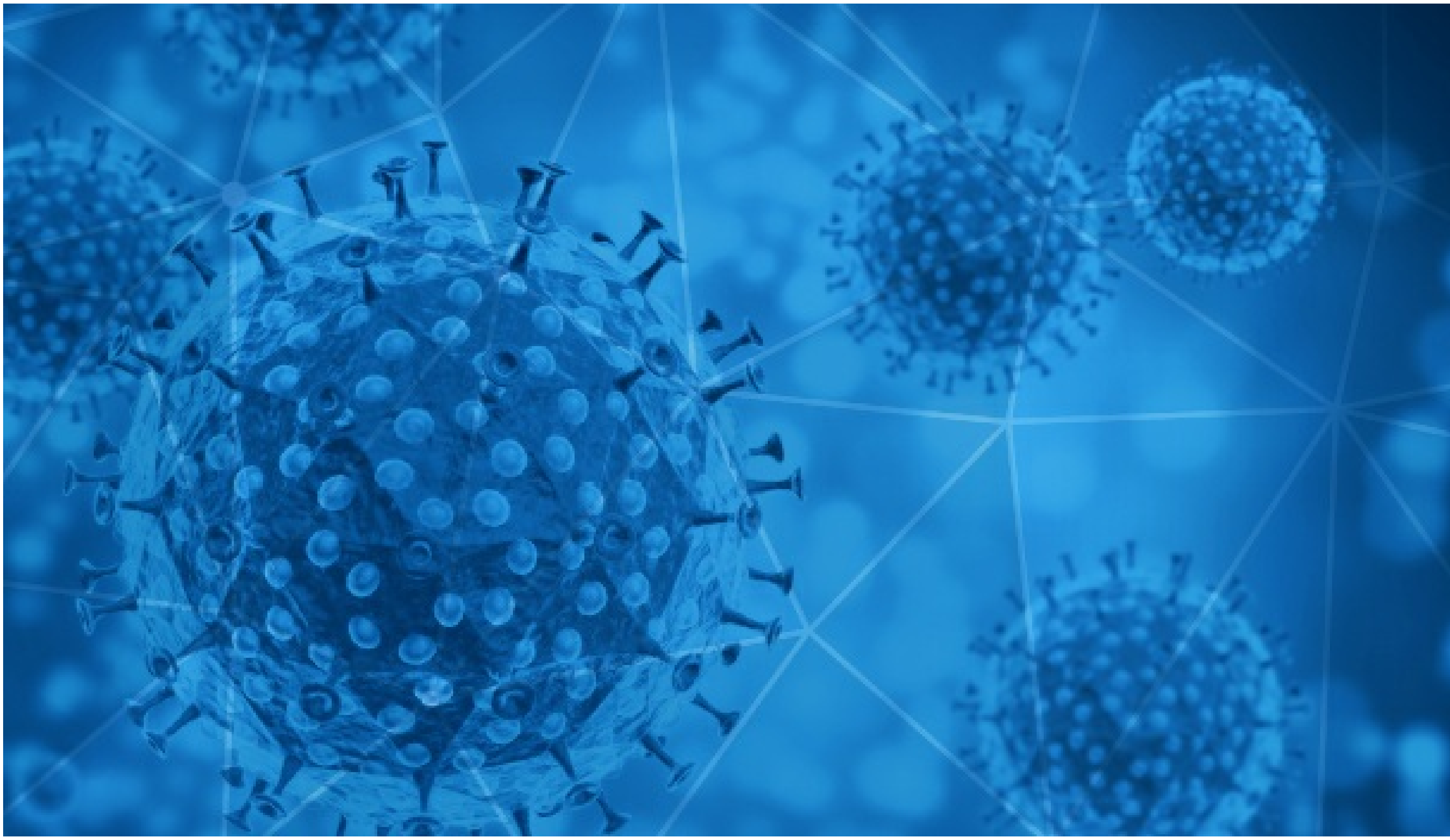
RiskIQ i3:

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

2020-05-27



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 2020-05-26 to 2020-05-27. During this period, RiskIQ analyzed 89,736 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 5,815 unique subject lines observed during the reporting period. The spam emails originated from 4,016 unique sending email domains and 7,374 unique SMTP IP Addresses. Analysts identified 12 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	15423
COVID-19 Stimulus Package Grant(s)	6452
Catalogo articulos prevencion Covid-19	5977
Re: Vanity upon Vanity, COVID -19.cc	4703
The Corona Letter: What's wrong with Gujarat's Covid model?	2891
Protejase del Covid-19, Productos Certificados	2602
Covid19- GRANT RELIEF FUNDS FOR CORONAVIRUS PANDEMIC	2370
Coronavirus cases rise in 18 states, why rats are getting aggressive, and more from Apple News	2102
- 3,5% bis 7,5% mit nachhaltigen Sachwerten: sinnvoll und solide investieren in Corona-Zeiten	1490
Re: UN COVID-19 Stimulus	1358
Informacion COVID-19	977
Demander votre kitde confinement COVID-19	864
Covid19- GRANT RELIEF FOR CORONAVIRUS PANDEMIC	825
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO ANTE EL COVID19	762
Products for COVID-19	708
Navigating Covid-19: The Economic Shakeup	705
Productos Covid 19	691
EN METROPOLITAN CARE ESTAMOS PREPARADOS PARA EL COVID-19	613
Soliciting For COVID-19: UN	607
¡Conoce los productos para combatir el Covid-19!&#128567;	604
Limpiapies Desinfectante covid 19	577
Operación renove en fichaje horario por COVID19	462
****Covid-19: Fordern Sie Ihre Versicherungsleistung an ****	452
COVID-19 Relief Payment Approval (Ref: C19V202991)	432
COVID-19 EMERGENCY DELIVERY OF YOUR CONSIGNMENT BOX TODAY.	425

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

toyotacarrr.com	15427
gmail.com	10595
trendingtopic.cl	9079
mail.ru	6452
outlook.com	3793
timesofindia.com	2895
163.com	2156
insideapple.apple.com	2102
alison1.xyz	1670
onet.eu	1358

Top-15 IPs Sending COVID Spam

82.134.25.158	6452
46.101.3.131	3897
91.143.80.127	3194
51.77.33.43	2326
51.77.33.39	2119
51.38.159.218	2012
51.77.33.44	1996
103.141.137.241	1358
51.38.157.47	1020
181.46.136.165	762

Top-15 Countries Sending COVID Spam

US	16996
JP	15816
FR	11318
NO	6464
DE	5635
GB	5223
IN	5049
CN	5024
--	2348
CA	2186

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Re: Contact Information Request/COVID 19 Request	5
COVID STOP - INOXIS ET PONDY LASER	3
Fw: Cas d'exposition fortuite à patient COVID	1

Top-15 Subjects Containing doc/xlsx Files

CIRCULAR 2 ON COVID 19 AND LEARNING	10
Covid-19 Related Products Price List	6
La crisis del COVID-19 disparará el número de hogares madrileños con todos sus miembros en paro	6
3DCOVID19.TECH cesa su actividad altruista tras donar miles de protectores faciales y piezas de respirador	6
Covid 19 Sanitizing tunnels -Affordable protection for your staff and clients	6
La crisis del COVID-19 disparará el número de hogares catalanes con todos sus miembros en paro	4
Confirmación de participación - Seminario Técnico: Implementación de protocolos de Seguridad y Salud, en la construcción, industria y minería frente al COVID-19	4
AUN NO INICIA ACTIVIDADES CURSO ENFRENTANDO EL CORONAVIRUS COVID 19 - GRUPO 7	3
Analisi idealo - E-commerce e prodotti per gli animali.\tAndamento\tricerche online e prezzi durante l'emergenza Covid	3
IMSS BOLETÍN 338.- Se reconoce al personal de salud del IMSS frente al COVID-19 con el “Mural a los Héroes de la Salud” del CMN Siglo XXI (LINK VIDEO Y FOTOS)	3

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: 98,774
Domains with Potential Mail Servers: 2,974
Email-Capable Domains and Hosts: 37,100
Live Hosts and Domains Not Parked: 39,653

Mobile Apps

Apps in Official Stores: 273

by Store

Apple	161
Google	105
WindowsPhone	6
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 557

by Store Type:

Hybrid	323
Secondary	208
Affiliate	26

Blacklisted Mobile Apps: 17

by Store Type:

Secondary	16
Official	1