NTT DATA
Trusted Global Innovator

注目されているセキュリティ事故・事件に関する情報 ＜2019年9月版 (第30号)＞(選り抜き版)

2019年9月25日
ＮＴＴデータ先端技術株式会社
セキュリティ事業本部

今回のサマリー

米金融大手で1億人超の情報漏えい
2019年7月、米金融大手Capital Oneは不正アクセスにより1億人以上の個人情報が漏えいしたと発表しました。ここでは、公開されている情報を整理し、企業が取るべき対策について解説します。

米金融大手で1億人超の情報漏えい

1. 米金融大手で1億人超の情報漏えいの概要 (1/2)

米金融大手Capital Oneで1億人超の情報漏えいが2019年7月に発覚しました。Capital OneのサイトはAWS(以下Amazon Web Service)に設置されており、Capital Oneが独自に構築したWAF(ModSecurity)の設定不備によって攻撃を許したことが原因とされています。

■ Capital Oneの漏えい件数

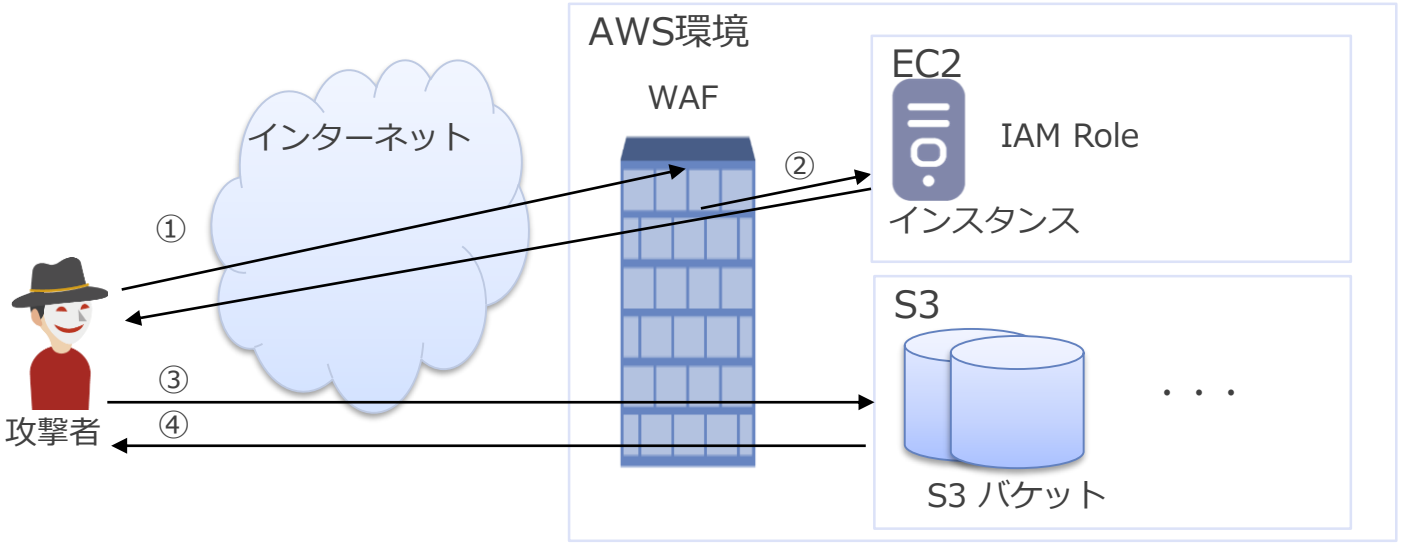
#	漏えい内容	アメリカ	カナダ
1	個人情報 (名前、郵便番号、住所、電話番号、電子メールアドレス、生年月日、自己申告による収入など)	1億件	600万件
2	社会保障番号	14万件	100万件
3	銀行口座番号	8万件	-

一部では、信用限度、残高などの顧客ステータスデータなども含まれていたとされています。

1. 米金融大手で1億人超の情報漏えいの概要 (2/2)

今回漏えいされた情報は、AWSのS3に保存されていました。

① 攻撃者はWAF(Capital Oneが独自に構築)へアクセス
② 攻撃者はEC2メタデータにWAF経由でアクセス
WAFは攻撃者に代わってEC2メタデータからIAM Role※の認証情報を取得し攻撃者へ応答
③ 攻撃者は取得したIAM Roleを使用してS3バケットにアクセス
④ S3 Sync(同期)機能で、ファイル取得



※IAM Role：おもにEC2インスタンスから、AWSの各種リソース(S3など)にアクセスする際の権限設定に使うAWS内の機能です。

2. タイムライン

今回の事象では、不正アクセス発生からCapital One側が外部からの報告により事象の発覚まで、3か月以上要しています。

年月日	概要
2019年3月12日-7月17日	犯人が同サーバにアクセス
2019年3月22日-23日	犯人による不正アクセス発生 S3にアクセスするためのキーを取得する攻撃とデータのダウンロードを実施
2019年4月	犯人がこの攻撃に関する情報をインターネット上に投稿 詳細をGitHubページに投稿、TwitterやSlackで攻撃について語っていた
2019年7月17日	外部(GitHubユーザ)からCapital Oneへ不正アクセスの報告
2019年7月19日	Capital OneがFBIへ連絡
2019年7月29日	Capital Oneが侵害があったことを公開
2019年7月29日	FBIが犯人を逮捕

3. 原因と考えられる対策

今回の事象における原因として、WAFの設定不備、IAM Role権限の設定不備、S3バケットのアクセス制御不備の大きく3つが挙げられます。

原因	概要	考えられる対策
WAFの 設定不備	WAFはAWS WAFではなくCapital Oneが独自にModSecurityを構築していた。Modsecurityに設定不備がありSSRF攻撃を防げなかった。	WAFがロギングモードだったことや設定(ルールセットなど)の不備は、監査や脆弱性評価などで検出可能。 あるいは、独自にWAFを構築せずにAWSで用意しているAWS WAFを利用することも有効な手段(AWSのWAFは、初期状態で適切な設定がされている)。
IAM Role 権限の 設定不備	EC2メタデータから“S3へアクセスできる非常に高いIAM Role権限”が取得可能だった。	AWS構成の監査を受けることで、必要最低限のIAM Role権限となっているか検出可能。
S3バケットの アクセス 制御不備	EC2からS3バケットへのアクセスを許可されており、ダウンロードが可能だった。	AWSに存在するアクセス制御テンプレートを利用する。(S3バケット以外にも、複数の段階におけるアクセス制御が必要) IAMやS3など、各リソースへのアクセス監視を行う。あるいは、AWS内の脅威検出サービスGuard Dutyを利用することで、大量データの移動が検知可能。

4. 事前に実施していた対策

Capital Oneは社会保障番号や口座番号などの項目は、今回のインシデント発生前からトークン化されていたため、漏えいされませんでした。

Capital Oneはクレジットカード情報保護を目的とした機関であるPCI SSCに加盟しています。そのため、事象前から今回のシステムでトークン化されていた箇所があったと、推測されます。

参考）同様の環境を保有する顧客に対して、AWS側が行っている支援

サービス名称	内容
AWS IAM アクセス アドバイザー	IAM(Identity and Access Management)アクセスアドバイザーにて、必要最小限のアクセス権が設定されているか確認することが可能。
Guard Duty	悪意のある操作や不正な動作を継続的にモニタリングする脅威検出サービス。今回のような大量データの移動を検知することが可能。
AWS WAF	SSRF含む一般的な攻撃の検知することが可能。
Amazon Macie	AWS内に保存された機密データを検出、分類、保護することが可能。
AWS 多要素認証	重要な箇所へのアクセスには、ワンタイムパスワードの設定することが可能。

5. 影響

■ 漏えいされた情報の二次被害

　容疑者は逮捕後、捜査官に対して盗んだデータを販売または共有していないと話しました。

　裁判所に提出された新しい書類の中で、米当局は容疑者がうそをついていることを示す証拠は見つかっていないと述べています。

■ 今回の事象による経済的影響

　Capital Oneは、今回の不正アクセスの顧客への通知および監視の強化などによって「2019年におよそ1億ドル(約110億円)から1億5000万ドル(約160億円)のコスト」が発生すると見込んでいます。

6. 結論/まとめ

■ 本事象の結論/まとめ

Capital Oneが独自に構築したWAF(ModSecurity)の設定不備が、攻撃者が不正アクセスした1つめのステップであり、侵害された1番の要因と考えられます。

さらに、S3バケットへのアクセスを可能にしたアクセス権限は、リリース以降だと修正することが困難な場合もあります。そのため、リリース前にアカウント権限の多角的なレビューを行うべきです。

■ インシデント対応として

事前の対策として、セキュアなサイトではなかったということも問題点ですが、3か月以上にわたって不正アクセスを検知できなかったこともまた大きな問題点です。

インシデントの早期発見・早期収束を図り、被害の局所化・最小化を確実にするために、AWS内の脅威検出サービスGuard Dutyを利用し、S3バケットの大量データが移動された時点で検知することも手段のひとつです。

他のクラウド事業者でも、各種リソースへのアクセスの検知や、データの移動を検知するようなサービスが用意されています。事象を早期に発見する仕組みの構築をお勧めします。

7. 参考URL (1/2)

- 米金融大手Capital Oneで1億人超の情報漏えい--容疑者はAWS元従業員の可能性
  https://japan.zdnet.com/article/35140621/
- 米金融大手Capital One情報漏えいの容疑者、さらに30社超からデータ盗難の疑い
  https://japan.zdnet.com/article/35141316/
- 1億人超の個人情報流出、容疑者はAmazon元従業員クラウドセキュリティに不安の声も
  https://www.itmedia.co.jp/news/articles/1908/05/news067.html
- SSRF攻撃によるCapital Oneの個人情報流出についてまとめてみた
  https://piyolog.hatenadiary.jp/entry/2019/08/06/062154
- キャピタル・ワンで約１億人分の情報流出、アマゾン元従業員を逮捕 Bloomberg
  https://www.bloomberg.co.jp/news/articles/2019-07-30/PVG8PB6JIJUR01
- Seattle Tech Worker Arrested for Data Theft Involving Large Financial Services Company
  https://www.justice.gov/usao-wdwa/pr/seattle-tech-worker-arrested-data-theft-involving-large-financial-services-company
- An SSRF, privileged AWS keys and the Capital One breach
  https://blog.appsecco.com/an-ssrf-privileged-aws-keys-and-the-capital-one-breach-4c3c2cded3af
- Capital One Security Incident & Key Lessons, so far anyway.
  https://medium.com/@ravi.ivat/capital-one-security-incident-key-lessons-so-far-anyway-d90a931da928

7. 参考URL (2/2)

- Capital One Announces Data Security Incident Capital One Announces Data Security Incident
  http://press.capitalone.com/phoenix.zhtml?c=251626&p=irol-newsArticle&ID=2405043
- Information on the Capital One Cyber Incident
  https://www.capitalone.com/facts2019/
- IAM ロール (対策の例)
  https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_roles.html
- AWS IAM Access Advisor　(対策の例)
  https://aws.amazon.com/jp/about-aws/whats-new/2019/06/now-use-iam-access-advisor-with-aws-organizations-to-set-permission-guardrails-confidently/
- Amazon GuardDuty (対策の例)
  https://aws.amazon.com/jp/guardduty/
- AWS WAF (対策の例)
  https://aws.amazon.com/jp/waf/
- Amazon Macie (対策の例)
  https://aws.amazon.com/jp/macie/

NTT DATA

Trusted Global Innovator