KASPERSKY lab

LE POUVOIR DE PROTÉGER

RISQUES DE DEMAIN : PRÉPAREZ-VOUS AUJOURD'HUI

Rapport spécial sur les stratégies d'atténuation des menaces avancées

http://www.kaspersky.fr/entreprise-securite-it/
#EnterpriseSec

SOMMAIRE

MENACES PERSISTANTES AVANCÉES DANS LE CONTEXTE ACTUEL

La cyber-sécurité est tout sauf un jeu de hasard. Sachant qu'une seule intrusion suffit pour infliger de sérieux dégâts à votre entreprise, une protection contre la majorité des attaques ne suffit pas.

C'est pourquoi il est préférable de focaliser notre attention sur les menaces les plus dangereuses et non sur les menaces les plus fréquentes.

L'« écosystème » des programmes malveillants est composé de menaces **connues** (70 %), de menaces **inconnues** (29 %) et de menaces **sophistiquées** (1 %).

Les menaces connues, qui représentent environ 70 % des programmes malveillants, sont relativement simples à contrer. À partir du moment où le code malveillant est reconnu, il est possible de le bloquer : les méthodes classiques basées sur les signatures permettent généralement de faire face à ce type de menaces.

Il y a ensuite 29 % des programmes malveillants qui entrent dans la catégorie des menaces inconnues. Combattre ces menaces exige des outils plus sophistiqués. Mais à l'aide de méthodes plus poussées que ce que proposent les anti-virus classiques, notamment les technologies d'analyse heuristique et de liste blanche dynamique, nous pouvons également contrer ce type de menaces.

Enfin, il y a les 1 % restants : les menaces sophistiquées, qui sont des attaques multiformes, continues et ciblées. Conçues pour s'introduire sur un réseau, rester invisibles et collecter des données sensibles, une fois en place, les menaces persistantes avancées (ou APT pour Advanced Persistent Threats) peuvent rester des années sans être détectées.

Une APT baptisée « Darkhotel » a utilisé le réseau wifi d'hôtels de luxe pour voler des données aux clients de ces hôtels pendant sept ans avant d'être découverte. Cette campagne d'espionnage était particulièrement intéressante, car elle était extrêmement ciblée (elle visait des dirigeants d'entreprise) et offrait une parfaite illustration des problématiques de sécurité informatique qui se posent lorsque les terminaux (ordinateurs portables et tablettes de l'entreprise) quittent le périmètre de sécurité de l'entreprise.

Une APT baptisée « Darkhotel » a utilisé le réseau wifi d'hôtels de luxe pour voler des données aux clients de ces hôtels pendant sept ans avant d'être découverte.

Bien que des entreprises très connues aient été victimes d'APT, il n'est pas nécessaire d'être exposé publiquement pour être dans le viseur des cyber-criminels. Les entreprises doivent être capables d'atténuer le risque que posent les APT et les conséquences qui peuvent découler d'une attaque, qu'il s'agisse d'une perte de données, d'une interruption d'activité prolongée ou d'une grave atteinte à leur réputation. Le mode opératoire des APT étant généralement silencieux et furtif, mieux vaut prévenir l'attaque plutôt que d'avoir à réparer les dégâts une fois le mal fait (car l'attaque a pu se produire plusieurs mois ou années auparavant et avoir fait des dégâts considérables).

Ce problème appelle plusieurs solutions. Les technologies utilisées pour combattre les menaces connues et inconnues sont certes utiles, mais sont inadaptées pour lutter seules contre les APT. Face à des menaces de plus en plus sophistiquées et complexes, il est nécessaire d'adopter une approche de sécurité multi-niveaux, dans laquelle plusieurs technologies intégrées sont combinées pour garantir une détection et une protection complètes contre les programmes malveillants connus, inconnus et sophistiqués et autres menaces.

L'objectif de ce rapport est de vous aider à être mieux préparé face aux APT.

Le coût moyen d'un incident causé par un programme malveillant est de 56 000 dollars pour une PME et 649 000 dollars pour une grande entreprise.[1]

Les APT peuvent avoir de graves conséquences. En 2014, Kaspersky Lab a contribué à la découverte de l'attaque Carbanak et de son fonctionnement. Cette attaque complexe a permis à un groupe international de cyber-criminels de dérober un milliard de dollars à plusieurs établissements bancaires. Le groupe a infecté le réseau d'une banque, a enregistré toutes les activités affichées sur les écrans des employés et a ainsi réussi à transférer de l'argent sans être détecté.

[1] Le coût élevé d'une violation de la sécurité, Kaspersky Lab.

L'ENTREPRISE COMME CIBLE : 5 POINTS IMPORTANTS

De par sa grande traille, vous êtes au courant des menaces de sécurité informatique qui pèsent sur votre entreprise. Il faut savoir que ces menaces sont de plus en plus ciblées et sophistiquées.

1 Avant même d'élaborer une stratégie appropriée pour lutter contre les APT, vous devez comprendre une chose : vous êtes une cible potentielle. Comme toutes les organisations, votre entreprise détient des informations dont les cyber-criminels peuvent tirer profit, qu'il s'agisse de propriété intellectuelle, de coordonnées ou de données bancaires. Même dans le cas où vos données ne les intéresseraient pas, ils peuvent utiliser votre réseau pour atteindre vos partenaires ou vos clients (comme cela a été le cas avec Darkhotel).

2 Nous devons ensuite renforcer la sensibilisation en matière de vulnérabilités. Dans les entreprises où un grand nombre d'employés travaillent sur plusieurs appareils, applications et plateformes, il peut être difficile de rester au fait de tous les risques et vecteurs d'attaque potentiels exploitables par les cyber-criminels. Les APT ciblent les vulnérabilités, humaines ou techniques. De ce fait, plus une entreprise est grande et complexe, plus il existe de points d'entrée possibles.

3 La montée du BYOD et de la flexibilité du travail complique encore un peu plus la situation. En plus d'être vulnérables en soi, les téléphones et tablettes sont souvent utilisés pour établir une connexion sur des réseaux non sécurisés. Et pour ne rien arranger, il est souvent plus difficile, en particulier sous certains systèmes d'exploitation comme l'iOS d'Apple, de dire si un appareil est infecté. Les collaborateurs en déplacement sont comme une cible mouvante. Les appareils utilisés en dehors du périmètre de sécurité de votre entreprise sont plus difficiles à surveiller. Votre stratégie sécuritaire doit donc impérativement inclure une protection efficace des terminaux.

4 Face à la diversification des terminaux et des méthodes utilisées par les cyber-criminels pour infecter un réseau, les mesures de sécurité spécifiques ne suffisent pas. Il faut au contraire de solides mesures d'atténuation combinant une veille des menaces, des politiques de sécurité et des technologies spécialisées qui, en plus de bloquer les menaces entrantes, repéreront les nouvelles, tout en utilisant des mesures telles que la liste blanche pour empêcher l'exécution de menaces encore inconnues.

5 Les efforts d'atténuation doivent se recentrer sur le terminal. Les cyber-criminels exploitent les vulnérabilités. Or, c'est souvent au niveau de ses terminaux que l'entreprise est la plus vulnérable : là où la sécurité est souvent compromise en raison de l'appareil en lui-même, mais aussi par laxisme de la part de l'employé ou en raison de l'environnement non sécurisé dans lequel il est utilisé. Si vos terminaux ne disposent pas d'une protection multi-niveaux, alors l'entreprise tout entière peut être exposée.

POURQUOI L'ATTÉNUATION EST-ELLE NÉCESSAIRE ?

L'atténuation est la base même de toute stratégie de sécurité pour les entreprises, la prévention étant bien plus efficace et économique que les mesures correctives après une attaque.

Les cyber-criminels qui développent les APT sont des experts déterminés et bien documentés. Toutefois, comme tous les cyber-criminels (à quelques exceptions près), ils choisiront toujours la solution la plus simple. C'est pourquoi, même s'il est impossible d'immuniser complètement votre entreprise contre les APT, vous pouvez mettre en place des mesures pour réduire les chances de succès d'une attaque.

Les APT étant souvent des menaces multi-niveaux, une réponse efficace contre les APT doit elle aussi être multi-niveaux. Les outils de sécurité basiques ne sont tout simplement pas suffisants.

Alors, à quoi ressemble cette approche ? L'Australian Signals Directorate, un service de renseignements australien, a créé ce que Kaspersky Lab considère comme une liste étendue et exhaustive des stratégies pour atténuer les menaces avancées. Nous pensons que ces stratégies conçues à l'échelle d'un pays peuvent sans problème être appliquées au niveau de l'entreprise et représentent un point de départ intéressant.

Ces stratégies regroupent quatre catégories principales :

1 POLITIQUES DE SÉCURITÉ ET SENSIBILISATION

La sécurité informatique ne repose pas uniquement sur l'informatique. L'erreur humaine est une aubaine pour les cyber-criminels. Les formations complètes et régulières sur les questions de sécurité, la valorisation des bons comportements et la mise en place de politiques pertinentes et concrètes sont autant de clés pour réduire le risque que vos employés laissent des cyber-menaces s'introduire dans votre entreprise.

2 SÉCURITÉ DU RÉSEAU

La structure de votre réseau peut considérablement influer sur l'impact potentiel d'une infection. Il existe plusieurs stratégies de sécurité réseau capables de réduire les risques et d'atténuer les menaces, par exemple, le fait d'isoler certaines sections du réseau pour réduire le nombre de terminaux pouvant accéder à des données sensibles, ce qui réduit de manière exponentielle le niveau de risque.

3 ADMINISTRATION SYSTÈME

Contrôler et restreindre les privilèges d'administration des utilisateurs par le biais de politiques de sécurité permet de réduire de façon significative le nombre de vulnérabilités que vous avez à gérer. De plus, le simple fait d'utiliser les fonctions de sécurité intégrées aux programmes que vous utilisez a toute son importance. En désactivant des fonctions superflues, vous pouvez optimiser les performances de vos logiciels et bloquer des axes d'exploitation potentiels.

Désactiver l'exécution du code Java dans votre navigateur est un parfait exemple de ce que vous pouvez faire pour éliminer certaines vulnérabilités présentes sur les ressources que vos collaborateurs utilisent.

4 SOLUTIONS DE SÉCURITÉ SPÉCIALISÉES

Les fonctions spécifiques des logiciels spécialisés sont autant de couches de protection indispensables. Mais l'intégration de ces solutions ne doit pas être synonyme d'investissements faramineux ou de centaines d'heures de main-d'œuvre. En fait, les trois solutions de sécurité spécialisées ci-dessous, associées à des droits d'administration restreints (selon la stratégie d'administration système décrite ci-dessus) permettent d'atténuer de 85 % les menaces de sécurité. Voici les trois solutions de sécurité spécialisées en question :

- Utiliser le contrôle des applications, la liste blanche et le mode de blocage par défaut
- Corriger les applications les plus souvent attaquées
- Corriger les vulnérabilités dans les systèmes d'exploitation

PRINCIPALES STRATÉGIES D'ATTÉNUATION

Il existe plusieurs stratégies d'atténuation que toute entreprise devrait avoir déjà mises en place ou du moins envisagées.

CONTRÔLE DES APPLICATIONS ET LISTE BLANCHE

La liste blanche est un outil puissant capable d'atténuer considérablement les APT et autres attaques. Plutôt que de lister les applications pouvant être dangereuses, cette technologie permet de lister les applications certifiées fiables. L'administrateur peut ainsi reprendre la main, quel que soit le comportement des utilisateurs. Une liste blanche est créée pour les applications connues et fiables et seules les applications de cette liste sont autorisées. Les programmes malveillants se manifestent souvent sous la forme d'un fichier exécutable quelconque. Avec cette approche, celui-ci sera bloqué. Il s'agit de l'approche opposée à l'utilisation traditionnelle de listes noires antivirus qui empêchent l'exécution d'une application si celle-ci figure déjà dans la liste des sources d'attaque connues.

Poussée à l'extrême, la liste blanche permet aux administrateurs de configurer un scénario de blocage par défaut, où seules les applications qu'ils ont pré-approuvées peuvent être exécutées, ce qui réduit massivement l'exposition aux risques. Si cette solution est efficace pour empêcher l'introduction de programmes malveillants sur votre réseau, vous devez toutefois veiller à ne pas bloquer des outils dont vos collègues auront réellement besoin pour travailler plus efficacement. Avec une plus grande granularité des contrôles des applications et une liste blanche dynamique, vous avez davantage d'outils de contrôle à votre disposition. Vous pouvez bloquer ou contrôler l'utilisation des applications par catégorie de logiciels, unité commerciale, utilisateur individuel et autres critères.

Bien entendu, avant de tirer efficacement parti d'une liste blanche, vous devez savoir quelles applications sont déjà exécutées sur vos machines. Car comment contrôler ce dont vous ignorez l'existence ? Il est donc indispensable de procéder à un inventaire.

POINT FORT DE KASPERSKY LAB : CONTRÔLE DES APPLICATIONS AVEC LISTE BLANCHE DYNAMIQUE

La base de données de Kaspersky Lab recensant sur liste blanche dynamique les applications légitimes contient bien plus d'un milliard de références et notamment 97,5 % des logiciels utilisés dans les entreprises. Grâce à notre veille des menaces, cette base de données est constamment mise à jour par Kaspersky Security Network via le cloud.

Notre contrôle des applications offre bien plus que la simple fonction « marche/arrêt ». En cas de blocage d'une application, tous les éléments non modifiés du système d'exploitation continuent de s'exécuter normalement. Vous pouvez donc contrer les attaques sans perturber les activités de vos utilisateurs. Kaspersky Lab simplifie également la mise en œuvre d'un mode de blocage par défaut : un mode test permet en effet d'anticiper les éventuelles complications de mise en route.

POINTS FORTS DE KASPERSKY LAB : GESTION DES VULNÉRABILITÉS ET GESTION DES CORRECTIFS

La base de données utilisée par notre technologie pour rechercher les vulnérabilités est vaste : Kaspersky Endpoint Protection for Business cherche et installe automatiquement les mises à jour Microsoft ainsi que les mises à jour (nouvelles versions) des applications autres que Microsoft. En d'autres termes, toutes vos applications et tous vos systèmes d'exploitation sont maintenus à jour, sans nécessiter des heures précieuses de main-d'œuvre.

« Avec le mode de blocage par défaut, seuls les programmes fiables sont autorisés à être exécutés sur votre ordinateur et croyez-moi, la grande majorité des programmes malveillants utilisés dans les attaques APT proviennent d'applications non fiables ou non corrigées. »

Costin Raiu, Director of Global Research and Analysis Team, Kaspersky Lab.

CORRIGER LES VULNÉRABILITÉS DES APPLICATIONS ET DES SYSTÈMES D'EXPLOITATION

Les applications comme les systèmes d'exploitation contiennent des vulnérabilités qui peuvent être exploitées par les cyber-criminels. Il est important de surveiller de près ces failles de sécurité et de les colmater avant qu'un code malveillant ne puisse y être introduit. Et ce sont les applications les plus utilisées qui contiennent souvent des vulnérabilités lorsque les correctifs ne sont pas installés.

Les outils de gestion des correctifs sont une composante clé de la sécurité informatique multi-niveaux, car ils permettent de mettre à jour automatiquement les applications sur l'ensemble des terminaux. Les éventuels points d'entrée d'une attaque sont ainsi fermés dans les plus brefs délais.

Encore une fois, nous insistons sur le fait qu'il n'existe aucune protection infaillible contre les APT.

Mais, mises en œuvre correctement et conjointement, les quatre stratégies décrites ici (privilèges d'administration, contrôle des applications, gestion des correctifs et gestion des systèmes d'exploitation) peuvent vous protéger contre 85 % des incidents liés à des attaques ciblées. Un code malveillant aura ainsi plus de difficultés à s'exécuter ou à le faire sans être détecté. La force de ces stratégies est de permettre une défense sur plusieurs fronts.

En 2014, des vulnérabilités dans Java d'Oracle, les navigateurs les plus utilisés et Adobe Reader ont représenté 92 % des failles de sécurité exploitées par des programmes malveillants.[2]

[2] Bulletin Kaspersky 2014 sur la sécurité, Kaspersky Lab

AUTRES STRATÉGIES TRÈS EFFICACES

Comme nous l'avons indiqué en introduction, la cyber-sécurité n'est pas un jeu de hasard. Même si les meilleures stratégies d'atténuation que nous venons de passer en revue vous protégeront contre la majorité des intrusions, vous devez encore et toujours aller plus loin.

Voici quelques techniques supplémentaires permettant de renforcer votre défense multi-niveaux :

ATTÉNUATION DES VULNÉRABILITÉS DES SYSTÈMES D'EXPLOITATION

Les technologies natives peuvent certes réduire nettement les vulnérabilités génériques des systèmes d'exploitation, mais les solutions spécialisées vous permettent d'aller encore plus loin. Et il est nécessaire d'aller plus loin. Car même si vous installez constamment les correctifs des applications et systèmes d'exploitation, vous êtes toujours potentiellement exposé à une attaque utilisant une vulnérabilité zero-day.

POINT FORT DE KASPERSKY LAB : AUTOMATIC EXPLOIT PREVENTION (AEP)

La fonction AEP (Automatic Exploit Prevention) effectue une série de vérifications de sécurité et s'attarde en particulier sur les programmes fréquemment ciblés comme Internet Explorer, Microsoft Office et Adobe Reader. Elle contrôle en permanence les processus en mémoire et est capable de discerner les comportements suspects caractéristiques de l'exploitation des failles (Exploits), qui sont beaucoup moins nombreux que les failles elles-mêmes. Cette approche permet à l'AEP de Kaspersky Lab de contrer les vulnérabilités zero-day.[3]

[3] D'après le test indépendant de MRG Effitas, la fonction AEP a protégé les terminaux testés contre des attaques de type 'Exploits' dans 95 % des cas, alors que l'ensemble des autres mécanismes de défense était désactivé.

C'est pourquoi il est important d'avoir une solution qui repère et neutralise les menaces connues d'un côté et détecte les anomalies et comportements suspects de l'autre, afin de vous protéger également des menaces inconnues. Vous pouvez ainsi vous défendre contre des attaques qui n'ont encore jamais été observées.

HOST-BASED INTRUSION PREVENTION

Comme nous l'avons vu, les APT sont des programmes malveillants sournois, capables de rester cachés pendant des mois, voire des années. Installer un périmètre de défense ne suffit pas puisque le code malveillant rôde peut-être déjà dans votre entreprise. Ce dont vous avez besoin, c'est d'une technologie qui reconnaît et bloque les activités applicatives considérées comme trop risquées, même si leur nature malveillante n'est pas avérée. Les systèmes de prévention d'intrusion sur les postes de travail (HIPS) limitent les activités applicatives dans le système en fonction de leur niveau de fiabilité. HIPS repère les anomalies d'exécution, c'est-à-dire des applications effectuant des fonctions ou des activités qui sortent du contexte et laissent supposer un risque. Le résultat est encore plus probant lorsque l'analyse est faite juste après l'installation de l'application, avant que celle-ci ait pu être corrompue par un programme malveillant furtif.

POINTS FORTS DE KASPERSKY LAB : SURVEILLANCE DES SYSTÈMES ET CONTRÔLE DES PRIVILÈGES DES APPLICATIONS

Avec ces deux fonctions, les événements qui se produisent à l'intérieur de vos systèmes informatiques peuvent être surveillés et enregistrés, afin de vérifier que les applications ne tentent pas d'effectuer des actions malveillantes. La fonction de surveillance des systèmes (System Watcher), avec son sous-système de restauration, est capable d'annuler les modifications indésirables. Quant au contrôle des privilèges, il empêche que de telles modifications se produisent si elles sont initiées par des applications dont le niveau de fiabilité est faible.

ANALYSE DYNAMIQUE DU CONTENU DES E-MAILS ET PAGES WEB

Tout comme l'approche basée sur les signatures ne peut rien contre une attaque zero-day, l'analyse statique traditionnelle, qui consiste à comparer le contenu des e-mails et pages Web à une base de données de programmes malveillants connus, ne vous protège pas contre les nouvelles menaces.

C'est en cela que l'analyse dynamique est très importante. Il vous faut une solution capable de repérer les caractéristiques suspectes encodées dans les e-mails et pages Web (par exemple, le fait qu'un programme cherche à modifier des exécutables) et de les bloquer avant leur ouverture.

Une attaque zero-day est une attaque ciblant une vulnérabilité encore non identifiée dans le système d'exploitation ou l'application, avant qu'un correctif puisse être proposé.

POINTS FORTS DE KASPERSKY LAB : FILTRAGE DE CONTENU ET ANTIVIRUS INTERNET

Notre technologie de filtrage de contenu vous permet de décider d'autoriser ou non les utilisateurs à accéder à certains sites, à la fois par utilisateur et par catégorie de sites Web (site de jeux, par exemple). Le trafic HTTP(S) est contrôlé, ce qui vous permet d'être certain que les ressources Web auxquelles les utilisateurs accèdent depuis leurs terminaux figurent bien sur votre liste blanche.

Dans le même temps, notre Antivirus Internet utilise une analyse dynamique pour repérer le code malveillant transmis par protocoles HTTP(S) et FTP, ce qui vous protège des APT utilisant les téléchargements ou les infections « drive-by » pour s'introduire dans un système.

POINTS FORTS DE KASPERSKY LAB : ANTIVIRUS COURRIER ET PROTECTION DES SERVEURS DE MESSAGERIE

S'appuyant sur des méthodes heuristiques et des analyses dynamiques et statiques, Kaspersky Endpoint Security for Business contribue à bloquer les menaces transmises par e-mail. En simulant la manière dont les pièces jointes peuvent se comporter, notre technologie est capable de détecter les vulnérabilités présentes dans les fichiers joints aux e-mails.

Kaspersky Security for Mail Server, avec son option de prévention des pertes de données (DLP), permet également d'empêcher la fuite de données sensibles. Vous pouvez rendre vos fichiers « non partageables » pour être certain qu'ils ne quitteront pas l'entreprise avec les pièces jointes de vos e-mails.

L'APPROCHE DE KASPERSKY LAB : UNE PROTECTION MULTI-NIVEAUX

Le paysage des menaces de sécurité est un paysage complexe qui évolue rapidement. Chez Kaspersky Lab, nous travaillons avec de grandes entreprises à la mise en œuvre d'une stratégie multi-niveaux, qui va de l'atténuation aux services de veille des menaces.

En tant qu'entreprise axée sur les technologies, nous avons mis au point pour vous des outils utiles pour élaborer une stratégie d'atténuation globale. Et parce qu'ils sont tous conçus à partir de la même base de code, ils s'intègrent parfaitement les uns aux autres et garantissent une armure sans point faible et une stratégie de sécurité complète.

Notre approche repose sur notre technologie primée de protection contre les programmes malveillants et notre pare-feu au niveau des terminaux. Combinées, ces deux technologies bloquent les menaces **connues**, soit 70 % du paysage des menaces. Ensuite, des outils plus **avancés**, comme les analyses comportementales et heuristiques, le contrôle des applications avec liste blanche dynamique et le filtrage de contenu, permettent de vous protéger des menaces **inconnues**. Enfin, pour les menaces sophistiquées, nous rajoutons encore une autre couche de protection avec l'utilisation d'outils évolués tels que Kaspersky Automatic Exploit Prevention et System Watcher.

VEILLE ET DÉTECTION : IDENTIFIER RAPIDEMENT LES ATTAQUES « EN DIRECT »

Une approche complète de l'atténuation est certes vitale, mais votre stratégie pour contrer les APT doit également inclure des mesures permettant de détecter les attaques « en direct », sans pour autant provoquer de fausses alertes, synonymes de perte de temps. En outre, votre stratégie doit inclure des technologies capables de bloquer rapidement une attaque et minimiser les dégâts pour votre entreprise.

L'approche que nous vous recommandons inclut une détection au niveau des terminaux, une détection au niveau du réseau, un sandboxing intelligent et une base de données complète sur l'historique des événements.

Récemment, plusieurs fournisseurs informatiques se sont intéressés à la question de la détection au niveau du réseau et beaucoup ont développé des dispositifs dédiés à cet objectif. Nous penchons néanmoins pour une autre solution, une solution qui utilise une architecture distribuée à sondes et qui offre des avantages significatifs. Le fait de placer des sondes sur les points stratégiques du réseau (sondes qui envoient les données vers un point central) permet d'améliorer la détection. De plus, cela permet une meilleure évolutivité et contribue à réduire les coûts de protection des réseaux d'entreprises complexes.

LA TECHNOLOGIE MAIS PAS QUE : SERVICES DE VEILLE DES MENACES

Même si la mise en place d'une stratégie d'atténuation réduira très nettement les risques pour votre entreprise, aucune solution de sécurité ne peut vous protéger à 100 %.

En cas d'attaque réussie, votre entreprise devra :

- Déterminer avec précision quelles données ont été volées, afin de prendre les mesures nécessaires pour limiter les dommages liés à cette perte de données
- Déterminer ce qui a permis de mener à bien cette attaque, afin de corriger les vulnérabilités et failles de sécurité en question

Il est donc important d'avoir à disposition les meilleures analyses criminalistiques, afin d'accéder sans délai à l'expertise en sécurité nécessaire.

Kaspersky Lab propose plusieurs services de veille des menaces. À vous de choisir le niveau de services qui convient le mieux à votre entreprise :

- Analyse des programmes malveillants : pour les clients qui disposent en interne d'une équipe d'analyse criminalistique
- Services d'analyse criminalistique des systèmes numériques, incluant l'analyse des programmes malveillants
- Services complets de réponse aux incidents, incluant des services d'analyse criminalistique

POURQUOI KASPERSKY LAB ?

Kaspersky Lab fait partie des entreprises en premières lignes dans la lutte contre les menaces persistantes avancées. Notre équipe GReAT (Global Research and Analysis Team) a contribué à la découverte de nombreuses menaces parmi les plus dangereuses et complexes au monde, notamment l'opération Red October ou plus récemment les agissements du groupe de cyber-espionnage « Equation Group ».

Pour les cyber-criminels, l'échelle n'est malheureusement pas vraiment un problème. Une fois que des cyber-armes évoluées sont mises au point, les groupes criminels n'ont aucun mal à les adapter à des cibles plus petites comme les entreprises. En d'autres termes, même les armes développées en secret et à grands frais par certains pays peuvent finir entre les mains de ces groupes.

Nous en sommes conscients. C'est pourquoi nous cherchons à redéfinir les règles du jeu. Nous utilisons les informations collectées lors des investigations des APT pour conseiller les gouvernements dans leur manière de se défendre contre les cyber-attaques. Mais ce n'est pas tout. Nous exploitons tous les enseignements tirés de ce travail pour concevoir des solutions à la fois efficaces et pragmatiques pour les entreprises.

Dans cette optique, nous combinons notre veille de sécurité inégalée à notre innovation technologique. Nous sommes les seuls sur le marché à affecter un pourcentage aussi important de nos effectifs à la recherche et au développement.

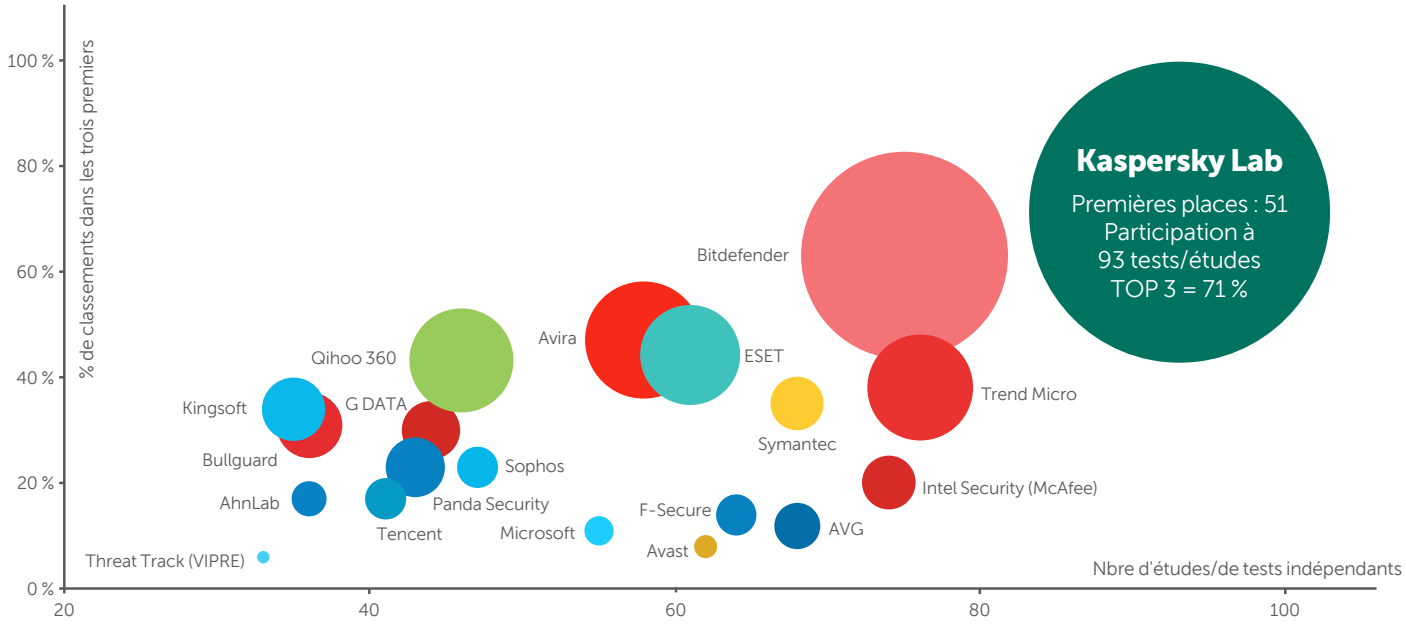
Le résultat est une vision multi-niveaux de la sécurité des entreprises, qui peut servir de trame à toute entreprise cherchant à mettre en œuvre une stratégie d'atténuation pour contrer les APT.

Parce que nous avons confiance en nos solutions, nous avons participé à plus de tests indépendants que n'importe quel autre fournisseur. Nous avons atteint des taux de détection de programmes malveillants de plus de 99 % et, parmi les 93 tests indépendants auxquels nous nous sommes soumis en 2014, nous avons fini 66 fois dans les trois premiers et 51 fois premiers[4] – des résultats bien supérieurs à ceux de nos concurrents. En outre, plus de 130 partenaires OEM nous font confiance et utilisent la technologie de Kaspersky Lab, ce qui veut dire que vous bénéficiez peut-être déjà du pouvoir de protection de Kaspersky Lab sans le savoir.

[4] http://media.kaspersky.com/en/business-security/TOP3_2014.pdf

KASPERSKY LAB : MEILLEURE PROTECTION DU MARCHÉ*

En 2014, Kaspersky Lab a participé à 93 études et tests indépendants. Nos produits ont reçu 51 premiers prix et ont figuré 66 fois parmi les trois premiers.



* Remarques :
D'après le résultat synthétisé d'un test indépendant réalisé en 2014 pour les produits d'entreprise, grand public et mobiles

Le résultat inclut des tests effectués par les laboratoires et magazines de tests indépendants suivants :
AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, VirusBulletin
La taille de la bulle représente le nombre de premières places

SÉCURISER L'AVENIR EN PROTÉGEANT LES INFRASTRUCTURES ACTUELLES

Dans un contexte où les menaces sont de plus en plus sophistiquées et complexes, une plateforme de sécurité multi-niveaux protégeant contre les menaces connues, inconnues et sophistiquées devient indispensable.

Rendez-vous sur **http://www.kaspersky.fr/entreprise-securite-it** pour en savoir plus sur l'expertise unique de Kaspersky Lab et sur ses solutions de sécurité destinées aux entreprises

EN SAVOIR PLUS

RETROUVEZ-NOUS SUR LES RÉSEAUX SOCIAUX

#EnterpriseSec

Visionnez nos vidéos sur YouTube

Rejoignez nos fans sur Facebook

Suivez-nous sur Twitter

Retrouvez-nous sur LinkedIn

Découvrez notre blog > https://business.kaspersky.com

Rejoignez-nous sur Threatpost

Retrouvez-nous sur Securelist

À PROPOS DE KASPERSKY LAB

Kaspersky Lab est le plus grand éditeur privé mondial de solutions de protection des terminaux. La société fait partie des quatre principaux éditeurs mondiaux de solutions de sécurité pour utilisateurs de terminaux informatiques*. Depuis plus de 17 ans, Kaspersky Lab fait figure de précurseur dans le domaine de la sécurité informatique, fournissant des solutions de sécurité numérique efficaces aux grandes entreprises, PME et particuliers. Kaspersky Lab, dont la holding est enregistrée au Royaume-Uni, opère actuellement dans près de 200 pays et territoires du monde entier et offre une protection à plus de 400 millions d'utilisateurs. Plus d'informations sur www.kaspersky.com.

* L'entreprise est classée quatrième fournisseur mondial de solution de sécurité des terminaux, en termes de chiffre d'affaires, par IDC en 2013. Ce classement a été publié dans le rapport IDC « Worldwide Endpoint Security 2014-2018 Forecast and 2013 Vendor Shares » (Sécurité des terminaux dans le monde : prévisions pour 2014-2018 et parts de marché des fournisseurs en 2013), document numéro 250210, août 2014. Ce rapport classait les éditeurs de logiciels selon leurs revenus provenant des ventes de solutions de sécurité des terminaux en 2013.