Wikipedia – British Airways Data Breech

On June 22, 2018, an attacker gained access to British Airways Network by means of compromised login details from an employee of Swissport, a third party cargo handler. The compromised account did not have multi-factor authentication enabled.

The attacker was initially restricted to a Citrix environment, but successfully broke out of the environment by unknown means. After breaking out of the environment, the attacker was able to login as an administrator after finding an administrator password stored in plaintext on the server.

On 26 July 2018, the attacker found plain text files, containing payment card details for British Airways redemption transactions. The UK Information Commissioner's Office's report highlighted this issue:

The logging and storing of these card details (including, in most cases, CVV codes) was not an intended design feature of British Airways' systems and was not required for any particular business purpose.

It was a testing feature that was only intended to operate when the systems were not live, but which was left activated when the systems went live. British Airways has explained that this card data was being stored in plaintext (as opposed to in encrypted form) as a result of human error. This error meant that the system had been unnecessarily logging payment card details since December 2015.

The impact of this failure was mitigated to some extent by the fact that the retention period of the logs was 95 days, which meant that the only accessible card details were those logged within the preceding 95 days. Nevertheless, the details of approximately 108,000 payment cards were potentially available to the Attacker.[1]

Customer Data Collection

British Airways' website used a JavaScript Library called Modernizr. British Airways had not updated their version of the library since 2012 and the version they were using had a known bug.

While inside the British Airways' network, the attacker was able to use the outdated library to redirect customer information to a fake domain, 'baways.com', controlled by the attacker. The payment process appeared legitimate to users.

Discovery

On 5th September, 2018, a third party informed British Airways of the malicious code acting on their website. Within 90 minutes it was removed. On the 6th of September British Airways informed the ICO and 500,000 affected customers.

On the 7th of September British Airways said the attack affected bookings from 21 August 2018 to 5 September 2018 with credit card details of around 380,000 total customers being compromised. The attackers obtained names, street addresses, email addresses, credit card numbers, expiration dates and card security codes – enough to allow thieves to steal from accounts. 77,000 customers had their name, address, email address and detailed payment information taken, while 108,000 people had personal details compromised which did not include card security codes.

British Airways urged customers to contact their banks or credit card issuer and to follow their advice. NatWest said that it received more calls than usual because of the breach. American Express said that customers would not need to take any action and that they would alert customers with unusual activity on their cards.