Reconnaissance

On: Rivian

Sep 24, 2023

Bit Dancing Studios
123 Some St.
Yourtown, IL 60547
https://bitsdanceforme.blog/

Point of Contact
Amy Devine
adevine@depaul.edu

Executive Summary

Bit Dancing Studios was contracted to perform reconnaissance on Rivian. Rivian has an international presence. In addition, Rivian seems to leverage cloud technology, from Amazon Web Services (AWS), Salesforce, Proofpoint, making some technical resolution difficult.

Overview of the company

Rivian is an eco-conscious company that is focused on designing automobiles while reducing carbon emissions and with an eye towards environmentally sound materials. Rivian was founded in 2009 and has taken over a decade to produce their first vehicles.

Locations

Rivian has a variety of locations in North America and Europe. There are main locations, mentioned in Table 1. Each of the locations mentioned in Table 1 correspond to a different legal entity. Rivian also has engineering centers and “spaces”.

Main Locations

United States			
Rivian Automotive, LLC 14600 Myford Road Irvine, CA 92606 United States	Rivian, LLC 14600 Myford Road Irvine, CA 92606 United States	Rivian Insurance Services, LLC 100 N Rivian Motorway Normal, IL 61761 United States	
Canada			
Rivian Automotive Canada, Inc. 1038 Homer Street Vancouver, BC V6B 2W9 Canada			
Mexico			
Rivian Mexico Sociedad			

de Responsabilidad Limitada de Equity Variable Hacienda San Sebastián 4400 Colonia Pedregal de Cumbres 64344 Monterrey, Nuevo León Mexico			
Europe			
RIV UK Engineering Limited 54 Portland Place London W1B 1DY United Kingdom	Rivian United Kingdom Limited 1 Albion House High St., Unit 6 Woking GU21 6BG United Kingdom	Rivian Europe B.V. Herengracht 433, Unit 2.01 & 2.02 Amsterdam 1017BR Netherlands	Rivian Netherlands B.V. Herengracht 433, Unit 2.01 & 2.02 Amsterdam 1017BR Netherlands
Rivian GmbH Marienstr. 15 c/o Bird & Bird LLP 60329 Frankfurt am Main Germany	Rivian SE Europe d.o.o. Beograd Krunska 73 Beograd 11000 Third Floor, Office No. 1 Serbia		

Table 1 - Main Locations

Engineering Centers

Rivian has additional locations focused on development and manufacturing of the vehicles. They are located on their webpage - https://rivian.com/our-company. IT is located in both the Irvine, CA and Normal, IL locations.

- Irvine, CA
  - Engineering, supply chain, IT, electronics
- Los Angeles, CA
  - Power Conversion, motors
- Palo Alto, CA
  - Vehicle software
- Normal, IL

- Manufacturing, engineering, supply chain, IT, QA
- Plymouth, MI
  - Supply chain/procurement
- Wittmann, AZ
  - Testing
- Woking, UK
  - Engineering
- Vancouver, BC
  - User Apps and Software

Spaces

In addition, Rivian offers “spaces” or places where the public can come and see Rivian vehicles. https://rivian.com/spaces

Locations in Chicago, IL, Vancouver, BC Canada, and Seattle, WA. More locations are opening up across North America, according to their website. People can sign up online to receive notifications from these spaces.

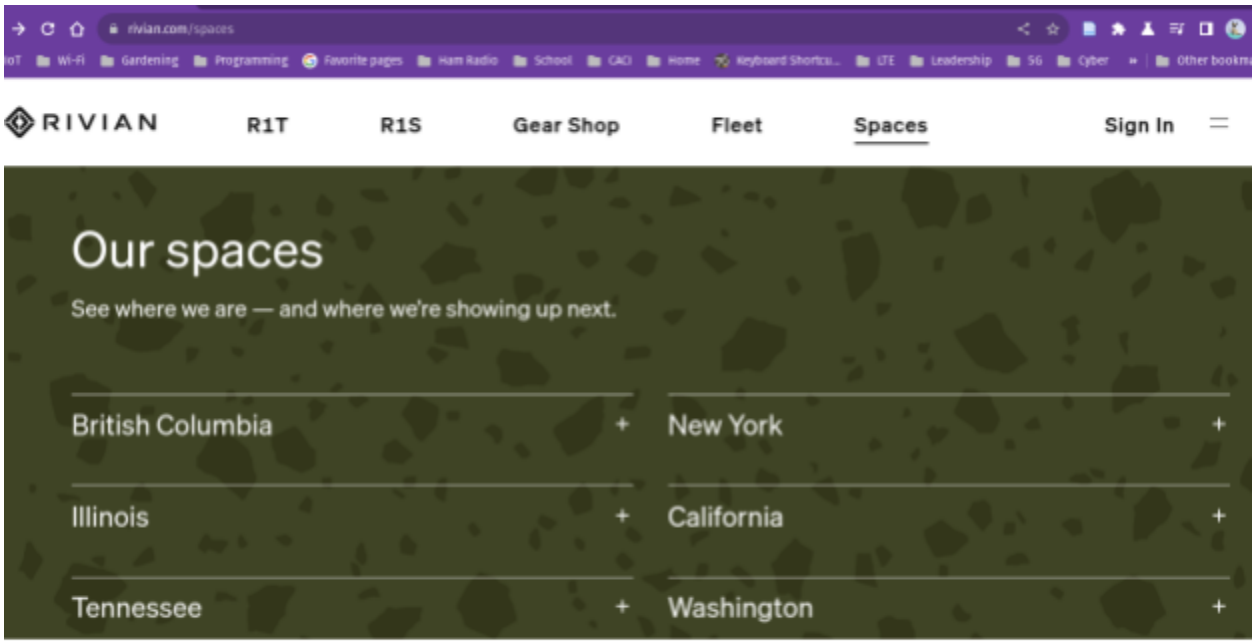


Figure 1 - Rivian Spaces

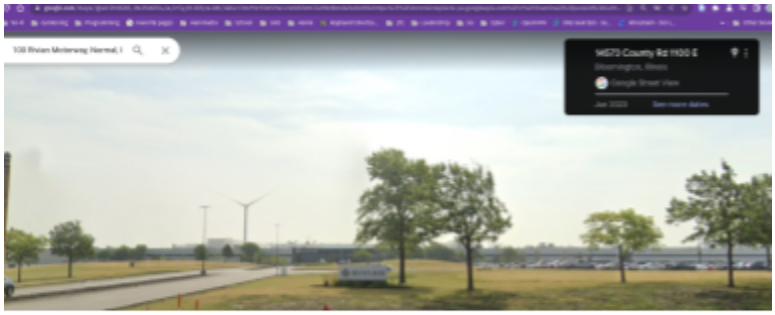
Spaces provide an opportunity for anyone to show up, experience Rivian vehicles, learn about the company and make connections to employees within the company. Given the right social engineer, corporate espionage may be possible leading to the acquisition of trade secrets, corporate badges or credentials, and human connections to inside the company. In person events are also a great way to start building trust with the target.

No registration is necessary to attend a space meaning that a social engineer or corporate spy could just walk right in.

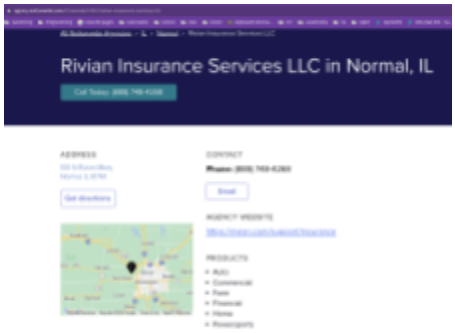
Business Structure

Rivian appears to be comprised of many different LLCs, based on location and “focus” - manufacturing, service, insurance.

Rivian Insurance Services LLC appears to be a Nationwide insurance agency in Normal, IL. Google Street View shows that there is no gate, no physical barrier to getting to the office. Someone could easily drive up, park, probably do some wi-fi recon as well.



Google Street View - Showing Physical Access to Normal, IL facility



Internet Information about Normal, IL


100 Rivian Motorway, Normal, I
RIVIAN


RIVIAN

Internet Presence

Rivian has multiple LLCs under it. For this reconnaissance phase, rivian.com was surveyed. Rivian.com seems to be hosted on Amazon Web Services (AWS) with

```
artemis@pop-os:~$ nslookup rivian.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   rivian.com
Address: 13.226.22.95
Name:   rivian.com
Address: 13.226.22.103
Name:   rivian.com
Address: 13.226.22.84
Name:   rivian.com
Address: 13.226.22.101
```

Non-authoritative
nslookup for rivian.com

Target Domain	URL	IP	Net Mask	IP Range	Notes
	rivian.com	13.226.22.95	13.224.0.0/14	13.224.0.0 - 13.227.255.255	Name is AMAZO-CF - Possibly amazon cloudfront, content distribution network (CDN).
DNS Servers	ns-280.awsdns-35.com	205.251.193.24	205.251.192.0/21	205.251.192.0 - 205.251.199.255	Has a published certificate associated with the whois.arin.net record.

Target Domain	URL	IP	Net Mask	IP Range	Notes
					Name is AMAZON-BYOIP (See Appendix A - References)
	ns-985.awsdns-59.net	205.251.195.217			
	ns-1408.awsdns-48.org	205.251.197.128			
	ns-1610.awsdns-09.co.uk	205.251.198.74			
Mail Servers	awsdns-hostmaster.amazon.com	92.249.37.12			
	mxb-005c6a01.gslb.pphosted.com				
	mxa-005c6a01.gslb.pphosted.com				
Subdomains	media.rivian.com				
	products.rivian.com				
	csadmin.gtm.stage.rivian.com				
	internal.rivian.com				
	coreservices.api.prod.rivian.com				
	ftp.rivian.com				

Target Domain	URL	IP	Net Mask	IP Range	Notes
	test.jac0b.com				

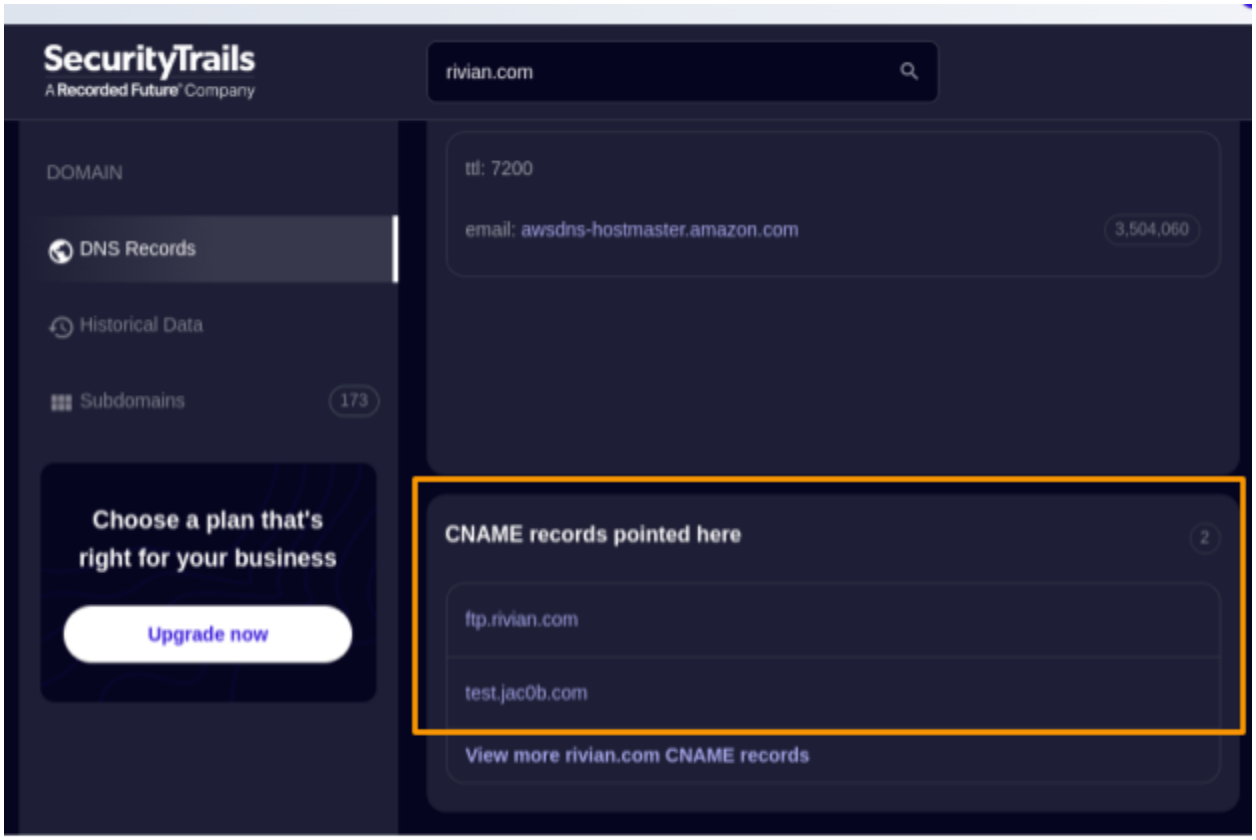
Table 2: Internet Recon for rivian.com

```
> set type=ns
> rivian.com
;; communications error to 192.33.14.30#53: timed out
Server:         192.33.14.30
Address:        192.33.14.30#53

Non-authoritative answer:
rivian.com      nameserver = ns-985.awsdns-59.net.
rivian.com      nameserver = ns-1610.awsdns-09.co.uk.
rivian.com      nameserver = ns-280.awsdns-35.com.
rivian.com      nameserver = ns-1408.awsdns-48.org.

Authoritative answers can be found from:
> artemis@pop-os:~$
```

Nameservers for rivian.com

dig was used to find the IP addresses for the nameservers.

Looking at SecurityTrails.com, we can see that there are two domains that alias to rivian.com.



Domains that alias to rivian.com

From the CNAME, we can see that there is an ftp site (ftp.rivian.com) and possibly a test site (test.jac0b.com)?

```
> test.jac0b.com
;; communications error to 127.0.0.53#53: timed out
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
test.jac0b.com  canonical name = rivian.com.
rivian.com
        origin = ns-280.awsdns-35.com
        mail addr = awsdns-hostmaster.amazon.com
        serial = 1
        refresh = 7200
        retry = 900
        expire = 1209600
        minimum = 86400

Authoritative answers can be found from:
>
```

Nslookup for test.jac0b.com - aliased to rivian.com

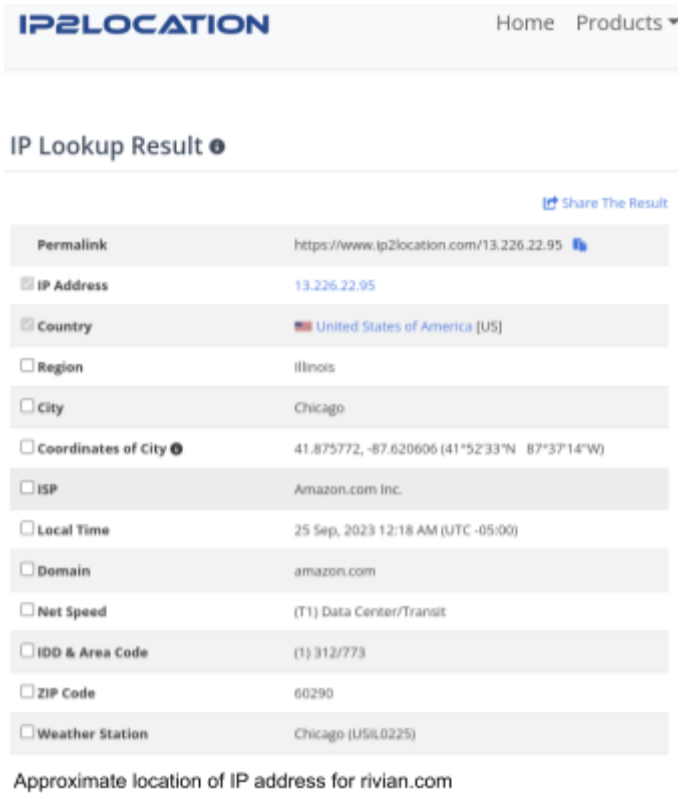
```
> ftp.rivian.com
;; communications error to 127.0.0.53#53: timed out
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
ftp.rivian.com  canonical name = rivian.com.
rivian.com
        origin = ns-280.awsdns-35.com
        mail addr = awsdns-hostmaster.amazon.com
        serial = 1
        refresh = 7200
        retry = 900
        expire = 1209600
        minimum = 86400

Authoritative answers can be found from:
>
```

Nslookup for ftp.rivian.com

Attempts to find additional information on ftp.rivian.com or test.jac0b.com did not prove fruitful.

Network Asset Locations

Reconnaissance was done with IP 154.47.25.114 provided by Surfshark VPN. When performing dns lookups for rivian.com, it appears that a local amazon cloudfront server is serving company information. The location of the CF server with IP:13.226.22.95 is in Chicago.



Approximate location of IP address for rivian.com

Linked Sites

Google dorking with link:rivian.com -site:rivian.com provides a list of websites that link back to rivian.com.

- https://www.georgia.org/rivian - new construction facility in GA, not listed in above locations - provides ability to get in early to construction site, do some advanced recon on the building/installation, get in good with the developers to discover good places/locations for extraction hardware to be placed. If someone could be implanted in any of the subcontractors typically used for construction projects, networks could be tapped very early on.
- Google Play Store - Rivian apps
- Rivian Case Study on AWS
- Reddit - Community around the products, quickly increase knowledge about the products, speak like a seasoned user. Potentially make initial human connections.

Personal Events

In addition to the locations and events mentioned in Spaces, Rivian has multiple ways to physically meet employees. Gatherings are mentioned on their webpage.

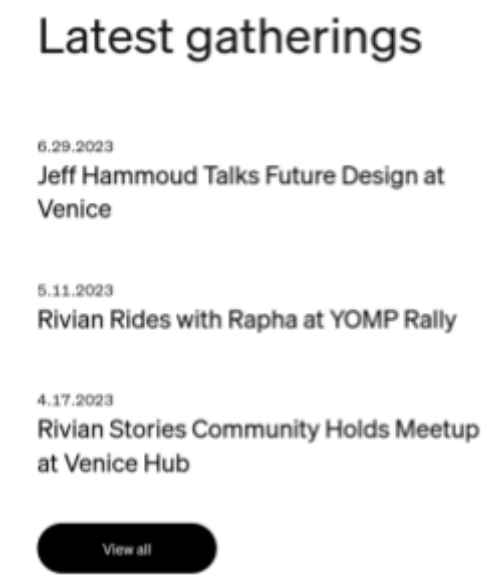


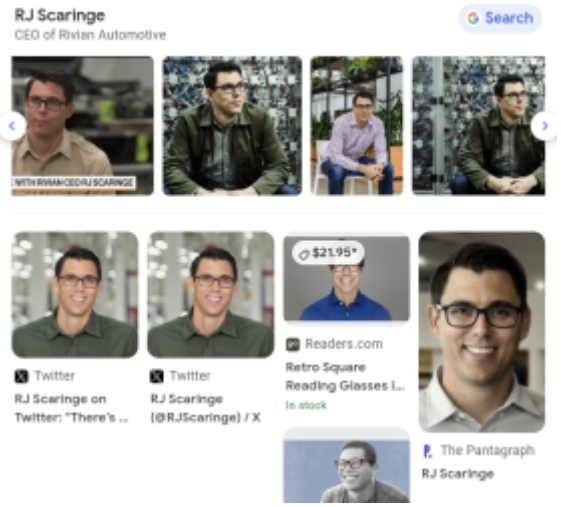
Figure 2 - Gatherings

Notable Personnel

Rivian leadership is posted at rivian.com/our-company. Names, titles, candid pictures as well as short bios about each person (click on their name).

RJ Scaringe - Founder and Chief Executive Officer

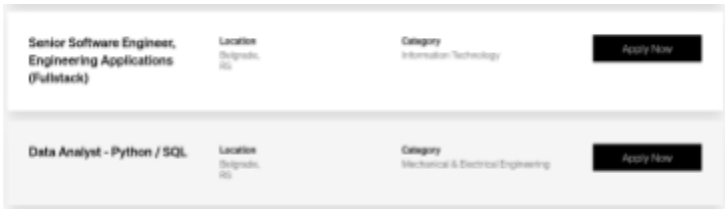
- Posts as @RJScaringe on X/Twitter
- Seems to enjoy the outdoors based on photos
- Engineer, BS from RPI, PhD at MIT
- Grew up in Melbourne, FL and rebuilt a Porsche 356s as a child. (See Forbes)
- MIT Alumni profile
- Married, has 3 kids



From the available information, a plausible MIT alumni fake story could be constructed to create trust with RJ Scaringe quickly. May also provide opportunities to meet up at MIT events.

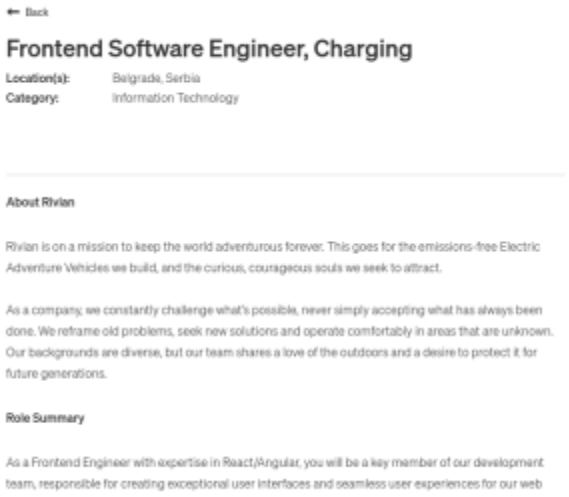
Technology Used

Job Postings



Jobs are searchable from the main website: https://careers.rivian.com/careers-home/
Some technologies include:

- Python
- SQL
- React/Angular
- Battery Management System (BMS)
- Software-in-the-Loop (SIL) testing
- Linux
- C/C++/Rust
- CAN bus



Many different disciplines are represented at Rivian. Software exploits could focus in these areas. Rivian is currently seeking an Information Technology Assurance Director to perform technology audits: IT governance, controls, cloud architecture, etc.
Questions about who and how cybersecurity is controlled and maintained within the company exist. Helpful google dork: site:linkedin.com intext:rivian AND intext:"IT" AND intext:"cybersecurity" leading to:

- David Johnson - Manager in Industrial/OT Cybersecurity
- Skylar Glass - Sr. Staff Cybersecurity Engineering at Rivian
- Quintin N - Cyber Threat Detection Lead

All three appear to have only been with Rivian for under 2 years. Perhaps the cybersecurity focus is relatively new.

Connected Vehicles

> "Rivian Insurance integrates with our connected vehicle platform and suite of safety features to bring you tailored, data-driven coverage."

Connected vehicles means that there is the opportunity for exploiting the data transferred between the vehicle and a server, somewhere. It also means that the vehicle has a digital fingerprint.

Appendix A - References

1. Active vs Passive techniques, ways to stay organized - securitysift.com
2. Nslookup - passive look-ups of DNS servers and IP addresses
3. ARIN.net - Registration information about IP addresses and domains
4. BYOIP - Bring Your Own IP, service offered by Amazon, used to understand how the DNS results might be interpreted
5. Google - Because it knows all, used for dorking and image searching
6. Proofpoint - Email security, background information only
7. IP2Location.com - Used to