MANDIANT®

ソリューション・ブリーフ

Mandiant Managed Defenseで戦略的ランサムウェアの脅威を回避する

メリット

- **重要なアラートに注目**
  専門家のサポートにより、組織の環境全体で技術的アラートを監視し、特定、調査、優先順位付けを行います。そこから、優先すべきアラートが絞り込まれ、コンテキスト情報とともに提供されます。
- **隠れた攻撃者を発見**
  MITRE ATT&CKフレームワークにマッピングされた予防的な脅威ハンティングにより、隠れた侵害や潜在的なサイバー攻撃を検知します。
- **迅速に阻止して対応**
  Mandiantのインシデント対応担当者とセキュリティ・アナリストにより蓄積された知識と経験を駆使して、Managed Defenseの専門家が攻撃への対応をサポートします。
- **セキュリティ・チームの能力をレベルアップ**
  専任のセキュリティ専門家チームが、組織のセキュリティ・チームにトレーニングとアドバイスを提供し、差別化されたサイバー・セキュリティの知識を共有し、組織の環境についての理解を深めます。
- **防御力の強化**
  関連する脅威インテリジェンスを踏まえた、継続的な診断と推奨事項を提供し、組織のセキュリティ体制を強化します。

ランサムウェア攻撃は2017年以降、頻度も深刻度も急速に増してきています。当初は妨害行為だと思われていたものが、高度なサイバー攻撃者によって、データの暗号化と情報の危殆化の脅威とを組み合わせた複雑かつ多段階の攻撃へと進化しています。これと時期を同じくして、攻撃者たちは、マルウェアを広範にばら撒く攻撃から、特定の組織や業界、場合によっては都市全体を標的とした攻撃へと対象を拡大してきました。現在、ランサムウェア攻撃の身代金の額は数百万ドルに達することもあります。

こうした脅威の進化に対応すべく、多くの組織がランサムウェアに対抗しうる戦術を評価、開発、更新し、対応の強化を図ってきました。Mandiant Managed Defenseのような効果的なManaged Detection and Response（MDR）機能があれば、APT攻撃グループが戦略的に展開するランサムウェアなどの脅威リスクを軽減できます。また、セキュリティ対策がきちんと実施されていることを経営陣や役員に示すこともできます。このような対策機能を社内で達成しようとすると、時間もかかり、リソースも必要になります。

Managed Defenseでランサムウェア対策

Managed Defenseでは、日々攻撃への対応や保護に携わっている専門家が、ランサムウェアを用いた高度な戦術や攻撃にさらされている組織をサポートします。

あらゆる攻撃経路からの重大な脅威を監視する

ランサムウェアを用いる攻撃者は、さまざまな攻撃経路を経由して標的の環境に入り込みます。経路としては、リモート・デスクトップ・プロトコル、不正なリンクや添付ファイルを用いたスピア・フィッシング・メール、不正なWebサイトからのドライブバイ・ダウンロードなどが挙げられます。侵入後、攻撃の成功率を高めるために、重要なシステムやデータを特定します。

多くの組織にとって、侵入後の高度な攻撃を検知するためには、企業全体にわたる可視性とコントロールを得ることが必須です。ここには、無数のエンドポイントや、現在急速に拡大しているネットワーク境界なども含まれます。Managed Defenseは、エンドポイントにとどまらず、エンドツーエンドのネットワークの可視性を維持することによって、不自然な振る舞いを特定し、重要なアラートの優先度を判断して調査を行います。さらに、Mandiantの専門家が、Eメールの行動から攻撃者の新たなトレンドやランサムウェアの配信メカニズムを特定します。

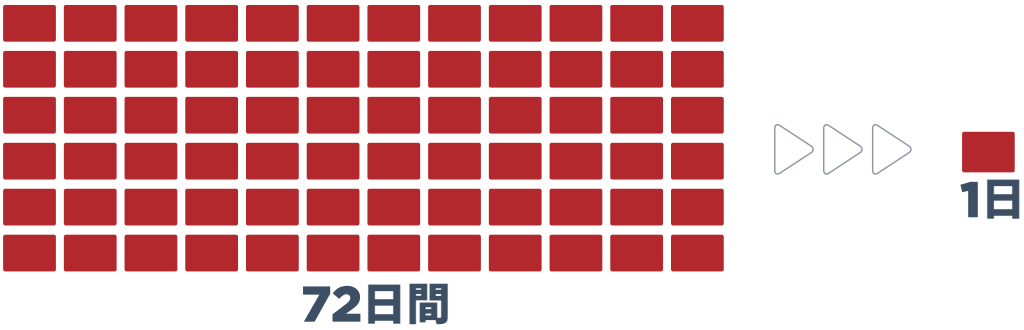
ランサムウェアの攻撃パターンを知る

ランサムウェア攻撃のTTP（Tactics、Techniques、Procedures）を熟知したアナリストにアクセスできるということは、組織にとってこれまで以上に重要な意味を持ちます。戦略的なランサムウェア攻撃では、目的を達成するためにまず足がかりを築き、それから標的環境への接続を維持する必要があります。例えば、Mandiantの専門家による調査では、MAZEを用いる攻撃グループが、侵害したネットワークを介して水平展開し、数多くのサーバーやワークステーションにペイロードをインストールしていました。このグループはその後、アクセスを取得、維持し、上位権限を取得し、水平展開をできるようになりました。

2019年のMandiantの調査では、インシデントレスポンス・サービスの顧客に対してAPT攻撃グループが戦略的に展開したランサムウェア攻撃で、セキュリティ侵害の発生から検知までに要した日数（ランサムウェアの展開前）は平均で72日間であったことがわかりました。Managed Defenseの顧客もAPT攻撃グループによるランサムウェア攻撃の標的にされていますが、ほぼすべての事例で、ランサムウェア・コンポーネントが展開される前に検知し、攻撃を回避しています。Managed Defenseでは、戦略的に展開するランサムウェア攻撃に対してセキュリティ侵害の発生から検知までに要した日数が72日間から24時間以下にまで短縮されています（図1を参照）。

図1:

2019年の顧客データによると、Managed Defenseは、セキュリティ侵害の発生から検知までに要した日数を大幅に短縮しています。



このような戦略的なランサムウェア攻撃を検知するには、まず隠れた攻撃者を見つけなければなりません。しかし、多くの企業は、現在および過去の攻撃者の振る舞いに関する専門知識を有する熟練した脅威ハンターを社内に擁していません。Managed Defenseの脅威ハンティング・チームは、最前線のサイバー脅威インテリジェンスと独自のインシデント対応の経験に基づいて、戦略的なランサムウェア攻撃のハンティングを行います。

被害が生じる前に対応する

戦略的なランサムウェア攻撃では、短期間で感染と暗号化が行われるため、迅速で効果的な対応が何よりも重要です。幅広く行われている最近のランサムウェア攻撃に対し、組織のセキュリティ・チームは、攻撃者の行動の全体像を把握し、徹底的に対処する必要があります。Managed Defenseでは24時間体制の監視とアラートの優先順位付けが行われるため、Mandiantの専門家は優先すべきアラートを速やかに特定し、調査を実施できます。

Managed Defenseは、15年間以上にわたるインシデント対応の豊富な経験を活用し、迅速な診断を行い、脅威を封じ込めます。Managed Defenseのコンサルタントは、Mandiantインシデントレスポンスの専門家と協力し、組織の環境内に潜む攻撃者を見つけ出し、攻撃を阻止します。このような迅速な対応により、組織はフル・インシデントレスポンスのコストを98%の割合で回避することができます。Managed Defenseの調査結果は、組織側のチームからの知見と合わせて発展させ、Managed Defenseポータル内に総合レポートとして提供されます。

戦略的なランサムウェア攻撃の発見と対応をサポートするMandiant Managed Defenseについての詳細は、**www.fireeye.jp/mandiant/managed-detection-and-response**をご覧ください。

ファイア・アイ株式会社
〒101-0054 東京都千代田区神田錦町3-22
テラススクエア8階 | 03-4577-4401 |
Japan@fireeye.com

Mandiant Solutionsについて

Mandiant Solutionsは、世界トップレベルの脅威インテリジェンスと最前線で得られた専門知識を継続的なセキュリティ検証と組み合わせ、セキュリティの有効性を高め、ビジネス・リスクを低減するために必要なツールをお届けします。

©2020 FireEye, Inc. All rights reserved. FireEyeおよびMandiantはFireEye, Inc.の登録商標です。その他のブランド名、製品またはサービス名はそれぞれその所有者の商標またはサービスマークとして登録されている場合があります。MD-EXT-SB-JA-JP-000335-01