シスコ IT ブリーフィング情報

Advanced Malware Protection をあらゆる場所に

マルウェアはますます悪質になっています。シグニチャベースの脅威から、より複雑な、動作ベースの侵害へと進化しています。ハッカーは、最強の侵入防御システム、ウイルス対策ソリューション、その他のポイントインタイム検出ツールをもすり抜ける高度なマルウェアを作成しています。IT 部門には、潜在的な侵害の範囲への可視性をさらに高めるとともに、高度なマルウェアによって損害や業務の中断が発生する前に検出して封じ込め、修復できるようになることが求められています。シスコの Cisco Advanced Malware Protection（AMP）の導入をご検討ください。

AMP は、一流のグローバル脅威インテリジェンスを基盤にして、攻撃前には既存の防御ラインを強化し、攻撃中には、マルウェアによる拡張ネットワークへの侵入をブロックします。万一マルウェアにこれらの防御を突破された場合、AMP は、問題を迅速かつコスト効率よく発見して修復するために必要な、すべての情報を提供します。AMP のブラウザベースの管理コンソールを利用すれば、影響を受けるユーザ、アプリケーション、そしてデバイス、マルウェアの発信元、マルウェアの動作、その阻止方法を、完全に可視化できます。Cisco® AMP は、ネットワーク、データセンター、エンドポイント、サーバ、モバイル デバイス、電子メール/Web ゲートウェイ、仮想環境を保護します。

シスコでは、自社の拡張ネットワーク全体に AMP を導入しようとしています。2016 年 1 月時点で実施済みの内容は、次のとおりです。

- シスコのインターネット接続ポイント（PoP）13 ヵ所すべてで AMP for Networks を運用。
- Android 向けに AMP for Endpoints を実稼働中。Windows と MAC OSX 向けにはパイロットを実施中。
- Web および E メール セキュリティ アプライアンスに AMP を統合。

ネットワーク内に展開されているシスコ製品には、AMP Threat Grid が統合されています。動的なふるまい分析機能とサンドボックス テクノロジーを備えた Threat Grid は、AMP 製品を補完する役割を果たします。

> 「私たちは、これまでのウイルス対策ソリューションでは検知できずにネットワークへの侵入を許してしまった新しいマルウェアが、AMP for Endpoints では検出されるのを確認しました」
>
> **ー 情報セキュリティ アーキテクト、Rich West**

情報セキュリティ（InfoSec）アーキテクトの Rich West はこう述べています。「あまり見たことのない不審なコードを AMP が取得すると、自動的に Threat Grid に送信されて分析されます。Threat Grid は、それがマルウェアである可能性を判断し、マルウェアと思われる場合にはフラグを付けて、人間の調査担当者の注意を喚起します。そのすべてが自動化されています」。Threat Grid は、受信した不審なサンプルおよびアーティファクトすべてについて、450 を超える（さらに増加中）指標に基づいてアクティビティを分析します。

電子メール マルウェア検出機能の強化

AMP は、急増する電子メールベースのマルウェアとの戦いに貢献しています。Cisco InfoSec の IT プログラム マネージャ、Scott Heider は、こう述べています。「シスコでは、Cisco E メール セキュリティ アプライアンス（ESA）を導入したことで、電子メールで送信されるマルウェア脅威の 80 ~ 90% がブロックされています。ESA ソリューションに AMP を統合したことにより、まるで干し草の中から針を探すような未知の脅威の検出作業を、新たなハードウェアやサポートの専門知識がなくても実施できるようになりました」

関連情報

Inside Cisco IT ブログ：AMP Threat Grid [英語]

Cisco Advanced Malware Protection ソリューション