KASPERSKY ENDPOINT SECURITY FOR BUSINESS : LA TECHNOLOGIE À L'ŒUVRE

Pour les menaces visibles comme invisibles

KASPERSKY lab

LE POUVOIR
DE PROTÉGER

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

#Securebiz

SOMMAIRE

94 % des entreprises ont subi une menace extérieure

Source : Enquête 2014 sur les risques informatiques au niveau mondial de Kaspersky Lab

PROTÉGEZ VOTRE ENTREPRISE DES MENACES VISIBLES COMME INVISIBLES

Il n'a jamais été aussi important de se doter des solutions de sécurité informatique adéquates.

CE QUI PEUT VOUS PORTER PRÉJUDICE SANS QUE VOUS LE SACHIEZ

Plus de 30 % des failles de sécurité surviennent dans des entreprises employant 100 personnes ou moins.[1] 44 % des petites et moyennes entreprises (PME) ont été attaquées par des cyber-criminels.[2]

Cependant, beaucoup ignorent les véritables menaces que représentent la cyber-criminalité et les programmes malveillants sophistiqués. Si à peine moins d'un cinquième des petites entreprises admettent qu'elles n'ont pris aucune mesure pour se protéger contre la cyber-criminalité, seules 60 % mettent leur logiciel de lutte contre les programmes malveillants à jour.[3]

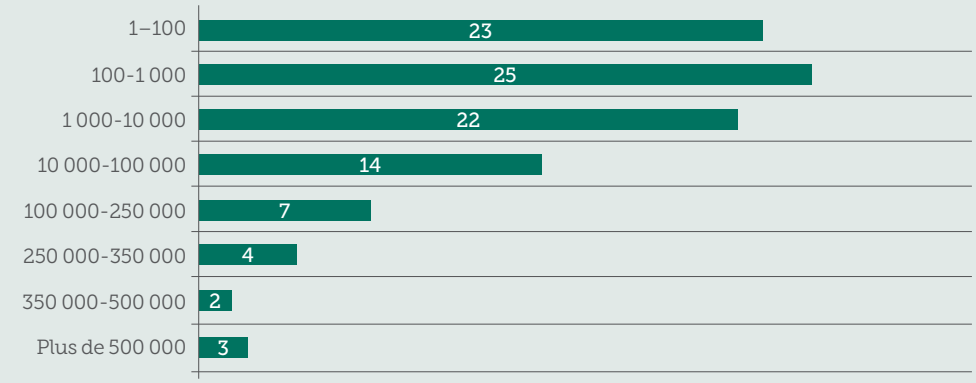
Vous pensez que vous êtes trop petit pour être intéressant ? C'est exactement la mentalité qu'exploitent les cyber-criminels pour lancer des programmes malveillants de plus en plus sophistiqués contre votre entreprise. Ils savent ce que de nombreuses PME ne savent pas : vous êtes une cible.

[1] Rapport 2013 d'enquêtes sur la violation des données de Verizon
[2] Enquête 2013 de l'Association nationale des petites entreprises
[3] Kaspersky Lab, Threatpost, 24 mai 2013

CE QUE VOUS NE POUVEZ PAS VOIR

Supposons que vous faites partie des 80 % de PME équipées d'une solution de sécurité informatique. Ne soyez pas trop insouciant pour autant : la plupart des utilisateurs en entreprise sous-estiment gravement le nombre de menaces.[4] Seules quatre pour cent des entreprises ayant répondu à l'enquête ont deviné le nombre approximatif de menaces détectées chaque jour.[4]

NOMBRE PERÇU DE NOUVEAUX ÉCHANTILLONS DE PROGRAMMES MALVEILLANTS DÉCOUVERTS CHAQUE JOUR (%)



Source : Enquête 2014 sur les risques informatiques au niveau mondial de Kaspersky Lab

Dans ce contexte, il n'est pas vraiment surprenant que certains utilisateurs considèrent la sécurité informatique comme un « produit de base », voyant peu la différence entre les différentes options disponibles. Il s'agit d'un dangereux mythe ; même une différence d'un pour cent dans les taux de détection peut représenter des centaines de milliers de programmes malveillants passant entre les mailles du filet au cours d'une année. Comment pouvons-nous le savoir ?

- Kaspersky Lab détecte 325 000 nouveaux programmes malveillants chaque jour.
- Au deuxième trimestre 2014, nos solutions de lutte contre les programmes malveillants ont détecté 528 799 591 attaques de virus sur les systèmes d'utilisateurs finaux, identifiant un total de 114 984 065 objets malveillants uniques.[5]

Les menaces les plus sérieuses sont celles que vous ne connaissez pas – des menaces que les experts de Kaspersky Lab suivent, analysent et atténuent chaque jour. Nous cherchons les anomalies. Et quand nous les trouvons, nos dix années d'expérience et de savoir-faire en surveillance des menaces nous permettent de fournir à votre entreprise une protection supplémentaire contre les menaces qu'elle doit à tout prix éviter, c'est-à-dire en particulier les programmes malveillants sophistiqués et les menaces persistantes sophistiquées (Advanced Persistent Threats, APT).

L'écart entre l'idée que ce font les entreprises du panorama des menaces et sa réalité ne cesse de se creuser. Nous avons baptisé ce phénomène « le décalage d'impression ». Il montre que les entreprises de toutes tailles sous-estiment largement tant la quantité que la gravité des menaces qui pèsent sur elles.

Costin Raiu, Global Research & Analysis Team, Kaspersky Lab

[4] Kaspersky Lab – Rapport 2014 sur les risques informatiques mondiaux
[5] Kaspersky Lab – Rapport 2014 sur l'évolution des menaces au 2e trimestre

PROACTIF, RÉACTIF, INTELLIGENT

Kaspersky Lab a depuis longtemps la réputation de savoir identifier les menaces les plus graves, parmi lesquelles Carbanak (auteur du plus important vol de données bancaires au monde), Dark Hotel, The Mask, Icefog et Red October. Plus d'un tiers de nos employés travaillent en Recherche et développement. Ils s'occupent uniquement du développement de technologies visant à contrer et anticiper les menaces en constante évolution sur lesquelles nos équipes de chercheurs enquêtent au quotidien.

Kaspersky Lab a pu, grâce à notre compréhension du fonctionnement interne d'attaques parmi les plus sophistiquées au monde, développer une plate-forme multi-niveaux de technologies de sécurité qui vous protège contre les menaces connues, inconnues et avancées. Nos technologies détectent et atténuent les menaces visibles comme invisibles.

Toutes les technologies de lutte contre les programmes malveillants et de détection des menaces de Kaspersky Lab fonctionnent ensemble, de façon simultanée, dès qu'un fichier est téléchargé. Cette combinaison unique de technologies reposant sur la veille permet une détection et une prévention multi-niveaux sur l'ensemble des terminaux et d'autres éléments d'infrastructure informatique.

DÉTECTER LES MENACES CONNUES

Lorsqu'un fichier va être téléchargé, une page Web ou une application ouverte, les moteurs avancés de Kaspersky Lab contre les programmes malveillants vérifient, détectent et protègent simultanément contre les virus connus, inconnus et avancés ; qu'ils soient sur Internet ou la messagerie, qu'il s'agisse de chevaux de Troie, rootkits, vers informatiques, logiciels espions, scripts, adwares et autres objets malveillants et menaces connus. Pour les menaces connues d'abord, ces moteurs reposent sur les éléments suivants :

BLOCAGE DES ATTAQUES RÉSEAU

Analyse l'ensemble du trafic réseau, à l'aide de signatures connues pour détecter et bloquer les attaques réseau, notamment le balayage des ports, les attaques par déni de service, les attaques par dépassement de la mémoire tampon ou toute autre activité malveillante à distance.

FILTRAGE DES URL

Analyse et compare les URL, dans le trafic entrant et sortant, à la base de données Kaspersky Lab de programmes malveillants et de sites de phishing et bloque les attaques en ligne, les logiciels malveillants polymorphes côté serveur et les serveurs « de commande et de contrôle » (C&C).

LISTE NOIRE

Des équipes d'analystes de programmes malveillants maintiennent les bases de données de Kaspersky Lab à jour avec les dernières signatures et données de programmes malveillants. Ces données et signatures servent à bloquer automatiquement tous les programmes malveillants connus.

PARE-FEU

Analyse chaque paquet qui entre ou sort du réseau en le bloquant ou l'autorisant, selon le risque de sécurité. Les connexions non autorisées sont détectées, ce qui réduit la zone d'attaque potentielle et les possibilités d'infection. Les machines infectées ou compromises voient leur activité réseau limitée, ce qui réduit leur capacité à diffuser des programmes malveillants et limite les dégâts causés par les violations des politiques de sécurité.

Les technologies de Kaspersky Lab basées sur des signatures bénéficient d'années de connaissances et d'expériences accumulées. Toutes ces technologies excellent dans le blocage des programmes malveillants connus (et grâce à Kaspersky Security Network, comme nous allons le voir plus loin, la plupart des menaces restent inconnues pendant très peu de temps). Mais qu'en est-il des menaces inconnues furtives ou avancées dont nous avons parlé ? Pour ces menaces aussi, nous avons la solution...

[6] La technologie de protection contre les messages indésirables de Kaspersky Lab a été classée au premier rang du VB Spam Test en novembre 2014, avec un taux de détection de 99,75 % et aucun faux positif.

DÉTECTER LES MENACES INCONNUES

Dès lors qu'un fichier est passé par les procédures de contrôle basées sur des signatures pour les menaces connues, que se passe-t-il lorsque l'on tente de l'ouvrir ? Les technologies proactives multi-niveaux de Kaspersky Lab analysent et vérifient les fichiers qui s'exécutent, à la recherche des activités suspectes ou malveillantes qui laissent présager une menace inconnue.

LISTE BLANCHE

L'analyse heuristique fournit une protection proactive contre les menaces qui ne peuvent être détectées à l'aide des bases de données antivirus habituelles. Les méthodes heuristiques de Kaspersky Lab permettent de détecter les nouveaux programmes malveillants ou des modifications inconnues sur des programmes malveillants connus. L'analyse statique recherche dans le code des signes de commandes suspectes associés à des programmes malveillants, et l'analyse dynamique examine le code machine que le fichier pourrait tenter d'exécuter, répondant à des simulations d'« appels » avec des « réponses » probables afin de déterminer si le code est sûr.

PROTECTION CONTRE LE PHISHING HEURISTIQUE

Pour les toutes nouvelles attaques de phishing n'ayant touché qu'un petit nombre d'utilisateurs, la technologie de Kaspersky Lab peut rechercher des preuves supplémentaires d'activité suspecte, telles que le vocabulaire employé, les formulaires de saisie ou les séquences de symboles illisibles. Cela vient s'ajouter à l'approche plus traditionnelle fondée sur les bases de données décrites plus haut.

Le phishing est le point de départ des dernières menaces avancées, particulièrement dangereuses.

HOST INTRUSION PREVENTION SYSTEM (HIPS – SYSTÈME DE PRÉVENTION DES INTRUSIONS DE L'HÔTE)

Le HIPS de Kaspersky Lab ajoute une couche de protection en détectant et gérant les applications et activités suspectes, et en empêchant les menaces de s'exécuter. Le HIPS permet de contrôler le comportement des applications par la définition de niveaux de confiance au terme de l'analyse initiale. Ces niveaux déterminent les ressources à utiliser, le type de données accessibles ou modifiables, etc. Ils interdisent l'exécution de programmes potentiellement dangereux sans affecter les performances des applications autorisées et sûres. Une application non fiable ne sera pas autorisée à faire quoi que ce soit, y compris à s'exécuter.

CONTRÔLE DES APPLICATIONS ET LISTE BLANCHE

Le contrôle des applications bloque ou autorise les applications déterminées par l'administrateur. L'approche de Kaspersky Lab s'appuie sur des listes blanches dynamiques : des listes continuellement mises à jour d'applications fiables et de catégories de logiciels autorisés à s'exécuter uniquement selon des règles et politiques spécifiques. Kaspersky Lab dispose d'un laboratoire dédié aux listes blanches et d'une base de données de plus d'un milliard de fichiers, qui s'alimente d'un million d'éléments supplémentaires chaque jour.

Le contrôle des applications et la liste blanche atténuent les risques présentés par les menaces que nous ne connaissons pas encore : la plupart des programmes malveillants prennent en effet la forme d'un fichier exécutable que l'on ne trouve dans aucune liste blanche. Les organisations qui adoptent cette approche (et les technologies qui l'accompagnent) peuvent donc empêcher tout fichier malveillant de s'exécuter, sans avoir besoin d'identifier ou de savoir ce que sont vraiment ces fichiers.

KASPERSKY SECURITY NETWORK

En tant que laboratoire de recherche de menaces basé sur le cloud, Kaspersky Security Network détecte, analyse et gère les menaces connues, inconnues et nouvelles, ainsi que les sources d'attaque en ligne en quelques secondes et intègre ces informations directement dans les systèmes des clients.

À l'aide de données en temps réel anonymisées provenant de 60 millions de capteurs placés sur des terminaux partout dans le monde, chaque fichier passant par les systèmes protégés de Kaspersky Lab est analysé en fonction des informations issues de la surveillance des menaces. Ces mêmes données garantissent que la mesure la plus appropriée est prise : en travaillant avec tous les autres composants du moteur de Kaspersky Lab, Kaspersky Security Network assure la protection contre les menaces inconnues avant la mise à disposition des signatures. Les réponses traditionnelles à base de signatures peuvent prendre plusieurs heures. Kaspersky Security Network n'a besoin que de 40 secondes.

DÉTECTER LES MENACES AVANCÉES

Votre fichier a été téléchargé et ouvert, les technologies Kaspersky Lab l'ont analysé, examiné et l'ont bloqué ou autorisé, que les menaces soient connues ou inconnues.

Mais qu'en est-il des menaces avancées ?

Les technologies avancées de détection de Kaspersky Lab sont prévues pour détecter et bloquer les menaces avancées à l'aide d'une série de mécanismes comportementaux proactifs et sophistiqués qui surveillent le comportement des processus, distinguent les comportements suspects, bloquent les activités malveillantes et annulent les changements nocifs, y compris les crypteurs.

Étudions tout cela de plus près...

SYSTEM WATCHER

Ce système surveille et collecte les données sur les activités des applications et sur d'autres activités système importantes en utilisant l'historique des activités et en distinguant des schémas de comportement. Ces informations sont fournies aux autres composants de protection de Kaspersky Lab déjà présentés. Toute activité correspondant aux schémas de menaces est gérée conformément aux politiques définies par l'administrateur ou, par défaut, ferme le processus malveillant et le met en quarantaine pour analyse.

Le pilote qui intercepte les opérations sur les fichiers pour le composant anti-programmes malveillants de Kaspersky Lab rassemble également des informations sur les modifications appliquées au registre, tandis que le pare-feu rassemble des données sur l'activité réseau des applications. Toutes ces informations alimentent la fonction System Watcher qui, elle, dispose de son propre module capable de réagir aux événements complexes du système tels que l'installation des pilotes.

Les actions malveillantes et les schémas comportementaux destructeurs qui signalent la présence de programmes malveillants sont bloqués.

PRÉVENTION AUTOMATIQUE DE L'EXPLOITATION DES FAILLES (AEP)

Cette technologie cible spécifiquement les programmes malveillants qui exploitent les vulnérabilités logicielles. Développée grâce à une analyse approfondie des caractéristiques et comportements des failles les plus répandues, elle est capable d'identifier des schémas comportementaux typiques des failles et de les bloquer dès le démarrage.

AEP agit comme un filet de sécurité, une couche supplémentaire de sécurité qui complète les autres technologies de Kaspersky Lab. Elle fonctionne avec la fonction System Watcher de Kaspersky Lab.

ANNULATION

Cette surveillance permanente et en détail des systèmes garantit une restauration système exceptionnellement précise, en limitant l'impact des infections et en rétablissant les paramètres sécurisés antérieurs des systèmes. Les mécanismes de restauration peuvent être mis à jour et fonctionnent avec des fichiers exécutables créés et modifiés, des modifications MBR, des fichiers Windows volumineux et des clés de registre.

BLOCAGE PAR DÉFAUT

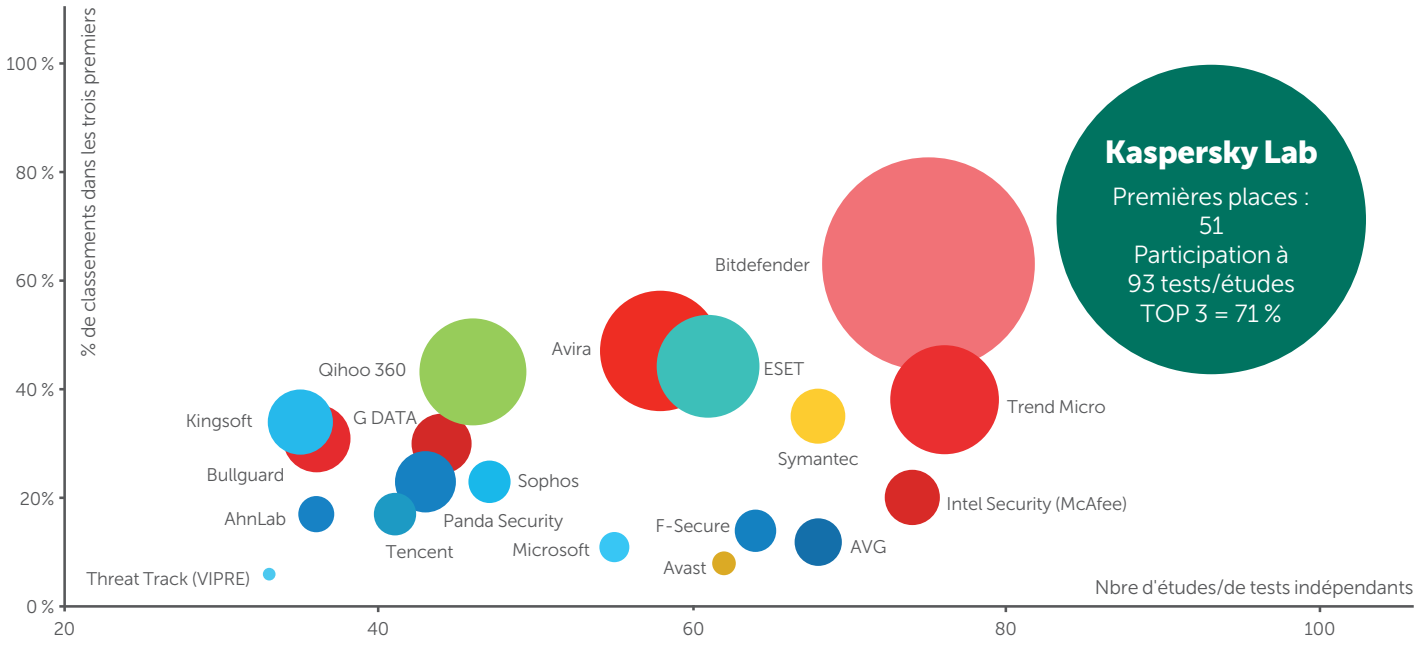
Cette mesure de sécurité est de plus en plus considérée comme la plus efficace face aux menaces avancées en constante évolution. Avec cette approche, l'exécution de toutes les applications est bloquée sur n'importe quel poste de travail. Seules les applications autorisées par l'administrateur peuvent être directement exécutées.

Le blocage par défaut implique que tous les différents programmes malveillants présents dans les fichiers sont automatiquement bloqués, même pour les attaques ciblées.

UN PETIT CHANGEMENT PEUT FAIRE TOUTE LA DIFFÉRENCE

Comme nous l'avons vu, même un seul pourcent supplémentaire dans le taux de détection peut se traduire par des centaines de milliers de programmes malveillants passant à travers les mailles du filet. Nous avons également vu comment les « filets » supplémentaires d'atténuation, de détection et d'analyse de Kaspersky Lab peuvent attraper des menaces inconnues voire avancées avant même qu'elles puissent agir.

KASPERSKY LAB : MEILLEURE PROTECTION DU MARCHÉ*



Les résultats des tests indépendants montrent sans équivoque que Kaspersky Lab fournit la meilleure protection du marché. Rien qu'en 2014, nous avons participé à 93 tests et examens indépendants, qui nous ont classé 51 fois au premier rang et dans le top 3 71 % du temps, un record. Ce n'est que l'une des raisons pour lesquelles les OEM (parmi lesquelles Microsoft, Cisco Meraki, Juniper Networks et Alcatel Lucent) font confiance à Kaspersky Lab pour leur fournir la sécurité qu'ils intègrent ensuite dans leurs propres produits.

Le développement et la maintenance de toutes les technologies de sécurité de Kaspersky Lab sont effectués en interne à partir de la même base de code, ce qui signifie qu'elles s'intègrent les unes aux autres en toute transparence, en constituant une plate-forme multi-niveaux complète. Ce niveau d'intégration se traduit également par de meilleures performances, des mises à jour plus rapides et une cohérence visuelle dans toutes les solutions, ce qui vous permet de vous concentrer sur votre cœur de métier, pendant que Kaspersky Lab s'occupe de la sécurité.

* 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 correspond au nombre de premières places.

N'ATTENDEZ PLUS : ESSAI GRATUIT DE 30 JOURS

Découvrez comment nos solutions de sécurité peuvent protéger votre entreprise des programmes malveillants et de la cyber-criminalité en les essayant gratuitement pendant un mois.

Rendez-vous dès aujourd'hui sur **http://www.kaspersky.fr/downloads/trials/business-trials** pour télécharger des versions complètes de nos produits et évaluer leur capacité à protéger parfaitement votre infrastructure informatique, vos terminaux et les données confidentielles de votre entreprise.

EFFECTUEZ UN ESSAI GRATUIT DÈS MAINTENANT

RETROUVEZ-NOUS SUR LES RÉSEAUX SOCIAUX

#Securebiz

Visionnez nos vidéos sur YouTube

Rejoignez nos fans sur Facebook

Suivez-nous sur Twitter

Retrouvez-nous sur LinkedIn

Retrouvez-nous sur Viruslist

Découvrez notre blog

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.fr.

* 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.

kaspersky.fr/
businesskaspersky.fr/
entreprise-securite-it
#Securebiz