KASPERSKY lab

RAPPORTS DE VEILLE

www.kaspersky.fr

RAPPORTS DE VEILLE

Soyez plus conscient et mieux informé des attaques de cyberespionnage les plus sophistiquées grâce aux rapports pratiques et complets fournis par Kaspersky Lab.

Grâce aux informations et aux outils fournis dans ces rapports, vous pouvez réagir rapidement aux nouvelles menaces et vulnérabilités en bloquant les attaques qui passent par des vecteurs connus, en réduisant les dommages causés par les attaques évoluées ainsi qu'en améliorant votre stratégie de sécurité ou celle de vos clients.

Rapports de surveillance des menaces APT

Toutes les menaces persistantes avancées ne sont pas signalées dès leur découverte, et nombre d'entre elles ne sont jamais révélées publiquement. Soyez le premier et le seul à en être informé grâce à nos rapports de surveillance des menaces APT détaillés et exploitables.

En tant qu'abonné aux rapports de surveillance des menaces APT de Kaspersky Lab, vous avez la possibilité d'accéder à tout moment à nos propres enquêtes et découvertes, y compris à toutes les données techniques disponibles dans différents formats sur chaque menace APT telle qu'elle a été découverte, ainsi que sur toutes les menaces qui ne seront jamais rendues publiques.

Nos experts, qui comptent parmi les chasseurs de menaces APT les plus compétents et les plus efficaces du secteur, vous alerteront également immédiatement s'ils constatent une modification dans les stratégies des groupes de cybercriminels et de cyberterroristes. De plus, vous aurez accès à tous les rapports des bases de données de menaces APT de Kaspersky Lab, un autre outil de recherche et d'analyse puissant venant compléter l'arsenal de sécurité de votre entreprise.

LES RAPPORTS DE SURVEILLANCE DES MENACES APT DE KASPERSKY LAB PROPOSENT :

- **Un accès exclusif** aux descriptions techniques des menaces les plus redoutables au cours de l'enquête, avant la publication des résultats.
- **Des informations sur les menaces APT non annoncées publiquement**. Parmi les menaces les plus graves, toutes ne sont pas révélées publiquement. En raison de l'identité des victimes, de la sensibilité des données, de la nature des opérations de correction des vulnérabilités ou des activités de maintien de l'ordre associées, certaines de ces menaces APT ne sont jamais rendues publiques. Néanmoins, toutes sont signalées à nos clients.
- **Une documentation technique détaillée**, des échantillons et des outils, avec notamment une liste complète d'indicateurs de compromission (IOC), disponibles dans des formats standard tels qu'openIOC ou STIX, sans compter l'accès à nos règles Yara.
- **Une surveillance continue des campagnes de menaces APT**. Accès aux informations exploitables au cours de l'enquête (information sur la distribution des menaces APT, les indicateurs IOC, l'infrastructure C&C).
- **Une analyse rétrospective**. Accès garanti à tous les rapports privés précédents durant toute la période de votre abonnement.

REMARQUE – RESTRICTION APPLIQUÉE AUX ABONNÉS

En raison du caractère sensible et spécifique de certaines informations contenues dans les rapports fournis par ce service, nous sommes tenus de limiter les abonnements aux organisations gouvernementales, publiques et privées de confiance.

KASPERSKY lab

RAPPORTS DE VEILLE

Rapports de veille sur les menaces spécifiques au client

Quel est le meilleur moyen d'organiser une attaque contre votre entreprise ? De quels canaux et informations dispose un pirate qui vous choisirait spécifiquement pour cible ? Une attaque a-t-elle déjà été organisée ou une menace imminente pèse-t-elle sur vous ?

Les rapports de veille sur les menaces spécifiques au client proposés par Kaspersky Lab répondent à toutes ces questions et à d'autres encore grâce au travail de nos experts, qui offrent un aperçu complet de votre situation actuelle en termes de sécurité, identifient les failles susceptibles d'être exploitées et découvrent les preuves d'attaques passées, actuelles et prévues.

Fort de cette vision d'ensemble unique, vous pouvez concentrer votre stratégie de protection sur les points identifiés comme étant des cibles privilégiées pour les cybercriminels, en prenant des mesures rapides et précises pour repousser les intrus et minimiser le risque qu'une attaque aboutisse.

Développés à l'aide de l'outil de renseignement de sources ouvertes (OSINT), d'une analyse profonde des systèmes et bases de données spécialisés de Kaspersky Lab et de nos connaissances des réseaux souterrains de cybercriminels, ces rapports abordent les domaines suivants :

- **L'identification des vecteurs de menaces** : identification et analyse de l'état de toutes les composantes essentielles de votre réseau, y compris des distributeurs automatiques, de la vidéosurveillance et d'autres systèmes utilisant les technologies mobiles, ainsi que des profils de réseaux sociaux et des comptes de messagerie personnels des employés, qui seraient susceptibles de devenir les cibles potentielles d'une attaque.
- **L'analyse du suivi des activités des logiciels malveillants et des cyberattaques** : identification, surveillance et analyse de tous les échantillons, actifs et inactifs, de logiciels malveillants visant votre entreprise, de toutes les activités présentes ou passées des botnets, ainsi que de toutes les activités suspectes liées au réseau.
- **Les attaques par des tiers** : preuves de menaces et d'activités des botnets ciblant spécifiquement vos clients, partenaires et abonnés, dont les systèmes infectés pourraient ensuite être utilisés pour vous attaquer.
- **Les fuites d'informations** : grâce à la surveillance discrète de communautés et de forums en ligne souterrains, nous repérons d'éventuelles discussions entre pirates planifiant une attaque contre vous ou, par exemple, des situations dans lesquelles un employé malhonnête vend des informations.
- **La situation actuelle en matière de sécurité** : les attaques APT peuvent rester inaperçues pendant de nombreuses années. Si nous détectons une attaque qui affecte votre infrastructure, nous vous donnons des conseils vous permettant de prendre des mesures correctives efficaces.

DÉMARRAGE RAPIDE - FACILE À UTILISER - AUCUNE RESSOURCE NÉCESSAIRE

Une fois les paramètres (pour les rapports spécifiques au client) et les formats de données personnalisés établis, aucune infrastructure supplémentaire n'est nécessaire pour commencer à utiliser ce service Kaspersky Lab.

Les rapports de veille sur les menaces de Kaspersky Lab n'affectent pas l'intégrité et la disponibilité des ressources, y compris celles du réseau.

KASPERSKY lab

KASPERSKY lab