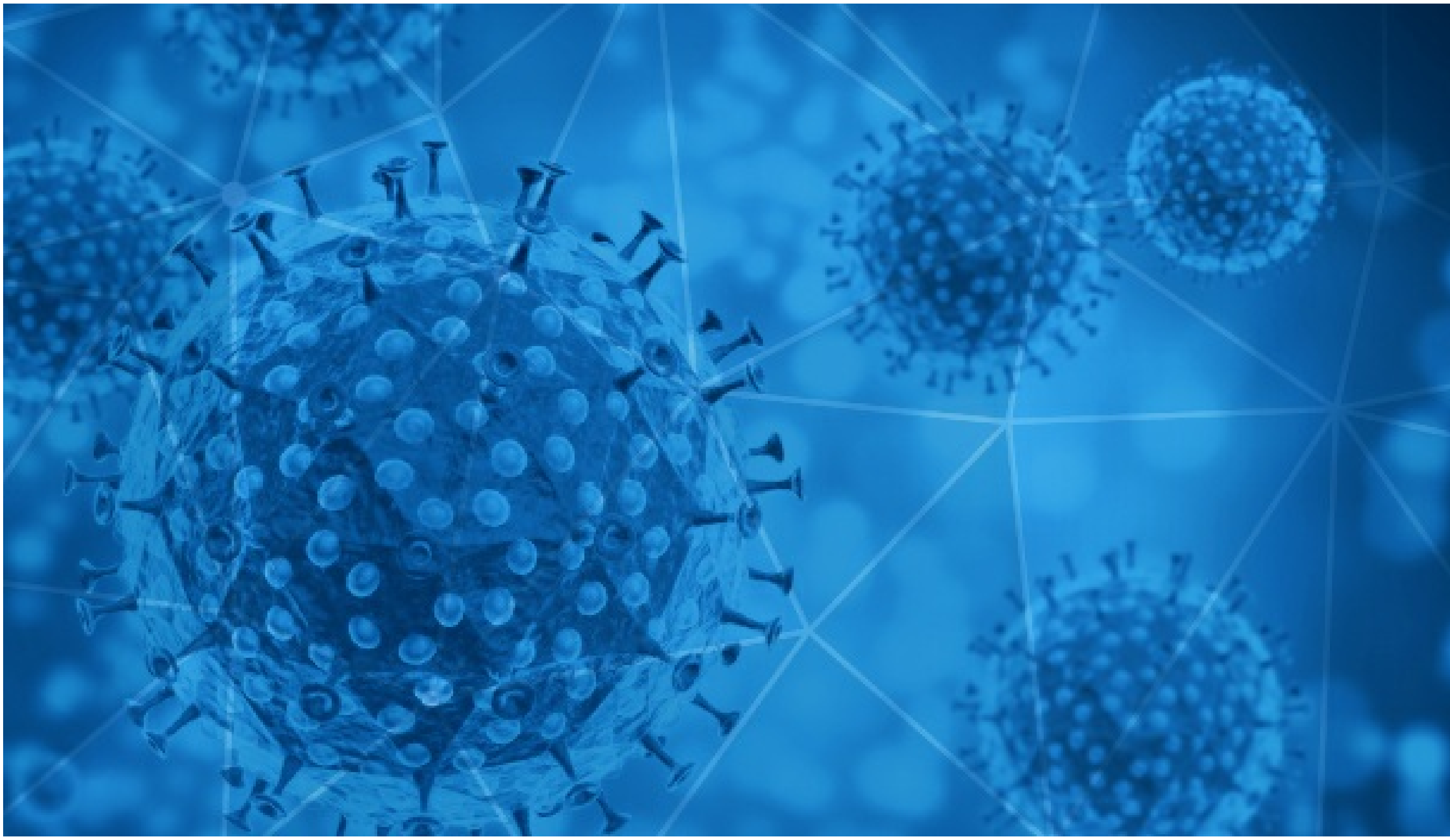
RiskIQ i3:

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

2020-05-21



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 2020-05-20 to 2020-05-21. During this period, RiskIQ analyzed 78,828 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 6,613 unique subject lines observed during the reporting period. The spam emails originated from 5,128 unique sending email domains and 9,235 unique SMTP IP Addresses. Analysts identified 63 emails which sent an executable file for Windows machines.

Top-25 Subjects

Re: UN COVID-19 Stimulus	3521
The Corona Letter: What number should India really be worried about?	3123
Products for COVID-19	2701
Venda muito mesmo em tempos de COVID-19	2665
Top universities to start online courses by May 30 | Cisco is hiring software engineers amid COVID-19; Apply here	2526
HELP IN DONATION FOR COVID-19	2514
Insumos Hospitalarios para DESINFECCION de Empresas COVID	2369
Re: Vanity upon Vanity, COVID -19	1627
Welche Maske sollten Sie gegen das Coronavirus tragen? Hier die Informationen und alles Wissenswerte	1476
New Inquiry from Mfl Group,Inc (Stay Safe against COVID-19)	1313
The COVID-19 Solidarity Response Fund	1289
COVID19 Offer -85%	1275
Competencias a desarrollar durante el Covid-19	966
Bain & Company's latest insights on the impact of COVID-19	965
Sales: Face Mask, Gloves & COVID-19 Safety Kits	960
Container Consolidation for Covid-19 prevention cargo	941
Per le Sue necessitï¿½, abbiamo una linea di dispositivi di Protezione AntiCovid. Ci contatti senza impegno	902
The COVID-19 Response Fund	872
USAID MONETARY DONATION FOR COVID-19	857
Redeem Your COVID-19-Financial Relief Today	702
Webinar gratuito - Prevención y control del covid en el trabajo	592
COVID-19: PAYMENT SUM OF US$2.2 MILLION	483
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO ANTE EL COVID19	458
Material Médico & Prevención Covid 19	428
ComputerVault: Stops Coronavirus with Remote Work	413

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmail.com	6599
onet.eu	3521
timesofindia.com	3125
medicproduction.com	2827
126.com	2588
techgig.com	2526
trendingtopic.cl	2369
163.com	2021
viaalagoas.uno	1982
yellowpagescloud.net	1498

Top-15 IPs Sending COVID Spam

103.141.137.241	3521
209.58.149.66	2700
219.65.84.187	2513
172.93.148.167	1312
23.254.202.134	1287
203.130.242.179	1179
80.211.76.14	1023
217.61.107.95	964
45.95.169.159	960
103.30.17.43	941

Top-15 Countries Sending COVID Spam

US	21776
CN	7346
IN	6751
--	5659
FR	4256
IT	3930
DE	3731
JP	3345
CZ	2912
AR	1621

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Bail-out funds Application for covid-19 Pandemic Treat as Urgent	53
consignes de réouverture des piscines et des jacuzzis dans le cadre de pandémie covid-19	1
CP - Covid-19 – Maintien de l’activité économique : retour sur un chantier exemplaire	1
piscines et covid	1

Top-15 Subjects Containing doc/xlsx Files

Covid-19 Compensation Fund	10
Mayo - 23 - Aplicación de la ley Humanitaria - Reducción de Horarios, Jornadas, Salarios / Directrices Laborales en emergencia sanitaria / COVID-19 como enfermedad común.	6
PROTEGE A TU EMPRESA FRENTE AL COVID	6
Best Protective Items against the COVID-19, 100% true CE certificate with NB number	5
Covid-19 Compensation Fund	5
Sale!!! All New Covid Safety Kits to Safeguard your Guests - as low as $3.48ea from GreatSunrise05152020.docx	5
Dokumentacja pracownicza w dobie COVID19 - szkolenie on-line	4
Rilis Di Masa Pandemic Covid-19, Tak Perlu Menunggu Akhir Ramadan untuk Berzakat & Atasi Dampak Covid-19, Ulama Bersama ACT Deklarasikan Gerakan Satu Bantu Satu	4
тесты на антитела Covid-19	2
05.19.2020 TeamAmerica Hotel Closures_Extensions_Updates_Covid19_No11	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: 96,828
Domains with Potential Mail Servers: 2,872
Email-Capable Domains and Hosts: 36,256
Live Hosts and Domains Not Parked: 38,674

Mobile Apps

Apps in Official Stores: 244

by Store

Apple	135
Google	102
WindowsPhone	6
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 522

by Store Type:

Hybrid	298
Secondary	199
Affiliate	25

Blacklisted Mobile Apps: 17

by Store Type:

Secondary	16
Official	1