SERVICES DE VEILLE STRATÉGIQUE : RÉPÉRAGE DES MENACES BOTNETS

Services professionnels de suivi et de notification pour identifier les botnets qui menacent vos clients et votre réputation

De nombreuses attaques réseaux sont lancées à l'aide de botnets. Ces attaques peuvent cibler des internautes particuliers, mais elles visent le plus souvent des entreprises spécifiques et leurs clients via Internet.

La solution experte de Kaspersky Lab surveille l'activité des botnets et donne rapidement (en 20 minutes) une notification des menaces associées à des utilisateurs de systèmes bancaires et de paiement en ligne individuel. Vous pouvez utiliser ces notifications pour alerter votre clientèle des menaces en cours, vos fournisseurs de services de sécurité et les autorités locales. Protégez votre réputation et vos clients sans plus attendre avec le service d'alertes sur les menaces botnet de Kaspersky Lab.

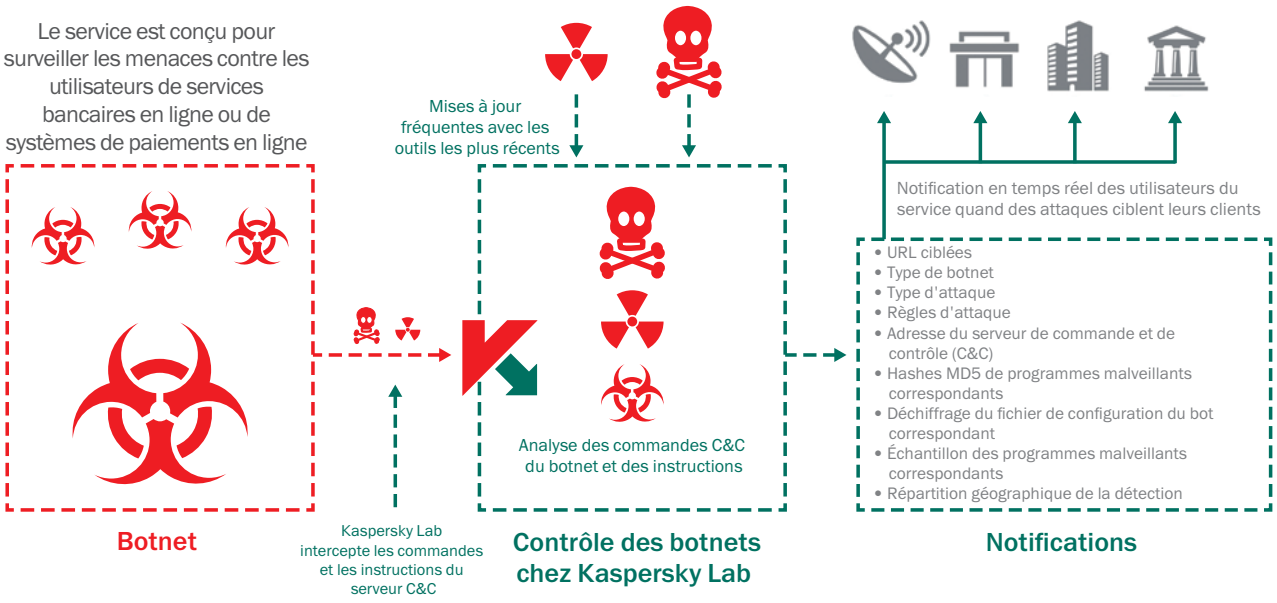
CAS D'UTILISATION / AVANTAGES DU SERVICE

- **Des alertes proactives** sur les menaces venant de botnets qui ciblent vos utilisateurs en ligne vous permettent d'avoir toujours une longueur d'avance sur les attaques
- **L'identification d'une liste d'URL des serveurs Command & Control de botnet** ciblant vos utilisateurs en ligne vous permet de les bloquer en envoyant des demandes aux CERT ou aux services de cyber-police
- **Amélioration de la sécurité en matière d'opérations bancaires et de paiement en ligne** grâce à la compréhension de la nature de l'attaque
- **Formation de vos utilisateurs en ligne** pour les aider à reconnaître et à éviter les pièges d'ingénierie sociale utilisés pour les attaques

AGISSEZ À L'AIDE DE CONTENUS EN TEMPS RÉEL :

Le service fournit un abonnement à des notifications personnalisées contenant des informations sur les marques correspondantes en suivant les mots-clés dans les botnets surveillés par Kaspersky Lab. Les notifications peuvent être livrées par e-mail ou RSS, soit au format HTML, soit au format JSON, et incluent les éléments suivants :

- **URL ciblée(s)** : les bots malveillants sont conçus pour attendre que l'utilisateur accède aux URL de l'entreprise ciblée pour démarrer l'attaque.
- **Type de botnet** : identifiez précisément le programme malveillant utilisé par le cyber-criminel pour atteindre vos clients. Exemples : Zeus, SpyEye et Citadel.
- **Type d'attaque** : déterminez l'objectif des cyber-criminels à l'origine du programme malveillant, par exemple l'injection de données Web, les effacements d'écran, la capture de vidéos ou le transfert d'URL de phishing.
- **Règles d'attaque** : identifiez les règles d'injection de code utilisées, par exemple des requêtes HTML (GET / POST) et les données de page Web avant et après injection.
- **Adresse du serveur de commande et de contrôle (C&C)** : vous permet d'avertir le fournisseur de services Internet du serveur à l'origine de l'attaque, afin de démanteler la menace plus rapidement.
- **Hash des programmes malveillants connexes** : Kaspersky Lab fournit la somme de hash utilisée pour la vérification des programmes malveillants.
- **Fichier de configuration déchiffré du bot connexe** : identifie la liste complète des URL ciblées.
- **Échantillon des programmes malveillants connexes** : pour effectuer un reverse engineering approfondi et un cyber-diagnostic de l'attaque.
- **Répartition géographique de la détection (10 principaux pays)** : données statistiques sur des échantillons de programmes malveillants connexes issus du monde entier.



La solution de Kaspersky Lab est proposée en formule standard ou premium selon les services et marques surveillées. Renseignez-vous auprès de Kaspersky Lab ou de votre partenaire revendeur pour déterminer la bonne solution pour votre entreprise.

NIVEAUX D'ABONNEMENT ET CONTENUS

Premium

Notification par e-mail ou au format JSON — 10 URL surveillées

- Déchiffrage du fichier de configuration du bot correspondant
- Échantillon du programme malveillant correspondant (sur demande)
- Répartition géographique des détections d'échantillons de programmes malveillants

Standard

Notification par e-mail — 5 URL surveillées

- Ciblage de l'URL (identification de l'URL où le programme de bot cible les utilisateurs)
- Type de botnet (par ex., Zeus, SpyEye, Citadel, Kins, etc.)
- Type d'attaque
- Règles de l'attaque, y compris : injection de données ; capture de vidéo, d'écran, d'URL, etc.
- Adresse C&C
- Hashes MD5 de programmes malveillants correspondants

POURQUOI KASPERSKY LAB ?

- Société fondée et dirigée par Eugene Kaspersky, l'expert le plus reconnu en matière de sécurité informatique
- Partenariats avec des organismes du maintien de l'ordre du monde entier, notamment Interpol et de nombreux CERT
- Outils cloud assurant le suivi en temps réel de millions de cyber-menaces dans le monde entier
- Équipes internationales chargées de l'étude et de l'analyse de cyber-menaces de toutes sortes
- Le plus grand éditeur indépendant de logiciels de sécurité au monde ; nos priorités : la veille stratégique des menaces et le leadership technologique
- Leader incontestable s'agissant des résultats aux tests indépendants de détection de programmes malveillants
- Reconnu comme un leader par Gartner, Forrester et IDC

Pour plus d'informations sur les services de veille stratégique de Kaspersky Security, veuillez nous contacter via intelligence@kaspersky.com.
POUR EN SAVOIR PLUS, RENDEZ-VOUS SUR www.kaspersky.com.

© 2015 Kaspersky Lab. Tous droits réservés. Les marques déposées et marques de service sont la propriété de leurs détenteurs respectifs.
Microsoft, Windows Server et SharePoint sont des marques déposées ou des marques commerciales de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.

KASPERSKY lab