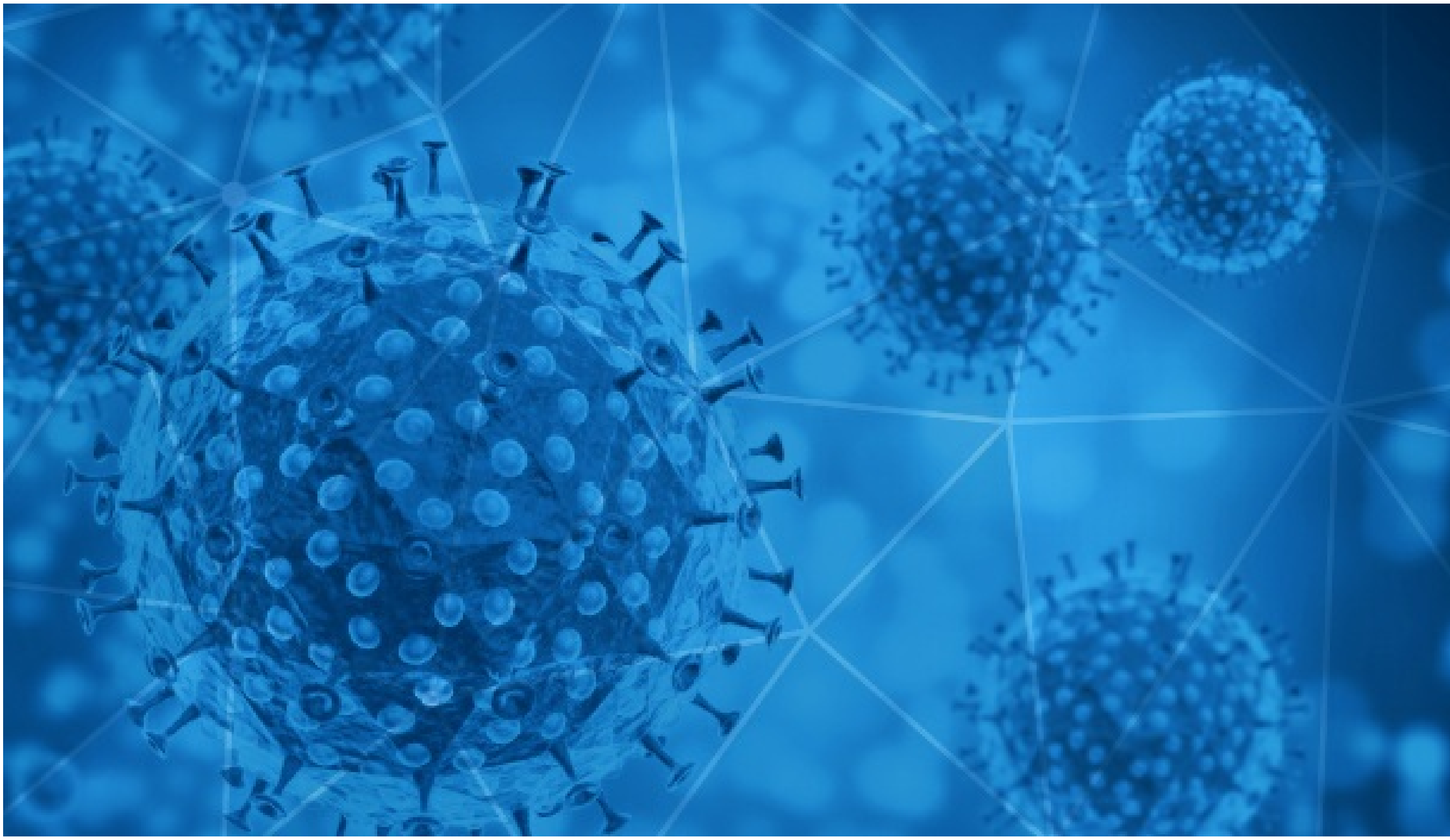
RiskIQ i3:

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

2021-02-12



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 2021-02-11 to 2021-02-12. During this period, RiskIQ analyzed 48,852 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 7,042 unique subject lines observed during the reporting period. The spam emails originated from 2,028 unique sending email domains and 4,305 unique SMTP IP Addresses. Analysts identified 450 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	17787
Lawmakers share harrowing new footage from Capitol attack, why the U.S. is underestimating COVID reinfection, and more from Apple News	5213
The Corona Letter: The silent treatment before or after getting a shot	3500
COVID-19 vaccines are becoming more available for people over 65	1883
TermoScanner e strumenti DPI Anti-Covid in pronta consegna con sconti oltre il 70% e prezzi a partire da Euro 39,00 + spedizione gratuita. Non Abbassiamo la guardia!!!	854
redacted@threatwave.com Test zur Erkennung von COVID-19 Antigene und Antikörper zum besten Preis an	749
UN Covid-19 Winning Notificationw	700
_Step_Closer_To_FDA_ Approval_ 20 People_Take COVID19_ PILL!	565
ICO Covid Inversión	500
Introducing Instant Covid-19 Home Test App	438
Can covid vaccines kill ice blasting this year?	425
Looking for the perfect COVID PROOF BUSINESS TODAY!?	326
Are Covid Restrictions or Economic Barriers Impacting your Bottom Line? Obtain Business Funding | Request Details	283
NHS faces Covid reforms	232
[CND Español - 4335]. Hotelería y Covid: Todo lo que llegó para quedarse	214
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	206
RE: CIERRE CONTABLE Y TRIBUTARIO 2020 | Impacto del COVID-19	202
Waarom de ‘geheime enveloppen’ zo belangrijk zijn voor De Pauw - Gerecht valt binnen in mestbedrijven - Mike Pence en Mitt Romney op de vlucht voor aanval op Capitool - Coronablog | Griepepidemie blijft uit in ons land - Jeff Hoeyberghs riskeert…	175
COVID-19 AFTERMATH.	173
Venta de pruebas Rápidas de Detección de Anticuerpos IgG/IgM y Antígenos para COVID-19	172
Covid 19 benefit Winner	170
Re: covid-19 touch monitor	134
SP CONTRA A COVID-19!	129
Re: Personal, SME & Business Relief [COVID-19]	122
Your Ultimate Protection against COVID-19. US FDA Registered	121

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

giant-pw.com	17790
insideapple.apple.com	5213
timesofindia.com	3509
hospiramedical.co.uk	3370
subscriptions.medicare.gov	1883
gmail.com	1541
herculist.com	889
livejob.it	864
kaufenantigentest.de	749
sabaziusiv.com	479

Top-15 IPs Sending COVID Spam

172.245.93.102	3256
185.221.173.42	864
103.225.55.228	840
103.225.53.40	752
96.9.253.31	749
103.225.53.68	592
216.87.190.231	564
219.65.85.11	552
103.225.53.105	485
84.38.133.27	438

Top-15 Countries Sending COVID Spam

US	18268
JP	17839
IN	3718
IT	1081
CN	905
FR	869
DE	812
NL	757
ES	671
GB	565

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Introducing Instant Covid-19 Home Test App	438
Communiqué de presse - COVID 19 - Arrivées du Vendée Globe à huis clos dans le cadre de l'urgence sanitaire	1

Top-15 Subjects Containing doc/xlsx Files

WEBINAR COVID 19 Superbonus 110%: novità Legge Bilancio, Circolare 30/E AdE, procedure, documentazione - 4 CFP Odcec - 11/3/21	24
Ocena ryzyka zawodowego w czasie pandemii COViD.- szkolenie on-line	9
UN Covid 19 Relief fund.	6
Workplace based Management courses post Covid19	5
Save the Date - Palisades Institute: The Impact of COVID-19 on Women in Business and Its Implications for the Future	4
Covid-19: estudo da UA diz que ‘super dissiminadores’ deveriam ser vacinados primeiro	3
Notification of Confirmed Covid-19 Case on the Campus	2
Báo cáo PCDB COVID-19, NGÀY 11/2/2021	2
Buletin de presa 11.02.2021 + comunicat actiuni COVID	2
covid	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: 143,251
Domains with Potential Mail Servers: 2,590
Email-Capable Domains and Hosts: 52,070
Live Hosts and Domains Not Parked: 44,620

Mobile Apps

Apps in Official Stores: 510

by Store

Apple	251
Google	242
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,083

by Store Type:

Hybrid	1066
Secondary	950
Affiliate	67

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1