**Capital One Breach**

An attack on Capital One’s cloud environment between March and July of 2019 compromised the personal data of approximately 100 million customers of this [financial institution](https://cipher.com/cybersecurity-for-financial-services/). The information was stored on Amazon S3. At the end of July, a Seattle court indicted a former Amazon employee for stealing credit card and bank account numbers, along with addresses, names, telephone numbers, ages and Social Security numbers. This case brings to light the dangers of managing sensitive data in the cloud, the criticality of managing sensitive data, and the risks arising from third-party service providers.

**Facts**

The breach started between the 22nd-23rd March and was discovered almost four months later by Capital One (19th July). The stolen information included credit card numbers, birth dates, addresses, names, phone numbers, transaction history, 140,000 Social Security numbers and 80,000 bank account numbers.

After initial speculations that pointed to a zero-day exploit, the culprit, an employee of Amazon Web Services (AWS), who used an SSRF attack, was arrested. An investigation has been opened that will affect Capital One, AWS and GitHub (the platform that published the stolen data).

Capital One’s stock market value plummeted in the days following the attack, which further affected the company’s reputation.

**Analysis**

Initially, when the case became known in mid-July, it was thought that the attack resulted from a zero-day vulnerability that was exploited by a group of hackers. This suspicion changed with the arrest of Paige Thompson, an employee of Amazon Web Services who had been sharing information about her activities openly on the Internet and uploading information to GitHub. As she used neither an alias nor concealed her acts, it was only a matter of time before she was arrested. Paige Thompson, the alleged hacker employed by Amazon, simply took advantage of a misconfiguration in the Amazon Web Services (AWS) web application firewall (WAF).

The type of cyberattack is known as a **Server-Side Request Forgery (SSRF),** which is a trick used to make a server execute unauthorized commands on behalf of a remote user. This trick enables the user to treat the server as a proxy for requests, thus gaining access to private endpoints. This is a common risk for any organization using a public cloud for data storage and a blow for a company that had fully committed to a cloud model and had announced that it would close its data centers by 2020.

Two main issues stand out in this case:

* Responsibility. The case involves Capital One, AWS and GitHub, as well as the attacker herself. Capital One had $400 million in cyber liability insurance. However, when it comes to determining whether the insurer will pay, it will be essential to prove that there was no negligence in the processing of sensitive data, especially with regard to the WAF configuration.
* Details of the attacker. She did not belong to any particular group, her motives were not clear, and she did not use any concealment systems or the Dark Web. Furthermore, it puts the role of platforms like GitHub in the public eye as it shared the information. The company has been singled out for encouraging hacking activities.

**Recommendations**

One general recommendation involves the importance of sensitive data encryption. Capital One pointed out that it used an encryption standard, but the attacker managed to decrypt the information.

In addition, the case highlights the need to properly assess the use of a public cloud storage provider and to ensure compliance with all security standards involved in its deployment. AWS indicated, in the information provided to KrebsOnSecurity, that the problem stemmed from the poor configuration of the WAF, and not from the company’s infrastructure. AWS also highlighted the services it offers clients to mitigate possible risks like the ones in this case: Access Advisor, GuardDuty, the AWS, WAF (which, according to Amazon, would detect SSRF attacks), Amazon Macie (which detects, classifies and protects sensitive data).

Moreover, this event also stresses the need to develop a crisis plan in cases where security standards are violated.

It is difficult to know whether the case will be affected by the GDPR, given that the victims do not appear to be based in the European Union. Nevertheless, it would be worthwhile to examine and review all the regulatory requirements as well as how to manage possible risks.

Among the measures adopted by Capital One, one of the most notable is its offer to provide free identity monitoring and protection to all affected customers. The customers who were targeted in this case could soon be victims of phishing attacks that take advantage of stolen and filtered credentials, or even scams in which cybercriminals pretend to be representatives of Capital One.