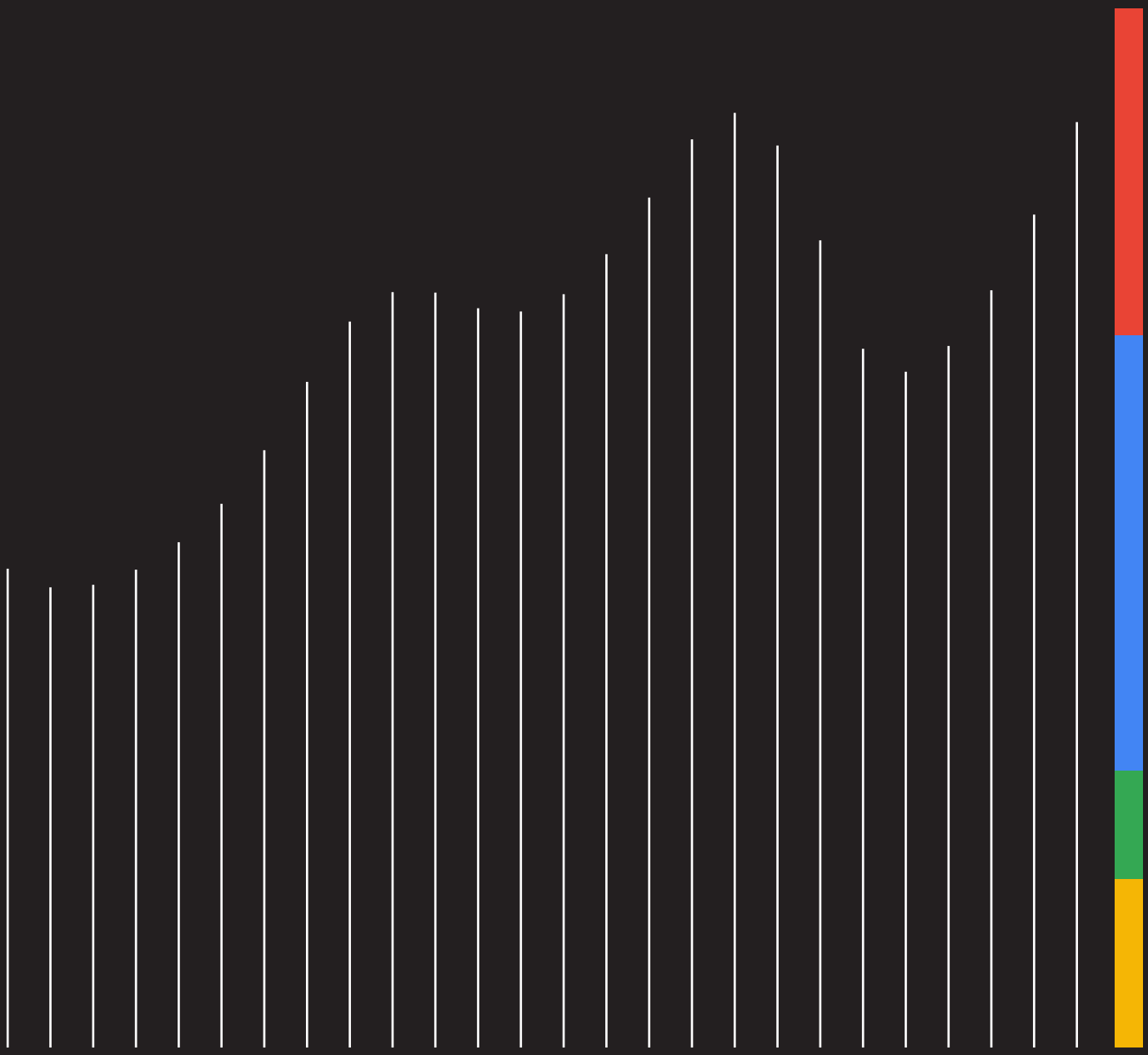
Mandiant

Google Cloud Security

M-Trends

2024 スペシャル・レポート

エグゼクティブ エディション



数字で見る: M-Trends のデータ

M-Trends 2024 で報告されている指標は、標的型攻撃に関して 2023 年 1 月 1 日から 2023 年 12 月 31 日までの期間に Mandiant Consulting が行った調査に基づくものです。

概要

- 滞留時間とは攻撃者がシステムに侵入してから検知されるまでの日数のことですが、世界全体で見た 2023 年の滞留時間の中央値は 10 日間であり、2022 年の 16 日間に比べて短くなっています。
- ランサムウェアを用いた事例の場合、世界全体で見た滞留時間の中央値は前年が 9 日間であったのに対し、当年は 5 日間です。
- システムへの侵入を外部ソースからの通知で初めて知った組織が 54% であったのに対し、侵入を組織内で検知した組織は 46% でした。2022 年には外部からの通知が 63% を占めていたことと比較すると、悪意のある行為に対する組織内の検知能力が高まっていることが示唆されています。
- ランサムウェアによる事例の 70% で、外部ソースからの通知を受けて組織が侵入を認識しています。外部ソースからのそうした通知のうち 76% が攻撃者からのものであり、24% が外部パートナーからのものでした。
- Mandiant が侵入に対応した回数が最も多かった業種は金融サービス機関（17.3%）であり、次いでビジネスおよびプロフェッショナル サービス（13.3%）、ハイテク（12.4%）、小売およびサービス業（8.6%）、医療（8.1%）、政府機関（8.1%）の順になっています。そうした業種の組織は、攻撃者にとって魅力的なさまざまなセンシティブ データを扱っています。
- 一般的な最初の感染経路は、脆弱性の悪用（38%）、フィッシング（17%）、過去の侵害（15%）、盗まれた認証情報（10%）でした。これらの数字は、2022 年のものとそれほど変わっていません。
- 動機を特定できた事例については、攻撃者の 52% が金銭上の利益を主な目的とし、10% がスパイ活動を主な目的としていました。金銭目的の攻撃は 2022 年の 48% から増加しています。これは、2023 年にランサムウェアと恐喝の事例が増加していることをある程度反映するものです。
- 2023 年に新たに追跡対象となった 626 種のマルウェア ファミリーの中で上位に位置付けられたものには、バックドア（33%）、ダウンローダー（16%）、ドロッパー（15%）、クレデンシャル スティーラー（7%）、ランサムウェア（5%）があります。

必要とされる行動

- 強力なインテリジェンスを活用したプロアクティブな脅威ハンティングを行うサイバー セキュリティ体制の構築と維持を行います。
- レッドチームとの演習で防御態勢のテストと不備な点の特定を行うとともに、侵入の検知と対応をセキュリティ チームが行うのに要する時間を計測します。
- 最新かつ最も関連性の高いマルウェア、脆弱性の悪用、最初の感染経路の各々に対する検知能力をテストするとともに、すべての従業員を対象としてフィッシングに関する意識などのテストを定期的に実施します。
- 机上演習などの訓練により手順を確立し、インシデント対応に関与するすべての従業員がいつでも（特に侵入が外部から通知された際に）対応できるようにしておきます。
- 脆弱性と漏えいに関する管理、最小権限の原則、ネットワーク セグメンテーション、セキュリティの強化といったセキュリティの基礎を徹底して実践します。

中国のスパイ活動
可視性の問題点が標的に

概要

- 中国(など)につながる攻撃者は、従来エンドポイント検知と対応(EDR) などのセキュリティソリューションが不足しているエッジデバイスやプラットフォームを標的にすることが増えてきています。
- これらのシステムを標的にし、ゼロデイを悪用することで、攻撃者は環境内の死角を利用して検出リスクを低減させながら、長期間システムに潜伏することができます
- 中国のスパイグループは検知を回避するために、ゼロデイ・エクスプロイトの獲得や、特定のプラットフォームを対象としたツールの整備に今後も注力し続ける可能性があります。
- 中国のスパイ活動グループは、引き続き、デバイスや目的に合わせてカスタマイズされたマルウェアエコシステムを展開すると予想されます。

必要とされる行動

- パッチの管理を継続的に行って、既知の脆弱性が悪用されるリスクを低減します。
- ゼロデイ脆弱性については、多層防御のアプローチにより、攻撃ライフサイクルが進む中で悪意のある活動の痕跡を検出できる可能性が高まります。
- 侵入が行われている可能性が示唆された場合、調査を行うとともに、ログを確認して侵入の形跡がないかを調べるなどのハンティング活動を実施します。
- 侵入が発生した場合、徹底的かつ包括的な調査を実施して、攻撃者がどのようにして環境内に入り込んだのか、また、どのようにして滞留し続けたのかを明らかにします。
- セキュリティ ベンダーが提供するアーキテクチャー強化ガイダンスに詳述されているセキュリティ管理手法の実装を検討します。

ゼロデイを対象とした攻撃活動
目的によりさまざま

概要

- 2023 年には、実際の環境で悪用されたゼロデイ脆弱性が合わせて 97 件確認されました。これは 2022 年の件数を 50% 以上も上回る結果です。
- 2023 年にゼロデイを悪用した攻撃者の中でも特に目立ったのは中華人民共和国のサイバー エスピオナージ グループであり、ゼロデイを対象とした活動で特にステルス型に焦点が当たっていました。
- 金銭目的の攻撃者は引き続きゼロデイを利用してシステムに侵入し、貴重なデータを盗み出して利益を得ることを目指しています。
- スパイ目的のグループは、探知されることなく長期間にわたって滞留することを重視する傾向があり、注意深くセキュリティ上の脆弱性を利用し、検知の可能性を可能な限り低減します。金銭目的の攻撃者は、スピードと効率を重視する傾向があり、ステルス性を犠牲にして、より早く利益を得たり、より広範に悪用を行ったりしようとする場合があります。

必要とされる行動

- ポリシー、脅威インテリジェンス、アクティブ モニタリングを組み合わせれば、ゼロデイを悪用しようとする攻撃者に対抗する早期警戒システムとして機能します。
- インシデント対応計画を確立し、環境モニタリングを幅広く行って、脆弱性が環境に及ぼす潜在的影響を評価する体制を強化します。
- レイヤ ネットワーク セグメンテーションと、効率的な対策を目的とした高度な EDR ソリューションを用いたロギングを行って、調査の開始と速やかな終結が可能になるようにします。
- ハードウェアとソフトウェアを環境内にデプロイする前に、ベンダーを対象としたセキュリティ プラクティスとネットワーク要件の評価を実施して、「通常の」使用と見なされるべきものに対する質的ベースラインを確立します。

進化するフィッシング
変容するセキュリティ対策への適応

概要

- 最近のフィッシング技術は、ユーザー教育やメール ゲートウェイ フィルタリング、MFA を重視してきた従来からのセキュリティ パラダイムに挑戦する存在です。
- 攻撃者は、現在用いられている数々のセキュリティ対策をかわすために、LNK ファイルや、兵器化された新たな形式の Microsoft Office ドキュメントなどの、さまざまなタイプのペイロードをばらまく実験を開始しています。
- 攻撃者は、攻撃対象の範囲を拡大してきています。現在ではメールにとどまらず、ソーシャル メディアや SMS メッセージなどの一般的なコミュニケーション プラットフォームを対象とするようになっています。
- 攻撃者は、会話の乗っ取りのような手法を使ったり、単に内部ユーザーを装ったりすることで、信頼関係やコミュニケーションを悪用しています。

必要とされる行動

- 侵入ライフサイクルのあらゆる段階で現れる行動の形跡に焦点を当てた、検知と脅威ハンティングに関する包括的な戦略を策定します。
- フィッシング攻撃が最初に発見されるのは、リスクを内包するログインの発生、メールボックス ルールの作成、不審な MFA デバイスの登録といったことに対するクラウド上のセキュリティ通知によることもあれば、不正使用されたユーザー アカウントから送られてきた不審なメールに関する内部ユーザーや外部ユーザーからの報告によることもあります。
- 通知が不審なアクティビティに対して生成されていることを確認し、ユーザー間でやりとりされたメッセージや URL が記録されている可能性のあるプラットフォーム ログを確認します。不審な内容に対して予防的な分析を行うことができます。

AiTM を利用して MFA を突破する攻撃者の実態

概要

- 多要素認証（MFA）を使って構成されたクラウドベースの ID を標的とした侵害の件数が増えています。
- 攻撃者は、MFA を突破する技術を磨いてきています。特に、保護されるべきログイン セッション トークンを盗むことで MFA の実装内容を無効化することができる手法（ウェブプロキシや AiTM（Adversary-in-the-Middle）フィッシング ページ）を使用するようになっています。
- 現在でも多くの組織がトークンの盗難を防止できないセキュリティ対策に依存していますが、トークンの盗難と、盗難にあったトークンの使用を抑制するシンプルな解決策は現在も存在しません。

必要とされる行動

- AiTM に耐性のある MFA の手法とアクセス ポリシーを追求します。
- ほとんどのクラウド認証サービスが、組織で定義した場所、デバイス管理状態、または履歴に残っているアカウントのログオン プロパティに基づくリスク評価を基準としてログオンをブロックできるアクセス ポリシーをサポートしています。
- 防御には、地理的にあり得ない（または思いもよらない）ソース IP アドレスや、データセンターで発生しているログイン操作のような異常のモニタリングが必要とされます。
- 認証ログには、フィッシングに使われたインフラストラクチャに関連付けられた IP アドレスが、ユーザーのソース IP アドレスとして記録され、盗難にあったトークンを使って認証が行われると、IP アドレス、および関連付けられたユーザー エージェント文字列も記録されることになります。

クラウドで見られる侵入のトレンド

概要

- クラウド環境や、クラウドとオンプレミスのハイブリッド環境の採用が企業で続けられている中、攻撃者もこれに追随してきています。
- さまざまな動機を持つ攻撃者がクラウド環境に目を転じて、クラウドでホストされたデータを標的とするようになると同時に、自分たちの活動にクラウド コンピューティング リソースを活用するようになっています。
- 攻撃者は、ID 管理の実践が十分に行われていない箇所と認証情報ストレージを標的として、正規の認証情報を取得し、MFA をすり抜けています。

必要とされる行動

- 認証ポリシーを変更して、強力なセキュリティ ポスチャーを維持します。
- 証明書ベースの認証や FIDO2 セキュリティ キーのような、広く受け入れられているフィッシング耐性のある MFA 手法を使用し、SMS、電話、時間ベースのワンタイム パスワードのような旧来の MFA 手法を廃止します。
- 追加的な対策を実施して、信頼性の確保されたデバイスにクラウド リソースへのアクセスを限定します。

AI とレッドチーム（およびパープルチーム）の活動

概要

- サイバーセキュリティの分野で生成 AI が大きな可能性を秘めているのが、予防的セキュリティとレッドチームによる評価の分野です。
- Mandiant のレッドチームは、生成 AI ツールをソーシャル エンジニアリングに利用してきました。特に、悪意のあるメールの下書きを作成する際に利用してきましたが、正規のものに見せかけたランディング ページを作成する際にも利用してきました。
- Mandiant のコンサルタント チームも、レッドチームとの演習を行うなか、生成 AI を利用してカスタムツールの開発を支援してきました。
- Mandiant のチームは、生成 AI を利用してさまざまなプラットフォームに対する理解を深めることで、そうしたプラットフォームのセキュリティに関する側面を明らかにしてきました。

必要とされる行動

- レッドチーム診断により事前に合意済みの攻撃を実行し、全般的なセキュリティの有効性を検証して改善に生かします。

レポート全文をダウンロードする。

Google Cloud

詳細: cloud.google.com