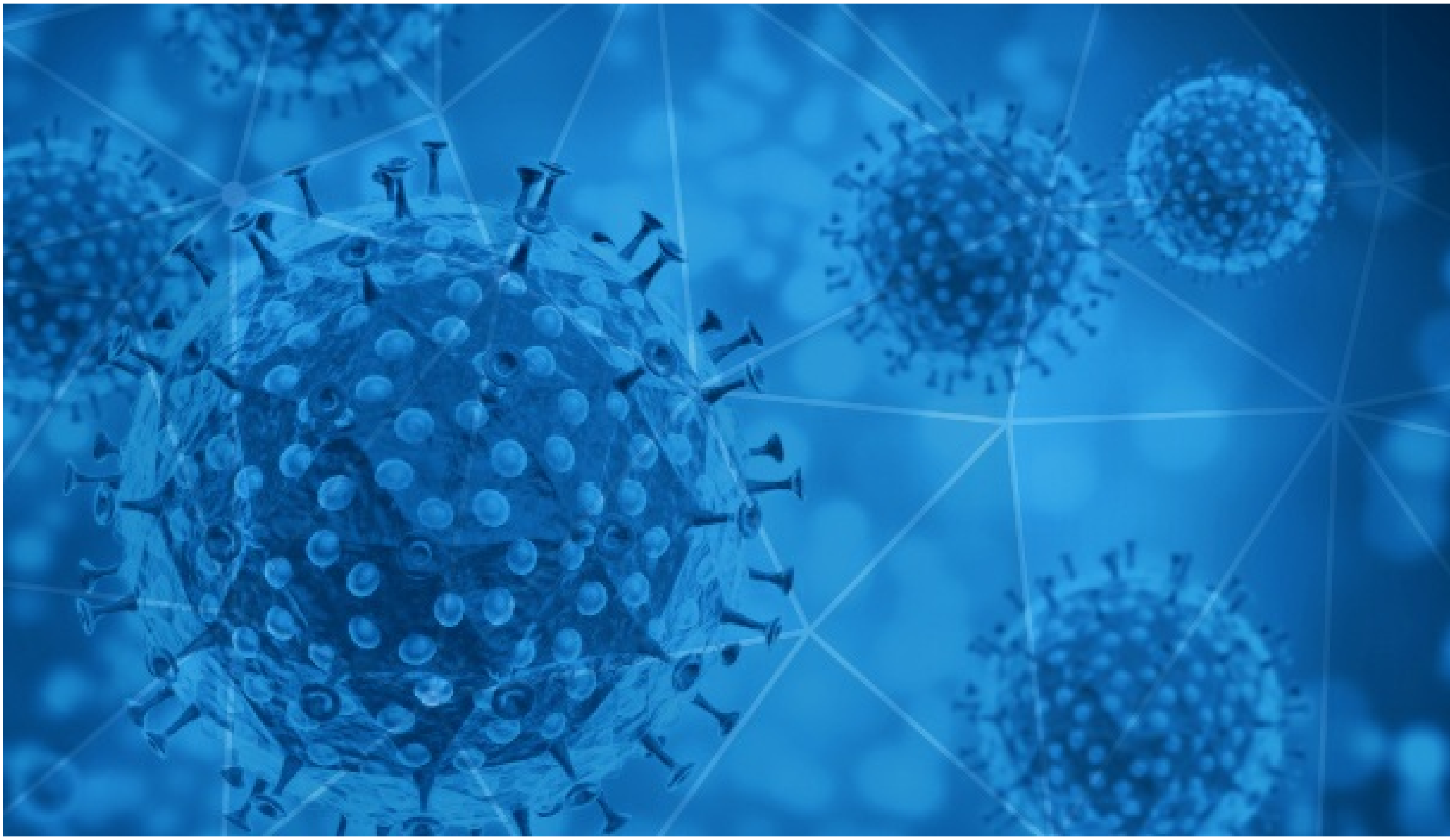
RiskIQ i3:

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

2020-11-04



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 2020-11-03 to 2020-11-04. During this period, RiskIQ analyzed 33,119 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,997 unique subject lines observed during the reporting period. The spam emails originated from 2,336 unique sending email domains and 4,654 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: How chronic Covid affects the entire body	3763
Test rapido para la deteccion del Coronavirus	1433
Corona Schnelltest	1113
CORONA-VIRUS RELIEF FUND UNITED NATION OFFICE{	1043
Proteja su negocio de covid y ofrezca seguridad a sus clientes	953
Triple test para covid de deteccion rapida	798
Ingresaron test de covid de deteccion rapida	583
Covid -19 SPENDE	567
Precio test covid	529
Test rapidos de covid aprobados por anmat	493
TermoScanner Anti-Covid in pronta consegna. Prezzi dimezzati e modelli a partire da soli Euro 499,00. Non Abbassiamo la guardia!!!	437
Evite el coronavirus en su negocio	434
Atencion covid Estudio Contable Legal e Impositivo para tu negocio	427
5 tys. zł za zachorowanie dziecka na COVID-19. Sprawdź>>	408
Covid-19 Impacts Babies with Birth Defects!	363
Best Method For Home Screening - Avoid COVID	322
COVID-19 EFFECT COMPENSATION	315
Avoid COVID - Home Screening Blood Oxygen Meter	311
Aprovecha productos COVID en oferta!!!	301
Conoce las líneas de atención exclusiva COVID 19	299
Vuelve el Covid19 con MÁS FUERZA	299
Contactless infrared body temperature thermometer defeat Coronavirus	289
ATALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ KHUẨN PHÒNG CHỐNG COVID -19	276
Re: Defeat Coronavirus, non contact fever alarm device	273
Instant Covid Antibody IgG + IgM test is available at Rs 750 only | Hurry, Confirm Soon.	259

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

walla.co.il	5650
timesofindia.com	3765
gmail.com	2603
covid-19-schnelltests-24.de	1113
126.com	922
keyable.net	800
yeah.net	785
timesjobs.com	680
conetworkgroup.com	493
livejob.it	437

Top-15 IPs Sending COVID Spam

190.247.226.211	1586
66.43.119.17	1092
201.231.6.251	919
190.247.240.182	898
201.231.6.215	793
113.89.43.70	752
201.231.83.108	716
162.144.52.230	599
89.185.234.197	493
185.221.173.42	436

Top-15 Countries Sending COVID Spam

US	6741
AR	6307
IN	4493
CN	3953
DE	1635
FR	1322
--	1217
IT	1014
GB	789
ES	643

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

PROROGA COVID 19 WEB DIRETTA STREAMING Gestione lavoro, CIGO-CIGD-FIS, contratti espansione, sicurezza, responsabilità 24/11/20	24
COVID 19 WEB DIRETTA STREAMING GESTIONE IMPRESA: obbligatorietà adeguati assetti e MOG 231/01-doveri e responsabilità 2/12/20	18
Dwudniowy kurs Kadry i płace w dobie COVID 19 - szkolenie on-line	17
“La Covid-19 está acabando con la Dieta Mediterránea”, según el Dr. Romero	6
Gruppo Maggioli | Gestione della crisi Covid - 19, una "guida" per piccoli imprenditori e professionisti	3
Oferta na środki ochrony indywidualnej przed Covid-19	3
Δες Άμεσα! COVID 19 - Ενίσχυση μικρών και πολύ μικρών Επιχειρήσεων, Μη Επιστρεπτέα Ενίσχυση!	3
TR: LKPG Promo covid gros volume papier et produits marque	2
Press Release - Celebrating festivals during COVID- 19: an insightful session with DR KK Aggarwal on the 3rd day of 27th HCFI Perfect Health Mela	2
Änderung Kita Öffnungszeiten Coronabedingt	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: 131,475
Domains with Potential Mail Servers: 2,651
Email-Capable Domains and Hosts: 49,986
Live Hosts and Domains Not Parked: 45,811

Mobile Apps

Apps in Official Stores: 468

by Store

Apple	235
Google	218
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,686

by Store Type:

Hybrid	886
Secondary	741
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1