FireEye FX

コンテンツ脅威対策

ファイル共有やコンテンツ・ストアに潜むマルウェアを検知、駆除

概要

FireEye® FXは、さまざまな形式のファイルを利用した攻撃からデータ資産を保護するための脅威対策プラットフォームです。Webメールやオンラインのファイル転送サービス、クラウド、携帯型のストレージ機器は、ファイル共有やコンテンツ・リポジトリで広まるマルウェアの感染源になるおそれがあります。FireEye FXは、ネットワーク・ファイル共有やエンタープライズ・コンテンツ管理ストアを検査することにより、次世代型のファイアウォール、IPS、アンチウイルス、セキュリティ・ゲートウェイをすり抜けて侵入したマルウェアを検知して隔離します。

ファイル共有に潜むマルウェアが引き起こす問題

今日の高度なサイバー攻撃は、高機能なマルウェアとAPT攻撃（Advanced Persistent Threat：高度で持続的な標的型攻撃）と呼ばれる手法を用いてセキュリティ対策をすり抜け、ファイル共有やコンテンツ・リポジトリ内で感染を広げます。これによってマルウェアは、ネットワーク内に確固たる足がかりを築き、インターネットに接続していないシステムを含め、複数のシステムに感染を拡大します。このようなコンテンツベースのマルウェアに対して特に脆弱なのが企業のデータセンターです。従来型のセキュリティ対策は、このタイプのマルウェアを効果的に検知できず、ごく単純な方法で侵入を試みるマルウェアさえ見逃してしまうことがあります。サイバー攻撃者は、この弱点を突いてネットワーク・ファイル共有にマルウェアを侵入させ、多数のファイルに不正なコードを埋め込みます。その結果、一部のファイルだけを修復しても繰り返し被害が発生します。

高度なサイバー攻撃のライフサイクル阻止に欠かせないファイルの保護

APTによるネットワーク資産の侵害を防ぎ、機密情報の漏洩やそれに伴う深刻な被害の発生を防止するためには、ファイルに潜むマルウェアを検知する必要があります。FireEye FXシリーズは、特許技術のFireEye Multi-Vector Virtual Execution™（MVX）エンジンを使用してファイル共有やエンタープライズ・コンテンツ・リポジトリを検査し、PDF、Microsoft Office、vCard、ZIP/RAR/TNEFなどの広く使用されているファイル形式や、QuickTime、MP3、Real Player、JPG、PNGなどのマルチメディア・コンテンツに埋め込まれた未知の不正なコードを見つけ出します。アクセス可能なネットワーク・ファイル共有やコンテンツ・ストアに対して再帰検査、定期検査、オンデマンド検査を実施することにより、内部に潜むマルウェアを検知して隔離し、高度なサイバー攻撃を構成するライフサイクルの早い段階で攻撃を阻止します。

未知の脅威を見つけ出すFireEyeのMVXエンジン

FireEye FXは、未知の脅威の検知を目的とした専用技術であるFireEyeのMVXエンジンを使用して各ファイルを検査し、ゼロデイ・エクスプロイトなどの不正なコードが埋め込まれていないかどうかを確認します。FireEye MVXエンジンは、安全性が確保された仮想環境で疑わしいコードを実行し、ダイナミックなシグネチャレスの解析により、ゼロデイ攻撃や複数のフローにわたる攻撃など、発見が困難な攻撃を検知します。未知のエクスプロイトやマルウェアをいち早く検知して、「キル・チェーン」と呼ばれる攻撃活動のステップのうち、感染および侵害の段階でサイバー攻撃を食い止めます。

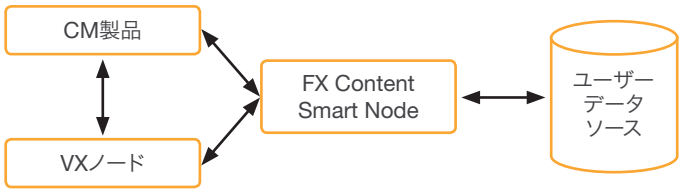
ハイライト

- 従来型のアンチウイルス・エンジンでは対応できない潜伏型のマルウェアを検知
- 隔離を行う防御モードと解析のみのモニター・モードに対応
- CIFSおよびNFS互換のファイル共有で再帰検査、定期検査、オンデマンド検査を実施
- WebDAVプロトコルを活用してSharePointをプロアクティブに保護
- PDFやMicrosoft Office文書、マルチメディア・ファイルなど多様なファイル形式の解析に対応
- AV-Suiteの統合によりインシデント対応の優先順位を効率よく判断し、マルウェアの命名規則に準拠
- FireEye CMおよびFireEye DTIクラウドを介して、別のFireEyeプラットフォームと脅威情報を共有

FireEye

FireEye MVX Smart Gridを有効活用

MVX Smart Gridは、先進的なネットワーク・セキュリティを活用しているほか、ハイブリッド・クラウドやプライベート・クラウド環境に対応した、柔軟性と拡張性に優れるアーキテクチャを採用し、さらなる進化を遂げています。FireEyeの先進的なMVXエンジンと、ハードウェアや仮想Smart Nodes™を分離するという画期的なアプローチを通じて、キャンパス、支店、遠隔ユーザーのセキュリティをより効果的に実現します。Smart Nodesは、MVXエンジンが核となるダイナミック解析を実行するのと並行して、インターネット・トラフィックを解析し、静的解析、IPS、応用インテリジェンスなど、さまざまな手法を駆使して脅威を検知、阻止します。



SharePointのコンテンツのプロアクティブな検査と隔離

FireEye FXは、SharePointリポジトリ内のコンテンツを継続的に検査し、マルウェアを確認した時点でアラートを発して永久的に隔離します。このプラットフォームはWebDAVプロトコルを活用してSharePointサービスと安全に統合し、SharePointリポジトリを活用する企業のビジネス・ワークフローを維持します。

YARAベースのルールでカスタマイズに対応

カスタムYARAルールをサポートするFireEye FXは、独自のルールで大量のファイルを解析し、特定の組織を狙った脅威を見つけ出すことができます。

インシデント対応の優先順位を効率よく判断

FireEye AV-Suiteを使用すると、FireEye FXがブロックしたマルウェアをアンチウイルス・ベンダーの製品で検知できるかどうかを詳しく解析できます。これにより、インシデント対応の優先順位を効率よく判断し、既知のマルウェアの一般的な命名規則に準拠できます。

マルウェア情報の共有

FireEye CMプラットフォームを導入している場合、ダイナミックに生成されたリアルタイムの脅威インテリジェンスをすべてのFireEye製品で共有し、ローカル・ネットワークの保護に利用できます。このインテリジェンスは、FireEye Dynamic Threat Intelligence™ (DTI) クラウドを介して世界規模で共有され、同クラウドに参加するすべてのFireEyeプラットフォームに新しい脅威の情報が行き渡ります。

ルールのチューニングは不要、誤検知もほぼゼロ

FireEye FXの導入は、チューニングを行うことなく完了し、クライアント・アプリケーションを介さず容易に管理できます。また環境固有の要件に応じて、解析のみのモニター・モードと隔離を行う防御モードの2種類のモードを柔軟に選択可能です。このため、ファイル共有に潜むマルウェアの調査、またそのマルウェアの感染拡大を直ちに防ぐこともできます。

ニーズに応じたセキュリティを実現するContent Smart Node

FireEye Content Smart Nodeを利用すると、コンテンツ管理者やセキュリティ管理者は、企業全体のミッション・クリティカルなコンテンツを保護する柔軟な仮想ソリューションを実現できます。さらに、FireEye MVX Smart Gridプラットフォームと組み合わせれば、コンテンツ・セキュリティをニーズに応じてシームレスに拡張、展開することが可能です。

表1: FireEye Content Smart Node

	FX 2500V
サポートするOS	Microsoft Windows/Mac OS X
パフォーマンス	7万ファイル/日
ネットワーク・インタフェース・ポート	Ethernet 1/2
CPUのコア数	2
メモリ	8 GB
ディスク容量	512 GB
サポートするハイパーバイザ	VMWare ESXi 6.0以降

詳細については、FireEyeのWebサイトをご覧ください。
www.FireEye.jp

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 | www.fireeye.jp
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.FireEye.com

FireEye®はインテリジェンス主導型のSecurity-as-a-Serviceのリーダー企業です。顧客企業は、FireEyeの革新的セキュリティ技術、国家レベルの脅威インテリジェンス、世界的に著名なMandiant®コンサルティングの知見が統合された単一プラットフォームを、自社のセキュリティ対策の一部としてシームレスに組み込むことができます。このアプローチにより、FireEyeは準備、防御、インシデントレスポンスといった、組織がサイバー攻撃対策をするうえでの課題となっていた複雑性や負担を解消します。FireEyeは「Forbes Global 2000」企業の940社以上を含む、世界67か国以上の5,000を超える組織で利用されています。