RiskIQ i3:

COVID-19 Daily Update

04/25/2020

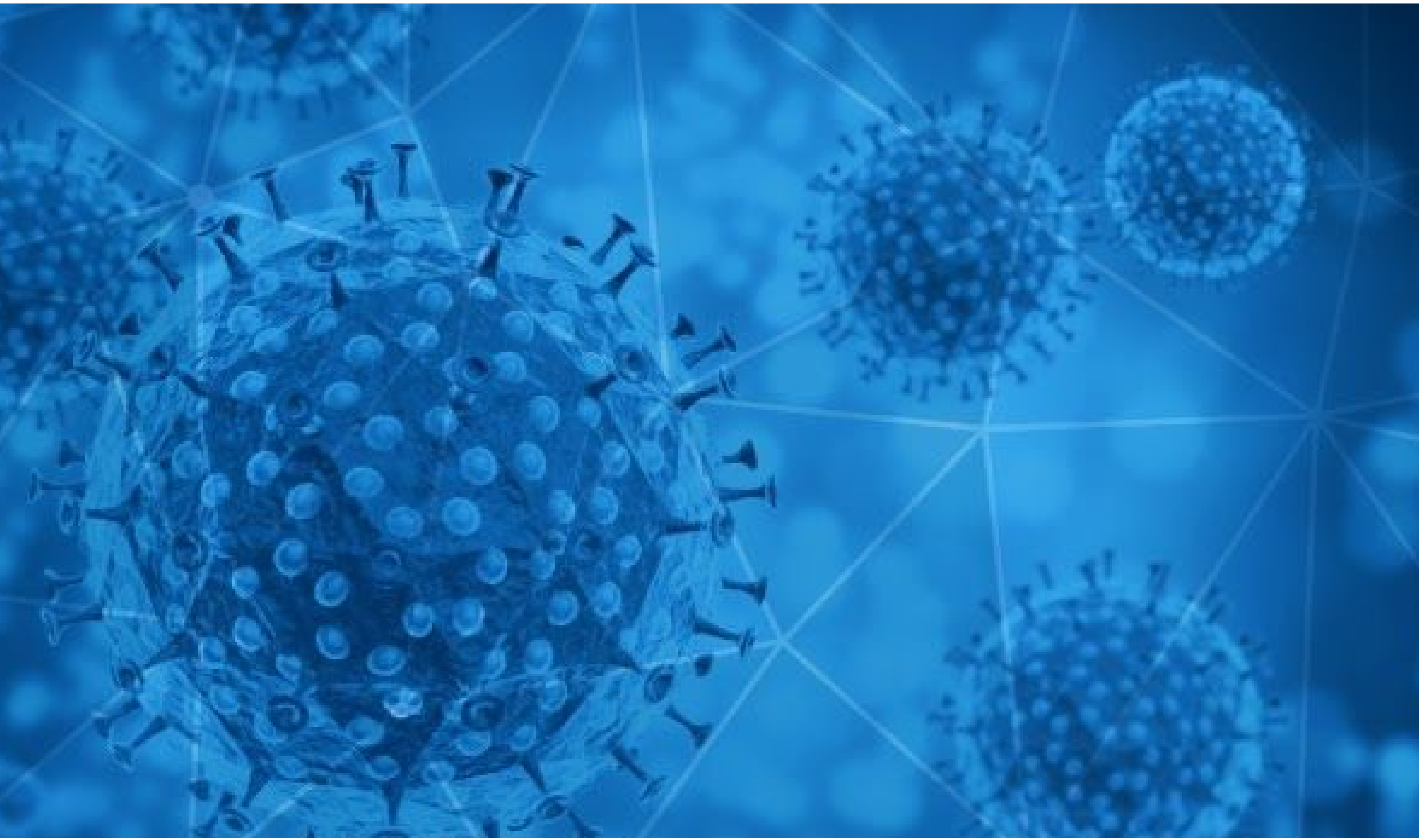


Table of Contents

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.

Digital Exploitation

From at least January - April 2020, hackers working for the Vietnamese Government have been targeting Chinese Government organizations tasked with managing the country's response to the coronavirus pandemic. According to research by FireEye, the hackers, who are likely identifiable with APT32 (also known as OceanLotus), sent emails containing the METALJACK malware to employees at China's Ministry of Emergency Management and the government of Wuhan to obtain non-public information on the crisis.

Two spearphishing campaigns leveraged the Agent Tesla information-stealing Trojan to target the oil and gas industry before and during a meeting between OPEC+ and the Group of 20 regarding oil production and pricing during the COVID-19 pandemic. The first campaign began around March 31st, and featured emails that appeared to come from Enppi, an oil company owned by the Egyptian government. These emails were sent widely to targets in Malaysia, the United States, Iran, South Africa, Oman, and others according to research conducted by Bitdefender. The second campaign began around 12 April and impersonated a shipment company to target victims in the Philippines.

New Blacklist Data

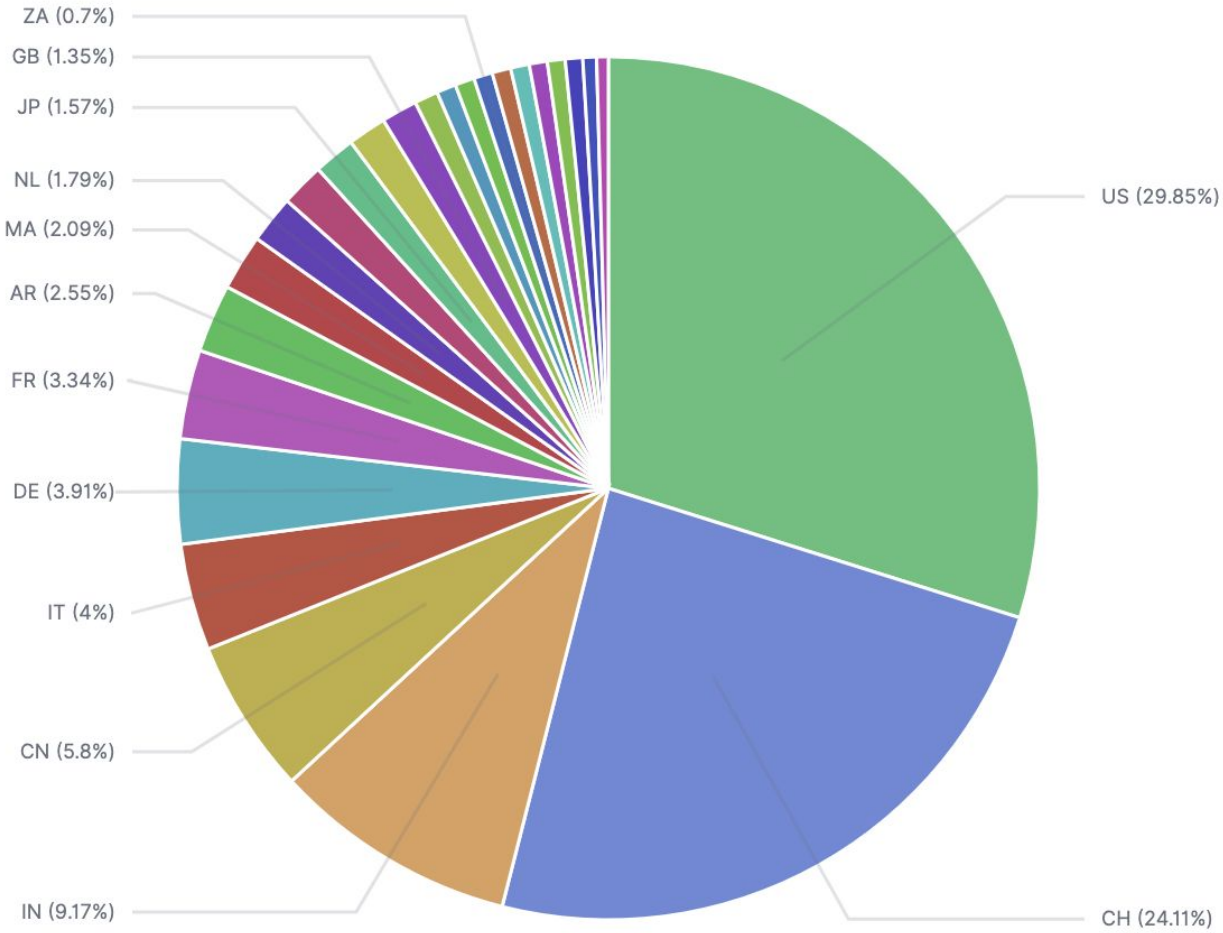
hxxp://covid-19remint[.]com/

hxxp://promo-covid-19[.]net/

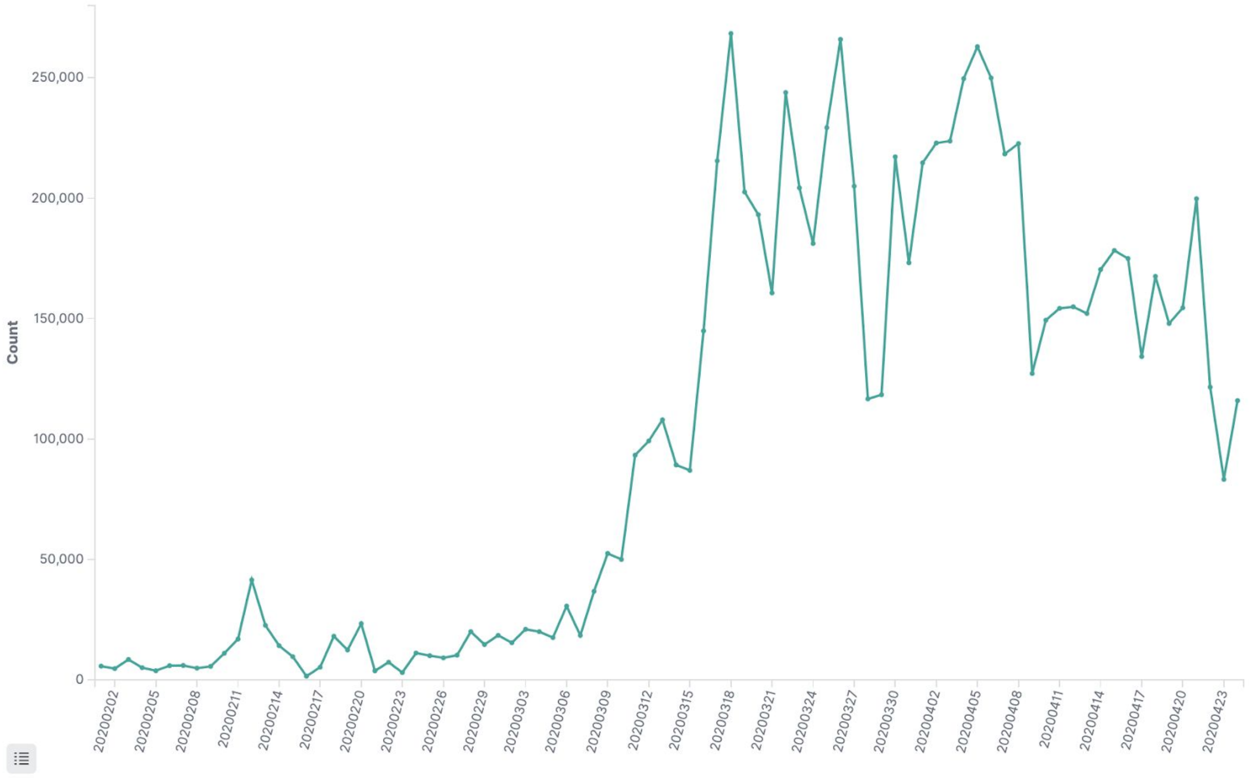
hxxp://gente-covid-19[.]gq/

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 04/24/2020-04/25/2020. During this period, RiskIQ analyzed 115,926 spam emails containing either “*corona*” or “*covid*” in the subject line. There were 18,619 unique subject lines observed during the reporting period. The spam emails originated from 11,428 unique sending email domains and 9,812 unique SMTP IP Addresses. Analysts identified 37 emails which sent an executable file for Windows machines.



Spam emails by country of origin



Spam emails by volume since February 1, 2020

Top 25 Subjects

1. 21,087 - FFP2 5,90 (SARS Corona Schutz)
2. 10,035 - Gesichtsmasken der Schutzklasse FFP2 ab 5,90 Euro (SARS Corona Schutz)
3. 3,992 - Re: Covid-19 / Vanity upon Vanity
4. 3,131 - The Corona Letter: Taking stock of the outbreak
5. 2,263 - Indian IT firms confirm to honour job offers amid Coronavirus outbreak | Python is the most preferred programming language
6. 2,237 - Collect ""COVID-19"" Aid Now
7. 2,039 - The COVID-19 Solidarity Response Fund
8. 1,746 - Top 5 books to master Deep Learning during lockdown | The demand for skilled cybersecurity professionals rises amid COVID-19
9. 1,509 - CORONA VIRUS PALLIATIVES
10. 1,495 - Covid-19 Entlastungsdarlehen fï¿½r Sie
11. 1,420 - Redeem Your SBSA-COVID-19-Financial Relief Today
12. 1,308 - Covid-19: ampliato l'intervento di MSF
13. 1,174 - Check out ""Conspiracy Theorists in the UK Burn 50 5G Towers Claiming Link to COVID-19"" on Wane Enterprises
14. 1,044 - Naukri.com - COVID 19 Impact Survey
15. 878 - Outsourcing y COVID-19: Actividades Vulnerables
16. 852 - coronavirus.mascarilla de proteccion facial
17. 843 - For those who fight against COVID-19
18. 814 - ATENCION COVID-19 Estudio Contable, Legal e Impositivo para tu negocio
19. 813 - Corona-Hilfe: Wir bezahlen Ihren Einkauf!
20. 789 - COVID-19 Asesoramiento contable para tu empresa
21. 720 - COVID-19 Impact - DONATE NOW
22. 709 - Dla tych, którzy walczą z pandemią COVID-19
23. 705 - The Covid-19 Solidarity Response Fund

24. 605 - Covid-19 เราต้องรอด! กับบริการทำความสะอาดและฆ่าเชื้อเพื่อลดความเสี่ยง

25. 484 - Contactless infrared body temperature thermometer defeat Coronavirus

Top 10 IP Addresses

1. 12,934 - 81.17.30.200
2. 9,730 - 81.17.30.208
3. 3,996 - 219.65.84.187
4. 3,648 - 69.12.82.222
5. 3,082 - 81.17.30.199
6. 2,237 - 81.192.231.96
7. 2,023 - 23.254.209.146
8. 2,004 - 148.163.135.245
9. 1,990 - 148.163.139.245
10. 1,514 - 212.66.96.52

Top 10 Domains (RDNS)

1. 12,934 - aeron.seuplanodesaude.med.br
2. 9,730 - edmure.seuplanodesaude.med.br
3. 3,996 - mgw07.tbsl.in
4. 3,648 - upas-occasional.goofmade.com
5. 3,082 - aegon.seuplanodesaude.med.br
6. 2,237 - adsl-96-231-192-81.adsl2.iam.net.ma
7. 2,023 - hwsrv-718421.hostwindsdns.com
8. 2,004 - mx0a-00178102.pphosted.com
9. 1,990 - mx0b-00178102.pphosted.com
10. 1,514 - webmail.webmail.it

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

1. 37 - REPROGRAMA SU ENTREGA DESPUÉS DE COVID-19 BLOQUEO ABAJO

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

1. 32,025 US
2. 25,870 CH
3. 9,841 IN
4. 6,218 CN
5. 4,288 IT
6. 4,199 DE
7. 3,581 FR
8. 2,741 AR
9. 2,245 MA
10. 1,922 NL
11. 1,753 HK
12. 1,682 JP
13. 1,553 LT
14. 1,445 GB
15. 952 RU
16. 783 CU
17. 780 TH
18. 753 ZA
19. 752 ES
20. 751 SG
21. 724 IR
22. 715 CA
23. 699 BR
24. 550 BE
25. 467 MX

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.

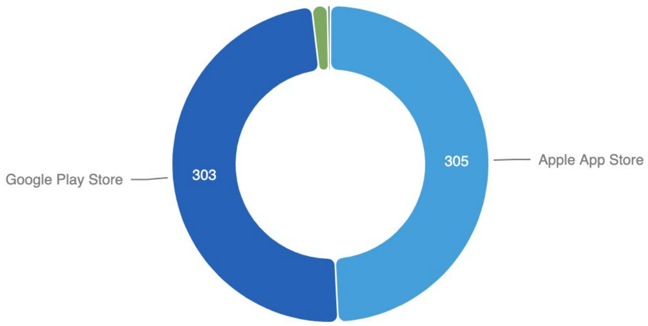
Domains and Hosts

Domains: 71,134
Hosts: 81,097
Hosts and Domains with Potential Mail Servers: 282
Email-Capable Domains and Hosts: 25,877
Live Hosts and Domains Not Parked: 32,862

Mobile Apps

1. Apps in Official Stores: 618 (See Graph)
    a. Google Play Store: 303
    b. Apple App Store: 305
    c. Windows Phone: 9
    d. Amazon: 1

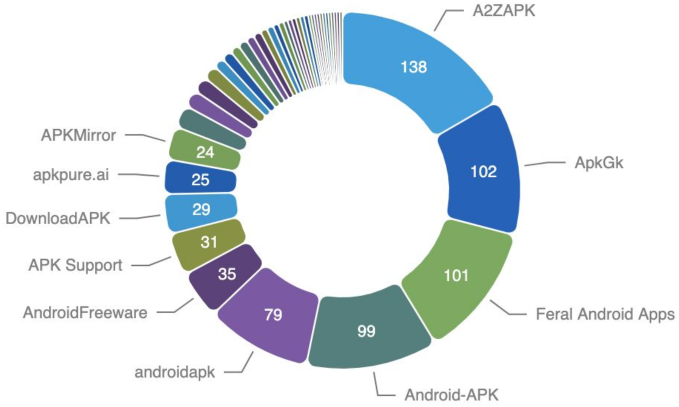
Apps on Official Stores



2. Apps in Secondary/Hybrid Stores: 786 (See Graph)

3. Blacklisted Mobile Apps by Store Type:
    a. Secondary: 28
    b. Hybrid: 1
    c. Official: 1

Apps on Secondary and Hybrid Stores by store



End Report