KASPERSKY lab

PLATE-FORME KASPERSKY ANTI TARGETED ATTACK

Détection des menaces avancées...
en temps réel

www.kaspersky.fr

Le nombre d'attaques ciblées visant les grandes entreprises ne cesse d'augmenter, et les techniques et compétences des cybercriminels sont plus sophistiquées que jamais. Les attaques ciblées et menaces avancées d'aujourd'hui sont plus difficiles à détecter, et souvent plus compliquées à contenir et à éliminer. Par conséquent, les grandes entreprises ont besoin d'une stratégie de sécurité adaptable.

Les points faibles de la sécurité et les menaces modernes

La plupart des grandes entreprises ont déjà investi de façon significative dans des solutions de sécurité informatique traditionnelles, surtout situées au niveau de la passerelle. Cependant, même si ces technologies de sécurité préventive peuvent s'avérer très efficaces pour se protéger contre les menaces courantes, y compris les programmes malveillants, les fuites de données, les attaques de réseau, etc., le nombre total d'incidents et d'atteintes à la sécurité des entreprises n'a pas baissé.

Les menaces avancées et ciblées peuvent agir sans être détectées pendant des semaines, des mois, voire des années, tandis que les cybercriminels rassemblent silencieusement des informations précieuses et/ou perturbent des processus métier essentiels. Pendant ce genre d'attaque, des technologies de sécurité axées sur la prévention pourraient détecter des incidents, mais n'arriveront généralement pas à déterminer que les problèmes individuels font partie d'une attaque beaucoup plus dangereuse et complexe qui pourrait provoquer de graves dommages à l'entreprise… et continuer d'en infliger sur le long terme.

Les attaques ciblées sont des processus à long terme qui compromettent la sécurité et permettent au cybercriminel d'accéder de façon non autorisée aux outils informatiques de sa victime, tout en évitant d'être repéré par les technologies de sécurité traditionnelles.

Bien que certains cybercriminels utilisent des menaces persistantes avancées (APT), qui peuvent être très efficaces, mais très coûteuses à mettre en œuvre, d'autres cybercriminels utilisent une technique unique, par exemple un programme malveillant avancé ou une attaque de type « zero-day ».

Pour améliorer les niveaux de sécurité que les solutions traditionnelles peuvent offrir, de nombreuses entreprises automatisent les processus, par le biais de systèmes de gestion des événements et des informations de sécurité (SIEM). Certaines entreprises franchissent le pas pour développer leur propre centre de sécurité dédié, afin de mettre en corrélation des événements et des données, centralisant ainsi la gestion de la sécurité et réagissant aux incidents. Cependant, pour être totalement efficace, cette approche demande une vision mondiale de la sécurité et une expertise approfondie dans l'analyse des cybermenaces. Même les organisations multinationales sont rarement capables de recruter, de former et de retenir les experts nécessaires au sein de leurs équipes de sécurité internes.

Surmonter les limites des technologies de sécurité préventive

Les approches uniquement préventives d'hier n'étant pas efficaces contre les attaques ciblées, les entreprises doivent repenser leur sécurité, ou elles risquent d'être dans l'incapacité de détecter un incident, lorsque les cybercriminels auront obtenu l'accès à leurs systèmes.

En tant que chercheur en cybermenaces reconnu internationalement, Kaspersky Lab soutient l'utilisation d'une stratégie selon laquelle les entreprises mettent en place un processus multi-niveaux continu afin de se défendre contre les attaques ciblées.

Identifier la présence d'une attaque ciblée requiert bien plus que de simplement trouver des échantillons malveillants ou des connexions non autorisées. Une détection avancée repose sur la compréhension du comportement normal du système et de l'utilisateur, ainsi que des analyses constantes de toutes les activités, afin de garantir une visibilité adéquate dans toute l'infrastructure informatique. Afin de s'assurer que les dernières menaces puissent être détectées, les entreprises ont aussi besoin de recevoir des mises à jour proactives sur les menaces et des informations provenant d'une veille mondiale concernant les nouvelles méthodes d'attaque.

Plus une entreprise déploie des efforts pour se protéger, plus cela coûte cher aux cybercriminels de porter atteinte à la sécurité des systèmes de cette entreprise. En premier lieu, il est essentiel que l'entreprise détermine les points faibles de ses systèmes actuels, puis élimine de façon proactive ces problèmes. Il est aussi important de s'assurer que les employés soient conscients des risques en matière de sécurité, sachant surtout que les cybercriminels reconnaissent le potentiel pour une « erreur humaine » et ciblent souvent délibérément les employés durant une attaque. De plus, les agents de sécurité de l'entreprise doivent être formés à identifier et à hiérarchiser les incidents qui sont liés à des attaques ciblées.

Une stratégie de sécurité adaptable

Kaspersky Lab bénéficie d'une expérience unique en tant que leader du secteur dans la détection d'attaques ciblées et d'APT. Presque le tiers des employés de l'entreprise sont des experts en recherche dans le domaine de la sécurité. Par ailleurs, le réseau basé dans le cloud Kaspersky Security Network (KSN) reçoit continuellement des données sur les nouvelles menaces, provenant des quatre coins du monde. Ces données précieuses « collectées sur le terrain » aident l'entreprise à découvrir plus de 310 000 nouveaux programmes malveillants et menaces chaque jour.

Kaspersky Lab est l'un des premiers éditeurs à aider les entreprises à changer leurs stratégies de sécurité pour contrer les menaces avancées et les attaques ciblées. Nous offrons une combinaison unique de technologies et de services, soutenus par le leader mondial de veille stratégique de sécurité, afin d'aider les entreprises à détecter les attaques ciblées et à atténuer les risques... de façon précoce, avant que des dommages graves ne soient causés.

Nous pensons que chaque entreprise a besoin d'établir une stratégie de sécurité adaptable qui est fondée sur quatre piliers essentiels :

- **PRÉVOIR :** pour aider les entreprises à évaluer leur sécurité actuelle et à déterminer comment de futures attaques ciblées pourraient frapper leur infrastructure
- **RÉAGIR** : en aidant les entreprises à mener à bien des enquêtes et à corriger leurs failles de sécurité

- **EMPÊCHER :** pour bloquer les menaces avancées et réduire le risque d'attaques ciblées
- **DÉTECTER :** utiliser une surveillance continue pour identifier les activités qui pourraient signaler une attaque ciblée

La plate-forme Kaspersky Anti Targeted Attack atteint un taux de détection extrêmement élevé parce qu'elle reçoit des flux en temps réel provenant du réseau Kaspersky Security Network, fondés sur les dernières informations de la surveillance des menaces et de la veille stratégique mondiales.

Offrir une stratégie de sécurité multi-niveaux et adaptable

La plate-forme Kaspersky Anti Targeted Attack fait partie d'une approche adaptable et intégrée de la sécurité de l'entreprise. La surveillance du trafic de réseau en temps réel, combinée au sandboxing d'objet et à l'analyse du comportement de terminaux, fournit une vision détaillée de ce qui se passe dans toute l'infrastructure informatique d'une entreprise. Cette approche de la sécurité adaptable protège les entreprises contre la plupart des menaces sophistiquées, des attaques ciblées, des nouveaux programmes malveillants, notamment les programmes ransomware et crimeware, ainsi que les menaces persistantes avancées.

En mettant en corrélation des événements provenant de plusieurs niveaux, y compris le réseau, les terminaux et le contexte mondial de menaces, la plate-forme Kaspersky Anti Targeted Attack fournit une détection « presque en temps réel » de menaces complexes et permet d'effectuer des enquêtes rétrospectives.

ANALYSE DES CHARGES UTILES D'OBJETS SUSPECTS ET DÉTECTION DES APT

Afin d'effectuer une analyse multi-niveaux d'objets, la plate-forme Kaspersky Anti Targeted Attack comprend :

- Des sondes de réseau qui surveillent le trafic du réseau, pour permettre la détection d'indicateurs de cyberattaque
- Des sondes de messagerie électronique qui exfiltrent des objets potentiellement nuisibles provenant de pièces jointes d'e-mail
- Des sondes Web qui exfiltrent des objets provenant du trafic Web en utilisant le protocole ICAP
- La technologie de sandbox avancée qui offre un environnement isolé et virtuel où les objets suspects provenant des sondes Web, de messagerie électronique et de réseau, ainsi que les artefacts qu'ils produisent, peuvent être examinés dynamiquement
- Les données provenant des sondes de réseau et de terminaux sont ensuite combinées et comparées au « tableau de référence » par l'analyseur d'attaque ciblée, afin de découvrir des activités suspectes et de donner à votre équipe de sécurité des alertes précises et au bon moment.

La sandbox est équipée de plusieurs technologies qui empêchent le programme malveillant de détecter qu'il fonctionne dans une sandbox. Ainsi, le programme malveillant ne peut pas se fermer automatiquement et évite de révéler des données sur ses activités.

SURVEILLER UN COMPORTEMENT ANORMAL ET SUSPECT

Afin d'effectuer une analyse avancée du comportement du réseau, la plate-forme Kaspersky Anti Targeted Attack comprend :

- Des sondes de terminaux (agents légers) qui recueillent des informations sur les processus actifs du réseau qui sont exécutés sur les terminaux de l'entreprise
- Des sondes de réseau qui interceptent le trafic IP brut et les activités Internet, pour exfiltrer des métadonnées
- Un analyseur d'attaque ciblée basé sur l'apprentissage et la création de modèles de comportement normal de l'entreprise, et qui détectera les anomalies sur le réseau par corrélation des métadonnées des sondes réseaux et des capteurs de terminaux

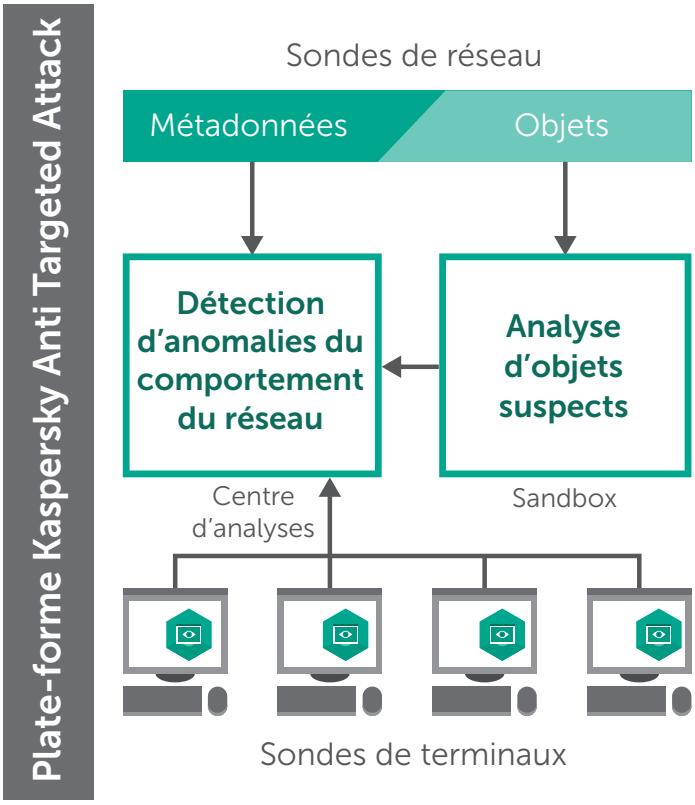
FACILE À UTILISER... ET À GÉRER

L'analyseur d'attaque ciblée reçoit des données des sondes de réseau et de terminaux pour effectuer une analyse approfondie et fournir des verdicts de détection. Tous les verdicts de détection sont conservés, pour être utilisés pendant les enquêtes de post-attaque.

Un tableau de bord, contenant un filtrage des résultats, donne « en un clin d'œil » des informations détaillées sur les activités et les problèmes potentiels... afin d'aider les entreprises à effectuer une détection précoce des incidents en matière de sécurité. Par ailleurs, pour aider à réagir à l'incident et à enquêter après l'attaque, des journaux d'alertes détaillés sont enregistrés pour être analysés sur la plate-forme Kaspersky Anti Targeted Attack. Les journaux des incidents peuvent aussi être transférés au système SIEM du client.

SERVICE DE GESTION DES INCIDENTS LIÉS À DES ATTAQUES CIBLÉES

Lorsque la plate-forme Kaspersky Anti Targeted Attack détermine qu'une entreprise subit une attaque, les experts en sécurité de Kaspersky Lab peuvent offrir un service complet de gestion des incidents, pour analyser l'attaque et aider à définir des mesures correctives. Le service de gestion des incidents peut tout traiter, de l'évaluation initiale de l'incident... à la collecte des preuves, en passant par les analyses criminalistiques, ainsi que l'envoi d'un rapport d'enquête détaillé et d'un plan de mesures correctives.



SERVICE DE DÉTECTION DES ATTAQUES CIBLÉES

Chez Kaspersky Lab, nous savons que les petites entreprises peuvent parfois être exposées à des attaques qui peuvent rester actives pendant très longtemps, tout en restant relativement indétectables. C'est la raison pour laquelle nous proposons un service de détection des attaques ciblées. Ce service fournit un audit de sécurité unique, sans aucune obligation d'acheter une solution de détection des attaques ciblées.

De plus, les experts en sécurité de Kaspersky Lab offrent des services de tests de pénétration, des services d'évaluation de la sécurité des applications et des services de formation à la cybersécurité, pour garantir que les entreprises sont mieux placées pour faire face à de futures attaques.

Plate-forme Kaspersky Anti Targeted Attack/Jan 2016/Mondial

KASPERSKY lab