脅威情勢レポート

特集：
Amazon Simple Storage Service (Amazon S3)

DEEP INSTINCT 脅威ラボ

2024 年 3 月

目次

著者

MARK VAITZMAN
脅威ラボチームリーダー

SIMON KENIN
脅威インテリジェンスリサーチャー

IVAN KOSAREV
脅威インテリジェンスリサーチャー

エグゼクティブサマリー

クラウドストレージは、拡張性、コスト効率、およびアクセス性に優れていることから、あらゆる規模の企業に人気のソリューションとなっています。Research and Markets によると、世界のクラウドストレージ市場は、**2022 年の 835 億 5,000 万ドルから 2023 年には 1,002 億ドル**に年平均成長率 19.9% で成長しました (2020 年はわずか 400 億ドルでした)。

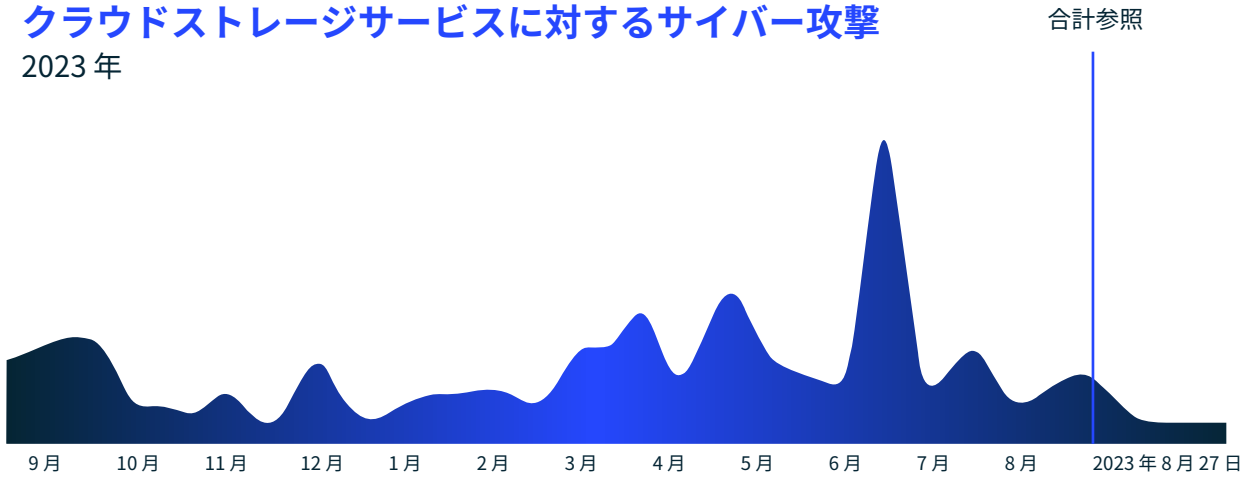
企業は、コストを削減して運用効率を向上させるため、クラウドストレージに移行する動きを強めています。しかしデジタル化が新たな優先事項となるにつれて、**クラウドセキュリティに関連する脅威もその対象を拡大しており**、クラウドストレージ、特に AWS の S3 バケットはサイバー犯罪者の主な標的となっています。

このレポートでは、特に AWS S3 の脅威情勢に焦点を当てて現在のクラウドストレージのセキュリティ状況を分析し、最近のサイバー攻撃、進化する MITRE 手法、攻撃者、影響、およびデータを保護するためのベストプラクティスについて説明します。

クラウドストレージの成長の原動力

クラウドストレージサービスに対するサイバー攻撃

2023 年



近年のクラウドストレージ導入の急速な増加は、いくつかの重要な動向とメリットに起因しています。

- **データの爆発的増大 :** 世界で生成されるデータ総量は指数関数的に増大しており、2015 年の 2 ゼタバイトから、2025 年には 181 ゼタバイトに達すると推定されています。このストレージの需要がクラウドの導入を後押ししています。
- **リモートワークとデジタルトランスフォーメーション :** パンデミック以来、リモートワークやクラウドベースサービスへの移行が加速し、クラウドストレージの利用はさらに増加しています。
- **コスト効率 :** クラウドストレージは、従来のオンプレミスインフラストラクチャよりも競争力のあるコストで、柔軟性と拡張性に優れたストレージオプションを提供しています。
- **アクセス性とコラボレーション :** クラウドストレージは、データのリモートアクセスとコラボレーションを容易にすることで、企業や個人にとっての魅力を高めています。

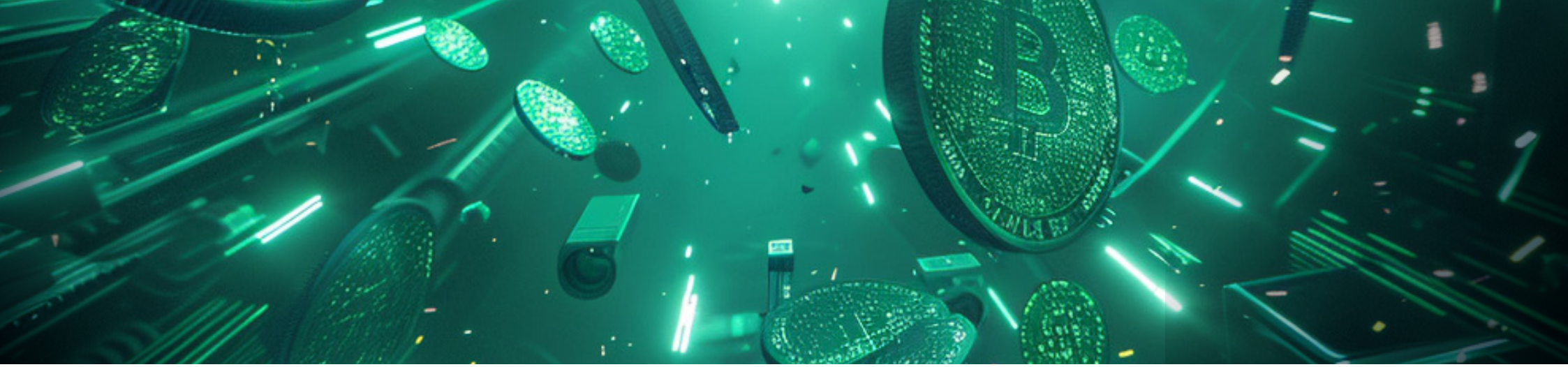
今後の展望

今後数年間、
クラウドストレージ市場は
力強い成長軌道を続けると
予想されており、
その規模は推定で

2029 年までに

3,700 億ドル

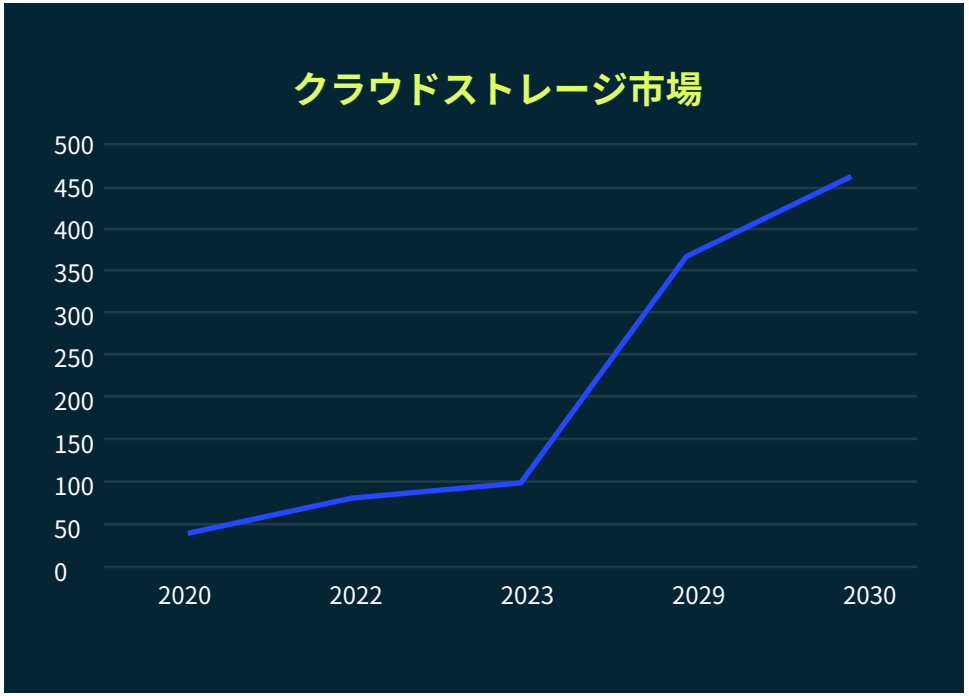
マルチクラウドの導入や
AI を活用したデータ管理
などの新しいテクノロジーが、
この状況をさらに後押し
していくと予想されます。



MITRE ATT&CK フレームワーク

クラウドストレージが至る所に存在するようになるにつれて、攻撃者は、設定ミスのある S3 バケットやその他の公開されているデータリポジトリを悪用しようと MITRE 手法を進化させています。以下に、クラウドストレージ分野で進化している主な MITRE 手法を紹介します。

- **偵察 (RECON):** 攻撃者は、公開状態の S3 バケットを自動化ツールでスキャンし、検索エンジンを悪用して、公開されているアクセス可能なデータを含むバケットを特定します。
- **リソースハイジャック (RHIJ):** 制限がかけられていない S3 バケットへのアクセスにより、攻撃者は、暗号通貨をマイニングしたり、DDoS 攻撃を仕掛けたり、クラウドでマルウェアをホストしたりすることができます。
- **水平移動 (LATERAL):** 1 つの S3 バケットへのアクセスを足がかりに、そこから AWS 環境内の他のクラウドリソースに移動して侵入することができます。
- **コマンドアンドコントロール (C2):** 攻撃者は、悪意のあるスクリプトや実行可能ファイルを S3 バケットに保存し、それらを使用して侵害したシステムを制御することができます。



動向

攻撃者は、新たな脆弱性や攻撃ベクトルを悪用して、Amazon S3 などのサービスに保存されているデータを侵害しています。以下に、この脅威情勢を形作っている主要な動向をいくつか紹介します。

- **更なる自動化 :** 攻撃者は、自動化されたツールやスクリプトを使用して、脆弱な S3 バケットを特定して悪用する傾向を強めています。
- **データの盗み出しに注力 :** 個人を特定できる情報 (PII) や財務情報を含む特定のファイルタイプを標的にすることが多い攻撃者にとって、その主な目的は依然として機密データの窃取です。アンダーグラウンド市場では、クラウドストレージからデータを窃取するためのツールやサービスが提供されており、脅威に晒される恐れがある、S3 バケットを含むクラウドストレージリストが公開されています。
- **マルチステージ攻撃 :** 攻撃者は、複数の MITRE 手法を組み合わせ、検知を回避して影響を最大化する高度な攻撃を仕掛けています。
- **サプライチェーン攻撃 :** クラウドストレージが統合されたソフトウェア市場を提供することから、S3 バケットと統合されたサードパーティのアプリケーションやサービスを標的にすることで新たな攻撃ベクトルが開かれています。
- **クラウドネイティブな攻撃 :** 特定のクラウド機能や API を悪用して S3 バケットを侵害する手法はますます巧妙になっています。
- **ランサムウェア :** S3 バケットに保存されたデータを暗号化して身代金の支払いを要求する手口はより大きな脅威となっています。
- **フィッシングとソーシャルエンジニアリング :** 標的型攻撃がより巧妙になり、ユーザーをだまして認証情報を開示させたり、アクセスを許可させたりしています。
- **コンテナ化された攻撃 :** クラウド環境でのマイクロサービスの展開に使用されるコンテナテクノロジーの脆弱性が悪用されています。

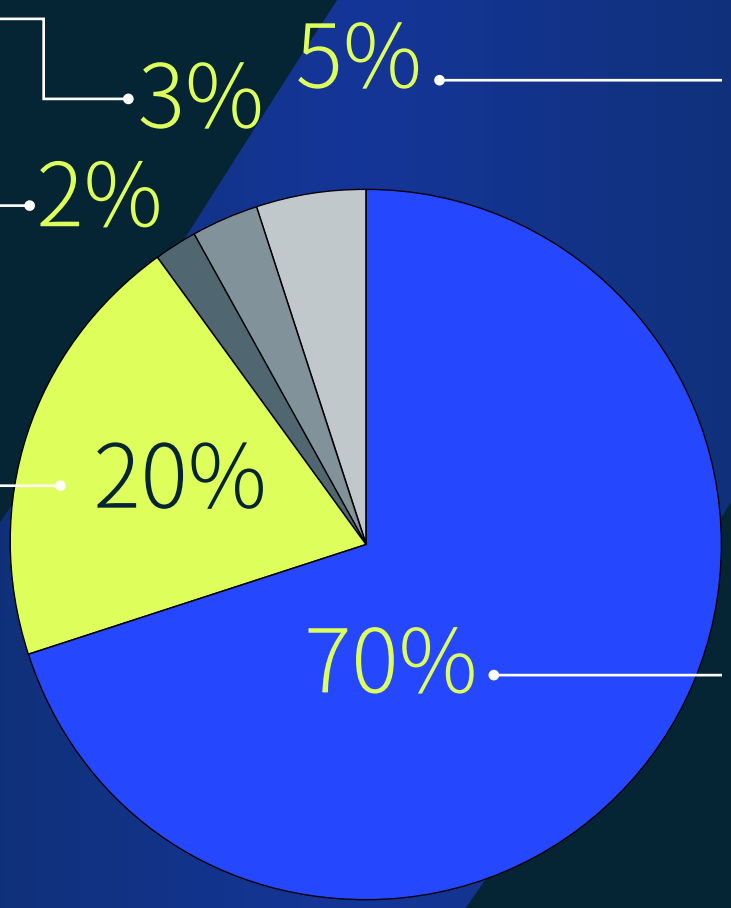
脅威情勢と脆弱性

クラウドストレージの脅威情勢には幅広い攻撃ベクトルがあり、攻撃者は設定ミス、脆弱性、その他の弱点を利用してデータを侵害します。最近の分析によると、攻撃を可能にする最も一般的な問題には次のようなものがあります。

サプライチェーン攻撃 (3%): クラウドストレージに接続されたサードパーティのアプリケーションやサービスの侵害が脅威の増大をもたらします。

標的型攻撃 (APT) (2%): 国家支援による攻撃者や巧妙化する犯罪組織による標的型攻撃は、発生頻度は低いものの重大な結果をもたらす可能性があります。

データ侵害 (20%): 内部関係者による脅威 (インサイダー脅威)、ソーシャルエンジニアリング、およびクラウドサービスの脆弱性は、データ漏洩につながる攻撃の約 20% を占めています。



ランサムウェア攻撃 (5%): クラウドストレージを標的としたランサムウェアはまだ初期段階にありますが、その数は増加しており、最近の攻撃の約 5% を占めています。

設定ミス (70%): 不適切なアクセス制御、古いソフトウェア、公開状態のバケットは、依然として最も頻繁に見られる脆弱性であり、クラウドストレージへの攻撃の約 70% でこれらが悪用されています。

クラウドストレージの脅威情勢

マルウェアの実行

S3 バケットは、実行のためではなく、主にストレージ用に設計されています。実行機能もわずかに存在しますが、その機能は限定的であり、複雑なマルウェア攻撃をサポートする可能性はほぼありません。しかし、オープンアクセスを許可するよう S3 バケットを誤って設定していたり、アクセス制御が不十分だったりすると、攻撃者がバケット内にマルウェアをアップロードして実行できることがあります。これには、AWS Lambda がサポートする Python や JavaScript などのスクリプト言語が使用されます。S3 バケットに関連付けられたサーバー側コードの脆弱性を悪用することで、攻撃者が悪意のあるコードを挿入し、バケットの環境内で実行できる可能性もあります。

最新のクラウドプロバイダーは、一般的に、環境内での悪意のあるコード実行の影響を制限できるセキュリティ対策とサンドボックスを実装しています。これにより、機密データを拡散したり機密データにアクセスしたりするマルウェアの能力を制限することができます。

マルウェアの配布

クラウドストレージでのマルウェアの配布にはさまざまな手法が使用されており、攻撃者はこれらを利用して、Amazon S3、Microsoft Azure Blob Storage、Google Cloud Storage などのプラットフォームを介して悪意のあるソフトウェアを拡散しています。以下に、最も一般的なマルウェアの種類を示します。

クリプトジャッキングマルウェア (50-60%):

- 金銭的利益を原動力とするクリプトジャッキングは顕著な脅威であり続けており、多くの場合、設定ミスのあるクラウドサーバーやコンテナ環境を利用してマイニングスクリプト (SIA など) を展開しています。
- 調査によると、これがクラウドストレージベースのマルウェアインシデントの大部分を占めています。

インフォスティーラー (20-30%):

- インフォスティーラーは金銭的利益やスパイ活動のために機密データを標的としており、システムを侵害した後、クラウドストレージを利用してデータを流出させます。
- このマルウェアの蔓延は、個人データや組織データの価値が高まっていることを示しています。

ランサムウェア (10-15%):

- ランサムウェア攻撃では、価値のあるデータが当該環境に集中しているという理由から、クラウドストレージが標的となることが増えています。
- クリプトジャッキングほど頻繁には発生しませんが、その影響は破壊的であり、重大な懸念事項となっています。

その他の種類 (5-10%):

- バックドア、ボットネットマルウェア、および破壊的なマルウェアは、クラウドストレージをベースに配布されるマルウェアのごく一部にすぎません。
- その出現と蔓延は、特定の動向や攻撃者の動機によって変化します。

暴かれたバケット

前出のツールを使用すれば、バケットのリストをスキャンしてファイルを取得し、設定ミスのある公開バケットを特定することができます。以下は、GrayHat Warfare による 2018 年から 2023 年にかけてのスキャンの結果です。

ファイル
27 億 /112 億

Amazon Web Services
4 万 800/31 万 2,000

Azure Blob Storage
4 万 4,600/5 万 400

Digital Ocean Spaces
7,000

Google Cloud Platform
3 万 2,800/7 万 2,500

Censys と専用ツールを併用してスキャンすることで、既存のバケットの最新リストを提供できます (以下の例を参照)。

```
exists    | assets.cable.co.uk | eu-west-1 | AuthUsers: [] | AllUsers: [READ, READ_ACP]"
exists    | ga-na-prod-norad-common-templates.prd-na-onega.wkgposvc.cloud | us-east-1 | AuthUsers: [] | AllUsers: [READ]"
exists    | assets.bankspower.com | us-east-1 | AuthUsers: [] | AllUsers: [READ]"
exists    | file.epdata.es | eu-west-1 | AuthUsers: [] | AllUsers: [READ]"
exists    | cdn.blisnetsurgeons.com | us-west-2 | AuthUsers: [] | AllUsers: [READ_ACP]"
exists    | cdn.theartsdesk.com | eu-west-1 | AuthUsers: [] | AllUsers: [READ_ACP]"
exists    | cdn.sixthman.net | us-east-1 | AuthUsers: [] | AllUsers: [READ]"
exists    | images.dealertrend.com | us-east-1 | AuthUsers: [] | AllUsers: [READ]"
exists    | photos.ahmadiah-idrisiah.com | us-east-1 | AuthUsers: [] | AllUsers: [READ]"
exists    | s3.ebook-bargains.com | us-east-1 | AuthUsers: [] | AllUsers: [READ]"
exists    | image.prd.kfh.artirix.com | eu-west-1 | AuthUsers: [] | AllUsers: [READ]"
exists    | iptvtest.marlin-tmo.com | us-east-1 | AuthUsers: [] | AllUsers: [READ_ACP]"
exists    | media.saffronart.com | us-east-1 | AuthUsers: [] | AllUsers: [READ]"
exists    | ga-na-qa-norad-common-templates.qa-na-onega.wkgposvc.cloud | us-east-1 | AuthUsers: [] | AllUsers: [READ]"
exists    | static.tapp.co | us-east-1 | AuthUsers: [] | AllUsers: [READ]"
exists    | download.virtualworks.com | us-east-1 | AuthUsers: [] | AllUsers: [READ_ACP]"
```

一般公開されているツール

- サブドメイン内の設定ミスのある S3 バケットの探索 : https://github.com/suvendu-dash/misconfig-s3-bucket
- S3 バケットの権限の確認 : https://github.com/clario-tech/s3-inspector
- 企業秘密、デジタル資産、およびその他の機密情報を探す S3 バケットインスペクター : https://github.com/redhuntlabs/BucketLoot
- アラートや侵入テストフレームワークを回避するためのバイパス機能を備えた、他の多くのスキャナー、スクレイパー、およびブルートフォース攻撃ツール (Spartan、gobuster)
- 一般公開されているツールの完全なリスト : https://github.com/mxm0z/awesome-sec-s3

サイバー攻撃

クラウドの設定ミスは、過去数年にわたってデータ侵害の主な原因となってきました。2017 年には、設定ミスのある S3 バケットが保護されていない状態に置かれ、Alteryx の機密性の高い顧客データが漏洩しました。2019 年には、ハッカーが S3 バケットの脆弱性を悪用し、何百万もの顧客のクレジットカードアプリケーションにアクセスしたことで、Capital One が大規模な侵害に見舞われました。さらに 2021 年、ハッカーは AWS API を呼び出して保護されていない S3 バケットをスキャンし、アクセスした後、防犯カメラメーカーの Verkada を侵害しました。

根本原因はさまざまですが、共通しているのは、クラウドストレージの設定ミスによって機密データが繰り返し大量に漏洩しているということです。残念なことに、人々の意識が高まっているにもかかわらず、このような事件は後を絶ちません。最近では、2023 年 10 月にインドの国家物流ポータルが S3 バケットを公開状態のまま放置し、貿易データと個人データが侵害を受けました。

S3 バケットに関連する既知の漏洩事案

日付	概要	補足
2023 年 10 月	インドの国家物流ポータル、機密個人データと貿易記録が流出	機密性の高い個人データとさまざま国家貿易および民間貿易の取引記録が漏洩
2022 年 8 月	クラウド設定ミスで Amazon S3 バケットに 3TB の空港機密データが流出：" 人命の危機 "	保護されていないサーバーから、空港職員の身分証明書の写真やその他の個人情報を含む 150 万を超えるファイルが漏洩
2022 年 7 月	マクグローヒルの S3 バケットから 10 万人の生徒の成績と個人情報が流出	22 TB のデータと 1 億 1,700 万を超えるファイルが漏洩
2020 年 8 月	S3 バケットでの情報流出、米国とカナダの高齢者データ 182GB が流出	消費者評価レビューサイトの SeniorAdvisor が所有する S 3 バケットで設定ミス
2020 年 7 月	Twilio：" 誰かが私たちの安全でない AWS S3 に侵入し、私たちの JavaScript SDK に「悪意のない」コードを追加した "	攻撃者が、S3 バケットでホストされている JavaScript ライブラリの更新と他のクライアントによる取得を試行
2020 年 1 月	" 暴露された AWS バケットが複数のデータ漏洩に再び関与 "	英国で働く何千人ものコンサルタントに関連するパスポートスキャン、税務書類、身元確認、求人応募、経費請求、契約、メール、および給与明細の情報が漏洩

日付	概要	補足
2020 年 6 月	"720 万件の記録が流出したが、BHIM アプリからの流出ではない "	保護されていない S3 バケットから BHIM のユーザーデータが漏洩
2018 年 10 月	MedCall が設定ミスしたデータベース侵害で数千件のアドバイザーの患者ファイルが流出	氏名、メールアドレス、住所、電話番号、生年月日、社会保障番号を含むデータベースと、患者の評価や医師との会話の記録、投薬、アレルギー、その他の詳細な個人の健康データを含むファイルが漏洩
2019 年 1 月	フォーチュン 100 社における AWS S3 サーバーからのデータ流出：フォード、ネットフリックス、TD 銀行	世界の大手企業にデータ管理、データウェアハウス、データ複製のサービスを提供するイスラエルの IT 企業 Attunity が、パスワード保護なしで 3 つの Amazon S3 バケットをインターネット上に公開し、顧客データの一部を漏洩
2018 年 3 月	医療記録と患者と医師の記録データが流出	181 の事業所の従業員情報と約 3,000 人の 個人情報が、Medcall Healthcare Advisors が所有する保護されていない S3 ストレージバケットから漏洩
2018 年 3 月	宝飾品サイトが誤って 130 万人分の個人情報（平文のパスワード含む）を流出	住所、郵便番号、メールアドレス、IP アドレス、さらにはプレーンテキストのパスワードを含むデータベースバックアップファイルが漏洩
2018 年 2 月	世界に丸見えだった S3 バケット：Octoly	本名、住所、電話番号、メールアドレスが判明
2017 年 12 月	Alteryx、S3 バケットを匿名ユーザーに開放：1 億 2,000 万世帯のアメリカ人の情報が晒される	自宅の住所、連絡先情報、住宅ローンの状況、財務履歴が漏洩
2017 年 11 月	ナショナル・クレジット・フェデレーションの 111GB の社内顧客情報流出 - フロリダ州タンパを拠点とする信用調査サービス	SSN、運転免許証、信用報告書などが漏洩
2017 年 11 月	Uber のハッキング、数百万件の記録が明るみに (最初の情報漏洩から数ヵ月後)	5,700 万人の Uber ユーザーの個人情報と運転免許証の番号が漏洩 (最初の攻撃自体は数か月前に発生)
2017 年 11 月	NSA 情報流出、陸軍の情報システム " レッドディスク " の失敗を暴露	陸軍諜報プロジェクト (コードネーム「Red Disk」) の 100 ギガバイトのデータが漏洩。リストには掲載されていないものの、ディスクイメージが公開された AWS ストレージサーバー上にパスワード保護なしで残され、誰でもダウンロードできるようになっていた

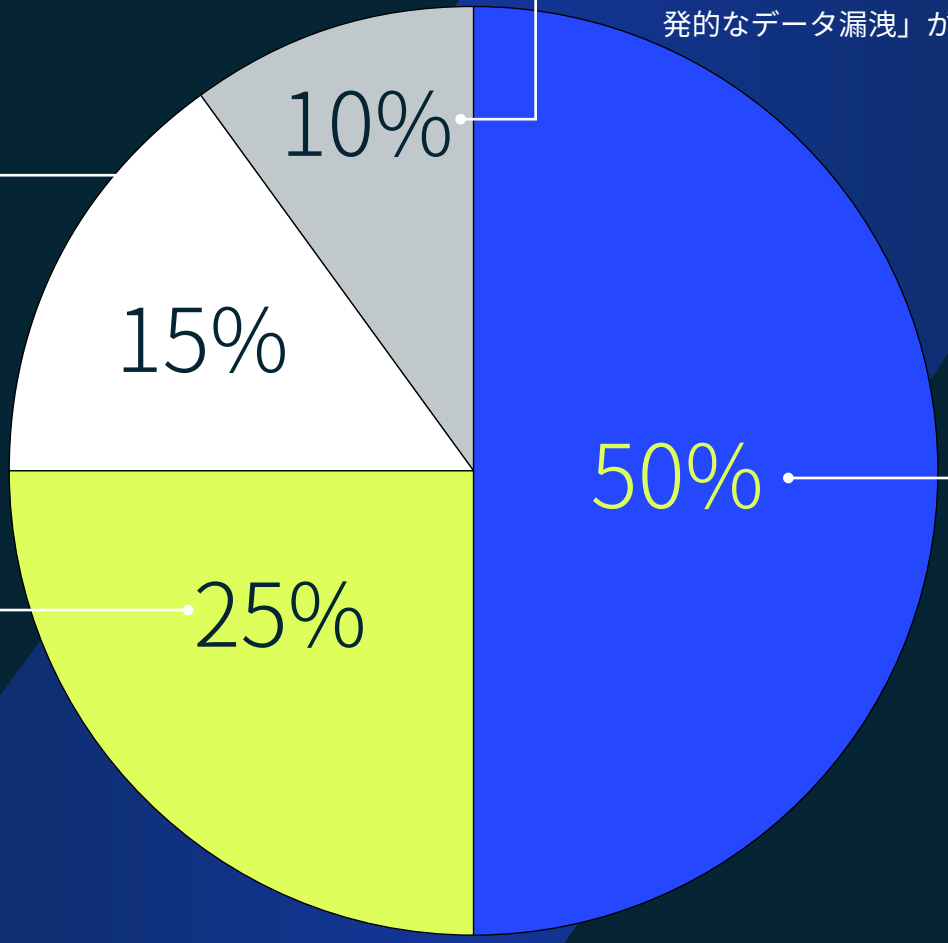
攻撃グループ

クラウドストレージを標的とする攻撃グループの種類はとりわけ数多くあります。以下に、主な脅威グループの種類について説明します。

内部脅威 (10%): 個人的な利益や復讐を動機とする、あるいは単なる不注意を原因とする内部脅威には、従業員、請負業者、またはクラウドストレージへのアクセスが許可されたサードパーティベンダーなどが関係しています。悪意のある人物によってデータが窃取されたり、システムが妨害されたり、攻撃者にアクセス権が販売されたりする可能性があります。場合によっては、誤って設定されたアクセス権や安全でないアクセス方法を使用してユーザーが機密データを不注意で共有した際の「偶発的なデータ漏洩」が原因となることもあります。

ハクティビスト (15%): イデオロギー的または政治的な動機に基づいて活動するこれらの攻撃者は、クラウドストレージを標的として、業務を妨害したり特定の事由に対する人々の関心を高めたりします。サービス拒否攻撃が仕掛けられたり、クラウドでホストしている Web サイトが改ざんされたりする可能性があります。

国家支援による攻撃者 (25%): スパイ活動や地政学的な意図に基づいて行動するこれらの攻撃者は、クラウドストレージを標的として、機密情報を窃取したり重要インフラを混乱させたりします。多くの場合、その攻撃は非常に洗練されており、標的が絞られています。



サイバー犯罪者グループ (50%): 金銭的利益を動機とするこれらのグループは、多くの場合、自動化ツールを使用して設定ミスのあるクラウドストレージバケットをスキャンし、脆弱性を悪用してデータを窃取します。その後、窃取したデータをダークウェブで販売したり、ランサムウェア攻撃に利用したりする可能性があります。

脅威グループの種類

脅威グループの活動事例：TeamTNT

TeamTNT はこれまで、クラウドストレージ環境を標的として、主に設定ミスのある Kubernetes クラスター、Docker API、Kubernetes UI ツール、Redis サーバー、および AWS S3 バケットを集中的に攻撃してきました。TeamTNT は、これらのプラットフォームを利用してクリプトジャッキングを実行したり、被害者の環境に暗号通貨マイナーを展開したり、後の攻撃で使用するために認証情報を窃取したりすることで知られています。

既知のエクスプロイトのタイムライン:

- **2020-2021:** TeamTNT は、クラウド環境の脆弱性を積極的に悪用し、クリプトジャッキングマルウェアを展開して、アクセス認証情報を窃取していました。特に、公開された Docker API や設定ミスのある Kubernetes インストールを標的にしたことで有名です。

- **2021-2023 (AWS にフォーカスした活動):** 2021 年 11 月、TeamTNT は Twitter で事実上の「引退」を発表しました。しかし研究者たちは、2022 年から 2023 年にかけて、AWS S3 バケットや Docker 環境を標的とした同様のマルウェアキャンペーンが展開されていたことを確認しています。これらのキャンペーンでは AWS の認証情報が搾取されており、これは同じ脅威グループ、あるいは同様の戦術を利用した模倣犯による活動の可能性を示唆しています。

- **2023 年 6 月 :** SentinelOne と Permiso は、AWS だけでなく Azure および Google Cloud Platform (GCP) サービスの認証情報の窃取にも焦点を当てた、TeamTNT と同様のツールを使用した悪意のある攻撃者のキャンペーンについて報告しました。

クラウドストレージを保護するためのベストプラクティス

クラウドストレージを安全に保持するための最低限のベストプラクティスには、次のものがあります。

- **最小権限のアクセス制御を実装する：**S3 バケットへのアクセスを、許可されたユーザーとアプリケーションに制限します。
- **バケットの暗号化を有効にする：**保存中および転送中のデータを暗号化して、不正なアクセスから保護します。
- **強力なパスワードと IAM ロールを使用する：**認証情報はハードコードせず、アクセス制御に IAM (Identity and Access Management) ロールを利用します。
- **アクセスログとアラートを監視する：**アクセスログを定期的に確認して、不審な活動にはアラートを設定します。
- **定期的なセキュリティ評価を実施する：**攻撃者に悪用される前に、S3 バケットの脆弱性を特定して対処します。
- **セキュリティのベストプラクティスについてユーザーを教育する：**フィッシングに対する認識、安全なパスワード管理、責任あるクラウドストレージの使用についてユーザーにトレーニングを行います。
- **高度なウイルススキャナーでクラウドストレージをスキャンする：**Deep Instinct のプラットフォームに代表される予防型データセキュリティのソリューションを導入し、脅威の侵入を監視します。

まとめ

AWS S3 の拡張性に優れたストレージは、コアビジネスプロセスにとって極めて重要なものですが、予期せぬ脆弱性をはらんでいます。進化する脅威情勢を理解し、ベストプラクティスを導入し、堅牢なセキュリティ制御を実装することで、組織はサイバー攻撃のリスクを大幅に削減し、クラウド内の機密データを保護することができます。

參照資料

- https://conscia.com/blog/cloud-storage-risk-assessment-our-privacy-rests-at-risk/
- https://www.einnews.com/pr_news/673477280/global-cloud-storage-market-projects-substantial-growth-set-to-reach-206-61-billion-by-2027
- https://www.fugue.co/blog/a-technical-analysis-of-the-capital-one-cloud-misconfiguration-breach
- https://github.com/nagwww/s3-leaks
- https://www.sisainfosec.com/weekly-threat-watch/new-supply-chain-attack-exploits-abandoned-aws-s3-buckets/#:~:text=New%20supply%20chain%20attack%20exploits%20abandoned%20S3%20buckets%20to%20distribute,without%20altering%20the%20modules%20themselves.
- https://checkmarx.com/blog/hijacking-s3-buckets-new-attack-technique-exploited-in-the-wild-by-supply-chain-attackers/
- https://buckets.grayhatwarfare.com/
- https://github.com/mxm0z/awesome-sec-s3