Solutions de cybersécurité de
Kaspersky Lab pour les entreprises

KASPERSKY lab

Protection contre les menaces avancées et atténuation des risques d'attaques ciblées

Solution Kaspersky Anti Targeted Attack

www.kaspersky.fr
#truecybersecurity

Le risque grandissant des menaces avancées et des attaques ciblées

Augmentation de 200 % des cas de récupération engagée la première semaine qui suit la détection d'une violation de la sécurité*

* Résultats de l'enquête mondiale 2016 de Kaspersky Lab sur les risques liés à la sécurité IT pour les entreprises

15 % des entreprises ont déjà été victimes d'une attaque ciblée, et plus de 53 % y ont perdu des données sensibles*

* Rapport 2015 de Kaspersky Lab sur les risques mondiaux liés à la sécurité IT

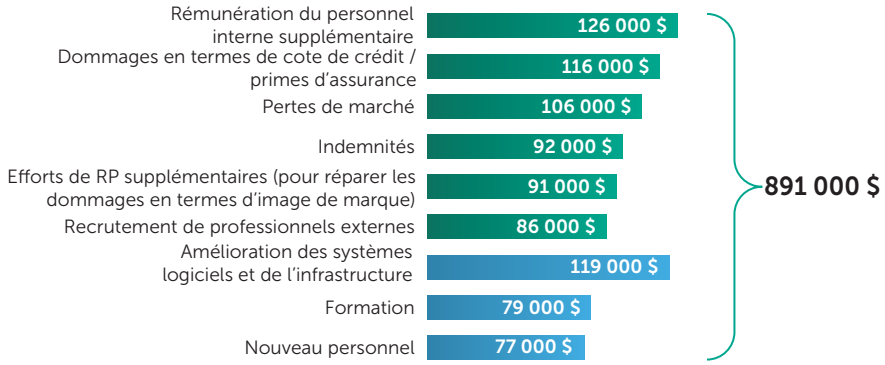
Toute entreprise suffisamment importante pour s'imposer sur le marché représente une cible potentielle. Les entreprises plus petites ne sont pas pour autant à l'abri, car elles sont souvent perçues comme un tremplin facile pour atteindre une plus grosse cible. Mais dans le cas des leaders d'un marché, la probabilité de subir une attaque augmente sensiblement. La question n'est pas « si », mais « quand »...

Paysage des menaces ciblant les entreprises

Les attaques ciblées et les menaces avancées, notamment les menaces persistantes avancées (Advanced Persistent Threats ou « APT »), font partie des principaux risques pour les systèmes d'entreprise. Pourtant, alors que les menaces et les techniques utilisées par les cybercriminels évoluent constamment, un trop grand nombre d'entreprises continuent de miser sur d'anciennes technologies de sécurité et adoptent une position archaïque pour contrer les menaces actuelles et futures.

Des menaces avancées et spécialement ciblées peuvent agir sans être détectées pendant des semaines, des mois, voire des années, tandis que leurs auteurs réunissent lentement et discrètement des informations et travaillent à exploiter la moindre vulnérabilité dans les systèmes de leurs cibles. Contrairement aux programmes malveillants habituels, les menaces avancées et ciblées sont activement contrôlées et gérées par les auteurs. Le but n'est pas seulement de diffuser un programme malveillant, mais bel et bien de s'infiltrer de manière persistante dans le périmètre de l'entreprise. Ces attaques sont le résultat de longues recherches, souvent minutieuses, menées par des auteurs qui sont prêts à attendre le temps qu'il faut.

Pertes moyennes dues à une seule attaque ciblée :



Qui attaque ?

Les cybercriminels : ils vendent les données au plus offrant ou volent simplement de l'argent. Ils créent souvent leurs cyberoutils eux-mêmes ou les achètent sur le Dark Web.

Les entreprises concurrentes : elles cherchent des données confidentielles ou commettent même des actes de sabotage. Elles « achètent » généralement les services de cybermercenaires.

Les cybermercenaires : maîtres du cyberespionnage, ils créent leurs propres outils et vendent leurs « services » au plus offrant.

Les hacktivistes : ils prétendent travailler pour la « bonne cause ». Ils sont inventifs, utilisent des outils complexes et sont une vraie menace pour l'entreprise qui attire leur attention.

Les agences gouvernementales : ils pourraient le nier, mais il est généralement reconnu que les gouvernements du monde entier surveillent quotidiennement des individus, des groupes et des entreprises. Leurs ensembles d'outils peuvent être extrêmement sophistiqués, chers et difficiles à détecter.

Facteurs internes et externes d'une attaque réussie

Les principaux facteurs contribuant à la réussite des attaques ciblées contre les infrastructures IT sont les suivants :

- Un manque de prévention et un excès d'optimisme quant à l'efficacité du périmètre de sécurité en place
- Un manque de sensibilisation des salariés quant aux risques en matière de sécurité des informations
- Un manque de visibilité sur l'environnement IT et notamment sur le routage réseau
- Des logiciels et des systèmes d'exploitation propriétaires et obsolètes
- Une équipe de sécurité pas assez compétente en matière de recherche de programmes malveillants, de cyberdiagnostic, de réponse aux incidents et de surveillance des menaces

Quels sont les risques ?

Toutes entreprises confondues :

- Transactions non autorisées
- Vol ou corruption de données critiques
- Manipulation discrète de processus
- Déstabilisation par la concurrence
- Chantage et extorsion
- Usurpation d'identité

Principaux secteurs d'activités :

Services financiers

- Transactions non autorisées
- Attaques de DAB et vol d'argent liquide
- Usurpation d'identité

Gouvernement

- Manipulation de données
- Espionnage
- Disponibilité restreinte des services en ligne
- Usurpation d'identité
- Actes de cyberactivisme

Production/fabrication et haute technologie

- Espionnage (savoir-faire)
- Processus technologiques stratégiques compromis

Télécommunications

- Attaques sur des entreprises utilisant l'infrastructure de télécommunications
- Manipulation des serveurs de messagerie électronique à des fins d'ingénierie sociale
- Contrôle du système de facturation
- Manipulation des ressources Web à des fins de phishing
- Utilisation d'une infrastructure compromise (appareils/IoT) aux fins d'attaques DDoS

Énergie et services publics

- Manipulation grâce aux données de calcul
- Attaques sur les réseaux technologiques et dommages physiques

Médias de masse

- Cyberactivisme
- Site Internet compromis (dégradation, phishing) et attaques de masse

Santé

- Vol d'informations sur des patients
- Attaques sur les équipements de télémédecine

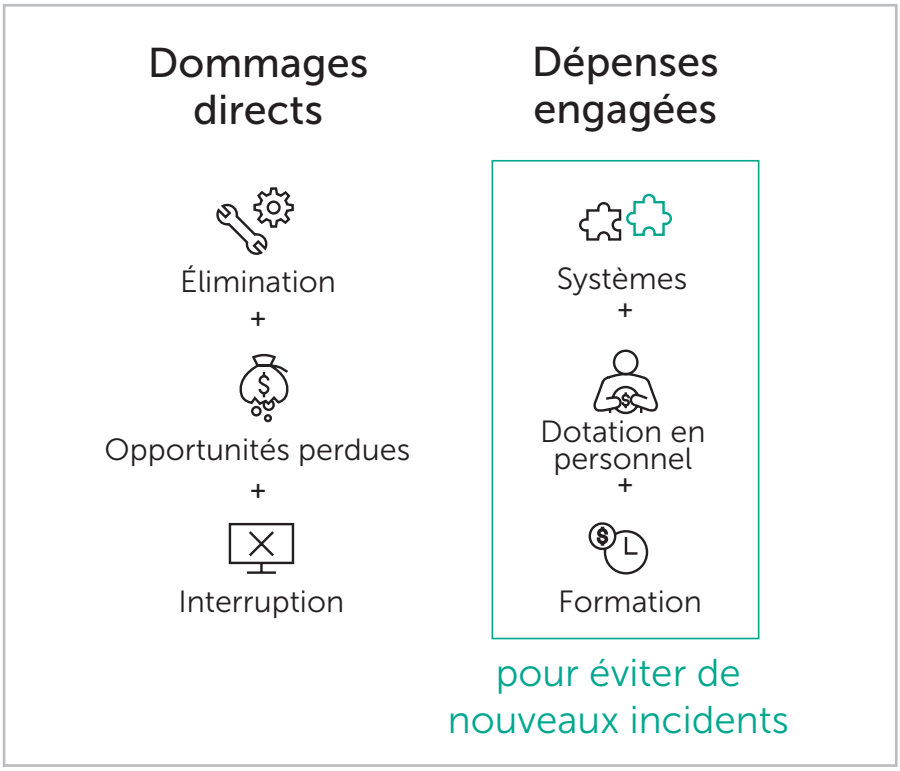
Attaques ciblées : cybercriminel, un métier à part entière

La plupart des attaques ciblées sont supervisées par des cybercriminels et des pirates hautement expérimentés qui savent comment adapter chaque phase de leur attaque : tromper les défenses traditionnelles, exploiter les failles et optimiser la quantité d'argent, de données confidentielles, etc. qu'ils peuvent dérober.

Les cybercriminels d'autrefois sont devenus des professionnels pour qui la cybercriminalité est un véritable métier. Leur seule motivation lorsqu'ils ciblent et attaquent une entreprise : dégager un maximum de bénéfices qu'ils prennent soin de calculer avant même de lancer l'attaque, en fonction des coûts associés et des gains possibles. Il s'agit bien évidemment de minimiser les coûts initiaux en lançant une attaque aussi bon marché que possible et avec un potentiel de gains financiers maximum.

La plupart des attaques ciblées combinent l'ingénierie sociale à un ensemble d'outils personnalisés. Le coût d'une attaque ciblée efficace a considérablement diminué, d'où une hausse proportionnelle du nombre total d'attaques à travers le monde.

Quelles sont les conséquences lorsqu'une entreprise telle que la vôtre est victime d'une attaque ciblée ?



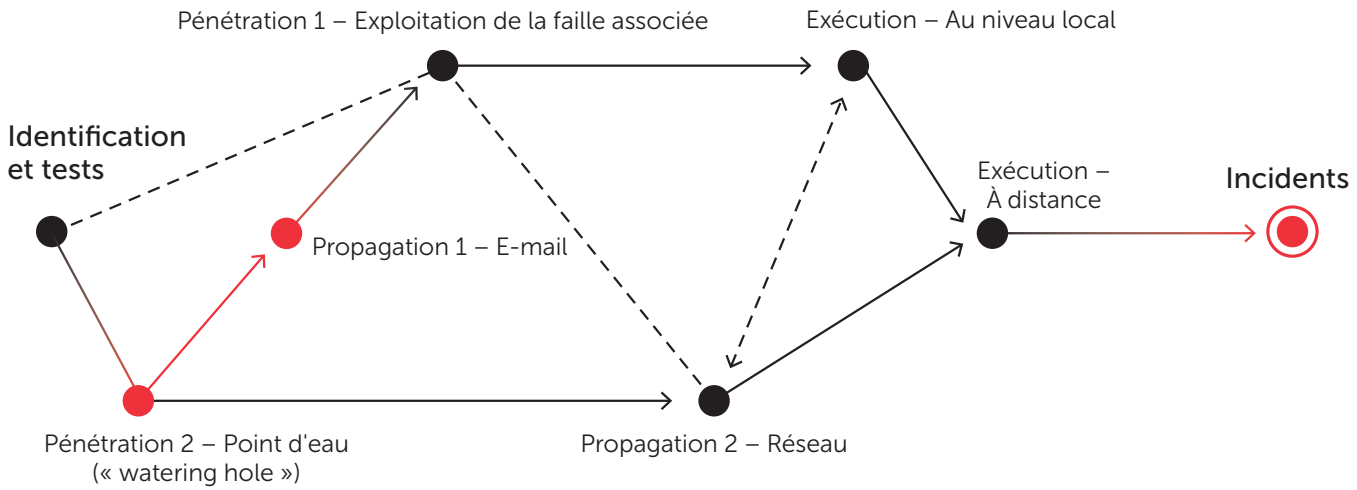
Pertes financières directes. Les cybercriminels peuvent voler vos identifiants de connexion bancaires afin d'accéder aux comptes de l'entreprise et d'effectuer des transactions frauduleuses.

Perturbation des processus métier clés. Alors que certaines attaques perturbent ou ralentissent simplement les processus métier stratégiques, d'autres prévoient délibérément de les saboter. Même si une attaque est découverte, des perturbations s'en suivent car l'entreprise ciblée conduira des investigations et restaurera ses opérations, perdant potentiellement d'autres opportunités commerciales.

Frais de nettoyage. Après une attaque, vous pouvez avoir à payer de nombreuses dépenses imprévues. Restaurer les systèmes et les processus nécessite souvent des dépenses en capital et opérationnelles, telles que l'embauche de consultants en sécurité et en systèmes IT.

Structure d'une attaque ciblée

En théorie, la chaîne de frappe d'une attaque ciblée paraît relativement simple : Reconnaissance et test, Pénétration, Propagation, Exécution, Résultat. Cela pourrait nous amener à croire qu'en bloquant automatiquement les premières étapes d'une attaque à plusieurs niveaux, l'attaque toute entière serait contrée.



Or, dans la réalité, les attaques ciblées sont extrêmement sophistiquées et non linéaires en termes de progression et d'exécution. Il convient donc de mettre en place une stratégie multiniveaux reposant notamment sur des capacités de détection automatisées, une surveillance en continu et la recherche de menaces.

Les attaques ciblées visent le long terme pour compromettre la sécurité et permettre au cybercriminel de contrôler les outils IT de sa victime, tout en évitant d'être repéré par les technologies de sécurité traditionnelles.

Certains utilisent des menaces persistantes avancées (« APT »), très efficaces, mais aussi très coûteuses à mettre en œuvre, tandis que d'autres adoptent une technique unique : un programme malveillant avancé ou une faille de type « zero-day ».

Une attaque ciblée est un processus long par lequel un cybercriminel viole un système de sécurité et contourne des procédures d'autorisation afin d'interagir avec une infrastructure IT sans être repéré par les technologies de détection traditionnelles.

Premièrement, il s'agit d'un processus suivi : d'un vrai projet, et non d'une simple action malveillante ponctuelle. D'après notre expérience, ces attaques durent généralement au moins 100 jours. Pour les agences gouvernementales, les grands acteurs du marché et les infrastructures critiques, elles peuvent même s'étendre sur plusieurs années.

Deuxièmement, ce processus vise une infrastructure particulière et est conçu pour déjouer des mécanismes de sécurité spécifiques. Aussi peut-il tout à fait cibler des salariés précis par e-mail ou via les réseaux sociaux. Cette approche n'a rien à voir avec celle des attaques classiques qui reposent sur l'envoi en masse de logiciels malveillants et qui poursuivent des objectifs complètement différents. Dans le cas d'une attaque ciblée, le mode opératoire et la chaîne de frappe s'articulent autour d'une victime précise.

Troisièmement, ce type d'attaque est généralement perpétré par un groupe ou une équipe de professionnels organisés, parfois de dimension internationale, dotés d'outils techniques sophistiqués. Plus qu'un simple projet, leurs activités pourraient être qualifiées d'opérations de combat groupé. Par exemple, les cybercriminels peuvent dresser une liste de salariés susceptibles de servir de « passerelle » vers l'entreprise et les réseaux ciblés, et étudier leur profil en ligne ainsi que leur activité sur les réseaux sociaux. Obtenir le contrôle de l'ordinateur professionnel de la victime n'est alors plus qu'une formalité. Une fois l'ordinateur infecté, les intrus prennent le contrôle du réseau et poursuivent leurs activités criminelles.

Défis auxquels les entreprises sont confrontées en matière de sécurité

À l'heure où les menaces sophistiquées grandissent de façon exponentielle, bon nombre d'entreprises mettent déjà en place des technologies et des services dans l'espoir d'atteindre un niveau de visibilité et de protection supérieur. Mais sans une approche multidimensionnelle et une planification stratégique, ces efforts peuvent être vains.

Voici quelques exemples de résultats décevants d'investissements en matière de sécurité « inégaux » ou non structurés :

1. De lourds investissements sont réalisés pour la mise en place d'une sandbox, de technologies autonomes ou d'un SOC, mais aucune de ces initiatives n'améliore proportionnellement la sécurité.

Les techniques de sécurité du périmètre comme les pare-feu et les logiciels de protection contre les programmes malveillants peuvent faire face à certaines des attaques les plus opportunistes. Le problème est autre avec les attaques ciblées.

Certains éditeurs ont cherché à contrer ces APT avec plusieurs produits autonomes et discrets : sandboxes, analyses d'anomalies du réseau, voire surveillance axée sur les terminaux. Si ces produits peuvent individuellement offrir – et offrent – une protection et bloquent la boîte à outils du cybercriminel, ils ne suffisent pas à détecter une attaque ciblée coordonnée.

L'identification d'une telle attaque requiert la détection de plusieurs événements survenant à tous les niveaux de l'infrastructure de l'entreprise. Les informations recueillies peuvent ensuite être traitées au moyen d'un système d'analyse multiniveaux et être interprétées grâce à une veille stratégique en temps réel fournie par une source fiable. En d'autres termes, le meilleur investissement consiste à intégrer la crème des technologies (dont une sandbox et des analyses d'anomalies de réseau et d'événements sur les terminaux) à un processus global et complet.

2. Les solutions actuelles génèrent bien trop d'événements de sécurité pour que votre équipe SOC puisse les traiter, les analyser, les trier et y répondre suffisamment vite.
3. Le niveau des compétences en sécurité n'est pas adapté au degré de sophistication actuel des menaces. Les experts peuvent savoir détecter des incidents et rapidement appliquer des mesures correctives (« Golden Image », liste noire d'URL/de fichiers, règles) sans pour autant savoir mettre en place un processus de réponse complet (définition du niveau de risque, analyse initiale, enquête, confinement, diagnostic).
4. L'entreprise peut manquer de visibilité sur les opérations. Pendant une attaque ciblée, les cybercriminels peuvent facilement contourner les solutions de sécurité traditionnelles au moyen d'identifiants volés et d'un logiciel authentique dissimulant toute violation du système.

Parce que les cybercriminels mettent tout en œuvre pour passer inaperçus, il peut être très difficile pour une équipe interne de sécurité IT de détecter une attaque. Les dommages peuvent donc s'étendre sur une longue période.

En réalité, le programme malveillant est responsable de seulement 40 % des atteintes à la sécurité, car les cybercriminels utilisent de nombreuses autres techniques d'accès aux systèmes.
De plus, si un programme malveillant est utilisé, il sera conçu à 70-90 % spécialement pour l'organisation qu'il viole (Verizon : Rapport d'enquêtes sur la violation des données).

5. Il est difficile de savoir quelle expertise développer en interne, quelles tâches de sécurité externaliser et lesquelles confier sans crainte à des systèmes automatisés.

Compte tenu de la gravité accrue des incidents et de leur impact potentiel sur l'efficacité globale de l'entreprise, le département de sécurité doit veiller à se doter d'experts dûment compétents et en nombre suffisant. C'est là l'un des principaux défis. Pour être totalement efficace, une stratégie de sécurité nécessite non seulement une surveillance en continu et des capacités de détection, mais aussi une réponse rapide, des mesures correctives appropriées et des processus de cyberdiagnostic adaptés.

Les équipes SOC traditionnelles ont tendance à se concentrer uniquement sur les tâches de détection et de réponse. Les solutions automatisées évitent aux experts d'avoir à exécuter les étapes suivantes du processus de gestion des incidents, mais rares sont les entreprises prêtes à assumer toutes les tâches de haut niveau en interne. L'enjeu est donc d'identifier quels éléments du processus global (gestion, définition du niveau de risque, hiérarchisation, reprise rapide) doivent être pris en charge par l'équipe interne et lesquels (recherche de programmes malveillants, cyberdiagnostics, réponse aux incidents, recherche de menaces) peuvent être externalisés auprès de spécialistes pour plus d'efficacité.

Un mot sur les sandboxes

De nombreuses « solutions de détection d'attaques ciblées » comprennent simplement une sandbox autonome. Même les éditeurs sans expérience dans la détection de nouvelles menaces avancées offrent des sandboxes, mais il s'agit souvent d'une simple extension de leurs moteurs de protection contre les programmes malveillants, sans capacités de veille significatives.

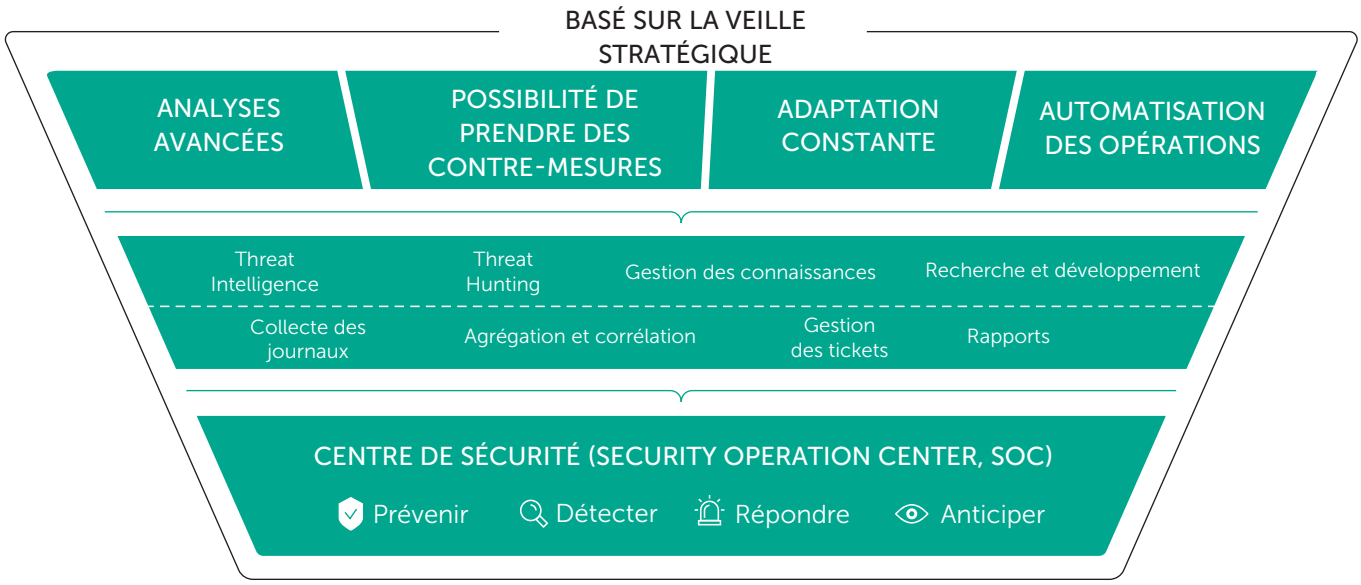
La sandbox avancée de Kaspersky Lab représente juste une autre partie de nos capacités de détection intégrée. C'est un dérivé direct de notre ensemble de sandboxes interne, la technologie que nous utilisons depuis plus de dix ans. Ses capacités ont été affinées d'après les statistiques recueillies après dix ans d'analyse des menaces, la rendant plus mature et plus focalisée sur les menaces ciblées que les sandboxes « miracles » actuellement proposées.

Le SOC d'entreprise basé sur la veille stratégique

Les cybercriminels ont adapté leurs techniques pour contourner les défenses traditionnelles et passer inaperçus sur les systèmes pendant des mois, voire des années. Il est temps que les systèmes de protection d'entreprise s'adaptent à leur tour avec une approche de sécurité IT multiniveaux, basée sur la veille stratégique.

Jusque récemment, il suffisait de défendre le périmètre de l'entreprise en utilisant des technologies de sécurité communément disponibles qui empêchaient les infections de programmes malveillants ou l'accès non autorisé au réseau de l'entreprise. Cependant, aujourd'hui, avec l'augmentation des attaques ciblées, cette approche simple n'est plus adaptée.

Pour permettre à votre département de sécurité de se prémunir contre les nouveaux dangers, vous aurez besoin d'une approche multidimensionnelle extrêmement flexible, articulée autour d'un SOC conventionnel s'appuyant sur une veille stratégique des menaces (Threat Intelligence) et des solutions de sécurité multiniveaux.



Améliorer les processus de sécurité de l'entreprise

Le département de la sécurité des informations est chargé de la protection organisationnelle et technique des informations critiques et des processus métier dans des environnements IT souvent complexes. Pour ce faire, il peut par exemple utiliser davantage de solutions automatisées et de composants logiciels et s'orienter vers une gestion électronique des documents.

L'augmentation fulgurante du nombre de menaces avancées et d'attaques ciblées a entraîné une multiplication du nombre de solutions. Les processus existants doivent être mis à niveau afin de pouvoir collecter, stocker et traiter les données non structurées générées et de pouvoir identifier et hiérarchiser des attaques multiniveaux complexes. Ces technologies sont les suivantes :

- Hiérarchisation manuelle des menaces et évaluation des facteurs signalant la possibilité d'une attaque ciblée
- Collecte d'informations sur les attaques ciblées et de statistiques sur les menaces avancées
- Identification des incidents et réponse
- Analyse des objets suspects dans le trafic réseau et les pièces jointes d'e-mails
- Détection d'une activité anormale / inhabituelle au sein de l'infrastructure protégée

Les grandes entreprises répondent aux menaces avancées actuelles en optant pour une gestion centralisée de la sécurité des informations, en consolidant les données issues de solutions de sécurité hétérogènes (via une collecte de données et une corrélation d'événements automatisés (systèmes SIEM)) et en unifiant leur présentation grâce à la création de centres de surveillance de la sécurité (Security Operations Centers ou « SOC »). Mais pour que cette approche soit efficace contre les attaques ciblées et les menaces avancées, il est nécessaire de comprendre pleinement les problèmes de sécurité et de maîtriser l'analyse des cybermenaces.

Notre solution

Kaspersky Lab a été la première à créer un laboratoire consacré aux menaces avancées, en 2008.

C'est grâce à lui que nous avons pu découvrir davantage de menaces avancées et ciblées que tout autre fournisseur de solutions de sécurité. Si vous entendez parler de la toute dernière menace persistante avancée, il y a de fortes chances que ce soit l'équipe d'élite Global Research and Analysis Team (GReAT) de Kaspersky Lab à l'avoir détectée.

Dotée d'une expérience unique en matière de détection d'attaques ciblées et d'APT, notre équipe GReAT est réputée pour ses services de surveillance des menaces. L'équipe a joué un rôle clé en découvrant la plupart des attaques les plus sophistiquées, comme :

- Stuxnet
- RedOctober
- Flame
- Miniduke
- Epic Turla
- DarkHotel
- Duqu
- Carbanak
- Equation

... et bien d'autres encore.

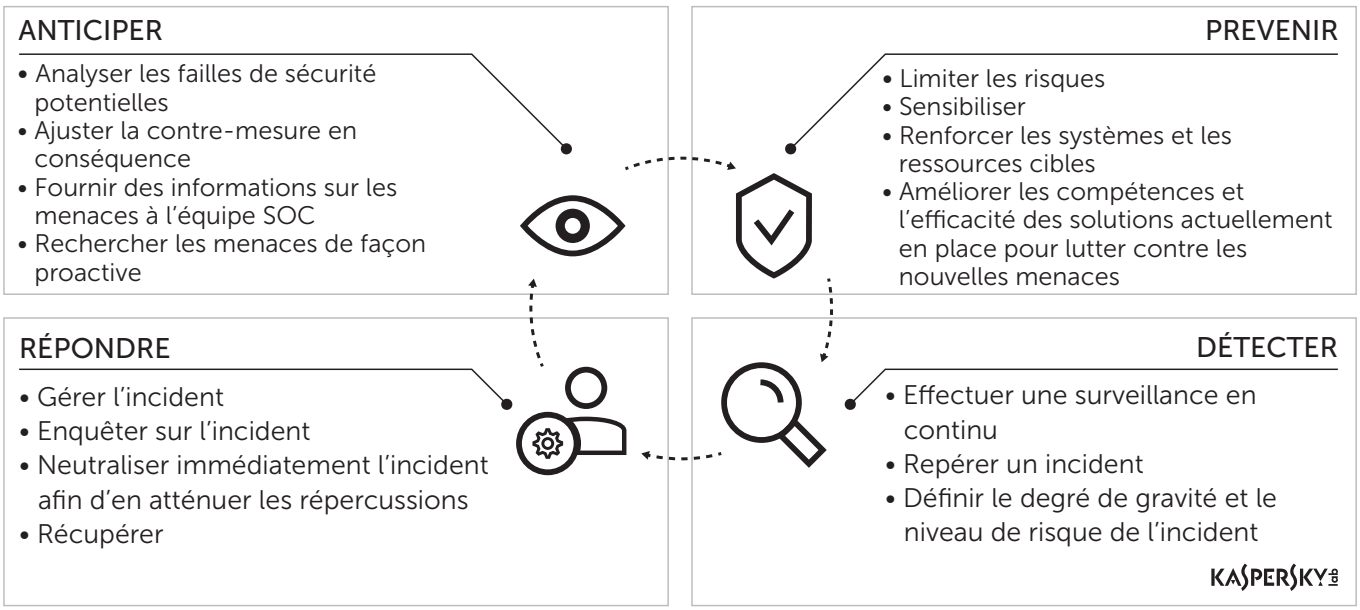
En disséquant le fonctionnement interne d'attaques extrêmement sophistiquées, Kaspersky Lab a pu développer un portefeuille stratégique de technologies et de services capables de fournir une approche de sécurité adaptable et entièrement intégrée. Notre expertise a permis à Kaspersky Lab d'obtenir davantage de premiers prix aux tests indépendants de détection et d'atténuation des menaces que n'importe quelle autre entreprise de sécurité informatique. À présent, nous avons consolidé cette expertise en matière de détection d'attaques ciblées en une solution autonome : l'aboutissement de deux décennies de recherches et d'analyses des pires menaces, débouchant sur des technologies matures et éprouvées.

Tandis que la majorité des cybermenaces simples peuvent être bloquées par des produits de sécurité traditionnels, basés sur les signatures et renforcés par des méthodes heuristiques, les cybercriminels et les pirates d'aujourd'hui utilisent des attaques incroyablement sophistiquées pour cibler des entreprises spécifiques. Les attaques ciblées, notamment les menaces persistantes avancées (Advanced Persistent Threats ou « APT »), font désormais partie des principaux risques auxquels les entreprises doivent faire face. Cependant, alors que les menaces et les techniques que les cybercriminels et pirates emploient sont en constante évolution, de nombreuses entreprises ne parviennent pas à adapter leurs stratégies de sécurité.

Plus difficiles à détecter et souvent plus compliquées à éliminer, les attaques ciblées et les menaces avancées requièrent une stratégie de sécurité exhaustive et adaptable. La stratégie de sécurité évolutive de Kaspersky Lab repose sur l'architecture de sécurité la plus viable qui soit, telle que décrite par Gartner. Notre approche consiste à proposer un cycle d'activités dans quatre domaines principaux : Empêcher, Détecter, Réagir et Prévoir.

- Prévenir : réduire le risque de menaces avancées et d'attaques ciblées
- Détecter : identifier les activités qui pourraient signaler une attaque ciblée
- Répondre : éliminer les failles de sécurité et enquêter sur les attaques
- Anticiper : savoir où et comment les prochaines attaques ciblées sont susceptibles de se produire

Concrètement, cette approche suppose que les systèmes de prévention traditionnels fonctionnent de pair avec les technologies de détection, les analyses de menaces, les capacités de réponse et les techniques de sécurité prédictives. De cette façon, il est possible de créer un système de cybersécurité capable de s'adapter en continu aux défis émergents auxquels sont confrontées les entreprises, et d'y faire face.



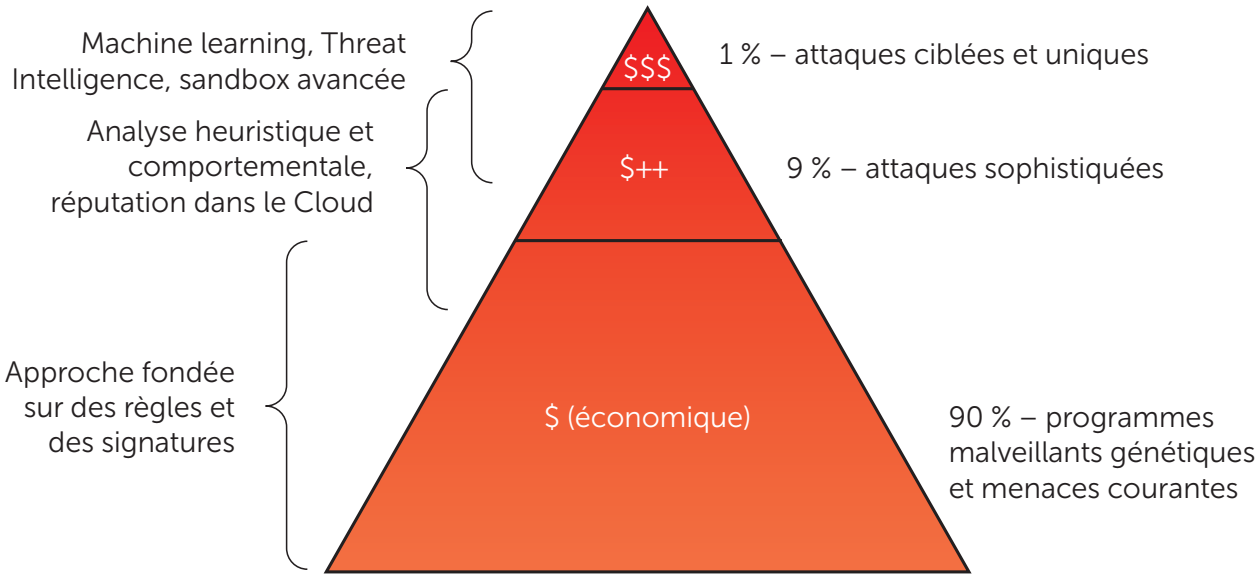
Prévenir : utiliser des technologies de sécurité primées pour réduire le risque d'attaques ciblées

Pour les attaques ciblées, les technologies de prévention s'avèrent utiles car elles permettent de filtrer les incidents sans intérêt, les objets malveillants courants et les communications non pertinentes.

Néanmoins, un système complet, avec des solutions de sécurité ciblées, des formations à la sécurité et des actions de sensibilisation, est tout aussi précieux. Les cybercriminels auront besoin de plus de temps et de plus d'argent pour pénétrer votre périmètre de contrôle, et vous attaquer sera beaucoup moins rentable.

Les produits de sécurité axés sur la prévention peuvent être très efficaces contre les menaces courantes (programmes malveillants, attaques réseau, fuites de données, etc.). Néanmoins, même ces technologies ne suffisent pas pour protéger une entreprise contre les attaques ciblées. Pendant une attaque ciblée, les technologies de sécurité conventionnelles axées sur la prévention peuvent détecter des incidents, mais n'arrivent généralement pas à déterminer que les incidents individuels font partie d'une attaque beaucoup plus dangereuse et complexe qui peut provoquer de graves dommages à votre entreprise... et continuer d'en infliger sur le long terme.

Toutefois, les technologies multiniveaux axées sur la prévention demeurent un atout clé dans la nouvelle approche proactive de protection contre les attaques ciblées.



À chaque menace, une technologie de sécurité adaptée

80 % des attaques ciblées commencent par une pièce jointe ou un lien dans un e-mail malveillant.

Les cibles de pénétration privilégiées par les cybercriminels sont notamment les RH, les centres d'appels, les assistants personnels des hauts dirigeants et les services externalisés de l'entreprise, car ils sont considérés comme les moins préparés.

Il est essentiel que les entreprises continuent d'utiliser les technologies de sécurité « traditionnelles » pour :

1. automatiser le filtrage et le blocage des événements et des incidents qui ne sont pas liés à des attaques ciblées, de façon à ne pas se disperser et à se concentrer sur la détection des incidents pertinents ;

2. renforcer l'infrastructure IT contre des menaces « bon marché » et simples d'exécution (ingénierie sociale, appareils amovibles et mobiles, programmes et e-mails malveillants, etc.). En effet, les dépenses consacrées à la sécurité du périmètre et des terminaux, associées aux contrôles mis en place, contraignent les cybercriminels à davantage d'efforts et d'investissements pour pénétrer dans votre réseau.

Cependant, si l'auteur de l'attaque est suffisamment motivé, voire engagé par un tiers pour réussir, une approche uniquement axée sur la prévention ne suffira pas.

Détecter : découvrir les menaces avancées aux vecteurs multiples avant qu'il ne soit trop tard

La plate-forme Kaspersky Anti Targeted Attack offre :

- Une architecture de sondes multiniveaux pour une visibilité à 360 degrés. Grâce à une combinaison de sondes réseau, Web et messagerie électronique, ainsi que de terminaux, la plate-forme KATA fournit une détection avancée à chaque niveau de l'infrastructure IT.
- Une sandbox avancée pour évaluer les nouvelles menaces. Résultat de plus de 10 ans de travail continu, notre sandbox avancée offre un environnement isolé et virtuel où les objets suspects peuvent être exécutés en toute sécurité, afin d'en observer le comportement.
- Des moteurs d'analyse puissants pour des diagnostics rapides et moins de faux positifs. Notre analyseur d'attaques ciblées évalue les données du réseau et des terminaux captées par les sondes, puis génère rapidement un rapport de détection des menaces destiné à l'équipe de sécurité.

Plus vous détectez une attaque tôt, moins vous subirez de pertes financières et de perturbations. Ainsi, la qualité et l'efficacité de la détection sont d'une importance capitale.

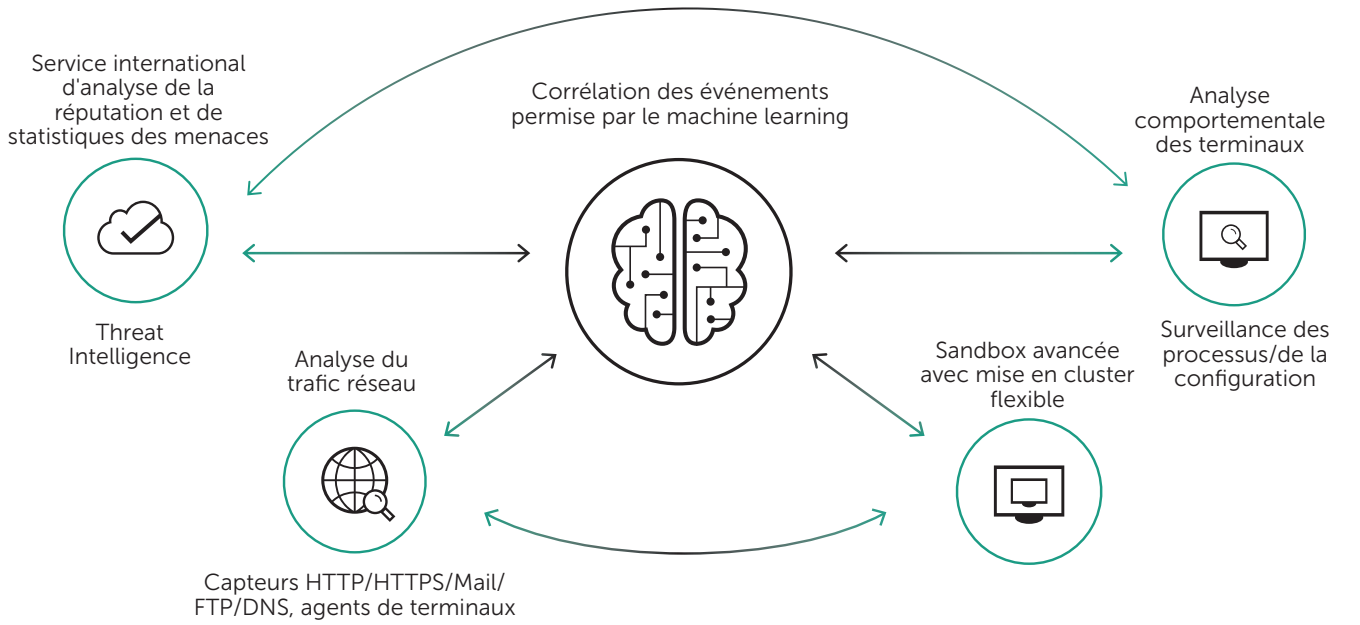
Étant donné que les attaques ciblées sont combinées et complexes, les détecter demande une connaissance pratique approfondie du fonctionnement des attaques avancées et ciblées. De simples solutions contre les programmes malveillants ne peuvent pas faire face à ces types d'attaques. Il vous faut plutôt des technologies de détection qui accèdent aux toutes dernières données de surveillance des menaces et analysent de façon détaillée les comportements suspects à différents niveaux de votre réseau d'entreprise.

Pour détecter des attaques ciblées, les solutions et services connectés suivants sont nécessaires :

- Une formation
- Une expertise en matière de détection d'attaques ciblées (audit ponctuel de l'infrastructure à la recherche de signes de compromission)
- Une solution spécialisée, à savoir la plate-forme Kaspersky Anti Targeted Attack
- Des flux d'informations sur les nouvelles menaces partagés et mis à jour en temps réel
- Des rapports personnalisés et sur les APT permettant de mieux comprendre les sources et les modes opératoires

La plate-forme Kaspersky Anti Targeted Attack (KATA) est une solution innovante qui fournit des capacités de détection allant bien au-delà des technologies de sécurité conventionnelles et axées sur la prévention.

La plate-forme Kaspersky Anti Targeted Attack repose sur une approche adaptable et intégrée de la sécurité de l'entreprise. La surveillance en temps réel du trafic réseau, associée au sandboxing d'objet et à l'analyse du comportement des terminaux, permet d'obtenir une vision détaillée de tout ce qui se passe dans l'infrastructure IT d'une entreprise. En corrélant plusieurs événements, issus du réseau, des terminaux et du paysage mondial de menaces, la plate-forme Kaspersky Anti Targeted Attack détecte « quasi en temps réel » les menaces complexes et permet d'effectuer des enquêtes rétrospectives.

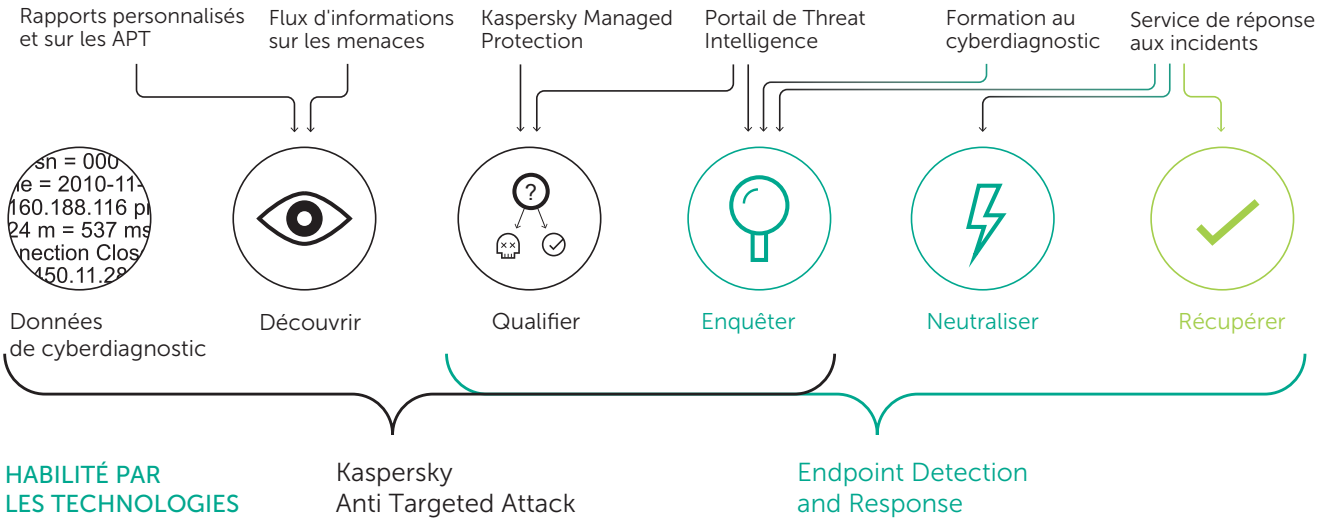


Répondre : aider les entreprises à se remettre des attaques

Bien entendu, parvenir à un niveau plus élevé de détection n'est qu'un élément de la bataille. Les meilleures technologies de détection ne servent pas à grand-chose si vous ne possédez pas les outils et l'expertise nécessaires pour répondre rapidement aux menaces qui endommagent potentiellement votre entreprise.

Après avoir détecté une attaque, vous devez avoir accès à des experts en sécurité reconnus qui ont les compétences et l'expérience pour :

- évaluer et réparer les dommages ;
- restaurer rapidement vos activités ;
- obtenir des informations utiles à l'issue du processus d'enquête sur l'incident ;
- établir un plan d'action permettant d'éviter une attaque à l'avenir.



Dès que la plate-forme Kaspersky Anti Targeted Attack détecte une attaque, nos experts peuvent aussi vous aider à l'analyser. Notre service de gestion des incidents comprend :

- Évaluation des incidents. Analyse initiale d'incident fournie rapidement (sur site ou à distance) pour réduire les dommages subis par votre entreprise.
- Collecte des preuves. Par exemple, rassembler des images de disque dur, des vidages de mémoire, des traces réseau et d'autres informations connexes à l'incident
- Analyse criminalistique. Une analyse détaillée pour permettre d'établir des informations sur les points suivants :
  - ce qui a été attaqué
  - qui a mené l'attaque
  - la période pendant laquelle votre entreprise a été attaquée
  - où l'attaque a débuté
  - pourquoi votre entreprise a été attaquée
  - comment l'attaque a été mise en œuvre
- Analyse des programmes malveillants. Analyse détaillée des programmes malveillants utilisés au cours de l'attaque.
- Plan des actions correctives. Plan détaillé qui aidera votre entreprise à empêcher le programme malveillant de se propager davantage sur votre réseau et création d'un plan de désinstallation.
- Rapport d'enquête. Un rapport détaillé sur l'investigation de l'incident et les actions correctives.

  Si votre propre équipe de sécurité est capable d'effectuer la plupart des tâches de gestion des incidents, vous souhaiterez peut-être utiliser un de nos autres services :
- Service d'analyse de programmes malveillants : soumet à une analyse détaillée le programme malveillant isolé par votre équipe.
- Service d'analyse criminalistique des systèmes numériques : analyse les preuves numériques et les effets de l'incident relevés par votre équipe.

Anticiper : faire davantage pour se protéger contre de futures menaces

Le paysage des menaces change sans cesse, et votre stratégie de sécurité doit suivre afin de relever les nouveaux défis.

La sécurité n'est pas une « activité ponctuelle », mais un processus continu qui exige une évaluation permanente :

- des dernières menaces
- de l'efficacité de votre sécurité IT

... afin que votre entreprise puisse s'adapter aux nouveaux risques et à l'évolution des exigences.

Avoir accès à des experts, qui vous tiennent à jour sur le contexte mondial des menaces et vous aident à tester vos systèmes et vos défenses existantes, est essentiel pour aider votre entreprise à s'adapter aux nouvelles menaces.

Au fil des ans, nos experts dans le monde ont réuni une grande quantité de connaissances sur le fonctionnement des attaques avancées et ciblées. De plus, nous analysons constamment de nouvelles techniques d'attaque. Cette expertise durement acquise nous place dans une position unique pour prévoir les nouvelles méthodes d'attaque et vous préparer à les combattre.

D'autre part, nous pouvons offrir des services spécialisés pour vous aider à « renforcer » votre infrastructure informatique :

- Services de test de pénétration : pour évaluer l'efficacité de vos dispositions actuelles en matière de sécurité
- Services d'évaluation de la sécurité des applications : pour trouver les vulnérabilités logicielles... avant les cybercriminels
- Formation avancée sur la cybersécurité : pour former vos propres experts et à créer votre propre centre de sécurité
- Rapports de veille stratégique et rapports personnalisés sur les menaces : pour être constamment informé de l'évolution des menaces
- Portail Threat Lookup : pour accéder à la base de données mondiale de Kaspersky Lab dans le cadre de votre recherche de programmes malveillants

La stratégie de sécurité évolutive de Kaspersky Lab repose sur l'architecture de sécurité la plus viable qui soit, telle que décrite par Gartner. Kaspersky Lab propose un cycle d'activités centré sur quatre domaines : Prévenir, Détecter, Répondre et Anticiper. Concrètement, cela suppose que les systèmes de prévention traditionnels fonctionnent de pair avec les technologies de détection, les analyses de menaces, les capacités de réponse et les techniques de sécurité prédictives. Il est ainsi possible de créer un système de cybersécurité qui s'adapte en continu aux défis émergents et y fait face.

La stratégie de sécurité avancée de Kaspersky Lab offre :

1. Le remplacement d'un modèle de sécurité réactif au profit d'un modèle proactif fondé sur la gestion des risques, une surveillance en continu, une réponse aux incidents plus éclairée et des capacités de recherche des menaces.
2. Un cadre opérationnel qui rationalise les processus de sécurité quotidiens et renforce l'efficacité des mesures à travers un modèle multiniveaux permettant de prévenir et de détecter les menaces avancées à chaque étape d'une attaque.
3. Une seule plate-forme intégrée réduisant le nombre d'alertes de sécurité pour soulager les équipes grâce aux informations sur les menaces et à la hiérarchisation des alertes ; cela améliore en outre les réponses tactiques grâce au partage des connaissances sur les menaces, à une expertise approfondie et à la veille stratégique.
4. Une meilleure visibilité sur les différentes étapes d'une attaque, selon une approche unifiée ; il est ainsi possible d'analyser les menaces en toute transparence et d'enquêter sur les menaces connues et inconnues avant qu'elles ne frappent.
5. Grâce au partage d'informations sur les menaces mondiales (via les portails de surveillance des APT et autres menaces), vous bénéficiez de renseignements proactifs sur les mobiles et les intentions de vos adversaires, ce qui vous permet de hiérarchiser vos politiques et vos plans d'investissement.

Un monde d'expertise en technologies Kaspersky Lab

L'efficacité des produits Kaspersky Lab est régulièrement prouvée par les résultats de tests indépendants. En 2016, la société est arrivée en tête du top 3 des fabricants de solutions de sécurité. Selon les résultats de 78 tests différents réalisés par des organismes réputés dans plusieurs pays, les solutions Kaspersky Lab figurent dans le top 3 de 90 % des tests et arrivent en tête à 55 occasions. C'est une preuve indéniable que Kaspersky Lab fournit la meilleure protection du secteur.

Une solution éprouvée contre les menaces avancées

La plate-forme Kaspersky Anti Targeted Attack a réussi le test indépendant de l'institut ICSA Labs. Ce test, rarement exécuté, porte sur l'efficacité des solutions spécialisées qui protègent contre les menaces avancées et ciblées.

Pendant les 33 jours du test, des serveurs simulant l'infrastructure d'une entreprise protégée par la plate-forme Kaspersky Anti Targeted Attack ont subi pas moins de 550 attaques au total. Le scénario comprenait en outre l'envoi de 377 « échantillons propres » à un réseau protégé, c'est-à-dire des objets bénins, mais susceptibles d'être considérés comme malveillants. D'après l'institut ICSA Labs, les attaques incluaient des objets malveillants nouveaux et peu connus, dont ceux non détectés par les solutions de prévention traditionnelles lors du test.

Au total, la plate-forme Kaspersky Anti Targeted Attack est parvenue à détecter 99,44 % des attaques simulées (n'en manquant que trois), et seul un faux positif relatif à un objet bénin a été enregistré. La solution de Kaspersky Lab a répondu à l'ensemble des exigences de l'ICSA Labs et a reçu la certification de l'institut de recherche.

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

Une approche visionnaire et complète

Depuis plusieurs années, le Groupe Radicati réalise une analyse indépendante du marché des fournisseurs de solutions contre les APT afin de les classer en quatre catégories : les leaders (Top Players), les pionniers (Trail Blazers), les spécialistes (Specialists) et les acteurs matures (Mature Players). D'après les résultats fraîchement publiés, l'approche de Kaspersky Lab pour lutter contre les attaques ciblées et les menaces avancées a reçu d'excellentes appréciations.

En 2017, la plate-forme Kaspersky Anti Targeted Attack a considérablement progressé, passant de la catégorie des spécialistes à celle des pionniers.

Les pionniers proposent des technologies avancées et de référence pour certaines de leurs solutions, mais n'offrent pas nécessairement toutes les caractéristiques et les fonctionnalités qui distinguent les leaders. Ils sont cependant susceptibles de « bouleverser » le marché avec des technologies ou modèles de livraison innovants. Avec le temps, ces fournisseurs ont de fortes chances de compter parmi les leaders.

« La plate-forme Kaspersky Anti Targeted Attack permet de détecter les menaces avancées et les attaques ciblées à tous les niveaux : infection initiale, communications de commande et de contrôle, mouvements latéraux et exfiltration de données. »

Solutions de sécurité Kaspersky Lab
pour les entreprises :
https://www.kaspersky.fr/enterprise-security
Actualités des cybermenaces : **www.viruslist.fr**
Actualités de la sécurité informatique :
business.kaspersky.com/

#truecybersecurity
#HuMachine

www.kaspersky.fr