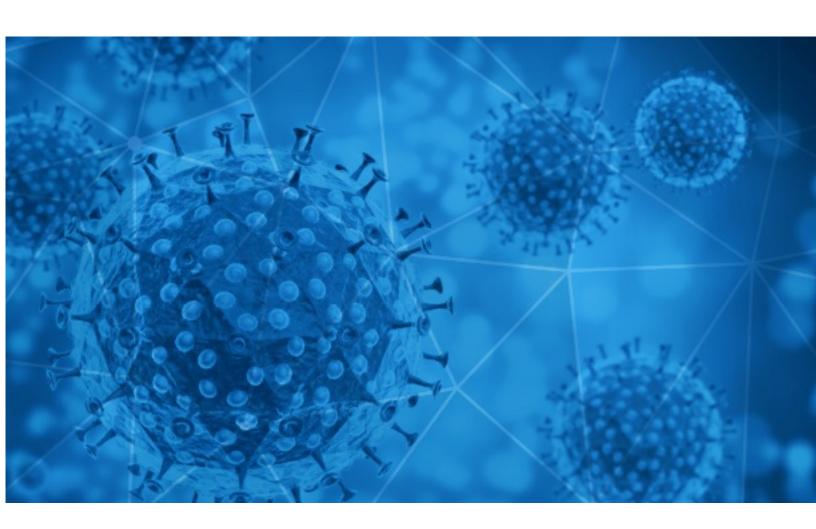


RiskIQ i3:

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

2021-03-03





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, RisklQ 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 RisklQ 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 RisklQ makes no representation or warranty, express or implied, as to the accuracy or completeness of the information. The customer agrees that RisklQ shall not have any liability resulting from their use of this information.

Notice

As of 05/15/2020 RisklQ changed the format and frequency of the COVID-19 Daily Update. Each Friday, RisklQ 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

RisklQ 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

RisklQ analyzed its spam box feed for the time period of 2021-03-02 to 2021-03-03. During this period, RisklQ analyzed 41,694 spam emails containing either "*corona*" or "*COVID*" in the subject line. There were 3,522 unique subject lines observed during the reporting period. The spam emails originated from 2,066 unique sending email domains and 3,991 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

elief OVID-19 Financial Relief to receive your R35,400 government issued financial elief The Corona Letter: Vaccination & your viral load Free Recorded Webinar How can you keep sales grow under Covid-19? Get repared for the digital trend! Redicare covers the COVID-19 vaccine at no cost to you INCHE IN ITALIA test COVID19 salivare OU ARE LUCKY WINNER OFPALLIATIVE PROMO OF COVID19 Fontactless infrared body temperature thermometer defeat Coronavirus Field Coronavirus, Thermographic Camera Field Price Coronavirus, non contact fever alarm device Field Price Recorded Webinary Field Recovery Fund of \$1,500,000.00 US Dollars Field Recovery Fund of \$1,500,000.00 US Dollars Field Representation Gamera defeat Coronavirus Field Representation Field Recovery Fund of \$1,500,000.00 US Dollars Field Representation Field Recovery Fund of \$1,500,000.00 US Dollars Field Representation Field Recovery Field	Top 23 Subjects	
Pelief The Corona Letter: Vaccination & your viral load Free Recorded Webinar How can you keep sales grow under Covid-19? Get prepared for the digital trend! Medicare covers the COVID-19 vaccine at no cost to you 1806 INCHE IN ITALIA test COVID19 salivare 1081 OU ARE LUCKY WINNER OFPALLIATIVE PROMO OF COVID19 2001 Contactless infrared body temperature thermometer defeat Coronavirus 201 202 203 203 204 204 205 205 206 207 207 207 207 207 207 207 207 207 207	COVID-19 Financial Relief to receive your R23,400 government issued financial relief	11287
Free Recorded Webinar How can you keep sales grow under Covid-19? Get prepared for the digital trend! Medicare covers the COVID-19 vaccine at no cost to you 1886 MINCHE IN ITALIA test COVID19 salivare 1881 OU ARE LUCKY WINNER OFPALLIATIVE PROMO OF COVID19 937 Contactless infrared body temperature thermometer defeat Coronavirus 656 Mefeat Coronavirus, Thermographic Camera 644 Mete: Defeat Coronavirus, non contact fever alarm device 628 Mermographic Automation Camera defeat Coronavirus 610 MIN COVID-19 Response and Recovery Fund of \$1,500,000.00 US Dollars 700 US PUNDS 700	COVID-19 Financial Relief to receive your R35,400 government issued financial relief	4605
Medicare covers the COVID-19 vaccine at no cost to you 1806 MCHE IN IT ALIA test COVID19 salivare 1081 OU ARE LUCKY WINNER OFPALLIATIVE PROMO OF COVID19 1081 1	The Corona Letter: Vaccination & your viral load	2908
INCHE IN ITALIA test COVID19 salivare OU ARE LUCKY WINNER OFPALLIATIVE PROMO OF COVID19 937 contactless infrared body temperature thermometer defeat Coronavirus 656 Defeat Coronavirus, Thermographic Camera 644 Defeat Coronavirus, non contact fever alarm device formographic Automation Camera defeat Coronavirus 610 NI COVID-19 Response and Recovery Fund of \$1,500,000.00 US Dollars 70 OVID FUNDS Penta de Pruebas Suizas Spring Healthcare para descarte de Covid-19. 71 Appum скидку 15% на обязательный ПЦР-тест на Covid-19 Petrogen is now performing diagnostic testing for COVID-19 Petrogen is now performing diagnostic testing for COVID-19 Petrogen is graph solution for Co	∏Free Recorded Webinar∏How can you keep sales grow under Covid-19? Get prepared for the digital trend!	1988
OU ARE LUCKY WINNER OFPALLIATIVE PROMO OF COVID19 Sontactless infrared body temperature thermometer defeat Coronavirus Sefeat Coronavirus, Thermographic Camera Set Defeat Coronavirus, non contact fever alarm device Set Defeat Coronavirus Se	Medicare covers the COVID-19 vaccine at no cost to you	1806
Contactless infrared body temperature thermometer defeat Coronavirus Defeat Coronavirus, Thermographic Camera Defeat Coronavirus, non contact fever alarm device Defeat Coronavirus, non contact fever alarm device Defeat Coronavirus, non contact fever alarm device Defeat Coronavirus Defeat Corona	ANCHE IN ITALIA test COVID19 salivare	1081
Refeat Coronavirus, Thermographic Camera Re: Defeat Coronavirus, non contact fever alarm device Remographic Automation Camera defeat Coronavirus Response and Recovery Fund of \$1,500,000.00 US Dollars ROVID-19 Response and Recovery Fund of \$1,500,000.00 US Dollars ROVID FUNDS Renta de Pruebas Suizas Spring Healthcare para descarte de Covid-19. Rapum скидку 15% на обязательный ПЦР-тест на Covid-19 Retrogen is now performing diagnostic testing for COVID-19 Retrogen is now performing diagnostic testing for COVID-19 Reterogen Suizas Spring Healthcare para descarte de Covid-19. Retrogen is now performing diagnostic testing for COVID-19 Retrogen is now performing diagnostic for English for COVID-19 Retrogen is now performing diagnostic for English for COVID-19 Retrogen is now performing diagnostic for English for COVID-19 Retrogen is now performing diagnostic for English for COVID-19 Retrogen is now performing for COVID-19 Retrogen is now performing for COVID-19 Retrogen i	YOU ARE LUCKY WINNER OFPALLIATIVE PROMO OF COVID19	937
Re: Defeat Coronavirus, non contact fever alarm device Thermographic Automation Camera defeat Coronavirus The COVID-19 Response and Recovery Fund of \$1,500,000.00 US Dollars TOVID FUNDS Tenta de Pruebas Suizas Spring Healthcare para descarte de Covid-19. TARABUM СКИДКУ 15% На ОБЯЗАТЕЛЬНЫЙ ПЦР-ТЕСТ НА COVID-19 THE CO	Contactless infrared body temperature thermometer defeat Coronavirus	656
Thermographic Automation Camera defeat Coronavirus IN COVID-19 Response and Recovery Fund of \$1,500,000.00 US Dollars SOVID FUNDS Tenta de Pruebas Suizas Spring Healthcare para descarte de Covid-19. Дарим скидку 15% на обязательный ПЦР-тест на Covid-19 Setrogen is now performing diagnostic testing for COVID-19 Setrogen is now performing diagnostic testing for COVID-19 Set Digital signage solution for Covid-19 QC] AT ALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ KHUẨN PHÒNG CHỐNG COVID-19 JC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation 188 Seronavirus briefing: Hunt for 'patient X' narrows En vivo: ¿Cómo manejar el estrés en los niños por la COVID-19?" 159 Defertas Test Rapido Covid 19 Session 2021 EEOC Issues Guidance for Employers Mandating COVID Vaccines at Vork ICJ Daily - New State Vax System. 30 New COVID Cases. NCJ Recipe Contest. A	Defeat Coronavirus, Thermographic Camera	644
IN COVID-19 Response and Recovery Fund of \$1,500,000.00 US Dollars 380 Yenta de Pruebas Suizas Spring Healthcare para descarte de Covid-19. Дарим скидку 15% на обязательный ПЦР-тест на Covid-19 280 Retrogen is now performing diagnostic testing for COVID-19 254 Gran Venta Outlet - Productos Covid 19 227 QC] AT ALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ KHUẨN PHÒNG CHỐNG COVID -19 218 JC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation 188 Goronavirus briefing: Hunt for 'patient X' narrows En vivo: ¿Cómo manejar el estrés en los niños por la COVID-19?" 159 Dession 2021 EEOC Issues Guidance for Employers Mandating COVID Vaccines at Vork ICJ Daily - New State Vax System. 30 New COVID Cases. NCJ Recipe Contest. A	Re: Defeat Coronavirus, non contact fever alarm device	628
З80 Zenta de Pruebas Suizas Spring Healthcare para descarte de Covid-19. Дарим скидку 15% на обязательный ПЦР-тест на Covid-19 Zetrogen is now performing diagnostic testing for COVID-19 Ziran Venta Outlet - Productos Covid 19 Ziran Venta Outlet - Productos Ou	Thermographic Automation Camera defeat Coronavirus	610
Venta de Pruebas Suizas Spring Healthcare para descarte de Covid-19. Дарим скидку 15% на обязательный ПЦР-тест на Covid-19 vetrogen is now performing diagnostic testing for COVID-19 veran Venta Outlet - Productos Covid 19 veran Venta Outlet - Productos Outlet Outlet I Salar Venta Outlet I Sa	UN COVID-19 Response and Recovery Fund of \$1,500,000.00 US Dollars	457
Дарим скидку 15% на обязательный ПЦР-тест на Covid-19 detrogen is now performing diagnostic testing for COVID-19 detrogen is now performing diagnostic testing for COVID-19 detrogen is now performing diagnostic testing for COVID-19 254 diran Venta Outlet - Productos Covid 19 227 QC] ATALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ KHUẨN PHÒNG CHỐNG COVID -19 218 JC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation 188 deronavirus briefing: Hunt for 'patient X' narrows En vivo: ¿Cómo manejar el estrés en los niños por la COVID-19?" 159 Defertas Test Rapido Covid 19 dession 2021 EEOC Issues Guidance for Employers Mandating COVID Vaccines at Vork ICJ Daily - New State Vax System. 30 New COVID Cases. NCJ Recipe Contest. A	COVID FUNDS	380
tetrogen is now performing diagnostic testing for COVID-19 254 231 231 227 227 227 227 227 228 227 227 228 227 228 227 228 227 228 227 228 227 228 227 228 227 228 228 227 228 228 227 228 227 228 228 227 228 227 228 228 227 228 228 227 228 227 228 228 227 228 227 228 228 227 228 2	Venta de Pruebas Suizas Spring Healthcare para descarte de Covid-19.	372
iran Venta Outlet - Productos Covid 19 227 QC] ATALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ KHUẨN PHÒNG CHỐNG COVID -19 218 JC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation 188 Coronavirus briefing: Hunt for 'patient X' narrows 180 En vivo: ¿Cómo manejar el estrés en los niños por la COVID-19?" 159 Ifertas Test Rapido Covid 19 159 Iession 2021 EEOC Issues Guidance for Employers Mandating COVID Vaccines at Vork ICJ Daily - New State Vax System. 30 New COVID Cases. NCJ Recipe Contest. A	🛮 Дарим скидку 15% на обязательный ПЦР-тест на Covid-19	280
te: Digital signage solution for Covid-19 QC] ATALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ KHUẨN PHÒNG CHỐNG COVID -19 JC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation 188 JC/Onation-ref:K011- You have been Chosen for our COVID-19 Donation 180 En vivo: ¿Cómo manejar el estrés en los niños por la COVID-19?" 159 Jession 2021 EEOC Issues Guidance for Employers Mandating COVID Vaccines at Vork ICJ Daily - New State Vax System. 30 New COVID Cases. NCJ Recipe Contest. A	Retrogen is now performing diagnostic testing for COVID-19	254
QC] ATALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ KHUẨN PHÒNG CHỐNG COVID -19 JC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation 188 Soronavirus briefing: Hunt for 'patient X' narrows En vivo: ¿Cómo manejar el estrés en los niños por la COVID-19?" 159 Session 2021 EEOC Issues Guidance for Employers Mandating COVID Vaccines at Vork ICJ Daily - New State Vax System. 30 New COVID Cases. NCJ Recipe Contest. A	Gran Venta Outlet - Productos Covid 19	231
JC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation 188 Soronavirus briefing: Hunt for 'patient X' narrows En vivo: ¿Cómo manejar el estrés en los niños por la COVID-19?" 159 Session 2021 EEOC Issues Guidance for Employers Mandating COVID Vaccines at Vork ICJ Daily - New State Vax System. 30 New COVID Cases. NCJ Recipe Contest. A	Re: Digital signage solution for Covid-19	227
Iso Coronavirus briefing: Hunt for 'patient X' narrows En vivo: ¿Cómo manejar el estrés en los niños por la COVID-19?" 159 Difertas Test Rapido Covid 19 159 Diession 2021 EEOC Issues Guidance for Employers Mandating COVID Vaccines at Vork ICJ Daily - New State Vax System. 30 New COVID Cases. NCJ Recipe Contest. A	[QC] ATALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ KHUẨN PHÒNG CHỐNG COVID -19	218
En vivo: ¿Cómo manejar el estrés en los niños por la COVID-19?" Difertas Test Rapido Covid 19 Session 2021 EEOC Issues Guidance for Employers Mandating COVID Vaccines at Vork ICJ Daily - New State Vax System. 30 New COVID Cases. NCJ Recipe Contest. A	LJC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation	188
Ofertas Test Rapido Covid 19 Lession 2021 EEOC Issues Guidance for Employers Mandating COVID Vaccines at Vork ICJ Daily - New State Vax System. 30 New COVID Cases. NCJ Recipe Contest. A	Coronavirus briefing: Hunt for 'patient X' narrows	180
vession 2021 EEOC Issues Guidance for Employers Mandating COVID Vaccines at Vork ICJ Daily - New State Vax System. 30 New COVID Cases. NCJ Recipe Contest. A	"En vivo: ¿Cómo manejar el estrés en los niños por la COVID-19?"	159
Vork ICJ Daily - New State Vax System. 30 New COVID Cases. NCJ Recipe Contest. A	Ofertas Test Rapido Covid 19	159
1/43	Session 2021 EEOC Issues Guidance for Employers Mandating COVID Vaccines at Work	148
	NCJ Daily - New State Vax System. 30 New COVID Cases. NCJ Recipe Contest. A Museum Worth Saving. A Healing Conversation.	143

- CONFIDENTIAL -



COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

. •	<i>-</i>
standardbank.co.za	15892
timesofindia.com	2909
keyable.net	2538
service.alibaba.com	1988
subscriptions.medicare.gov	1821
sicurezzanews.it	1081
gmail.com	1014
vivaldi.net	937
unremittanceoffice.us	380
hospiramedical.co.uk	374

Top-15 IPs Sending COVID Spam

, 1	
109.199.69.21	8091
178.22.234.45	7395
113.116.205.0	2387
161.47.81.122	937
82.135.19.130	545
82.135.19.131	536
91.103.25.74	457
88.202.186.250	406
45.117.210.137	380
23.254.229.176	374

Top-15 Countries Sending COVID Spam

	5
US	9870
PL	8183
NL	7608
CN	5202
IN	3512
DE	1616
GB	982
АМ	457
FR	428
RU	381



COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

REGISTER NOW! Living in an Anxious World: COVID-19, Substance Misuse, and the Impact on Families	3
COVID REINFECTION REPORTING FORMAT	3
COVID VACCINATION INFORMATION FOR CHILD CARE PROVIDERS	2
WEB OnLine COVID 19 Appalti e subappalti: direzione e controllo, gestione cantieri e tutela dei lavoratori 25/3/21	2
Buletin de presa 02.03.2021 + comunicat actiuni COVID	2
Calabria: Covid, la sindaca e l'assessore alla Salute del Comune di San Giovanni in Fiore scrivono ai commissari Longo e La Regina, "bisogna vaccinare subito gli anziani e i più fragili"	2
WEB COVID 19 Superbonus 110%: Legge Bilancio 2021, Circolare 30/E AdE, procedure per cessione bonus fiscale 11/3/21 4 CFP Odcec	2
AVISO FORMATO NUEVO COVID-19	2
NHS Test and Trace: COVID-19 testing for students returning from Mon 8 Mar - Reminder.	2
Maski FFP3 z zaworem i bez, FFP2, KN95, Testy Covid i inne produkty - NAJNIŻSZE CENY NA RYNKU APTECZNYM!!!	2

- CONFIDENTIAL -



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: 148,114

Domains with Potential Mail Servers: 2,545 Email-Capable Domains and Hosts: 52,879 Live Hosts and Domains Not Parked: 45,398

Mobile Apps

Apps in Official Stores: 513

by Store

Apple	253
Google	243
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,150

by Store Type:

Hybrid	1091
Secondary	991
Affiliate	68

Blacklisted Mobile Apps: 29

by Store Type:

Secondary	26
Official	2
Hybrid	1