

ScamNation

Monetizing the Pandemic Through Partisan Content Farms and Subscription Traps



Authors:
Jordan Herman, RiskIQ
Ryan Foote, Independent Researcher

Table of Contents

- Executive Summary** 3
- Introduction** 3
- Investigation** 4
 - The Bytesignal Content Farm 4
 - The Bytesignal Traffic Funnel..... 5
 - The COVID-19 Subscription Trap..... 8
 - Breadcrumbs: Subscription Trap Infrastructure Connections.....12
 - Connecting the Subscription Trap Companies.....17
- Conclusion**21

Executive Summary

During headline-grabbing events, threat actors leverage rapidly changing information environments—press, social media, and even government channels—to lend credence to the delivery mechanisms they use to carry out malicious activity. This tactic has proven especially effective during the COVID-19 pandemic, as scams purporting to contain information, news, and remedies related to the virus have saturated the internet. In this report, we'll use RiskIQ's internet-wide visibility and unique data sets to identify and explicitly define entities exploiting the pandemic for monetary gain through the spread of false information and the sale of fraudulent products online.

RiskIQ researchers have identified a network of "content farm" websites publishing misleading, highly partisan content that has lately focused on COVID-19. Scammers use these sites to promote ads that lure users into "subscription traps," which, through misleading messaging and hidden language in the fine print, trap buyers into making monthly payments that are difficult, if not impossible, to get out of.

In some cases, when visiting one of these content farm sites and viewing an article about the pandemic, ads are served that play on pandemic-related concerns. Clicking on the ad leads the user to a subscription trap page, typically pushing a product that claims to protect against the coronavirus. Using RiskIQ data, we were able to find several other examples of the ad and product in question, map out related infrastructure, and identify several companies behind these subscription trap offerings and associated digital ads.

Introduction

On March 27, 2020, a few days after stay-at-home or shelter-in-place orders went into effect across the United States due to COVID-19, RiskIQ researchers saw an interesting thread on Twitter.¹ It mentioned using RiskIQ Community, the free version of RiskIQ's Threat Hunting platform, for an investigation that would be used for an academic paper on spam email campaigns. These spam campaigns appeared to be exploiting the pandemic for personal gain.

In the spirit of collaboration, RiskIQ researchers reached out to Ryan Foote, an independent researcher and the author of the Twitter thread and a co-author of this report, to see if we could help further his work and dig deeper into the organizations uncovered during his initial investigation. Beyond actively looking for malicious activity related to COVID-19 for our customers, RiskIQ has been ramping up efforts to provide guidance for security issues created or exacerbated by the crisis, and have made our datasets and parts of our platform available to researchers investigating cybercrime exploiting the pandemic.

The joint investigation that followed led to the mapping out of interconnected networks of websites—often referred to as "content farms"—that push fake or misleading news articles covering multiple topics, including the COVID-19 pandemic.² The investigation also led to identifying the actors behind these fraudulent networks.

Content farm publishers typically monetize through ad revenue, and the publishers described here are no different. In recent years, partisan content farms have proved highly lucrative for their operators,³ which has led to their proliferation on a massive scale. According to a recent report from Graphika, a company that maps social media data, right-wing groups have been some of the most prolific spreaders of misinformation, and their readers are the most likely to engage with misinformation related to the COVID-19 pandemic.⁴ The articles on the content farms we identified followed this pattern, consisting of

1. <https://twitter.com/skykn0t/status/1243580592698122241>

2. https://en.wikipedia.org/wiki/Content_farm

3. <https://www.buzzfeednews.com/article/craigsilverman/inside-the-partisan-fight-for-your-news-feed>

partisan, right-wing news articles that include COVID-19 misinformation

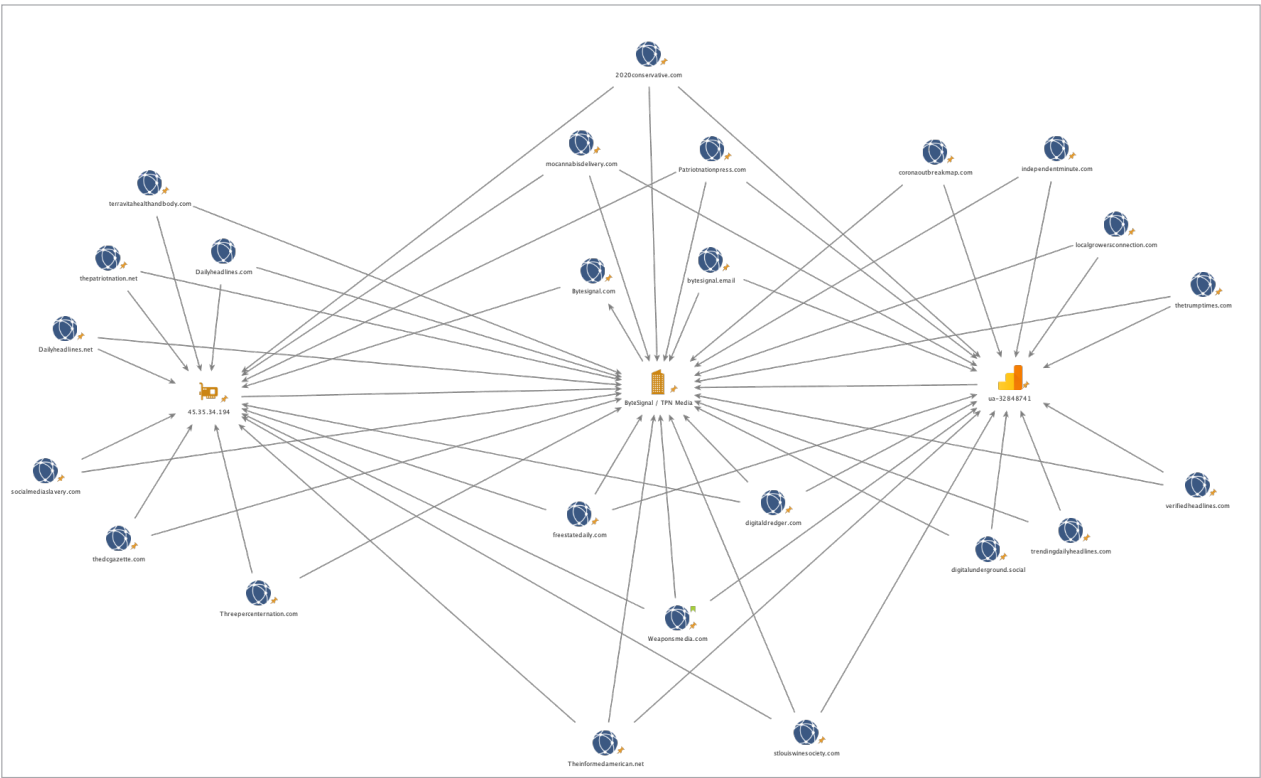
Our research found that several of the advertisements loaded on these fake news sites lead to subscription traps. A subscription trap works by offering a free or deeply discounted trial of a product while hiding clauses in the terms of service that sign victims up for costly payments remitted on a repeated basis, usually monthly. Our investigation connected hundreds of similar content farm sites to ads leading to subscription traps, pointing to a symbiosis between purveyors of fake content and subscription trap schemers.

These ads appear to be endemic to content farm sites. However, we were able to attribute some of the most egregious of these subscription traps—ones exploiting fears about the pandemic for financial gain—to a specific group of connected companies and individuals. This group creates and pushes the advertisements and profits from the sale of a product purporting to be a COVID-19 cure.

Investigation

The Bytesignal Content Farm

The first step in the sequence leading victims to the subscription traps is a content farm run by Bytesignal / TPN Media, which consists of several websites purveying inflammatory content that is often wholly false.



The Bytesignal content farm

4. <https://graphika.com/reports/the-covid-19-infodemic/>

Among this network of sites is coronaoutbreakmap[.]com, which RiskIQ's systems have crawled several times along with other sites in the network. On May 4, 2020, RiskIQ captured a snapshot of one of the articles posted to coronaoutbreakmap.com (shown below). The article states that COVID-19 was engineered as a bioweapon, which is a baseless conspiracy theory.⁵ The page also features ads placed by a company called PowerInbox, which lead to subscription traps. Connections between PowerInbox and hundreds of content farm websites and subscription traps were documented as part of this investigation, but are out of scope for this report. A RiskIQ Community Project linked at the end of this report provides our data on these connections.

The screenshot shows a web browser window with the URL <https://sf.riskiq.net/crawlview/snapshot/snapshot?crawlStateGuid=cf128748-0881-470d-8f84-a86f728b8f3a&pageGuid=6>. The article title is "Alarming New Study Suggests Coronavirus Is Man Made Bio-Weapon [WATCH]". The author is "By Staff" and it was "Posted on February 2, 2020". Below the title are social media sharing buttons for Facebook, Twitter, Pinterest, Email, and a comment icon. The article text reads: "A **scientific report** from the Kusuma School of Biological Sciences in New Delhi, India, proves the Coronavirus is a man-made bioweapon." Below the article is a "YOU MIGHT LIKE" section with four recommended items, each with a thumbnail image and a title:

- **Drink 1 Cup Before Bed, Watch Your Belly Fat Melt Like Crazy**
eonlinenews.co
- **Melania Trump Says Goodbye**
[READ MORE]
- **US MD: I Beg Americans To Throw Out This Veg Now**
United Naturals
- **CBD Oil Is Being Given Away For Free - Get It Here**
Get Your Free Bottle Now

<https://sf.riskiq.net/bl/460034494/ea26fb3e013b89b3? sg=%2Fm8fZIUKSIC%2FY%2BbNI73D%2Fw%3D%3D>

Google Analytics accounts are used by website owners to track traffic and user activity. Therefore, this data point can be used to connect different websites to a single person or business entity. The coronaoutbreakmap[.]com domain shares a Google Analytics account number with several other Bytesignal controlled domains, such as independentminute[.]com, 2020conservative[.]com, and patriotnationpress[.]com.

5. <https://www.washingtonpost.com/outlook/2020/04/26/no-coronavirus-is-not-biological-weapon/>

Tours

ua-32848741 (GoogleAnalyticsAccountNumber)

Tracker Search: Hosts 16

Tracker Search: IP Addresses 92

DATA

HOSTNAME (16 / 16)

✓ x 2020conservati... 1

✓ x americonnews.... 1

✓ x app.localgrowe... 1

✓ x coronaoutbrea... 1

✓ x digitaldredger.c... 1

Show More

TAG

SYSTEM TAG

TRACKER SEARCH ⓘ

☐

Show : 25

◀ 1-16 of 16 ▶

Sort : Last Seen Descending ▾

Total Records : 16

Hostname	First Seen	Last Seen
<input type="checkbox"/> independentminute.com	2017-07-17	2020-04-27
<input type="checkbox"/> patriotnationpress.com	2016-07-27	2020-04-26
<input type="checkbox"/> 2020conservative.com	2019-11-08	2020-04-26
<input type="checkbox"/> theinformedamerican.net	2016-04-17	2020-04-26
<input type="checkbox"/> verifiedheadlines.com	2020-01-15	2020-04-26
<input type="checkbox"/> digitalunderground.social	2020-03-15	2020-04-24
<input type="checkbox"/> trendingdailyheadlines.com	2019-07-12	2020-04-23
<input type="checkbox"/> coronaoutbreakmap.com	2020-02-12	2020-04-21
<input type="checkbox"/> localgrowersconnection.com	2017-12-06	2020-04-16
<input type="checkbox"/> mocannabisdelivery.com	2020-03-30	2020-04-12
<input type="checkbox"/> app.localgrowersconnection.com	2018-05-09	2020-04-12

<https://community.riskiq.com/search/trackers/GoogleAnalyticsAccountNumber/ua-32848741>

Additionally, several of these sites have been hosted on the same IP address, 45.35.34[.]194.⁶ This IP has also hosted several other domains, including threepercernation[.]com, weaponsmedia.com, and bytesignal.com. Starting in February, most of the Bytesignal content farm websites began featuring articles about the coronavirus and events connected to the pandemic.

The Bytesignal Traffic Funnel

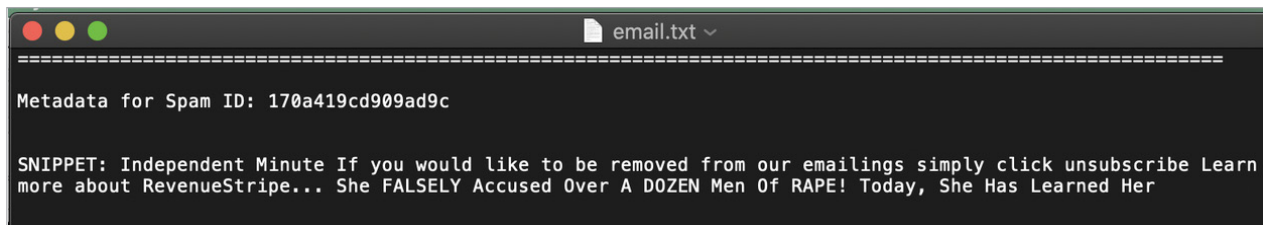
The Bytesignal network drives traffic to its sites through spam email and social media. Messages sent as part of Bytesignal spam campaigns follow a similar format: a clickbait subject line and a blurb trying to get the reader to click on the link to the site.⁷

6. <https://community.riskiq.com/search/45.35.34.194>

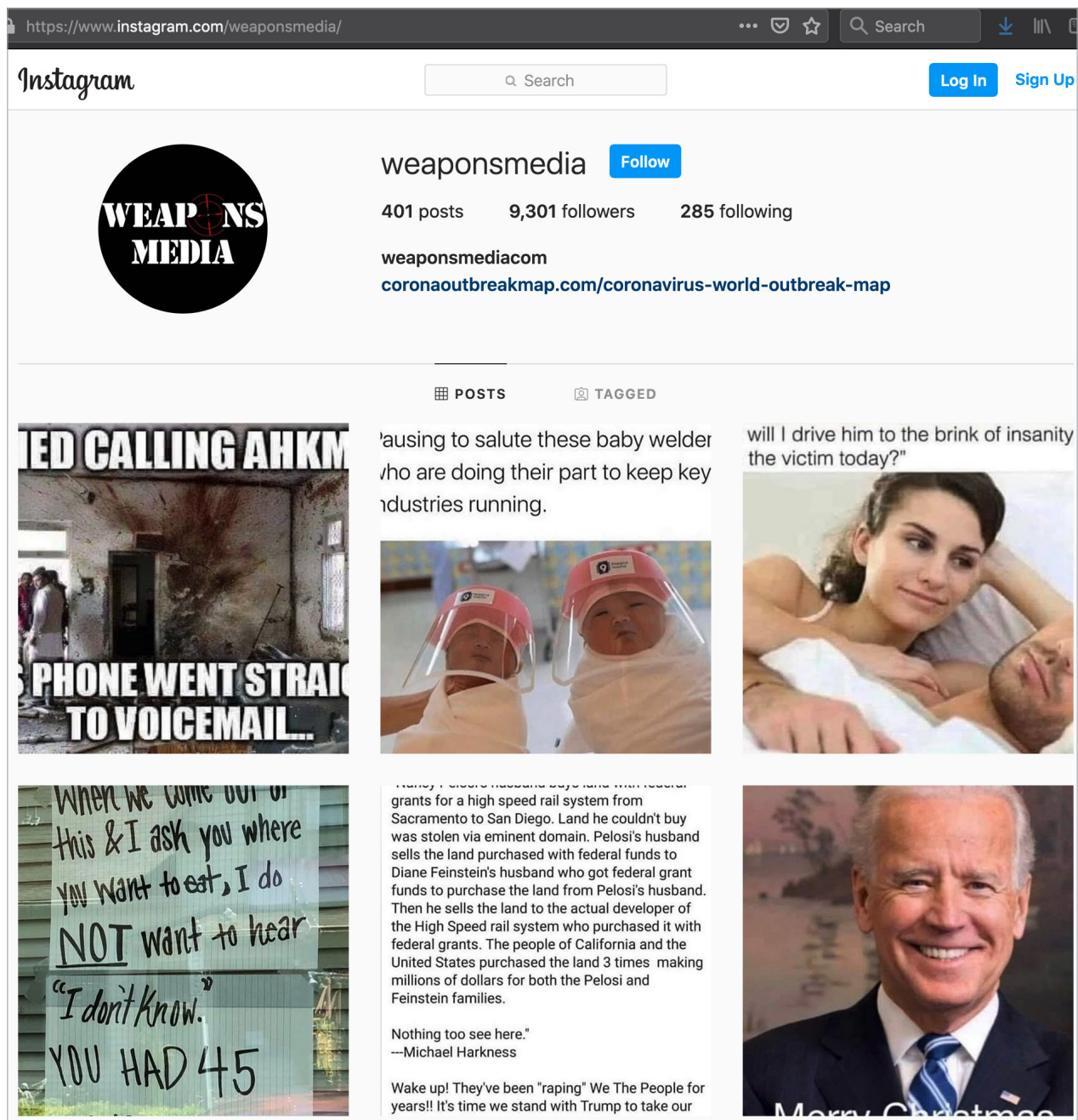
7. These spam emails were the original catalyst for this investigation, which began as an academic paper on social engineering. The objective of the paper was to use Open Source Intelligence ("OSINT") to investigate spam emails, and attempt to link the sophistication of social engineering techniques used by the sender. The initial investigation was carried out through the following process. A Python script was created to utilize the Gmail API to pull metadata and MIME content for each spam message in order to get samples of spam to analyze. Each message was then categorized based on the subject matter and social engineering technique. The Python script is available on Ryan's github: <https://github.com/Skykn0t/SpamGrabber>

6

ScamNation Intelligence Report

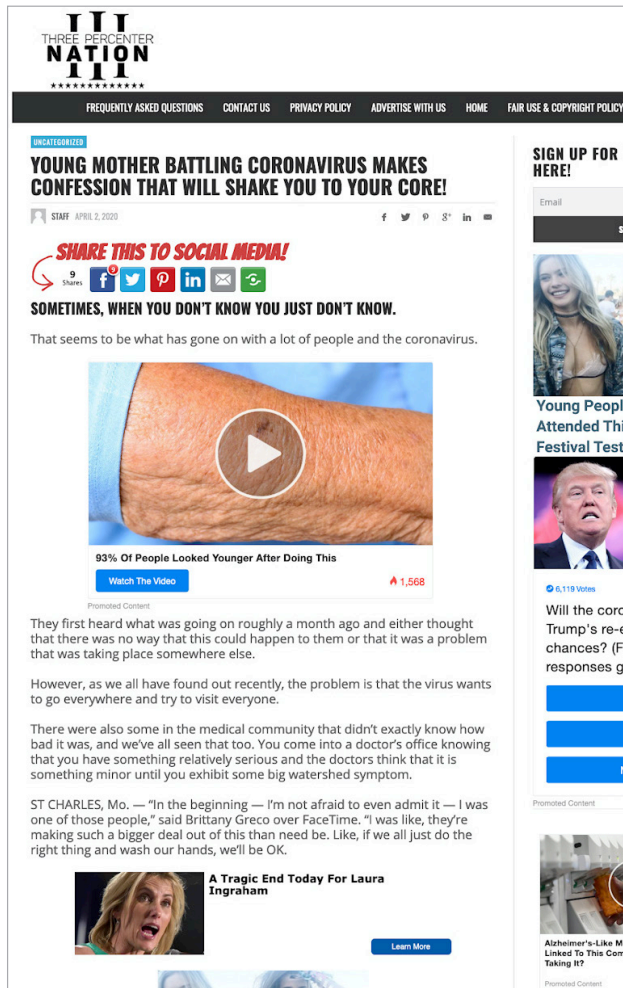


Bytesignal is just as active on social media. An Instagram page entitled "weaponsmedia" (weaponsmedia[.]com is another site in the Bytesignal network) features a steady stream of memes. It currently has over 9,000 followers and features a link to the Bytesignal site coronaoutbreakmap[.]com. Several Twitter accounts have also shared links to coronaoutbreakmap[.]com as well as other domains controlled by Bytesignal. A search for tweets that mentioned any domain in the Bytesignal network returned 43,189 tweets starting in 2016.



The COVID-19 Subscription Trap

RiskIQ observed the Bytesignal-owned domain threepercernation[.]com hosting the below story about a "young mother battling COVID-19." The content appears to have been copied directly from legitimate news source KSDK, an NBC affiliate in St. Louis, MO.⁸ Both of these Bytesignal websites, threepercernation[.]com and coronaoutbreakmap[.]com, are using COVID-19-related stories, often containing false information, to drive traffic which operators monetize through advertising. In the middle of this particular story, we observed an ad using pandemic-related content to attract clicks. This ad slot was filled by the Newsmax Feed Network, which connects publishers and advertisers to provide "targeted content-driven advertising."⁹



THREE PERCENTER NATION

FREQUENTLY ASKED QUESTIONS CONTACT US PRIVACY POLICY ADVERTISE WITH US HOME FAIR USE & COPYRIGHT POLICY

UNCATEGORIZED

YOUNG MOTHER BATTLING CORONAVIRUS MAKES CONFESSION THAT WILL SHAKE YOU TO YOUR CORE!

STAFF APRIL 2, 2020

SHARE THIS TO SOCIAL MEDIA!

9 Shares

SOMETIMES, WHEN YOU DON'T KNOW YOU JUST DON'T KNOW.

That seems to be what has gone on with a lot of people and the coronavirus.

93% Of People Looked Younger After Doing This

Watch The Video 1,568

Promoted Content

They first heard what was going on roughly a month ago and either thought that there was no way that this could happen to them or that it was a problem that was taking place somewhere else.

However, as we all have found out recently, the problem is that the virus wants to go everywhere and try to visit everyone.

There were also some in the medical community that didn't exactly know how bad it was, and we've all seen that too. You come into a doctor's office knowing that you have something relatively serious and the doctors think that it is something minor until you exhibit some big watershed symptom.

ST CHARLES, Mo. — "In the beginning — I'm not afraid to even admit it — I was one of those people," said Brittany Greco over FaceTime. "I was like, they're making such a bigger deal out of this than need be. Like, if we all just do the right thing and wash our hands, we'll be OK."

A Tragic End Today For Laura Ingraham

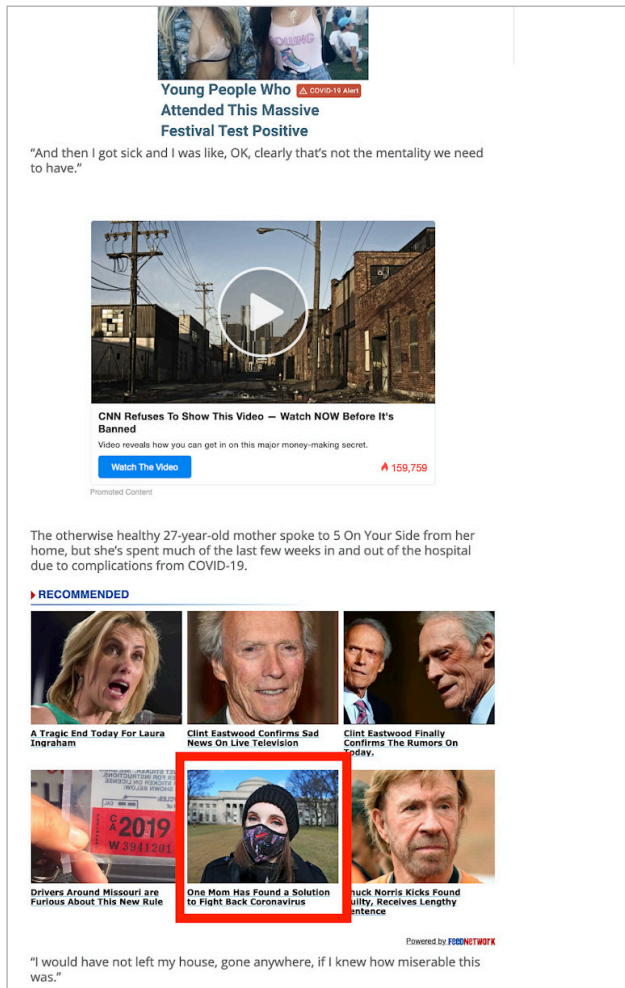
Learn More

Will the coronavirus re-evaluate Trump's chances? (F... responses ge

Promoted Content

Alzheimer's-Like Me... Linked To This Com... Taking It?

Promoted Content



Young People Who Attended This Massive Festival Test Positive

COVID-19 Alert

"And then I got sick and I was like, OK, clearly that's not the mentality we need to have."

CNN Refuses To Show This Video — Watch NOW Before It's Banned

Video reveals how you can get in on this major money-making secret.

Watch The Video 159,759

Promoted Content

The otherwise healthy 27-year-old mother spoke to 5 On Your Side from her home, but she's spent much of the last few weeks in and out of the hospital due to complications from COVID-19.

RECOMMENDED

A Tragic End Today For Laura Ingraham

Clint Eastwood Confirms Sad News On Live Television

Clint Eastwood Finally Confirms The Rumors On Today

Drivers Around Missouri are Furious About This New Rule

One Mom Has Found a Solution to Fight Back Coronavirus

Huck Norris Kicks Found Guilty, Receives Lengthy Sentence

Promoted Content

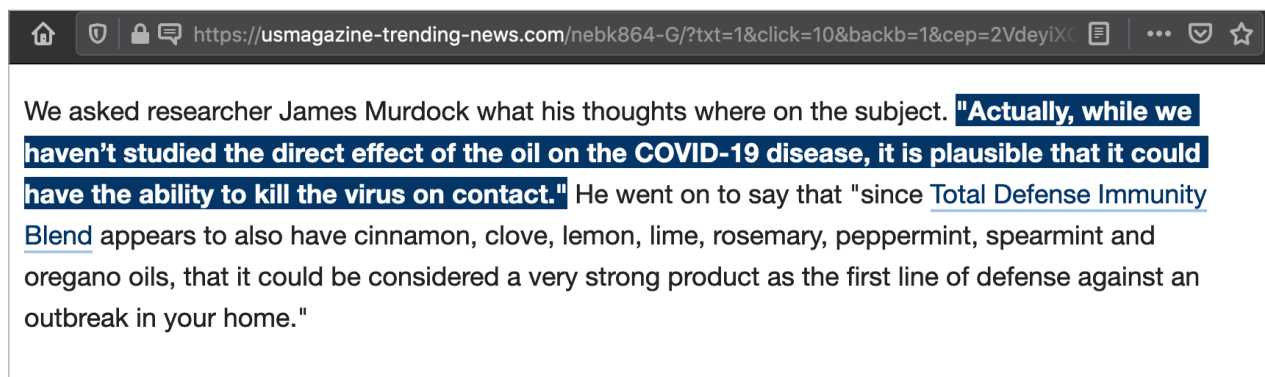
Powered by **FEEDNETWORK**

"I would have not left my house, gone anywhere, if I knew how miserable this was."


9. <https://www.newsmaxfeednetwork.com/>



The page is a lengthy advertisement for CBD oil, containing claims such as "...it is plausible that it could have the ability to kill the virus on contact..." and "This immunity oil actually will disinfect any surface including your skin."



At the bottom of the page is a link to get a bottle of "Immunity Blend" for 40% off, with language meant to encourage a reflex in the reader to hurry up and purchase it. Creating urgency is a typical sales tactic, but in cases of subscription traps, it's a trick meant to get the victim to bypass the fine print.



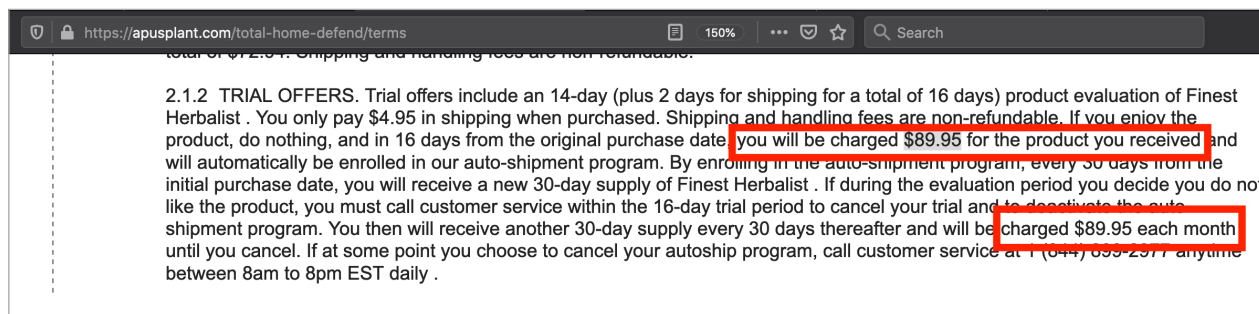
Update:

There are still bottles of Pure Herbal Immunity Blend Available.
If you hurry, you may be one of the few to try this out for yourself..

[Click Here to Get 40% OFF](#)

11. see also https://en.wikipedia.org/wiki/Snake_oil

The click-through page contains the hidden recurring costs of the subscription trap buried in the terms of service. In this particular case, the unfortunate victim will be charged \$89.95 per month.

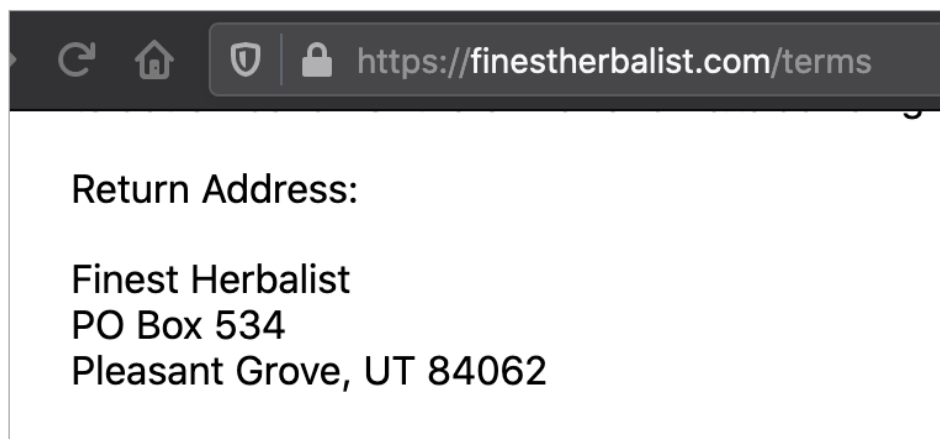


Interestingly, also hidden in the terms and conditions is the name of a company, Finest Herbalist, with an address in Las Vegas.

Return Address:

Finest Herbalist
5892 Losee Rd, Ste. #132-375 North Las Vegas, NV 89081

Finest Herbalist is not the company behind these subscription traps. However, the Finest Herbalist website at finestherbalist[.]com yields a clue as to who is. Buried in their Terms & Conditions is yet a different address: PO Box 534, Pleasant Grove, UT 84062.



This return address is used by several different LLCs with business addresses in many different states. Gary Warner of the University of Alabama posted a blog on March 22nd connecting this address to several businesses that have been the subject of numerous complaint reports to the Better Business Bureau since 2017.¹² The complaints indicate the businesses are running subscription traps.¹³ Here is Warner's list of troublesome companies:

- ▶ First Class Herbalist CBD
- ▶ Keto Ultra Diet

¹² <https://www.bbb.org/us/ut/pleasant-grv/profile/online-retailer/prime-forskolin-diet-1166-90023434>, <https://www.bbb.org/us/ut/pleasant-grv/profile/health-and-wellness/keto-ultra-diet-1166-90023137/complaints>

¹³ <http://garwarner.blogspot.com/2020/03/cauce-spamfighters-rally-against-corona.html>, <https://twitter.com/GarWarner>

- ▶ Manifest Health Plan
- ▶ Primal Pro Wellness
- ▶ Sunshine Health and Wellness
- ▶ Plant Pure Diet and Beauty
- ▶ Tru Slim Living

Breadcrumbs: Subscription Trap Infrastructure Connections

The subscription trap page described in the prior section is hosted on several different domains, including:

- ▶ apusplant[.]com
- ▶ flameserum[.]com
- ▶ amaranthserum[.]com
- ▶ amethystlifestyle[.]com

The domains apusplant[.]com, flameserum[.]com, amaranthserum[.]com, and amethystlifestyle[.]com are connected by the Google Analytics account ua-130095210. This account also connects to 463 other domain names, all of which appear related to the products sold by the businesses listed by Gary Warner on his blog.

The screenshot shows the RiskIQ interface for tracking Google Analytics account ua-130095210. The top navigation bar includes the RiskIQ logo, a search bar with the account ID, and links for Tours and Enterprise. Below the navigation bar, the account ID is displayed. The main content area is divided into two sections: Tracker Search: Hosts (463) and Tracker Search: IP Addresses (752). The Hosts section is active, showing a list of domains tracked by the account. The list includes filters for Hostname, Tag, and System Tag. The Tracker Search section shows a table of results with columns for Hostname, First Seen, and Last Seen. The table lists five domains: www.chronicpainreliefnews.com, zalophusherbalistoils.com, daisymoisturizer.com, vulpesherbalthemp.com, and variegatedhempoil.com, all with first and last seen dates in 2020.

Hostname	First Seen	Last Seen
www.chronicpainreliefnews.com	2020-01-24	2020-04-26
zalophusherbalistoils.com	2020-04-23	2020-04-26
daisymoisturizer.com	2020-04-26	2020-04-26
vulpesherbalthemp.com	2020-04-26	2020-04-26
variegatedhempoil.com	2020-04-26	2020-04-26

<https://community.riskiq.com/search/trackers/ua-130095210>

14. <https://community.riskiq.com/search/trackers/ua-130095210>

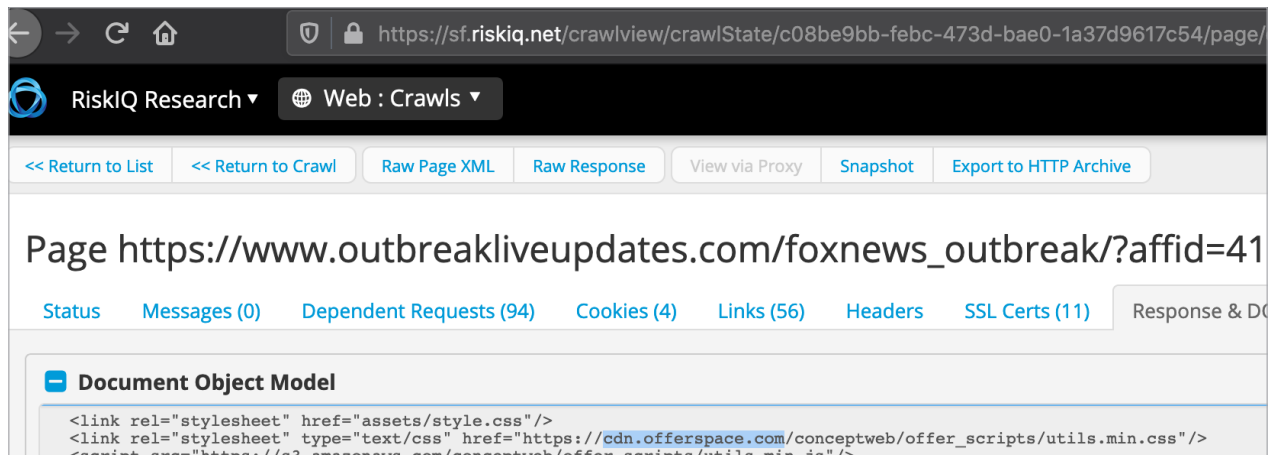
RiskIQ's crawling of these domains cataloged similar pages pushing the same CBD Immunity Blend product seen on usmagazine-trending-news[.]com.¹⁵ A RiskIQ crawl of outbreakliveupdates[.]com captured a scam page nearly identical to the usmagazine-trending-news[.]com page. These pages feature a distinctive script tag (a `<script>` element in the HTML of a page that either contains scripting statements, or points to an external script file through the `src` attribute) that routes traffic through traffic.webclickroute[.]com to the subscription trap page:



The script tag is:

```
<script>window.Exit.enable("https://traffic.webclickroute.com?router=33BF89A232C8F2148BC443E1577652025571", "#ExitPop", false, false)</script>
```

This script tag links these scams to several other scams that have been running for years—all connected to the same company, Offer Space. These scam pages load content from cdn.offerspace.com and cdn2.offerspace.com.



¹⁵ https://sf.riskiq.net/bl/459279069/d0074f76d60d733b?_sg=KkA%2FWTfmztzfkUXfqdIOfQ%3D%3D

RiskIQ's Host Pairs dataset allows us to take this observation and extrapolate other connections. Host pairs are unique parent-child relationships between websites. These relationships provide an understanding of redirection sequences and dependent requests between sites, as observed through RiskIQ crawling. Looking at the host pairs connected to the Offer Space CDN subdomains, we find many hostnames related to CBD oil and other products pushed through subscription trap offerings.¹⁶

RISKIQ

cdn2.offerspace.com

Tours

First Seen2018-06-28

Last Seen2020-06-09

RegistrarGoDaddy.com, LLC

RegistrantOffer Space, LLC

+

Categorize

DATA

15

9

0

119

0

9

576

2

3

16

0

Resolutions

Whois

Certificates

Subdomains

Trackers

Components

Host Pairs

OSINT

Hashes

DNS

Projects

Cc

FILTERS

DIRECTION

✓ parents

✓ children

PARENT HOSTNAME (10 / 135)

✓ x cdn2.offersp...106

✓ x almanachealth...4

✓ x azuritehealthpl...4

✓ x ailuropodalifest...3

✓ x alabasterketo.c...3

Show More

CAUSE (8 / 576)

✓ x script.src171

✓ x parentPage169

✓ x link.href128

✓ x xmlhttprequest78

HOST PAIRS

1 - 25 of 576

Sort : Last Seen Descending

25 / Page

Parent Hostname	Child Hostname	First	Last
<input type="checkbox"/> cdn2.offerspace.com	cdn2.offerspacebranddns.com	2020-02-25	2020-06-09
<input type="checkbox"/> www.totallyvoice.com	cdn2.offerspace.com	2020-05-09	2020-06-09
<input type="checkbox"/> cdn2.offerspace.com	tepuiberbrelief.com	2020-05-12	2020-06-08
<input type="checkbox"/> tepuiberbrelief.com	cdn2.offerspace.com	2020-05-12	2020-06-08
<input type="checkbox"/> tepuiberbrelief.com	cdn2.offerspace.com	2020-05-12	2020-06-08
<input type="checkbox"/> cdn2.offerspace.com	cdn.offerspace.com	2018-07-22	2020-06-08
<input type="checkbox"/> natrespurelabs.com	cdn2.offerspace.com	2020-06-08	2020-06-08
<input type="checkbox"/> natrespurelabs.com	cdn2.offerspace.com	2020-06-08	2020-06-08
<input type="checkbox"/> cdn2.offerspace.com	natrespurelabs.com	2020-06-08	2020-06-08
<input type="checkbox"/> cdn2.offerspace.com	berlepschsherbalsolution.com	2020-05-01	2020-06-08
<input type="checkbox"/> berlepschsherbalsolution.com	cdn2.offerspace.com	2020-05-01	2020-06-08

<https://community.riskiq.com/search/cdn2.offerspace.com/hostpairs>

In 2017, RiskIQ crawled reviewsforhomebusiness[.]com.¹⁷ The reviewsforhomebusiness[.]com page is an ad mimicking a CNN article and promoting a business called Daily Web Biz. At the bottom of the page is the text “Offer Expires on J ul 29, 2016.”

16. <https://community.riskiq.com/search/cdn2.offerspace.com/hostpairs>, <https://community.riskiq.com/search/cdn.offerspace.com/hostpairs>
17. https://sf.riskiq.net/bl/459404955/d0074f76d60d733b?_sg=I7vvyvtd7csljktD6yCnPw%3D%3D

14

ScamNation Intelligence Report


https://sf.riskiq.net/crawlview/snapshot/snapshot?crawlStateGuid=388e5376-92f2-4e40-9ebf-28384cdd340a&pageGuid=

CNN News Video TV Opinions More... Adveritorial





U.S. World Politics Tech Health Entertainment


"Warren Buffet reveals simple plan to help every American earn more money."

- And Reveals What Average Americans NEED To Do To Protect Themselves

 [Anderson Cooper](#), CNN

Updated 8:11 AM ET, March 29th, 2017



Extending the Drop
Post-Brexit bounce proves temporary for sterling

■ British Pound


BUFFET WARNS ABOUT BREXIT CHAOS
Can Americans double or even triple their income this year?
BUFFET SAYS "YES"

CNN 8:45 PM ET


Buffet's plan to guard against Brexit Chaos with called [The Daily Web Biz](#).

The Simple Plan

Step 1

 Go to [Daily Web Biz](#) and fill out the form to get instant online access to the program

Step 2

 Use [Sandra Barnes' Daily Web Biz Course](#) and follow the simple

The fake CNN article redirects to a page recruiting people to sign up for an opportunity to make money from home with zero experience or skills required. The page is hosted on [webinternetprofits\[.\]com](#). A cookie named `coresess` is loaded on this page from [mastertraffic.offerspace\[.\]com](#).

Page <https://www.webinternetprofit.com/earnmoney?affid=314556&s>

[Status](#)
[Messages \(4\)](#)
[Dependent Requests \(52\)](#)
[Cookies \(11\)](#)
[Links \(3\)](#)
[Headers](#)
[SSL Certs \(0\)](#)
[Response](#)

Domain	Name	Value	Path	Comment	Expires
.webinternetprofit.com	__cfduid	d440cf75c987a798eca57132ea40263ef1490843...	/		2018-03-29
www.webinternetprofit.com	gengcookie		/		08:06 AM PDT
.reviewsforhomebusiness.com	__cfduid	d138e141e9b71d11d070d581caa6dccb21490843...	/		2018-03-29
www.track4cr.com	LTTCC_364668	03_188903115_b9af5b6e-423c-422a-bd0a-dac...	/		2017-04-05
.offerspace.com	__cfduid	ddf8531d449556f1867d0ad47bd23a8f01490843...	/		2018-03-29
mastertraffic.offerspace.com	ServerID	1050	/		08:06 AM PDT
mastertraffic.offerspace.com	PHPSESSID	g61e3ms97s9s0893bkqmv8s545	/		08:06 AM PDT
mastertraffic.offerspace.com	coresess	a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs...	/		2017-03-29
webinternetprofit.com	AWSELB	A759CDAF1E166C835BEDEFAE7AE8025874F9B5BC...	/		2017-03-30
www.webinternetprofit.com	PHPSESSID	h13rb5dmiaohbak40bs1u2eal1	/		08:06 AM PDT
www.webinternetprofit.com	coresess	a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs...	/		2017-03-29

This cookie is linked to 1,459 unique domains dating from November, 11, 2016 through January 13, 2020. These domain names are related to products such as CBD oil, keto supplements, nutraceuticals, and beauty creams, all products we observed used as subscription traps during this investigation.

RISKIQ
coresess
Tours
Enterprise

FILTERS ⓘ

PATH (25 / 25)

- ✓ ✕ ailuropodalifest... 1
- ✓ ✕ alalungaserum.... 1
- ✓ ✕ berlepscsherb... 1
- ✓ ✕ cinereousherba... 1
- ✓ ✕ colossalketo.com 1

[Show More](#)

HOSTNAME (25 / 25)

- ✓ ✕ ailuropodalifest... 1
- ✓ ✕ alalungaserum.... 1
- ✓ ✕ berlepscsherb... 1
- ✓ ✕ cinereousherba... 1
- ✓ ✕ colossalketo.com 1

[Show More](#)

TAG

SYSTEM TAG

COOKIE SEARCH ⓘ

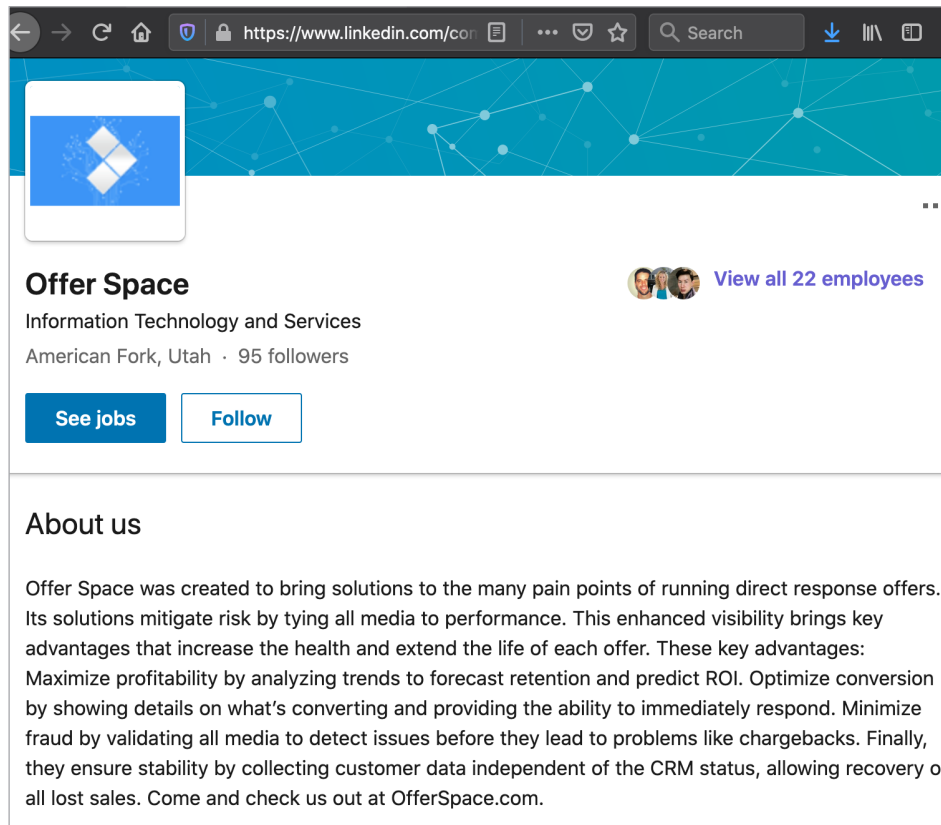
☐ Show : 25 ◀ 1-25 of 2,040 ▶ Sort : Last Seen Descending ▼ Total Records : 2,040

	Hostname	Domain	First Seen	Last Seen	Tags
<input type="checkbox"/>	tepuitherbreief.com	tepuitherbreief.com	2020-04-25	2020-06-08	Download Copy
<input type="checkbox"/>	berlepscsherbalsolution.com	berlepscsherbalsolution.com	2020-04-23	2020-06-08	
<input type="checkbox"/>	notoriousketo.com	notoriousketo.com	2019-11-28	2020-06-08	
<input type="checkbox"/>	phocoenacleanse.com	phocoenacleanse.com	2020-05-10	2020-06-08	
<input type="checkbox"/>	colossalketo.com	colossalketo.com	2020-04-07	2020-06-08	
<input type="checkbox"/>	flippedhealthpro.com	flippedhealthpro.com	2020-04-09	2020-06-07	
<input type="checkbox"/>	ailuropodalifestyle.com	ailuropodalifestyle.com	2020-04-26	2020-06-07	
<input type="checkbox"/>	usefullifestyle.com	usefullifestyle.com	2019-09-22	2020-06-07	
<input type="checkbox"/>	zalophusherbalistoils.com	zalophusherbalistoils.com	2020-04-23	2020-06-07	
<input type="checkbox"/>	ratiteherbal.com	ratiteherbal.com	2020-04-24	2020-06-07	

<https://community.riskiq.com/search/cookies/name/coresess>

Connecting the Subscription Trap Companies

According to the company's LinkedIn page, Offer Space is a direct-response marketing and CRM company that "minimizes fraud by validating all media."¹⁸ As we detailed above, Offer Space's content delivery network and its coresess cookie ties it to multiple domains pushing various products, a large portion of which we directly connect to subscription traps, including those exploiting the pandemic. In this section, we connect Offer Space to the LLCs enumerated by Gary Warner and the company behind Immunity Blend CBD oil. This analysis will illustrate how these entities are intertwined.



According to the Better Business Bureau, Offer Space's address is 1261 S 820 E Ste 210, American Fork, UT 84003-3875.¹⁹ In 2015, offerspace[.]com was registered to Jonathan Virgin. While he is no longer listed in public Whois information, RiskIQ's historical database allows us to see prior registrant information.


¹⁸ <https://www.linkedin.com/company/offer-space>

¹⁹ <https://www.bbb.org/us/ut/american-fork/profile/online-shopping/offer-space-llc-1166-90026217>

<https://community.riskiq.com/search/offerspace.com/whois>

Jonathan Virgin is listed as the founder of another company, Modernized Media, that also lists its address as 1261 S 820 E Ste 210, American Fork, UT 84003. This address is an office building ten minutes away from the post office in Pleasant Grove, Utah, the location used for the return address of the subscription trap LLCs named earlier.

The Modernized Media website also features another breadcrumb: a testimonial from Ryan Dean Hoggan, who is listed as the president of Real Oil, LLC.



[Our Process](#)
[Clients](#)
[About Us](#)
[Contact Us](#)


OUR CLIENTS BELIEVE IN US

HERE IS WHAT A FEW OF THEM SAY

In six months, Modernized Media worked together with me to ideate, develop and launch a new e-commerce brand. The late nights have paid off as we are now shipping 20,000 orders a month and will grow from \$400,000 in revenues in 2016 to over \$10M in 2018. They have been instrumental to our growth and are partners I trust. I am so glad my competitors didn't find them first.

Ryan Dean Hoggan MBA, MGM

President, Real Oil, LLC
realoil.com



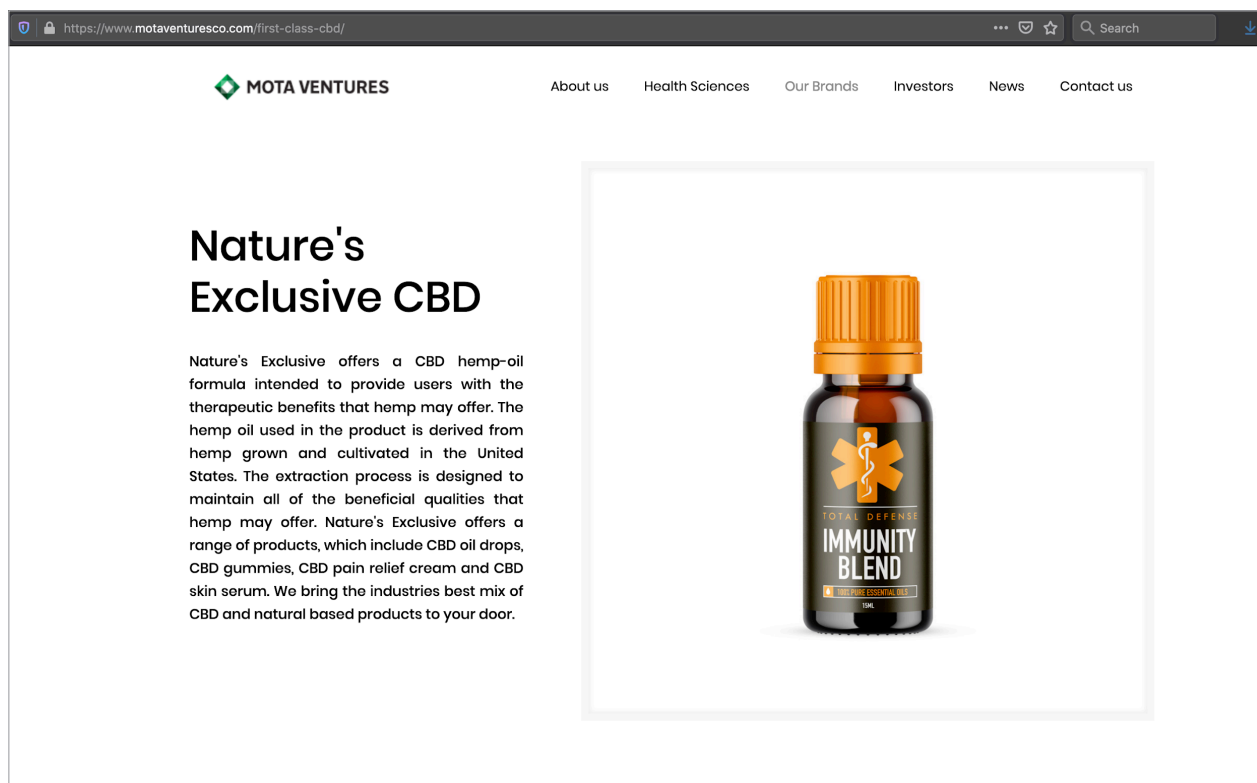
18. <https://www.linkedin.com/company/offer-space>

19. <https://www.bbb.org/us/ut/american-fork/profile/online-shopping/offer-space-llc-1166-90026217>

On February 22, 2020, a press release announced that a company named Mota Ventures had acquired First Class CBD (possibly the same company mentioned in Gary Warner's blog post as First Class Herbalist CBD). It also stated that the founder of First Class CBD, Ryan Dean Hoggan, had been appointed CEO of Mota Ventures. Hoggan was also previously the president of both Offer Space, LLC and Real Oil, LLC (see above), which the release describes as:

...two rapidly growing E-commerce and technology companies focused on serving U.S. based and international consumers in the CBD and natural health products market... the business has generated a database of over 4.5 million customer records and facilitated over \$200 million in consumer transactions from more than one million paying customers in sectors such as beauty, nutrition and CBD products.

The markets mentioned here are the same as those served by the businesses Warner enumerated. These markets also align with the domains connected to the ua-130095210 Google Analytics account. In 2019, Hoggan divested Offer Space and Real Oil to Unified Funding, LLC, another company he founded. The final line of the press release states that "direct to customer sales channels will provide the foundation for the success of Mota."²¹ A visit to Mota Ventures' website shows the Immunity Blend CBD product being pushed by the COVID-19 ads documented above.



On June 5, 2020, Mota Ventures signed a binding agreement to acquire Unified Funding, giving the company direct control over Unified's various services which includes creation and execution of demographically targeted digital marketing campaigns.²²

21. <https://apnews.com/f6b71a440153f933e613a036d735757d>

22. <https://www.benzinga.com/pressreleases/20/06/ac16197354/mota-ventures-signs-binding-term-sheet-to-acquire-e-commerce-platform-leader-unified-funding-with>

According to [proactiveinvestors\[.\]com](https://proactiveinvestors.com), Mota's Immune Support product line brought in 20,959 new customers in March of 2020.²³ From our research, it appears that many of these new customers have likely signed up for expensive subscriptions for CBD oil that does not offer the protection against COVID-19 its advertising promised.

As of now, our investigation of this subscription trap scheme has revealed that:

- ▶ Several LLCs were created over the last few years using the same return address: PO Box 534, Pleasant Grove, UT 84062. The PO Box is near the Offer Space / Modernized Media office.
- ▶ The LLCs all list different business addresses and are registered to different individuals.
- ▶ The Terms of Service used by these various LLCs are word-for-word identical.
- ▶ The various LLCs are the subject of numerous complaints regarding subscription traps and other questionable activity.
- ▶ Offer Space / Modernized Media operate in the direct marketing and e-commerce space, focusing on beauty, nutrition, health, and CBD products. A shared physical address and whois records dating to 2015 connect Offer Space and Modernized Media via Jonathan Virgin.
- ▶ <https://community.riskiq.com/search/offerspace.com/whois>
- ▶ Various indicators tie thousands of domains related to the above products to Offer Space / Modernized Media.
 - Google Analytics account ua-130095210 connects domains observed loading the Immunity Blend CBD oil subscription trap to hundreds of other domains related to beauty, nutrition, health, and CBD products.
 - <https://community.riskiq.com/search/trackers/ua-130095210>
 - Host pairs connect Offer Space's Content Delivery Network to hundreds of domains connected to the ua-130095210 account.
 - <https://community.riskiq.com/search/offerspace.com/hostpairs>
 - A cookie named "coresess" connects Offer Space to over 1,400 suspect domains dating back to 2016.
 - <https://community.riskiq.com/search/cookies/name/coresess>
- ▶ The content observed on these domains is similar or, in many cases, identical.
- ▶ Offer Space is connected to the misleading content contained in these pages.
- ▶ The various ad pages observed on these domains are similar and often identical: misleading pages made to look like legitimate news stories to push subscription traps.
- ▶ Offer Space is connected to Mota Ventures through their work on content pushing the Immunity Blend product, through the founder of Offer Space, who now serves as CEO of Mota Ventures, and through Mota Ventures acquisition of Unified Funding, LLC, which also owns Offer Space.
- ▶ The Immunity Blend subscription trap was repeatedly observed being pushed by ads claiming the CBD oil could protect against COVID-19.
- ▶ The Immunity Blend product is sold through LLCs connected to the Pleasant Grove PO Box, obfuscating Mota Ventures' connection to the subscription traps and the ads.

23. <https://www.proactiveinvestors.com/companies/news/917858/mota-ventures-brings-in-another-c28m-from-placing-to-advance-sales-917858.html>

Conclusion

The evidence above helps us draw distinct connections between the fake news sites, affiliate advertising networks, and subscription trap companies such as Mota Ventures, Offer Space, Modernized Media, and all those LLCs connected to the PO Box in Pleasant Grove. We can also see how this particular traffic funnel—from fake news site to subscription trap—works.

The main commodity of the internet is traffic. Our investigation did not directly connect Bytesignal to Offer Space and Mota Ventures, but it's obvious that these entities are interdependent, relying on each other for traffic and monetization. The Bytesignal websites gather traffic by the spread of their inflammatory content on social media and via sending spam email. Once users are on one of these sites, they are served advertisements through services such as PowerInbox and the Newsmax Feed Network, which monetize the traffic gathered by the content farm sites.

In many instances, the advertisements we observed lead to pages masquerading as legitimate news sources. In turn, these lead to subscription traps off which companies like Offer Space and Mota Ventures profit by convincing people to sign up for costly subscriptions for a range of products, including beauty cream, diet supplements, and CBD oil, etc. In the specific case of Mota Ventures, these subscriptions are for a fraudulent COVID-19 cure.

In this investigation, we found that sales of many questionable goods were carried out through several LLCs, obscuring the connections between the products and the companies that produce them—Immunity Blend CBD oil from Mota Ventures, for example. However, by following the traffic and digging into the data points along the way, we can pull back the curtain protecting these organizations that trade in misinformation and false COVID-19 cures.

Bytesignal / TPN Media project

<https://community.riskiq.com/projects/629aac04-028a-4160-bdfd-5246553e06d3>

Mota Ventures / Offer Space project

<https://community.riskiq.com/projects/875cdcdc-8ea6-47f0-81f9-0ee069e6f18d>

PowerInbox

<https://community.riskiq.com/projects/c84f45db-6951-4e1c-891e-5e550b70a931>

Fake News Ecosystem

<https://community.riskiq.com/projects/00f1756f-cdee-4047-8a35-4d53f8d8206d>

Surfacing Scam Campaigns Through Deep Knowledge of the Internet

This investigation would not have been possible without the data sets, collected over ten years of crawling the internet and intelligently correlated to link infrastructure across the web in our [Internet Intelligence Graph](#). By pivoting across these data sets in RiskIQ PassiveTotal®, researchers can link seemingly disparate elements together to create broad context and a larger, tighter narrative.

RiskIQ collection keeps the full HTML of a web page, saving any dependent file used in its loading process—document object model (DOM), links, console messages, cookies, headers, independent requests, JavaScript, and other files. Because web pages are made up of many of these remote resources that get assembled to form a cohesive user experience, RiskIQ can link infrastructure showing the interconnectivity of various entities across the web, identifying dependencies and pathways of each web asset.

To make our conclusions, we threaded together various seemingly unaffiliated indicators with RiskIQ's in-depth knowledge of the internet made accessible to researchers in PassiveTotal. For example, via a Google Analytics account in the Trackers data set, domains loading the Immunity Blend CBD oil subscription trap connected to hundreds of other subscription traps. Via the Host Pairs data set, Offer Space's Content Delivery Network showed links to hundreds of domains related to that same Google Analytics account. And, via the **"coresess"** cookie in Trackers, Offer Space showed connections to over 1,400 suspect domains dating back to 2016.

To learn more about the data sets and investigation capabilities in RiskIQ PassiveTotal and to try them yourself, sign up today for free with a corporate email address.



RiskIQ, Inc.

22 Battery Street, 10th Floor
San Francisco, CA. 94111

✉ sales@riskiq.net

☎ 1 888.415.4447

Learn more at riskiq.com

Copyright © 2020 RiskIQ, Inc. RiskIQ, the RiskIQ logo and RiskIQ family of marks are registered trademarks or trademarks of RiskIQ, Inc. in the United States and other countries. Other trademarks mentioned herein may be trademarks of RiskIQ or other companies. 08_20