2012 – LinkedIn Data Breach

More than 100 Million of data stolen

How the attack has happened

Step 1 – Some social engineering

Attackers very brilliantly searched for LinkedIn employees with title including “SRE” and “DevOps” in LinkedIn.

This lead attacker to understand the technologies used in LinkedIn, as well as determining the technology to attack to target just by examining the tech employees ‘ profiles working for LinkedIn.

Step 2 – Finding a hole

The attacker found that there is a website with vulnerability which is hosted by an employee on employee’s own iMac and used this website to get into the computer and found the key to get into LinkedIn servers using employee’s VPN, and SSH credentials gathered by a brute force.

Step 3 – Cracking The Passwords

Once the attacker is in, and he has been there for 3 months, he was looking ways to crack passwords until he found a way before LinkedIn found him.

This has lead more than 6.5 Million of account data to be stolen with the hack happened on June 5, 2012. But in 2016 LinkedIn realized the worst truth : Stolen data was 100 Millon+.

Tracing the hacker

LinkedIn has found a way to trace the hacker, ie: They found multiple logins with the key of the employee from Russia, but that employee was never been there.

Then they have found the IP addresses and realized an unusual user-agent header in the requests.

By the help of FBI, tracing messages and e-mail data they finally caught their guy on vacation in Czechia.

How ALISA could help?

ALISA can understand if there is a deviation or anomaly in every single header and every single query stiring like user-agent.

The attacker used “Sputnik” in custom user-agent header. Since ALISA had never seen something like “Sputnik” or containing “Sputnik”, she would directly warn the admins with generating rules to prevent attack in web application firewalls.