Detected in 2018, a biggest cyber attack after Yahoo happened which we called the Marriott hotel attack. What is blunderous about this is that it took almost 2 year to be detected. If we talk about technological advancement in mankind where everything happens in second like if we try to open a website and if took delay of minutes in open than we will not see that webpage, but here its not about minutes but a couple of years that a database clusters infected with virus remain undetected in the machine for 2 years.

Now, I think we understand the impact of the attack. Lets see the incident in detail, as we all know that a few years back there was a big chain of hotels called as starwood hotel and in 2016 another big hotel called as Marriot acquired this hotel. As we all know that acquiring means all the assets of starwood will come under marriott including the information system which includes a database of their customers and this leads to the center of malicious threat into the marriott hotel database. So, in terms of dates hackers hacked the starwood hotel database in 2014 and until 2016 it remained undetected in starwood hotel system after this marriott acquired it and then it remained with this global leading chain for 2 years till 2018 when accenture who is maintaining the database detected it. By using the IBM Cardiom Database solution Data engineers of Accenture find that an unusual SQL query was processed before a few days of detection.

Although Marriott detected the malicious activity and hacking of their database by the hackers, it was delayed by a big fraction of time. What they are able to find is Guest payment card information, guests general records and passport numbers got breached. Among this almost 9.1million encrypted payment card number, expiration dates out of which 385000 cards are working at time of breach, 385 million general records including general details such as full names, mailing address, phone number, email address, general address, rewards information, arrival/departure information and passport numbers of 5.25million unencrypted out of 18.5 million encrypted got breached by alleged Chainese Hackers Group. Out of 339 million records 30 million records are of EU personnel and 7 million are of UK citizens.

As a consequence of this. ICO information commissioner office United Kingdom fined Marriott hotel by a charge of infringement of gdpr regulation and with a 99.2 million pound fine. As per ICO marriott didn't do their due diligence carefully and not taken precaution. As per Infringement gdpr fines will be equal to 4% global turnover 20 million pound whichever highest and Marriott Hotel turnover is approx 14 billion and 618 million pound. Thus, as per law Marriott was fined 99.2 million pound.

Taking this into consideration this global hotel chain started a thorough investigation by calling 3 party investigators to find scope of breach. They took into consideration logs deleted by hackers. Endpoint protection solutions are implemented from 17 thousand all the way to 200thousands. Also, they whitelisted the internal database IP address and performed network segmentation to protect sensitivity of data.

Best thing happened about this incident is that Marriott hotel has insured with the cyber insurance which means that they got big part of 3 months loss from initial discovery till the end which is about 524624800million pounds out of which they receive 51893900 as insured amount and they have to pay 731000 pound from their pocket in addition to 99.2 million pound.