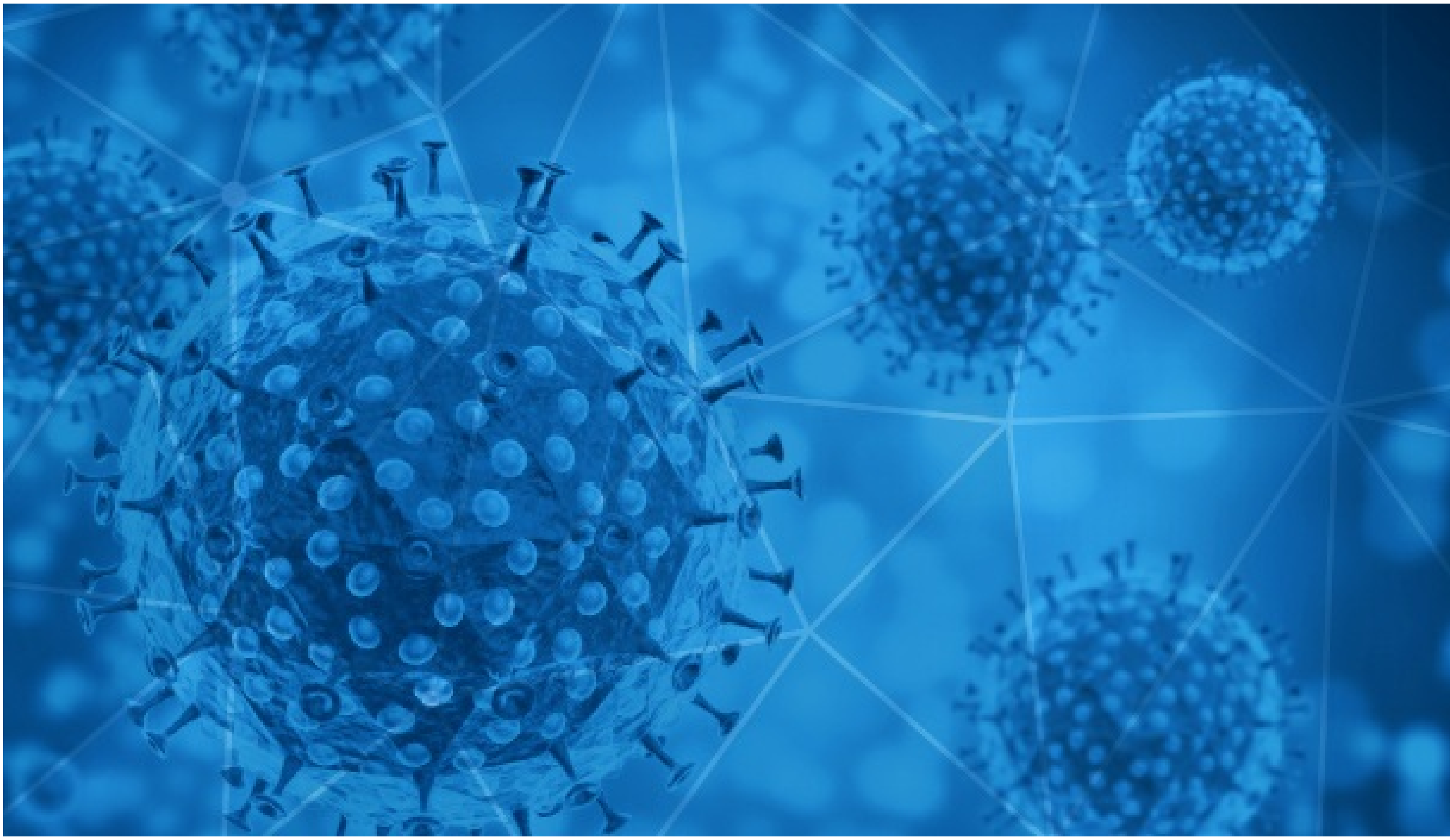
RiskIQ i3:

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

2020-10-29



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 2020-10-28 to 2020-10-29. During this period, RiskIQ analyzed 36,152 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,857 unique subject lines observed during the reporting period. The spam emails originated from 2,191 unique sending email domains and 4,504 unique SMTP IP Addresses. Analysts identified 10 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Misguided antibodies behind Covid mysteries	3636
Test rapidos de covid19 aprobados por ANMAT	1313
Boost your internet speeds while you're quarantined from the CoronaVirus	1298
Precio test covid19	1290
Proteja su negocio de COVID19 y ofrezca seguridad a sus clientes	1240
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	1017
Evite el coronavirus en su negocio	605
COVID19 - PANDEMIC GRANT FUNDS	590
Covid-19-Solidaritï¿½tsreaktionsfonds	585
ATENCION COVID-19 Estudio Contable, Legal e Impositivo para tu negocio	583
WORLD HEALTH ORGANIZATION $500,000 GRANT CONFIRMATION FOR CORONA VIRUS	558
COVID-19 Asesoramiento contable para tu empresa	544
COVID-19 PANDEMIC RELIEF GRANT FUNDS OF $2,200,000 USD	510
Facebook COVID-19 Relief Support Fund	486
COVID-19 Compensation Claim	473
Save your family! Covid19 initiative	409
Protégete RESPONSABLEMENTE Contra el Covid -19 / Los Mejores Precios	406
How to make $3780.23/mth during the 'corona recession'	406
Productos Covid-19	365
Covid Antibody IgG and Total Antibodies - Free Home Visit - Rs.800/-	351
Re: Your Order Corona virus pills and Sex pills	319
Contactless infrared body temperature thermometer defeat Coronavirus	308
Re: Defeat Coronavirus, non contact fever alarm device	297
Fortify Your Digital Assets in the Post COVID-19 Era I Sync Up With Top CISOs @ ETCISO Decrypt I 6 Nov	295
Aprovecha Productos COVID en Oferta!	295

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

walla.co.il	5575
timesofindia.com	3640
gmail.com	3559
yandex.com	1100
126.com	930
keyable.net	885
timesjobs.com	867
yeah.net	805
bowellobby.cyou	732
deletetrick.cyou	566

Top-15 IPs Sending COVID Spam

190.247.223.222	2034
190.247.223.187	1552
204.246.137.80	1100
181.46.136.168	1017
201.231.115.236	806
201.231.5.153	740
91.151.88.58	723
82.223.68.130	652
113.116.206.175	600
91.151.88.66	558

Top-15 Countries Sending COVID Spam

US	7887
AR	6769
IN	5420
CN	4325
FR	1577
DE	1501
TR	1413
ES	978
IT	903
JP	602

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

COVID-19/FluA+B Antigen Combo Rapid Test	8
Questionnaire COVID	1

Top-15 Subjects Containing doc/xlsx Files

Dwudniowy kurs Kadry i płace w dobie COVID 19 - szkolenie on-line	11
COVID-19 WEBINAR DIRETTA STREAMING Processi di DIGITALIZZAZIONE e DEMATERIALIZZAZIONE: presidi normativi e GDPR 1/12/20	9
PHHS 10 27 2020 End of Day COVID 19 Summary	7
PHHS 10 28 2020 End of Day COVID 19 Summary	7
Laguna Travel Agency: CAPODANNO 2020/21 "Tour tra le meraviglie di VENEZIA & LE ISOLE DI MURANO, BURANO E TORCELLO" dal 31 Dicembre 2020 al 03 Gennaio 2021 - 03 ESCURSIONI CON GUIDA & GIRO IN GONDOLA - in omaggio Assicurazione Covid-19	5
Enfermeras expertas en vacunación instan a inmunizar a los niños del meningococo ACWY para evitar mayores problemas de salud pública durante la crisis del COVID-19	4
COMUNICATO STAMPA Coronavirus, Confagricoltura: bene l’impegno per l’agroalimentare, ma serve un piano per la ripresa oltre l’emergenza	3
[Università di Verona] Servizi pubblici per la crescita - domani appuntamento con la rassegna "Economia veneta e Covid"	2
Dinant Brinda Apoyo a 100,000 Familias Ante Emergencia de Covid-19	2
FAO Headteacher: Coronavirus Update 27 October	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: 130,749
Domains with Potential Mail Servers: 2,647
Email-Capable Domains and Hosts: 49,500
Live Hosts and Domains Not Parked: 46,399

Mobile Apps

Apps in Official Stores: 466

by Store

Apple	235
Google	216
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,657

by Store Type:

Hybrid	872
Secondary	727
Affiliate	58

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1