Incident Report: 2013 Target Breach

Summary:

This report details the attack flow of the 2013 Target data breach, which compromised the personal and financial information of millions of Target customers. The attackers targeted a third-party HVAC company, Fazio Mechanical, to gain initial access to Target's network. They then moved laterally through the network, compromising servers and deploying malware on Point-of-Sale (POS) systems to collect credit card data.

Attack Details:

The attackers began by conducting reconnaissance on Target's network, gathering information on network configurations and identifying third-party suppliers. They discovered Fazio Mechanical, an HVAC company that had access to Target's network for billing, contract submission, and project management purposes.

Using a combination of phishing emails and malware, the attackers compromised Fazio Mechanical's systems, stealing credentials that allowed them to access Target's Ariba external billing system and establish a foothold in Target's network.

Once inside Target's network, the attackers used their initial access to move laterally, compromising additional servers using stolen credentials and exploiting software vulnerabilities. They may have also compromised a default account on Target's BMC Software Management system to further their access.

The attackers then identified and targeted Target's POS systems, deploying a customized version of the BlackPOS malware designed to steal credit card data. The malware resided on the POS systems' RAM, scanning for credit card data and sending it to an internal "dump" server within Target's network.

To evade detection, the malware used common ports (80, 139, and 443) to blend in with normal network traffic and employed a scheduled transfer process, sending data to the dump server only during specified hours (between 10 AM and 5 PM). The data was temporarily stored on the dump server and, once the transfer was complete, an ICMP packet was sent to an external server to notify the attackers that the data was ready for exfiltration.

The attackers then used unknown methods to exfiltrate the stolen credit card data from the dump server to external FTP servers under their control.