Introduction

On July 29, 2019, we learned of a massive cyberattack and data breach targeting Capital One. The Securonix Threat Research Team has been actively investigating the details of the attack to help our customers detect, mitigate, and respond to such attacks [1,2].

Here is a summary of what we currently know and our recommendations on some possible Securonix predictive indicators and security analytics that can be used to detect the current, and potentially future, attack variants. We will update indicators as we receive more information.

Note: If you are not currently collecting/analyzing your cloud infrastructure and application logs, including WAF, AWS S3 Server Access, and AWS CloudTrail, we strongly recommend that you start collecting the logs and using them in your analysis to ensure that you are able to detect the latest attacks.
Summary

Impact
Here are some of the key details that are currently known regarding the impact of this massive cyber attack/data breach [1, 2]:

• ~30GB of sensitive PII data exfiltrated impacting an estimated 100M and 6M customers in the US and Canada, respectively.
• Some of the PII compromised included: Social Security numbers (SSN); Bank account numbers and credit card numbers; Income, names, addresses, zip codes; Emails, phone numbers, DOB; Portions of credit card customer data such as credit scores, credit limits, payment history and bits of transaction data.
• Based on the latest details, there were likely several other companies compromised by the attacker besides Capital One [1].

Attack Vector(s)
According to the publicly available details, the primary attack vector used involved an AWS WAF/IAM misconfiguration [2]. (The exact vulnerability targeted by the attackers for initial infiltration has not been disclosed yet.)

The misconfiguration resulted in over 700 AWS S3 buckets accessed using an authorized WAF role account with permissions to access the buckets containing the sensitive Capital One customer PII data. The data was subsequently exfiltrated via TOR exit nodes/IPredator VPN to the attacker-controlled server [1,2]. Based on the currently available details, there is a possibility that some of the attack vectors leveraged a variant of Server-side Request Forgery (SSRF) followed by credential stealing. (This is still to be confirmed, see [1, 3] and details below.)
Some Relevant Software Security Issues/CWEs

- CWE-16
- CWE-88 (to be confirmed)
- CWE-918 (to be confirmed)

Figure 2: Capital One 100M Cyberattack - Obtaining AWS Credentials Through WAF Example

Capital One Cyberattack - Securonix Technical Analysis

While many technical details of the attack, particularly the initial infiltration stages, are currently unknown, based on the publicly available details, our technical analysis, and our expertise, here are some of the key technical details describing the likely progression of this high-profile cyberattack involving critical Capital One customers’ PII data (to be confirmed):
• The attacker scanned and identified a misconfigured WAF that enabled accessing the corresponding AWS EC2 instance/ECS task *metadata* using Server-side Request Forgery (SSRF) bypass [3]:

```plaintext
GET /?caponeurl=http://169.254.169.254/latest/meta-data/ HTTP/1.1
Host: [removed].capitalone.com
[...]
```

• The attacker checked for further details from the associated EC2 instance, including AMI ID, etc. using http://169.254.169.254/latest/meta-data/latest/meta-data/ami-id, UserData scripts with API keys, and/or in case of ECS Task, obtained credentials through:

  http://169.254.170.2/v2/credentials/<UUID> endpoint (after obtaining UUID via e.g. file:///proc/self/environ if a Linux AMI was used), list of IAM roles associated with the machine via e.g. http://169.254.169.254/latest/meta-data/iam/security-credentials/

• The attacker then continued with internal recon, executing more queries, including querying the ISRM-WAF-Role IAM role using, e.g. http://169.254.169.254/latest/meta-data/iam/security-credentials/ISRM-WAF-Role to obtain the required credential details (see Figure 2).

• During the internal recon stage, the attacker was able to obtain information about the available AWS S3 buckets, and then the stolen credentials were potentially leveraged to obtain STS as part of a direct AWS API query, e.g.:

```python
aws_sts = boto3.client(
    'sts',
    aws_access_key_id=access_key,
    aws_secret_access_key=secret_key,
    aws_session_token=session_token)

> print(aws_sts.get_caller_identity()['Arn'])
> arn:aws:sts::[axed]:assumed-role/ISRM-WAF-Role_UUID/<axed>
```
• The ECS instance/task permissions likely included access to the Capital One S3 buckets containing sensitive PII data:
  - **Effect:** Allow
  - **Action:**
    - `s3:GetObject`
    - `s3:ListBucket`
  - **Resource:** `<*/Capitalone s3 bucket resources>`

• This most likely enabled the attacker to access sensitive PII data either through `s3 sync` CLI or using AWS API, e.g. using the following:
s3_capital_one_breach = boto3.client('s3',
    aws_access_key_id=access_key,
    aws_secret_access_key=secret_key,
    aws_session_token=session_token )

resource = boto3.resource('s3')
s3_capital_one_breach.get_object( Bucket='capitalone-bucket', Key='[/tmp/','[axed].snappy.parquet' )

• This was likely followed by iterating through over 700 S3 buckets containing over ~30GB of data/snappy parquet files, downloading the files from the buckets (see Figure 3).

Detection – Securonix Behavior Analytics/Security Analytics

Based on the publicly available details about the Capital One Financial Corporation attack, proper visibility into the cloud environment, including WAF logs, S3 logs, CloudTrail logs, etc. and the ability connect anomalies across different entities (S3 buckets, Roles, IP Addresses, etc.) was most likely key to be able to detect the attack.
Taking into account our expertise and the known techniques used by the threat actors in similar real-world attacks, particularly those targeting cloud environments, some high-level examples of the relevant Securonix behavior analytics/predictive indicators that could help detect such attacks in your environment include:

• **Suspicious Cloud Activity - Peak AWS S3 GetObject For Account Analytic**
  This can be used to identify unusual access to S3 buckets. As we know from Capital One breach, there were over 700 S3 buckets containing PII that were accessed from both TOR exit node addresses and IPredator bulletproof VPN hosting IP addresses etc.

• **Suspicious Cloud Activity - Rare ListBuckets Role For AWS S3 Logs Analytic**
  This can be used to identify suspicious activity associated with different roles’ access to AWS S3 buckets. In the case of the Capital One breach, the files in the Capital One buckets including “snappy.parquet” were accessed by the ISRM-WAF-Role IAM role.
• **Suspicious Cloud Activity - Rare ListBuckets Role For AWS S3 Logs Analytic**

This can be used to identify attempts to access buckets utilizing a suspicious role. In the case of the Capital One attack, the ISRM-WAF-Role accessed an S3 bucket containing the `*c000.snappy.parquet` file on March 21, 2019, which was the only time the account accessed the file from January 1, 2019 to July 20, 2019.

And a number of other Securonix behavioral analytics/predictive indicators including **CLO-AWS4-BDI, CLO-AWS3-ERI, CLO-AWS10-BDI, CLO-AWS14-ERI, CLO-AWS6-ERI, CLO-AWS16-BPI, CLO-AWS17-BPI, CLO-AWS15-ERI**, et al.

Some examples of successful detection of this real-world attack in practice using Securonix are shown in Figures 4-6.

![Figure 6: Practical Capital One Cyberattack Detection Using Securonix - III](image-url)
References


ABOUT SECURONIX
Securonix is radically transforming all areas of data security with actionable security intelligence. Our purpose-built, advanced security analytics technology mines, enriches, analyzes, scores and visualizes customer data into actionable intelligence on the highest risk threats from within and outside their environment. Using signature-less anomaly detection techniques that track users, account and system behavior, Securonix is able to detect the most advanced insider threats, data security and fraud attacks automatically and accurately.

CONTACT SECURONIX
www.securonix.com
info@securonix.com | (310) 641-1000