KASPERSKY lab

ボットネットの追跡サービス

www.kaspersky.co.jp

ボットネットの追跡サービス

顧客と評判を脅かすボットネットを特定するための、エキスパートによる監視および通知サービス

多くのネットワーク攻撃はボットネットを使って組織化されています。このような攻撃は通りがかりのインターネットユーザーを対象とする場合もありますが、多くの場合、特定の組織のオンライン顧客が標的となります。

Kaspersky Lab のエキスパートソリューションはボットネットの動作を追跡して、個々のオンライン決済システムやバンキングシステムのユーザーに関連する脅威を迅速に（20 分未満で）通知します。お客様はこの情報を使用し、目下の脅威について、顧客やセキュリティサービスプロバイダ、警察機関に通知および助言することができます。Kaspersky Lab のボットネット追跡サービスを使用して、組織の評判と顧客を保護しましょう。

ユースケースおよびサービスのメリット

- オンラインユーザーを標的としたボットネットがもたらす脅威についての事前警告により、常に攻撃の一歩先を行くことができます。
- オンラインユーザーを狙うボットネットのコマンド & コントロールサーバーの URL 一覧を識別することで、CERT または警察機関に要請を送ってこれらをブロックすることができます。
- 攻撃の性質を理解することで、オンラインバンキングまたは決済キャビネットの機能を強化できます。
- オンラインユーザーの教育を通じて、攻撃に使用されるソーシャルエンジニアリングの認識と被害の防止を可能にします。

リアルタイムの情報提供による対策:

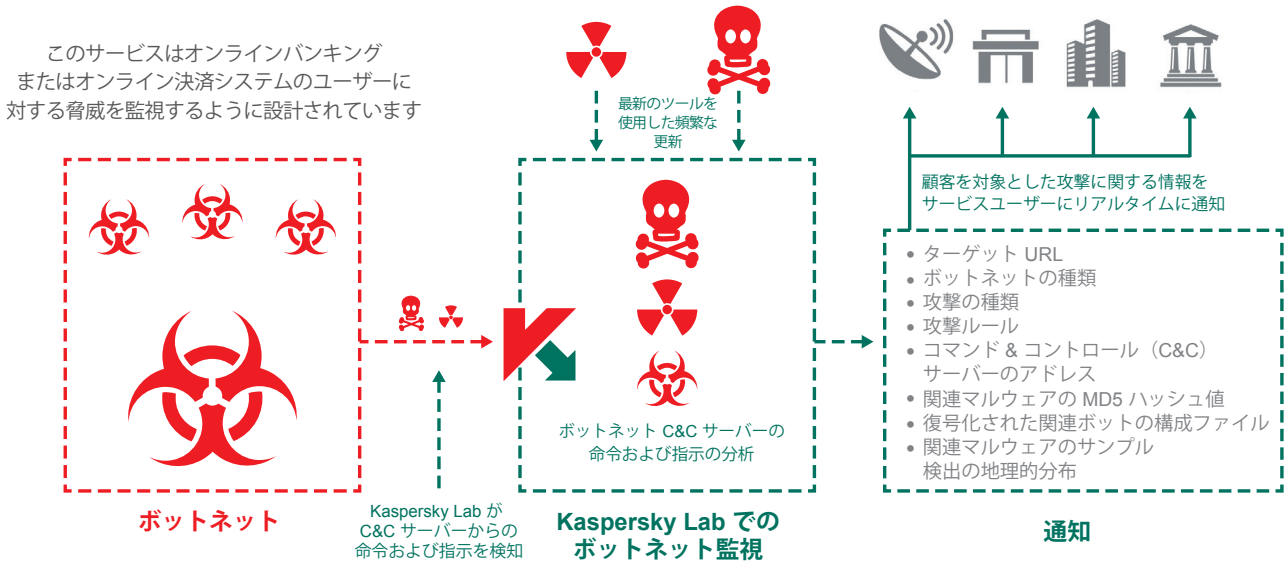
このサービスは、Kaspersky Lab が監視するボットネット内のキーワードを追跡して、一致したブランド名に関する情報を含む、個別化された通知をサブスクリプションとして提供します。通知はメールまたは RSS を介して、HTML あるいは JSON 形式で提供されます。通知に含まれる内容は以下のとおりです:

- **ターゲット URL** – ボットマルウェアは、ユーザーがターゲット組織の URL にアクセスするのを待ってから攻撃を開始するように設計されています。
- **ボットネットの種類** – 顧客のトランザクションを危険にさらすためにサイバー犯罪者が、どのようなマルウェアの脅威を利用しているのかを正確に識別します。例には、Zeus、SpyEye、Citadel が含まれます。
- **攻撃の種類** – サイバー犯罪者がマルウェアを使用する目的を特定します。例には、Web データインジェクション、画面ワイプ、ビデオキャプチャ、フィッシング URL への転送が含まれます。
- **攻撃ルール** – Web コードインジェクションでどのルールが使用されているかを特定します。例には、HTML リクエスト（GET または POST）、インジェクション前のデータまたは Web ページ、インジェクション後のデータまたは Web ページがあります。
- **コマンド & コントロール（C&C）サーバーのアドレス** – インターネットサービスプロバイダに問題のサーバーを通知して、迅速に脅威を解消できるようにします。
- **関連マルウェアの MD5 ハッシュ値** – マルウェアの検証に使用するハッシュサムを提供します。
- **復号化された関連ボットの構成ファイル** – ターゲット URL の完全なリストを特定します。
- **関連マルウェアのサンプル** – ボットネット攻撃のリバース解析やデジタル科学分析に使用します。
- **検出の地理的分布（上位 10か国）** – 世界中から取得したマルウェアサンプルの統計データを提供します。

KASPERSKY lab

ボットネットの追跡:アーキテクチャ

C&C サーバーから



Kaspersky Lab のソリューションには、各種のサービス内容と監視対象 URL 数に応じて、標準版とプレミアム版があります。お客様に適したパッケージを確認するには、カスペルスキーまたは再販業者にお問い合わせください。

サブスクリプションレベルとサービス内容

プレミアム版

メールまたは JSON 形式での通知 — 監視対象 URL 数:10

- 復号化された関連ボットの構成ファイル
- 関連マルウェアのサンプル（要望に応じて）
- 関連マルウェアサンプルの検出に対する地理的分布

標準版

メール形式での通知 — 監視対象 URL 数:5

- ターゲット URL（ボットプログラムがユーザーを狙っている URL の特定）
- ボットネットの種類（Zeus、SpyEye、Citadel、Kins など）
- 攻撃の種類
- 攻撃ルール:Web データインジェクション、URL、画面、ビデオキャプチャなど
- C&C アドレス
- 関連マルウェアの MD5 ハッシュ値

KASPERSKY lab