FireEye

データシート

Malware Analysis System

高度な標的型攻撃に対する次世代のフォレンジック分析

ハイライト

- 不審なファイル、Web コード、実行ファイルの分析作業を簡素化
- システムレベルでの OS とアプリケーションの変更（ファイルシステム、メモリ、レジストリ）を詳しく報告
- サンドボックス分析またはライブモード分析でゼロデイエクスプロイトを特定
- 配備作業を軽減（事前に設定された環境を調整、仮想テストイメージを自動的にセットアップ）
- ローカルの保護対策が使用するマルウェア情報を動的に生成し、Central Management System（CMS）経由で配布
- パケットを収集し、不正な URL セッションとコードの実行を分析
- カスタム YARA ルールに対応（バージョン 1.3 互換）
- AV-Suite でインシデント対応の優先度を素早く判断
- ローカル認証だけでなく、リモートにあるサードパーティの AAA（Authentication, Authorization, and Accounting）ネットワークサービスも利用可能

VX エンジンによる分析の状態（完了、保留中）が MAS ダッシュボードに表示される

FireEye Malware Analysis System（MAS）を利用すると、自動構成の強力なテスト環境でファイル、添付ファイル、Web オブジェクトに潜む高度なマルウェア、ゼロデイ攻撃、標的型 APT 攻撃を実行し、脅威の調査を安全に行うことができます。

サイバー犯罪者は特定の企業、ユーザーアカウント、システムに侵入するため、標的に合わせた攻撃を実行します。このような標的型攻撃を迅速に検知して対処するには、使いやすいフォレンジックツールが不可欠です。

OS、ブラウザー、アプリケーションに対する攻撃を評価

FireEye の Virtual Execution（VX）エンジンにより、社内のアナリストは最初に実行されるエクスプロイトからコールバック先、後続のバイナリダウンロードまで、攻撃全体をあらゆる角度で分析することができます。VX エンジンは、事前に構成された Windows 仮想分析環境で不審なコードを実行し、一般的なファイル形式、電子メールの添付ファイル、Web オブジェクトを詳しく分析します。 FireEye MAS は、特定のファイルまたは一連のファイルでマルウェアの感染を調査し、複数のプロトコルでアウトバウンド接続を追跡します。

管理作業ではなく、分析作業に集中

VX エンジンの機能は、仮想化されたハードウェア上で完全な Microsoft OS、ブラウザー、プラグイン、サードパーティのアプリケーションを利用します。MAS アプライアンスでは、マルウェアの手動解析に使用する仮想マシン環境をセットアップする必要はありません。ベースラインの設定や復元も不要です。

分析モードの選択（サンドボックスまたはハニーポット）

サンドボックスモードでは、特定のマルウェアサンプルの実行パスを検証し、匿名化した攻撃プロファイルを動的に作成できます。この情報は、CMS を介して他の FireEye Web、Email、File Malware Protection System（MPS）アプライアンスに配布されます。マルウェアの攻撃プロファイルには、マルウェアコードの ID、エクスプロイトの URL、感染元や攻撃元の情報が記述されます。また、情報窃盗を動的にブロックするため、マルウェアの通信プロトコルの特徴も共有されます。

「FireEye ソリューションの大きな魅力の一つは、仮想実行環境で解析を行い、問題のコードが脅威かどうか判断できる点です。この詳細な解析結果のおかげで、最適な問題解決策がすぐに見つかり、どのように対処すべきかを正確に判断できます。」

— エネルギー業界のサイバーセキュリティ責任者

サンドボックス分析以外に、FireEye では、ネットワーク上にハニーポットを構築し、マルウェアのライフサイクルを詳しく分析することができます。現在の高度なマルウェアは様々な段階で従来のセキュリティ対策を回避します。脆弱性の悪用は攻撃の初期段階に過ぎません。

FireEye は、インバウンドとアウトバウンドの検査機能を統合し、複数のプロトコルを調査します。これにより、OS、Web、電子メール、アプリケーションの脅威を総合的に分析できます。

YARA ベースルールによるカスタマイズ

MAS では、カスタム YARA ルールをインポートすることができます。バイトレベルのルールを指定して不審なオブジェクトを調査し、組織固有の脅威を解析できます。カスタムルールを使用すると、既に不正と分類されているオブジェクトだけでなく、不正な可能性があるオブジェクトも特定できます。

マルウェア対策のグローバルネットワーク

Malware Analysis Systems は、マルウェアのフォレンジックデータを FireEye CMS 経由で他の MPS アプライアンスと自動的に共有できます。これにより、情報窃盗のアウトバウンド送信をブロックし、インバウンドの既知の攻撃を阻止します。MAS の脅威データを FireEye Malware Protection Cloud（MPC）で共有し、新たに発生する攻撃を防ぐこともできます。

事前に設定された仮想実行エンジンを使用するため、調整は不要です。FireEye MAS では、管理者がセットアップや構成作業に時間を割く必要はありません。これは管理が容易で、費用対効果に優れたソリューションです。ネットワークやセキュリティの管理作業を増やすことなく、高度な標的型攻撃を分析することができます。

技術仕様

	MAS 4310	MAS 7300
筐体サイズ	1U ラックマウント	1U ラックマウント
重量	13.6 Kg	13.6 Kg
寸法（幅 x 奥行 x 幅）	43.7 x 65.0 x 4.3 cm	43.7 x 65.0 x 4.3 cm
格納装置	19 インチラック	19 インチラック
管理用インターフェース	10/100/1000 BASE-T ポート 2 個	10/100/1000 BASE-T ポート 2 個
モニタリングインターフェース	N/A	N/A
処理能力	25,000 オブジェクト / 日	50,000 オブジェクト / 日
AC 入力電圧	100 ~ 240 VAC 自動切換え（全範囲）	100 ~ 240 VAC 自動切換え（全範囲）
AC 入力電流	8.5-6 A	8.5-6 A
電源装置 /RAID	冗長 /2 SAS HDD（HW RAID1）	冗長 /2 SAS HDD（HW RAID1）
周波数	50-60 Hz	50-60 Hz
AC 電源	最大 700 W	最大 700 W
周囲温度	40° C	40° C