Sourcefire is now part of Cisco.

ホワイト ペーパー

高度なマルウェア防御（AMP: Advanced Malware Protection）を選ぶ基準

はじめに

高度な技術を持つ昨今の攻撃者は、いつ、どのような組織に対しても攻撃をしかけられるだけのリソースと専門的知識を持ち、長期にわたって執拗に攻撃を加えてきます。事実、マルウェアはわたしたちの周囲に蔓延しています。こういった攻撃には、ファイアウォールやエンドポイントの保護を含む従来の防御策では対抗できません。マルウェア対策のプロセスは「すばやく」進化し対応する必要があります。

マルウェアとそれに代表される標的型の執拗な攻撃は、発生時点だけの制御や単独の製品のみでは効果的に対処しきれません。高度なマルウェア防御（AMP）を導入し、対象となるマルウェアと同じように広範に浸透させる必要があります。このような保護には、攻撃前（Before）、攻撃中（During）、攻撃後（After）にわたって脅威を検出、確認、追跡、分析、修復するための統合された一連の制御と、継続的なプロセスが必要です。ネットワーク、エンドポイント、そしてその間にあるすべての場所に防御策を組み込み、拡大し続ける攻撃の種類や手口に対応する必要があります。

状況は良くなるどころか悪化しています。多様なマルウェアの増大に伴い、組織が 1 時間あたりに直面する新しいマルウェアのサンプルは数万件に上ります。また、攻撃者はシンプルなマルウェア ツールを利用してデバイスを危険にさらすことができます。既知の不正なマルウェアのシグネチャとファイルを照合するブラックリスト型のアプローチでは、もはやこの変化のスピードについていけなくなっており、サンドボックスなどの新しい検出技術の有効性も 100 % ではありません。さらに、攻撃を仕掛ける方法も、単に個々のコンピュータではなく、インターネットのインフラストラクチャのパワーを束ねて利用するサイバー犯罪が増加しています。この方法が台頭している証拠として、2014 年のシスコ年次セキュリティ レポートによると、インタビューした Fortune 500 のすべての企業で、マルウェアが存在するWeb サイトにアクセスしていたことがわかっています。メールや Web ゲートウェイにまで保護を拡大することが不可欠です。

図 1. レトロスペクティブ セキュリティは、Sourcefire（現シスコ）独自の機能であり、高度なマルウェア防御を支える基盤です。これはビッグデータ分析機能を継続的に提供するもので、連続的なファイル追跡と分析、アラートの送信、また当初は安全と思われていたが後から悪意のあることが分かったファイルの修復を目的として広範囲のネットワークでデータやイベントを集約します。

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

この『高度なマルウェア防御を選ぶ基準』では、高度なマルウェア防御を提供するベンダーに確認すべき重要な質問を記載しています。また、ビッグ データ分析と集約されたセキュリティインテリジェンス、そしてネットワーク、エンドポイント、セキュア ゲートウェイ、仮想システム、モバイル デバイス全体を通じたセキュリティの施行（エンフォースメント）、さらに独自のレトロスペクティブ セキュリティを組み合わせることにより、シスコがどのようにしてマルウェア攻撃の被害を食い止めるかについて説明します。

マルウェア問題に対するビッグデータ分析と集約されたセキュリティ インテリジェンスの適用

既知のマルウェアの急増を受けて、エンドポイント保護を提供してきたベンダーは、顧客サービス向上のため、「クラウドアシスト型のウイルス対策」の機能を導入しました。これは簡単に言うと、シグネチャ データベースをクラウドに移行したものです。これは、数十億件ものウイルス シグネチャを 5 分ごとに各エンドポイントに配布しますが、シグネチャベースの検出を巧みにかわすよう設計されている高度なマルウェアの進化した機能には対応できていませんでした。

高度なマルウェア防御を提供するベンダーに確認すべき項目

1. 執拗なマルウェアの特定にビッグデータをどのように活用していますか？
2. マルウェアの挙動を正確に判断するためにどのような分析を行っていますか？
3. 検出機能の自動更新にマルウェアの分析結果をどのように利用していますか？
4. 新たなマルウェアの脅威に関する情報やデータをどのように収集していますか？
5. レトロスペクティブなマルウェア検出のために、継続的な分析をどのように行っていますか？

クラウドアシスト型の ウイルス対策モデルには、もう 1 つの壁があります。それは、攻撃者は時間と忍耐力という武器を使って有利に事を進められるということです。ほとんどのマルウェア対策テクノロジーは、ファイルが最初に確認された検出時点にばかり着目し（いわゆる、特定時点の検出）、その持続性と状況の把握が不十分です。今日、マルウェアに見えなかったものが、明日（または明後日）には簡単にマルウェアへ変化してしまうわけです。このため、ネットワークの継続的な分析だけでなく、最新の脅威情報に基づいて、ファイルのステータスを当初の「良性」から「悪性」へと変更することができる機能が求められます。

高い技術を持つマルウェアの作成者は、さまざまな手法を使って（または新しい手法を開発して）、マルウェアの目的をわかりにくくし、検出を難しくしています。このような手法には、シグネチャ エンジンを欺くために少しだけ変化するポリモルフィック ファイル、コマンド＆コントロール（CnC）ネットワークからの要求に乗じてマルウェアを侵入させる高度なダウンローダ、自身のコンポーネントを削除する消去型のトロイの木馬などがあり、調査担当者によるマルウェア検出や分析を妨げています。これらはほんの一部に過ぎません。これまでのやり方でマルウェアを特定できなくなっている今、マルウェアの挙動と移動先を理解し、悪意のある動作はもちろん、最初の検出期間後に脅威が発生し、特定時点の検出技術では見過ごされた可能性がある危険性を検出するために、マルウェアをそのライフサイクルを通して捕捉および分析する新しい手法が必要です。

Sourcefire（現シスコ）は、マルウェアの検出においてこれらの問題に対処するため、新しい、より包括的なアプローチを採用しています。数千ものグローバル企業の顧客ベース、および実際に使用されている数百万のエンドポイント マルウェア保護エージェントから、シスコは毎月数百万件のマルウェア サンプルを収集しています。マルウェアと悪意のないソフトウェアを分類するために、Collective Security Intelligence クラウド内で数万のソフトウェア属性が分析されています。また、ネットワーク トラフィックの状態を分析することにより、CnC ネットワークを探しているマルウェアの特定も行います。

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

さらに、Sourcefire とシスコ[1] の製品ラインで使われている AMP の巨大なインストール ベースを活用し、グローバル、および特定の顧客組織内の両方における正常なファイルとネットワーク アクティビティの挙動を判別し、比較の基準とします。

従来の検出方法を巧みにかわすよう設計されているマルウェアの検出には、高度な技術が必要です。シスコは、見た目ではなく、挙動に基づいてマルウェアを特定できるよう特化したモデルを使い、ゼロデイ攻撃を含む新しいタイプの攻撃の検出を可能にしています。これらのモデルではマルウェアの変化の速さに追随できるよう、Sourcefire VRT®（脆弱性調査チーム）が発見した新しい攻撃の方法に基づいて、リアルタイムに自動更新されます。

Sourcefire の Collective Security Intelligence の利点は、ファイルが検出のためのポイントを通過してしまった後も有効です。Sourcefire のクラウド分析では、最新の脅威情報に対してファイルが長時間継続して評価されるため、AMP ソリューションはファイルを最初に分析した時から時間が経過していてもアラートを送信することができます。

最後に、これらの利点は AMP コミュニティ全体にも及びます。AMP コミュニティは、ファイルの性質が変更されると必ずアラートを受け取ります。この場合、クラウドで「集団免疫」機能が有効になっていれば、Collective Security Intelligence クラウドを利用しているすべての組織は即座に、悪意のあるファイルに関する通知を受け取ります。

マルウェア対策のベンダーに確認すべき項目

1. ネットワーク、および危険にさらされたデバイス上でマルウェアが増加している程度を判断するためどんな手法を取っていますか？
2. マルウェアの検出が発生の数時間後または数日後になった場合、マルウェアにさらされたデバイスをどのように特定しますか？
3. 初期検出をかわしたマルウェアや、ネットワークでブロックされなかったマルウェアにはどのように対処しますか？
4. 疑わしい活動の根本的な原因分析をすばやく実行できますか？
5. アウトブレイクや根本的な原因を阻止するためにどのような制御方法がありますか？

レトロスペクティブ セキュリティ：継続的な分析を使用して、当初は悪意がない、または不明と判断されたが、その後悪意があると判断されたファイルに関するアラートを送信します。レトロスペクティブ セキュリティは、アウトブレイクの範囲を判別してそれらを抑制し、最終的にはマルウェアの被害を遡及的に自動修復します。

攻撃者の時間を巻き戻すレトロスペクティブ セキュリティ

攻撃者はじっとしていません。配備されているセキュリティ制御について常に調査し、それに応じて自分たちの作戦を変え、防御策の裏をつきます。実際、攻撃者のほとんどが主要なマルウェア対策製品で自分たちのマルウェアをテストしてから攻撃を開始しています。ブラックリスト アプローチの効力が衰える中、仮想マシン（VM）ベースのダイナミック分析を利用してマルウェアを調査および研究しようとしているセキュリティ会社が増えています。それに対して攻撃者は作戦を変更して対抗しています。評価期間中に悪意のある行為を何もしなければファイルは安全と判断されるという想定のもと、何も実行しないか、または VM で実行される数時間（または数日）だけ攻撃の実行を遅らせます。もちろん、この待機期間が過ぎれば、デバイスは危険にさらされます。残念ながら、特定時点のみの検出テクノロジーでは、このようなファイルを再度分析する方法はありません。いったん安全と判断されたファイルは、検出手法がその後改善されても、ファイルがマルウェアの挙動を示しても、「安全」とみなされたまま変わることはありません。さらに悪いことに、マルウェアが検出をかわすと、これらの制御

[1] 2013 年のシスコによる Sourcefire の買収後、AMP 機能はシスコの E メールおよび Web セキュリティ ソリューションにおいて、追加ライセンスとして利用できるようになりました。詳細については、www.cisco.com/go/amp [英語] をご覧ください。

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

機能には、マルウェアの環境内での増殖を追跡する方法、根本原因を把握する方法、マルウェアの入口となっている場所（感染拡大の拠点となり、システムが繰り返しマルウェアに感染する）を特定する方法などはありません。

これは、マルウェアの作成者が巧みにセキュリティ会社を出し抜く（また、既存のマルウェア対策の制約を示す）ほんの一例に過ぎません。最善のアプローチは、マルウェアを 100 % 防御できる検出方法はないことを念頭に置いておくことです。検出の機能だけで完璧な保護を実現できると考えるならば、それは重要な資産を守る自身の能力を買いかぶり、敵の攻撃能力を軽視することになります。そのため、組織は自らの防御がかわされることを想定する必要があります。つまり、感染の範囲や状況を理解し、被害を迅速に封じ込め、脅威、根本原因、マルウェアのゲートウェイを排除できる能力が必要となります。これらすべてに対応するには、レトロスペクティブ セキュリティが必要です。

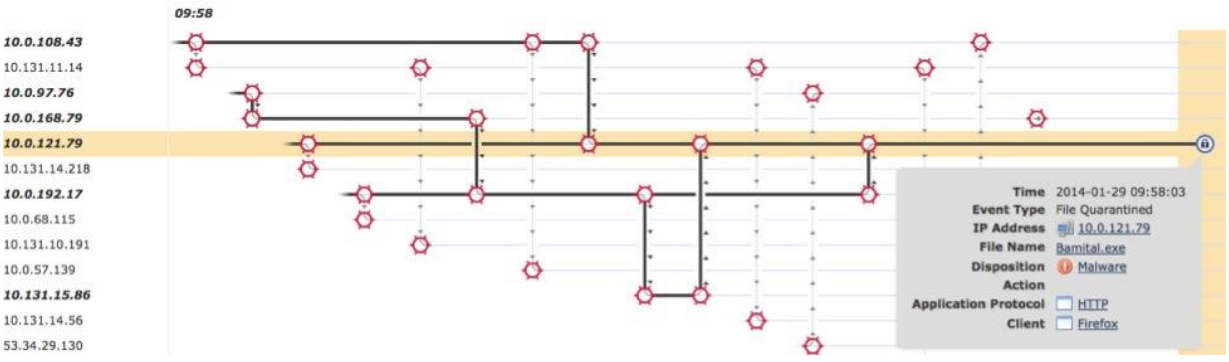
AMP のレトロスペクティブ セキュリティ機能により、組織は時間を遡り、ファイルがマルウェアであると特定された時期に関係なく、マルウェアにさらされたデバイスを特定できます。この機能では、保護ネットワークを通過するすべてのファイルを追跡し、すべての保護デバイスで生じるすべてのアクションを系統立てて表示し、ファイルが組織内を移動した様子とファイルがシステム上で実行したことを視覚的にマッピングする必要があります。

通常、従来のマルウェア対策による防御では、ファイルが将来のある時点でマルウェアだと判断された場合の選択肢が限られています。タイム マシンに乗り込んで過去に遡り、侵入してくるファイルをブロックすることはできません。ファイルはすでに環境の中に入り込んでおり、大混乱を引き起こしている可能性もあります。ほとんどのマルウェア対策制御はこれで終わりになります。問題の全体像は知らされないまま、次にどうすればよいのかもわかりません。

しかし、AMP の基盤であるビッグデータ分析はここで威力を発揮します。File Trajectory と呼ばれる機能により、ファイルが組織を移動した経路をすばやく正確に判断できるほか、マルウェアを追跡し、影響を受けたデバイスを即座に（場合によっては自動的に）取り除くことがきます。さらに重要なことは、AMP はすべてのファイルのすべての使用状況を追跡するため、組織は「0 号患者」（マルウェアの最初の犠牲者）と影響を受けたその他のすべてのデバイスを見つけ、感染を撲滅できます。消去後にわずか 1 つでもマルウェアのインスタンスが残っていると、再感染の可能性が非常に高くなります。

さらに、File Trajectory はファイル活動に関連する情報を単に分析するのではなく、ファイルの系統、使用状況、依存関係、通信、プロトコルに関する情報を追跡できるほか、マルウェアをインストールするファイルを特定し、マルウェアや疑わしい活動の根本原因の迅速な分析に役立てることができます。セキュリティ チームは、攻撃中にすぐに検出から制御に切り替えることが可能で、アウトブレイクの範囲や根本原因をすばやく把握し、さらなる感染を効果的に阻止します。

図 2. 侵入場所、マルウェアの活動、関わっているエンドポイントに関する情報とマルウェアの伝播を示す File Trajectory のデモ画面

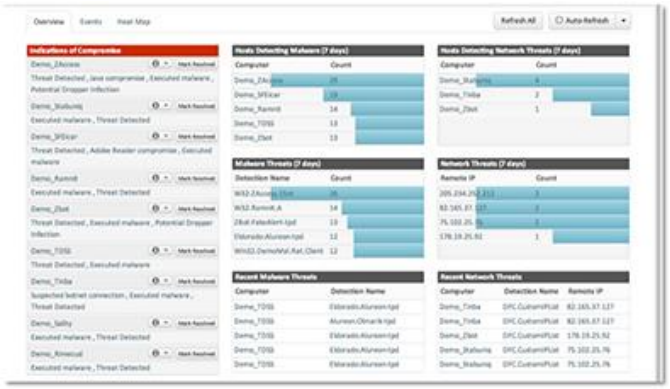


もう 1 つ、検出イベント、特にマルウェア関連のイベントが殺到した場合に問題になることがあます。つまり、優先的に対応する必要があるイベントの判断です。単一のイベントなら、たとえそれがエンドポイントでブロックした悪意のあるファイルであっても、必ずしもネットワークが危険にさらされていることを意味するものではありません。ただし、複数のイベントが一斉に動作する場合は、それらが悪意のない活動のように見えたとしても、システムが危険にさらされ、侵害が切迫しているか、進行中である危険が大幅に高まります。

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

AMP のもう 1 つの機能である Indicators of Compromise は詳細な分析を実行し、危険性の高い症状を示しているシステムを見つけます。これは、特定時点の検出テクノロジーでは提供できない機能です。マルウェアを最初に検出した後も継続してマルウェア関連の活動の捕捉、分析、関連付けを行うことで、Indicators of Compromise は自動分析とリスクの優先順位付け機能を提供します。

図 3. システムが危険にさらされている可能性を示唆する、悪意がないように見えるイベントを示す Indicators of Compromise のデモ画面。高度なマルウェアは、ウイルス対策シグネチャと正確に一致するような「決定的証拠」を残すことはほとんどないため、これは重要です。



最後に、いったん企業内に足掛かりを得たマルウェアは、通常 CnC サーバに通信を返そうとします。また、攻撃者が直接コントロールしている場合は、狙っている標的に外側から入り込むための偵察活動を開始します。

AMP は、保護されているエンドポイント上の通信活動を監視し、Collective Security Intelligence 分析と比較して危険が生じているかどうかを判断し、必要に応じてエンドポイントでのマルウェアの通信や配布をブロックします。この機能は、リモート ワーカーやモバイル ワーカーが使用するシステムなど、企業ネットワークの防護壁で守られていないエンドポイントでマルウェアの急増を制御するセキュリティ担当者にとって、大きな利点となります。さらに、File Trajectory と Indicators of Compromise では、取得したネットワーク活動の情報を利用して、調査や危険性の優先順位付けを迅速化します。

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

連携を高める：ネットワーク、セキュリティ ゲートウェイ、物理および仮想エンドポイント、モバイル デバイスのエンフォースメント

孤立したセキュリティ制御などありえません。高度なマルウェアによる攻撃を防ぐためには、ネットワーク、ゲートウェイ、エンドポイントの防御、および脅威と修復活動を追跡する管理コンソールとの間できめ細かい調整を行う必要があります。シスコは、Collective Security Intelligence クラウド、高度なネットワーク分析、複数のエンフォースメント ポイントを使った統合システムを提供し、組織のわずかな隙間から高度なマルウェアが侵入するのを防ぎます。

AMP のベンダーに確認すべき項目

1. セキュリティ ゲートウェイとネットワーク、物理および仮想エンドポイント、モバイル デバイスで、マルウェアとその根本原因をブロック、追跡、分析および修復できますか？
2. 保護されたネットワークの外で移動しているデバイスはどのように保護しますか？
3. 常に危険にさらされているデバイスはどのように特定しますか？
4. システムが常に危険にさらされているかどうかをどのように確認できますか？その修復はどのように行いますか？
5. 独自の攻撃を修復するためのカスタム マルウェア検出ルールはサポートされていますか？それはどのように行われていますか？

シスコの幅広い AMP 機能はネットワークを起点として、侵入するマルウェアを検出してブロックします。ファイルがネットワークを出入りするたびに、AMP はファイルのフィンガープリントを生成し、Cisco FireSIGHT® 中央管理コンソールに問い合わせて悪意のあるファイルとして特定されているかどうか判断します。

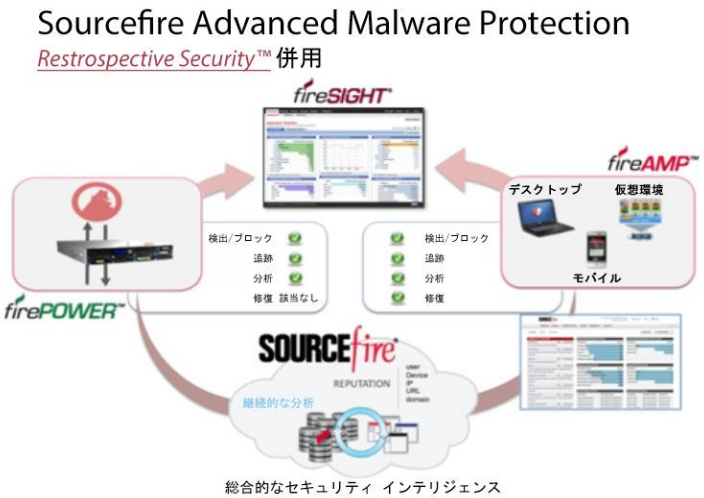
FireSIGHT コンソールで調査したことがないファイルの場合は、Collective Security Intelligence クラウドを確認し、Collective Security Intelligence ネットワークで調査したことがあるかどうかすぐに判断します。この軽量な自動照合機能は、ネットワーク上のすべてのファイルをサンドボックス化するよりも大幅に拡張性に優れたアプローチであり、遅延の影響もありません。悪意のあるファイルが特定された場合は、FireSIGHT コンソールが提供する File Trajectory 機能により、これらファイルにさらされた状況と範囲を把握します。

また、軽量なエンドポイント 用のマルウェア保護エージェント（FireAMP™ コネクタ、新名称Cisco AMP for Endpoint）を各保護デバイスに実装することもできるため、そのデバイス上のすべてのファイル活動を Collective Security Intelligence クラウドに対してチェックし、それらのファイルが既知のマルウェアかどうか特定できます。FireAMP コネクタは、単に悪意のあるファイルを探すだけではありません。これまで調査したことがないファイルであっても、そのようなファイルによるマルウェアの挙動をデバイス上で検出してブロックできるため、ゼロデイ攻撃に対してもエンドポイントを保護できます。FireAMP コネクタは、上記で説明したレトロスペクティブ セキュリティと File Trajectory 機能も活用し、アウトブレイクの範囲を特定し、ただちに修復が必要なデバイスを特定します。

疑わしいと判断されたファイルの場合、AMP はさらに詳細な分析を実行します。上記で説明したように、クラウドベースの分析は、ファイルがどのように実行しているかを正確に判断し、悪意のあるファイルと判断した場合は攻撃のプロファイリングを行い、危険性インジケータとその他の属性を生成します。これらは、強力なビッグデータ分析機能を使って検索できます。

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

これらマルウェアのプロファイルを使うことで、AMP は組織がマルウェアのアウトブレイクに対して積極的に対応できるようにします（図 2 を参照）。レトロスペクティブ セキュリティ機能により、あるファイルが事後に別の環境で悪意のあるファイルと判断された場合、Collective Security Intelligence クラウドはこの決定を組織の FireSIGHT コンソールに送信できるため、ネットワークまたはエンドポイントのいずれかでそのマルウェアをブロックし、残りの AMP コミュニティで集団免疫機能を実行できます。さらに、ローカルの管理者がローカライズされた攻撃を特定し、即座に対策を取る必要がある場合、組織は特定のファイルや IP アドレスをブロックするカスタム ルールを設定できます。



FireAMP Mobile コネクタは、同じ Collective Security Intelligence クラウドを使い、脅威の可能性がないか Android アプリケーションをすばやくリアルタイムに分析します。モバイル デバイスにまで可視性を広げることで、感染しているデバイスやマルウェアをシステムに持ち込んだアプリケーションをすぐに把握できるようになります。攻撃を阻止したい場合、FireAMP Mobile には特定のアプリケーション（ブラックリスト）をブロックできる強力なコントロールが含まれているため、企業のリソースにアクセスするモバイル デバイスで使用できるアプリケーションの制限を徹底できます。また、FireAMP Virtual コネクタは、同様の機能と高度なマルウェア防御を VMware 仮想インスタンスに拡大します。

2013 年のシスコによる Sourcefire の買収後、AMP 機能はシスコの E メールおよび Web セキュリティ ゲートウェイで利用できるようになり、これら侵入場所での高度なマルウェアの検出とブロックが強化されています。重要な AMP 機能には、ファイル レピュテーションと上記で説明したファイル サンドボックスがあります。さらに、レトロスペクティブなアラート機能では、脅威のレベルの変化に対応するため、Collective Security Intelligence クラウドからのリアルタイム アップデートを使い、E メールや Web のゲートウェイを通過するファイルの継続的な分析が行われます。悪意のあるファイルが脅威と特定されると、管理者には AMP からアラートが送られ、感染している可能性がある対象とその時期が示されます。これにより、お客様は被害が広がる前にすばやく攻撃を特定して対処できます。

これまで説明してきたように、マルウェアはモバイル デバイスや仮想システムから、セキュリティ ゲートウェイやネットワークを通り抜けたり、直接エンドポイントを経由して、組織に侵入することができます。このため、組織全体を通したすべての活動を把握できることが重要です。グローバルなセキュリティ インテリジェンス ネットワークを使い、ゲートウェイ、ネットワーク、エンドポイント、モバイル デバイス、仮想システム上でアウトブレイクを検出、ブロック、追跡、調査、修復する機能を備えることで、組織は、対象範囲の広さに欠ける他のセキュリティ ソリューションではどうしても生じる盲点を排除することができます。

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

高度なマルウェア防御のしくみ

統合された高度なマルウェア防御が可能にすることとはどのようなものでしょうか。公表される 2 日前に Java ゼロデイ攻撃を検出した場合の例を見てみましょう。この例で、FireAMP コンソール（エンドポイント、モバイル、仮想コネクタの管理コンソール）を見ていたお客様は、数台のデバイス上でマルウェアと思われる動きをしている奇妙な活動を検出しました。お客様は Collective Security Intelligence クラウドを使ってファイルを分析し、マルウェアだという確信を得ました。

次に行うべき手順は、攻撃の範囲を確認し、できるだけ速やかにマルウェアを取り除くことでした。まず、FireAMP の Trajectory機能を使い、問題のファイルにさらされたデバイスや攻撃と思われる動きが見られるデバイスを探しました。影響を受けたデバイスを取り除いてから、これらのファイル、および悪性を示したマルウェアの両方をブロックするカスタム ルールを作成しました。

これらのカスタム ルールが必要となったのはほんの短い期間だけでした。というのも、AMP を導入したすべてのお客様は、対象のファイルやインジケータがビッグデータ分析エンジンに追加されると集団免疫機能を利用できるためです。お客様は、それぞれの環境でこれと同じ攻撃が見つかるとアラートを受け取りました。このため、AMP を利用するお客様全体がゼロデイ攻撃の発覚前に保護されました。

まとめ

高度なマルウェア攻撃を検出して修復するには、革新的なソリューションが必要だということは業界で共通の認識ですが、あまりに多くの組織が、従来のエンドポイント保護スイートか新しい「特効薬」的な防御かにかかわらず、検出にばかり労力を費やしています。これでは確実に失敗します。業界ではデータ損失やデータ漏洩の問題が跡を絶たない状況です。

現代の攻撃を少しでも効果的に防御できるように、ソリューションではネットワークを横断して、物理および仮想環境、保護エンドポイントとモバイル デバイス上でのファイルのやり取りや活動を追跡するためにビッグデータ分析機能を利用する必要があります。多くの攻撃が、検出期間中だけ活動を休止するということ考慮すると、時間を遡って判断を「悪意がある」に変更し、これらのファイルとインジケータの軌跡を組織全体で追跡することができれば、お客様は高度な攻撃からの被害をさらに効果的に抑制して修復することができます。

最後に、一貫した保護レベルを提供するために、高度なマルウェア防御はエンドポイント デバイスの保護だけではなく、ネットワーク、モバイル デバイス、仮想システムも対象とする必要があります。次に受ける攻撃の標的を予想できる人はだれもいないのです。

高度なマルウェア防御は以下を提供します。

- 一貫したポリシーを使用した、エンドポイント、ネットワーク、セキュリティ ゲートウェイ、モバイル デバイス、仮想システムへの柔軟な展開
- 新しく発生した攻撃を業界が検出するよりも前に特定して分析するのに役立つ Collective Security Intelligence クラウドの利点
- マルウェアを遡って特定する機能、および Trajectory 機能により、拡散する前に組織内にあるマルウェアのすべてのインスタンスを見つける機能
- 最先端の調査を利用できる AMP コミュニティへの参加による集団免疫の利点。この調査は、Sourcefire VRT およびグローバルな数千の顧客に導入されている数百万のエンドポイント マルウェア防御エージェントで確認されたファイル サンプルに基づくものです。

高度なマルウェア防御に AMP ソリューションの評価をご希望の場合は、下記までお気軽にお問い合わせください。

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

©2014 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)
この資料に記載された仕様は予告なく変更する場合があります。

お問い合わせ先

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

14.06