データシート

Malware Analysis

攻撃分析のためのフォレンジック・ソリューション

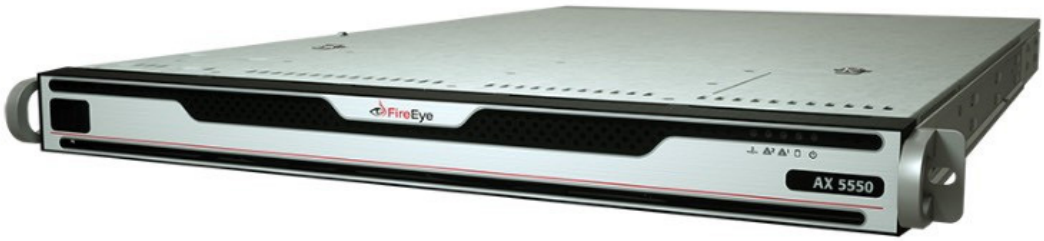

図1：FireEye Malware Analysis AX 5550 アプライアンス

ハイライト

- FireEye MVX エンジンにより、攻撃のライフサイクル全体に対して詳細なフォレンジック分析を実施
- 疑わしい Web コード、実行可能ファイル、各種ファイルを一括して効率的に解析
- OS やアプリケーションによるファイル・システム、メモリ、レジストリに対するシステムレベルの変更を詳細にレポート
- ライブ・モードまたはサンドボックス・モードによる解析でゼロデイ攻撃を検知
- FireEye Central Management との統合により、脅威インテリジェンスをダイナミックに生成し、ローカル環境を直ちに保護
- パケットをキャプチャして、不正な URL セッションとコード実行を解析
- FireEye AV-Suite と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
- Windows 環境と Mac OS X 環境をサポート

概要

FireEye Malware Analysis は、Webページや添付ファイル、各種ファイルに埋め込まれた高度なマルウェアやゼロデイ攻撃、APT攻撃（Advanced Persistent Threat：高度で持続的な標的型攻撃）を、自動構成された強力なテスト環境で安全に実行、検査するためのフォレンジック分析ソリューションです。

今日のサイバー攻撃者は、標的とする企業やユーザー・アカウント、システムに合わせて攻撃方法を変化させています。このような悪意のある標的型攻撃に素早く対処するためには、使いやすいフォレンジック・ツールが欠かせません。

オペレーティング・システム、Web ブラウザ、アプリケーションに対する攻撃を検証

Malware Analysis では、FireEye Multi-Vector Virtual Execution™（MVX）エンジンを使用して、攻撃の第1段階で実行されるエクスプロイトからコールバック先、その後に行われるバイナリのダウンロードに至るまで、あらゆる角度から攻撃を解析してその全体像を把握できます。

アプリケーションなどが事前構成された Microsoft Windows および Apple Mac OS X 仮想解析環境で疑わしいコードを実行し、一般的な Web オブジェクトや添付ファイル、各種ファイルを詳細に検査します。Malware Analysis では MVX エンジンを用いて、特定のファイルや一連のファイルを検査してマルウェア感染の有無を確認し、複数のプロトコルにまたがるアウトバウンド接続の試みを追跡します。

最小限の管理作業で解析に集中

手動でのマルウェア解析のように、仮想マシン環境のセットアップや基準値の設定、復元に長い時間を費やす必要がありません。カスタマイズ機能を備え、ペイロードの実行をきめ細かく制御できる Malware Analysis により、フォレンジック分析プラットフォームはネットワーク固有の要件に合わせて効率よく攻撃の全体像を把握できます。

ライブ・モードとサンドボックス・モードの 2 つの解析モード

Malware Analysis には、ライブ・モードとサンドボックス・モードという 2 つの解析モードが用意されています。外部への接続を含め、マルウェアの攻撃ライフサイクルを完全に解析できるライブ・モード（ネットワーク・モード）では、複数の経路から段階的に行われる高度な攻撃のプロセス全体を追跡します。一方、サンドボックス・モードでは、対象マルウェアの実行パスを仮想環境内に限定しながらその動作を可視化します。

どちらのモードでも、匿名化された動的な攻撃プロファイルを生成し、FireEye Central Management 経由で他の FireEye ソリューションと共有できます。Malware Analysis が生成するマルウェアの攻撃プロファイルには、マルウェア・コードの識別子、エクスプロイトの URL、感染元や攻撃元に関するその他の情報が含まれます。また、マルウェアが使用する通信プロトコルの特性も FireEye Dynamic Threat Intelligence™（DTI）経由で共有され、マルウェアによる外部へのデータ送信の試みが FireEye 環境全体でダイナミックに遮断されます。

YARA ベースのルールでカスタマイズに対応

Malware Analysis は、カスタム YARA ルールのインポートをサポートしています。このため、バイトレベルのルールを使用して疑わしいオブジェクトを素早く解析し、特定の組織を狙った脅威を見つけ出すことができます。

世界規模のマルウェア対策ネットワーク

Malware Analysis では、マルウェアのフォレンジック・データが集中管理システム経由で他の FireEye ソリューションと自動的に共有されるため、マルウェアによるアウトバウンドのデータ送信の試みが遮断され、インバウンドの既知の攻撃が阻止されます。また、Malware Analysis からの脅威データを FireEye DTI クラウド経由で共有すると、同クラウドに参加する世界中の FireEye ソリューションで最新の攻撃を防御できるようになります。

事前に構成済みの FireEye MVX エンジンは、ヒューリスティックのチューニングが不要で、セットアップや構成に時間を費やす必要がありません。このソリューションでは、ネットワークやセキュリティ管理の手間を省きながら高度な標的型攻撃の解析を行うこともできます。

表 1：技術仕様

	AX 5550
パフォーマンス *	最大 8,200 個のオブジェクト / 日
サポートする OS	Microsoft Windows / Apple Mac OS X
ネットワーク・インタフェース・ポート	10/100/1000BASE-T ポート x 2
IPMI ポート（背面パネル）	搭載
前面パネル LCD およびキーパッド	搭載
PS/2 キーボードおよびマウス、DB15 VGA ポート（背面パネル）	搭載
USB ポート（背面パネル）	Type A USB ポート x 4
シリアル・ポート（背面パネル）	115,200 bps、パリティなし、8 ビット、1 ストップ・ビット
ディスク容量	1 TB HDD 4 台、RAID 10、3.5 インチ、フィールド交換対応
エンクロージャ	1RU、19 インチ・ラックに適合
シャーシの寸法（幅 × 奥行 × 高さ）	437 x 706 x 43.2 mm
DC 電源	非搭載
AC 電源	冗長電源（1 + 1）750W、100 ～240 VAC、 9–4.5 A、50 ～60Hz、IEC60320-C14 インレット、フィールド交換対応
消費電力（最大）	292W
熱放散（最大）	996 BTU/ 時

表 1：技術仕様

	AX 5550
平均故障間隔（MTBF）	54,200時間
重量（アプライアンスのみ / 梱包時）（kg）	15 kg / 22 kg
安全性に関する適合規格	IEC 60950、EN 60950、CSA 60950-00、CE Marking
EMC/EMI の適合規格	FCC（Part 15 Class-A）、CE（Class-A）、CNS、AS/NZS、VCCI（Class A）
規制への対応	RoHS、REACH、WEEE
温度（動作時）	10°C～35°C
相対湿度（動作時）	10% ～ 85%（結露なきこと）
動作高度	1,500 m

注：パフォーマンス値は、Malware Analysis のデフォルトの解析時間に基づいていますが、実際の数値はシステム構成や処理するトラフィックの特性によって異なります。

FireEye の詳細については、**www.FireEye.jp**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

会社概要
FireEye は、インテリジェンス主導型のセキュリティ企業です。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、インシデント対応といった、組織がサイバー攻撃対策をする上での課題となっていた複雑性や負担を解消します。