**Darknet diaries Ep**

Evaldas Rimašauskas, inspired by Facebook's acquisition of Instagram for $1 billion, became interested in finding ways to make more money through illegal means. He and his friends devised a plan to steal money from Facebook and other companies. They started by obtaining crucial information from Facebook's finance department through fake customer service complaints, emails, and social engineering techniques.

Once they learned about Facebook's business partners, they targeted a company called Quanta Computer, which Facebook did business with. Evaldas posed as Quanta Computer and issued fake invoices to Facebook, redirecting payments to his own accounts. To make the scheme look legitimate, he created fake companies in Latvia and Cyprus with the same name as Quanta Computer. This allowed them to receive substantial amounts of money from Facebook over a two-year period.

Later, they discovered that Quanta Computer also worked with Google and replicated the same fraudulent scheme, receiving more money. However, their scheme eventually came to an end when the real Quanta Computer started demanding payment for their legitimate work. Authorities launched investigations, and it was discovered that the fake domains used by Evaldas were linked to his personal email. This information led to his identification and capture by law enforcement.

**3.2 Intrusion Kill Chain**

A kill chain is a organised process for engaging an adversary to achieve specific goals. In cybersecurity, the intrusion kill chain outlines the different stages attackers go through to breach into an environment:

* Reconnaissance: Research and target selection.
* Weaponization: Combining malware with exploits.
* Delivery: Transmitting malicious content.
* Exploitation: starting malicious code.
* Installation: Establishing a presence.
* Command and Control: Creating a communication channel.
* Actions on Objectives: Achieving the attacker's objectives.

**Defence**

The intrusion kill chain model is a practical tool in cybersecurity for defenders to analyse and take necessary measures to cyber threats. It involves evaluating the effectiveness of security measures at each stage of an attack, identifying vulnerabilities, and taking necessary defensive actions. The course of action process describes how defenders can respond to different phases of an attack, using various tools and techniques. In essence, the intrusion kill chain model enables defenders to align their security efforts with attacker actions, strengthening overall cybersecurity resilience.