Who was attacked?

**Target** is a US discount-retail giant with more than 1,790 locations throughout North America.

What was the attack-narrative?

Between mid-November and mid-December 2013, 110 million Target customers had their personal information or credit card details stolen. In May 2014, Target hired a new CIO, and CEO Gregg Steinhafel resigned. Victims claim that, though Target installed a new security system just months before the attack, triggered alerts were ignored. Though this is a common reaction to being overwhelmed by false-positives, in 2014, a Minnesota District Court judge ruled that banks could sue Target for negligence. Excluding legal costs and damage to its brand, Target announced that the data breach cost $162 million.

How did the attack operate?

Victims claim that hackers probed Target’s network for weaknesses and found that an air-conditioning subcontractor had limited access. Attackers ran a spear-phishing campaign against the subcontractor to gain access to the Target network.

With limited network-access, attackers found cracks in network segmentation and began exploring the network via lateral movements, eventually locating payment and customer-data servers, and uploading malware.

A Target server was used to collect stolen data and unencrypted POS information, and the sensitive information was then exfiltrated and sold on the black market.

When the malware was discovered, it was reportedly not recognized by standard malware-scanners as malicious.

How would illusive have detected the attack before the payload-launch?

**Prevention Through Detection**

The illusive Deceptions Everywhere® solution detects attacks before sensitive data is reached, keeping data safe without relying on recognized attack-signatures. During a breach, illusive immediately collects forensics directly from the compromised host, which help mitigation-teams isolate and neutralize attacks.

- illusive deceptions include realistic credentials, sensitive RDP servers, and database connections. Unseen (and therefore unused) by valid users and tools, use of these deceptions indicates a breach with zero false-positives.

- The illusive Attacker View™ reveals attack vectors and at-risk resources that connect segmented subnets.