KASPERSKY lab

脅威データ
フィード提供サービス

www.kaspersky.co.jp

脅威データフィード提供サービス

絶えず更新される包括的なデータを通じて、サイバー脅威と標的型攻撃に対する知見を提供することで、SIEM、ファイアウォール、IPS/IDS、APT 対策、サンドボックス / シミュレーション技術を含む既存のネットワーク防御ソリューションを強化します。

過去数年でマルウェア群とその変種は急増しており、Kaspersky Lab は現在、1 日あたり約 325,000 種類の新しいマルウェアサンプルを検知しています。これらの脅威からエンドポイントを守るために、ほとんどの組織は、アンチマルウェアソリューションや侵入防止システム、脅威検知システムなどの従来の保護対策を導入しています。変化の急速な環境では、サイバーセキュリティが常にサイバー犯罪の 1 歩先を行くことが求められており、従来のソリューションは、脅威に関する最新情報へアクセスして強化する必要があります。

Kaspersky Lab が提供する脅威データのフィードは、既存のセキュリティ情報およびイベント管理(SIEM)システムに統合することで、追加の保護層を提供することを目的としています。脅威データのフィードを統合することで、たとえば、各種ネットワークデバイスから SIEM に送信されるログを Kaspersky Lab から受け取った URL フィードと関連付けることができます。HP ArcSight SIEM への接続が含まれており、Splunk と QRadar 向けのコネクタも提供されています。

ユースケースおよびサービスのメリット

Kaspersky Lab が提供する脅威データのフィードによるメリットは以下のとおりです:

- 有害な URL に関するデータを活用することで、SIEM ソリューションを補強各種ネットワークデバイス(ユーザーの PC、ネットワークプロキシ、ファイアウォール、その他のサービス)から SIEM に送信されるログを介して、マルウェア、フィッシング、ボットネットの C&C URL に関する情報が SIEM に届けられる
- 絶えず更新される脅威の情報を通じて、ファイアウォール、IPS/IDS、SIEM ソリューション、APT 対策、サンドボックス / シミュレーション技術、UTM アプライアンスなどの主要ネットワーク防御ソリューションを強化
- 脅威に関する有意義な情報と標的型攻撃の背景にある考えをセキュリティチームに提供することで、お客様のフォレンジック機能を改善
- お客様の調査の支援:有害な URL と悪意のあるファイルの MD5 ハッシュ値に関する情報は、脅威調査プロジェクトに貢献する有益な情報

Kaspersky Lab は、3 種類の脅威データフィードを提供しています:

1. 悪意のある URL とマスク
2. 悪意のあるオブジェクトデータベースの MD5 ハッシュ値
3. モバイルスレッドのフィード

フィードの説明

悪意のある URL - 悪意のあるリンクと Web サイトを含む URL。マスキングされたレコードまたはマスキングされていないレコードを使用できます。

フィッシング URL - Kaspersky Lab がフィッシングサイトとして識別した URL。マスキングされたレコードまたはマスキングされていないレコードを使用できます。

ボットネットの C&C URL - ボットネットのコマンド & コントロール(C&C)サーバーと関連する悪意あるオブジェクトの URL。

マルウェアハッシュ値(ITW) - KSN が持つインテリジェンスを通じて提供されたもっとも危険かつまん延しているマルウェアを対象とした、ファイルハッシュ値と対応する分類。

マルウェアハッシュ値(UDS) - Kaspersky Lab のクラウド技術を使い、ファイルのメタデータと統計情報に基づいて(オブジェクト自体を保持せずに)検知されたファイルハッシュ値(UDS は緊急検知システムの意)。これにより、その他の手法では検知されない新たな(ゼロデイの)悪意あるオブジェクトを識別できます。

モバイルマルウェアハッシュ値 - モバイルプラットフォームに感染する悪意あるオブジェクトを検知するためのファイルハッシュ値。

P-SMS 型トロイの木馬フィード - モバイルユーザーへの高額請求や、攻撃者による SMS メッセージの盗用、削除、応答を可能にする SMS 型トロイの木馬を検知するためのコンテキストとトロイの木馬のハッシュ値。

モバイルボットネットの C&C URL - モバイルボットネットの C&C サーバーを対象としたコンテキストと URL。

KASPERSKY lab