Course material

Course:

Understanding the digital supply chain and its stakes for humanitarian actors

Video:

1.3.3 Case Study n1 - Eyes go Blind

Concepts (extracted from automatically generated subtitles):

Concrete case studies. Critical infrastructure. First case study. Heads up. Case studies. Radar systems. Supply chain. First point. Shelf microprocessors. Single points of failure. Backdoor access. Incoming missiles. Alice. Alice's nuclear facilities. Mallory.

to video sequence search
(within Understanding the digital supply chain and its stakes for humanitarian actors.)

to video

Hardware Supply Chain Case Study 1 Eyes go Blind

Shweta Shinde
Assistant Professor
Secure & Trustworthy Systems Group
ETH Zurich

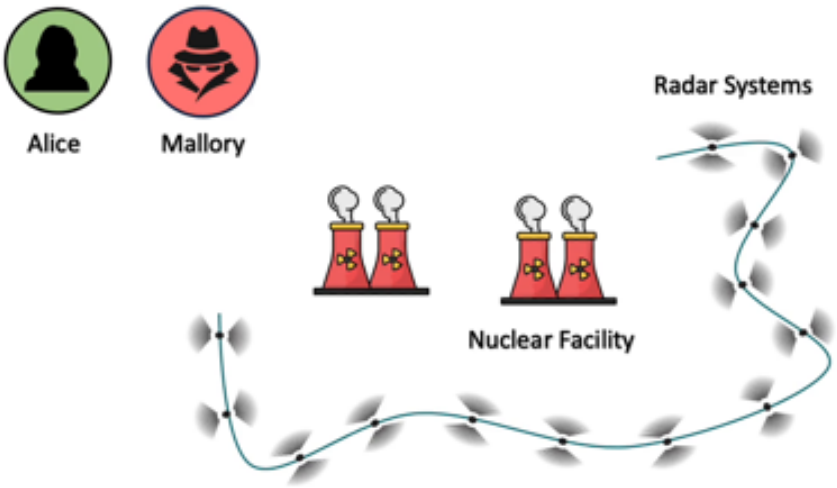
...

notes

summary

0m 0s

Case n°1: Eyes go Blind



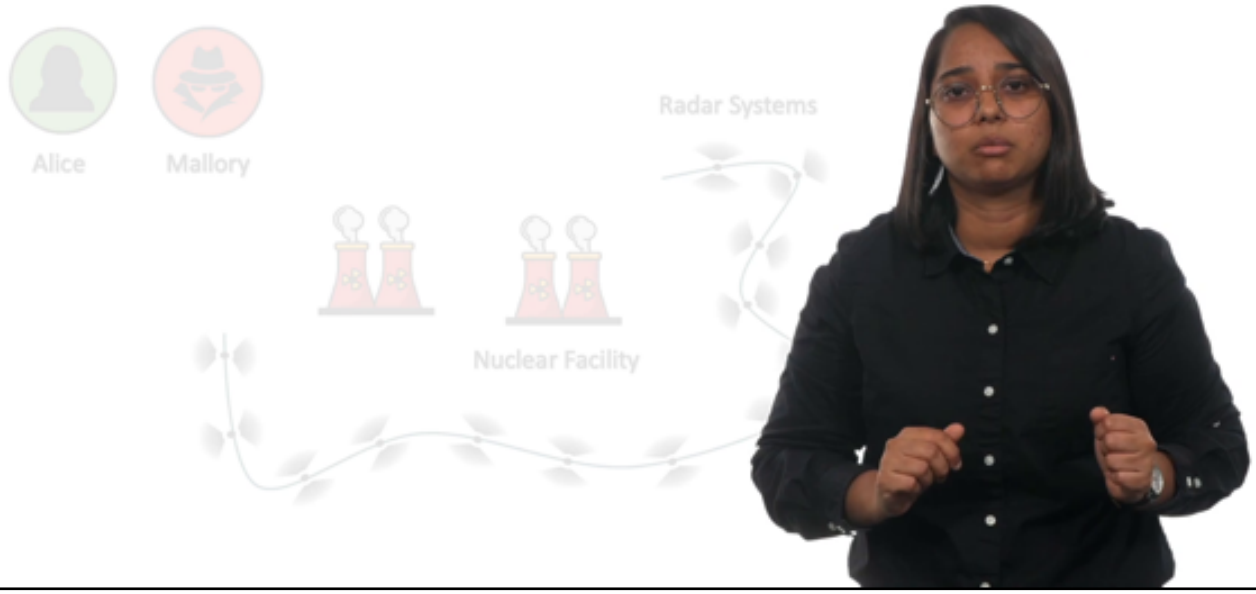
So far we have looked at the stakeholders and threats in the supply chain. Now, it is time to get into some concrete case studies that showcase what we have learned so far and put it to use. The goal is to understand the scenario, analyse the gaps, and then learn from these examples. We will look at three case studies or more like fictional stories, complete with victims and attackers and even James Bond-esque gadgets. Heads up, I do not have a military or defence background, so bear with me and my espionage storytelling skills. I call the first case study, Eyes Go Blind. Imagine a victim. Let's call her Alice. Alice has a nuclear facility and wants to protect it. She has deployed radars to detect incoming missiles and notify her, so then she can do counterattacks to neutralise the missiles before they hit the nuclear facility. On the other side, we have our attacker. Let's call her Mallory. Mallory wants to launch missiles, raid and destroy Alice's nuclear facilities. But Mallory doesn't want to get caught doing this, for reasons, so she must evade detection.

notes

summary

0m 2s

Case n°1: Eyes go Blind



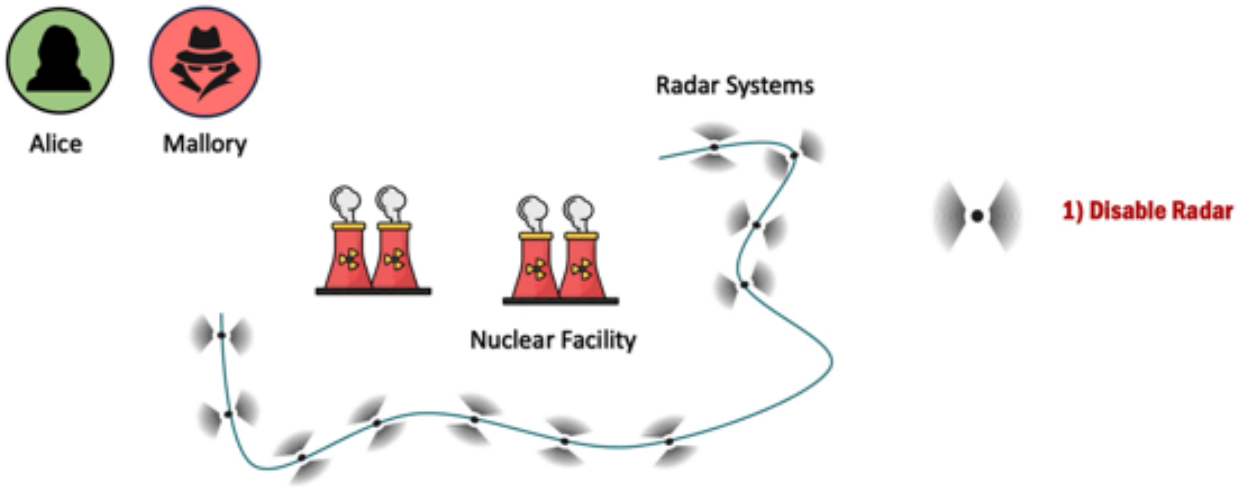
Now, remember, Alice has radars for this. Unfortunately for Alice, one night, her nuclear facility is struck by missiles. Somehow, her radars failed to detect them. But how? As it turns out, Alice was using off the shelf microprocessors in her radar systems,

notes

summary

1m 25s

Case n°1: Eyes go Blind



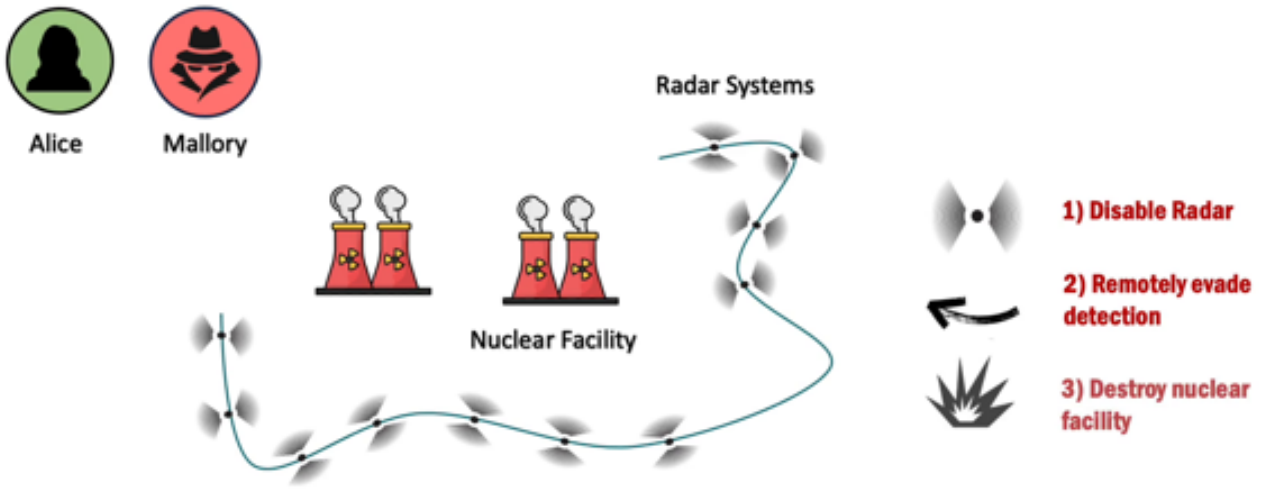
and it just so happens that Mallory had backdoor access to these particular off the shelf microprocessors. All Mallory had to do was use the backdoor

notes

summary

1m 49s

Case n°1: Eyes go Blind



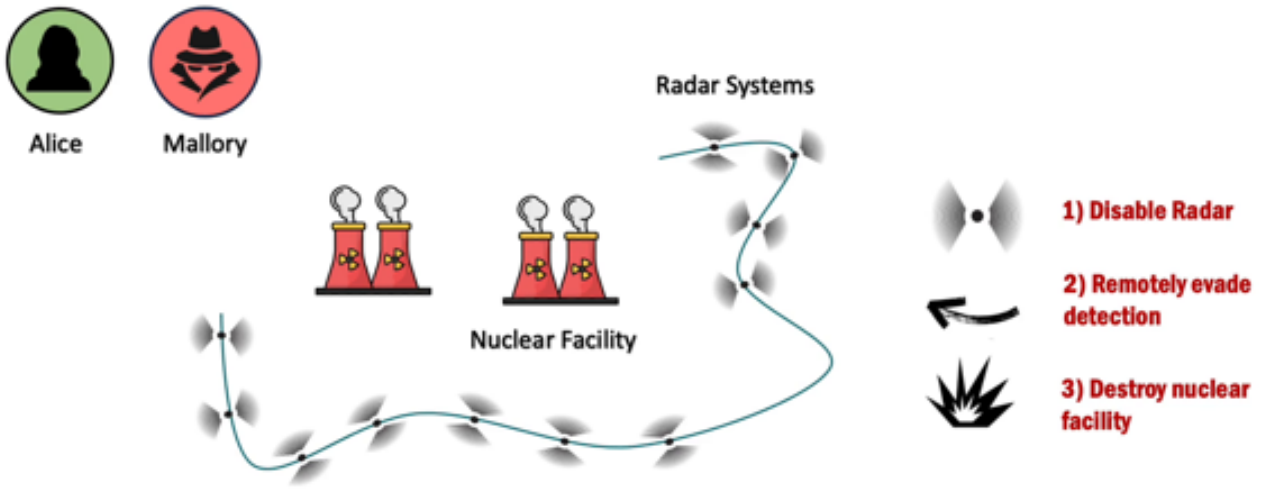
to disable the radars with a kill switch just before she launched the raid. Now, this way, Mallory was able to remotely evade detection and succeed in her mission

notes

summary

2m 1s

Case n°1: Eyes go Blind

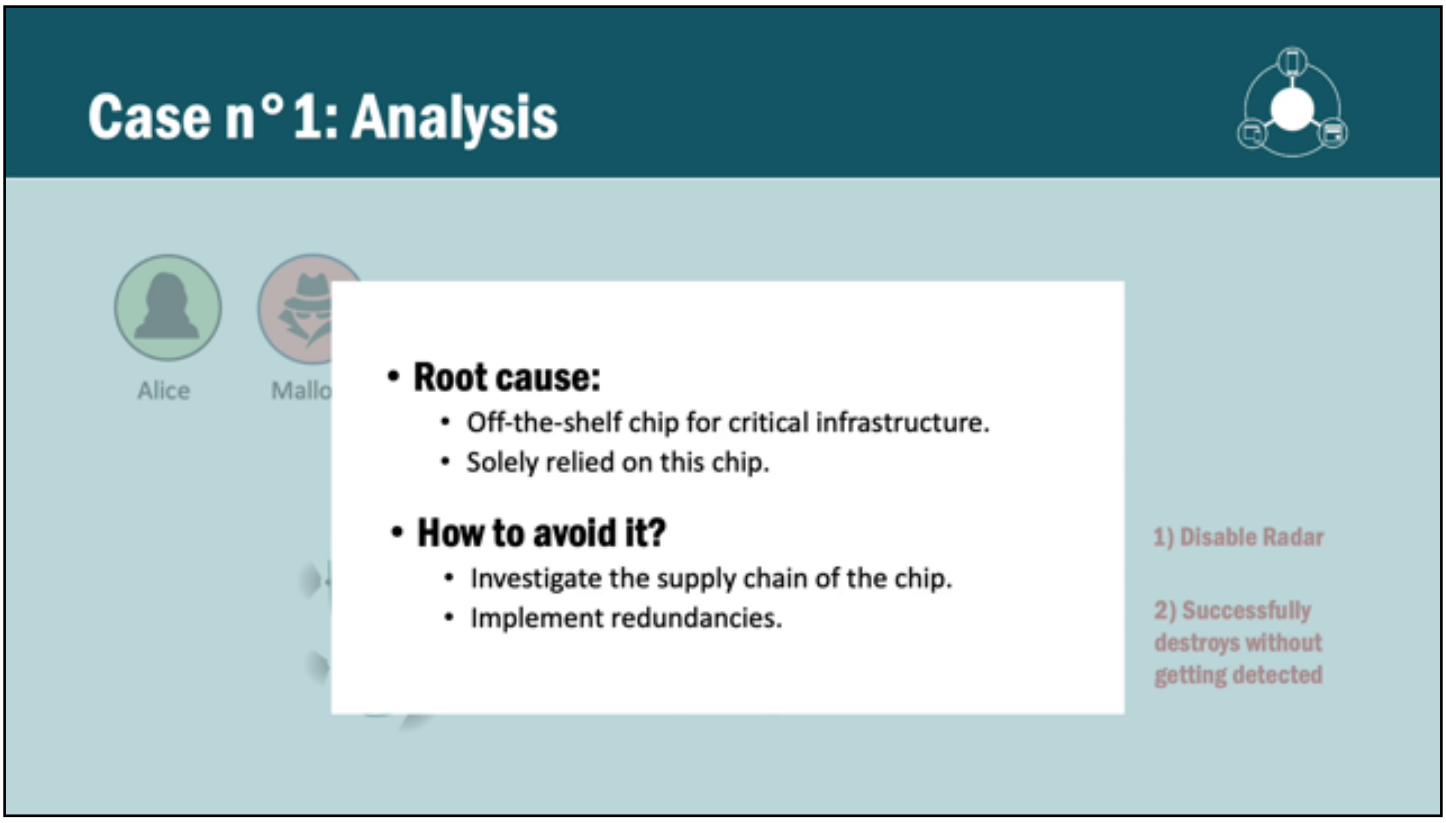


to ultimately destroy Alice's nuclear facility.

notes

summary

2m 12s

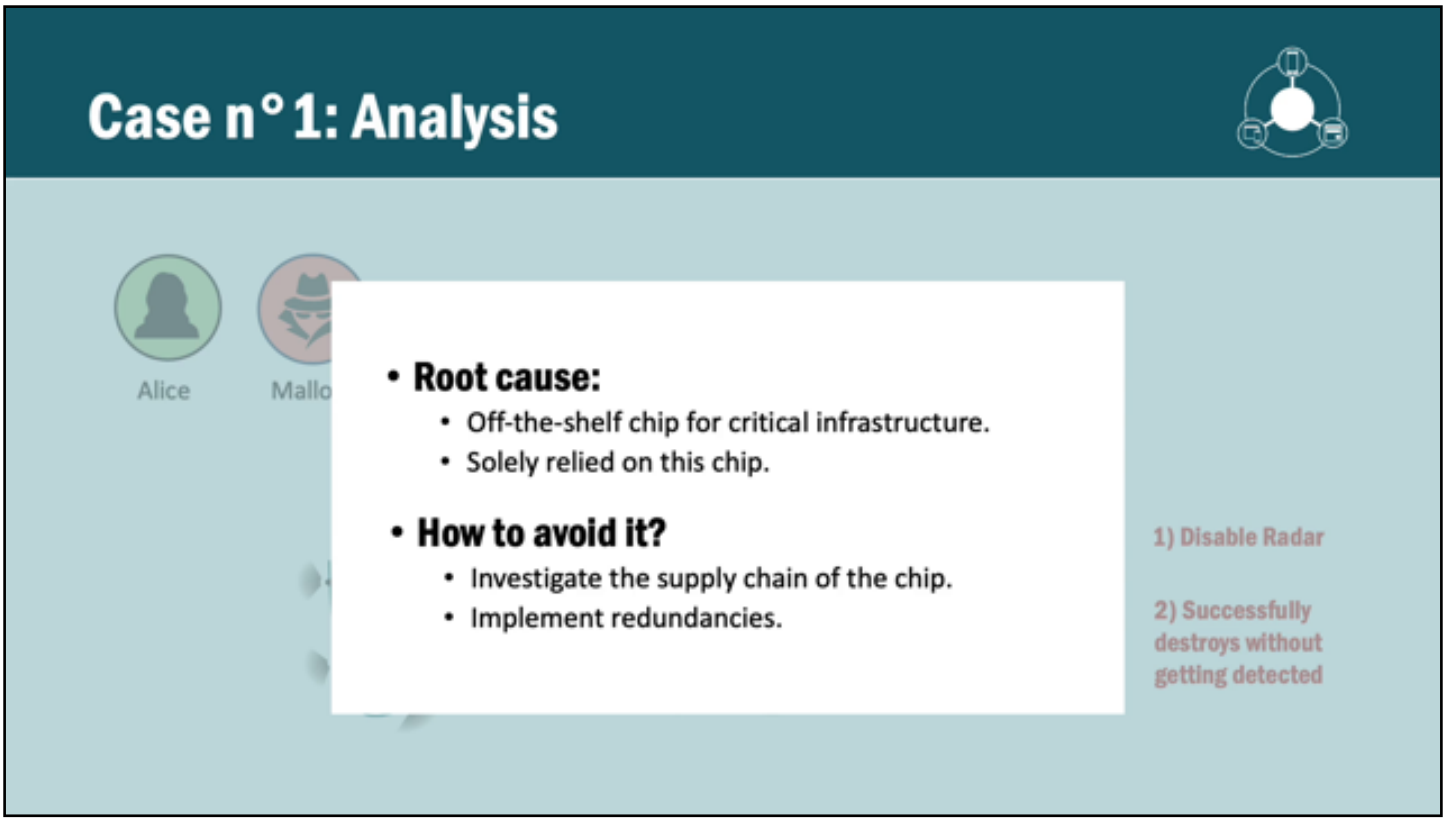


Now, what can we learn from the tale of Alice and Mallory? First point to note,

notes

summary

2m 13s

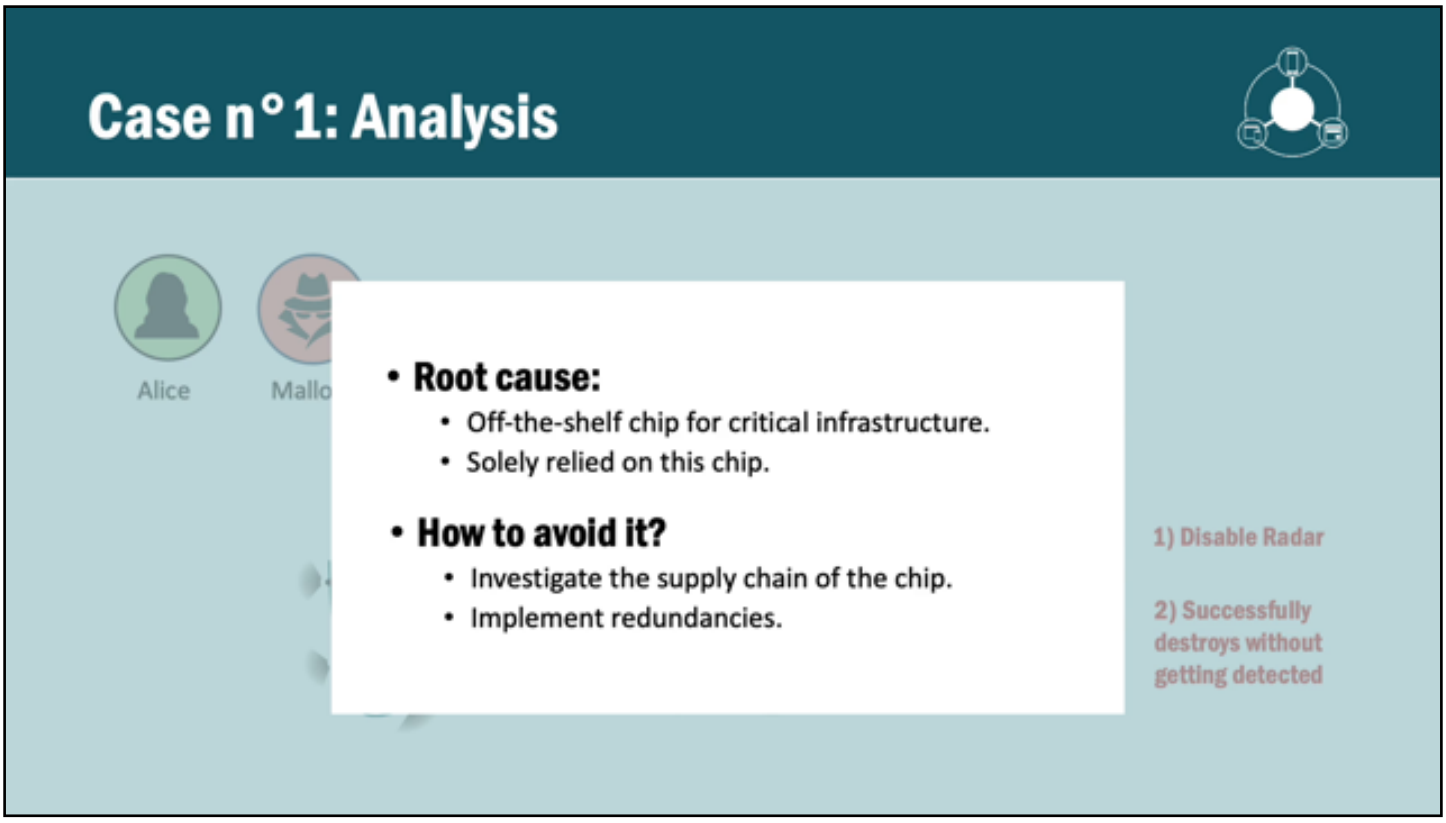


Alice used an off the shelf chip for critical infrastructure. Next, she solely relied on this chip. What could have Alice done instead?

notes

summary

2m 26s

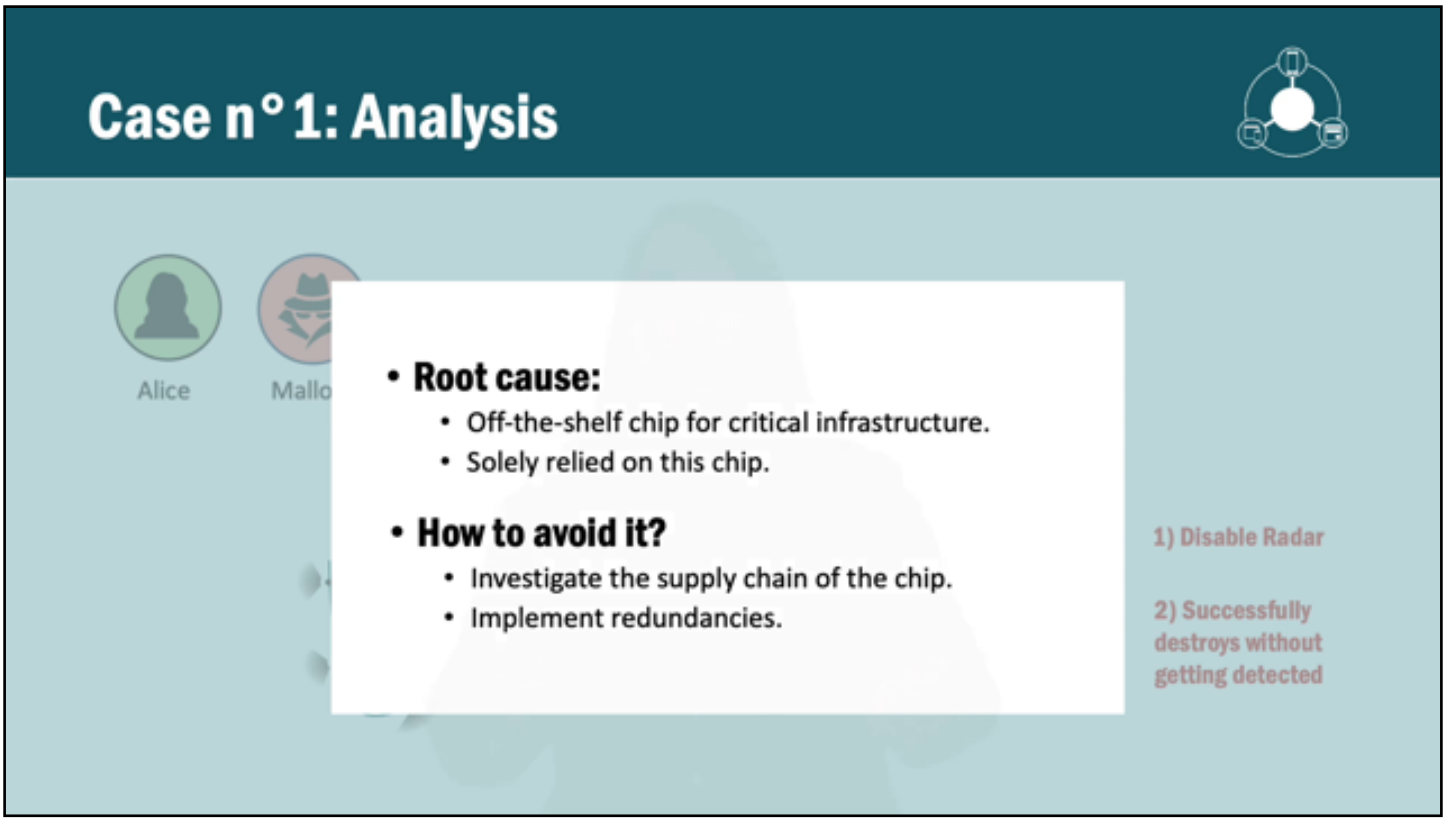


For starters, she should have investigated the supply chain of the chip she used, specifically checked if any of the components or manufacturing steps

notes

summary

2m 37s



were carried out in a hostile environment. Say, for example, controlled by her enemies like Mallory. Then, to avoid single points of failure in her critical infrastructure, Alice should have invested in redundant infrastructure built using diverse set of suppliers.

notes

summary

2m 49s

That's the story of Alice and Mallory.

notes

summary

3m 8s