

大手メーカーが Enterprise Threat Protector によりセキュリティ体制を強化



要件

- 既存のセキュリティスイートにさらに一段の防御層を追加する
- ネットワークの中断を最小限に抑える
- セルフサービス対応が可能で、サポートを最小限に抑える

状況

ヨーロッパの某大手メーカーは、進化し続けるサイバー脅威に対して、自社のセキュリティ体制を全面的に強化することを検討していました。Akamai の担当チームとの最初のミーティングでは、どのようなセキュリティ層を追加すべきか具体的なアイデアはありませんでしたが、セキュリティの潜在的ギャップを特定するために、Akamai に協力を依頼しました。Enterprise Threat Protector は既存のセキュリティ脆弱性に対応し、使いやすく、展開後のサポートも最小限で済むため、魅力的なオプションでした。同社は Akamai とのミーティング後すぐに、製品試用版に登録しました。

試用版プログラム

わずか 2、3 週間で 7,000 件を超える DNS リクエストが、同社のネットワーク上の潜在的脅威として検出されました。Akamai のチームがさらに分析した結果、これらのコマンド&コントロール (CnC) リクエストに、Conficker.B マルウェアが関係していることがわかりました。Conficker (別名 Downup、Downadup、Kido) は、Windows オペレーティングシステムを標的とするコンピューターワームです。Windows OS ソフトウェアの欠陥を利用して、管理者のパスワードを辞書攻撃し、ボットネットを形成します。高度なマルウェアテクニックを多数組み合わせるため、対策が非常に困難です。

Enterprise Threat Protector は、Cryptolocker と Locky ランサムウェアの拡散に使用されることで知られる、正当なウェブサイトへの DNS リクエストも検出しました。このマルウェアがエンタープライズのネットワークにインストールされると、ネットワーク内を移動して、エンドポイントデバイスやサーバー上のファイルを暗号化します。ランサムウェアは現在、エンタープライズにとって大きな脅威となっており、過去 1 年間で注目される事例も多数発生しています。

これらの発見は、同社が Enterprise Threat Protector の購入を急ぐのに十分な事例となりました。新しいセキュリティ層を追加したいという漠然とした要望が、事前対応型のエンタープライズ保護へと具体的な方法へとシフトしたのです。

なぜ Akamai なのか

同社は試用版を使用した後、現在のセキュリティ製品スイートに Enterprise Threat Protector を追加する必要があるとの認識に至りました。すでに使用しているセキュリティ製品 (エンドポイントのウイルス対策や Dell ファイアウォール) とのシームレスな統合が可能だけでなく、リアルタイムインテリジェンスのアップデートにより、将来の攻撃への事前対応型の保護も提供されるからです。

今では、同社のすべての外部再帰 DNS トラフィックが Enterprise Threat Protector にリダイレクトされます。Akamai の脅威インテリジェンスにより、リクエストされたドメインのリスクがリアルタイムに評価されるので、ユーザーやデバイスが悪意あるドメインやサービスにアクセスしないよう事前対応が可能です。IP 接続前にこうした検証が行われるため、防御線からはるか離れた場所にあるセキュリティ・キル・チェーンで、事前に脅威を阻止できます。Enterprise Threat Protector は使用が簡単でネットワークの大きな変更も必要としないうえ、一貫したポリシーを全社的に実施できます。



Akamai は世界で最も信頼された世界最大のクラウド配信プラットフォームを提供しています。使用するデバイス、時間、場所を問わず、お客様が安全性に優れた最高のデジタル体験を提供できるようにサポートします。Akamai の大規模な分散型プラットフォームは、世界 130 か国に 20 万台を超えるサーバーを擁する比類のない規模を誇り、お客様に優れたパフォーマンスと脅威からの保護を提供しています。Akamai のポートフォリオに含まれる、ウェブおよびモバイルパフォーマンス、クラウドセキュリティ、エンタープライズアクセス、動画配信の各ソリューションは、卓越した顧客サービスと 24 時間体制の監視によりサポートされています。大手金融機関、EC リーダー企業をはじめ、メディアおよびエンターテインメントプロバイダー、政府機関が Akamai を信頼する理由について、www.akamai.com/jp/ja/ または blogs.akamai.com/jp/ および Twitter の [@Akamai_GK](https://twitter.com/Akamai_GK) で詳細をご紹介します。全事業所の連絡先情報は、<https://www.akamai.com/jp/ja/locations.jsp> をご覧ください。2017 年 12 月発行。