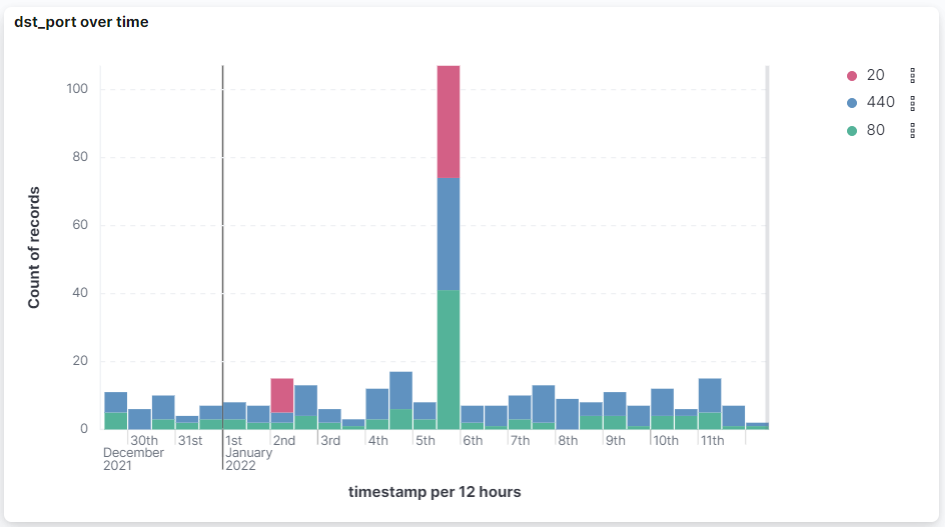
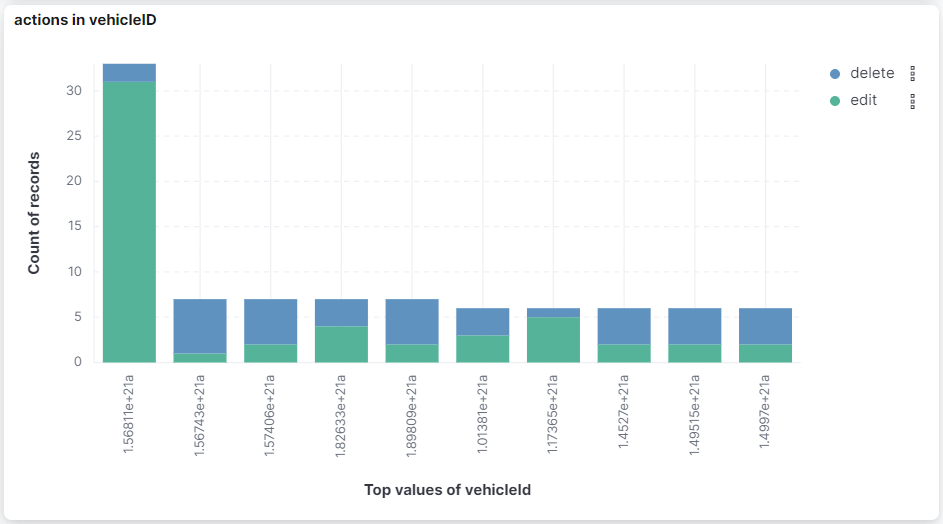
**Cymotive**Vehicle Num. 1.56811e+21

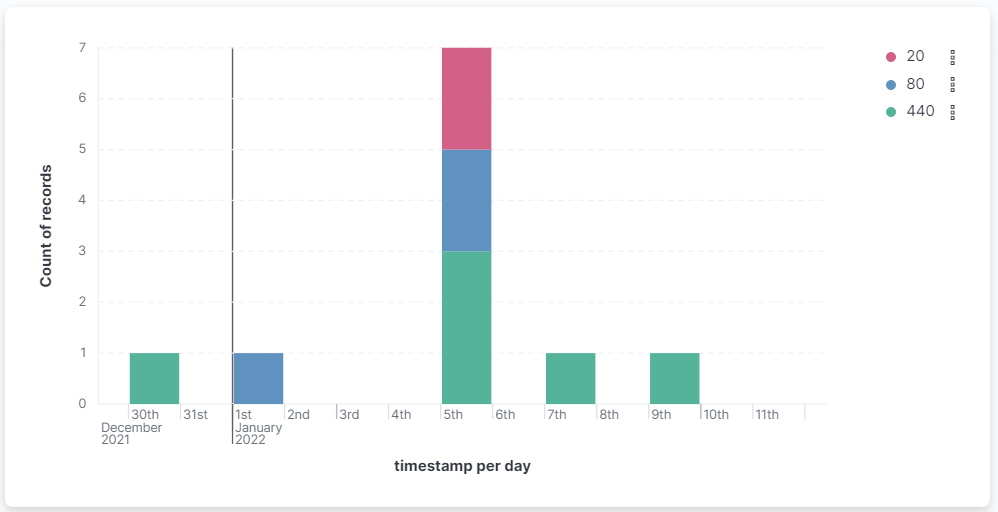
* The start was to see if there any anomaly behavior during the time,  
  founded two days that have records from unusual port, that also not secure.



* Also, start to search anomaly behavior in the files, filtered (by delete and edit) to see if there any vehicle that have a lot of changes.  
  found that 1.56811e+21 have very high number of changes.

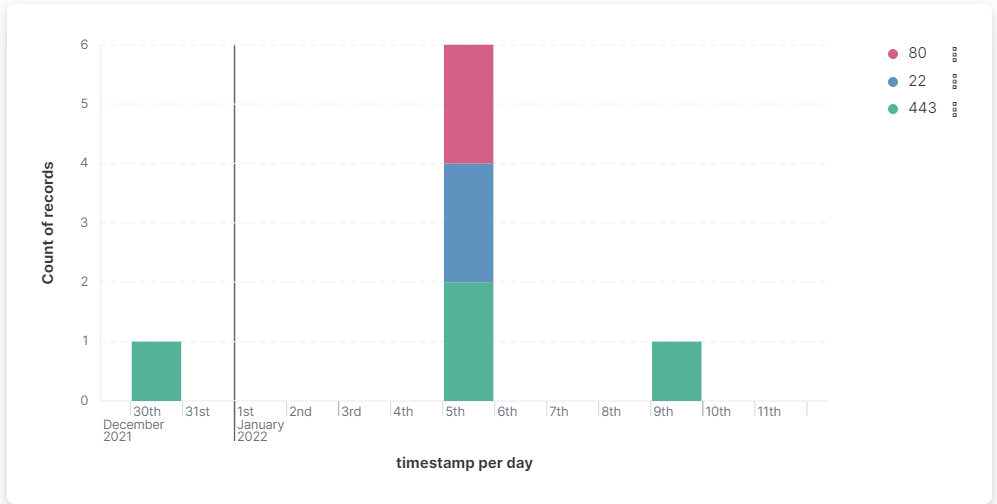


* Filtered the timeline by the suspicious vehicle.  
  The records are quiet except Jan 5, that have 7 records.

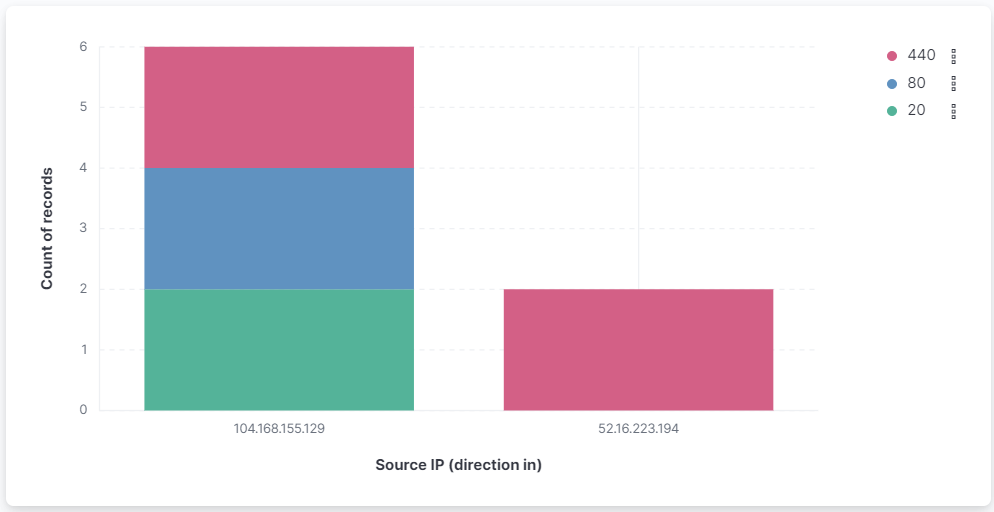


FireWall event in 1.56811e+21

* When we filter the result for only incoming records, we can still see that Jan 5 have strange behavior.



* Not all the records from the Jan 5 are secure, as they use in port 80 (HTTP) and 22 (SSH).
* We check which IPs use in which ports,  
  and inform that attack's IP is 104.168.155.129, because only this IP have use unsecure ports, and those ports also used in Jan 5.

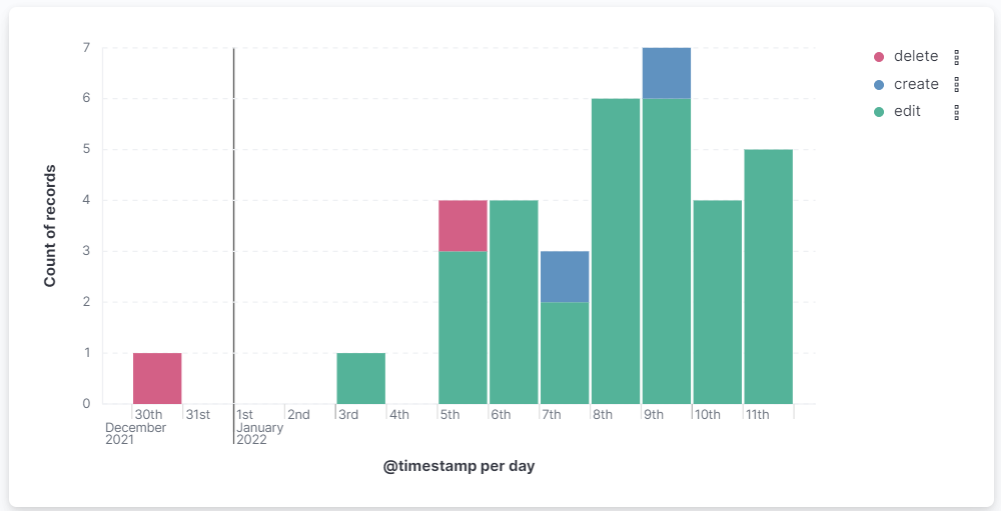


* After we know the IP of the attacker, we can see that the user is Scar67.  
  [this user has security breach only to one vehicle.]

תמונה שמכילה ריבוע

התיאור נוצר באופן אוטומטי

* We check which actions have happened in the Jan 5,  
  found only Delete and Edit.



**All the action from Jan 5:**

* At first, the SSL has changed, what allow for the hacker to do stuff.
* After that, he changes the file that control the brake's pressure.
* He's next step is to edit the pm\_async[[1]](#footnote-1) file and send more brakes orders.
* Finally, namespace.conf[[2]](#footnote-2) deleted to Blurring traces.

|  |  |  |  |
| --- | --- | --- | --- |
| **action** | **filePath** | **@timestamp** | **vehicleId** |
| delete | /etc/security/namespace.conf | Jan 5, 2022 @ 22:03:53.078 | 1.56811e+21a |
| edit | /sys/power/pm\_async | Jan 5, 2022 @ 18:10:22.201 | 1.56811e+21a |
| edit | /sys/module/vmpressure | Jan 5, 2022 @ 10:57:53.955 | 1.56811e+21a |
| edit | /etc/ssl/certs | Jan 5, 2022 @ 09:41:52.167 | 1.56811e+21a |

**The Deleted actions over time.**

* It's possible that deleting FW file without updating it – cause to this security breach.

|  |  |  |  |
| --- | --- | --- | --- |
| **action** | **filePath** | **@timestamp** | **vehicleId** |
| delete | /etc/security/namespace.conf | Jan 5, 2022 @ 22:03:53.078 | 1.56811e+21a |
| delete | /lib/firmware/DWC\_ETH\_QOS\_fw.bin | Dec 30, 2021 @ 02:20:21.843 | 1.56811e+21a |

**When we got the information from the vehicle itself, we learned couple things:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **8713** | 20.145305 | CANFD | 6 | Tx | msg5 | 26 | 5a | 1 | 44 | c0 | 80 | 17 | c1 |

* On timestamp 20.145305 – the airbag starts to open.  
  Apparently it was at the time of the accident.
* Before the accident, the steering wheel changed direction drastically.  
  Which can indicate remote control of the steering wheel.



* Also, sometimes we can see that even when the brake was used (with high pressure), the vehicle still has growth his speed.  
  Which can indicate remote control of the gas pedal.



* After more digging, we found that **the attack starts at Jan 5, 2022 @ 18:10:22.201** [or 16.907468 in the TRACE].

**The conclusion:**

Almost in all types of 'Massage', the 'B2' value is ordered by the time, the common one is from 1 to 0f (16 in decimal).

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16.868002 | CANFD | 2 | Tx | msg3 | a0 | 2 | 7 | 2 | 0 | 3 | 14 | 64 |
| 16.887467 | CANFD | 2 | Tx | msg3 | 86 | 3 | 7 | 2 | 0 | 8 | 14 | 64 |
| 16.907468 | CANFD | 2 | Tx | msg3 | 8a | 4 | 27 | 2 | 0 | 0d | 14 | 64 |
| 16.907469 | CANFD | 2 | Tx | msg3 | 8a | 4 | 27 | 2 | 0 | 1 | 14 | 64 |
| 16.92761 | CANFD | 2 | Tx | msg3 | 90 | 5 | 27 | 2 | 0 | 14 | 1b | 64 |
| 16.947778 | CANFD | 2 | Tx | msg3 | ee | 6 | 27 | 2 | 0 | 1a | 1d | 64 |

At 16.907469 we start to see anomaly, and number 4 was duplicate.  
and after more and more duplicate rows.

After 1-2 seconds, the steering wheel start to change his direction frequently from left to right.

As we know, before the 'async' edited, the 'vmpressure' file was edited.

**The cause for the accident can be:**

1. The brakes are not active enough pressure, so the vehicle keep going,  
   the driver sew that he can't slow with the brakes, so he tried to slow down by moving the vehicle from side to side.
2. The brakes are activated suddenly (by the hacker), so its cause to the vehicle to slip on the road,  
   so the driver tried to stable it using the steering wheel.

The second option is making more sense, as the brakes work by mechanics (so the driver control the pressure himself), but this can be different in each vehicle.

1. The /sys/power/pm\_async file controls the switch allowing the

   user space to enable or disable asynchronous suspend and resume

   of devices. If enabled, this feature will cause some device

   drivers' suspend and resume callbacks to be executed in parallel with each other and with the main suspend thread. It is enabled if this file contains "1", which is the default. It may be disabled by writing "0" to this file, in which case all devices will be suspended and resumed synchronously [↑](#footnote-ref-1)
2. <https://man7.org/linux/man-pages/man5/namespace.conf.5.html> [↑](#footnote-ref-2)