Firewall Vulnerabilities - Are You Leaking Data Similar To Capital One?

This month's big security news involved a data breach at Capital One that, by the company's own estimate, affected approximately 100 million individuals in the United States and approximately 6 million Canadians. Among the data leaked were 140,00 Social Security Numbers (SSNs) and 80,000 bank account numbers belonging to secured credit card customers. It has been claimed that the Capital One breach may be as far reaching as the Equifax breach of 2017, which affected an estimated 147 million consumers and cost the company at least $575 million in fines and up to $700 million in compensation.

So, what exactly happened at Capital One, how did it happen and what lessons can we learn from yet another massive data breach?

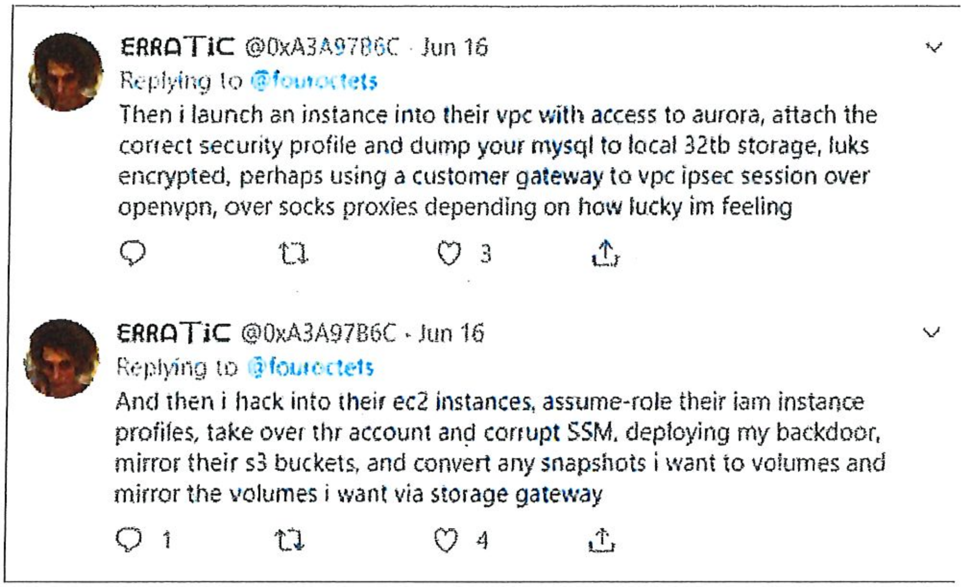
What Happened At Capital One?

As has been well-documented since the news broke earlier this week, an individual by the name of Paige A. Thompson, *aka* Erratic on Twitter (her account has since been suspended), was indicted by the FBI on July 29, 2019 on a single count of Computer Fraud and Abuse. The charge pertains to an alleged network intrusion that resulted in the exfiltration and theft of Capital One confidential consumer data, including credit card applications and other digital documents.

The hack is said to have taken place on or after March 12, 2019, when Thompson allegedly used a vulnerability in a firewall application to access a privileged account. Once she had gained access, the FBI claim, she went on to use it to issue server commands to obtain personally identifying information belonging to applicants of a Capital One credit card product between 2005 to 2019. The information disclosed includes names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and income.

The investigation was triggered by an email sent to Capital One's Responsible Disclosure email address – a channel the company uses to receive intel on bugs, vulnerabilities and other security issues – by an unidentified security researcher. Despite the FBI not naming the Cloud Service provider used by Capital One to host the breached server, the security researcher's email refers to "leaked s3 data". The reference to "s3" clearly indicates Amazon's Simple Storage Service (S3). Capital One have, also, been vocal about being clients of Amazon S3 in the past.

Although the technical details of how Thompson allegedly hacked into the server are sparse at this time, we do know that, according to Capital One, the leak occurred through a firewall vulnerability issue. Amazon's S3 and other cloud services come strongly touted with a Web Application Firewall known as AWS-WAF, which can be hosted on the Amazon CloudFront. Ms. Thompson's CV, a partial screenshot of which appears below, indicates that she was formerly employed by Amazon, and had extensive experience of networking, S3 and CloudFront technologies.



ERRATiC @0xA3A97B6C · Jun 16
Replying to @fouroctets
Then i launch an instance into their vpc with access to aurora, attach the correct security profile and dump your mysql to local 32tb storage, luks encrypted, perhaps using a customer gateway to vpc ipsec session over openvpn, over socks proxies depending on how lucky im feeling

ERRATiC @0xA3A97B6C · Jun 16
Replying to @fouroctets
And then i hack into their ec2 instances, assume-role their iam instance profiles, take over thr account and corrupt SSM, deploying my backdoor, mirror their s3 buckets, and convert any snapshots i want to volumes and mirror the volumes i want via storage gateway

What Are Web Application Firewalls (WAFs)?

According to Capital One's statement, the firewall configuration vulnerability has now been fixed. Although it has not been confirmed, given what we do know, it's a reasonable assumption that the issue concerned Capital One's configuration of Amazon's Web Application Firewall, the AWS-WAF.

Web Application Firewalls are intended to protect particular web applications by analyzing packets of incoming traffic according to a set of rules or policies and filtering out potentially harmful traffic. Amazon's AWS-WAF allows customers like Capital One to either set up their own rules or buy pre-configured Managed Rules from AWS Marketplace sellers. The fact that there is a market for managed rules testifies to the fact that configuring and maintaining WAFs is no simple matter. It is not just a matter of configuring a WAF once and letting it run; rather, WAFs need to be actively maintained as the application behind a WAF is itself likely to evolve with development and user demand and require different rules for its traffic over time. Because of this, WAFs can be subject to both a high degree of false positives (blocking harmless traffic) and false negatives (allowing malicious traffic). They can also impact performance if not configured correctly. These and other considerations create the need for specialist third-party vendors to provide and maintain Managed Rules.

What Can We Learn From the Capital One Breach?

The primary takeaway from the Capital One breach is that businesses need to ensure that firewalls and Web Application Firewalls are properly configured and maintained, and that credentials are secure. The apparent speed with which Capital One were able to claim the configuration vulnerability had been fixed may suggest the remedy was obvious once known, and that in turn may indicate a simple oversight like not securing a Secret Access Key. Make sure you have a dedicated expert team managing critical security devices and policies.