2019 Capital One Cybersecurity Incident

Elliot Mason

CYSE 300: Introduction to Cybersecurity

Professor Joe Kovacic

January 30, 2025

On July 19, 2019, Capital One, a major U.S based financial corporation determined that an outsider of the company gained unauthorized access into their system. This individual obtained personal and private information about Capital One credit card members and those who had applied for a Capital One credit card. Capital One immediately responded to the breach and coordinated with federal law enforcement agencies. The Federal Bureau of Investigations (FBI) was able to locate the outsider who stole the customers information and federal agencies were able recover the data. It was determined that approximately 100 million U.S individuals and approximately 6 million Canadian individuals were affected (capitalone.com)

The vulnerability and initial entry point that led to Capital One's major cybersecurity incident was a misconfigured Web Application Firewall (WAF). The open-source *ModSecurity* WAF was implemented and deployed with the responsibility to protect the web application. It would do so by filtering and monitoring the HTTP traffic between the application and internet in order to protect against common attacks. However, the deployment of the WAF was misconfigured, this allowed the external perpetrator to reach Capital One's internal resources (Khan et al., 2022)

On its own, the misconfiguration is not a major issue, however, the combination with the misconfiguration and AWS infrastructure and metadata service, created a critical threat. The AWS metadata service is a cloud specific component that most security controls do not protect. There was a lack of understanding between the WAF and the AWS cloud structure, highlighting an issue of roles and responsibilities between Capital One and AWS (Khan et al., 2022)

Paige Thompson, a former software engineer at AWS, used her knowledge of the AWS cloud infrastructure and the misconfigured WAF to infiltrate Capital One's customer information. Thompson used Server-Side Request Forgery (SSRF) commands to send request through the

application to gain credentials into an account that could allow her access into certain data folders. Once in the account, Thompson wrote commands to extract the data using the accounts permissions (Borkar, 2019).

As stated, approximately 106 million credit card holders and applicants were affected. The data accessed contained credit scores, limits, balances, payment history and customer contact information. It also contained a number of transactions during 2016 to 2018. Approximately 140,000 Social Security numbers and 80,000 bank account numbers were compromised. This cybersecurity incident resulted in a class action lawsuit resulting in a 190-million-dollar settlement and 80-million-dollarsfine from the Office of the Comptroller of the Currency (OCC). The hacker, Paige Thompson, was arrested and charged with the unauthorized access to data (investor.capitalone.com).

Not all cybersecurity attacks can be prevented, but a majority of them can. Companies must do their service in ensuring their infrastructure and data is safe and secure. Capital One could've implemented penetration testing and vulnerability scanning to identify any vulnerability such as the WAF misconfiguration. Unfortunately, this did not happen, causing the attacker, Thompson, to identify the vulnerability herself and use it to her advantage. Capital One also should have encrypted all their data while at rest as well as in transit, however they did not, encryption could have stopped Thompson from seeing the data or at the minimum slowed her down. Other security methods such as better monitoring for suspicious activity and the least privilege principle could've halted the attack on customers data (Cinar, 2025).

References

2019 capital one cyber incident: What happened. Capital One. (n.d.). https://www.capitalone.com/digital/facts2019/

Borkar, P. (2025, April 8). *A look at the capital one data breach through the lens of Mitre ATT&CK*. Exabeam. https://www.exabeam.com/blog/ueba/a-look-at-the-capital-one-data-breach-through-the-lens-of-mitre-attck/#:~:text=The%20breach%20on%20Capital%20One,One%20include%20the%20AWS%20WAF.

Capital one announces data security incident. Capital One Financial Corp. (n.d.). https://investor.capitalone.com/news-releases/news-release-details/capital-one-announces-data-security-incident

Cinar, A. (2025, April 19). *One packet away from disaster: Capital one and the SSRF breach*. Medium. https://medium.com/@cinar0arda/one-packet-away-from-disaster-capital-one-and-the-ssrf-breach-5c75a2f5b034

Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022). A systematic analysis of the Capital One Data Breach: Critical Lessons Learned. *ACM Transactions on Privacy and Security*, *26*(1), 1–29. https://doi.org/10.1145/3546068