

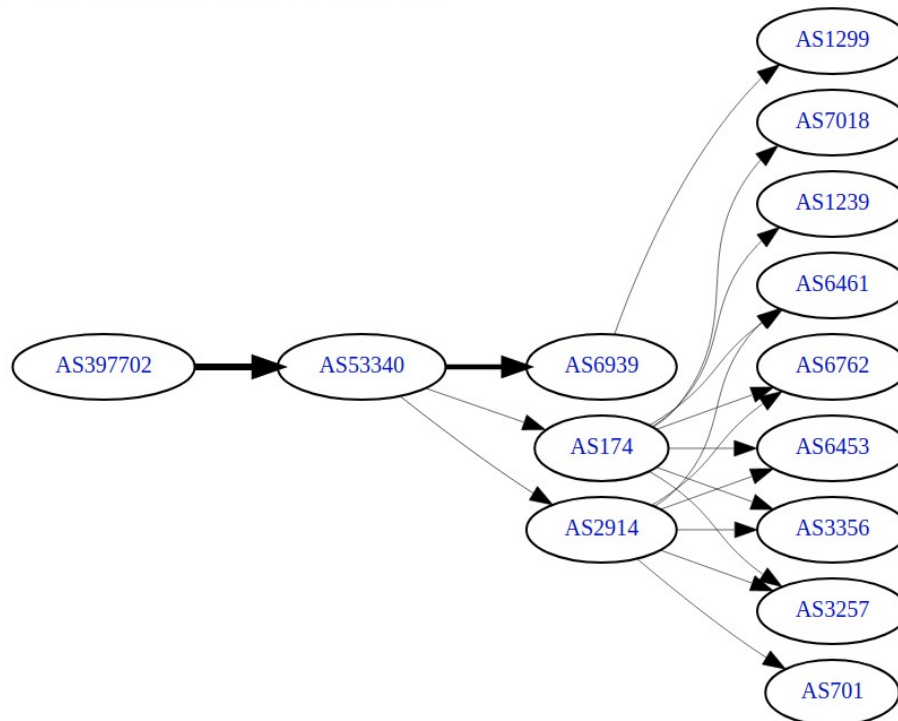
Infrastructure Analysis

Today the onforums.net site is protected by the Cloudflare CDN. Cloudflare has been notoriously uninterested in policing their customer base for extremists. 8Chan was ejected after three mass shootings and prior to that Daily Stormer was sent packing in 2017 after endless provocation. Applying RiskIQ to the problem, we find a clue in the form of what appears to have been a configuration slip in late 2019, revealing AS397702 – 1776 Solutions, LLC.

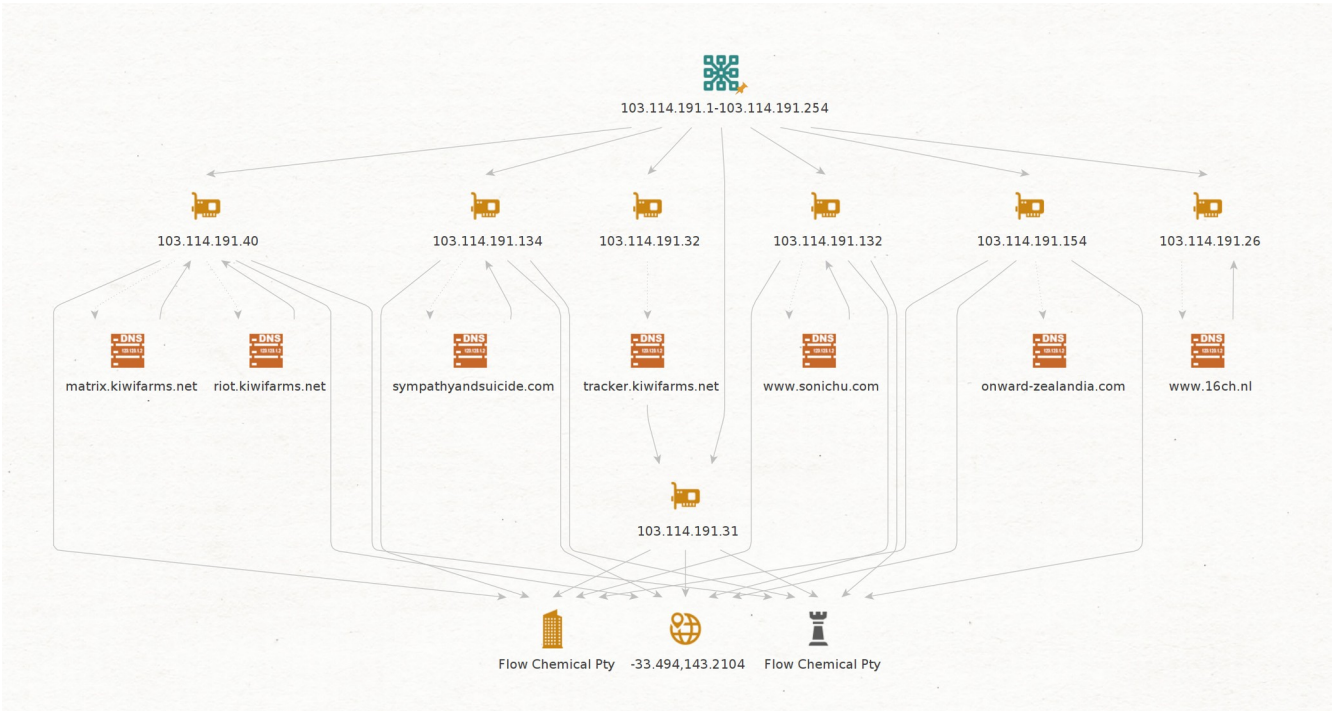
<input type="checkbox"/>	104.31.79.16	US	104.31.64.0/20	13335	2020-01-10	2020-01-31
<input type="checkbox"/>	2606:4700:30::681f:4f10	US	Unknown		2020-01-12	2020-01-12
<input type="checkbox"/>	2606:4700:30::681f:4e10	US	Unknown		2020-01-12	2020-01-12
<input type="checkbox"/>	103.114.191.153	AU	103.114.191.0/24	397702	2019-12-08	2020-01-10
<input type="checkbox"/>	103.114.191.153	AU	103.114.191.0/24	397702	2019-12-09	2019-12-14

This autonomous system is a bit curious, as it only offers 103.114.191.0/24 via BGP and it has just a single peer. BGP is almost always implemented to provide multiple upstreams, as seen here for AS53340, VegasNAP.

AS397702 IPv4 Route Propagation



We inspected the 103.114.191.0/24 subnet using Maltego and found further clues. There were no signs of onaforums.net in this type of scan, but Josh Moon’s Kiwi Farms is clearly present, as are a number of other intriguing domains.



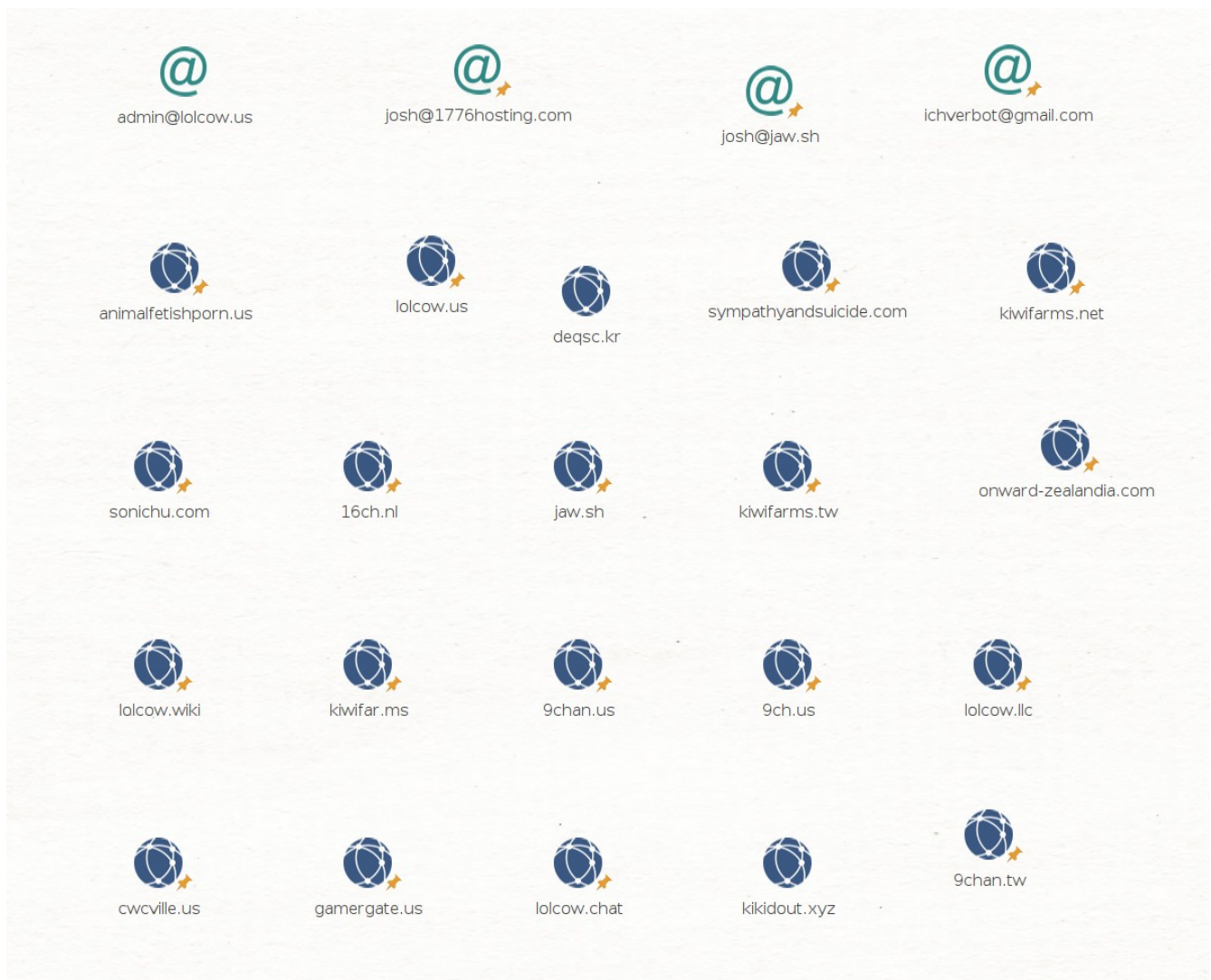
A bit more digging with Google turned up additional connections for Moon.

☐ ▼ Show : 25 ◀ 1-3 of 3 ▶ Sort : Registered Descending ▼ Total Records : 3

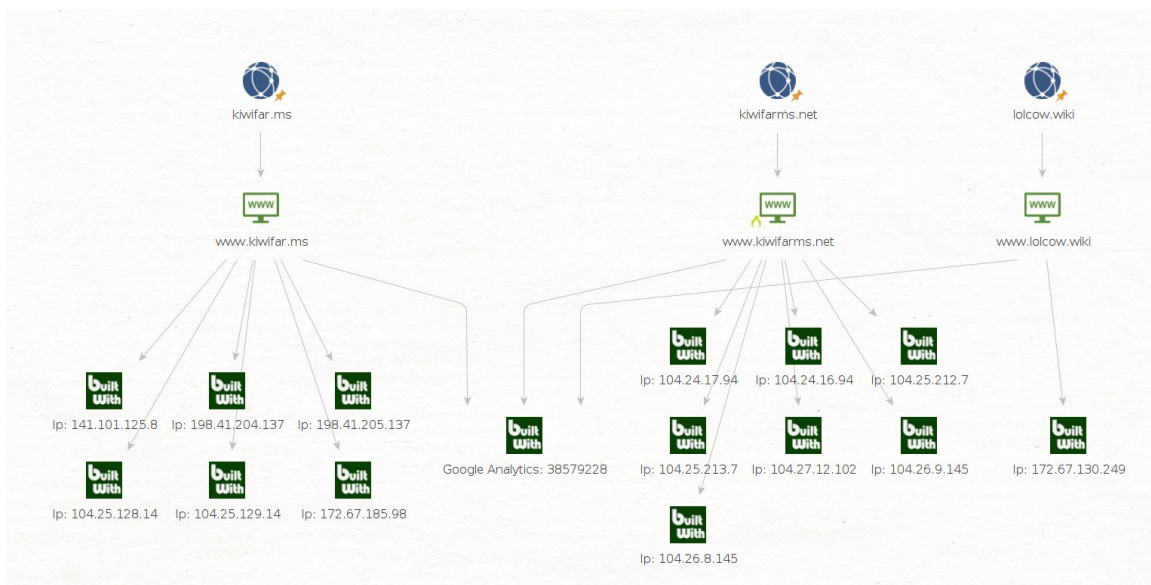
	Focus	Email
<input type="checkbox"/>	103.114.191.0	abuse@1776hosting.com
<input type="checkbox"/>	as397702	josh@1776hosting.com
<input type="checkbox"/>	kiwifarms.tw	ichverbot@gmail.com

1-3 of 3

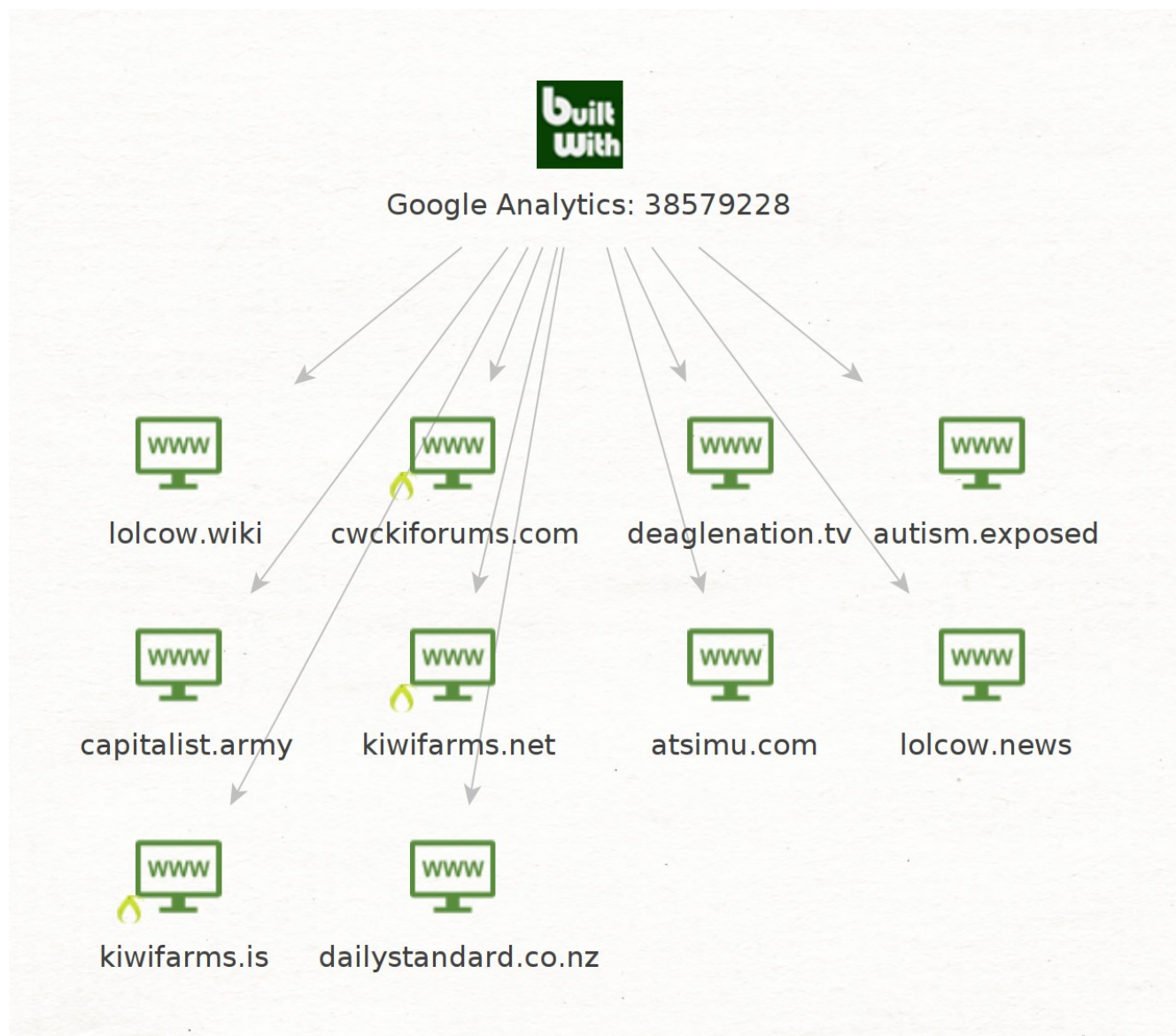
We continued this iterative process of applying Google, Maltego, and RiskIQ until we had what we believe to be a fairly complete top level map of Moon’s holdings, which is preserved as JoshMoonTopLevel-2020-07-21.mtg, a Maltego file.



An inspection of these domains using BuiltWith revealed further entanglement:

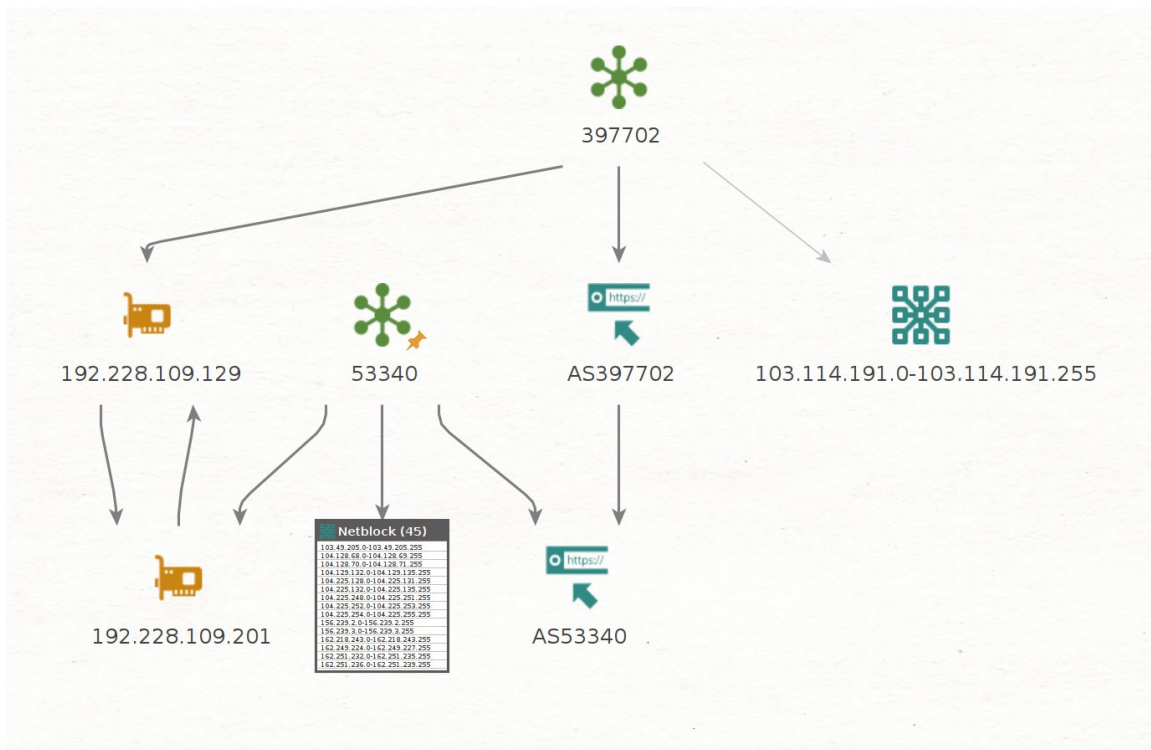


The presence of a shared Google Analytics ID binds the domains together and shows which of them may have been monetized using Google Ads. Pursuing that leads, we find more domains that seem like they fit with the rest of Moon's holdings. The Daily Standard domain seems out of place, but not only is it owned by Moon, it reveals what may be a home address in Pensacola, Florida. Further examination turned up another residential address some sixty miles from the first.



Properties owned by an operator like Moon may be revenue producers based on advertising, pet projects that have not been developed, or names that have been squatted, perhaps to harass a high value target. Given his career path, Moon must have some revenue producing activity that is immune to public pressure against him.

What worked against 8chan, and against Daily Stormer before them, was attention to their technical infrastructure. We already noted the unusual arrangement 1776 Solutions AS397702 has with its upstream, VegasNAP AS53340.



1776 Solutions has a single block of 256 IP addresses, 103.114.191.0/24, which was assigned by APNIC, the Asia Pacific regional internet registry. VegasNAP has fifty IPv4 prefixes of their own amount to nearly 38,000 public IPs and they seem to provide transit for another hundred prefixes. That makes sense, given that NAP is industry shorthand for Network Access Point.

Prior to digging deeply, we want to be sure about locations. While the autonomous system is VegasNAP, the response page for Hurricane Electric instead shows FiberHub.com.


AS53340 VegasNAP, LLC

[ks](#)
[home](#)
[report](#)
[report](#)
[report](#)
[s](#)
[routes](#)

[port](#)
[stics](#)
[s](#)
[s App](#)
[nnel](#)
[tion](#)
[s](#)

[AS Info](#)
[Graph v4](#)
[Graph v6](#)
[Prefixes v4](#)
[Prefixes v6](#)
[Peers v4](#)
[Peers v6](#)
[Whois](#)
[IRR](#)
[IX](#)

Company Website: <http://www.fiberhub.com>

Country of Origin: [United States](#) 

Internet Exchanges: 3


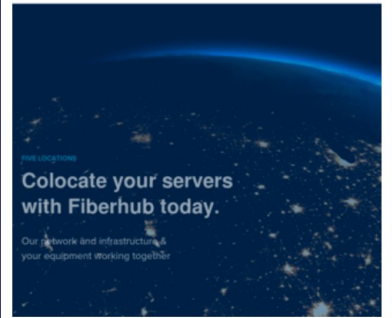
Prefixes Originated (all): 57
Prefixes Originated (v4): 50
Prefixes Originated (v6): 7

Prefixes Announced (all): 163
Prefixes Announced (v4): 156
Prefixes Announced (v6): 7

BGP Peers Observed (all): 202
BGP Peers Observed (v4): 201
BGP Peers Observed (v6): 28

IPs Originated (v4): 37,632
AS Paths Observed (v4): 46,341
AS Paths Observed (v6): 651

Average AS Path Length (all): 4.216
Average AS Path Length (v4): 4.224
Average AS Path Length (v6): 3.591

A lookup of fiberhub.com produced a street address of 1110 Palms Airport Drive, Las Vegas, NV. The view from above was promising:



There are five key points about this facility:

- Railroad tracks nearby; which are often used for fiber optic right of way.
- Office space density of air conditioning units on the right side of roof.
- Very heavy air conditioning gear on left side of roof.
- Two large generators at left rear.
- No vehicles in parking lot.

What this says to an experienced colocation operator, on Google Maps satellite imagery alone, is that there is a data center inside the left half of this building. Being in Las Vegas, tornadoes are not a concern, so an above ground facility would still be considered carrier grade. The right side is either mixed office/warehouse, or undeveloped. The FiberHub.com web site reveals more information about their national network.

NETWORK

Our Infrastructure

Fiberhub operates network PoP's in some of the most carrier-dense facilities in the world.

- ✓ 10Gbps private transport between each facility
- ✓ Multiple 10Gbps uplinks to carriers like NTT, Cogent, HE.Net and more
- ✓ Latest generation Brocade networking gear

Looking Glass

The presence of 10Gbps links clearly shows they have fiber of their own between their sites. Searching for additional FiberHub autonomous systems we found AS36114. “Announcing bogons” is network operator slang for offering inappropriate prefixes via BGP. This can be RFC1918 private address space or a simple misconfiguration. Hurricane Electric’s BGP Looking Glass reports that this AS offered two blocks of unallocated space from 162.0.0.0/8, which is managed by ARIN, the American Registry of Internet Numbers.

Plausible explanations for these blocks being offered include a simple misconfiguration, as listed above, but IPv4 address space is increasingly dear, and this may have been an attempt to employ these blocks, which were retired by the previous user.

AS36114 VegasNAP, LLC

Links

[Home](#)
[Report](#)
[Report](#)
[es](#)
[Routes](#)
[port](#)
[istics](#)
[ss](#)
[ls App](#)
[nnel](#)
[ation](#)
[ss](#)
[e](#)

AS Info

Graph v4

Graph v6

Prefixes v4

Prefixes v6

Peers v4

Peers v6

Whois

IRR

AS36114 announces bogons.

Country of Origin: United States

Prefixes Originated (all): 23

Prefixes Originated (v4): 22

Prefixes Originated (v6): 1

Prefixes Announced (all): 23

Prefixes Announced (v4): 22

Prefixes Announced (v6): 1

BGP Peers Observed (all): 1

BGP Peers Observed (v4): 1

BGP Peers Observed (v6): 1

IPs Originated (v4): 29,184

AS Paths Observed (v4): 942

AS Paths Observed (v6): 356

Average AS Path Length (all): 4.446

Average AS Path Length (v4): 4.548

Average AS Path Length (v6): 4.177

A player of this size is not going to get their hands dirty directly, but being based in “Sin City” they likely have shady customers in gaming, adult entertainment, and other industries involving vices. Searching for FiberHub on LinkedIn, we find that this is a small family owned business. Four of the visible employees are clearly related. This is a plausible staff size for the management of the facility. There aren’t enough technical staff listed here given the square footage. Checking VegasNAP reveals that Betty’s husband is a co-founder.



Natalie Tyree • 2nd
CFO at Fiberhub
Las Vegas, Nevada Area



Betty Fisher-Reed • 3rd
Administrative Officer
Las Vegas, Nevada Area



Rob Tyree • 2nd
Colocation, Web Hosting, and Managed IT Services Expert
Las Vegas, Nevada Area



Bob Tyree • 3rd
Data Center tech at Fiberhub
Las Vegas, Nevada Area



Emmalee Tyree-Greatwood • 3rd
Sales Account Manager at Fiberhub
Las Vegas, Nevada Area



Billy Cooter • 2nd
Business Development Specialist at Fiberhub
Spokane, Washington Area

2 results



Don Reed • 3rd
Co-Founder, VegasNAP
Las Vegas, Nevada Area

Connect

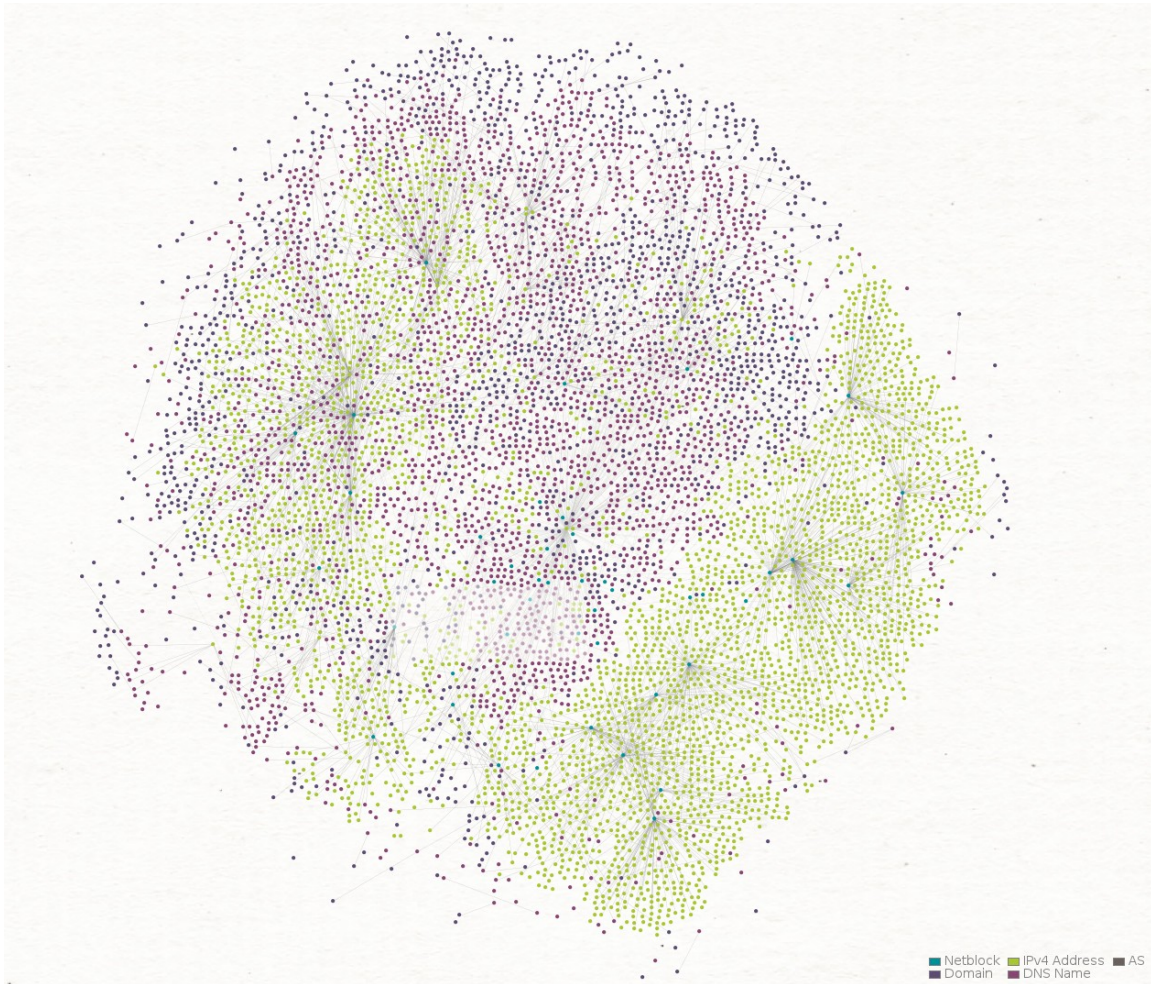


Natalie Tyree • 2nd
CFO at Fiberhub
Las Vegas, Nevada Area

Connect

New Zealand

What does any of this have to do with New Zealand? Moon is nominally in Florida, the hosting operation is in Las Vegas, and they have some sort of facility in Los Angeles, which might be a place for New Zealand businesses to locate their systems. We scanned the VegasNAP AS's address space and found 1,475 domain names. We then dug a bit further to see if we could correlate any of them with Moon's holdings. This produced no additional signs of entanglement.



That is an enormous body of information and we wanted to narrow it down. We applied the following procedure to the dataset:

- Searched all domains to see which ones had email addresses in use, 112 total.
- Focused on domains in the .nz top level domain.
- Identified a few companies that are global in scope using the facility.
- Final list of 64 domains that might not wish to be associated with Kiwi Farms.

While drafting this report we discovered that Maltego had only queried about 20% of all domains for email due to our API limits with them. There were 330 in the .nz top level domain we had missed, but 64 was still an acceptable sample size for our examination.

Domains With Multiple Active Email Addresses

christchurchlawnmowing.co.nz	promotepr.co.nz	liquidwaste.co.nz	heybabycovers.com
darfieldrugby.co.nz	textmarks.com	neurosky.com	lifetimebucketlist.com
seitech.co.nz	lihsi.com	dogrescuedunedin.nz	sanctuarybayofislands.co.nz
logicgroup.co.nz	mananclinic.com	moelong.com	cathaycinemas.co.nz
careerideas.co.nz	castlerockcafe.co.nz	kuranuicollege.school.nz	scotweb.co.nz
completewebsol.com	stronach.co.nz	naithani.co.in	bombich.com
musicglue.com	theartistgoldsmith.com	ecsbatam.com	rcmtg.com
cambridgeraceway.co.nz	avjskills.com	plastoeltronics.com	lanwriter.com
cuttingroom.co.nz	forthe love of dance.co.nz	nzpta.org.nz	fibresheet.com
change.org.nz	robur.co.nz	mcraesglobal.com	electricplum.com
jbbusiness.co.nz	imsb.maori.nz	mci.net.nz	deckprismsports.com
yewtec.com	gtpop.com	essencesoflight.co.nz	schooltransport.org.nz
accuradio.com	rubygems.org	fitlifepedia.com	msfoody.com
salberg.org	macsep.com	earth-soil.com	shobhaproducts.com
caltopo.com	webgas.co.nz	everestfibre.com	rupeeinvestments.com
highbuilddepoxy.com	bankersnursing.com	logdown.com	mauriora.co.nz

The big question is this: *“How many of these businesses are aware they share infrastructure with the web site that distributed Christchurch shooter Brenton Tarrant’s manifesto?”*

Reaching out one at a time, trying to identify which of these entities is newsworthy, would be an exercise in frustration for a non-native. The obvious first stop would be the New Zealand Parent Teacher Association ... but one of our analysts did some checking, and it seems to be disbanded.

We chose at this point to hunt for a New Zealand based journalist who could better untangle things.

1776 Solutions

Moon’s operation, 1776 Solutions, has a few assets and associates that appear to be intentionally concealed behind VegasNAP and Cloudflare.

- Autonomous System Number 397702¹
- IPv4 prefix 103.114.191.0/24²
- Flow Chemical Pty.³
- Vincent (Shi) Zhen, Chinese national from Hohhot, Inner Mongolia
- 1776 Solutions, LLC⁴, originally **Final Solutions**, a Wyoming LLC.

1 <https://bgp.he.net/AS397702>

2 <https://wq.apnic.net/static/search.html?query=103.114.191.0/24>

3 <https://opengovau.com/company/154040490>

4 <https://wyobiz.wyo.gov/Business/FilingDetails.aspx?eFNum=034127143077132130035027094038122174129088154221>

The registration of AS397702 seems to be in order.

ASNumber: 397702
ASName: US-SSSS
ASHandle: AS397702
RegDate: 2019-07-03
Updated: 2019-07-03
Ref: <https://rdap.arin.net/registry//autnum/397702>

OrgName: 1776 Solutions, LLC
OrgId: FSL-189
Address: 30 N. Gould Street
Address: Suite 6883
City: Sheridan
StateProv: WY
PostalCode: 82801
Country: US
RegDate: 2017-08-14
Updated: 2019-07-03
Ref: <https://rdap.arin.net/registry//entity/FSL-189>

OrgNOCHandle: MOONJ18-ARIN
OrgNOCName: Moon, Joshua
OrgNOCPhone: +1-757-932-5494
OrgNOCEmail: josh@1776hosting.com
OrgNOCRef: <https://rdap.arin.net/registry//entity/MOONJ18-ARIN>

OrgAbuseHandle: MOONJ18-ARIN
OrgAbuseName: Moon, Joshua
OrgAbusePhone: +1-757-932-5494
OrgAbuseEmail: josh@1776hosting.com
OrgAbuseRef: <https://rdap.arin.net/registry//entity/MOONJ18-ARIN>

OrgTechHandle: MOONJ18-ARIN
OrgTechName: Moon, Joshua
OrgTechPhone: +1-757-932-5494
OrgTechEmail: josh@1776hosting.com
OrgTechRef: <https://rdap.arin.net/registry//entity/MOONJ18-ARIN>

The registration for the 103.114.191.0/24 prefix shows something curious – an Australian company is marked as the owner. Some times registrations of prefixes can be stale, but the contact for the organization was changed in May of 2018 and the company involved changed in July of 2019? This seems like subterfuge on first glance, so we contacted an Australian associate to assist us in untangling the particulars of Flow Chemical Pty.

irt: IRT-1776-US
30 N Gould St
address: Suite 6884
Sheridan, WY 82801
e-mail: admin@1776hosting.com
abuse-mailbox: abuse@1776hosting.com
admin-c: JM2339-AP
tech-c: JM2339-AP
auth: # Filtered
mnt-by: MAINT-1776-US
last-modified: 2018-05-12T02:26:35Z
source: APNIC

[Report invalid contact](#)

person: Joshua Moon
address: 913 Beal Pkwy NW Suite A-1017
country: US
phone: +17579325494
e-mail: josh@1776hosting.com
nic-hdl: JM2339-AP
mnt-by: MAINT-1776-US
last-modified: 2018-05-15T21:32:51Z
source: APNIC

[Report invalid contact](#)

% Information related to '103.114.191.0/24AS397702'

route: 103.114.191.0/24
origin: AS397702
descr: Flow Chemical Pty Ltd
8/179 Sir Fred Schonell Dr
mnt-by: MAINT-1776-US
last-modified: 2019-07-11T17:41:37Z
source: APNIC

- Flow Chemical Pty Ltd
 - Aus gov register : <https://abr.business.gov.au/ABN/View?id=53154040490>
 - never been registered for GST, means trading turnover under 75K, if any
 - likely a dormant or shelf company
 - Registered since 18 Jan 2012
 - Address is St Lucia, Queensland 4067
- searching ASIC register :
 - actual registration date (date docs lodged) : 02/11/2011
 - registered address : '8', 179 Sir Fred Schonell Drive, ST LUCIA QLD 4067
 - one director :
 - Name: VINCENT ZHEN
 - Address: '8', 179 Sir Fred Schonell Drive, ST LUCIA QLD 4067
 - Born: 12/02/1985, HOHHOT, CHINA
 - Appointment date: 02/11/2011
 - Zhen is the only shareholder as well
 - since registration no other forms lodged to update details etc
 - company was registered using an online service : ECompanies
- 179 Sir Fred Schonell Drive, ST LUCIA
 - appears to be an old residential block of units
 - Google Maps search :



1776 Solutions LLC is registered in Wyoming, a known haven for shell companies. The entity was originally registered as Final Solutions, LLC. That comports nicely with the same thin cover used for ONAforums.



Wyoming Secretary of State
2020 Carey Avenue
Suite 700
Cheyenne, WY 82002-0020
Ph. 307-777-7311

For Office Use Only
Ed Murray, WY Secretary of State
FILED: Aug 11 2017 10:16AM
Original ID: 2017-000764572

Limited Liability Company Articles of Organization

I. The name of the limited liability company is:
Final Solutions, LLC

II. The name and physical address of the registered agent of the limited liability company is:
Registered Agents Inc.
412 N Main St Ste100
Buffalo, WY 82834

III. The mailing address of the limited liability company is:
30 N. Gould Street Suite 6884
Sheridan, WY 82801

IV. The principal office address of the limited liability company is:
30 N. Gould Street Suite 6884
Sheridan, WY 82801

V. The organizer of the limited liability company is:
Registered Agents Inc.
412 N Main St Ste 100 Buffalo, WY 82834



Ed Murray
Wyoming Secretary of State
2020 Carey Avenue, Suite 700
Cheyenne, WY 82002-0020
Ph. 307.777.7311
Fax 307.777.5339
Email: Business@wyo.gov

Ed Murray, WY Secretary of State
FILED: 10/06/2017 10:11 AM
Original ID: 2017-000764572
Amendment ID: 2017-002142574

Limited Liability Company Amendment to Articles of Organization

1. Name of the limited liability company:

Final Solutions, LLC

2. The date of filing its articles of organization: 08/11/2017

3. Article number(s) 1 is amended as follows:

The name of the limited liability company is:
1776 Solutions, LLC

Signature:
(Shall be executed by a person authorized by the company.)

Print Name: Riley Park

Title: Authorized Individual

Date: 09/29/2017
(mm/dd/yyyy)

Contact Person: Riley Park

Daytime Phone Number: (307) 200-2803

Email: reports@registeredagentsinc.com

(Email provided will receive annual report reminders and filing evidence)

Conclusions

Josh Moon was instrumental in the creation of 8chan, which while under the command of the father/son team of Jim and Ron Watkins, served as the outlet of choice for three mass shooters.

- Brenton Tarrant – Christchurch, NZ, 51 dead, 49 injured.
- John Timothy Earnests – Poway, CA, 1 dead, 3 injured.
- Patrick Crusius – El Paso, TX, 23 dead, 23 injured.

Moon profanely refused to turn over data to New Zealand investigators related to Brenton Tarrant⁵. His profile on Rational Wiki led to this pithy writeup in New York Magazine's Intelligencer⁶. If Moon is not a psychopath, he's doing an amazing job of acting line one online. Any attempt at shaming is a waste of time; characters like him relish the attention and benefit from the perception of being an "untouchable".

The intentional transnational jurisdictional mess provides a forbidding barrier to any civil action. If Moon could be found and served, given that his sites are seen as assets by the violent fringe right, there will likely be some sort of pro bono legal representation available. The defense will lean on the protections service providers have due to Section 230 of the Communications Decency Act, the 1st Amendment, and counsel will face a full throttle assault from Kiwi Farms and ONAforums regulars.

The Final Solution

The only available means of putting a stop to this behavior, short of a federal indictment, requires a two pronged approach towards deplatforming. Administrative attention on the digital assets such the autonomous system, the IP prefix, and other more esoteric approaches may provide some operational friction, which is beneficial. If the employees and customers of FiberHub/VegasNAP find themselves holding the bag for Moon's despicable behavior, they will not hesitate to eject one problem customer for the sake of retaining many hundreds of others.

As happened with 8chan, Moon's digital assets will move. 8chan had several false starts at new locations that immediately ejected them once they were made aware of their presence. The ultimate refuge for 8chan was rebranding to 8kun and a relationship with a Russian hosting firm. Moon will find similar options, given the utility he has in relation to Russia's attempts to interfere in the 2020 election.

Once Russian support is confirmed, every business entity connected to the remaining effort must be made aware that their relationship likely involves dealing with entities that are under international sanctions, as well as participating in providing cover for what can be characterized as a foreign intelligence operation. These tactics have been employed for the last three years on smaller players, mostly relieving them of SSL certificates. Once those are gone, e-commerce is much more difficult, and search engine rankings drop precipitously.

5 https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=12214017

6 <https://nymag.com/intelligencer/2016/07/kiwi-farms-the-webs-biggest-community-of-stalkers.html>