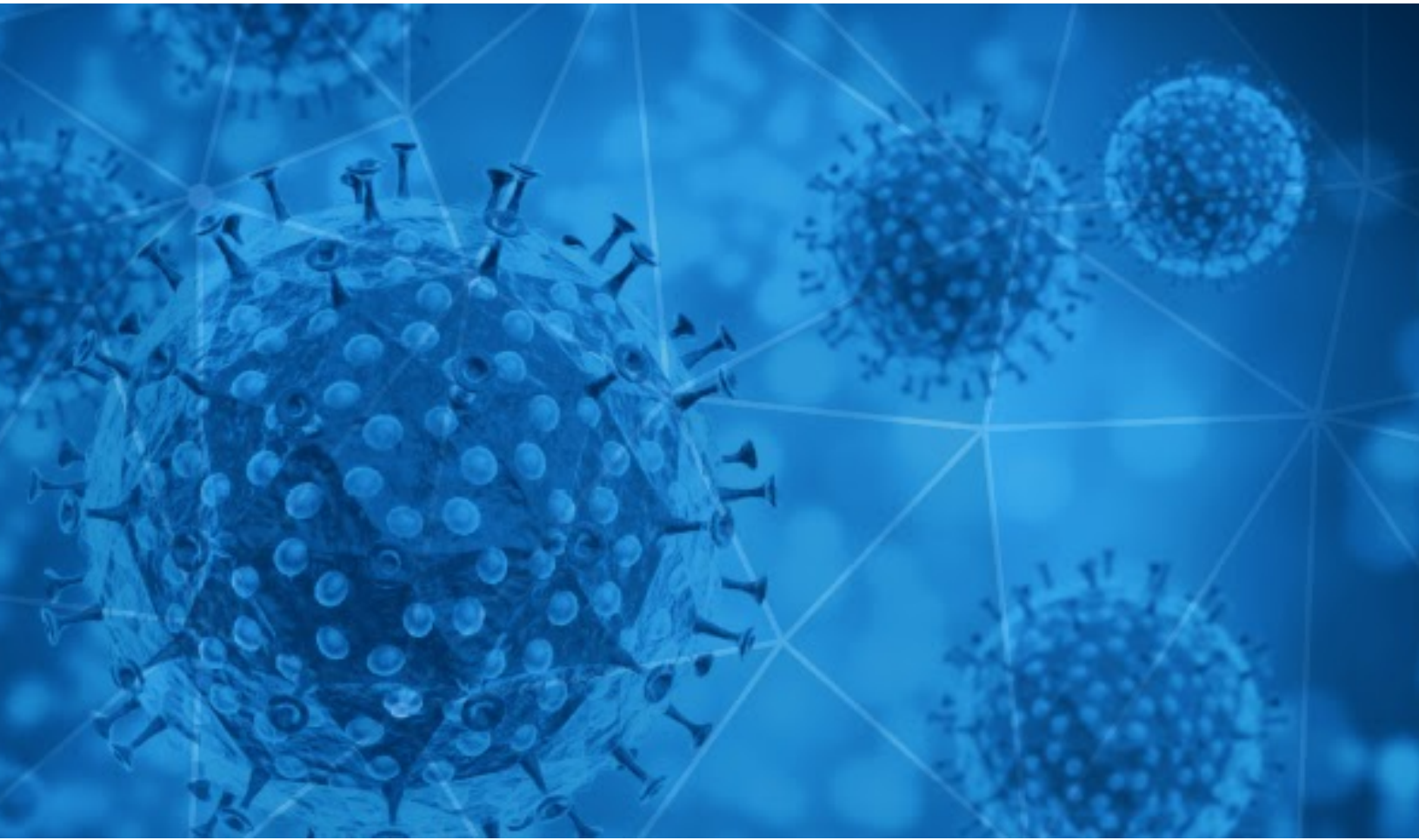
RISKIQ®

RiskIQ i3:

COVID-19 Daily Update

03/31/2020



RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

Table of Contents

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

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. Customer agrees that RiskIQ shall not have any liability resulting from Customer's use of this information.

Notable Events: Previous 24 Hours

Amazon warehouse workers on Staten Island, New York walked off the job in protest of Amazon's treatment of them amid the COVID-19 crisis on 3/30/2020. Amazon tech workers sided with the warehouse workers by demanding the company improve its policies regarding the COVID-19 outbreak. Workers at Amazon-owned Whole Foods are organizing a "sick out" strike to demand better protections.

Moscow went into lockdown on 03/30/2020 and the Russian parliament is expected to approve a bill on 03/31/2020 authorizing prison sentences and fines up to $25,000 for anyone violating the lockdown.

Michigan Governor Gretchen Whitmer is expected to sign an executive order this week which will extend school closures through the rest of the school year.

COVID-19 fatalities in the U.S. have exceeded 3,000 as of 03/31/2020. To date, Wyoming and Hawaii have not reported fatalities. Monday, 03/30/2020, was the deadliest day yet, with more than 500 recorded deaths.

Three out of four Americans are currently under some form of lockdown procedure. Approximately 245 million Americans are under such policies, with 32 of 50 states enacting lockdown policies. Many localities in states without statewide lockdown policies have enacted their own orders. Economic consequences of lockdown procedures are being felt, as the Federal Reserve suggests up to 47 million Americans could be out of work over the coming months.

The Department of Justice (DOJ) is investigating at least one lawmaker's stock transactions leading up to the COVID-19 outbreak. Senator Richard Burr, R-NC, is the only lawmaker known to be under investigation at this time. The investigation is allegedly a cooperative effort between the DOJ and Securities and Exchange Commission (SEC). Neither the DOJ nor the SEC have responded to media questions regarding the investigation.

Macy's, Kohl's, and Gap all announced plans to furlough large portions of their respective workforces without pay. Macy's reported the majority of its 125,000 member workforce would go on furlough this week, but impacted employees would continue to receive health coverage with a fully-covered premium. Gap's furlough will affect around 80,000 employees. Gap will continue to offer benefits to all furloughed employees until stores reopen. Kohl's will furlough store, distribution center, and corporate associates. Kohl's will continue to offer benefits to impacted employees.

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

Digital Exploitation

The Department of Health and Human Services Office of the Inspector General (OIG)'s updated strategy for 2020 to 2025 outlines its goals to fight fraud and abuse, promote quality and safety, and advance innovation. Fighting against cybersecurity threats within the HHS and the healthcare sector is one of the newly added priorities in the OIG's strategy, according to Bloomberg Law reporting.

An Interisle Consulting Group study reveals widespread problems with access to and the reliability of domain name registration data systems (WHOIS). These failures have real-life security implications, which are being seen in the current wave of cybercrime accompanying the COVID-19 pandemic.

RiskIQ has observed a large malware campaign originating out of an Iranian-operated IP address (see Appendix A). The campaign seeks to trick users by impersonating Dr. Gaudean Galea, the official WHO Representative in China, and asking end users to read an attached PDF for updates regarding the novel coronavirus. The email server, 194.180.224.65, has sent over 3,500 emails containing the AgentTesla malware family in the last week alone. The emails are received from the spoofed address of galleag@who.int with a display name of "WHO Representative." RiskIQ continues to further observe and research the campaign.

New Blacklist Data

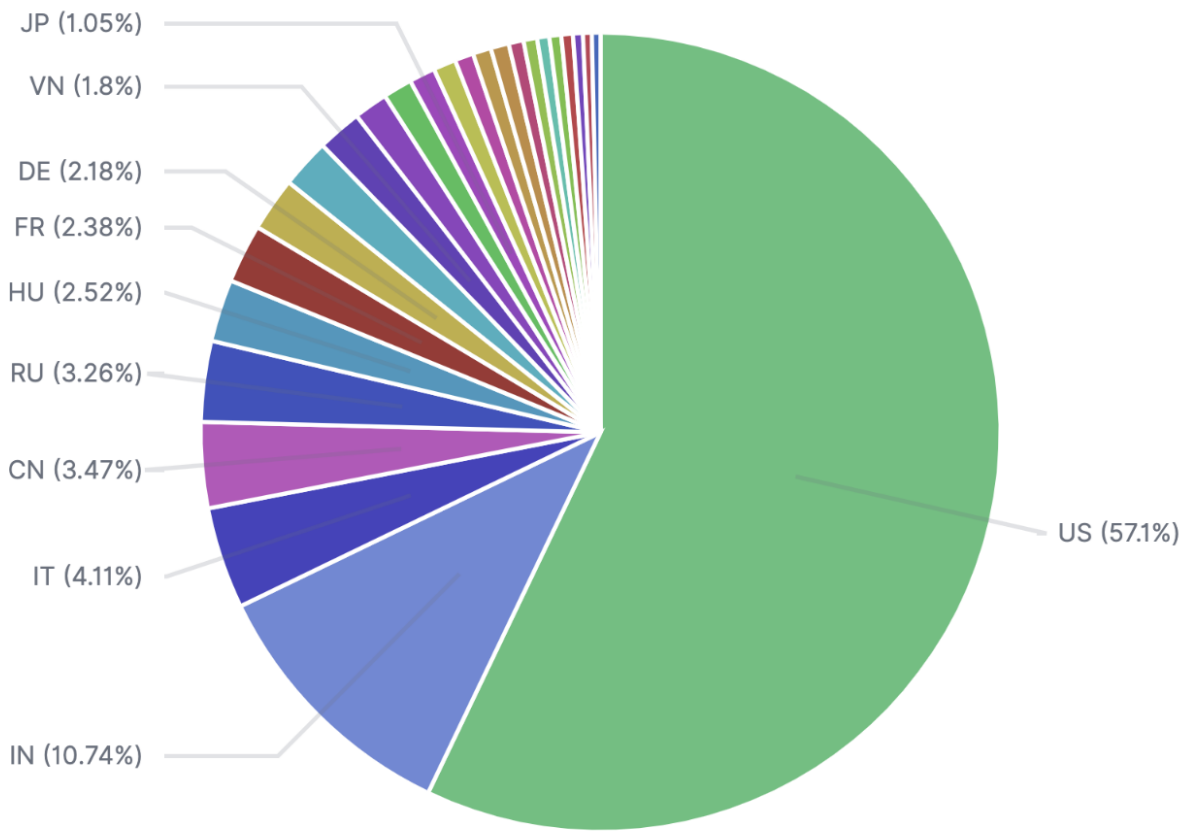
hxxps://coronavirushometestkit[.]co[.]uk/

hxxps://covid-19calistrong[.]com/

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 03/30/2020-03/31/2020. During this period, RiskIQ analyzed 217,169 spam emails containing either “*corona*” or “*covid*” in the subject line. There were 15,692 unique subject lines observed during the reporting period. The spam emails originated from 9,592 unique sending email domains and 15,700 unique SMTP IP Addresses. Analysts identified 1,625 emails which sent an executable file for Windows machines.



Spam emails by country of origin

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

Top 25 Subjects

1. 17,671 - 9,90 - Atemschutzmasken FFP1 (COVID 19)
2. 17,624 - Here is your chance to contribute in India's war against COVID-19!
3. 16,969 - 3 shocking reasons why South Koreans arenâ€ t dying from coronavirus
4. 12,638 - (Quick delivery) Protective mask and Diagnostic kit for COVID-19, goggles, infrared thermometer, protective clothing
5. 11,076 - Notbestände Schutzmasken im Angebot FFP1 (COVID 19)
6. 10,048 - The Mask that can prevent Coronavirus now
7. 8,173 - 10 Schutzmasken 99,- FFP1 (COVID 19)
8. 7,687 - Direkt lieferbare Schutzmasken (COVID 19)
9. 5,006 - Coronavirus is spreading, this specialized mask can control it
10. 3,929 - CORONAVIRUS ï¿½ Senzatetto, senza difese
11. 3,275 - The Corona Letter: Your foodgrain is missing labourers
12. 2,934 - sincerely grateful for your donation to our COVID 19 pandemic frontline health workers
13. 2,815 - [Covid-19] AtualizaÃ§Ã£o de SeguranÃ§a.
14. 2,704 - Feeling Helpless Against Corona?
15. 2,690 - URGENT NEED: U.S. Department of Health & Human Services/COVID-19 Face Mask/ Forehead thermometers
16. 1,959 - COVID19 Offer -85%
17. 1,434 - COVID-19 Solidarity Response Fund for WHO - DONATE NOW
18. 1,314 - Kann das CORONAVIRUS vorgebeugt werden? Atemmaske für wirksamen Schutz
19. 1,296 - Droht CORONAVIRUS? Mit Atemmaske können Probleme vorgebeugt werden
20. 1,286 - Coronavirus, Grippe? Hier ist die Atemmaske mit einem speziellen Filter
21. 1,257 - Hast du Angst vor dem Corona-Virus? Neue Atemmaske, schütze deine Lieben
22. 1,254 - Check out ""Tampa Pastor Arrested for Packing Megachurch During Coronavirus Out Break"" on Wane Enterprises
23. 1,243 - Würdest du das CORONAVIRUS stoppen? Die Atemmaske schützt auch vor neue Infektion
24. 1,224 - Atualizacao de Seguranca devido ao COVID 19.
25. 1,214 - Uma aliada contra o Corona Virus

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

Top Subjects Containing Attachments with Executable Files for Windows Machines (PE/EXEs)

1. 1,095 - Covid19"" Latest Tips to stay Immune to Virus !!
2. 452 - Customer Advisory - COVID-19 UPDATE
3. 30 - COVID-19 UPDATE !!
4. 27 - Covid19"" Latest Tips to stay Immune to Virus !!Type a message
5. 26 - Important Notice to Our Corporate Clients & Partners - COVID -19
6. 18 - TNT Express Notification/ Your shipment was returned to our office!!! BECAUSE OF COVID-19 OUTBREAK.
7. 3 - COVID-19 UPDATE !!!
8. 1 - COVID-19 Job Retention Scheme update

Top Countries Sending SPAM - Covid/Coronavirus Contained in Subjects (by Geolocation on SMTP IP Address)

1. 116,558 US
2. 21,919 IN
3. 8,395 IT
4. 7,083 CN
5. 6,665 RU
6. 5,146 HU
7. 4,863 FR
8. 4,450 DE
9. 4,068 BR
10. 3,672 VN
11. 2,811 GB
12. 2,393 CA
13. 2,149 JP
14. 1,866 AR
15. 1,551 NL
16. 1,508 ES
17. 1,500 HK
18. 1,226 ID
19. 1,127 KR
20. 1,003 SA
21. 977 BD
22. 957 ZA
23. 812 UA
24. 728 PL
25. 709 BE

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

COVID-19 Host, Domain, and Mobile App Tracking

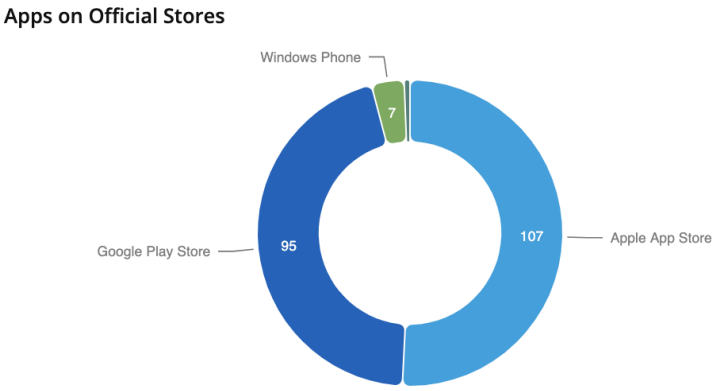
RiskIQ gathers data relating to newly-observed hosts and domains containing COVID-19, COVID19, or Coronavirus in the host or domain name and mobile apps containing COVID-19, COVID19, or Coronavirus in the title or description. A summary of data collected is contained in this section.

Domains and Hosts

Domains: 42,248
Hosts: 47,041
Hosts and Domains with Potential Mail Servers: 210
Email-Capable Domains and Hosts: 14,925
Live Hosts and Domains Not Parked: 18,785

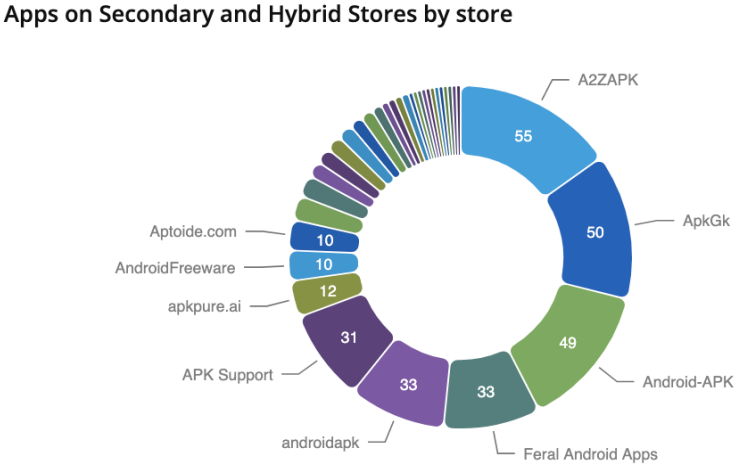
Mobile Apps

1. Apps in Official Stores: 210 (See Graph)
    a. Google Play Store: 95
    b. Apple App Store: 107
    c. Windows Phone: 7
    d. Amazon: 1



2. Apps in Secondary/Hybrid Stores: 349 (See Graph)

3. Blacklisted Mobile Apps by Store Type: 14
    a. Secondary: 13
    b. Hybrid: 1



RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

Facts and Figures at a Glance

Data is from [Johns Hopkins Coronavirus Resource Center](#).

Global

Total Cases: 801,400
Total Fatalities: 39,014
Countries w/ Confirmed Cases: 179

U.S.

Total Cases: 164,719
Total Fatalities: 3,170
Jurisdictions Reporting Cases: 54 (50 states, District of Columbia, Puerto Rico, Guam, and U.S. Virgin Islands)

Highest COVID-19 Case Count: U.S.

States

1. New York: 67,384
2. New Jersey: 16,636
3. California: 7,394

Counties

1. New York City (NY): 38,087
2. Westchester County (NY): 9,326
3. Nassau County (NY): 7,344
4. Suffolk County (NY): 5,791
5. Cook County (IL): 3,727
6. Wayne County (MI): 3,195
7. Rockland County (NY): 2,511
8. Bergen County (NJ): 2,482
9. Los Angeles County (CA): 2,474
10. King County (WA): 2,330

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

Stay-At-Home/Shelter-In-Place Orders

State	Start Date	End Date
California	03/19	TBD
Illinois	03/21	04/07
New Jersey	03/21	TBD
New York	03/22	TBD
Connecticut	03/23	04/22
Kentucky	03/23	TBD
Louisiana	03/23	04/13
Ohio	03/23	04/06
Oregon	03/23	TBD
Washington	03/23	04/06
Delaware	03/24	05/15
Indiana	03/24	04/06
Michigan	03/24	04/13
New Mexico	03/24	04/10
Massachusetts	03/24	04/17
West Virginia	03/24	TBD
Hawaii	03/25	04/30
Wisconsin	03/25	04/24
Vermont	03/25	04/15
Idaho	03/25	04/15
Colorado	03/26	04/11
Minnesota	03/27	04/10
New Hampshire	03/27	05/04
Montana	03/28	04/10
Rhode Island	03/28	04/13
Alaska	03/28	04/11
Kansas	03/30	04/19
North Carolina	03/30	04/29
Maryland	03/30	TBD
Virginia	03/30	06/10
Arizona	03/31	04/30
Washington, DC	04/01	04/24

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

Governmental Guidance

State & Local Governments

California

As of 03/31/2020, California has 7,394 confirmed COVID-19 cases and 149 deaths. California Governor Gavin Newsom issued an executive order Monday that extends tax and regulatory deadlines for small businesses. The order allows for a 90-day extension for tax returns and payments for businesses filing a return for less than $1 million in taxes, and extends the deadline to file a claim for refund by 60 days. The order also allows for mail-in renewals of driver's licenses to the DMV for the next 60 days.

Illinois

As of 03/31/2020, Illinois has 5,058 confirmed cases of COVID-19 and 74 deaths. Illinois Governor JB Pritzker announced that part of the McCormick Place Convention Center will be temporarily converted into an alternate care facility for COVID-19 patients with mild symptoms who do not require intensive care. The facility will have the capacity to care for up to 3,000 patients. The buildout will take place in phases, with up to 500 beds expected to be assembled by the end of this week.

Massachusetts

As of 03/31/2020, Massachusetts has 5,752 confirmed cases of COVID-19 and 56 deaths. The Department of Unemployment Assistance will hold daily virtual town hall meetings Tuesday through Friday to better assist people who are unemployed as a result of the coronavirus pandemic. Representatives will walk filers step-by-step through the claim process and take questions from the claimants. For more information, see here.

New York

As of 03/31/2020, New York has 67,384 confirmed COVID-19 cases and 1,342 deaths. New York City makes up more than half of the statewide cases of COVID-19 with 38,087. New York City Mayor Bill de Blasio announced a partnership with the Federal Emergency Management Agency (FEMA) to bring additional ambulances to New York City amid the coronavirus pandemic. The partnership between FEMA and New York City will bring 250 ambulances and approximately 500 EMTs and paramedics to the city. These resources aim to help the city

increase capacity for medical transport between medical sites and also assist the FDNY with responding to what is now a record number of medical calls.

Washington, DC

As of 03/31/2020, the Washington, D.C. region has a total of 2,934 confirmed COVID-19 cases with 1,021 in Virginia, 1,414 in Maryland, and 499 in the District. Washington, D.C., Mayor Muriel Bowser announced a stay-at-home order Monday, barring residents from leaving their homes for all but essential purposes or limited recreational activity. Mayor Bowser also said that those who willfully violate the order could be convicted of a misdemeanor and subject to a maximum of 90 days in prison and a fine of up to $5,000. Virginia Governor Ralph Northam also issued a stay-at-home order Monday. Governor Northam said people should only leave their homes to obtain food, supplies or medical care, or for exercise. All gatherings of more than 10 people are banned.

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

Appendix A: Iranian Malware Campaign - Technical Details

Originating Address:

galleag@who.int

Originating IP Addresses:

194.180.224.65

203.78.107.120

Subject Lines:

COVID-19 UPDATE !!

COVID-19 UPDATE !! MUST READ!!!

Malware File Names:

Covid-19-UPDATE-9000986666.exe

Covid-19-UPDATE-9000986666.zip

COVID-19_UPDATE.iso

Used Display Names:

WHO Representative

Gauden Galea

Dilcia Alcazar

Email Body Sample:

From: "WHO Representative" <galleag@who.int>

Subject: COVID-19 UPDATE !! MUST READ!!!

Hello info

We are pleased to inform you that recent ongoing research has

proven effective against coronavirus (Covid-19).

The enclosed PDF contains safety measures and preventive vaccines

for lethal viruses.

Thank you.

W. Gordon Gallia

WHO Representative

Phone: +86 10 65327189

GPN: 81218

Fax: +86 10 65322359

Email: galleag@who.int

Dongwai Diplomatic Office Building 401

No. 23 Dongzhimenwai Street, Chaoyang District
100600 Beijing, China
Phone: +8610 6532 7189
+8610 6532 7190
+8610 6532 7191
+8610 6532 7192
Fax: +8610 6532 2359
Email: who@chn.wpro.who.int

ASN: REBECCAHOST, US

Email Volume for 194.180.224.65

SMTP_IP	RDNS	TAG	COUNT	FIRST_SEEN
194.180.224.65	NXDOMAIN	openrelay	230	2020-03-14 19:53:57
194.180.224.65	NXDOMAIN	spam	9476	2020-03-09 03:14:24

ASN: NETWAY-AS-AP Netway Communication Co.,Ltd., TH

Email Volume for 203.78.107.120

SMTP_IP	RDNS	TAG	COUNT	FIRST_SEEN
203.78.107.120	cloudvps.personnelconsultant.co.th	openrelay	4	2020-03-25 14:13:56
203.78.107.120	cloudvps.personnelconsultant.co.th	spam	41	2019-12-11 02:15:35

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

End Report