BigQuery Usage for EV Cyberattack Data

Presented By: Alex Clemovitz, Chris Nichols, Diana Amaya Nino, Isagani Hernandez, and Harish Kumar Nalumas

Problem Statement

At Lucid Motors, our EV charging stations have been increasingly targeted by cyberattacks that disrupt our services and negatively affect our operating costs. At the present, we lack visibility into which attacks are the most destructive to our bottom line, making it difficult to determine where to allocate our resources most efficiently. By identifying and analyzing which cyberattacks cause the greatest operational and financial damage, we aim to determine how to best allocate company resources to curb losses as quickly as possible.

The Business of EV and Cyber

EV & Lucid Motors:

- Lucid Motors relies on software-driven cars
- Cybersecurity is crucial to protect vehicle data, charging infrastructure and passenger safety
- EV network security helps prevent financial loss & operational issues

Cyberattacks & Security:

- Cyberattacks disrupt operations, costs and damage brand image
- Important to invest in prevention, detection and data protection

Dataset Understanding

Our dataset was chosen from the University of New Brunswick's Canadian Institute of Cybersecurity.

The data was collected in a lab-environment where researchers set up multiple Level-2 EV charging stations and deliberately attacked them with various cyberattacks. Measurements of several system parameters were taken during both attack and benign conditions to determine the overall operational impacts on their charging infrastructure.

Types of Cyberattacks in Dataset

Vulnerability Scans (vuln-scan): an attack scans a system looking for security flaws, like a burglar who checks for unlocked doors and windows. Usually precedes an attack.

TCP Flood: A type of Denial of Service (DoS) in which a system if overwhelmed with service requests

Backdoor Attack: an attack that bypasses authentication through malware. Can also be a precursor for future attacks.

SYN-Flood: Another type of DoS attack that exploits the TCP handshake process in which connect processes are initiated but never completed, which overwhelms the system.

Crytopjacking: an attack installs cryptocurrency mining software to steal cryptocurrencies such as Bitcoin.

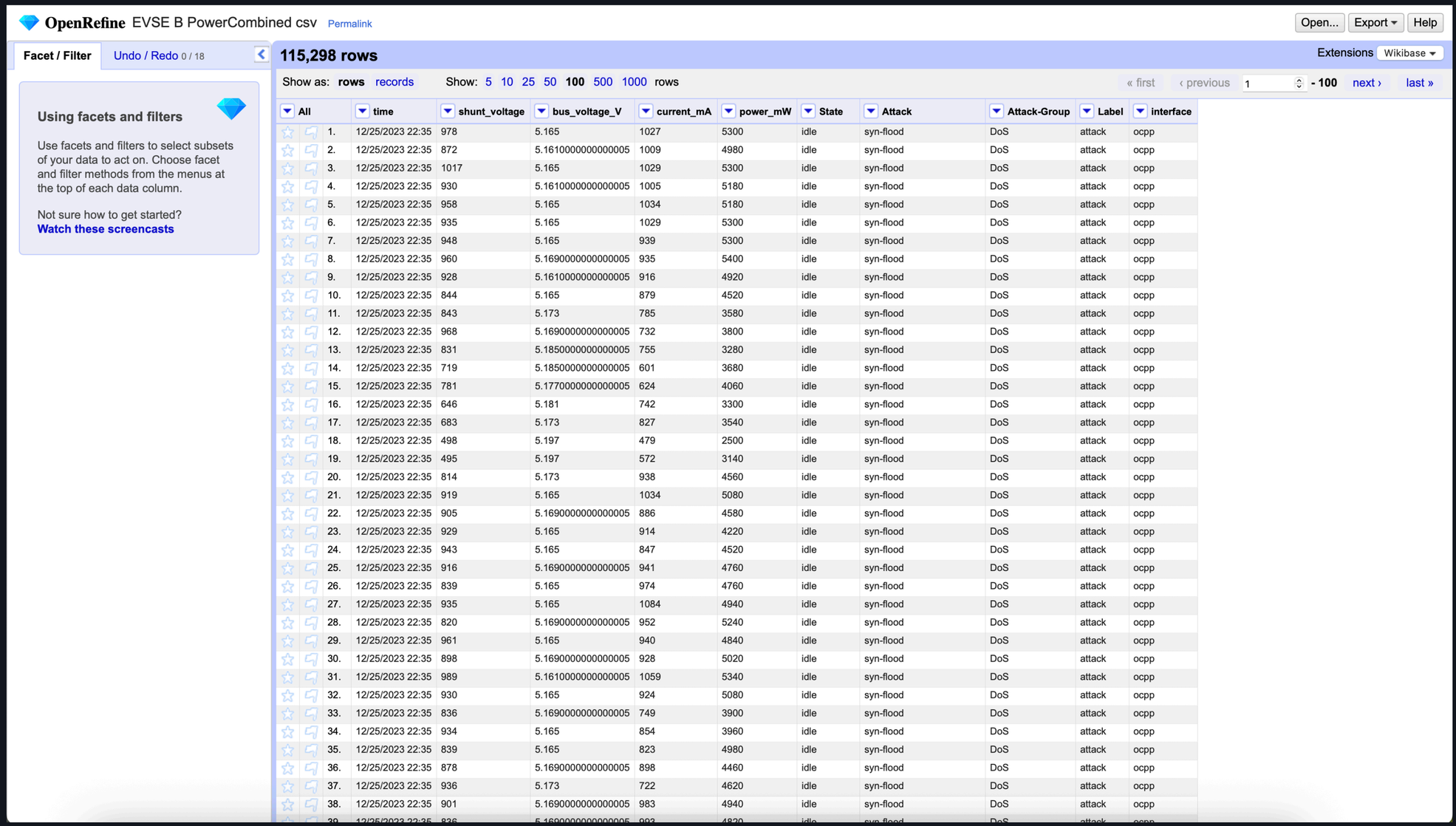
Stealth Scan (SYN-Scan): attacks probe open ports without using the TCP handshake system. Unlike the TCP Flood, thisdoes not overwhelm the system.

• • •

Data Prep with OpenRefine-Before

Main Issues:

- Inconsistent column title casing
- Multiple unintuitive column titles
- Timestamps treated as text strings instead of times/dates
- Numbers treated as text strings instead of numerical values
- Inconsistent rounding of numerical values



All	time	shunt_voltage	bus_voltage_V	current_mA	power_mW	State	Attack	Attack-Group	Label	interface
1.	12/25/2023 22:35	978	5.165	1027	5300	idle	syn-flood	DoS	attack	ocpp
2.	12/25/2023 22:35	872	5.1610000000000005	1009	4980	idle	syn-flood	DoS	attack	ocpp
3.	12/25/2023 22:35	1017	5.165	1029	5300	idle	syn-flood	DoS	attack	ocpp
4.	12/25/2023 22:35	930	5.1610000000000005	1005	5180	idle	syn-flood	DoS	attack	ocpp
5.	12/25/2023 22:35	958	5.165	1034	5180	idle	syn-flood	DoS	attack	ocpp
6.	12/25/2023 22:35	935	5.165	1029	5300	idle	syn-flood	DoS	attack	ocpp
7.	12/25/2023 22:35	948	5.165	939	5300	idle	syn-flood	DoS	attack	ocpp
8.	12/25/2023 22:35	960	5.1690000000000005	935	5400	idle	syn-flood	DoS	attack	ocpp
9.	12/25/2023 22:35	928	5.1610000000000005	916	4920	idle	syn-flood	DoS	attack	ocpp
10.	12/25/2023 22:35	844	5.165	879	4520	idle	syn-flood	DoS	attack	ocpp
11.	12/25/2023 22:35	843	5.173	785	3580	idle	syn-flood	DoS	attack	ocpp
12.	12/25/2023 22:35	968	5.1690000000000005	732	3800	idle	syn-flood	DoS	attack	ocpp
13.	12/25/2023 22:35	831	5.1850000000000005	755	3280	idle	syn-flood	DoS	attack	ocpp
14.	12/25/2023 22:35	719	5.1850000000000005	601	3680	idle	syn-flood	DoS	attack	ocpp
15.	12/25/2023 22:35	781	5.1770000000000005	624	4060	idle	syn-flood	DoS	attack	ocpp
16.	12/25/2023 22:35	646	5.181	742	3300	idle	syn-flood	DoS	attack	ocpp
17.	12/25/2023 22:35	683	5.173	827	3540	idle	syn-flood	DoS	attack	ocpp
18.	12/25/2023 22:35	498	5.197	479	2500	idle	syn-flood	DoS	attack	ocpp
19.	12/25/2023 22:35	495	5.197	572	3140	idle	syn-flood	DoS	attack	ocpp
20.	12/25/2023 22:35	814	5.173	938	4560	idle	syn-flood	DoS	attack	ocpp
21.	12/25/2023 22:35	919	5.165	1034	5080	idle	syn-flood	DoS	attack	ocpp
22.	12/25/2023 22:35	905	5.1690000000000005	886	4580	idle	syn-flood	DoS	attack	ocpp
23.	12/25/2023 22:35	929	5.165	914	4220	idle	syn-flood	DoS	attack	ocpp
24.	12/25/2023 22:35	943	5.165	847	4520	idle	syn-flood	DoS	attack	ocpp
25.	12/25/2023 22:35	916	5.1690000000000005	941	4760	idle	syn-flood	DoS	attack	ocpp
26.	12/25/2023 22:35	839	5.165	974	4760	idle	syn-flood	DoS	attack	ocpp
27.	12/25/2023 22:35	935	5.165	1084	4940	idle	syn-flood	DoS	attack	ocpp
28.	12/25/2023 22:35	820	5.1690000000000005	952	5240	idle	syn-flood	DoS	attack	ocpp
29.	12/25/2023 22:35	961	5.165	940	4840	idle	syn-flood	DoS	attack	ocpp
30.	12/25/2023 22:35	898	5.1690000000000005	928	5020	idle	syn-flood	DoS	attack	ocpp
31.	12/25/2023 22:35	989	5.1610000000000005	1059	5340	idle	syn-flood	DoS	attack	ocpp
32.	12/25/2023 22:35	930	5.165	924	5080	idle	syn-flood	DoS	attack	ocpp
33.	12/25/2023 22:35	836	5.1690000000000005	749	3900	idle	syn-flood	DoS	attack	ocpp
34.	12/25/2023 22:35	934	5.165	854	3960	idle	syn-flood	DoS	attack	ocpp
35.	12/25/2023 22:35	839	5.165	823	4980	idle	syn-flood	DoS	attack	ocpp
36.	12/25/2023 22:35	878	5.1690000000000005	898	4460	idle	syn-flood	DoS	attack	ocpp
37.	12/25/2023 22:35	936	5.173	722	4620	idle	syn-flood	DoS	attack	ocpp
38.	12/25/2023 22:35	901	5.1690000000000005	983	4940	idle	syn-flood	DoS	attack	ocpp

Data Prep with OpenRefine-After

Resolved Issues:

- All columns now have consistent title casing
- Column titles are more intuitive to the viewer
- All timestamps are now in recognized time/date format
- All numbers are now treated as numerical values
- All numbers are consistently rounded in each column

OpenRefine EVSE B PowerCombined2 csv Permalink

Open... Export Help

Facet / Filter | Undo / Redo 15 / 15

Using facets and filters

Use facets and filters to select subsets of your data to act on. Choose facet and filter methods from the menus at the top of each data column.

Not sure how to get started?
Watch these screencasts

115,298 rows

Extensions: Wikibase

Show as: **rows** records Show: 5 10 25 **50** 100 500 1000 rows

« first ‹ previous 1 - 50 next › last »

All	Time	Shunt_Voltage	Bus_Voltage_V	Current_Consumption_mA	Power_Consumption_mW	Charging_State	Attack_Type	Attack_Group	Attack_Conditions	Targeted_Interface
1.	2023-12-25T22:35:00Z	978	5.165	1027	5300	idle	syn-flood	DoS	attack	ocpp
2.	2023-12-25T22:35:00Z	872	5.161	1009	4980	idle	syn-flood	DoS	attack	ocpp
3.	2023-12-25T22:35:00Z	1017	5.165	1029	5300	idle	syn-flood	DoS	attack	ocpp
4.	2023-12-25T22:35:00Z	930	5.161	1005	5180	idle	syn-flood	DoS	attack	ocpp
5.	2023-12-25T22:35:00Z	958	5.165	1034	5180	idle	syn-flood	DoS	attack	ocpp
6.	2023-12-25T22:35:00Z	935	5.165	1029	5300	idle	syn-flood	DoS	attack	ocpp
7.	2023-12-25T22:35:00Z	948	5.165	939	5300	idle	syn-flood	DoS	attack	ocpp
8.	2023-12-25T22:35:00Z	960	5.169	935	5400	idle	syn-flood	DoS	attack	ocpp
9.	2023-12-25T22:35:00Z	928	5.161	916	4920	idle	syn-flood	DoS	attack	ocpp
10.	2023-12-25T22:35:00Z	844	5.165	879	4520	idle	syn-flood	DoS	attack	ocpp
11.	2023-12-25T22:35:00Z	843	5.173	785	3580	idle	syn-flood	DoS	attack	ocpp
12.	2023-12-25T22:35:00Z	968	5.169	732	3800	idle	syn-flood	DoS	attack	ocpp
13.	2023-12-25T22:35:00Z	831	5.185	755	3280	idle	syn-flood	DoS	attack	ocpp
14.	2023-12-25T22:35:00Z	719	5.185	601	3680	idle	syn-flood	DoS	attack	ocpp
15.	2023-12-25T22:35:00Z	781	5.177	624	4060	idle	syn-flood	DoS	attack	ocpp
16.	2023-12-25T22:35:00Z	646	5.181	742	3300	idle	syn-flood	DoS	attack	ocpp
17.	2023-12-25T22:35:00Z	683	5.173	827	3540	idle	syn-flood	DoS	attack	ocpp
18.	2023-12-25T22:35:00Z	498	5.197	479	2500	idle	syn-flood	DoS	attack	ocpp
19.	2023-12-25T22:35:00Z	495	5.197	572	3140	idle	syn-flood	DoS	attack	ocpp
20.	2023-12-25T22:35:00Z	814	5.173	938	4560	idle	syn-flood	DoS	attack	ocpp
21.	2023-12-25T22:35:00Z	919	5.165	1034	5080	idle	syn-flood	DoS	attack	ocpp
22.	2023-12-25T22:35:00Z	905	5.169	886	4580	idle	syn-flood	DoS	attack	ocpp
23.	2023-12-25T22:35:00Z	929	5.165	914	4220	idle	syn-flood	DoS	attack	ocpp
24.	2023-12-25T22:35:00Z	943	5.165	847	4520	idle	syn-flood	DoS	attack	ocpp
25.	2023-12-25T22:35:00Z	916	5.169	941	4760	idle	syn-flood	DoS	attack	ocpp
26.	2023-12-25T22:35:00Z	839	5.165	974	4760	idle	syn-flood	DoS	attack	ocpp
27.	2023-12-25T22:35:00Z	935	5.165	1084	4940	idle	syn-flood	DoS	attack	ocpp
28.	2023-12-25T22:35:00Z	820	5.169	952	5240	idle	syn-flood	DoS	attack	ocpp
29.	2023-12-25T22:35:00Z	961	5.165	940	4840	idle	syn-flood	DoS	attack	ocpp
30.	2023-12-25T22:35:00Z	898	5.169	928	5020	idle	syn-flood	DoS	attack	ocpp
31.	2023-12-25T22:35:00Z	989	5.161	1059	5340	idle	syn-flood	DoS	attack	ocpp
32.	2023-12-25T22:35:00Z	930	5.165	924	5080	idle	syn-flood	DoS	attack	ocpp
33.	2023-12-25T22:35:00Z	836	5.169	749	3900	idle	syn-flood	DoS	attack	ocpp
34.	2023-12-25T22:35:00Z	934	5.165	854	3960	idle	syn-flood	DoS	attack	ocpp
35.	2023-12-25T22:35:00Z	839	5.165	823	4980	idle	syn-flood	DoS	attack	ocpp
36.	2023-12-25T22:35:00Z	878	5.169	898	4460	idle	syn-flood	DoS	attack	ocpp
37.	2023-12-25T22:35:00Z	936	5.173	722	4620	idle	syn-flood	DoS	attack	ocpp
38.	2023-12-25T22:35:00Z	901	5.169	983	4940	idle	syn-flood	DoS	attack	ocpp

Making Queries in BigQuery

Untitled query Run Save Download

```
1  SELECT Attack, COUNT(*) AS count
2  FROM nichols2adta.evdataset.evdataset
3  GROUP BY Attack
4  ORDER BY count DESC;
```

Query completed

Query results

Job information | Results | Visualization | JSON | Execution d

Row	Attack	count
1	vuln-scan	26246
2	tcp-flood	21367
3	Backdoor	21137
4	none	14363
5	syn-flood	13517
6	cryptojacking	11596
7	syn-stealth	7072

Here the count of each type of attack is tabulated and group by type of attack. We can see the top three types of attacks were vulnerability scans, TCP Floods, and Backdoor attacks.

Making Queries in BigQuery

Untitled query | Run | Save | Download | Share | Schedule | Open in | More

```
SELECT Time, power_mW, Attack
FROM nichols2adta.evdataset.evdataset
ORDER BY Time;
```

Query completed

Query results | Save result

Job information | Results | Visualization | JSON | Execution details | Execution graph

Row	Time	power_mW	Attack
1	2023-12-24 16:18:00 UTC	2400	syn-stealth
2	2023-12-24 16:18:00 UTC	2420	syn-stealth
3	2023-12-24 16:18:00 UTC	2420	syn-stealth
4	2023-12-24 16:18:00 UTC	2780	syn-stealth
5	2023-12-24 16:18:00 UTC	2400	syn-stealth
6	2023-12-24 16:18:00 UTC	2400	syn-stealth
7	2023-12-24 16:18:00 UTC	2420	syn-stealth
8	2023-12-24 16:18:00 UTC	2460	syn-stealth
9	2023-12-24 16:18:00 UTC	2420	syn-stealth
10	2023-12-24 16:18:00 UTC	2420	syn-stealth
11	2023-12-24 16:18:00 UTC	2420	syn-stealth
12	2023-12-24 16:18:00 UTC	2420	syn-stealth

Results per page: 50 | 1 – 50 of 11

In this query, we are showing the different attacks and what the battery power in mW was during the attack. In this image, we mainly are focusing on the SYN-stealth attack on 12/24/2023 which occurred multiple times on 12/24/2023 during the 6:00 hour.

Making Queries in BigQuery

Untitled query | Run | Save | Download | Share | Schedule | Open in | More

```
SELECT
  Attack,
  TIMESTAMP_TRUNC(Time, HOUR) AS hour,
  AVG(power_mW) AS avg_power
FROM
  nichols2adta.evdataset.evdataset
WHERE
  Attack != 'None'
GROUP BY
  Attack, hour
ORDER BY
  hour, Attack;
```

Query completed

Query results | Save results | Open in

Job information | Results | Visualization | JSON | Execution details | Execution graph

Row	Attack	hour	avg_power
1	syn-stealth	2023-12-24 16:00:00 UTC	2535.735110370...
2	syn-stealth	2023-12-24 17:00:00 UTC	2531.462994836...
3	syn-stealth	2023-12-24 18:00:00 UTC	2548.860759493...
4	vuln-scan	2023-12-24 18:00:00 UTC	2533.603238866...
5	vuln-scan	2023-12-24 19:00:00 UTC	2544.497991967...
6	vuln-scan	2023-12-24 20:00:00 UTC	2518.187033849...

Results per page: 50 | 1 – 42 of 42

In this query, we are tracking the average battery power usage during charging by the hour on 12/24/2023. We can see what types of attacks are occurring for during each hour in our dataset. In the image, we can see that a SYN-stealth and vulnerability scan both happened at around 6:00 on that day.

Making Queries in BigQuery

Untitled query | Run | Save | Download | Share | Schedule

```
SELECT
  Attack,
  DATE(Time) AS date,
  MAX(power_mW) AS peak_power,
  MIN(power_mW) AS min_power
FROM
  nichols2adta.evdataset.evdataset
WHERE
  Attack != 'None'
GROUP BY
  Attack, date
ORDER BY
  peak_power DESC
LIMIT 100;
```

Query completed

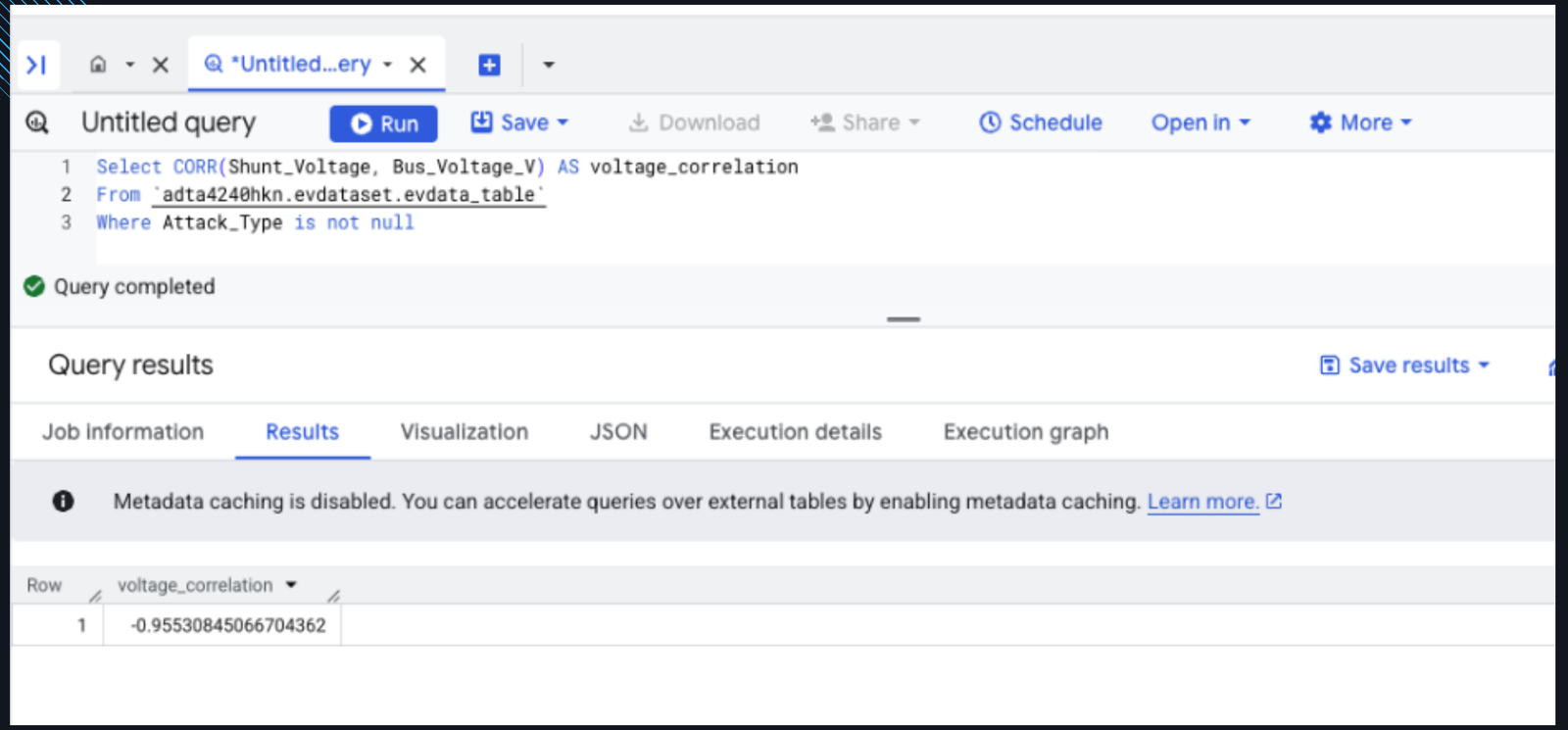
Query results

Job information | Results | Visualization | JSON | Execution details | Execution graph

Row	Attack	date	peak_power	min_power
1	syn-flood	2023-12-26	6300	2460
2	cryptojacking	2023-12-26	6100	3800
3	syn-flood	2023-12-25	6020	2500
4	Backdoor	2023-12-30	5840	2420
5	none	2023-12-26	5180	2160

In this query, we are seeing what the peak and minimum battery powers were during specific days for each type of attack in order to find patterns when predicting future attacks.

Making Queries in BigQuery



In this query, we are seeing the correlation between Shunt Voltage and Bus Voltage. The correlation value indicates, its negatively correlated. That means it's behaving in an inversely proportional manner. If **Bus Voltage** rises, the **Shunt Voltage** drops, or vice versa

Making Queries in BigQuery

Targete... ace | *Untitled...ery

Untitled query | Run | Save | Download | Share | Schedule | Open in

```
1  Select Targeted_Interface, CORR(Power_Consumption_mW, Shunt_Voltage) AS power_shunt_correlation,
2    CORR(Power_Consumption_mW, Bus_Voltage_V) AS power_bus_correlation
3  From `adta4240hkn.evdataset.evdata_table`
4  Group by Targeted_Interface
5  Order by  Targeted_Interface
```

Query completed

Query results

Job information | Results | Visualization | JSON | Execution details | Execution graph

Row	Targeted_Interface	power_shunt_corr...	power_bus_correl...
1	any	0.823894372219...	-0.868682588041...
2	none	0.541907855134...	-0.640340593757...
3	ocpp	0.970347104059...	-0.971661991699...

In this query, we are seeing the correlation between power consumption and shunt voltage, and the correlation between power consumption and Bus voltage. The results show that while the power shunt correlation is positive and strong, the power bus correlation is negative. This indicates that there is some potential to optimize the power system by adjusting voltage settings.

Making Queries in BigQuery

*Untitled...ery

Untitled query | Run | More | Save | Download | Share | Schedule | Open i

```
1  Select Targeted_Interface, Attack_Type, Count(*) AS attack_count
2  From `adta4240hkn.evdataset.evdata_table`
3  Where Attack_Type is not null
4  Group by Targeted_Interface, Attack_Type
5  Order by attack_count Desc
```

Query completed

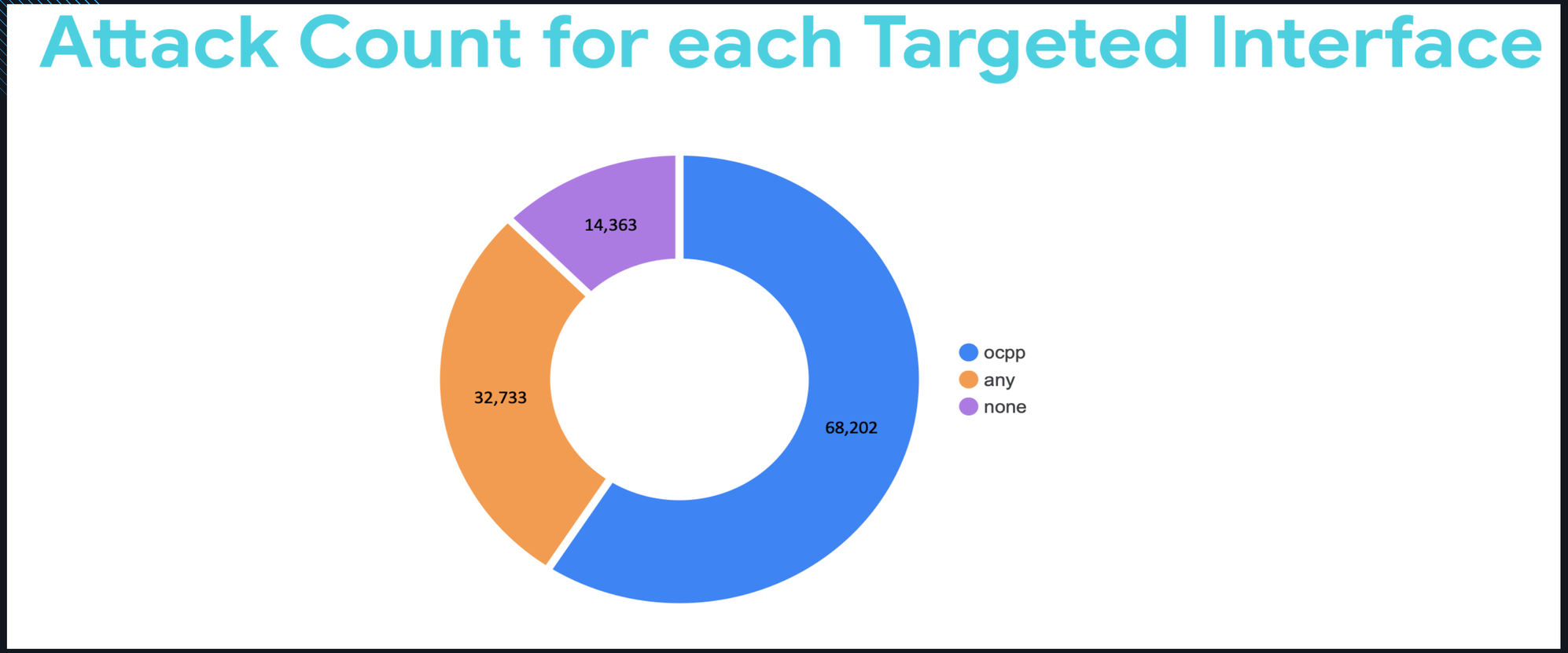
Query results | Sav

Job information | Results | Visualization | JSON | Execution details | Execution graph

Row	Targeted_Interface	Attack_Type	attack_count
1	ocpp	vuln-scan	26246
2	ocpp	tcp-flood	21367
3	any	backdoor	21137
4	none	none	14363
5	ocpp	syn-flood	13517
6	any	cryptojacking	11596
7	ocpp	syn-stealth	7072

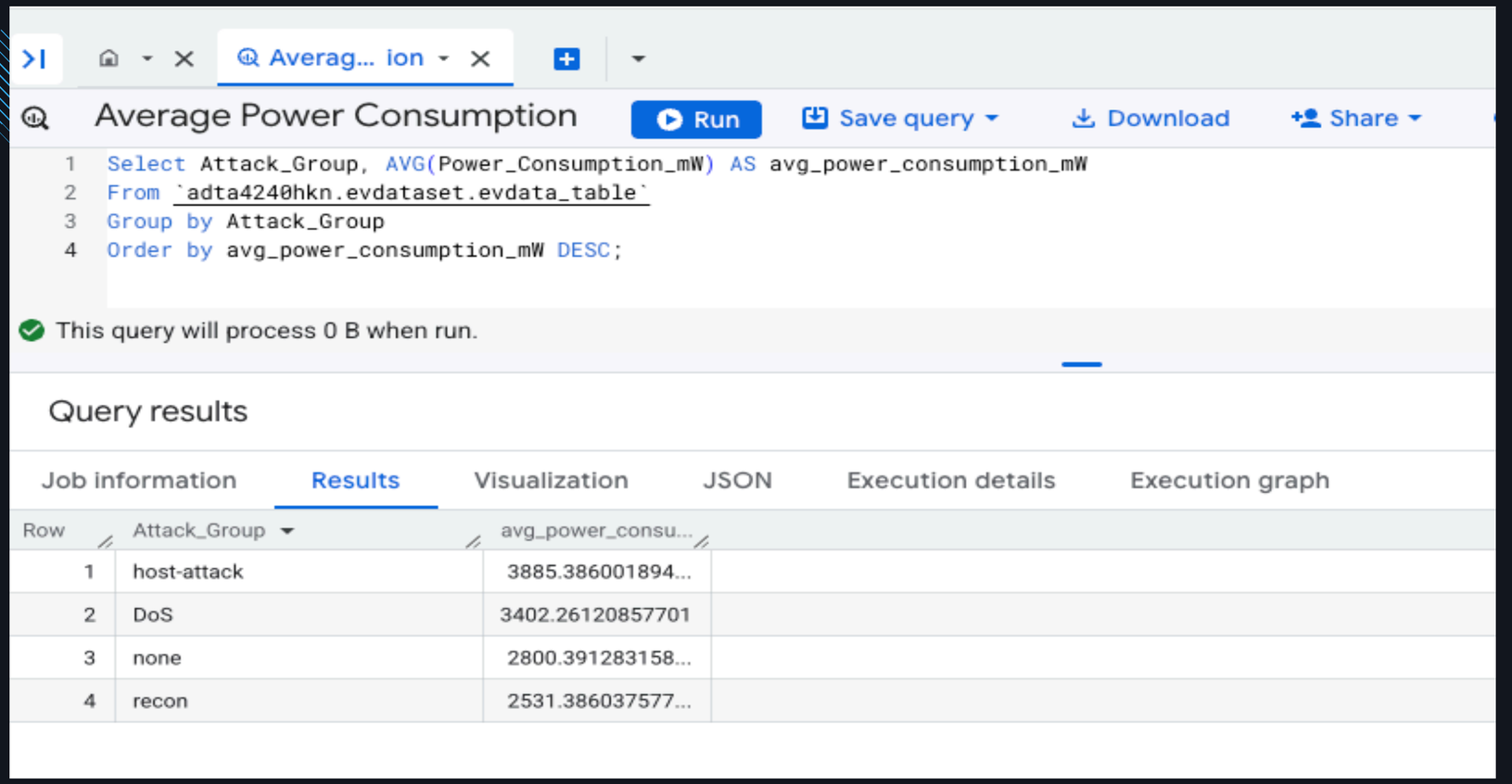
In this query, we are seeing the number of attacks by combination of **Targeted Interface and Attack types**. This helps to identify which communication protocols are more vulnerable to specific attack types. As per the query results, ocpp (Target Interface) and vuln-scan (Attack type) is experiencing more frequent and intensive attack activity

Visualization



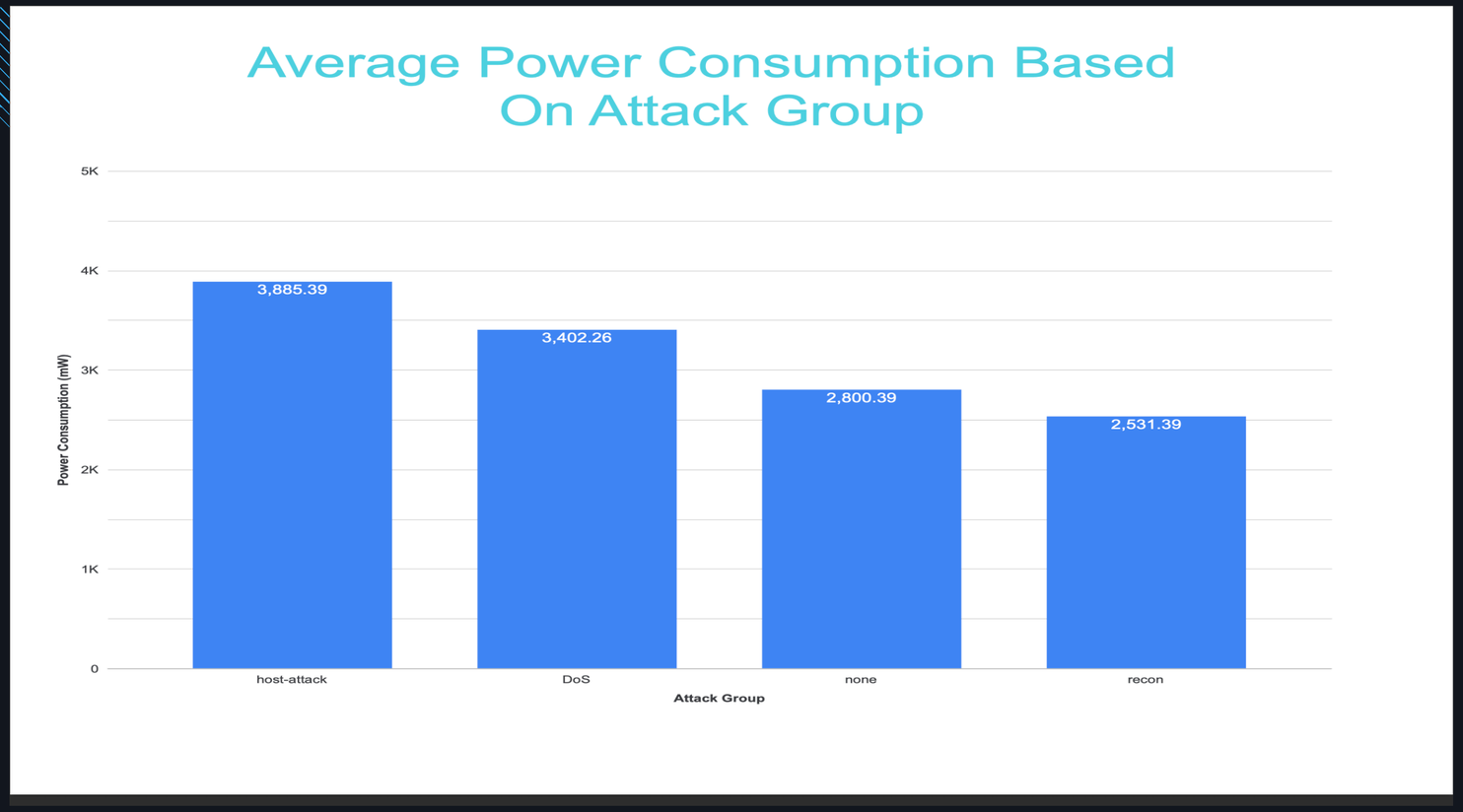
This visualization demonstrates that the vast majority of cyberattacks target the interface labeled "ocpp", Open Charge Point Protocol with 68,202 attacks.

Making Queries in BigQuery



In this query, we are seeing the average current consumption by Attack group. While the average power consumption for host-attack and DoS are almost same, average power consumption for "host-attack" is highest. That means this attack group generates more network traffic and requires more processing power

Visualization



This visualization depicts the average power consumption based on the attack group using a bar graph.

Making Queries in BigQuery

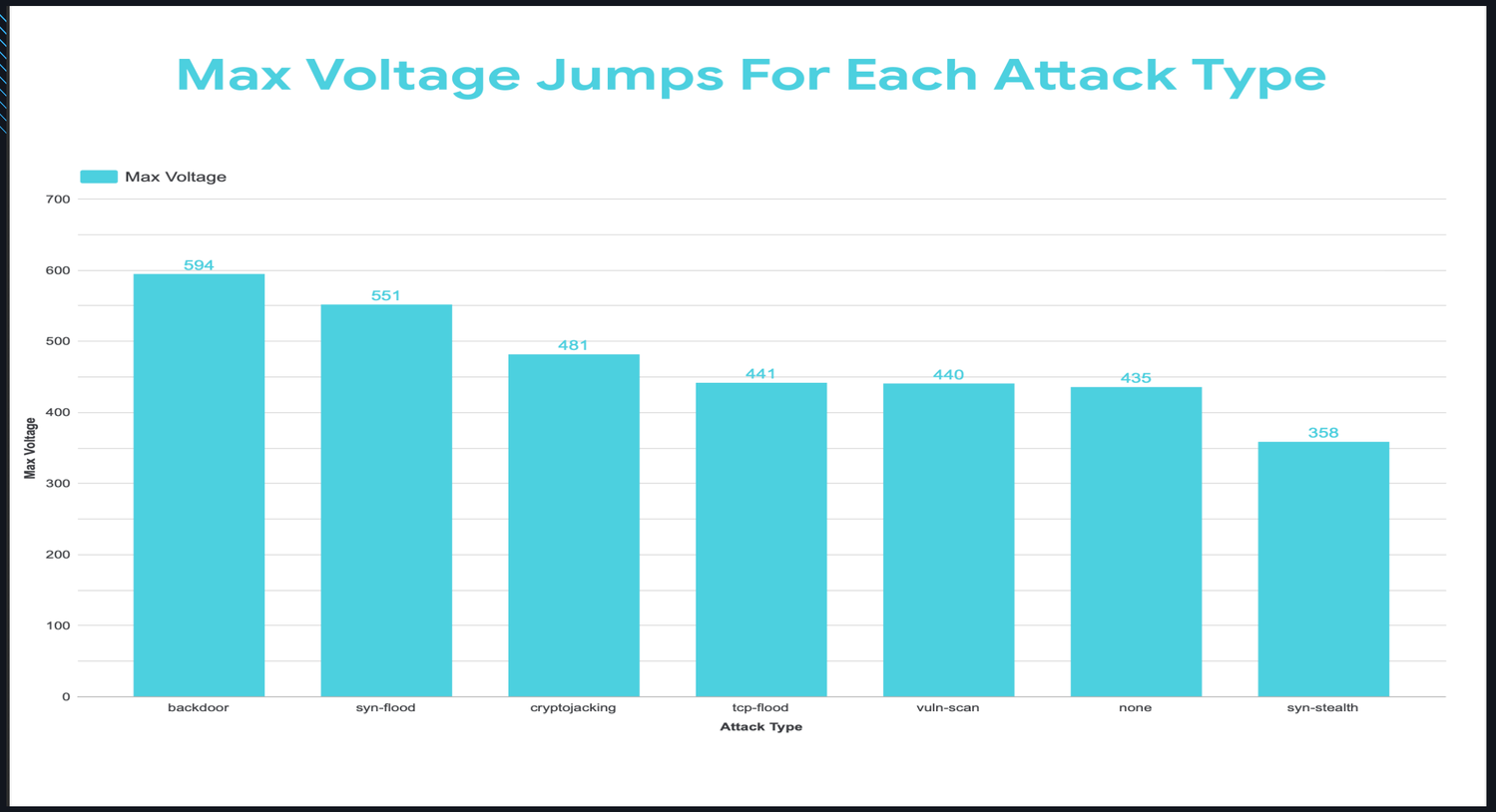
```sql
WITH voltage_differences AS (
  SELECT
    Time,
    Attack,
    shunt_voltage,
    LAG(shunt_voltage) OVER (ORDER BY Time) AS prev_shunt_volt,
    ABS(shunt_voltage - LAG(shunt_voltage) OVER (ORDER BY Time)) AS shunt_volt_diff
  FROM
    nichols2adta.evdataset.evdataset
  WHERE
    Attack IS NOT NULL
)

SELECT
  Attack,
  MAX(shunt_volt_diff) AS max_voltage_jump
FROM
  voltage_differences
GROUP BY
  Attack
ORDER BY
  max_voltage_jump DESC;
```

Job information | **Results** | Visualization | JSON

Row	Attack	max_voltage_jump
1	syn-flood	606
2	Backdoor	594
3	tcp-flood	458
4	none	444
5	vuln-scan	440
6	syn-stealth	358
7	cryptojacking	331

In this query, we are seeing how the shunt voltage, or voltage across a resistor in the battery changes for each type of attack. From the data, we can see the SYN-floods and Backdoor attacks cause the greatest voltage jumps while cryptojacking causes the least amount.

Visualization



This visualization depicts the maximum voltage jump for each attack type using a bar graph.

Making Queries in BigQuery

*Time Ba...sis

Time Based Analysis | Run | Share | Schedule | Open in | More | Save query

```
1
2  SELECT EXTRACT(HOUR FROM Time) AS hour, Attack_Type, SUM(Current_Consumption_mA) AS total_current_consumption
3  FROM `adta4240hkn.evdataset.evdata_table`
4  GROUP BY hour, Attack_Type
5  ORDER BY hour, total_current_consumption DESC;
```

Query completed

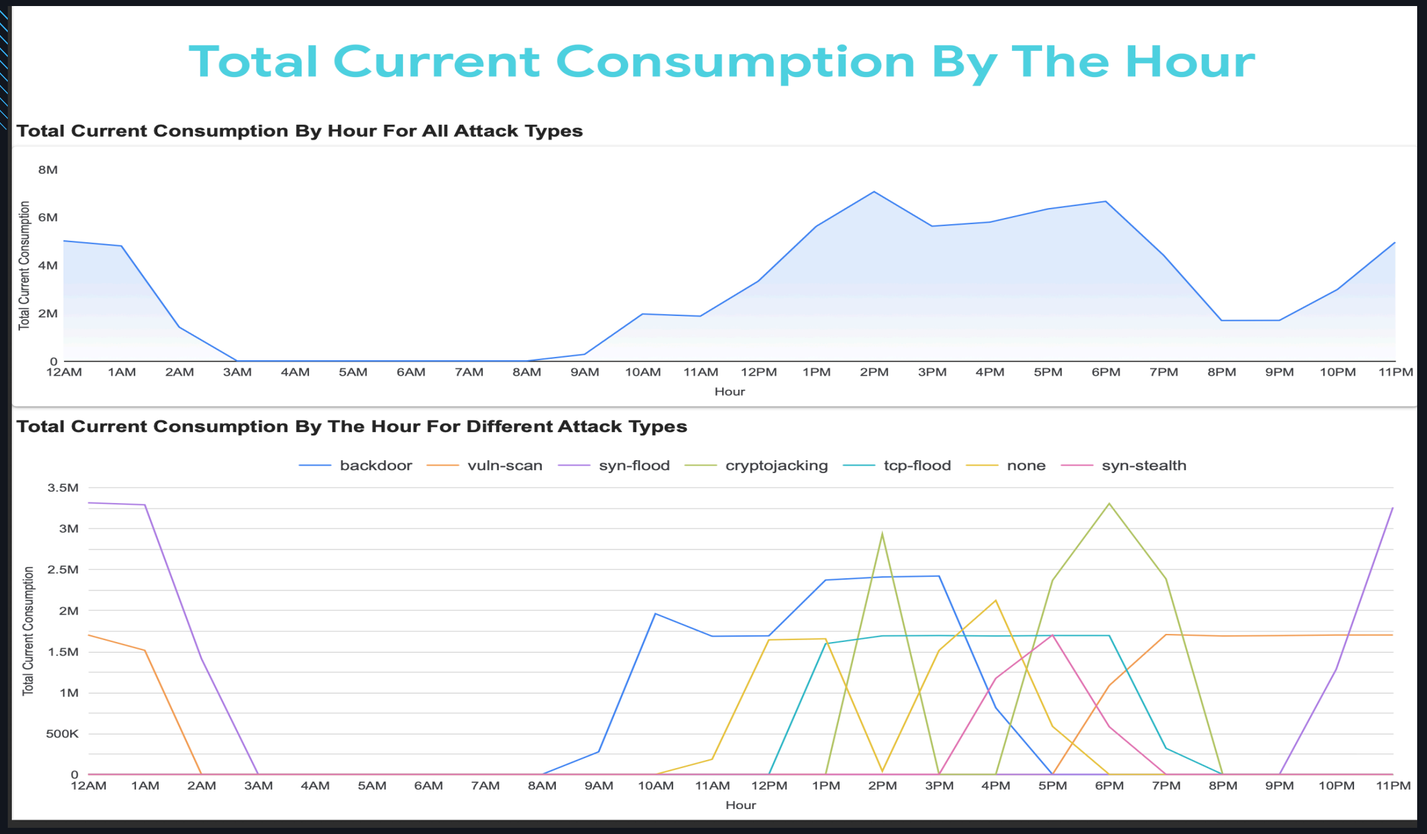
Query results

Job information | Results | Visualization | JSON | Execution details | Execution graph

Row	hour	Attack_Type	total_current_con...
1	0	syn-flood	3310527
2	0	vuln-scan	1699047
3	1	syn-flood	3286161
4	1	vuln-scan	1512240
5	2	syn-flood	1408778
6	9	backdoor	275286
7	10	backdoor	1959114

In this query, we are seeing the total current consumption by hour for each attack type. The current consumption is more at 0th (attach type - syn-flood), 1st (attach type - syn-flood), 18th (attach type - cryptojacking) and 23rd (attach type - syn-flood) hour

Visualization



This visualization depicts the total current consumption by the hour. The top visualization shows the total consumption for all attack types by the hour, while the bottom shows the total current consumption for each attack type by the hour.

Making Queries in BigQuery

Untitled query Run Save Download Share Schedule Open in

```
SELECT
  Time,
  shunt_voltage,
  Attack
FROM
  nichols2adta.evdataset.evdataset
WHERE
  Attack IS NOT NULL
ORDER BY
  Time ASC;
```

Query completed

Query results

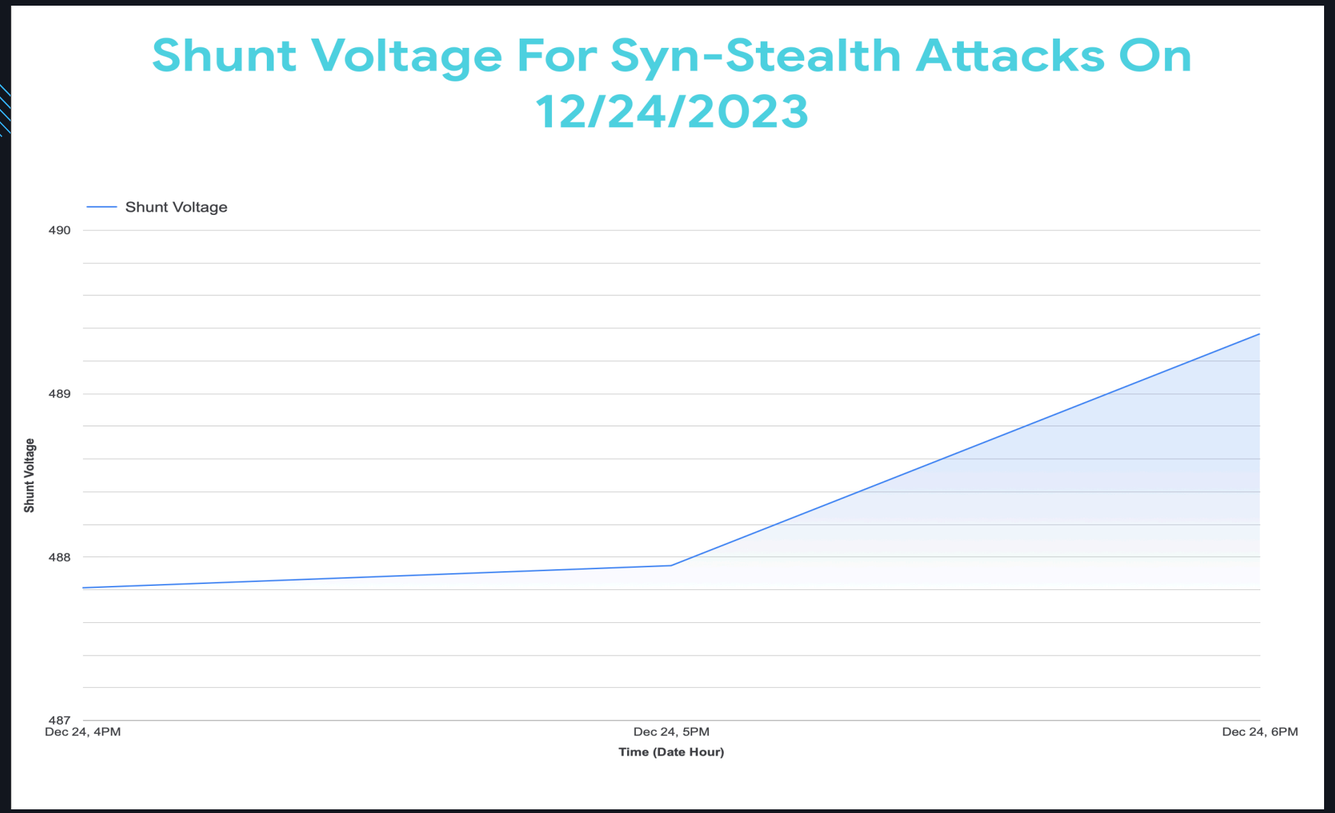
Job information | Results | Visualization | JSON | Execution details | Execution graph

Row	Time	shunt_voltage	Attack
1	2023-12-24 16:18:00 UTC	462	syn-stealth
2	2023-12-24 16:18:00 UTC	465	syn-stealth
3	2023-12-24 16:18:00 UTC	477	syn-stealth
4	2023-12-24 16:18:00 UTC	464	syn-stealth
5	2023-12-24 16:18:00 UTC	484	syn-stealth
6	2023-12-24 16:18:00 UTC	467	syn-stealth

Results per page: 50

In this query, we are seeing how the shunt voltage, or voltage across a resistor in the battery changes during specific cyberattacks during the day. In this example, we are tracking how the voltage changes on 12/24/2023 during a SYN-stealth attack.

Visualization



This visualization depicts the shunt voltage by the hour for Syn-Stealth attacks on 12/24/2023, using a time series area chart.

Making Queries in BigQuery

Untitled query | Run | Save | Download | Share | Schedule | Open in | More

```
1  SELECT State, Attack, COUNT(*) AS event_count
2  FROM nichols2adta.evdataset.evdataset
3  WHERE Label = 'attack'
4  GROUP BY State, Attack;
5
```

Query completed

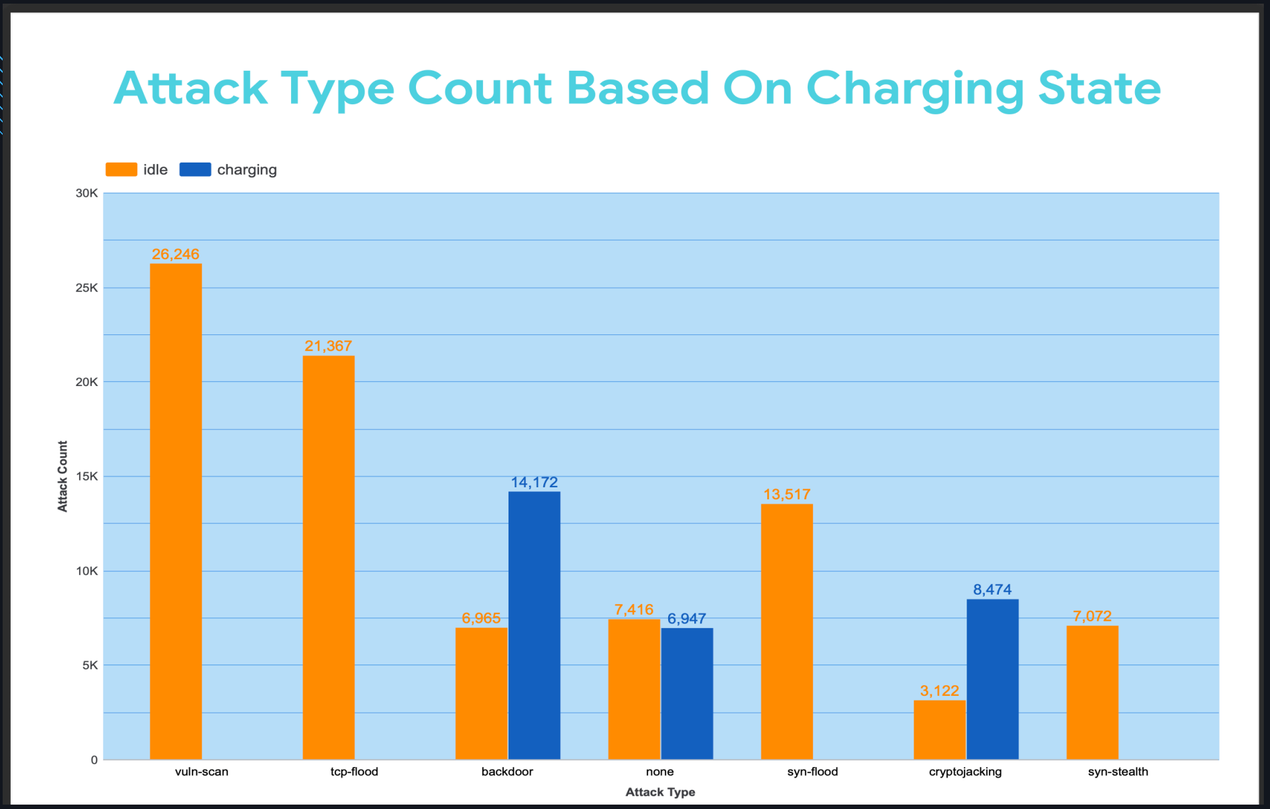
Query results | Save results

Job information | Results | Visualization | JSON | Execution details | Execution graph

Row	State	Attack	event_count
1	idle	syn-flood	13517
2	idle	tcp-flood	21367
3	charging	cryptojacking	8474
4	idle	cryptojacking	3122
5	idle	syn-stealth	7072
6	idle	vuln-scan	26246
7	charging	Backdoor	14172
8	idle	Backdoor	6965

Here, we analyze which types of attack occur during idle or charging states of the EV's. We can see that floods (SYN or TCP), syn-stealth, and vulnerability scans mainly take place during idle states while cryptojacking and backdoor attacks occur in both idle and charging states.

Visualization



This visualization depicts the attack count for each attack type based on charging state using a side-by-side bar chart.

Making Queries in BigQuery

Untitled query | Run | Save | Download | Share | Schedule

```
1  SELECT Attack,
2         AVG(power_mW) AS avg_power,
3         AVG(current_mA) AS avg_current
4  FROM nichols2adta.evdataset.evdataset
5  GROUP BY Attack;
```

Query completed

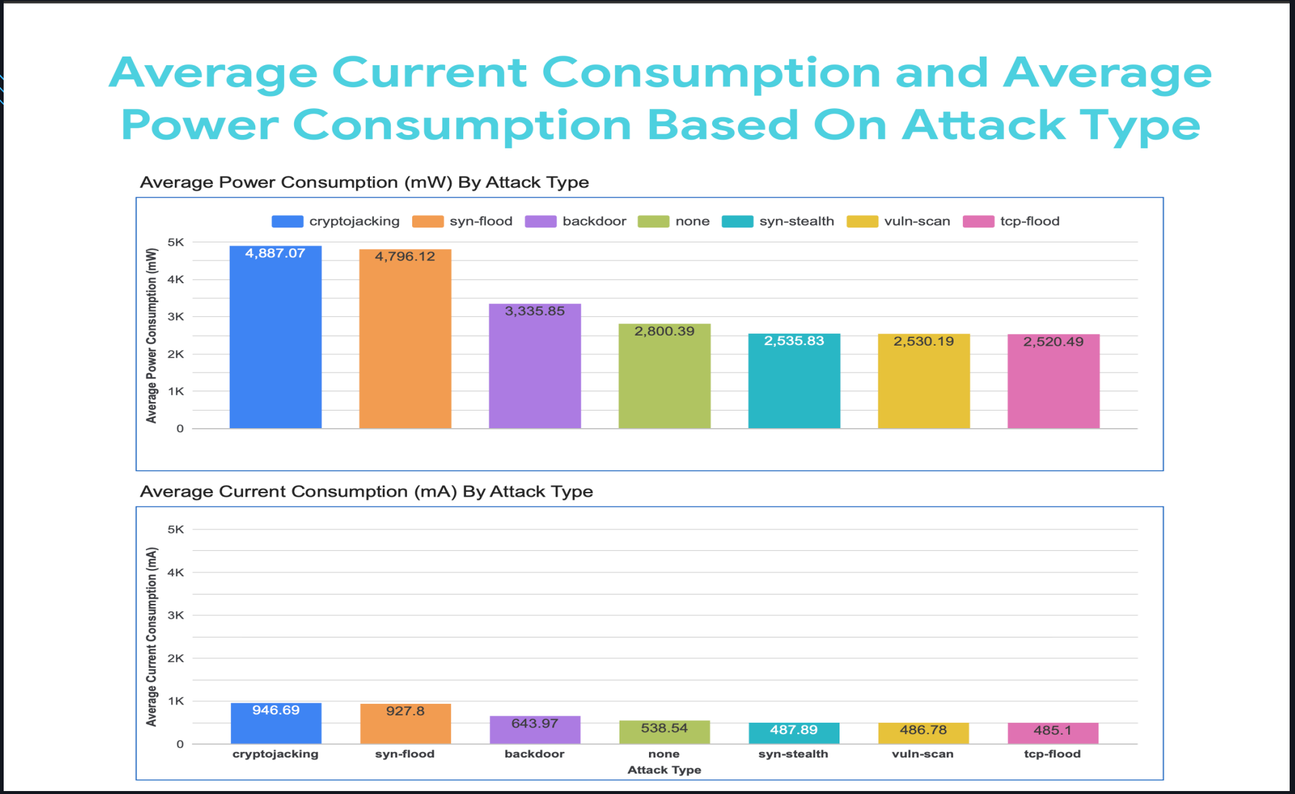
Query results

Job information | Results | Visualization | JSON | Execution details | Execution graph

Row	Attack	avg_power	avg_current
1	syn-flood	4796.124879781...	927.8048383517...
2	tcp-flood	2520.487667899...	485.0988440117...
3	none	2800.391283158...	538.5354034672...
4	cryptojacking	4887.067954467...	946.6892031735...
5	syn-stealth	2535.828619909...	487.8889988687...
6	vuln-scan	2530.188981178...	486.7830907566...
7	Backdoor	3335.851823816...	643.9735534844...

In this query, we are grouping the average battery power usage and current usage during the different types of attacks as well as during normal battery charging. We can see from the image, that SYN-flooding and Cryptojacking tend to cause the greatest surge in battery power and current.

Visualization



This visualization depicts the average current consumption and average power consumption based on the attack type. The bottom bar graph shows the average current consumption (mA), and the top bar graph shows the average power consumption (mW). Each attack type corresponds to the legend at the top with its specific color.

Summary and Recommendations

After analyzing a variety of parameters including but not limited to attack count, average power and current consumption, voltage jumps, current consumed by time of day, etc., our team determined the most impactful factors on which to base our recommendation are the attack count and average power consumption. We extrapolated these two parameters to determine which attacks consumed the most unnecessary power during the experiment, and thus, likely consume the most power (and money) in real-world scenarios. We recommend Lucid Motors allocate resources to prioritize the mitigation of these attacks first, as they have the greatest impact on the company's bottom line.

Total Observed Power Consumed During Experiment (most critical attacks):

1. Backdoor – 70.936 kW
2. SYN-Flood – 64.828 kW
3. Cryptojacking – 56.438 kW

LEAST CONCERN: SYN-Stealth, Vuln-Scan, and TCP-Flood (these three attack types surprisingly induced systems to consume LESS power than the control)

TEAM MEMBERS & ROLES

Alex Clemovitz – Locate Dataset, Define Problem Statement, Prepare Data with OpenRefine, Summarize Recommendations

Chris Nichols – Create BigQuery Queries and Document in Google Docs, Research and Summary of Attack Types

Diana Amaya Nino – Research Company/Scenario, Notate Team Meetings, Submit Project for Grading

Isagani Hernandez – Assist with Queries, Create Visualizations of Notable Queries

~~**Harish Kumar Nalumas –**~~ Create BigQuery Queries, and Visualizations of Notable Queries

References

Buedi, E. D., Ghorbani, A. A., Dadkhah, S., & Ferreira, R. (2024). CIC EV charger attack dataset 2024 (CICEVSE2024) [Data set]. Canadian Institute for Cybersecurity (UNB). https://www.unb.ca/cic/datasets/evse-dataset-2024.html

GeeksforGeeks. (2025, September 13). *SQL WITH clause*. GeeksforGeeks. https://www.geeksforgeeks.org/sql/sql-with-clause/

Law, R. (2024, November 4). *Securing Singapore's Electric Vehicle Future: Addressing the Cybersecurity Challenges of EV Infrastructure*. Cyber Security Asean; Cyber Security Asia. https://cybersecurityasia.net/securing-sg-ev-cyber-security-challenges/

Murach, J. (2019). *Murach's MySQL* (3rd ed.). Mike Murach & Associates.

Salahuddin, I. (2024, July 5). *Understanding the LAG() Function in SQL: A Comprehensive Guide*. DataCamp. https://www.datacamp.com/tutorial/sql-lag

Sayegh, E. (2024, March 12). *Is Cybersecurity The Achilles' Heel Of The Electric Vehicle Revolution?* Forbes. https://www.forbes.com/sites/emilsayegh/2024/03/12/is-cybersecurity-the-achilles-heel-of-the-electric-vehicle-revolution/

THANK YOU

...