MANDIANT
NOW PART OF Google Cloud

M-Trends 2023 スペシャル・レポート

エグゼクティブ・サマリー

今回で第14号となる『M-TRENDS 2023』は、www.mandiant.jp/m-trendsで入手できます

数値で見る被害の統計 - M-Trendsデータ

提供される情報は、2022年1月1日～2022年12月31日の期間にMandiantコンサルティングが行った調査に基づきます。

知っておくべきこと

- 世界的に見て、攻撃はより早期に検知される傾向になっており、南北アメリカとEMEA地域では改善が見られます。しかし、APAC地域では改善されていません。
- 侵害の検知・報告は、組織のセキュリティチームよりもセキュリティ・ベンダーなどの外部ソースによって行われるケースが多くなっています。しかし、組織内のチームが攻撃を検知する場合は、外部ソースから報告される場合よりも早期に行われます。
- 攻撃者は、組織へのアクセスを得るために、地域ごとに最も有効な手法を用いています。南北アメリカではエクスプロイト、EMEAではフィッシング、APACでは過去の侵害が利用されています。

CISOへの質問

- 検知と対応にかかる時間の測定方法と、検知から対応や修復までにかかる時間の中央値は？
- 最も一般的なマルウェア、エクスプロイト、フィッシングなどの初期感染経路に対する検知・対応への備えは万全か？
- 第三者から侵害の可能性があると連絡を受けた際の対応手順はどうなっているか？
- 既知の脆弱性があるシステムに対して、エクスプロイトを確実に回避するためにどのような態勢を取っているか？

ウクライナ侵攻

知っておくべきこと

- Mandiantでは、2022年2月24日のロシアによるウクライナ侵攻前にも侵攻後にも、大規模なサイバー・エスピオナージ活動、妨害攻撃や破壊的サイバー攻撃、情報操作工作が行われていることを確認しています。
- ロシアの活動は産業制御システムや重要インフラに被害をもたらしています。その中には、侵攻前に行われた活動や取得したアクセスによって可能になったものもあります。
- ロシアのウクライナ侵攻は、新たなデ・ファクト・スタンダードとして、サイバー活動と実際の戦闘とが重なり合う可能性を示しています。

CISOへの質問

- 妨害攻撃や破壊的な攻撃に対して、システムを強固にするための対策をとっているか？
- バックアップと事業継続計画に対する直近の検証結果はどうだったか？
- 情報操作工作に対抗するために脅威インテリジェンスを活用すべきか？

北朝鮮による金銭目的の攻撃

知っておくべきこと

- 2022年、北朝鮮の工作員は、従来の情報収集の任務や破壊的な攻撃のほかに、暗号通貨の窃取と使用にも高い関心を示しました。
- これらは利益が高く魅力的な活動であり、2023年もその勢いが続くと見られます。

CISOへの質問

- 自組織が警戒すべき金銭目的の脅威に対して、どの程度準備ができているか？

焦点の変化と一般的ではない手法

知っておくべきこと

- 技術的スキルの低い攻撃者が、大きな被害をもたらすようになっています。
- このような攻撃によって、データの窃取、知的財産の窃取、社会的信用の失墜が生じています。
- このような攻撃者は、金銭目的やエスピオナージよりも、標的組織の評判をおとしめることを動機としており、処理能力が高く、目的を達成するためには賄賂や嫌がらせ、脅迫も厭わないようです。

CISOへの質問

- ソーシャル・エンジニアリングなどの脅威が従業員に及ぶリスクを防ぐために、どうしているか？
- このような攻撃から従業員（特に経営幹部や目立ちやすいポジションにある従業員）を守るために、どのようなプログラムがあるか？
- 機密情報や顧客の個人情報が窃取され、それを脅迫に使われた場合、どのように対応するか？
- 脅迫に対応する際に、暗号通貨を迅速に取得するための手順があるか？

クラウド重視 – レッドチームの事例

知っておくべきこと

- レッドチーム演習を実施することで、実際の攻撃シナリオに対する自組織のセキュリティ・プログラムの対応能力を評価し、セキュリティ態勢を改善することができます。
- Mandiantは、ある公益企業に対し、重要なクラウドや運用テクノロジー環境のリソースに攻撃者がアクセスする方法を実際に示しました。

CISOへの質問

- 組織のクラウド利用状況について、正確かつ完全に把握できているか？
- 攻撃者が悪用できるような設定ミスの有無を定期的にチェックしているか？
- クラウド・アーキテクチャ導入のテストを行っているか？

攻撃活動と世界的なイベント

知っておくべきこと

- 2022年、Mandiantのキャンペーンおよび世界イベント担当チームは、顧客の保護を強化するため、ロシアのエスピオナージ活動、ランサムウェア、Log4Shellなどの重要な脆弱性について調査を行いました。
- Mandiantは、こうした活動から顧客や地域社会が身を守れるよう、貴重なインテリジェンスや指標を共有しています。

CISOへの質問

- ネットワークの脆弱性を追跡し、パッチを当てるために何を行っているか？
- 最新の脅威インテリジェンスを意思決定にどのように活かしているか？

APT42 - 注目すべき昇格

知っておくべきこと

- APT42は、高度なフィッシング攻撃やソーシャル・エンジニアリング攻撃を用いてエスピオナージ活動を行う、イランが関与する攻撃グループです。
- APT42の活動は、特に米国、英国、イスラエルにおけるイラン関連のプロジェクトに携わる外交政策担当者、評論家、ジャーナリストにとって脅威となっています。

CISOへの質問

- 全従業員を守るために、セキュリティ、IT、業務の各チームに何ができるか？
- ソーシャル・エンジニアリングの脅威が従業員に及ぶリスクを、どのように低減しているか？
- フィッシングなどのソーシャル・エンジニアリング攻撃について、従業員にどのように認識させるか？

詳しくはwww.mandiant.jp/m-trendsをご覧ください。

マンディアント

〒106-0032 東京都港区六本木6丁目10番1号
六本木ヒルズ森タワー | 03-4577-4401 |
japan@mandiant.com

Mandiantについて

Mandiantは、ダイナミックなサイバー防御、脅威インテリジェンス、インシデントレスポンス・サービスのリーダーとして知られています。長年にわたり攻撃の最前線で得た豊富な経験を活かし、サイバー脅威に対する防御と対応においてお客様組織を支援します。Mandiantは現在、Google Cloudの一部です。

MANDIANT
は現在、Google Cloud の一部です。