enterprise

Trusteer Apex
企業向けマルウェア対策

Trusteer

ゼロデイ・アプリケーションの悪用とデータ盗難の阻止

標的型攻撃およびAPT (Advanced Persistent Threat: 高度な継続的脅威)は、企業にとって深刻なセキュリティ上の脅威です。 これらの攻撃を阻止するには、情報を盗み出す高度なマルウェアによって従業員のエンドポイントが攻撃されるのを防ぐ必要があります。高度なマルウェアは、ブラックリスト方式の検出方法を回避します。 ホワイトリスト方式のアプローチは、マルウェアによる回避を最小限に抑えますが、実装や管理が困難です。効果的で管理しやすいエンドポイントのマルウェア対策を実現する新しいアプローチが必要とされています。

攻撃方法: アプリケーションの悪用とソーシャルエンジニアリング

高度なマルウェアは、以下のいずれかの方法で企業のエンドポイントを危険にさらします。

- **アプリケーションの悪用:** サイバー犯罪者は、兵器化されたドキュメントやWebページに埋め込まれたコードを使ってアプリケーションの脆弱性を悪用し、従業員のエンドポイントにマルウェアを忍び込ませて社内ネットワークに侵入します。
- **ユーザーによるインストール:** サイバー犯罪者は、さまざまな手法を使ってユーザーを巧みに誘導し、マルウェアが含まれたアプリケーションをインストールさせます。 Webサイトからのダウンロード、感染したUSBドライブ、または電子メールの添付ファイルなどを経由して、悪意のあるアプリケーションが配布されます。

マルウェアに感染すると、感染したエンドポイントを使ってシステムにアクセスし、データを収集してインターネットに送信することができます。

マルウェアに感染した後、数分でデータの盗難が可能になるため、できる限り速やかに感染を特定して対処することが重要です。

Trusteer Apex は、ステートフル アプリケーション制御を適用することにより、効果的で導入や管理が簡単な自動化されたマルウェア対策を実現します。

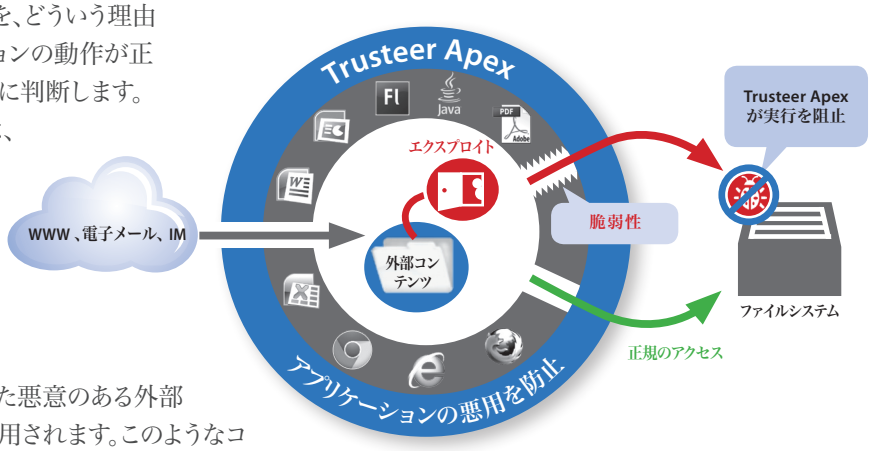
ブラックリスト方式とホワイトリスト方式: 現在のエンドポイント管理に足りないもの

多くの大企業が、市場で主流のエンドポイント保護ソリューションを用いているにもかかわらず、情報を盗み出す高度なマルウェアによって絶えず侵害されています。 従来型のエンドポイント保護ソリューションは、パターンファイルや悪意のある動作のブラックリストに基づいていたため、単純にブラックリストルールを回避する高度な脅威にはほとんど対処できていませんでした。

アプリケーションコントロールおよびホワイトリスト方式のソリューションは、「信頼された」ファイルにのみエンドポイントでの実行を許可するので、従来の方法よりも回避策に対する抵抗力があります。 しかし、ユーザー環境は変化が激しく、アプリケーションファイルは頻繁に変更されるため、組織にとってこれらのソリューションの実装および管理は非常に困難でした。

Trusteer Apex: ステートフル アプリケーション制御

Trusteer Apexは、ステートフル アプリケーション制御という新しい手法を用いて、ゼロデイ・アプリケーションの悪用およびデータの盗難を阻止します。Trusteer Apexは、アプリケーションが何 (動作) を、どういう理由 (状態) で行っているのかを解析し、アプリケーションの動作が正規のものか悪意のあるものかを、正確かつ自動的に判断します。Trusteerのステートフル アプリケーション制 御は、導入の簡素化と管理コストの最小化を 実現しながら、セキュリティを最大限に強化する企業のマルウェア対策の自動化を可能にします。



Trusteer Apex は、脆弱性を悪用してファイルシステムに書き込まれたファイルの実行をブロックし、マルウェアによるエンドポイントへの攻撃を防止します。

アプリケーションの悪用を阻止

アプリケーションの脆弱性を突くコードが含まれた悪意のある外部コンテンツを処理するときに、アプリケーションが悪用されます。このようなコードは、既知または未知(ゼロデイ)の脆弱性を利用して、ファイルシステムにファルを書き込み、それを実行します。 ブラウザー、 Adobe Acrobat、 Flash、 Java およびMS-Officeなどは広く利用され、よく悪用されるアプリケーションです。Trusteerは、信頼できない外部コンテンツを処理するこれらのアプリケーションを保護します。Trusteer Apexは、正規アプリケーションがファイルの書き込みや実行を行うときに、正規アプリケーションの状態がすべて含まれているアプリケーションの状態のホワイトリストを使用します。 Trusteer Apexは、これらのアプリケーションの脆弱性を悪用して作成されたファイルの実行をブロックし(つまり、アプリケーションが未知の状態になったとき)、マルウェアによるエンドポイントへの攻撃を防止します。

データの盗難を防止

データを盗み出す場合、インターネットと通信(C&C (Command and Control: コマンドアンドコントロール)サーバーとの通信など)するためのマルウェアが必要になります。 Trusteer Apexは、外部通信を有効にする可能性がある慎重に行うべき操作を、信頼できないファイルが実行できないよう制限します。 たとえば、外部通信チャネルを開いたり、他のアプリケーションプロセスに手を加えて外部通信トラフィックを隠したりできないようにします。信頼できないファイルはTrusteerに送信して解析し、承認するかまたはエンドポイントから削除します。

自動管理

Trusteerのステートフル アプリケーション制御エンジンは、維持管理が簡単に行えます。これは、アプリケーションの更新や修正が行われても、正規アプリケーションの状態はめったに変わらないためです。 Trusteerは、 3000万の保護対象エンドポイントから成るネットワーク上で絶えずリサーチを行い、ホワイトリストを自動更新します。 自動更新は、エンドユーザーの作業を中断させることなく行われ、ITスタッフの作業は最小限で済みます。操作の性質からTrusteerによって制限される特定のコードを、必要に応じて顧客がホワイトリストに追加できます。

Trusteerについて

ボストンを拠点とするTrusteerは、金融不正行為とデータ侵害に対して組織を保護するエンドポイントサイバー犯罪防止ソリューションにおいて業界をリードするプロバイダーです。 何百もの組織と何千万ものエンドユーザーが、オンラインの脅威と情報を盗み出す高度なマルウェアから管理対象および非管理対象エンドポイントを保護するために、Trusteerを使用しています。

Trusteer K.K.
恵比寿ガーデンプレイス（18階） | 〒150-6018 | 東京都渋谷区恵比寿4-20-3
T: +81-3-5789-5747 | info.jp@trusteer.com | www.trusteer.com/ja

*new threats, **new thinking***