CERT-EU

Memo

02/08/2019 - TLP:WHITE

Massive breach at Capital One, purportedly due to a cloud misconfiguration

Reference: Memo [190802-1] – Version: 1.0
Keywords: cybercrime, finance, personal data, cloud
Sources: Publicly available information

Key Points

- A breach at Capital One, a major US bank, compromised data belonging to more than 106 million customers in both the US and Canada.
- The breach was reportedly detected thanks to a vulnerability notification made by an ethical security researcher.
- The alleged hacker, who was arrested, was reportedly an employee of the Amazon Web Services cloud service company, of which Capital One was a customer.
- The breach purportedly exploited a misconfigured web application used to access the cloud infrastructure.

Summary

On July 19, Capital One, a major US bank, determined[1] that an outside individual gained unauthorised access and obtained information about its credit card customers and individuals who had applied for its credit card products. The breach reportedly occurred on March 22 and 23, 2019. Capital One discovered the incident thanks to an ethical external security researcher who reported a configuration vulnerability.

The breach affected approximately 100 million individuals in the United States and around 6 million in Canada. The compromised data includes credit card application data (applicant names, addresses, contact information, etc.), but also fragments of transaction data as well as customer-related information such credit scores, limits, balances, etc.

On July 29, FBI agents arrested[2] Paige A. Thompson on suspicion of downloading nearly 30 GB of Capital One credit application data from a rented cloud data server. She reportedly had stored some of the leaked data in the open on GitHub, a source code management platform.

According to Ray Watson[3], a cybersecurity researcher at cloud security firm Masergy, the attacker was a former employee of Amazon Inc. and Capital One is a customer of Amazon Web Services (AWS). 'She [Thompson] allegedly used web application firewall credentials to obtain privilege escalation. Also the use of Tor and an offshore VPN for obfuscation are commonly seen in similar data breaches.' According to an Amazon spokesperson[4], 'AWS was not compromised in any way and functioned as designed. The perpetrator gained access through a misconfiguration of the web application and not the underlying cloud-based infrastructure. As Capital One explained clearly in its disclosure, this type of vulnerability is not specific to the cloud.'

The hacker, Thompson, under her nickname 'erratic', spoke openly on Twitter, over several months, about finding huge stores of data intended to be secured on various Amazon instances. This might have incited or facilitated the work of other cybercriminals.

Comments

The way the incident was discovered confirms that the implementation of a voluntary and responsible reporting program can be an efficient manner to detect incidents. CERT-EU has implemented such a program for its constituency (see Hall of Fame, https://cert.europa.eu/cert/newsletter/fr/latest_HallOfFame_.html).

This incident also underlines the potential danger represented by former (IT) employees, a kind of insider threat. This is especially dangerous when the employer is a cloud service company. In Capital One's case, the hacker seemed to be interested in hacking into improperly secured Amazon cloud instances.

Misconfiguration issues affecting web applications are common. When they affect web applications used to access cloud-storage infrastructure, the impact can be huge, like in the Capital One case. CERT-EU strongly recommends its constituents that have migrated or are going to migrate to the cloud to fully understand their responsibility as regards the type of offer they choose (IaaS, SaaS, etc.) and the secure management of web-based applications to access their cloud resources. If needed, do not hesitate to contact CERT-EU for further assistance.

[1] https://www.capitalone.com/facts2019/
[2] https://krebsonsecurity.com/2019/07/capital-one-data-theft-impacts-106m-people/
[3] ibid.
[4] https://www.newsweek.com/amazon-capital-one-hack-data-leak-breach-paige-thompson-cybercrime-1451665