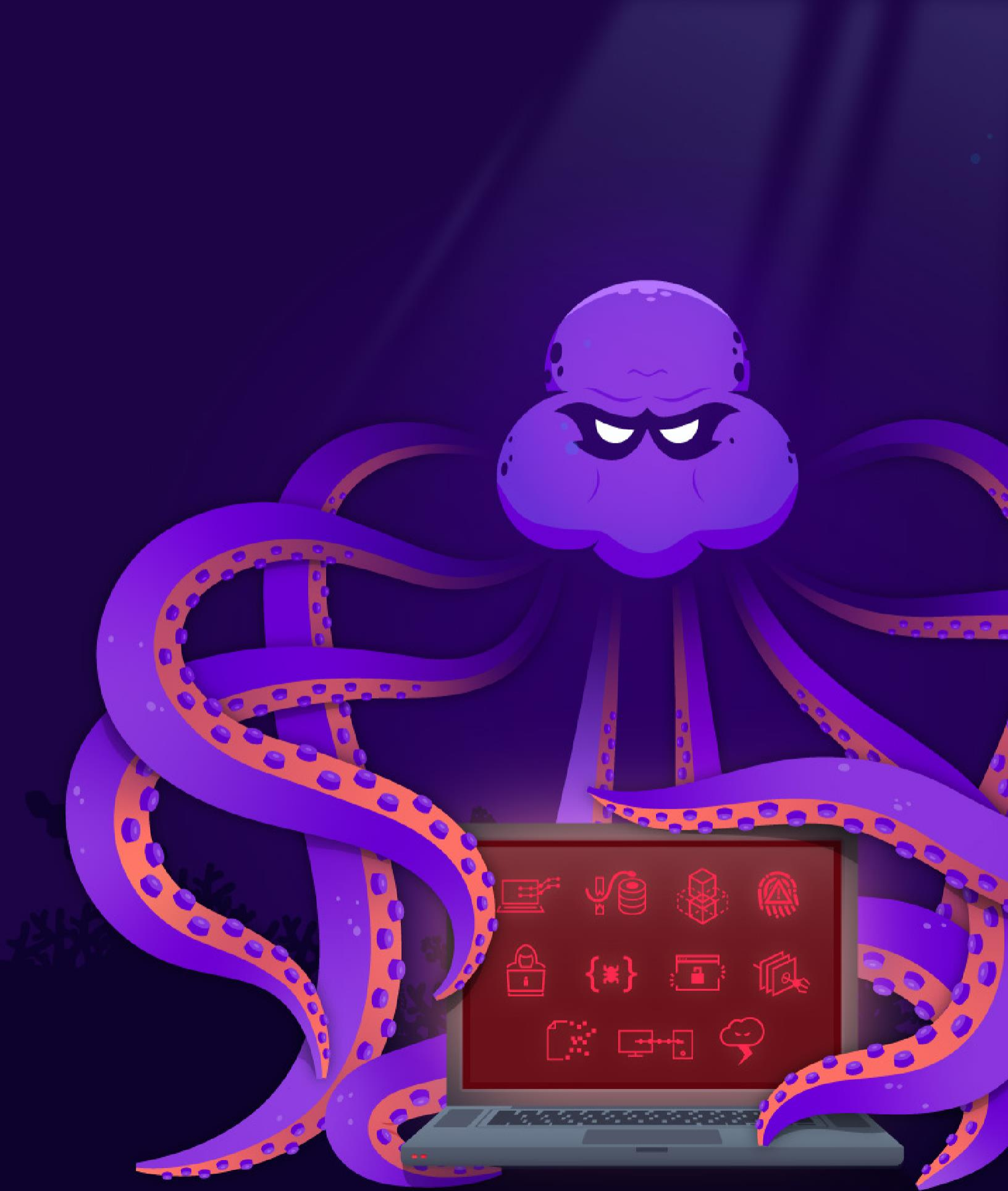
クラウドコンピューティングの重大脅威：

11の悪質な脅威ディープダイブ

CSAJC cloud security alliance℠ Japan Chapter

CSA cloud security alliance®



「11の悪質な脅威：クラウドコンピューティングの重大脅威」のためのケーススタディ分析とセキュリティ業界の侵害分析

Working group community may be found here: https://circle.cloudsecurityalliance.org/community-home1?CommunityKey=202830f1-b186-4b55-8c48-f1f2e38c7151

Forward

Top Threats Working Groupについて

かつてない速さで、クラウドコンピューティングはビジネスと政府を同時に変革し、新たなセキュリティの課題を生み出しました。クラウドサービスモデルの発達は、これまで以上に効率的にビジネスを支えるテクノロジーをもたらしました。従来のクライアント/サーバー型からサービスベースのモデルへの移行は、テクノロジー部門がコンピューティング技術やアプリケーションについて考え、設計し、提供する方法を変革しつつあります。しかし、クラウドコンピューティングの進歩により提供される価値が向上した一方で、新たなセキュリティ上の脆弱性が発生しており、その影響力がまだ十分には明らかになっていないセキュリティ課題も含まれています。"CSA Top Threats Working Group" は、クラウドの導入戦略に関して、リスク管理の知識に基づいた意思決定を行うために、クラウドセキュリティのリスク、脅威、脆弱性に関して、専門家による最新の見解を提供することを目的としています。"

Case Study Projectの成り立ち

2019年のBlack Hat USAカンファレンスにて、クラウドセキュリティアライアンス（CSA）は、クラウドコンピューティングの最も重要かつ喫緊の課題を明確にするために、2年ごとに調査レポートを更新したことを発表しました。2010年以来、CSAの「クラウドの重大セキュリティ脅威」レポートは、クラウドにおける最新の脅威、リスク、脆弱性に関する貴重な業界の洞察を提供することで、大きなギャップを埋めてきました。しかし、セキュリティ専門家は、レポートの中の重大なクラウドの懸念事項は、全体像のほんの一部を指摘しているに過ぎないことを認識しています。その他の考慮すべき要素としては、アクター、リスク、脆弱性、実世界の攻撃や侵害による影響などがあります。これらの不足している要素に対処するために、Cloud Security Alliance Top Threats Working Groupでは、アーキテクチャ、コンプライアンス、リスク、および緩和策に関係するより技術的な詳細を説明しています。重大脅威ディープダイブドキュメントの作成では、CSA 重大脅威の中で明らかにされたエピソードやケーススタディの限界に対処し、追加の詳細と実行可能な情報を提供しています。このデータによって、教訓と緩和策の概念が実世界のシナリオにどう適用できるかを明確に理解しつつ、CSAの重大脅威がより大きなセキュリティ分析のどこに、どのように適合するかを確認できることが理想です。

Top Threats Working Groupの最近の寄稿

「重大脅威ディープダイブ 2020」では、「11の悪質な脅威」の調査結果に関連する課題の例を複数挙げています。これらのエピソードは、サイバーセキュリティ管理者が幹部や同僚とのコミュニケーションを円滑にすることや、技術スタッフとの議論のコンテキストを提供することを可能にしますが、セキュリティ分析の観点から、緩和策や対策を実装するための詳細な情報を提供するものではありません。

謝意

このケーススタディでは、「重大脅威ディープダイブ」の基礎として引用されている9つの実際の攻撃や侵害を使ったセキュリティ分析に関して、CSA重大脅威の点と点を結びつけることを試みています。9つの事例は、それぞれが（1）参考図表 と (2)詳細説明 の形式で紹介されています。参考図表のフォーマットは、脅威や脆弱性からエンド・コントロールや緩和策に至るまで、アクターの攻撃スタイルの概要を提供します。

私たちは、アーキテクトやエンジニアに対して、自組織における分析や比較を行うための出発点として、この情報を利用することをお勧めします。詳細説明の長い記述は、追加の文脈（事件がどのようにして起こったか、どのように対処すべきであったかなど）と、さらなる研究のためのリファレンスを提供します。影響や緩和などの詳細が公表されていないケースについては、想定される結果や可能性も含まれています。

あなたにとってこの取り組みが有用であることを願います。また、フィードバックや今後の出版物への参加をお待ちしております。

あなたの将来の成功に向けて

Jon-Michael C. Brook, CISSP, CCSK
Chair, Top Threats Working Group

Acknowledgments

Top Threats Working Group Co-chairs

Jon-Michael C. Brook

Lead Authors

Suhas Bhat
Jon-Michael C. Brook
Begum Calguner
Tal Eliyahu
Alex Getzin
Vic Hargrave
Ebudo Osime
Michael Roza
John Yeoh
Nabeel Yousif

Key Contributors

Prabu Natarajan
Brian Kinsley
Frank Guanco

CSA Staff

Sean Heide (Analyst)
Stephen Lumpe (Cover Design)
AnnMarie Ulskey (Layout Design)

目次

日本語版提供に際しての告知及び注意事項

本書「クラウドコンピューティングの重大脅威: 11 の悪質な脅威 ディープダイブ」は、Cloud Security Alliance (CSA)が公開している「Top Threats to Cloud Computing: Egregious Eleven Deep Dive」の日本語訳です。本書は、CSA ジャパンが、CSA の許可を得て翻訳し、公開するものです。原文と日本語版の内容に相違があった場合には、原文が優先されます。
翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSA ジャパンは何らの保証をするものではありません。
この翻訳版は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。

変更履歴

日付	バージョン	変更内容
2020 年 11 月 25 日	日本語版 1.0	初版発行

CSAジャパン成果物の提供に際しての制限事項

日本クラウドセキュリティアライアンス（CSA ジャパン）は、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

１．　責任の限定

CSA ジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。

(1) 本書の内容の真正性、正確性、無誤謬性
(2) 本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと
(3) 本書の内容に基づいて行われた判断や行為がもたらす結果
(4) 本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

２．　二次譲渡の制限

本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。

ただし、以下の場合は本項の例外とします。

(1) 本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。
(2) 本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。
(3) CSA ジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。
(4) 転載、再掲、複製の作成と配布等について、CSA ジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

３．　本書の適切な管理

(1) 本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。
(2) 本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する（組織内の利用者に順守させることを含む）ようにしなければなりません。
(3) 本書をダウンロードした者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。
(4) 本書を印刷した者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

４．　原典がある場合の制限事項等

本書が Cloud Security Alliance, Inc.の著作物等の翻訳である場合には、原典に明記された制限事項、免責事項は、英語その他の言語で表記されている場合も含め、すべてここに記載の制限事項に優先して適用されます。

５．　その他

その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSA ジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、info@cloudsecurityalliance.jp までお願いします。

日本語版作成に際しての謝辞

「クラウドコンピューティングの重大脅威: 11 の悪質な脅威 ディープダイブ」の日本語訳は、CSA ジャパン会員の有志により行われました。
作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。
以下に、翻訳に参加された方々の氏名を記します。（氏名あいうえお順・敬称略）

伊賀　誠
井上　淳
上田　将司
小野　貴博
金田　祐加子
昆　　資之
神保　冬和子
高瀬　一彰
成川　達也
成田　和弘
松浦　一郎
満田　淳
諸角　昌宏
山澤　昌夫
山下　亮一
渡邉　浩一郎

重大脅威 EE:DDの分析

ケーススタディによる「重大脅威」のカバレッジ

Top Threats Item #	Capital One	Disney+	DowJones	Github	Imperva	Ring	Tesco	Tesla	Zoom
EE 1									
EE 2									
EE 3									
EE 4									
EE 5									
EE 6									
EE 7									
EE 8									
EE 9									
EE 10									
EE 11									

所見

9つのディープダイブケーススタディは、11の悪質な脅威のすべての要素をカバーしています。(EE:DD)

各ケーススタディに推奨されるCloud Controls Matrix (CCM)ドメイン:

CCM Control Domain	Capital One	Disney+	Dow Jones	Github	Imperva	Ring	Tesco	Tesla	Zoom
AIS		X			X		X		
AAC			X	X		X	X		
BCR		X		X					
CCC	X				X		X	X	
DSI	X				X	X			
DCS						X			
EKM					X		X	X	
GRM	X	X			X				X
HRS	X	X	X				X	X	X
IAM	X	X	X		X	X	X	X	X
IVS	X	X		X	X			X	X
IPY									
MOS									
SEF	X	X	X	X		X	X	X	X
STA			X		X	X	X		
TVM	X	X			X	X	X	X	X

所見

9つのケーススタディに適用される緩和策とコントロールは、Cloud Controls Matrix（CCM）の16ドメインのうち13ドメインをカバーしている。データセンターサービス（DCS）と相互運用性と移植性（IPY）の内容は、主にクラウドサービスプロバイダー施設でのデータセンター運用を対象としており、ケーススタディやクラウドコンピューティング向けの「重大脅威」には合致しない。モバイルセキュリティ（MOS）のコントロールは、モバイルエンドポイント保護に関連して使用され、エンタープライズ環境で一般的に使用される防止策が含まれています。

ケーススタディとCCMコントロールの関連性

CCM Control	Capital One	Disney+	Dow Jones	Github	Imperva	Ring	Tesco	Tesla	Zoom
IAM	3	2	2		1	1	1	1	4
SEF	4	1	1	2		4	1	2	2
TVM	1	1			1	1	1	2	2
HRS	1	1	1				2	1	1
IVS	3	1		2	4			1	1
CCC	1				1	1	1	2	
AAC			2	2		1	1		
GRM	2	1			1				1
STA			2			4	3		
AIS		1			1		1		
DSI	1				1				
EKM					1		1	1	
BCR		1		1					
DCS									
IPY									
MOS									
Total Controls	16	9	8	7	11		12	10	11

所見

上の表のドメインは、各ドメインの緩和管理策が関連する頻度が高い順に並べ替えられています。

本年の報告書では、アイデンティティとアクセス管理（IAM）のコントロールが最も関連性の高い緩和策であり、9件のケーススタディのうち8件を占めています。攻撃の影響を受けた場合の計画策定とその計画の実行を含む、セキュリティインシデント管理、e-ディスカバリ、クラウドフォレンジック（SEF）が、引用されたすべてのインシデントのうち1件を除き、インシデントへの対応を成功させるために最も重要でした。IAMとSEFはそれぞれ17コントロールを占めていました。

脅威と脆弱性管理（TVM）は、2番目のディープダイブである脆弱性とパッチ管理（TVM-02）で高得点を獲得しており、これらのインシデントで悪用された脆弱性の多くを防止するのに役立つでしょう。いまだに、1988年のMorris Wormの発生を受けIT業界にて推奨されるようになったセキュリティパッチのプロセスは適正に実行されていません。

Capital One

脅威アクター	脅威	脆弱性	テクニカルインパクト	ビジネスインパクト	コントロール
内部要因: 経験の少ないクラウドアーキテクト、経験の少ないソリューションアーキテクト	**EE1** *データ侵害:* 1億600万人の顧客口座から窃取された機微な情報	**EE 2** *設定ミスと不適切な変更管理-* ModSecurity Web アプリケーションファイアウォール（WAF）がサーバサイドリクエストフォージェリ（SSRF）を許容	**EE9** *メタストラクチャとアプリストラクチャの障害:*デフォルトのハイパーバイザの信頼関係がサービスの検出と問い合わせを許容。	**財務面** - 通知に1億5000万ドル（推計） - 株価の6.9%下落 - 規制当局による罰金の可能性	**予防** - DSI-02 - GRM-01 - IAM-02 - IVS-13 - SEF-01
	EE11 *クラウドサービスの悪用・乱用・不正利用:身元を偽装するためにVPNおよび匿名ネットワークサービスを使用*	**EE4** *ID、資格情報、アクセス、鍵の不十分な管理:* WAFとストレージに対するEC2及びS3のロールの過度の割り当て	過度な権限を与えられたクラウドアプリケーションにより、保護されたクラウドストレージの公開と大量のデータへのアクセスを許容	**運用面** - インシデントレスポンス - フォレンジック調査 - 影響を受けた関係各所への連絡	**検知** - CCC-03 - GRM-02 - IAM-13 - IVS-01
外部要因: *EE5* *内部者の脅威 - AWSの運用に関する深い知識を持ち、信頼のあった元CSPの内部関係者*	**複雑な環境** 正しい実装及び設定に関する判断をするための高度な知識の必要性	**EE8** *弱い管理プレーン -* AWSがメタデータへの問い合わせを許容 **EE10** *クラウド利用の可視性の限界 -* AWS IMDS v1のSSRF攻撃に対する脆弱性が未知または未対応	クレジット申し込み情報から1億600万人分の個人識別情報（PII）が漏洩	**コンプライアンス** - 機微な情報の漏洩 - 集団訴訟 - 議会による調査 - 通貨監督庁（OCC）による8000万ドルの罰金 **評判** - CSPの信頼喪失 - 長期的な株価	**是正** - HRS-09 - IAM-07 - IVS-06 - SEF-02 - SEF-03 - SEF-04 - TVM-02

攻撃の詳細

アクター:プラットフォームの脆弱性について内部的な知識を有する元AWSのエンジニアが、保護されたクラウドフォルダから機微な情報を抽出するために設定ミスのあるWebアプリケーションから認証情報を取得しました。
攻撃: オープンソースの匿名ネットワーク（Tor）とVPNサービス（iPredator）が攻撃者の発見を困難にした。Capital One が AWSクラウドの運用に利用していた設定ミスのある ModSecurity WAF は 資格情報を含む AWS クラウドメタデータサービスをクラウドインスタンスに中継していました。そしてWAFに対して与えられた過度のアクセス権限が、同期データの読み取りと機微な情報の窃取を可能とし、保護されたクラウドストレージ（AWS S3バケット）へ攻撃者がアクセスする原因となりました。
脆弱性:プラットフォーム上のサーバーサイドリクエストフォージェリ（SSRF）脆弱性により、攻撃者からのリクエストが偽装され、サーバー（例えばCapital OneのWAFなど）が外部にアクセスするときに使われる認証情報を含むクラウドサーバの設定情報（EC2メタデータサービスなど）にアクセスされました。

テクニカルインパクト

情報漏洩: WebアプリケーションがIAM認証情報のために侵害され、複数のクラウドフォルダへのアクセスが行われた。アクセスされたクラウドフォルダは盗み出された1億600万人の顧客情報の読み取り権限がありました。
データ損失: 漏洩したデータは2005年から2019年の間のクレジットカード申し込み情報とクレジットカード顧客のステータスレポートだった。申し込み情報からの個人識別情報（PII）には、申し込み者名、住所、郵便番号、電話番号、メールアドレス、誕生日、申告された収入情報が含まれていました。クレジットカード顧客PII及び財務情報にはクレジットスコア、利用限度額、利用残高、支払い履歴、連絡先、社会保障番号、紐づけされた銀行口座が含まれており、およそ14万件の社会保障番号、8万件の担保付クレジットカードに紐づけられた銀行口座番号が漏洩しました。

ビジネスインパクト

財務: 顧客の銀行口座情報の漏洩は、顧客に経済的損失、金融機関に保険料による損失を与える可能性があrます。1億600万人への影響に関し、顧客のクレジットカードの利用状況の監視、IDの復旧サービス、詐欺などの顧客情報の悪用などに対応するため、OCCによる8000万ドルの和解が行われました。このほかに規制条項への違反が罰金につながる可能性があります。罰金や懲罰金の支払いの増加により収益に影響が出た場合には株価への影響も予想されます。
運用: インシデントレスポンスと追加の法的捜査、セキュリティスタッフの変更と再教育、リスクアセスメント及び脆弱性診断とアプリケーションの再設定、顧客への連絡と通常のビジネスオペレーションへの影響。
コンプライアンス: 顧客のPIIの漏洩はGDPRや他のプライバシー規制の違反とみなされた場合、懲罰金などの制裁が科されます。また、金融サービスなどの高度に規制された産業では顧客の保護を目的に厳しい制裁を含む監督が行われます。例えばEquifaxは2017年に1億4700万人の顧客情報の漏洩で米FTC(連邦取引委員会)から5億7500万ドルの罰金を科されます。
評判: 顧客及び申込者の情報の漏洩により、Capital Oneの顧客と一般からの信頼に影響が出ることが予想されています。このため、事件後3年間、新規顧客が減少することにより収益が減少することが見込まれます。またCISOの交代と十数名のセキュリティプロフェッショナルの退職により、内部の評価が損なわれました。

予防的緩和策

DSI-02: *データの管理表とフロー* – インベントリ、文書化及びデータフローの維持により、古くなった顧客情報の特定と、安全なアーカイビングと破棄、廃棄を確立します。
GRM-01: *ベースライン要件* – 確立したセキュリティ要件はベースライン構成からの逸脱を防ぎ、アプリケーションの実装と利用の前に脆弱性を特定します。
IAM-02: *資格証明のライフサイクル/プロビジョニング管理*– 適切なポリシーと手順、プロセスと手段は、クラウドフォルダや機微な情報への過度なアクセスといった必要以上の権限の付与を防ぎます。
IVS-13: *ネットワークアーキテクチャ*– アーキテクチャ図とデータフローはネットワークへの侵入とデータ侵害の速やかな検知と対応に有用です。
SEF-01: *監督当局との連絡体制の維持* – 侵害が起こった場合、すぐにコンプライアンス対応とフォレンジック調査ができるよう、規制当局及び法執行機関の連絡窓口を準備します。

検知的緩和策

CCC-03: *品質テスト*– そのシステムとサービスの機密性・完全性・および可用性に影響を与えるアプリケーションの設定ミスについて品質変更管理とテストは確立されています。
GRM-02: *データフォーカスリスクアセスメント*– データに着目したアセスメントにより、適切または不適切な利用、保管、廃棄、機微な情報へのアクセスを検出します。
IAM-13: *ユーティリティプログラムアクセス*– AWSサーバーのSSRF攻撃に対する脆弱性を特定し、IMDSメタデータの悪用を抑制します(AWS IMDSv2はこのタイプのSSRF攻撃の発生に対する修正を行っています)。
IVS-01: *監査ログ / 侵入検知* – セキュリティ侵害行為の調査のために、適切なログ管理による疑わしいネットワーク上のふるまいの検知や、ファイル完全性の異常が記録されています。

是正的緩和策

HRS-09: *訓練/認識向上* – クラウドアーキテクチャとデータライフサイクル管理は設定ミス、過剰にパーミッションを割り当てられたアプリケーション、不適切なデータ管理プロセスを特定します。クラウドプラットフォームとセキュリティテクニックに関する継続的な教育は最新のプラットフォームの機能と最新の攻撃の傾向に対する準備をスタッフにさせます。
IAM-07: *第三者アクセス*– クラウドサービスへのサードパーティのアクセスによって発生するリスクのアセスメントは、過剰にパーミッションを割り当てたり、WAFや他のアプリケーションによって不適切なアクセスが発生していることを特定します。
IVS-06: *ネットワークセキュリティ*– 信頼された/信頼されない接続からのアクセスとふるまいの監視のために最新のデザインと設定テクニックを実装します。
SEF-02: *インシデント管理*, **SEF-03:** *インシデントレポーティング*, **SEF-04:** *インシデントレスポンスの法的準備* – インシデントへの対応、侵害の通知、フォレンジックの手続きは影響を受ける顧客、サードパーティ、規制当局、およびその他の法的に必要とされるエンティティとの間でタイムリーに実施されます。
TVM-02: *脆弱性パッチ管理*– IMDSプラットフォームにおけるSSRF脆弱性の特定と、CSPパッチの適用またはプッシュ。

指標

主要業績評価(KPI): 設定ミスのスキャン、クラウドアーキテクチャの専門知識、データインベントリモデル、認証プロビジョニング

コントロールの効果測定: アーキテクチャとデータフロー図、データの保管と廃棄、アーカイブ、アクセスコントロールのアラートの実装

重要なポイント

- クラウドサービスのメタデータは設定ミスによって外部に曝されることがある点に注意。
- 過剰な権限を与えられているクラウドアプリケーションは侵害された際に不必要なデータへのアクセスを引き起こします。
- アーカイビング、廃棄、破棄といったデータインベントリ/ライフサイクルの実践によりデータが外部に曝されることを抑制します。

Disney+

脅威アクター	脅威	脆弱性	テクニカルインパクト	ビジネスインパクト	コントロール
外部要因 侵害されたアカウントを収益化しようとするハッカー。	**EE5** *アカウントハイジャック:* ストリーミングサービス ディズニープラスのユーザーアカウントの露出と誤用。	**EE2** *クラウドセキュリティのアーキテクチャと戦略の欠如 -* 単一のアカウント、およびディズニーストアレクリエーションパークとディズニープラスアカウントの資格情報について侵害が発生した場合のインシデント対応戦略を定める前に本番稼働が開始された。 **EE4** *不十分なIDと認証情報の管理 -* ユニークなパスワードの欠如、義務付けられていないMFA。	**EE1** *データ侵害:* ユーザーの資格情報の紛失、PII データの漏洩。	**財務面** - 潜在的な株主・ユーザーの抑止 - 運用コストの上乗せによる財務コスト - オーバーヘッドの増加 **運用面** - インシデント対応(サポートラインで何時間も待たされた人たち) - フォレンジック分析 - 強制的なダウンタイム **コンプライアンス** - アイデンティティの窃取や個人情報漏洩の可能性 - 規制上の罰金と問い合わせ **評判** - ブランドイメージと顧客の信頼に悪影響を与える可能性があります。	**予防** - IAM-02 - IAM-12 - AIS-02 - GRM-10 - HRS-09 **検知** - IVS-01 - TVM-02 **是正** - SEF-02 - BCR-02

攻撃の詳細

アクター: ディズニープラスのユーザーアカウントを乗っ取って収益化を図る外部の悪意ある者。
攻撃: 同期的なクレデンシャルスタッフィング攻撃(訳注: 日本では一般的にリスト型攻撃と呼ばれる)により、犯罪者は多くのユーザーアカウントを乗っ取り、売りに出しました。記録によると、ハッカーはログイン認証情報だけでなく、登録されたデジタルマスク(ネットワークとデバイスの種類)も入手し、ディズニープラスが何らかの緩和策を講じても、取得したアカウントの収益性を確保していました。
脆弱性: 既存のディズニーストアとレクリエーションパークのアカウントの単一アカウントと資格情報、および新規のディズニープラスアカウント、共有アカウント、多要素認証の欠如

テクニカルインパクト

データ侵害: ユーザー資格情報の紛失、アイデンティティの窃取、個人情報の漏洩の可能性。
データ損失: ハッカーはログイン認証情報だけでなく、登録されたデジタルマスク(ネットワークとデバイスの種類)も入手し、ディズニープラスが何らかの緩和策を講じても、取得したアカウントの収益性を確保していました。

サービス拒否: 何千人ものユーザーが自分のアカウントからロックアウトされ、ハッカーによってアカウントが売りに出されました。

ビジネスインパクト

財務: 差し迫ったディズニープラスの株価下落はありませんでしたが、新しいプラットフォームの立ち上げ時にこのようなインシデントが発生したことは、潜在的なステークホルダーや将来の顧客にとっては抑止力になる可能性があります。ユーザーが電話やチャットで1時間以上待たされたことによるヘルプデスクの過負荷によるオーバーヘッドの増加や、インシデント対応によるオーバーヘッドのコストも考慮に入れる必要があります。
運用: ユーザーからの苦情への対応、アカウントの復旧、ネットワークの安全性確保、フォレンジック分析、強制的なダウンタイムのために費やした時間と労力が含まれます。
コンプライアンス: コンプライアンスへの影響には、ユーザーアカウントの詳細が侵害されると、顧客の個人データも漏洩する可能性があることから、開示通知やGDPRなどの規制当局が課す罰則などの罰金や負債が含まれる可能性があります。
評判: 会社に対する信頼の喪失(ブランドの評判の低下)、既存のユーザーがプラットフォームを放棄する可能性があるため、顧客体験に影響を与えます。

予防的緩和策

IAM-02: アイデンティティ、権限、アクセス管理 – ディズニー・プラス・プラットフォームで提供されるサービスのユーザーに対して、適切なID、権限、アクセス管理を確実にするために、適切な技術的および手続き的管理が必要です。クレデンシャルスタッフィング攻撃に関連するリスクを緩和するために、同一プラットフォームで提供される異なるサービスに対して、それぞれ固有のパスワードを持つ新しいユーザーアカウントを作成するなど、強力なユーザーアカウント管理を実践します。
IAM-12: アイデンティティとアクセス管理 – ユーザーID資格情報には、リスクを緩和するために、多要素認証（MFA）やcaptchaの使用などの強力な認証メカニズムを含める必要があります。
AIS-02: APIのアクセス制御 – 顧客などの一般の人々にアクセスを提供する前に、設計段階で適切なアプリケーションとインターフェースのセキュリティ制御を検討する必要があります。
GRM-10: リスクアセスメント – セキュリティリスクを特定し、緩和するために、新しいサービスを開始する前に徹底したリスク評価を実施する必要があります。
HRS-09: ユーザー認識の向上 – すべてのサービスユーザーに、アカウントパスワードを定期的に変更し、強力でユニークなパスワードを使用するなど、セキュリティのベストプラクティスを認識させる必要があります。

検知的緩和策

IVS-01: 侵入検知 – 不審な認証の試みなどのセキュリティインシデントをタイムリーに検知して対応し、セキュリティ侵害が発生した場合のフォレンジック調査機能をサポートするために、サービスをホストするプラットフォームは、セキュリティイベントログを適切に保存し、強力な侵入検知機能を備えている必要があります。
TVM-02: 脆弱性 /パッチ管理 – 新サービスをサポートするプラットフォームの脆弱性スキャンは、タイムリーな脆弱性の検出と修正、および実装されたセキュリティ対策の効率性を確保するために不可欠です。新サービスの一般公開に先立ち、システムのユーザー認証やアカウント管理モジュールなどの重要なセキュリティ領域の脆弱性を特定し緩和する必要があります。

是正的緩和策

SEF-02: セキュリティインシデント管理 – サービスを開始する前に、新たに開始されるサービスの加入者のアカウント乗っ取りなどの潜在的なセキュリティインシデントへのタイムリーな対応と解決を確実にするために、堅牢なセキュリティインシデント管理の枠組みを構築する必要があります。
BCR-02: 事業継続性のテスト – 事業継続計画とオペレーショナル・レジリエンスは、計画された間隔でテストされ、ユーザーのロックアウトや DoS 攻撃などの特定の障害に対するセキュリティインシデント対応計画を検証する必要があります。テストで指摘された欠点や改善点は、組織の事業継続計画やインシデント対応計画に含める必要があります。

指標

重要指標 (KPI):
- サービスプラットフォーム、基盤となるインフラストラクチャ、そのインターフェイスコンポーネントで実行された脆弱性スキャン。
- サービス加入者に対する多要素認証（MFA）などの強力な認証機能のロールアウト。

管理策の効果測定:
- ホストされているアプリケーション、システム、インターフェースで発見された脆弱性の数。
- アカウント認証で利用可能な追加のセキュリティ機能を使用しているユーザーの割合。

重要なポイント

- 強力なユーザー認証を講じるため、多要素認証（MFA）の有効化。
- 1つのアカウントの侵害が他のサービスに影響を及ぼさないように、同一プラットフォームにおいてもサービスごとに異なる種類のログイン資格情報の実装。
- アカウントごとに強力でユニークなパスワードを使用するなど、ユーザーがセキュリティのベストプラクティスに従っていることを確実にするためのユーザー意識向上キャンペーン。

Dow Jones

脅威アクター	脅威	脆弱性	テクニカルインパクト	ビジネスインパクト	コントロール
内部要因 セキュリティやその他のITサービスを提供するベンダーの採用や審査を担当するダウ・ジョーンズのセキュリティスタッフ	**EE1** データ侵害：機微データの露出	**EE2** *設定ミスならび不適切な変更管理* - ダウジョーンズウォッチリストデータベースがセキュアに保存されたことを検証することもパスワードで保護されることもなくAWSに配置された.	機微なパーソナルデータ、企業データ、政府データの露出	**財政面** 訴訟費用と罰則による収益の損失	**予防** - HRS-07 - IAM-02 - IAM-07
	EE6 *内部者の脅威:* ダウ・ジョーンズデータの不注意な取扱い			**運営面** - センシティブデータの漏えい - 訴訟の潜在的可能性	**検知** - AAC-01 - AAC-02
外部要因 ダウ・ジョーンズ認定サードパーティベンダー	**EE6** 内部者の脅威: ベンダーに対する管理監督の欠如	**EE3** 不適切な ID,資格,アクセス,および鍵の管理 パスワード保護なしでAWS Elasticsearchデータベースにデータが保存された. つまりIAMコントロールが使用されなかった.	露出したデータが、無制限で他のデータベースにコピーやリプリケートされる恐れ.	**コンプライアンス** - インシデント対応 - セキュリティベンダーの審査 - データベースリソースの監視	**是正** - SEF-02 - STA-08 - STA-09
				評判 -ダウ・ジョーンズの評判とブランド名へのダメージ -不十分な企業ブランドの認識	

攻撃の詳細

アクター：ダウ・ジョーンズに帰属する、AWSがホストするElasticsearchデータベースのパスワードによる保護に失敗したダウ・ジョーンズ認定サードパーティベンダー。

攻撃：データベースはパスワードで保護されておらず、誰にでも利用される状態でした。また、この不具合は誰でも利用が可能なIoT検索エンジンで見つけることができるものでした。この誤って設定されたデータベースは、著名なセキュリティ研究者によって2019年に発見され、ダウ・ジョーンズへ報告されました。
脆弱性：おそらく信頼された認定セキュリティベンダー中の1社がダウ・ジョーンズデータベースをパスワードで保護しなかった。

テクニカルインパクト

データ漏えい： データベースには、政治的影響力のある人物(Politically Exposed Persons(PEP))、彼らの関係者、関連する企業、国家政府および国際政府の制裁リスト、世間の注目を浴びた事件で有罪判決を受けた人々や容疑者、連邦機関や法執行機関の内部文書を引用した文書など、240万人ものウォッチリストレコードが格納されていました。このデータ露出は著名なセキュリティ研究者が発見し、ダウ・ジョーンズの技術スタッフに報告されました。
データ消失：ダウ・ジョーンズのデータは、暗号化されず、タグとインデックス付けられて保存されていたため、容易に表示、取得、複製が可能でありました。露出を発見したセキュリティ研究者以外の誰かがデータベースをアクセスしたことの確かな証拠はありません。しかし、アクセスできる状態であったことは、記載されている当事者のプライバシーに重大なリスクをもたらしたと言えます。

ビジネスインパクト

財務：ダウ・ジョーンズのデータ侵害による財務面、コンプライアンス面への影響は複雑に絡み合っている。財務的な観点から個人情報が公開されたことによって重大な損害を受けたと主張する人々や組織が、ダウ・ジョーンズに対して起こした訴訟に対し、かなりの費用がかかったと思われます。

運用：ダウ・ジョーンズが今後このようなインシデントを回避するためには、セキュリティベンダーを精査し、標準のセキュリティプラクティスに従っていることを確認するため、ポリシーと手順を改善し運用する必要があります。データセキュリティを向上させるための標準と手順を開発することにより、ダウ・ジョーンズの技術運用コストが増加する。ダウ・ジョーンズは、このインシデント事案の回復作業とインシデントレスポンスの他、将来これに類似する作業を担当することとなり、インシデント対応コストの増加が予想されます。

コンプライアンス：とにかく(いずれにせよ)、パスワードで保護されず、暗号化されずにデータをクラウドに保存すると、データが公開され、簡単にアクセスできるようになります。これにより、データに情報が含まれている人や組織のプライバシーが侵害されます。
評判：重大なデータ侵害があった企業はどんな企業でも、企業およびブランドの評判に対する損害が起こり得ます。 2019年のダウ・ジョーンズのデータ漏えいは初めてではなく、2017年にも同様のインシデントが発生しました。

予防的緩和策

HRS-07: *ロール / 責任* – 社内およびサードパーティのセキュリティプロバイダーのセキュリティチームメンバーの役割と責任を明確に文書化する必要がある。特に、組織とそのサードパーティのクラウド/セキュリティサポートパーティ、または請負業者の間で共有されるクラウドサービスを展開、維持、保護する責任を特定することが重要です。
IAM-02: *資格証明のライフサイクル/プロビジョニング管理* – ダウ・ジョーンズのサードパーティプロバイダーのように、パスワード保護なしでデータをクラウドに保存することは絶対にしてはならない。さらに、クラウド内のデータへのアクセスを許可されるユーザーには、ユーザーごとに個別アカウントを付与すべき。役割に基づくアクセスのレベルを実装すべき。システム管理者はフルアクセス権を持つが、その他のユーザーは読み取り専用の権限を付与すべき。データアクセスは、読み取り専用であっても、仕事のためにデータアクセスを必要とするユーザーだけに制限すべき。可能な限りデータは暗号化された形式で保存すべきである。ダウ・ジョーンズの場合、社内外の誰もが自分のデータに無制限にアクセスできました。

IAM-07: *第三者アクセス* –
サードパーティのサービスを採用する前に、サードパーティがデータにアクセスを必要とするビジネスプロセスによってもたらされるリスクの特定、リスク評価、優先度判断を明確にしておくべきである。サードパーティのセキュリティおよびマネージドサービスプロバイダーは、標準のセキュリティ慣行に従っていることを確認するため、厳格に精査する必要がある。また、サードパーティの評判を調べ、適切なサービス提供に失敗していないことを確認することも重要である。要するに、どのようなサードパーティのサービスであろうとも、そのサービスを採用する前に、組織自らが何に取り組むのかを明確に決定しておくべきです。

検知的緩和策

AAC-01: *監査計画* – 企業がクラウドサービスを展開した後、それが企業またはサードパーティによって行われたかどうかにかかわらず、機能の観点から、サービスが適切に実行されているかどうかを定期的にチェックする計画を立てる必要があります。そしてセキュアに。クラウド内のデータベースがパスワードで保護されたユーザーアカウントで保存され、データへのアクセスを必要とするユーザーのみに表示されることを確認するための監査を実施する必要があります。会社に所属していないユーザー、またはデータへのアクセスが不要になったユーザーのアカウントは削除する必要があります。これらの監査は、年に1回以上行う必要があります。ダウ・ジョーンズのインシデントでは、セキュリティ監査により、ウォッチリストデータが安全に保管されていなかったという事実が検出されました。

AAC-02: *独立監査* – 組織は強力な監査組織を持っている場合もありますが、組織のセキュリティチームが何かを見逃していないことを確認する目的で、信頼できる監査法人による独立監査の実施が推奨されます。ここでのキーワードは「評判の良さ」である。独立したセキュリティ監査人は、サードパーティの請負業者や企業であり、サードパーティや請負業者自身が持つセキュリティリスクをもたらす。この点で、脆弱なダウ・ジョーンズデータベースを発見したセキュリティ研究者は、独立監査人の行動を取ったと言えます。彼はこの目的のために会社に雇われていませんでした。

是正的緩和策

SEF-02: *インシデント管理* – 問題を効率的に解決し、データのセキュリティとビジネスの継続性を維持するために、セキュリティインシデントに対応するための手順を実施する必要があります。ここではHRS-07が実際に役立つ。サードパーティのサービスによって維持されている企業のクラウドデータに関連するセキュリティインシデントが発生した場合、インシデントを修正する責任の問題が発生する可能性があります。そのデータを所有する会社がサードパーティがインシデントを処理すると想定し、サードパーティはそうでないと想定した場合、サービスが危険にさらされたままになります。インシデント管理の責任は、会社とそのサードパーティのサービスプロバイダーとの間のサービス契約で明確に記載されている必要があります。

STA-08: *第三者の評価* – ダウ・ジョーンズは、サードパーティのプロバイダーが、健全なセキュリティ慣行に従い、定期的にメソッドを検証することについての書面による保証を強く要求すべきでした。
STA-09: *第三者の監査* – サードパーティのサービスプロバイダーは、サードパーティの契約に含まれる情報セキュリティと機密性、アクセス制御、サービス定義、およびデリバリーレベル契約への準拠を実証する必要があります。これは、特定のサードパーティのセキュリティおよびマネージドサービスプロバイダーを使用するかどうかを決定する際の重要な側面です。サードパーティプロバイダーは、データを管理する前に、標準のセキュリティ慣行を順守する必要があります。

指標

重要指標 (KPI): データベースインフラストラクチャへの軽微な損傷または損傷が発生していないことを示す定期的および定期的なインシデントレポート
管理策の効果測定: データ検証の脆弱性スキャンとセキュリティ監査がセキュアな状態に維持されていること

重要なポイント

- クラウドへのデータ格納は暗号化とIAMの使用によってセキュアでなくてはならない。
- サードパーティのセキュリティサービスプロバイダーが信頼できるか、標準のセキュリティプラクティスに従っているかを確認するため精査しなくてはならない。

Github

脅威アクター	脅威	脆弱性	テクニカルインパクト	ビジネスインパクト	コントロール
内部要因 N/A	増幅ペイロードを含むUDPパケット配送	**EE2** 設定ミスと不適切なアクセス制御-ポート開放	**EE 2** memcachedサーバの設定ミス	**財政面** 報告無し	**予防** - IVS-04 - BCR-09 - IVS-06
		EE3 クラウドセキュリティアーキテクチャ及び戦略の欠如-不適切なアーキテクチャ設計	**EE 3** インターネットに公開されているmemcachedサーバーに関するアーキテクチャと知識の欠如	**運営面** - 運用の中断発生	**検知** - AAC-01 - AAC-02
外部要因 不特定の攻撃者		**EE3** クラウドセキュリティアーキテクチャ及び戦略の欠如-不十分な事業戦略	**EE9** メタストラクチャとアプリストラクチャの障害：完全性についての報告無し	**コンプライアンス** 報告無し	**是正** - SEF-02 - SEF-03
		内部者へのトレーニング不足	可用性システムのダウン	**評判** 報告無し	
		古いバージョンのソフトウェア利用			

攻撃の詳細

脅威アクター-Githubのオペレーションを妨害することによるサービス停止を狙った不特定の外部のアクターによるもの
脅威源/イベント-アクターは、Memcrashingと呼ばれる手法を使用してDDoS攻撃を行いました。Memcrashingは、認証不要で接続可能な状態でパブリックインターネットに公開されたままになっているmemcachedデータベースサーバを悪用することで機能します。
本DDoS増幅攻撃は、次のように機能します：アクターは、公開されたままになっているmemcachedサーバーに小さなデータベースコマンドを送信し、そのリクエストのUDPパケットに送信元インターネットアドレスとしてGithubサーバーを設定します。memcachedデータベースは、コマンドで受信したデータ量の約50,000倍を送信元に返します（203バイトのリクエストが100MBの応答となります）。Githubに到達するトラフィックは、ピーク時には1.35Tbps、または1秒当たり1億2,690万パケットとなりました。膨大な量のデータがGitHubのコンピューターを圧倒し、通常のユーザーへの応答ができなくなりました。
脆弱性：内部者 - 信頼できるネットワーク内にサーバーを配置したり、更新されたMemcachedバージョンをインストールしたり、ポート11211を閉じたりすることについて、不適切なトレーニングを受けた、従業員、コンサルタント

テクニカルインパクト

機密性：機密性の喪失なし
完全性：完全性の喪失なし
可用性：システムとそのデータが利用できない状態となったのは約5分間であり、Githubが何らかの重大な影響があったと報告をうけるほどの時間ではなかった。もし、システムが長期間使用できなくなっていた場合、ソフトウェア開発用のコラボレーションプラットフォームであるGithubにとって、サービス利用者の開発プロジェクトに大きな遅延を招く恐れがあった。

ビジネスインパクト

財務：経済的影響は報告されていない。しかしながら、混乱が長期間続いた場合、利用者がプロジェクトを進めることができなくなっていた可能性があり、プラットフォームによって生み出された収益に深刻な影響が及んでいた可能性がありました。
運用：システムとデータは利用できない状態となったが、重大な影響は報告されていない。利用できない状態が長く続いた場合、多数のプロジェクトが中断され、開発プロジェクトに遅延を生じる可能性がありました。
コンプライアンス：コンプライアンス上の問題は報告されていません。しかし、GDPR 条項32および49では、可用性およびDDoS攻撃についての言及があり、結果としてGDPRの罰金および懲罰が発生する恐れがありました。
評判：経済的損失は報告されていないが、サービスの中断は、経営陣による、会社のサービスとセキュリティを適切に管理する能力に対する信頼を損なうことに繋がり、ブランド価値に影響を与える可能性があります。

予防的緩和策

IVS-04: インフラと仮想化のセキュリティ-ネットワークアーキテクチャ-ネットワークアーキテクチャ図により法令遵守に影響を及ぼす可能性があるリスクの高い環境とデータフローを明確に特定できるようにしなければならない。技術的対策を実施し、異常な入出力トラフィックパターン（MACスプーフィング、ARPポイズニング攻撃等）や、分散型サービス拒否（DDoS）攻撃に関連するネットワークベースの攻撃を検出し、タイムリーに対処するための多層防御技術（ディープパケット分析、トラフィックスロットリング、ブラックホール等）を適用しなければならない。
IVS-06: インフラと仮想化のセキュリティ-ネットワークセキュリティ-ネットワーク環境と仮想インスタンスは、信頼できる接続と信頼できない接続の間のトラフィックを制限し、監視するよう設計し、構成されなければならない。これらの構成は、少なくとも年1回はレビューされ、許可されたすべてのサービス、プロトコル、ポートの利用及び代替コントロールにより適切であることが文書により示されなければならない。
BCR-09: 事業継続管理と運用レジリエンス-影響分析-組織（クラウドサービスプロバイダー、クラウドサービス利用者）の混乱・影響を判断するため、次の事項を含む定義、文書された手順等を定めなければならない。重要な製品とサービスの特定。プロセス、アプリケーション、ビジネスパートナー、サードパーティのサービスプロバイダー等、すべての依存関係の特定。重要な製品やサービスに対する脅威の理解。計画的又は計画外の中断により生じる影響と時間経過に伴う変化の判断。混乱の最大許容期間。回復の優先順位。重要な製品及びサービスを最大許容期間内に再開するための回復時間の目標。再開に必要なリソースの積算。

検知的緩和策

AAC-01: 監査計画-監査計画は、ビジネスプロセスの混乱に対処するために作成および維持されなければならない。 監査計画は、インシデント対応計画、ルータ、ファイアウォール、ポートの構成、ネットワークとフィルタリングの許容量等、セキュリティ/運用の実装と継続的なパフォーマンスの効率と有効性のレビューに焦点を当てなければならない。
AAC-02: 独立した監査-組織がベストプラクティスを促進し、確立されたポリシー、標準、手順、およびコンプライアンス義務の不適合に対処することを保証するため、独立したレビューと評価を少なくとも年に1回実施しなければならない。インシデント対応計画、ルータ、ファイアウォール、ポートの構成、ネットワークとフィルタリングの許容量等の運用を効率的かつ効果的にカバーするには、第三者および内部監査を調整しなければならない。

是正的緩和策

SEF-02: インシデント管理-確立済みのITサービス管理ポリシーとプロシージャに沿って、Githubのセキュリティ関連のイベントを優先順位付けし、タイムリーで徹底的なインシデント管理を確実にできるポリシーと手順、およびそれらを支援するビジネスプロセスと技術的対策が実装される必要があります。
SEF-03: インシデントレポーティング-従業員と外部事業者の関係について、それぞれの責任を知らされる必要があります。また、必要に応じ、すべてのGithubの情報セキュリティイベントをタイムリーに報告することに同意し、契約上も同意を得る必要があります。Githubの情報セキュリティイベントは、予め定義された通信チャネルを通じて、適用される法令上、法定、規制のコンプライアンス義務を遵守し、タイムリーに報告されなければならない。

指標

重要指標 (KPI)：目標復旧時間（RTO）目標復旧時点（RPO）、検出までの平均時間（MTD）、応答までの平均時間（MTR）、信頼できないとリスク判断された接続数/全接続数、継続的に許可されている、信頼できないとリスク判断された接続の比率、インシデントの優先度、ステータス（未処理、処理中、解決済み）、およびインシデントプロセスの各ステップとインシデント解決プロセス全体の経過時間。
管理策の効果測定：問題の数と重大度の削減、検出時間と応答および回復時間の削減。

重要なポイント

Githubサービスにおける要点

- 緊急時に追加可能なネットワーク、フィルタ容量の事前準備
- 詳細なテスト済みインシデント対応計画が準備済みであること
- Memcachedサーバーに対する次のコマンド応答"shutdown \r\n"または"flush_all \r\n"
- ルータ及びファイアウォール設定によりすべての無効なIPアドレスからの通信を確実に遮断していること
- Memcachedサーバー 11211ポートを発信元とするUDPトラフィックのブロック

Memcachedサーバーにおける要点

- memcachedサーバーのTrusted ネットワークの中への配置
- デフォルトでUDPプロトコルが無効化されている新しいバージョンのmemcachedのインストール

Imperva

脅威アクター	脅威	脆弱性	テクニカルインパクト	ビジネスインパクト	コントロール
内部要因 内部クラウドチームによる設計及びヒューマンエラー	**EE1** データ侵害：機密データを含むデータベーススナップショットの公開につながる本番用AWSのサーバインスタンスとアクセスキーの侵害	**EE2** 設定ミスと不適切な変更管理 -機密データベーススナップショットへのアクセスを持つサーバーがインターネット接続可に設定されていた	**EE1** データ侵害：Incapsulaの顧客のメールアドレス、パスワード、APIキー及び証明書に関する一部のデータの侵害	**財政面** - データなし	**予防** - DSI-05 - EKM-04 - IVS-07 - IVS-06
		未公開サーバーの脆弱性 -攻撃者はクラウドサーバが面しているインターネットからピボット可能であった、つまり未公開の脆弱性あるいは重大な設定ミス経由で侵害可能だった	**クラウドのインスタンス侵害**：攻撃者はAWS EC2を侵害可能	**運用面** -マーケティング、セキュリティ及び運用チームによるインシデント対応 -数万に及ぶ顧客の証明書、パスワード及びAPIキーの再発行及び再登録	**検知** - IVS-06 - IVS-01 - TVM-02
外部要因 - 未知の脅威アクター - 未公開バグ報奨金ハンター	クラウドサーバ及び資格情報の侵害：攻撃者はAWS EC2のサービスインスタンスを侵害可能、且つサーバー上の資格情報を悪用可能だった	**EE3** クラウドセキュリティアーキテクチャと戦略の欠如 -本番用データベーススナップショットにアクセス可能なサーバーがテスト用に使用されていた。一時的な資格情報というより、インターネットに接続されAWS APIキーを使用していた。	クラウドアクセスキーの資格情報の侵害	**コンプライアンス** -GDPRに基づき侵害通知が発行される	**是正** - AIS-04 - CCC-03 - GRM-02 - IAM-08
				評判 N/A	

攻撃の詳細

アクター： 未知の外部脅威アクター及び未公開バグハンター
攻撃： 2018年10月、Impervaのクラウドサーバが侵害され、本番用AWSアカウントの一つの管理APIキーが不正に利用された。これにより、メール、ハッシュ及びソルトが行われたパスワードを含むデータベーススナップショットが公開されていた。

脆弱性： 内部のクラウドチームによる内部設計とヒューマンエラーが、サーバーの弱点(**未公開サーバの脆弱性**)及び侵害を可能にする条件を招いた。具体的には、サーバーをインターネット接続可能にし(**EE2 -設定ミスと不適切な変更管理**)、このサーバーからAWS API アクセスキー経由で本番用データベーススナップショットにアクセスするよう設定されていた(**EE3 –クラウドセキュリティアーキテクチャと戦略の欠如**)。

テクニカルインパクト

クラウドインスタンスの侵害：攻撃者はImpervaがテスト用途で運用していたAWS EC2サーバーを侵害することが可能であった。

EE1 – データ侵害：Incapsulaの顧客のメールアドレス、パスワード、APIキーと証明書のサブセットが攻撃者により抽出された。
クラウドアクセスキー資格情報の侵害：侵害されたサーバー上のAWS API アクセスキーが攻撃者によって利用、抽出されたことにより、侵害された。

ビジネスインパクト

財務: 2018年時点において、Imperva社は非公開企業につき、経済的影響またはImpervaの評価にかかる影響に関するデータは存在しない。
運用:
- マーケティング、セキュリティ及び運用チームによるインシデント対応
- 数万に及ぶ顧客の証明書、パスワード及びAPIキーの再発行及び再登録

コンプライアンス: プライバシー法で義務付けられている通り、GDPRに基づき違反の通知が行われた
評判: 顧客、メディア、国際法執行機関及び規制当局に連絡。加えて、ニュース媒体により当該過失及びインシデントについて長期にわたり報じられます。
ビジネスへの影響: Imperva社CEOは当該侵害事案発生を受け辞任。一方、会社側は辞任と当事案の関係性について正式には認めていない。

予防的緩和策

DSI-05: 本番環境のデータは、本番以外の環境にコピーしたり使用したりしてはならない。本番以外の環境における顧客データの使用は、いかなる場合も、影響が及ぶ全ての顧客からの明確な文書による承認、且つ機微なデータ要素の洗い出しを必要とします。
EKM-04: オープンな検証済みの形式かつ標準アルゴリズムであるプラットフォームやデータに適した暗号化方式(AES-256など)を使用しなければならない。本ケースにおいて、侵害されたと考えられる機密データは暗号化されていなかった。
IVS-07: オペレーティングシステムは、業務に必要十分なポート、プロトコル、サービスのみを提供するように補強しなければならない。また、ウイルス対策、ファイル完全性モニタやログ収集などの技術的管理策を装備しなくてはならない。侵害されたサーバー上の外部公開サービスについては、サーバセキュリティソリューションが予防と検知に効果があったと想定されます。
IVS-06: ネットワーク環境及び仮想インスタンスは、信頼できる接続と信頼できない接続との間のトラフィックを制限し監視するよう設計し構成されなければならない。当該のデータ侵害は、サーバーからインターネット接続が必須ではなかったにもかかわらず接続可となっていたため実現した。

検知的緩和策

IVS-01: 本ケースのような普段と異なる利用と侵害を特定するには、ID及び資格情報の侵害と利用の監視を行うべきである。ホスト侵入検知ソリューションにより、業務の侵害やその類の試行を特定し対応しなければならない。

IVS-06: ネットワーク環境及び仮想インスタンスは、信頼できる接続と信頼できない接続との間の(ネットワーク)トラフィックを制限し監視する管理策を装備します。

TVM-02: 組織が所有または管理するアプリケーション、IT基盤のネットワーク及びシステムコンポーネント内の脆弱性をネットワーク脆弱性評価、ペネトレーションテスト等により遅滞なく検知し、実装されたセキュリティコントロールの有効性及び欠陥の修復を確実にします。(このケースでは、複数ある欠陥のたった1つが、単なるインシデントではなくデータ侵害に発展。)

是正的緩和策

CCC-03: 機密性にフォーカスし、システムやサービスを定義されきちんした変更管理とテストプロセスがあれば、機密の本番データやインターネットに接続したサーバーからアクセスできるような類のデータセキュリティ上の懸念が明らかになっていたかもしれない。
AIS-04: サーバー及びアプリケーションに(a)インターネットや(b)データストアへの新たなインターフェースを作成する際はデータセキュリティを考慮するべきである。これにより、データ侵害を防ぐことができた可能性があります。
GRM-02:
- データガバナンス要件に関連するリスクアセスメントは、計画された頻度で、かつ以下の事項を考慮して実施しなければならない。
- 機微データが、アプリケーション、データベース、サーバー、ネットワーク基盤間のどこで保持され、伝送されるかの認識
- 定められた保存期間と、使用終了時の廃棄に関する要件の遵守
- データの分類と、許可されていない使用、アクセス、紛失、破壊、改ざんからの保護

どのデータがどこに、なぜ保存されているか、そのデータがリスクに晒されているか否かを評価するためのプロアクティブなアプローチにより、誤用や誤操作の防止が可能になります。
IAM-08: 認証に用いられるID(本人識別情報)に許容される保存及びアクセスを考慮することにより、AWS APIアクセスキーの利用を防止し、最小権限付与の実践と安全な取扱いを確実にする。これによりAWSロールがベタープラクティスとなる(エクスプロイトや誤用が困難)。

指標

重要指標 (KPI):クラウド設定ミス件数の削減、機微なデータ及び本番データストアへのアクセスの削減、外部公開IPアドレス件数の削減
管理策の効果測定:電子情報開示と関連するデータの分類とタグ付け。攻撃対象領域及びクラウド設定ミスの継続的な削減。ID及びアクセス侵害検知テストの実施。サーバー侵害検知テストの実施。外部脆弱性スキャンの実施。

重要なポイント

- クラウドサービスのアジリティは、より多くのヒューマンエラー、デザインの欠陥及びポリシー違反を可能にします。
- クラウドサービス及びクラウド上の資産保有は、攻撃対象領域を拡大させる。検知と削減が重要となります。
- クラウド利用している規模の小さい組織や環境であっても、クラウドシステム、ネットワーク、アカウント及びIDの正しい構成及び設計は、熟慮された他の防御と同様に有益。

Ring

脅威アクター	脅威	脆弱性	テクニカルインパクト	ビジネスインパクト	コントロール
内部要因 収集されたデータを個人的な目的のために利用する可能性がある、潜在的な悪意のある内部関係者	**EE1** *データ侵害:* サードパーティのトラッカーを通じた顧客のPII	ユーザーのプライバシー侵害の可能性を発見できたはずの、不適切なプライバシーのリスク評価	**EE1** サードパーティのトラッカーによる消費者のPIIの*データ侵害*	**財政面** -訴訟により損失を被るリスク **運用面** - インシデントを是正するための追加リソース **コンプライアンス** - 公表前の監査結果 - 漏洩後の罰金 **評判** - Ringへの信頼の失墜 - 長期的な市場シェアへの影響 - Amazonの株価への潜在的影響AmazonはRingを買収済。	**予防** - IAM-07 - STA-01 - STA-05 - STA-06 - STA-08 **検知** - AAC-02 - CCC-03 - DSI-02 - STA-04 - TVM-02 **是正** - SEF-02 - SEF-03 - SEF-04 - SEF-05 - STA-02
外部要因 顧客のPIIに許可されていないアクセスができる可能性がある潜在的な脅威アクター		**EE2** 機能の欠如に起因する*設定ミス*。ユーザーのコンテンツを検索し企業によるユーザデータ共有を拒否するようなオプションが望まれた。	**EE11** 広告、データマイニング、プロファイリング、監視目的での消費者のPIIの乱用および不正利用		

攻撃の詳細

アクター: 悪意のある外部の脅威アクターや内部関係者が消費者を搾取するために利用した、Ringのアンドロイド向けインターホンアプリ上のサードパーティのトラッカー
攻撃: Ringのアンドロイド向けアプリがサードパーティのトラッカーが、顧客の個人情報 (PII) を分析およびマーケティングの企業4社に送信していることをEFFチームが発見した。つまり、プロファイリング、監視、データ盗難等の不正な目的のためにデータが悪用される可能性があります。

テクニカルインパクト

データ侵害: 不正な第三者が顧客のPIIにアクセスし、ユーザーのプライバシーが侵害されていました。ユーザーの氏名、メールアドレス、OSバージョンとモデル、Bluetoothアクティビティ、ローカルIPアドレスなどの情報が収集され、分析やデータマイニングのために転送されていた。
クラウドサービスの乱用と不正利用: 収集されたデータの種類を考慮すると、このデータが広告、データマイニング、ユーザープロファイリング、国家による監視、データの不正管理、ソーシャルエンジニアリング目的の脅威アクターによる犯罪などに使用される可能性があります。

ビジネスインパクト

財務: このデータ侵害により、制裁金や顧客データの不適切な処理に怒った顧客による集団訴訟で、金銭的損失が生じる可能性があります。
運用: インシデント対応チームがインシデントを是正するために要した時間と労力。また、顧客のデータをサードパーティの組織と共有することで、データの漏洩や乱用につながるリスクもあります。
コンプライアンス: 違反に対する制裁金の可能性と被害を受けた消費者からの訴訟の可能性。
評判: この発見はRingにとってマイナス評価となり、Ringの消費者のデータのプライバシーを保護する能力に対する消費者の信頼を損なった可能性が高い。

予防的緩和策

IAM-07: 第三者アクセス- 組織または顧客のデータへのアクセスを要求するサードパーティにアクセスを許可する場合は、適切な注意が必要です。
STA-01: データ品質と完全性- Ringは、適切なデータ品質が維持され、エラーが低減されることを保証する必要があります。
STA-05: サプライチェーン管理、合意、サプライチェーンの合意/契約には、顧客データを保護するための情報セキュリティ要件を明示的かつ明確に記載する必要があります。
STA-06: ガバナンスレビュー- 組織は、パートナーのクラウドサプライチェーンの他のメンバーから移転されたリスクが明確であることを確実にするために、パートナーのガバナンスおよびリスク管理ポリシーを再確認する必要があります。
STA-08: 第三者評価- ポリシーと手順のコンプライアンスおよび有効性を確実にするために、年に1回サードパーティの評価を実施する必要があります。これは、組織を危険にさらす可能性のある、サードパーティによる不適切な行為を検知できるコントロール手段です。

検知的緩和策

AAC-02: 独立した監査– 少なくとも年に1回実施される独立したレビューおよびリスク評価により、確立されたプライバシーコンプライアンスに関する義務との不適合が検出され、是正されなければならない。
CC-03: 品質検査– 消費者の機密性と信頼性に影響を与える可能性のある重要な機能における問題を検知するために、適切なテストが行われる必要があります。
DSI-02: データの管理表とフロー – アプリケーションのデータフローを確認するためにポリシーを確立する必要があります。Ringの場合、適切なインベントリとデータフローのレビューにより、データ収集および転送の事前に顧客の同意を得る必要があるという、要件の欠落を明らかにすべきでした。
STA-04: 内部評価– サードパーティは、内部統制の有効性と適合性について内部評価を実施し、その結果をRingに提供する必要があります。
TVM-02: 脆弱性/パッチ管理- 重要な機能の欠落など、アプリケーション内の問題点を迅速に検知します。

是正的緩和策

SEF-02: インシデント管理- 組織は、インシデントレスポンスのプロセスが定義されているか確認する必要があります。
SEF-03: インシデントレポート– サードパーティは、どのようなデータの漏洩やセキュリティインシデントも報告するという契約に合意する必要があります。
SEF-04: インシデントレスポンスの法的準備- サードパーティが関与するデータ漏洩が発生した場合は、法的措置の可能性に対応するために、適切なフォレンジックの手順に従い証拠を収集する必要があります。
SEF-05: インシデントレスポンスのメトリック- 会計および将来的な予算への影響について、それぞれのインシデントは、費やされた時間とリソースに基づき記録される必要があります。
STA-02: インシデントレポート– セキュリティインシデントの影響を受けたすべての顧客に通知し、RFI (情報提供依頼書)を通じて追加の情報を求めている顧客に応えるために、適切な対策を講じる必要があります。

指標

重要指標 (KPI): サードパーティ関連のインシデント数、顧客からのRFIの数、品質テスト中に検出された機能ギャップの数、アプリケーション開発中のプライバシー機能評価の有無など。
管理策の効果測定: 本番環境への導入前にアプリケーションの問題点を明らかにする自動化されたスキャン、内部およびサードパーティのリスク評価の定期的な実施、顧客満足度調査。

重要なポイント

- Ringは、サードパーティのトラッカーやデータマイニングに引き渡すことで、利用可能となる顧客データから利益を得ている。Ringはプライバシーダッシュボードを追加し、顧客がプライバシーとセキュリティの設定を管理できるようにした。
- 消費者は、自分のプライバシーへの本当の影響を理解せずに、自分のモバイルデバイスにインストールするアプリの隠れた危険性を認識しなければならない。

Tesco

脅威アクター	脅威	脆弱性	技術インパクト	事業インパクト	管理策
内部要因 Webアプリケーションを保守するサードパーティ・サービスプロバイダー	**EE1** *データ侵害:* ユーザーの個人データの暴露	**EE2** *構成ミス及び不十分な変更管理 –* 個人データを保管するパブリッククラウドストレージは安全対策が取られていなかった。	**EE1** *データ侵害:* 結果として、英国内19拠点にわたってユーザーの個人データを含む数百万もの画像を晒した。	**財務面** ・アプリ停止時間コスト ・脆弱性解消運用コスト ・規制当局の罰金 ・被害ユーザーからの損害賠償訴訟	**予防** - AIS-01 - CCC-02 - EKM-03 - HRS-09 - HRS-07 - IAM-02
		EE4 *不十分なアイデンティティ・資格・アクセス管理 –* 駐車証明Webアプリは認証制御がなかった。		**運用面** ・インシデント対応 ・GDPR規制に基づく被害ユーザーへの漏えい告知	**検知** - AAC-02 - STA-08 - TVM-02
外部要因 安全対策が取られていないデータにアクセスする外部のユーザー	**EE6** *内部者の脅威:* アプリケーション保守チームに属する訓練不足のスタッフによる個人データの取扱い	**EE7** *不安定なインターフェースとAPI –* Webインターフェースの不安定な実装が個人データを暴露した。	**EE11** *クラウドサービスの悪用・乱用・不正利用:* 外部の攻撃者が、パブリッククラウド上に保管されている画像を容易に取得することができて。違法目的に使うことができる。	**コンプライアンス** ・個人データ流出 ・規制当局の罰金と取り調べ	**是正** - SEF-02 - STA-02 - STA-09
				評判 ・ブランドイメージと顧客の信頼に悪影響が及ぶ。	

攻撃の詳細

アクター: Tesco向けのWebアプリケーションを保守するサードパーティのサービスプロバイダーは、顧客の個人データ、すなわちANPR（ナンバープレート自動認識）画像を何らの認証を確保せずにパブリッククラウドストレージ・プラットフォームにせる保管した。
攻撃: パブリッククラウドに保管された画像にアクセスし、違法目的で大量の画像を取得する外部のユーザー
脆弱性: Webアプリケーションが使用するパブリッククラウド上に保管されたデータにアクセスするための認証メカニズムの欠如。データ移行プロセスにおける不十分なセキュリティ点検。管理もレビューも不十分な仕組みなどの、低レベルのベンダー・リスク管理

テクニカルインパクト

データ漏えい: ANPRソフトウェアを使って撮影した、顧客の車両及びそのナンバープレートの画像がパブリック環境に晒された。顧客のプライバシーを画像として晒した違反はタイムスタンプが付けられており、データ履歴の集計で顧客の位置と活動をトレースできることになります。

データ損失: 英国内の19拠点にわたって取得された数約万にのぼるライセンス・プレートと車両の画像。
法規制違反: スーパーマーケットを訪れた顧客の個人データの漏えい。プライバシー法規制、すなわちGDPR違反は、ユーザーの個人データが適切に保護されるべきであることを要求しています。

ビジネスインパクト

財務: 各種メディアに晒され周知される程度によるが、顧客がマーケットを訪れるという選択をしないということになれば、事業インパクトは短期間のうちに深刻になり得る。データ漏えいが不利益な結果に繋がるなら、影響を被ったユーザーは会社を損害賠償で訴えるかもしれない。データ管理者とデータ処理者は、両者ともにGDPRの義務に沿ってユーザーの個人データを保護する責任があるため、規制当局の罰金に繋がる可能性があります。
運用: データ暴露が公になったとたんに駐車場アプリは終了となった。運用面のインパクトは、ぜい弱はアプリを安全にするためかかった時間と作業を含む。
コンプライアンス:コンプライアンスに対するインパクトは、GDPRのような規制当局が課す公示や罰などの罰金や責任を含むことになるでしょう。
評判: メディアで盛んに取り上げられることで、ユーザーは近い将来も自分たちの個人データをもってスーパーマーケットを信頼することを躊躇するようになるでしょう。評判が悪化するので、組織のブランドも被害を受けることになるでしょう。

予防的緩和策

AIS-01: *アプリケーションのセキュリティとインターフェースのセキュリティ* – 組織は、パブリック環境に晒されるアプリケーション及びプログラミングのインタフェース(API)の設計・開発・テスト・提供において、安全なSDLC実務慣行が遵守されることを確実にしなければならない。
CCC-02: *アウトソース先の開発における変更管理・構成管理* – アウトソース先のサービスプロバイダーは、特にデータ移行活動等の顧客データの取扱いにおいて、変更管理・リリース・テストのための安全な手続きを確実に実施しなければならない。
EKM-03: *個人データの保護* – 組織は、認可されないアクセスを回避するために保存データ・移動中のデータ・使用中のデータを暗号化すること等の技術的手段を利用することによって、ユーザーの個人データを保護しなければならない。
HRS-09: *契約者向けのセキュリティ意識向上トレーニング* – 全ての契約者及び全てのサードパーティ・サービスプロバイダーには、組織の各職務に関する手続き・プロセス・ポリシーにおいて、適正なセキュリティ意識、そのトレーニング、定期的なトレーニングの更新が提供されなければならない。
HRS-07: *契約者の役割と責任* – 契約者とサードパーティ・サービスプロバイダーが情報セキュリティに関係する業務契約に文書化される契約者とサードパーティ・サービスプロバイダーの役割と責任。
IAM-02: *アイデンティティ資格・アクセス管理* – 最小権原の原則に基づき、機微なデータへのアクセスを認定ユーザーと認定手続きだけができることを確実にするために導入される十分な技術的・手続的管理。

検知的緩和策

AAC-02: *監査保証とコンプライアンス* – 組織は、ITプロセスとITシステムの独立した監査が計画した時間間隔をとって執り行われ、情報セキュリティとコンプライアンスに照らして特定された発見やギャップが早期に解決されることを確実にしなければならない。

STA-08: *ベンダー評価* – 組織は、組織の情報サプライチェーン全体にわたって遵守されているセキュリティ実務慣行についての合理的保障を獲得するために、ベンダーやアウトソース先のサービスプロバイダーが対応する運用プロセスとセキュリティ・プロセスについて年度単位のレビューを行わなければならない。

TVM-02: *脆弱性/パッチ管理* – パブリック環境に晒されるアプリケーションとインターフェースについての定期的な脆弱性スキャニングは、組織のアプリケーション・システム・ネットワーク構成要素等におけるパッチ漏れに適用する等の、脆弱性についての時節に適う発見と修正に必須です。

是正的緩和策

SEF-02: *セキュリティインシデント管理* – セキュリティインシデント管理手続きを維持すること、そしてインシデント管理のための適正な技術的管理を導入することは、データ漏えい等のセキュリティインシデントに対して組織が時期に適う妥当な対応を提供できるようになることを確実にします。
STA-02: サービスプロバイダー・インシデント報告 – 顧客データを含むデータ漏えいの場合、サービスプロバイダーは、各種の電子的手段を介して、影響を被る全ての顧客に向けてセキュリティインシデント情報が入手できるようにしなければならない。
STA-09: *サードパーティ監査* – 情報セキュリティに関連する契約義務に照らしてコンプライアンス状況を検証するために、全てのサードパーティ・サービスプロバイダーに対する監査を少なくとも年に一度行わなければならない。

指標

重要指標 (KPI):
- サードパーティのサービスプロバイダー要員が実践しなければならないセキュリティ責任を詳細に示すセキュリティ意識向上トレーニング
- パブリックにオープンなアプリケーション、その運用基盤であるインフラストラクチャ、インフラストラクチャとのインターフェースを有する各種コンポーネントでスキャニングされる脆弱性

管理策の効果測定:
- サードパーティのサービスプロバイダーが保守するアプリケーションに関連して報告されるセキュリティインシデントの件数
- パブリッククラウド上のアプリケーション、システム、インターフェースで発見される脆弱性の件数

重要なポイント

- サービスプロバイダーの意書は、サプライヤーのセキュリティ責任を明確に述べなければならない。
- 組織のポリシー、手続き、標準に照らしてベンダーの遵守状況を検証するために、定期的に保証型監査を実施しなければならない。
- 機微なデータがインターネット上でアクセスされる場合は特に、機微なデータ保管を常に暗号で保護しなければならない。

Tesla

脅威アクター	脅威	脆弱性	テクニカルインパクト	ビジネスインパクト	コントロール
内部要因 意図しない内部関係者による管理コンソールへのアクセスの保護の失敗。	**EE5** AWSアクセス認証情報のアカウントハイジャック。	**EE2** Kubernetes管理インターフェースの設定ミス。	**EE1** データ侵害：車両のテレメトリデータの漏洩につながる。	**財政面** - -暗号通貨のマイニングに消費されるリソースのコストが増加する可能性がある。 - 企業の競合他社に貴重な知的財産を盗み出し、競売にかけるリスクの可能性。	**予防** - CCC-04 - EKM-03 - IAM-02 - HRS-09 - TVM-02
	回避的な暗号通貨マイニングスクリプトのインストール。	**EE4** 不十分なIDおよび資格情報管理は、AWSアクセス資格情報の保護の失敗、多要素認証の欠如が原因である可能性がある。			**検知** - CCC-03 - IVS-01 -TVM-01
外部要因 悪意のあるハッカー	侵入を検出するための不十分なセキュリティ監視。	**EE7** 安全でないKubernetesインターフェースがAWSアクセス認証情報を露出させてしまった。	**EE11** 暗号通貨マイニングのためのセキュリティで保護されていないKubernetesインスタンスの悪用と不正使用。	**運用面** - インシデント対応チームがインシデントを修正するために費やした時間と労力。	
	悪意のあるスクリプトの実行を防ぐには不十分なマルウェア対策ソリューション。			**コンプライアンス** - 機微データの露出	**是正** - SEF-02 - SEF-05
				評判 - ブランド価値の低下と消費者の信頼の喪失の可能性	

攻撃の詳細

アクター：外部の悪意のあるハッカーが、セキュリティで保護されていないKubernetes管理インターフェースにアクセスしました。これはセキュリティ研究者によって発見され、テスラに報告されました
攻撃：攻撃者は、セキュリティで保護されていないKubernetes管理インターフェースを介してAWSアクセス認証情報にアクセスしました。これらの資格情報は、非公開の車両テレメトリデータを含むS3バケットへのアクセスをさらに提供しました。さらに、攻撃者はハイジャックされたKubernetesインスタンスにマイニングスクリプトをインストールして、暗号通貨をマイニングしました。
脆弱性：Kubernetesコンソール内の安全な認証メカニズムの設定ミスにより、認証情報を含む機密データへのアクセスが提供されました
•不十分な資格情報管理と効果的な暗号化対策により、ネットワーク全体の横方向の移動が容易になる可能性があります。
•マルウェア対策とセキュリティの監視が不十分で、マイニングスクリプトのインストールの検出と防止に失敗しました。

テクニカルインパクト

データ漏えい：攻撃者は、内部で使用されるエンジニアリングテストカーに関連する知的財産を格納するAWS S3バケットにアクセスすることができました。
マルウェア感染：侵入により、攻撃者は回避的な暗号通貨マイニングスクリプトをインストールできました。コンピューティングリソースを盗むことに加えて、これらの悪質なスクリプトは、適切に検出および修正されない場合、攻撃者が環境内にとどまるための手段を提供します。

ビジネスインパクト

財務：攻撃者が侵害されたネットワーク内で暗号通貨のマイニングに費やした時間の長さによっては、クラウドコンピューティングリソースのコストが増加する可能性があります。
- 貴重な知的財産を盗み出し、最高入札の競合他社に販売するリスクの可能性。

運用：マルウェア感染を管理し、アクセス認証情報を取り消し、Kubernetes管理インスタンスを確実に再構成するために、デジタルフォレンジクスおよびインシデントレスポンス（DFIR）チームが費やした時間と労力。
コンプライアンス：顧客のPII（個人情報）などの機密データが露出されていないため、この攻撃はコンプライアンス違反による直接的な影響を与えない可能性があります。ただし、企業秘密に関連している可能性のある機密データの機密性が失われました。
評判：データ漏えいは、消費者の信頼の低下とブランド価値の認識の低下につながった可能性があります。

予防的緩和策

CCC-04:不正なソフトウェアのインストール---組織は、エンドポイントおよびサーバーへの不正なソフトウェア（マルウェアを含む）のインストールを制限するために、アプリケーションのホワイトリストポリシーを設定する必要があります。
EKM-03:機密データの保護---クラウドに保存されている機密データには暗号化を適用する必要があります。CSPは、クライアント側またはサーバー側の暗号化を選択するオプションを顧客に提供する必要があります。 可能な場合、お客様は、保護されているデータの価値と使用を補完する暗号化メカニズムを選択する必要があります。
IAM-02: 資格証明のライフサイクル / プロビジョニング管理–データにアクセスできるすべてのユーザーに適切なIDとアクセス管理を保証するビジネスプロセスと技術的制御をサポートするユーザーアクセス制御ポリシーの確立。
HRS-09:従業員トレーニング---インテリジェンス主導のセキュリティ意識向上トレーニングをDevOpsチームに安全な開発慣行について提供する必要があります。これは、セキュリティの設定ミスのリスクを緩和するのに役立ちます。
TVM-02:脆弱性/パッチ管理---アプリケーション、インフラストラクチャ、ネットワーク、およびシステムコンポーネントの構成内の弱点をタイムリーに検出することで、実装されたセキュリティ制御の有効性を確保できます。 たとえば、アプリケーションの侵入テストでは、攻撃者に悪用される前に修正する必要がある弱い認証メカニズムの存在を明らかにすることができます。

検知的緩和策

CCC-03:品質テスト---組織は、アプリケーションをテストし、本番環境に展開する前に、変更管理とテストプロセスを定義する必要があります。 これは、システムとサービスの機密性、完全性、および可用性に影響を与える可能性のある誤って構成されたサービスを検出するのに役立ちます。
IVS-01:監査ログ/侵入検知--- CSPは、環境内の潜在的に疑わしいネットワークの動作/異常を検出する機能をお客様に提供する必要があります。さらに、CSPは、フォレンジック調査を支援するために、監査ログの機密性、完全性、および可用性が常に維持されていることを確認する必要があります。
TVM-01:アンチウイルス/悪意のあるソフトウェア---一部のエンドポイント検出および応答（EDR）ソリューションは、マルウェアの侵入の影響を検出および軽減することができます。 完全に網羅されているわけではありませんが、これらのソリューションは、少なくとも、現在も攻撃者によって実際に使用されているコモディティマルウェアまたは公に知られているツールの実行を検出および防止するのに役立ちます。

是正的緩和策

SEF-02: インシデント管理---インシデント対応チームは、疑わしいセキュリティイベントをトリアージ/調査し、インシデント対応プロセス内で確立されたインシデントのタイムリーで徹底的な管理を確保する必要があります。
SEF-05:インシデント対応メトリック---インシデントの管理に費やされた時間とリソースの正当性を提供するために、各インシデントを追跡する必要があります。 これは、インシデント対応プロセスを改善するために必要な投資決定を行う際に経営陣を支援します。

指標

重要指標 (KPI):影響を受けるサーバーにインストールされたウイルス対策ソリューションによって生成された悪意のあるイベントの数、ユーザー行動分析システムによって生成された疑わしいアラートの存在、時間の経過に伴うCPU使用率の傾向、カスタマイズされたユーザーセキュリティ意識向上トレーニングなど。

管理策の効果測定:自動スキャンで明らかに 本番環境に展開する前の構成の弱点、資格情報の定期的なローテーション、最小特権アクセスの実施、重要な資産でのウイルス対策ソリューションの利用など。

重要なポイント

- 緊急時の追加のネットワークとフィルタ容量の手配を含む、詳細でテスト済みのインシデント対応計画を準備します。
- 適切な脅威モデリングを実行します。
- ベストプラクティスのネットワーク設計（ACL、ファイアウォール、ポートとプロトコルのブロック、無効なIPアドレスの拒否）による攻撃対象領域の削減

Zoom

脅威アクター	脅威	脆弱性	テクニカルインパクト	ビジネスインパクト	コントロール
内部要因 Webアプリケーションを保守するサードパーティのサービスプロバイダー。	**EE1** *データ侵害:* Zoomのセキュリティ保護不足を突き、Zoom爆撃者が機微情報を窃取する。	**EE2** *設定ミスと不適切な変更管理* –Zoomアカウントの一部で、パスワードが容易に推測できる(もしくは未設定の)状態で、会議情報を公開していた。	**EE11** *クラウドサービスの悪用・乱用・不正利用:* Zoom爆撃者が幅広く混乱を引き起こした。	**財政面** - CoVID-19による在宅勤務需要の結果、インシデントによる株価下落が緩和 - 罰金の可能性 - 頻繁なコードリリース	**予防** - IAM-02 - IAM-05 - IVS-13 - TVM-02
		EE4 *ID、資格情報、アクセス、鍵の不十分な管理* - 認証情報の使い回しや、弱いパスワードハッシュのチェックに対して、テストが不十分であったため、クレデンシャルスタッフィング攻撃を許した。	*データ損失:* UNCを悪用した漏洩により、企業のWindows環境におけるネットワーク接続保護をバイパスすることができた。	**運用面** - セキュリティの新機能提供 - デフォルト設定の見直し - 会議開催の必要条件について説明 - ハイジャックされたアカウントの復旧	**検知** - AAC-02 - STA-08 - TVM-02
外部要因 未保護のデータにアクセスする外部のユーザー。	**EE5** *アカウントハイジャック:* クレデンシャルスタッフィング攻撃への対策不足により、アカウント認証情報の収集を許してしまう。	**EE7** *安全でないインターフェースとAPI* – 簡素な操作と使用法を追求した、もしくは脅威モデリングを十分に行わなかった。	*国家機密の露見:* ドイツとイギリスの政府が重大なインシデントを起こした。	**コンプライアンス** -機微データの漏洩 -複数の集団訴訟 -アメリカ政府による「政府向けZoom」の提供要請	**是正** - SEF-02 - STA-02 - STA-09
				評判 - 製品の信頼性への疑い - 複数の自治体がZoomを禁止	

攻撃の詳細

アクター: Zoom爆撃を行うスクリプトキディ。アカウント収集を行う外部の攻撃者。
攻撃: 招待していないゲストによるログイン。クレデンシャルスタッフィング攻撃による50万件のユーザーアカウント収集。
脆弱性: CoVID-19パンデミックによってZoomのユーザーが大幅に増加し、2020年初めに複数のインシデントが発生した。いくつかの問題が潜んでおり、ランダム化が不十分で容易に推測できる会議室情報や、幅広く公開している会議室情報に対して、発見的または予防的セキュリティ管理策が十分に備わっていなかった。顧客による認証情報の使い回しは珍しくないが、Zoomは適切な是正的セキュリティ管理策を備えていなかった。最後に、攻撃者は、ZoomのWindowsクライアントに備わるグループチャット機能を使って、Windowsのネットワーク認証情報を漏洩するリンクを共有することができました。これは、ZoomがWindowsのUNCパスをクリック可能なリンクに変換する際に発生します。

テクニカルインパクト

データ侵害: 仮想会議中に、攻撃者が企業の知的財産の機密性を侵害する可能性がある。影響を受ける情報には、ソースコード、営業秘密、その他の機密性が高い情報を含む。
データ損失: チャットセッションでUniversal Naming Convention(UNC)を悪用する漏洩は、ネットワーク保護をバイパスすることにより、Windows共有を使っている企業組織を脅威に晒す。
国家機密の露見: イギリス首相のボリス・ジョンソンは、CoVID-19危機中の政府業務に、会議毎に発行されるコードではなく、固定されたPersonal Meeting ID(PMI)を使った。ジョンソン首相は、スクリーンショットをTwitterに投稿したことにより、会議に加えて、国家業務に関する議論を危険に晒した可能性があります。
認証情報の侵害: 外部からのアカウント収集により、Zoomのユーザー基盤全体で50万件を超えるユーザー名とパスワードが侵害された。
幅広い混乱: 攻撃者は、人種的な扇動や、性的に露骨な画像によって、企業や学校の会議を妨害した。

ビジネスインパクト

財務: 侵害されたシステムによっては、知的財産の喪失から検討段階の戦略の漏洩に至るまで、ビジネスへの影響が大きくなる可能性がある。いくつかの組織が、コミュニケーション基盤としてZoomを使用することを禁止したため、直接、月額サブスクリプションによる収益が減少した。
運用: オペレーションへの影響には、ユーザー情報のリセットにかかる時間と工数を含む。Zoomは、新しいセキュリティ管理策として、会議のロック、待合室、一般的なプライバシーを導入した。Zoom は、問題が起きた6か月の間に、全ての会議でパスワードを必須とし、設定メニューにある会議コードを全て非表示にし、全ての新規会議に対してデフォルトで安全な設定が適用されるようにした。
コンプライアンス: コンプライアンスへの影響には、侵害の開示および通知（個人を特定できる情報の場合）や、規制当局による罰則など、罰金や責任を含む。複数の政府機関が製品のカスタマイズを要請し、政府向けZoomがアメリカのFedRAMP Authority To Operateを取得した。
評判: Zoom爆撃の影響を受けたZoomユーザーは、言葉遣いや映像に起因する否定的なイメージにより風評被害を受けた可能性があります。ニューヨークの州立学校、Google、ドイツ政府など、複数の組織がZoom会議を直ちに禁止した。このような動きは、組織の顧客や一般の人々に見えるかたちで発生した。

予防的緩和策

IAM-02: *資格証明のライフサイクル / プロビジョニング管理* – 使い捨ての会議IDとランダムな会議の暗証番号の導入により、攻撃者が、過去の会議招集を利用したり、新しい会議を推測したりする機会を最小化します。
IAM-05: *職務の分離* – 会議へのアクセス（会議への接続）と管理者の役割（画面共有や待合室からの入室許可）分離することにより、Zoom爆撃を困難にします。
IVS-13: *ネットワークアーキテクチャ* – セキュリティとプライバシーの管理策などの技術的対策は、脅威モデリングを行いながら設計することにより、会議開催の非公開や適切な乱数の使用を反映します。
TVM-02: *脆弱性／パッチ管理* – 脅威に対するテストで、未招待の従業員による攻撃経路を明らかにできなかったため、厳格なポリシーの実装や、会議パスワード、開催者より早い会議参加の禁止、参加者による画面共有、会議開始後のロックに対するデフォルト設定を考慮することができなかった。

検知的緩和策

IAM-02: *資格証明のライフサイクル／プロビジョニング管理* – 侵害されたパスワードの一覧に対して、アカウントの認証情報をチェックする。認証情報の使い回しに対して、パスワードハッシュやレインボーテーブルを使ったテストを行う。パスワードリセット、特権の使用、クレデンシャルスタッフィング攻撃の可能性など、アカウントパスワードの乱用を監視します。
IAM-12: *ユーザアクセスレビュー* – 個人用会議室の利用、不自然なアカウントの振る舞い、重要なプロフィールの変更についてデータ分析を行う。アカウント作成、削除、普段使われないアカウントの監視により、管理者の設定に普段と差異がないか監査します。開催された会議、ゲストが使用したID、ゲストがどこから参加したかなどの指標を記録します。
GRM-02: *データフォーカスリスクアセスメント* – チャットや仮想環境における他手段によって、データが外部に共有される。監査やログ取得のため、サードパーティのCASB監視ツールを検討します。

是正的緩和策

EF-02: *インシデント管理* – インシデント対応チームが即時対処を担当する。プレイブックの共有により、事象への誤った対処や解決までの時間を最小化します。
SEF-04: *インシデントレスポンスの法的準備* – フォレンジック調査には、正確で法廷に認められる証拠が必要である。会議の妨害から児童ポルノの掲示まで、いくつかの訴訟がアメリカ国内で係争中です。
HRS-09: *訓練／認識向上* – Zoomは、新しいセキュリティ機能を迅速に実装した。待合室の作成や、開催者より早い会議参加の禁止、デフォルトでの会議パスワード設定など、新しいセキュリティ機能についてユーザーを訓練します。
TVM-02: *脆弱性／パッチ管理* – Zoomはソフトウェア製品であり、サイバー犯罪者は、古いバージョンを標的にする傾向があります。

指標

重要指標 (KPI):
- 認証情報データベースに対するテストの規模
- テストを実施した認証情報の割合
- ユーザーの振る舞い分析

管理策の効果測定:
- ヘルプデスクに対する苦情
- 顧客の満足度調査

重要なポイント

- 適切な脅威モデリングを行うことにより、セキュリティアーキテクトと開発者に、管理策の不備を評価する機会が生まれます。
- セキュリティの保護は、後付けをするのではなく、あらかじめ組み込む。
- アジャイル開発は、機能要件に対する迅速な対応を可能にします。

Glossary

Capital One

EC2 - Amazon Elastic Compute Cloud
GDPR - 一般データ保護規則
IMDS - アマゾンウェブサービスのインスタンスメタデータサービス version 1
S3 - Amazon Simple Storage Service
SSRF - サーバーサイドリクエストフォージェリ
VPN - 仮想プライベートネットワーク
WAF - Webアプリケーションファイアウォール

Disney+

クレデンシャルスタッフィング - 侵害されたユーザクレデンシャルリストを用いて攻撃者がシステムに侵入するサイバー攻撃方法です。攻撃者はボットを使用して自動化とスケーリングを行い、また、多くのユーザーが複数のサービス間でユーザー名とパスワードを再利用しているという想定に基づいています。

Dow Jones

Elasticsearch - Elasticsearchは、Apache Luceneで構築されたオープンソースの分散データ検索および分析エンジンです。RESTful APIまたはLogstashなどの取り込みツールを使用して、JSONドキュメント形式でデータをElasticsearchに送信できます。Elasticsearchは自動的に元のドキュメントを保管し、クラスタのインデックスに対し、当該ドキュメントを検索可能とする参照先を追加します。その後、Elasticsearch APIを使用してドキュメントを検索および取得できます。AmazonはフルマネージされたElasticsearchサービスを提供しており、Elasticsearchのデプロイ、セキュリティ確保、および大規模な運用を可能にしています。
IoT検索エンジン - コンピューティング機能を内蔵している物理デバイスを検索できるInternet of Things (IoT)サーチエンジン
- インターネットに接続され、インターネットを介してデータ交換可能なWebカメラ、家電製品、医療機器など。IoT検索エンジンの2つの例は、Thingful（ https://www.thingulf.com ）とShodan（ https://www.shodan.io ）です。
政治的に露出している人物 -著名な地位や影響力を持つことで、贈収賄や汚職に関与する可能性が高い人物。

Github

アンプ攻撃 - 攻撃者が単一接続上で可能な能力よりも多くのリソースを用いる攻撃。増幅係数は、少ないリソースでターゲットの被害が大きくなるという非対称性を利用して攻撃力を倍増させます。**Memcachedサーバー** - 動的データベースで駆動されるWebサイトで速度を向上させるために使用される、汎用分散メモリキャッシングシステム。
Memcrashing - UDPポート11211上のMemcachedサーバーの弱点を利用してアンプ攻撃を実行し、ホスティングサーバを麻痺させること。
ポート11211 - Memcachedクライアントはクライアントサイドのライブラリを使用してサーバーに接続します。デフォルトでは、Memchachedサーバーは、TCPとUDPの両ポート11211でサービスを公開します。
UDP - (User Datagram Protocol) は主に、低レイテンシーで耐欠損性を持つインターネット上のアプリケーション間の接続を確立するために使用される通信プロトコルです。

Imperva

Unknown threat actor - 未認可なアクセスは確認されたが、攻撃者に関するアイデンティティやその他の情報は一切公開されていないもの。全く知られていないことが多いかどうかは疑問である。
GDPR - 一般データ保護規則
AWS EC2 - Amazon Web Servicesのサーバワークロード（エラスティックコンピュート）サービスで、主にAWSインフラ上で顧客が実行する仮想マシンとして使用されます。
AWS API Access Key - AWS APIのプログラムによる使用を目的としている、ユーザー名/パスワードクレデンシャルとは異なるAWSユーザーの認証情報ペア。

Ring

なし。

Tesco

Unknown threat actor - 未認可なアクセスは確認されたが、攻撃者に関するアイデンティティやその他の情報は一切公開されていないもの。全く知られていないことが多いかどうかは疑問である。
GDPR - 一般データ保護規則
AWS EC2 - Amazon Web Servicesのサーバワークロード（エラスティックコンピュート）サービスで、主にAWSインフラ上で顧客が実行する仮想マシンとして使用されます。
AWS API Access Key - AWS APIのプログラムによる使用を目的としている、ユーザー名/パスワードクレデンシャルとは異なるAWSユーザーの認証情報ペア。

Tesla

Kubernetes - 複数のホストにまたがる、コンテナ化されたアプリケーションのデプロイメント、スケーリング、および管理を自動化するためのオープンソースのコンテナオーケストレーションシステム。

Zoom

Zoombombing - 招待されていない者がビデオ会話を乗っ取り、通常の議事を妨害する行為。
Credential Stuffing - 攻撃者は既知のユーザー名とパスワードのデータベースを取得し、他のデジタルサービスのログインページへそれらのクレデンシャルの「詰め込み」を試行すること。複数のサイトでパスワードが再利用されていることから、攻撃者は多くの場合、1つのクレデンシャル情報を使って複数のアカウントのロックを解除できることがよくあります。
UNC - 初期における、エンタープライズ環境内のシステムを識別するための方法として、Windowsが提供していたユニバーサル命名規則。

References

Capital One

Capital One Breach Details

1. https://cloudsecurityalliance.org/blog/2019/10/10/cloud-penetration-testing-the-capital-one-breach/
2. https://cloudsecurityalliance.org/blog/2019/08/09/a-technical-analysis-of-the-capital-one-cloud-misconfiguration-breach/
3. https://www.capitalone.com/facts2019/
4. https://www.scmagazine.com/home/security-news/capital-one-breach-exposes-not-just-data-but-dangers-of-cloud-misconfigurations/
5. https://krebsonsecurity.com/tag/capital-one-breach/
6. https://krebsonsecurity.com/tag/paige-a-thompson/
7. http://web.mit.edu/smadnick/www/wp/2020-07.pdf

SSRF

8. https://www.hackerone.com/blog-How-To-Server-Side-Request-Forgery-SS
9. https://blog.appsecco.com/server-side-request-forgery-ssrf-and-aws-ec2-instances-after-instance-meta-data-service-version-38fc1ba1a28a

Estimated cost of Capital One breach

10. https://fortune.com/2019/07/31/capital-one-data-breach-2019-paige-thompson-settlement/
11. https://www.forbes.com/sites/greatspeculations/2019/09/11/how-could-the-recent-data-breach-affect-capital-ones-stock/#f2faa4437b79
12. https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-101.html

Job Loss at Capital One

13. https://www.bankinfosecurity.com/following-massive-breach-capital-one-replacing-ciso-report-a-13385

Regulatory Breach Fines and Penalties

14. https://techcrunch.com/2019/07/22/equifax-fine-ftc/#:~:text=FTC%20slaps%20Equifax%20with%20a%20fine%20of%20up,M%20for%202017%20data%20breach&text=Credit%20agency%20Equifax%20will%20pay,a%20data%20breach%20in%202017.

Disney+

15. https://www.wired.com/story/disney-plus-hacks-credential-stuffing/
16. https://www.zdnet.com/article/thousands-of-hacked-disney-accounts-are-already-for-sale-on-hacking-forums/
17. https://blog.eccouncil.org/disney-plus-accounts-hacked-within-hours-of-its-most-awaited-launch-heres-how/
18. https://popculture.com/streaming/news/quarantine-disney-plus-users-hacked-accounts/
19. https://medium.com/online-io-blockchain-technologies/thousands-of-disney-plus-accounts-got-hacked-heres-why-f2f0b7b569a2
20. https://www.imperva.com/learn/application-security/credential-stuffing/#:~:text=Credential%20stuffing%20is%20a%20cyberattack,and%20passwords%20across%20multiple%20services.

Dow Jones

21. Amazon Elasticsearch Service
22. Cloud Leak: WSJ Parent Company Dow Jones Exposed Customer Data – Dan O'Sullivan
23. Data Breaches/Privacy – Justia
24. Dow Jones Risk Screening Watchlist Exposed Publicly in a Major Data Breach – Bob Diachenko
25. Dow Jones Watchlist of risky businesses exposed on public server – Lisa Vaas
26. Dow Jones' watchlist of 2.4 million high-risk individuals has leaked – Zack Whittaker
27. The what, why and how of IoT search engine – FutureIo Editors
28. What is a Politically Exposed Person (PEP)? – Accuity

Github

29. https://www.theregister.co.uk/2018/03/05/worlds_biggest_ddos_attack_record_broken_after_just_five_days/
30. https://www.theregister.co.uk/2018/03/01/github_ddos_biggest_ever/
31. https://www.globaldots.com/memecached-servers-ddos-attacks-complete-analysis/
32. https://www.geekwire.com/2018/memcached-servers-used-launch-record-setting-ddos-attacks/
33. https://memcachedscan.shadowserver.org/stats/

Imperva

34. https://www.imperva.com/blog/ceoblog/
35. https://krebsonsecurity.com/2019/08/cybersecurity-firm-imperva-discloses-breach/

Ring

36. https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers
37. https://www.geekwire.com/2020/ring-customers-cameras-breached-hackers-sue-amazon-proposed-class-action-lawsuit/
38. https://www.eff.org/deeplinks/2019/12/ring-throws-customers-under-bus-after-data-breach
39. https://www.businessinsider.com/amazon-ring-passwords-credit-card-exposure-leak-hack-2019-12
40. https://securitytoday.com/articles/2019/12/23/ring-faces-intense-scrutiny-after-hacks.aspx
41. https://www.securitymagazine.com/articles/91469-amazon-ring-leaks-thousands-of-customer-data
42. https://abcnews.go.com/US/amazon-ring-face-million-proposed-class-action-lawsuit/story?id=67948687

Tesco

43. https://www.theregister.co.uk/2019/09/20/tesco_parking_app_10s_millions_anpr_photos_exposed/
44. https://cyware.com/news/unsecured-microsoft-azure-blob-exposes-millions-of-automatic-number-plate-recognition-images-9b04c528
45. http://securitydive.in/2019/09/how-the-tescos-parking-app-exposed-millions-of-automatic-number-plate-recognition-images/
46. https://thedataprivacygroup.com/blog/2019/9/23/tesco-shutters-parking-app-following-license-plate-image-leak
47. https://www.techradar.com/news/tesco-shutters-parking-app-following-license-plate-image-leak
48. https://www.anprcameras.com/about-us/understanding-anpr/
49. https://panopticonblog.com/2016/11/10/anpr-personal-data/

Tesla

50. https://info.redlock.io/hubfs/WebsiteResources/RedLock_CSI_report_May2018.pdf
51. https://www.zdnet.com/article/tesla-systems-used-by-hackers-to-mine-cryptocurrency/
52. https://www.osradar.com/tesla-cloud-account-data-breached/
53. https://fortune.com/2018/02/20/tesla-hack-amazon-cloud-cryptocurrency-mining/
54. https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html
55. https://kubernetes.io/
56. https://github.com/kubernetes/kubernetes

Zoom

57. https://www.npr.org/2020/04/03/826129520/a-must-for-millions-zoom-has-a-dark-side-and-an-fbi-warning
58. https://www.sumologic.com/blog/zoom-security-challenges/
59. https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/
60. https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/
61. https://www.npr.org/2020/04/03/826968159/senator-zoom-deceived-users-over-its-security-claims
62. https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic
63. https://www.lawfareblog.com/prosecuting-zoom-bombing
64. https://www.pcworld.com/article/3535213/how-to-prevent-zoom-bombing-by-being-smarter-than-boris-johnson.html