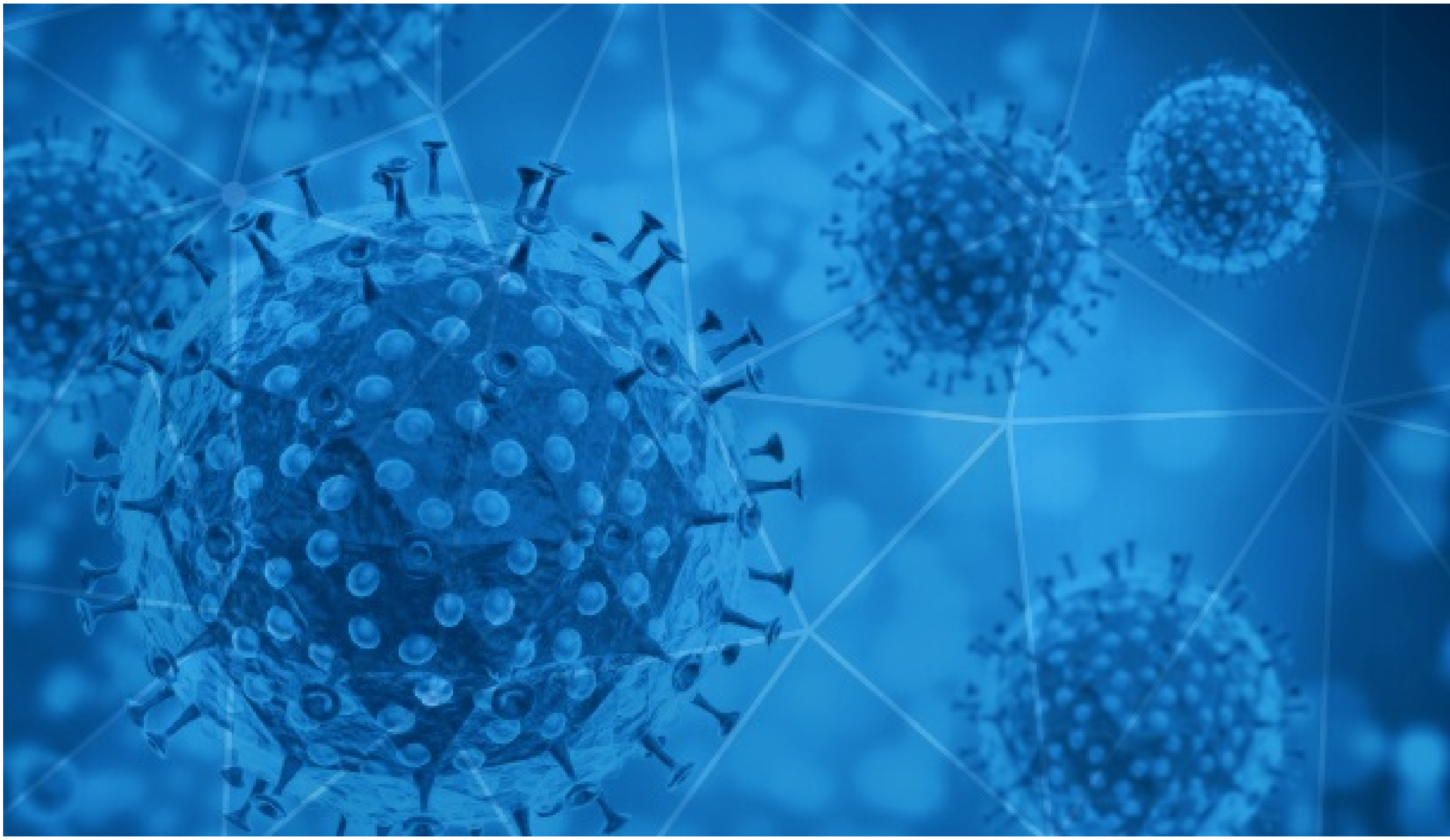
RiskIQ i3:

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

2020-05-22



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 2020-05-21 to 2020-05-22. During this period, RiskIQ analyzed 63,745 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 5,301 unique subject lines observed during the reporting period. The spam emails originated from 4,068 unique sending email domains and 7,646 unique SMTP IP Addresses. Analysts identified 27 emails which sent an executable file for Windows machines.

Top-25 Subjects

COVID-19 Stimulus Package Grant(s)	7797
Insumos Hospitalarios para DESINFECCION de Empresas COVID	4495
Re: UN COVID-19 Stimulus	4111
The Corona Letter: If India were to follow a 50-30 lockdown strategy…	2961
Re: Vanity upon Vanity, COVID -19	2638
Covid19 - Corona virus compensation.	2451
Information on MSMEs engaged in manufacturing of COVID related products	1029
A global coronavirus milestone, how to fall back asleep, and more from Apple News	987
The COVID-19 Response Fund	919
COVID19 Offer -85%	910
Products for COVID-19	886
Redeem Your COVID-19-Financial Relief Today	776
ComputerVault: Stops Coronavirus with Remote Work	730
Oferta Producto Covid-19	572
KVB BAGIC Health Infinity policy - covers COVID - 19	528
Notification on your IMF Corona-Virus relief Aid.	483
Corona-Virus-Spende von 2.800.000 Euro	447
Cabinas para la prevencion del coronavirus?	388
Como volver a la actividad post coronavirus?	380
Webinar gratuito - Prevención y control del covid en el trabajo	379
[□□□□□□□] LS, COVID-19 □□ □□ □□ □□ □□	372
Productos eficientes para combatir y prevenir el Covid-19	363
[eRehabData] New COVID-19 Measure Added, Outcome Report Review Conference Calls	336
Plan de Vigilancia, Prevención y Control del COVID19 para la Reanudacion de Actividades	314
You've Won Covid-19 Support For You and Your Family	311

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

mail.ru	7797
gmail.com	6169
trendingtopic.cl	4495
onet.eu	4111
timesofindia.com	2961
126.com	2141
163.com	2057
outlook.com	1664
yellowpagescloud.net	1080
sampark.gov.in	1029

Top-15 IPs Sending COVID Spam

82.134.25.158	7797
103.141.137.241	4111
91.143.80.127	2451
165.22.142.211	2120
51.77.33.44	1700
23.254.202.153	919
209.58.149.66	886
51.38.157.47	849
51.77.33.43	793
100.0.45.37	730

Top-15 Countries Sending COVID Spam

US	16526
NO	7810
CN	6331
--	5642
FR	5426
IN	5060
DE	4409
IT	1810
AR	902
BR	862

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

FYI Documents due to Covid 19	27

Top-15 Subjects Containing doc/xlsx Files

CII - Webinar on 'Managing Supply Chains to Maximise Sales Post Covid-19': Wednesday, 27 May 2020: 3:00 p.m. to 5:00 p.m.	10
Ergebnisse der Bystronic Covid-19-Umfrage zwischen dem 4. und 20. Mai 2020 und die Produktionsänderungsraten im Vergleich zum 27. April und 1. Mai 2020	5
[DIV39FORUM] Fwd: [COR] Update on APA's global COVID-19 work	3
Tarcza Antykryzysowa 4.0-zmiany w prawie pracy w dobie covid19	3
NP - Mantener el saldo del móvil, cuestión vital para millones de personas en tiempos de coronavirus	3
YES, we are OPEN and Shipping Canada to KINGSTON JAMAICA, COVID-19 update	3
Press Release : Built-for-India, Built-by-India II 3 innovators #Innovate2BeatCOVID; create ingenious PPE solutions	3
Fighting COVID-19: UNDP and AGFUND Triage Unit Serves Refugees and\tHost Communities in the North of Jordan	3
CommuniquÃ© de Presse: Les Ãmirats Arabes Unis dÃ©veloppent une technologie de test par laser rapide pour lutter contre le coronavirus	3
Financial Accounting Impact of COVID-19- An In-depth Look at IFRS	2

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: 97,225
Domains with Potential Mail Servers: 2,886
Email-Capable Domains and Hosts: 36,426
Live Hosts and Domains Not Parked: 38,770

Mobile Apps

Apps in Official Stores: 244

by Store

Apple	134
Google	103
WindowsPhone	6
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 528

by Store Type:

Hybrid	302
Secondary	201
Affiliate	25

Blacklisted Mobile Apps: 17

by Store Type:

Secondary	16
Official	1