

Capital One

# What is Capital one ?

Capital One is the fifth largest consumer bank in the U.S. and eighth largest bank overall , with approximately 50 thousand employees and 28 billion US dollars in revenue in 2018.

Capital One is a tech-driven U.S. bank and an early adopter of cloud computing. In its 2018 investor report, the company stated it’s building *“a technology company that does banking,”* with 85% of its tech workforce being engineers. It uses agile practices, APIs, microservices, and cloud-based systems for most of its operations and customer-facing apps.

Capital One was among the first banks to shift from on-premise data centers to the cloud, a move that later contributed to a 2019 data breach. Since 2014, it has worked with AWS to reduce its data centers from eight to three (planned by 2020). The bank also developed a cloud security framework to meet strict compliance standards before migrating workloads.

# Technical Assessment of the Capital One Incident

Despite the strong investments on IT infrastructure, in July 2019 Capital One disclosed that the company had sensitive customer data assessed by an external individual. According to Capital One’s public report released on July 29, 2019 , On July 19, 2019, we determined that an outside individual gained unauthorized access and obtained certain types of personal information from Capital One credit card customers and individuals. The company claimed that compromised data corresponded to “personal

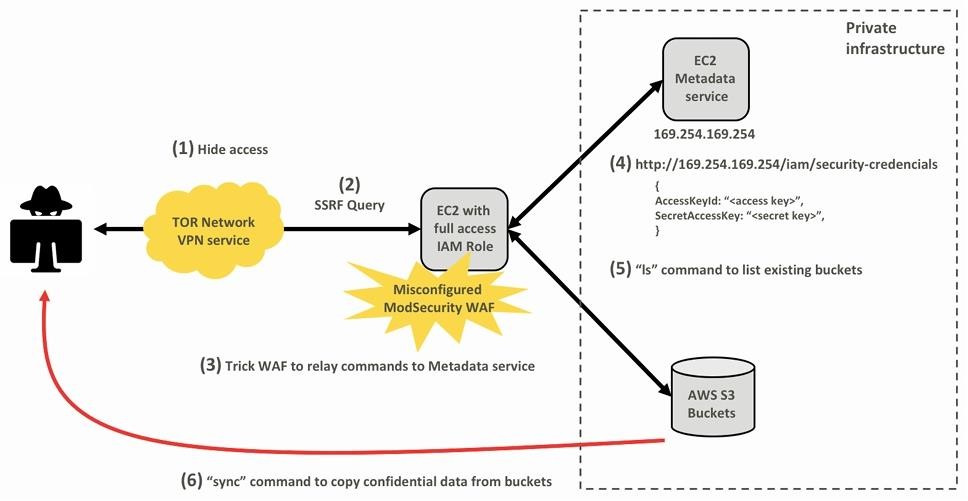
information Capital One routinely collects at the time it receives credit card applications, including names, addresses, zip codes, phone numbers, e-mail addresses, dates of birth, and self-reported income.” The unauthorized access “affected approximately 100 million individuals in the United States and approximately 6 million in Canada”.

Capital One learned about its 2019 data breach not through its own security monitoring, but because an outside person reported it via the bank’s Responsible Disclosure Program on July 17, 2019. According to the FBI’s court filing, someone emailed Capital One to warn that sensitive customer data had been leaked and was publicly visible on GitHub

.

The FBI arrested a woman named Paige Thompson from Seattle for hacking into Capital One’s cloud servers. Investigators found out she used to work at Amazon, which may have given her technical knowledge about cloud systems. She didn’t just target Capital One—the U.S. government accused her of

# How the attacker got access ?



1). The FBI and Capital One investigators noticed that the hacker (Paige Thompson) accessed their systems using hidden digital pathways designed to conceal her identity.

She used two tools to cover her tracks:

**TOR Network**: Made her internet traffic untraceable by bouncing it through random computers worldwide.

**IPredator VPN**: Further disguised her real location by making it appear as if the attacks came from Sweden.

1. The SSRF (Server-Side Request Forgery) attack allowed the hacker to exploit Capital One’s misconfigured web firewall by tricking its cloud server into obeying malicious commands as if they came from a trusted user. the attacker sent crafted requests that bypassed security checks, forcing the server to reveal sensitive credentials (digital "keys"), list private data folders, and copy customer information. This worked because the firewall failed to verify requests properly. To hide her identity, she routed attacks through anonymizing tools like TOR (The Onion Router) and IPredator VPN, masking her real location. The breach exposed over 100 million customers’ data, highlighting how a single security oversight (misconfigured firewall + SSRF vulnerability) can cascade into a massive leak when exploited by someone with technical skill (like Thompson’s Amazon cloud experience).
2. The fatal vulnerability occurred when Capital One's misconfigured Web Application Firewall (WAF) failed to block external access to AWS's internal metadata service (located at [http://169.254.169.254](http://169.254.169.254/)) - a critical security oversight. Normally protected like a secure back-office, this service provides temporary cloud credentials that act as master keys for the server's environment. The attacker exploited the WAF's weak configuration by sending crafted requests that bypassed security checks, tricking the server into revealing these sensitive credentials - essentially fooling the system into handing over its own access badges. These stolen credentials then granted the hacker unauthorized access to Capital One's S3

storage buckets,

1. By combining the SSRF attack and the WAF misconfiguration, the attacker used the URL “<http://169.254.169.254/iam/security-credentials>” to obtain the AccessKeyId and SecretAccessKey credentials. The resulting temporary credentials allowed the criminal to run commands in AWS environment via API, CLI or SDK.
2. By using the credentials, the attacker ran the “ls” command multiple times, which returned a complete list of all AWS S3 Buckets of the compromised Capital One account.
3. Lastly, the attacker used the AWS “sync” command to copy nearly 30 GB of Capital One credit application data from these buckets to the local machine of the attacker. This command gave the attacker access to more than 700 buckets.

# Challenges and Issues Caused by the Data Breach

* 1. **Cybersecurity Vulnerabilities**
     + Misconfigured firewall and lack of robust security measures.

# Regulatory and Legal Consequences

* + - Fines and penalties from regulatory bodies.
    - Lawsuits from affected customers.

# Customer Trust and Brand Reputation

* + - Erosion of customer confidence in Capital One’s security measures.
    - Negative media coverage and public perception.

# Operational Disruptions

* + - Internal investigations and audits.
    - Resource allocation for breach remediation.

# How Capital One Overcame the Data Breach

* 1. **Immediate Remediation Efforts**
     + Fixing the misconfigured firewall and enhancing security protocols.
     + Offering free credit monitoring and identity protection to affected customers.

# Strengthening Cybersecurity Measures

* + - Investment in advanced cybersecurity tools and technologies.
    - Implementation of multi-layered security frameworks.

# Regulatory Compliance and Transparency

* + - Cooperation with regulators and law enforcement.
    - Regular updates to customers and stakeholders.

# Rebuilding Customer Trust

* + - Launching campaigns to reassure customers about improved security.
    - Enhancing customer communication and support.
* **6.5 Long-Term Strategic Changes**

1. **Lessons Learned from the Data Breach**
   1. **Importance of Proactive Cybersecurity**
      * Need for regular security audits and vulnerability assessments.

# Role of Employee Training

* + - Ensuring staff are aware of security best practices.

# Balancing Innovation and Security

* + - Integrating security into every stage of digital transformation.

# Customer Communication in Crisis

* + - Importance of transparency and timely updates during a breach.

**CONCLUSION:**