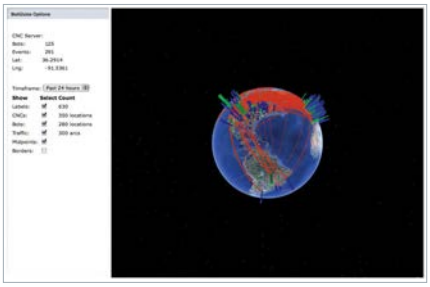
データシート

Malware Protection Cloud

グローバルな脅威情報の共有で新たに発生しているゼロデイ攻撃を阻止

ハイライト

- Web、電子メール、ファイルを狙った新たな脅威の情報をグローバルで共有
- アプライアンスでゼロデイのマルウェアと標的型攻撃のデータを取得し、サイバー犯罪者の侵入を阻止
- コールバック先の情報を常に更新し、マルウェアの通信と情報漏洩を阻止
- 脅威情報の公開はオプション（サイトで共有方法を決定）



FireEye Malware Protection Cloud により FireEye の研究者とアプライアンスの間で脅威情報を動的に共有する

FireEye Malware Protection Cloud（MPC）は、Malware Protection Systems（MPS）を相互に接続するグローバルネットワークで、確認したゼロデイ攻撃の脅威情報がリアルタイムに交換されます。

このサイバー犯罪監視システムは、ゼロデイ攻撃やマルウェアのコールバック先に関する最新の情報を利用者に提供します。

グローバルなマルウェア情報をリアルタイムに共有

FireEye MPC は、世界各地の顧客、テクノロジーパートナー、サービスプロバイダーのネットワークに配備された FireEye アプライアンスを相互に接続します。MPC はグローバルな分散ハブとして機能し、自動生成されたマルウェア情報（新しいマルウェアのプロファイル、脆弱性のエクスプロイト、難読化技術など）を効率よく共有します。また、FireEye Malware Intelligence Lab が発見した新しい脅威やサードパーティのセキュリティ情報も共有されます。MPC により、FireEye アプライアンスは既知のマルウェアだけでなく、サイバー犯罪者やサイバースパイ、偵察攻撃で利用されるゼロデイの標的型攻撃も検出できます。

高度な標的型攻撃を阻止する方法

FireEye Web MPS、Email MPS、File MPS、MAS アプライアンスは高度な標的型攻撃を阻止するために Web、電子メール、ファイルを利用した脅威を分析します。各アプライアンスの Virtual Execution（VX）エンジンは不審な Web トラフィック、電子メールの添付ファイル、ファイルの分析結果からセキュリティコンテンツを動的に作成します。FireEye Central Management System（CMS）は、ローカルで動的に生成されたセキュリティコンテンツを各アプライアンスに配布し、FireEye 配備環境全体をリアルタイムに保護します。

MPC を利用している企業や組織は MPC から脅威データを受信します。また、世界各地の利用者に脅威データを送信し、新たに発生する脅威を防ぐことができます。

「FireEye アプライアンスは侵害を検出してから数秒以内に必要な情報を提供するので、優先順位の高い項目に集中できます。この情報は、組織固有のものではく、科学者やエンジニアにとっても非常に重要なデータです。」

— 政府機関のサイバー犯罪対策主任アナリスト

未知のゼロデイ攻撃を動的に分析

多段階の VX エンジンは様々なブラウザー、プラグイン、アプリケーション、オペレーティング環境で不審なバイナリと Web オブジェクトを実行し、ゼロデイ攻撃のマルウェアと標的型攻撃を検出します。VX エンジンは、脆弱性の悪用、メモリ破壊による任意のコードの実行など、攻撃で実行される不正な操作を追跡します。仮想環境での攻撃が終了すると、ゼロデイ攻撃のコールバックチャネルを収集し、このチャネルをブロックするルールを作成します。

複数の脅威に対する MPS の検査を統合するとにより、OS、Web、電子メール、アプリケーションに対する脅威を総合的に分析することができます。この統合で、既知のマルウェアだけでなく、高度な標的型攻撃で使用されるゼロデイのマルウェアに対して包括的な保護対策を実施できます。Malware Protection Cloud では、ローカルでの検出結果がグローバルでリアルタイムに共有されるため、企業を狙った脅威を回避することができます。

新たに発生する脅威の情報

次の脅威情報が提供されます。

- マルウェアの攻撃プロファイル（マルウェアコードの MD5、ネットワーク上での振る舞い、難読化技術）。確認済みの既知の攻撃を識別できます。
- ファイル共有オブジェクト、電子メールの添付ファイル、URL の分析結果
- 情報送信と犯罪者からの命令の受信にマルウェアが使用するコールバック先（宛先 IP アドレス、プロトコル、ポート）
- マルウェアの通信プロトコルの特徴（転送セッションのインスタンス化に使用されるカスタムコマンドなど）

実際のデータに基づくブロックで誤検知を回避

レピュテーションや危険度による脅威情報ネットワークでは、シグネチャを配布してコードの危険性を推測するため、トラフィックが誤ってブロックされたり、許可される場合があります。FireEye システムでは、不正なアクティビティを確認します。FireEye システムの評価は、仮想実行環境で不審なコードを徹底的にテストした後で生成されるため、最終的な評価となります。たとえば、リアルタイムの情報更新の流れは次のようになります。

1. FireEye アプライアンスが、司令（C&C）システムとして機能している不正な IP アドレスを特定し、このアドレスをアウトバウンド通信でブロックします。
2. アプライアンスがマルウェアの宛先 IP アドレス、ポート、プロトコルを FireEye MPC に自動的に通知します。
3. MPC 利用者の FireEye アプライアンスが更新情報を定期的に受信します。同じポート番号とマルウェアプロトコルを使用する IP アドレスはブロックされます。
4. すべての MPC 利用者サイトで、侵害されたシステムとボットネットの C&C システムとの接続が切断されます。

FireEye, Inc. | 1390 McCarthy Blvd. Milpitas, CA 95035 | +1 408.321.6300 | japan@fireeye.com（日本語可） | www.fireeye.com