AXシリーズ

サイバー攻撃の全体像把握を実現するフォレンジック分析プラットフォーム

図1：AX 5550およびAX 8400

概要

FireEye® AXシリーズは、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プラットフォームです。

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。このような悪質性の高い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

FireEye AXシリーズでは、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。FireEye MVXエンジンは、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

FireEye AXシリーズでは、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FireEye AXシリーズにより、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。

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 CMプラットフォームとの統合により、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

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

FireEye AXシリーズには、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 CMプラットフォーム経由で他のFireEye製品と共有できます。FireEye AXプラットフォーム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）Enterprise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

FireEye AXシリーズは、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

FireEye AXシリーズは、FireEyeのすべての脅威対策ポートフォリオと容易に統合可能です。マルウェアのフォレンジック・データがFireEye CMシリーズ経由で他のFireEyeプラットフォームと自動的に共有されるため、マルウェアによる外部へ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、FireEye AXシリーズの脅威データを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プラットフォーム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。FireEye AXシリーズでは、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ができます。

表1：技術仕様

	AX 5500	AX 8400
パフォーマンス*	最大8,200個のオブジェクト/日	最大1万6,000個のオブジェクト/日
サポートするOS	Microsoft Windows / Apple Mac OS X	Microsoft Windows
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	10/100/1000BASE-Tポート x 2
IPMIポート（背面パネル）	搭載	搭載
前面パネルLCDおよびキーパッド	搭載	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	搭載
USBポート（背面パネル）	Type A USB 4ポート	Type A USB 2ポート
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	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	900 GB HDD 4台、RAID 10、2.5インチ、フィールド交換対応	600 GB HDD 2台、RAID 1、2.5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	2RU、19インチ・ラックに適合
シャーシの寸法（幅×奥行×高さ）	437×706×43.2 mm	437×711×86.6 mm

表1：技術仕様

	AX 5500	AX 8400
DC電源	非搭載	非搭載
AC電源	冗長電源（1+1）750W、100～240 VAC、9-4.5 A、50-60 Hz、IEC60320-C14インレット、フィールド交換対応	冗長電源（1+1）750W、100～240 VAC、9-4.5 A、50-60 Hz、IEC60320-C14インレット、フィールド交換対応
消費電力（最大）（ワット）	292W	506W
熱放散（最大）（BTU/時）	996 BTU/時	1,726 BTU/時
平均故障間隔（時）	4万700時間	6万8,900時間
重量（アプライアンスのみ/梱包時）	15 kg / 22 kg	19 kg / 26 kg
安全性に関する適合規格	IEC 60950、EN 60950、CSA 60950-00、CE Marking	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）	FCC（Part 15 Class-A）、CE（Class-A）、CNS、AS/NZS、VCCI（Class A）
規制への対応	RoHS、REACH、WEEE	RoHS、REACH、WEEE
温度（動作時）	10℃～35℃	10℃～35℃
相対湿度（動作時）	10%～85%（結露なきこと）	10%～85%（結露なきこと）
動作高度	1,500 m	1,500 m

注：パフォーマンス値は、FireEye AXプラットフォーム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。

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4割以上を含む、世界67か国以上の6,000を超える組織で利用されています。