KASPERSKY lab

インテリジェンス レポート

www.kaspersky.co.jp

インテリジェンス レポート

注目度の高いサイバースパイキャンペーンの認識と知識を高める、包括的かつ実用的な Kaspersky Lab のレポート

インテリジェンスレポートで提供される情報とツールを活用すると、新しい脅威と脆弱性に素早く対応できるため、既知の経路からの攻撃をブロックし、先進の攻撃による損害を軽減し、セキュリティ戦略を強化することができます。

APT インテリジェンスレポート

発見されるすべての Advanced Persistent Threat が即座に報告されるわけではなく、多くは公表されないままになります。APT に関する詳細かつ実用的な Kaspersky Lab のインテリジェンスレポートを通じて、誰よりも早く、詳しい情報を手に入れましょう。

カスペルスキー APT インテリジェンスレポートの利用者は、発見されたすべての APT に関して、幅広い形式で提供される完全な技術データを含むカスペルスキーの調査および発見結果に継続的にアクセスできます。これには、公開されることのない脅威もすべて含まれています。

Kaspersky Lab のエキスパートは、業界でもっとも高いスキルと実績を持つ APT 発見者であり、サイバー犯罪者とサイバーテロリストのグループが戦術を変更した場合は、ただちにお客様に警告を送ります。また、お客様は、企業のセキュリティ戦略にとって強力な研究および分析コンポーネントとなる、Kaspersky Lab の完全な APT レポートデータベースにアクセスできます。

カスペルスキー APT インテリジェンスレポートのメリット:

- **専用アクセス**:最先端の脅威に関する技術的な情報を、公開前の調査段階で入手できます。
- **非公開の APT 情報**:注目を集めるすべての脅威が公開の対象となるわけではありません。被害を受けた組織やデータの機密性、脆弱性解消プロセスの性質、または関連する警察の活動が原因となって、公開されない脅威もあります。しかし、カスペルスキー APT インテリジェンスレポートの利用者には、すべての脅威が報告されます。
- **詳細な関連情報**:標準形式(openIOC、STIX など)で提供される不正アクセスの痕跡(IOC)の広範なリストを含む技術データ、サンプル、ツールに加えて、Yara ルールへのアクセスを提供します。
- **継続的な APT キャンペーンの監視**:実用的なインテリジェンスに調査段階でアクセスできます(APT 分類、IOC、C&C インフラストラクチャに関する情報)。
- **遡及的分析**:サブスクリプション期間中はずっと、以前に発行されたすべてのプライベートレポートにアクセスできます。

注 - サブスクリプションの制限事項

本サービスのレポートに含まれる情報の機密性と固有性により、レポートのサブスクリプションは信用ある政府、公共団体、民間団体に限定することが義務付けられています。

KASPERSKY lab

インテリジェンス レポート

お客様専用の脅威インテリジェンスレポート

組織に攻撃を仕掛けるためにもっとも有効な方法は何でしょうか。標的を絞った攻撃者は、どのような経路と情報を利用できるでしょうか。すでに攻撃が開始されているか、または攻撃の脅威にさらされつつあるでしょうか。

お客様専用のカスペルスキー脅威インテリジェンスレポートは、これらの疑問に答えるだけにとどまりません。Kaspersky Lab のエキスパートが現在の攻撃状況を総合的につなぎ合わせて、悪用可能な弱点を特定し、過去/現在/将来の攻撃の痕跡を明らかにします。

お客様は提供される固有の情報を活用して、サイバー犯罪者の一番の標的として特定された領域を重視した防御戦略を策定し、迅速かつ正確な行動で侵入者を撃退し、攻撃が成功するリスクを最小限に抑えることができます。

オープンソースインテリジェンス（OSINT）や、Kaspersky Lab のエキスパートシステムおよびデータベースによる詳細分析、アンダーグラウンドのサイバー犯罪ネットワークに関する知識を使用して開発されたインテリジェンスレポートは、以下の領域を対象としています:

- **攻撃経路の識別**:外部から利用でき、攻撃の対象となりうるネットワーク上の重要コンポーネント（ATM、モバイル技術を使ったビデオ監視などのシステム、従業員のソーシャルネットワークプロファイルと個人用メールアカウントなど）を特定し、その状況を分析します。
- **マルウェアとサイバー攻撃の追跡分析**:お客様の組織を標的とするマルウェアサンプル（活動中/非活動中）、過去または現在のボットネット動作、ネットワークベースの疑わしい動作のすべてを識別、監視、分析します。
- **第三者攻撃**:お客様の顧客、パートナー、サービス利用者を明確に標的とした脅威やボットネット動作がある場合、感染システムが攻撃に使用される可能性があるため、その痕跡を確認します。
- **情報漏洩**:アンダーグラウンドのオンラインフォーラムやコミュニティを慎重に監視することで、ハッカーがお客様を念頭に置いた攻撃計画を話し合っているか、たとえば不誠実な従業員が情報を売買しているかどうかを突き止めます。
- **現在の攻撃ステータス**:APT 攻撃は、何年にもわたって気付かれることなく継続される場合があります。お客様のインフラストラクチャに影響を与えている現在の攻撃を見つけた場合、有効な修正手順をアドバイスします。

クイックスタート - リソース不要の使いやすさ

パラメータ（お客様専用レポート用）とデータ形式がいったん決まったら、Kaspersky Lab のサービスを使用し始めるためにインフラストラクチャを追加する必要はありません。

カスペルスキー脅威インテリジェンスレポートは、ネットワークリソースを含むリソースの整合性と可用性にまったく影響を与えません。

KASPERSKY lab

KASPERSKY lab