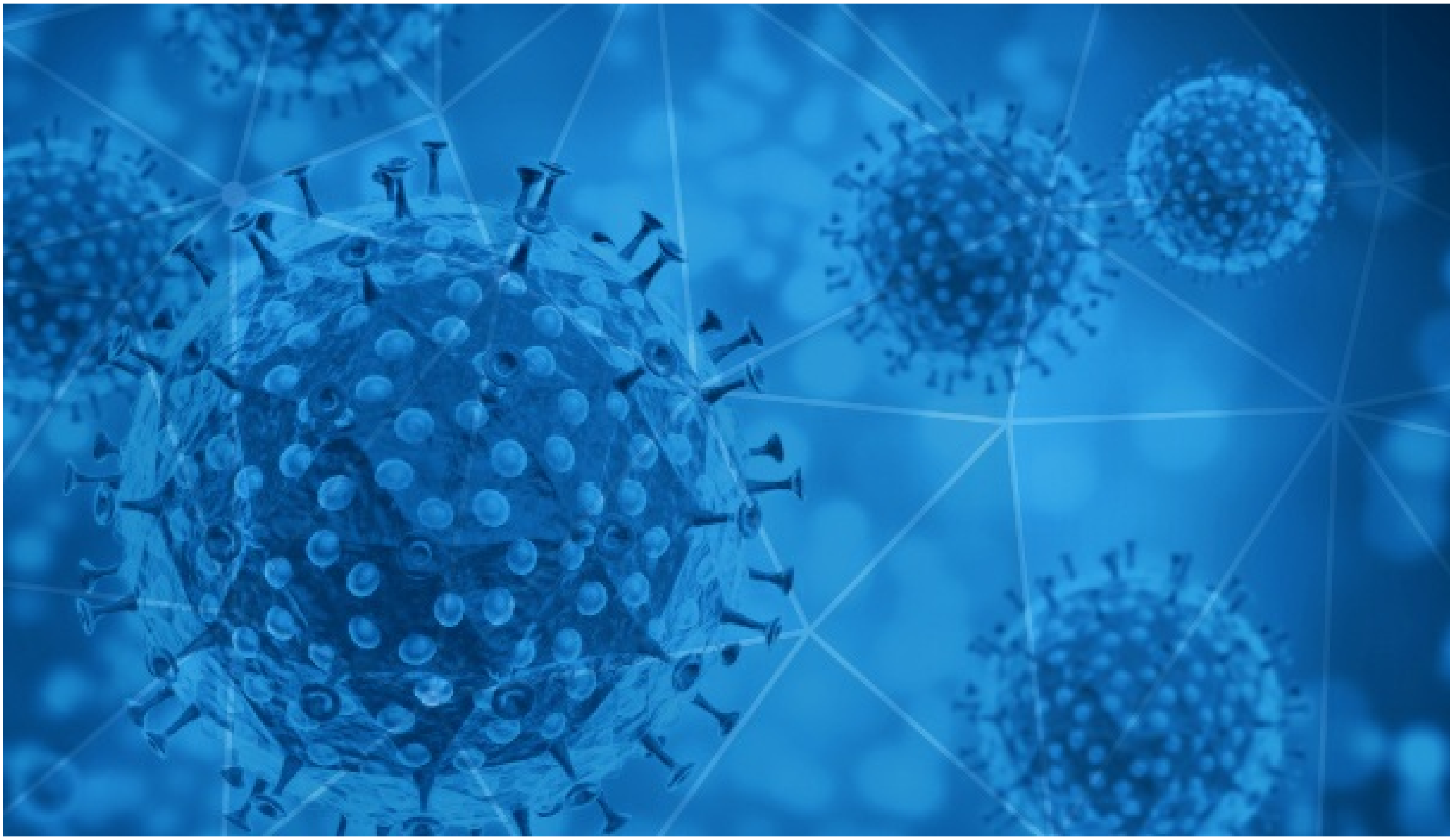
RiskIQ i3:

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

2021-01-11



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

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 2021-01-10 to 2021-01-11. During this period, RiskIQ analyzed 44,951 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,001 unique subject lines observed during the reporting period. The spam emails originated from 985 unique sending email domains and 2,497 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□□	23844
The Corona Letter: How India's vaccination effort will roll out	4902
Re: Covid-19 Donations..	2588
Ask details for the Covid Relief F und	1236
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	858
COVID-19 PROMO.	824
Shop While Supplies Last: Stock Up On KN95 Official Certified Mask To Avoid COVID19 Virus	777
HERZLICHEN GLÜCKWUNSCH, CASH COVID-19 PALLIATIVEN AUS MEINEN LOTTERIEGEWINNEN	598
LJC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation	507
PAID 2 fight COVID 2 Ways and CRYPTO Fortunes	356
Re: Personal, SME & Business Relief (COVID-19) *	316
Covid-19 Relief F und	276
Re: Mashalat Capital Relief (COVID-19).	273
COVID-19 PANDEMIC COMPENSATION FUND	252
Let’s fight together to get through the COVID-19	240
Safety measures to stay protected against COVID-19	239
UNDF CASH DONATION (COVID-19)	210
Re: Maslahat Mutual Relief. (COVID-19).	201
Meer dan 20.000 coronadoden in ons land - Kan Trump nog oorlog starten? - "Heel wat spanning na 100 dagen De Croo" - Brokstukken vermist vliegtuig gevonden	182
IDEX Research: US watch and jewelry prices surge as IDEX Polished Price Index returns to pre-Covid level	148
□ Det här händer när du tar coronavaccinet…	133
Chinese protective products of COVID-19	130
Extra editie: blijf bouwen en verbouwen in corona-wintertijd	129
Covid-19 Donation	122
COVID-19 Chinese protective products	116

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

epc-store.com	23848
timesofindia.com	4910
zohomail.eu	2588
aclipisa.it	1259
gmail.com	1145
covt-com.tk	824
cmbmutualfunds.com	813
iwanttogofurhterfaster.com	778
blydestrustonline.com	506
akhirawahdanshaamolananjibobih.com	411

Top-15 IPs Sending COVID Spam

187.63.183.27	2588
67.227.229.151	1236
103.225.53.5	844
117.50.15.143	824
213.142.149.69	775
103.225.54.76	652
103.225.54.80	618
5.83.23.13	597
103.225.54.206	572
103.225.54.229	551

Top-15 Countries Sending COVID Spam

JP	23952
IN	5068
US	4717
BR	2719
CN	1659
UA	818
PH	812
TR	791
--	679
BE	602

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

ANC Weekly COVID-19 Reports	34
(■■■■■■■■■■) ■■■■■■■■■■■ ■■■■■■■■■■■■■■■■■■■■■■■■■■ ■■■■■■■■■■■■■■■ ■■■■■■■■ COVID 19	4
KÉK Tesztpont Covid szűrés	4
CCS/11051 Reporte COVID-19: Suman 4 mil 398 defunciones y 47 mil 466 contagios en la entidad	2
IMSS BOLETÍN DE PRENSA 016.- Realiza IMSS reconversión hospitalaria en ocho entidades ante el aumento de contagios de COVID-19 (LINK DE VIDEO, FOTOS Y PRESENTACIÓN PDF)	2
Battling Covid-19	2
RV: 210108- Declaración responsable y cambios protocolo Covid	1
Info über Corona-Impfung	1
Fwd: Comunicato 3043/CAV - emergenza Coronavirus 2019 - ulteriore aggiornamento dei dati	1
LA COVID-19 Update	1

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: 139,061
Domains with Potential Mail Servers: 2,551
Email-Capable Domains and Hosts: 52,962
Live Hosts and Domains Not Parked: 53,588

Mobile Apps

Apps in Official Stores: 502

by Store

Apple	245
Google	241
WindowsPhone	15
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,008

by Store Type:

Hybrid	1035
Secondary	910
Affiliate	63

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1