カペルスキー、アナリストに聞く

kaspersky BRING ON THE FUTURE

脅威の継続的な調査

脅威の継続的な調査を通じて、カスペルスキーは攻撃者やサイバー犯罪者が出入りする世界中のクローズドのコミュニティやダークウェブの犯罪者フォーラムを発見、侵入、監視しています。カスペルスキーのアナリストは、このアクセスを利用して、もっとも有害で悪名高い脅威のほか、特定の組織を挟撃にした脅威を率先して検出・調査できます。

カペルスキー、アナリストに聞く

サイバー犯罪者は企業を標的とする洗練された攻撃手法の開発を続けています。急激に変化する不安定な今日の脅威状況では、ますます俊敏化するサイバー犯罪技術が利用されています。企業は、非マルウェア攻撃、ファイルレス攻撃、自給自足/環境寄生型攻撃、ゼロデイ脆弱性攻撃や、それらすべてを組み合わせた複合的な脅威、APT に類似した攻撃、標的型攻撃による複雑なインシデントに直面しています。

業務に深刻な被害をもたらすサイバー攻撃が蔓延する中、以前にも増してサイバーセキュリティの専門家が重要になっていますが、このような人材を見つけて確保するのは簡単なことではありません。信頼できるサイバーセキュリティチームが社内にいるとしても、高度な脅威との戦いに単独で挑むことを常に期待することはできません。**社外のエキスパートの支援を要請できる体制が必要になります。**外部の専門知識に頼ることで、複雑な攻撃やAPT攻撃に利用されるおそれのある攻撃ルートを割り出し、それを排除することができる根本的な対策に関して、実用的なアドバイスが得られることがあります。

Ask the Analyst の成果物

(統合されたリクエストベースのサブスクリプション)

Kaspersky Ask the Analyst サービスは、カスペルスキーの脅威インテリジェンスポートフォリオを拡張するもので、お客様が現在直面している脅威や関心をお持ちの脅威に関するガイダンスやインサイトをお求めいただけます。このサービスでは、カスペルスキーの高度な脅威インテリジェンス機能と調査機能をそれぞれの企業に固有のニーズに合わせて調整することで、お客様の組織を標的とする脅威に対するレジリエントな防御態勢の構築を可能にします。

APT とクライムウェア

公開されたレポートや継続中の調査に関する追加情報（APT またはクライムウェアのインテリジェントレポートに付加）[1]

マルウェア解析

- マルウェアのサンプル解析
- その他の是正措置に関する推奨事項

脅威、脆弱性、関連する IoC に関する説明

- 特定のマルウェアファミリーに関する基本的な説明
- 脅威に関する追加のコンテキスト（関連するハッシュ、URL、CnC など）
- 特定の脆弱性に関する情報（重大度や、カスペルスキー製品が対応できる防御メカニズム）

ダークウェブインテリジェンス[2]

- 特定のアーティファクト、IP アドレス、ドメイン名、ファイル名、メールアドレス、リンク、画像についてダークウェブで調査
- 情報の検索と分析

ICS関連リクエスト

- 公開レポートに関する追加情報
- ICS脆弱性情報
- 地域/産業ごとのICS脅威統計および傾向
- 規制または基準に関するICSマルウェア分析情報

[1] APT やクライムウェアに関するインテリジェンスレポートを現在利用しているお客様のみ

[2] Kaspersky Digital Footprint Intelligence サブスクリプションに既に含まれています

本サービスのメリット

専門知識を補足

業界のエキスパートにオンデマンドで相談できるため、希少なフルタイムの専門家を探し出して採用するための投資が不要

調査を加速

調整された詳細なコンテキスト情報に基づいてインシデントのスコーピングと優先順位付けを効果的に実施

迅速に対応

カスペルスキーのガイダンスに従って脅威と脆弱性に迅速に対応し、既知の経路からの攻撃をブロック

仕組み

Kaspersky Ask the Analyst は別個にご購入いただくことも、他の脅威インテリジェンスサービスの付加サービスとしてご購入いただくこともできます。

企業のお客様のためのサポートポータルであるカスペルスキーカンパニーアカウントからリクエストをお送りいただけます。リクエストにはメールでご対応しますが、お客様の同意がある場合は必要に応じて電話会議や画面共有セッションもご用意いたします。リクエストが受諾された場合、リクエストの処理に必要な予想時間をお伝えします。

本サービスのユースケース：

- 以前に公開された脅威インテリジェンスレポートの特定の詳細情報に関する明確化
- 既に提供された IoC に関する追加のインテリジェンスを取得
- 脆弱性の詳細と、その悪用に対する防御方法の推奨を取得
- 興味のある特定のダークウェブアクティビティの追加情報を取得
- マルウェアのふるまいや、その潜在的な影響、カスペルスキーが確認した関連アクティビティに関する詳細を含む、マルウェアファミリーの概要レポートを取得
- ショートレポート経由で提供された関連 IoC の詳細な背景情報と分類に基づく、アラート/インシデントの効果的な優先順位付け
- 検知された疑わしいアクティビティが APT やクライムウェアに関連するものかどうかを特定するためにサポートを利用
- マルウェアファイルを送信し、包括的な分析を依頼して、提供したサンプルのふるまいと機能について把握

知識とリソースを拡張

Kaspersky Ask the Analyst では、カスペルスキーの中核的なリサーチャーグループに案件ベースでアクセスできます。本サービスを通じて、エキスパートと包括的にコミュニケーションを取ることで、既存の社内リソースをカスペルスキーの知識とリソースで補強していただけます。

www.kaspersky.co.jp