KASPERSKY lab

PLATE-FORME KASPERSKY ANTI TARGETED ATTACK : LA CENTRALE INTERNE DE DÉTECTION DES MENACES

www.kaspersky.fr

INTRODUCTION

Chaque année, Kaspersky Lab découvre de plus en plus d'attaques ciblées, une tendance qui se poursuit, avec un nombre d'attaques en augmentation constante. Les services de sécurité des informations des entreprises doivent prendre en compte cette nouvelle réalité lors de la création ou de la mise à jour de leurs systèmes de défense. S'ils ignorent le problème, ils s'exposent à des risques importants en termes financiers et de réputation, comme l'ont montré plusieurs incidents gouvernementaux, stratégiques et commerciaux.

Après avoir accepté la réalité du nombre grandissant d'attaques ciblées, il convient de se poser la question suivante : comment pouvons-nous automatiser la détection ?

Kaspersky Lab a été la première entreprise de technologie à établir un laboratoire consacré aux menaces, en 2008. C'est pour cette raison que nos chercheurs ont découvert davantage de menaces avancées et ciblées que toute autre entreprise de sécurité. Cette surveillance et cette connaissance des menaces fournissent directement des informations au service de création de produits de Kaspersky Lab. Tandis que Kaspersky Security Network s'appuie sur la veille en temps réel générée par plus de 60 millions de nœuds dans le monde, notre équipe d'experts du GReAT offre un ensemble de compétences et une expertise uniques pour contribuer à nos capacités de détection et de recherches en matière de menaces, élaborant des solutions pour détecter des menaces incroyablement complexes et sophistiquées.

Aujourd'hui, nous consolidons cette expertise en matière de détection d'attaques ciblées en une solution autonome : une combinaison entre une décennie de recherches et d'analyses des pires menaces et des technologies matures et éprouvées : ***la plate-forme Kaspersky Anti Targeted Attack***. La plate-forme traite continuellement le trafic réseau brut, Web et de messagerie. Elle sélectionne, classe et vérifie les objets qui s'y trouvent. Les artefacts et les métadonnées du trafic sont enregistrés, analysés séparément et juxtaposés afin d'identifier des signes pouvant indiquer la présence potentielle d'une attaque.

Pour garantir une mise en œuvre et un fonctionnement optimaux, Kaspersky Lab propose des services d'expert offrant une installation professionnelle et la formation du personnel au fonctionnement de la plate-forme et à l'efficacité des réactions aux incidents. Ces **services** sont essentiels à la plate-forme Kaspersky Anti Targeted Attack et sont fournis par Kaspersky Lab au moment de la livraison du produit. La plate-forme Kaspersky Anti Targeted Attack est divisée en deux sections logiques : ***acquisition des données*** et ***traitement des données***. L'ensemble de la séquence de détection commence par la section d'acquisition, puis les modules de traitement des données du centre d'analyses entrent en action.

ACQUISITION DES DONNÉES : EFFICACE ET PRATIQUE ?

Plusieurs types de sondes sont utilisés pour rassembler des données depuis différents niveaux de réseau à des fins d'analyse supplémentaire. La configuration peut varier selon les besoins. La plate-forme Kaspersky Anti Targeted Attack permet une flexibilité en termes de nombre et de type de sondes déployées pour chaque installation spécifique. D'une part, cette approche offre la protection des infrastructures informatiques de votre entreprise, quelles que soient la complexité et la configuration (y compris l'utilisation de solutions de sécurité tierces), en plaçant les sondes nécessaires à des emplacements clés. D'autre part, cette approche permet de diminuer le budget de mise en œuvre puisqu'il est inutile d'avoir une solution distincte pour chaque canal de données (e-mail, Web, etc.) si nous disposons de tous les types de sondes nécessaires. Toutes les sondes peuvent fonctionner en parallèle et sont indépendantes.

Sondes réseau

Pendant une décennie passée à détecter, analyser et combattre les programmes malveillants, Kaspersky Lab a accumulé (et continue d'ajouter) des données significatives concernant les fichiers malveillants et légitimes, les modèles de comportement suspect et normal, les adresses Internet malveillantes et de confiance. La plate-forme Kaspersky Anti Targeted Attack utilise toutes ces données pour détecter les cyberintrusions, analyser le trafic réseau et exécuter des objets identifiés avec des sandboxes, vérifier les activités des hôtes et juxtaposer tous les événements. Les **sondes réseau** sont responsables de la collecte des données du trafic réseau et sont basées sur les normes industrielles pour ces solutions.

Les sondes réseau interceptent le trafic IP brut par le biais d'un système de distribution (TAP) du lecteur de réseau virtuel ou d'un port SPAN (Switched Port Analyzer), puis l'analysent en fonction des protocoles des applications, comme HTTP, FTP et DNS. En filtrant l'intégralité du flux de données, les sondes surveillent l'établissement des sessions et génèrent des métadonnées les décrivant. Elles attribuent et sélectionnent des objets du trafic contrôlé. Par la suite, les **objets** et les **métadonnées** sont analysés en utilisant différents modules du centre d'analyses.

Sondes Web

La plate-forme Kaspersky Anti Targeted Attack peut également comprendre des **sondes Web** allouées séparément. Elles utilisent des méthodes différentes de collecte des statistiques et sont souvent appliquées lorsque l'infrastructure de l'entreprise ne peut pas accéder facilement (voire pas du tout) à une copie du trafic depuis un port SPAN. Par exemple, lorsque le trafic https du réseau chiffré n'existe sous forme ouverte non chiffrée que sur le serveur proxy de l'entreprise[1]. Dans de tels cas, il est possible d'accéder à ce trafic par le biais de la plate-forme Kaspersky Anti Targeted Attack grâce au protocole ICAP. Ce type de configuration permet d'identifier des attaques qui utilisent https pour les communications entre les hôtes infectés et les serveurs de commande ou pour télécharger des modules supplémentaires de programmes malveillants.

Il ne s'agit pas de l'unique scénario d'utilisation des sondes Web : elles sont utiles dans tous les cas où ICAP est plus pratique pour l'entreprise que l'obtention d'une copie du trafic depuis le port SPAN.

Sondes de messagerie électronique

La plupart des attaques ciblées débutent par des e-mails de phishing complets. Ne faites pas l'erreur de penser que seuls les employés qui ne sont pas préparés peuvent tomber dans ce piège. Une collecte préalable d'informations permet aux pirates informatiques de concevoir des e-mails adaptés comportant des objets, des pièces jointes et des liens malveillants d'une pertinence telle que même les collaborateurs avertis, y compris les hauts dirigeants et les spécialistes informatiques, cliqueront dessus. Par exemple, les cibles de l'attaque Pawn Storm (avalanche de pions), y compris la Maison Blanche, ont reçu des e-mails de phishing ciblés traitant de sujets liés à la situation politique actuelle.

Ainsi, les modules de contrôle des e-mails s'avèrent essentiels dans toute solution de détection d'attaques ciblées. La sonde de messagerie électronique permet aux clients de contrôler la transmission des pièces jointes. Elle décrypte les éléments indispensables de la correspondance d'entreprise dans une boîte de messagerie spéciale. Le mécanisme de copie caché (BCC) des e-mails est utilisé pour rassembler les e-mails nécessaires, permettant de ne sélectionner que les boîtes de messagerie pertinentes. Par exemple, l'agent de sécurité d'un client peut vouloir que la sonde ignore les comptes d'administrateurs qui reçoivent principalement des avertissements/rapports automatisés et qui sont peu susceptibles de recevoir des e-mails de phishing.

1 Si la surveillance du trafic chiffré, ou « homme du milieu de l'entreprise », est intégrée à un réseau informatique particulier.

Sondes de terminaux

S'il n'est pas possible d'ignorer les types de sondes mentionnés ci-dessus sans réduire les niveaux de sécurité de manière significative, les **sondes de terminaux** sont principalement optionnelles. Sans les **sondes de messagerie**, le produit ne comporte aucun contrôle du trafic de messagerie. Sans les sondes de terminaux, l'ensemble de la sécurité n'est pas affecté, mais il vous manquera des données précieuses supplémentaires concernant les événements qui touchent les terminaux, et qui peuvent augmenter de manière significative la compréhension approfondie de la situation générale de l'attaque. Elles recueillent des informations concernant le comportement lié au réseau de processus exécutés sur des terminaux spécifiques. Le processus qui génère le trafic suspect est découvert grâce aux sondes de terminaux. En consolidant les données concernant les activités de l'hôte et les données du trafic réseau, la plate-forme Kaspersky Anti Targeted Attack réussit à développer une compréhension plus détaillée de ce qui s'est produit à l'intérieur du périmètre de sécurité et permet donc aux agents de sécurité de fournir des réponses plus efficaces et pertinentes.

Les sondes de terminaux sont des agents légers qui n'ont que très peu d'impact sur les performances des terminaux. De plus, elles peuvent fonctionner avec les fournisseurs de solutions de sécurité les plus populaires. Les clients n'ont donc pas à se préoccuper des problèmes de compatibilité.

Les informations rassemblées par les sondes sont finalement utilisées pour les analyses automatisées. Ce qui nous amène au second bloc de modules de la plate-forme Kaspersky Anti Targeted Attack : le **centre d'analyses**. Il permet d'effectuer un traitement et des analyses supplémentaires en fonction du type d'objet détecté et des menaces potentielles qu'il représente. De nombreuses technologies créées par Kaspersky Lab au fil des ans sont incluses dans la plate-forme Kaspersky Anti Targeted Attack, et différents moteurs sont appliqués à différents types de données ou objets. Par exemple, il est possible d'utiliser une sandbox pour les fichiers exécutables, mais pas pour JavaScript ou des langages de programmation interprétés, ce qui signifie que seuls les moteurs d'analyse pertinents s'en chargeront. De même, seules les applications Android peuvent être analysées en fonction du **niveau de risque**.

CENTRE D'ANALYSES, MODULES DE TRAITEMENT DES DONNÉES

Sandbox avancée

L'analyse dynamique est capitale pour détecter les programmes malveillants sophistiqués. Ceci implique l'exécution du fichier sous contrôle strict. Les objets exécutables fournis par les sondes sont analysés sur des machines virtuelles isolées avec différents systèmes d'exploitation et applications (ceci est connu sous le nom de « sandboxing »). Les mécanismes de la sandbox contrôlent le comportement en temps réel des programmes suspects, sans pour autant permettre aux programmes malveillants de dépasser l'environnement virtuel et d'infecter l'infrastructure informatique de l'entreprise.

Le point potentiellement négatif de l'utilisation d'une sandbox par l'analyse dynamique est que les programmes malveillants sophistiqués peuvent détecter les environnements contrôlés et restreindre leur exécution, ce qui leur permet de passer inaperçu. En pareils cas, il ne suffit pas de simplement déployer un nombre de machines virtuelles avec les systèmes d'exploitation appropriés. La sandbox avancée de Kaspersky Lab comprend plusieurs technologies qui empêchent le programme malveillant de détecter qu'il fonctionne dans une sandbox. Ainsi, il ne peut pas se fermer automatiquement, ce qui l'empêcherait de révéler des données sur ses activités.

De plus, certaines techniques d'évasion de type sandbox utilisées par les programmes malveillants peuvent avoir un effet contraire à celui prévu : la sandbox avancée peut identifier certains comportements associés aux techniques d'évasion, les interpréter correctement comme indiquant la présence de programmes malveillants et réagir en conséquence.

Comme dans le cas des sondes, le nombre et le type de machines virtuelles peuvent varier en fonction des besoins spécifiques du projet.

Moteurs d'analyse

Ce bloc comprend plusieurs technologies qui offrent une détection multi-niveaux très puissante pour différents types de données fournies par les sondes.

Disposant de règles uniques, un système de détection des intrusions (IDS) conforme à la norme du secteur et développé par Kaspersky Lab reconnaît de nombreux modèles d'activité malveillante du réseau et fournit ses propres diagnostics de détection. Il est également possible d'ajouter des indicateurs de compromission aux moteurs d'analyse sous la forme de règles YARA décrivant des attaques ciblées actives connues. De plus, Kaspersky Lab a développé une technologie Android spécifiquement destinée à la plate-forme Kaspersky Anti Targeted Attack. Les applications Android sont analysées en fonction du **niveau de risque**, qui est capable d'évaluer les niveaux de suspicion des fichiers .apk.

Toutes les informations réunies par Kaspersky Security Network sont utilisées pour évaluer la fiabilité des URL et des fichiers. Les moteurs d'analyse comprennent également le moteur de protection contre les programmes malveillants de Kaspersky Lab doté des mécanismes heuristiques « NextGen », qui fait partie des pilotes qui exécutent continuellement des processus d'apprentissage internes. Ceci améliore le traitement des menaces connues et inconnues. Les fichiers binaires ne sont pas les seuls objets que le moteur de protection contre les programmes malveillants peut analyser. Les dll, les scripts en plusieurs langages d'interprétation et autres types d'objets, capables, en théorie, d'endommager les systèmes à l'intérieur du périmètre de sécurité, sont également analysés.

Bien que les informations traitées par Kaspersky Security Network soient totalement anonymes et dissociées de leur source, Kaspersky Lab sait que certaines entreprises exigent un verrouillage absolu des données, pour des raisons de conformité ou en raison de leur politique. Jusqu'ici, de telles entreprises ne pouvaient généralement pas utiliser les services de sécurité basés dans le Cloud.

Cependant, Kaspersky Lab a développé pour ces clients un produit autonome : **Kaspersky Private Security Network**, qui permet aux entreprises de bénéficier de la plupart des avantages liés à la surveillance des menaces basée dans le Cloud sans diffuser *de données* hors de leur périmètre de contrôle. C'est aussi simple que cela : il s'agit d'une version totalement privée, locale et personnelle de Kaspersky Security Network[2] pour entreprise.

Analyseur d'attaques ciblées

Une analyse statistique unique du trafic réseau pour la détection d'anomalies est effectuée dans le module **analyseur d'attaques ciblées**. Ce module reconnaît les activités normales de l'infrastructure et signale tout écart suspect par rapport aux schémas habituels. Pour évaluer les risques, l'analyseur d'attaques ciblées utilise la veille stratégique de Kaspersky Lab concernant la popularité des domaines au niveau mondial, les données « whois » et la connaissance des domaines populaires au sein d'une entreprise en particulier. Par exemple, l'utilisation soudaine d'un domaine créé la veille, auquel personne n'a jamais accédé depuis le réseau de l'entreprise, paraît suspect et déclenchera une alerte. De même, les PC utilisés par le service Comptabilité disposent généralement de fonctionnalités du Web et d'applications limitées. Une utilisation soudaine d'outils d'administration à distance avec un trafic sortant ou une visite de sites Web spécialisés en ingénierie serait un comportement inhabituel pour ce genre de systèmes qui déclencherait des alertes.

2 La disponibilité de renseignements basés dans le Cloud est essentielle au fonctionnement de la plate-forme Kaspersky Targeted Attack. Par conséquent, tout client ayant besoin d'un verrouillage complet des données devrait ajouter Kaspersky Private Security Network au groupe de produits qu'il achète.

L'analyseur d'attaques ciblées utilise des techniques avancées et intelligentes d'analyses et d'***apprentissage machine*** pour détecter rapidement des comportements inhabituels sur les réseaux clients. Les mécanismes d'apprentissage machine aident Kaspersky Lab à constituer nos bases de données heuristiques internes, qui sont aussi utilisées pour la mise en cluster d'échantillons selon des indices de similitude et autres algorithmes mathématiques. Ces techniques servent également à créer le tableau de référence permettant la comparaison des activités du réseau.

Surveillance des menaces

La plate-forme Kaspersky Anti Targeted Attack présente le grand avantage de pouvoir utiliser l'ensemble du portefeuille de services et de technologies de Kaspersky Lab. À l'aide de Kaspersky Security Network, la plate-forme peut accéder à de nombreuses bases de données mondiales contenant des informations sur :

- les réputations des URL et des fichiers, permettant une évaluation efficace des risques du trafic
- les serveurs actifs de commande et de contrôle
- les points de distribution de programmes malveillants, etc.

La base de données est continuellement mise à jour en temps réel. La plate-forme Kaspersky Anti Targeted Attack reçoit également un flux d'informations unique comprenant une liste des domaines utilisés par des attaques ciblées actives. Cette base de données est le résultat de recherches et d'analyses effectuées par notre équipe ***Global Research and Analysis Team (GReAT)*** connue dans le monde entier, qui s'occupe également de la gestion de la base. Cela permet d'accélérer et de simplifier le processus de détection lorsque les hôtes en question sont déjà connus comme étant associés à certaines attaques ciblées.

En plus de la réception et du traitement des métadonnées et des objets par des sondes et des modules du centre d'analyses, la plate-forme Kaspersky Anti Targeted Attack offre des services de déploiement en option afin de garantir une mise en œuvre et une maintenance optimales par un personnel bien formé. Les experts de la sécurité internes peuvent également bénéficier d'une formation à la gestion des incidents produit. Et, comme toutes les données collectées et analysées doivent être présentées aux agents de sécurité dans un format adapté, la plate-forme Kaspersky Anti Targeted Attack offre des fonctionnalités intégrées pour la **visualisation** et l'**intégration** avec des solutions tierces.

Console

Compte tenu de l'étendue des systèmes modernes de protection contre les attaques ciblées, une **console centralisée** est un élément indispensable. La console d'administration centralisée de la plate-forme Kaspersky Anti Targeted Attack permet non seulement une utilisation simple, mais elle facilite aussi les analyses de données et la visualisation dans un format pratique pour les agents de sécurité. Dans le même temps, **la recherche rétrospective** est un puissant outil criminalistique. La base de données des diagnostics, qui est complétée par tous les moteurs du produit, permet d'effectuer cette recherche. Le filtrage flexible des événements s'ajoute à l'ensemble des avantages : seuls les événements enregistrés de différentes façons et par plusieurs modules peuvent être affichés, aidant à recréer leur historique et à suivre les dépendances.

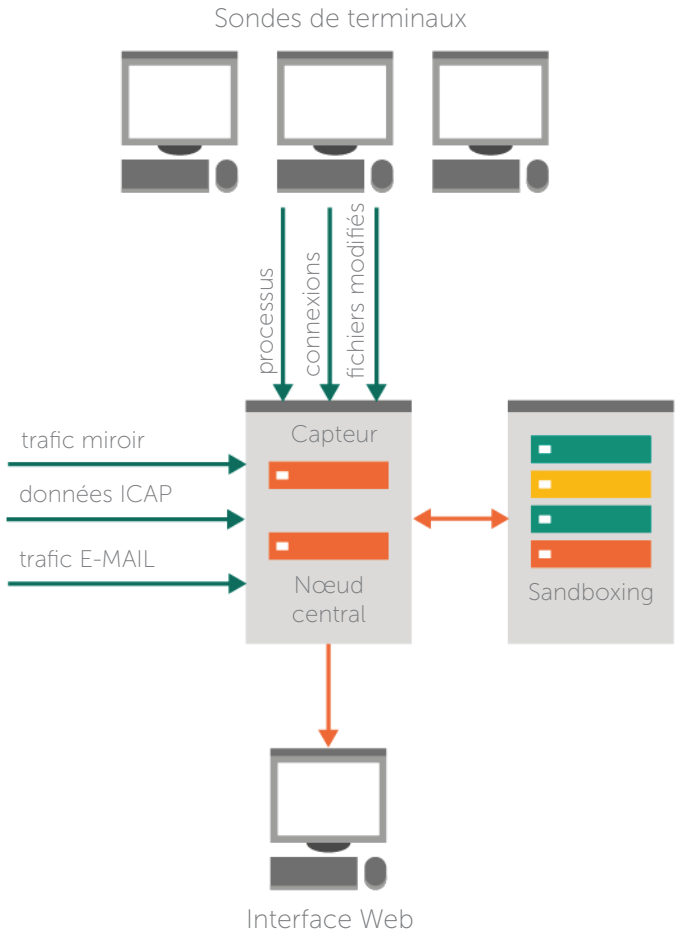
La base de données des diagnostics stocke toutes les données concernant des événements qui ont eu lieu au sein de l'infrastructure informatique de l'entreprise. Son niveau le plus détaillé comprend des **journaux** qui gardent une trace de chaque événement, ce qui s'avère extrêmement précieux lors d'enquêtes, au moment de récupérer la chaîne de frappe d'une cyberattaque. Pour permettre un traitement plus rapide et des périodes plus longues de stockage des données, les journaux sont agrégés de deux manières différentes. **L'agrégation par horodatage** regroupe les données enregistrées au cours d'une période spécifique. **L'agrégation des faits** collecte les enregistrements d'événements pertinents uniquement pour un hôte local, un hôte distant et un processus en particulier (tous les trois doivent participer à l'événement). De plus, certains artefacts du processus de détection sont stockés pendant quelque temps, comme les fichiers téléchargés, dans la sandbox.

Solution de gestion des événements et des informations de sécurité tierce

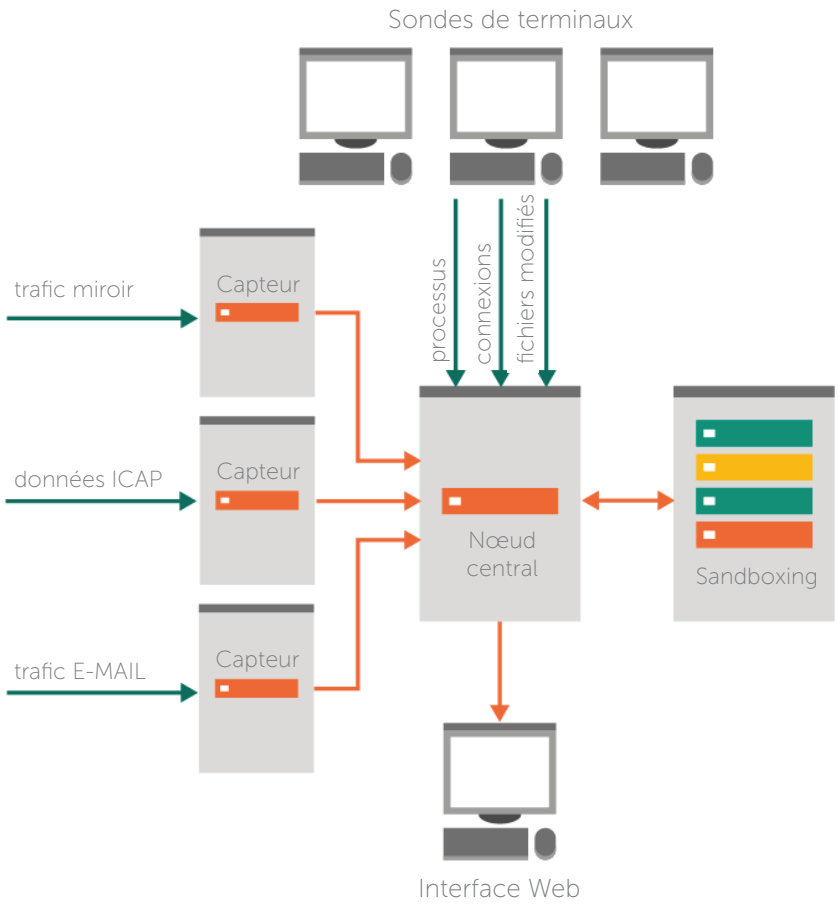
En plus de la console d'administration centralisée de Kaspersky Lab, la plate-forme Kaspersky Anti Targeted Attack supporte l'intégration avec les systèmes de gestion des événements et des informations de sécurité (SIEM) tiers. Elle exporte des événements au format courant syslog, qui peuvent ensuite être importés dans d'autres solutions, dont HP ArcSight, IBM QRadar et Splunk.

Carte matérielle

La configuration matérielle minimale pour l'installation de la plate-forme Kaspersky Anti Targeted Attack est de deux serveurs. Dans ce cas, toutes les sondes (à l'exception des sondes de terminaux) fonctionneront sur le même serveur :



Un déploiement d'entreprise complet requiert quatre serveurs ou plus. Dans ce cas, plusieurs sondes utiliseront différents serveurs pour fonctionner :



Conclusion

Les attaques ciblées requièrent des solutions de sécurité complètes. Les services de sécurité informatique ne peuvent se limiter à protéger uniquement des domaines spécifiques de l'infrastructure informatique ou à analyser uniquement certains événements. Tout mérite notre attention : toute omission peut entraîner des dommages financiers ou porter atteinte à notre réputation.

Le modèle multi-niveaux de Kaspersky Lab permet une détection exhaustive des menaces multi-composants ciblées. Plusieurs types de sondes collectent des données concernant ce qui se produit à l'intérieur du périmètre de sécurité. Les objets du trafic Web et les e-mails potentiellement dangereux sont distillés, pendant que le centre d'analyses contrôle tous les objets à l'aide des moteurs pertinents, grâce aux dernières informations sur les menaces mondiales, récupérées dans le Cloud par Kaspersky Lab.

L'arrivée de la plate-forme Kaspersky Anti Targeted Attack marque la disponibilité publique de notre propre expertise et de nos instruments pour détecter les attaques ciblées, qui n'étaient préalablement disponibles que pour nos chercheurs. Notre longue expérience en matière de détection et de défense contre les attaques ciblées et les programmes malveillants est maintenant accessible aux entreprises clientes qui se préoccupent de la question de l'augmentation rapide des attaques ciblées.


Twitter.com/
kasperskyfrance


Facebook.com/
kasperskylabfrance


https://www.youtube.com/
user/KasperskyFrance

Kaspersky Lab
www.kaspersky.fr

Tout savoir sur la sécurité sur
Internet : www.securelist.fr

Rechercher un partenaire près de chez vous :
http://www.kaspersky.fr/partners/buyoffline/
liste-des-partenaires

KASPERSKY lab