LA PROTECTION DES ENTREPRISES S'ADAPTE

Le panorama des menaces actuel était inimaginable il y a dix ans. Les cybercriminels ont adapté leurs techniques pour contourner les défenses traditionnelles et passer inaperçus sur les systèmes pendant des mois ou même des années. Il est temps pour les systèmes de protection des entreprises de s'adapter en adoptant une approche intelligente de sécurité informatique multi-niveaux, basée sur la veille stratégique.

« L'intelligence, c'est la capacité de s'adapter au changement. »
– Stephen Hawking.

LA PROTECTION DES ENTREPRISES S'ADAPTE

Les menaces persistantes avancées (APT), les programmes malveillants sophistiqués et les attaques ciblées ne sont que quelques-unes des nouvelles menaces en constante évolution auxquelles les entreprises sont exposées. Les cybercriminels sont parfaitement conscients des limites des protections traditionnelles basées sur un périmètre de sécurité : c'est là qu'ils recherchent les failles dans l'armure de l'entreprise.

Les cybercriminels changent de forme en permanence, mais il serait honnête de préciser que certaines technologies pour les entreprises leur fournissent également des vecteurs d'attaque bien utiles : les appareils mobiles, les applications Web, les appareils de stockage amovibles, la virtualisation, les technologies basées sur le cloud offrent aux cybercriminels des opportunités auxquelles les protections traditionnelles de prévention et de blocage ne peuvent pas répondre à elles seules.

Une nouvelle approche intégrée et plus adaptable reposant sur quatre piliers (prévision, prévention, détection et réaction) est nécessaire.

LES QUATRE PILIERS DE LA PROTECTION D'ENTREPRISE ADAPTABLE

Prévision : personne ne peut voir l'avenir dans une boule de cristal, mais les entreprises ayant accès aux informations les plus récentes sur les menaces et les tendances sont mieux placées pour anticiper et éviter les incidents. La formation des employés à la reconnaissance des tactiques utilisées dans les attaques permet d'améliorer l'analyse prédictive, tout comme la capacité à apprendre de ses erreurs en effectuant une analyse du diagnostic des violations. Quant aux tests de pénétration, ils permettent de mettre à jour les points faibles.

Prévention : l'objectif clé consiste à réduire la surface d'attaque, qu'il s'agisse de programmes malveillants traditionnels basés sur les signatures, de contrôles de périphériques ou de correction des vulnérabilités des applications. Il convient pour cela de renforcer les systèmes et de placer autant d'obstacles que possible sur le chemin des cybercriminels, deux éléments d'une approche plus large qui vise notamment à limiter la capacité des attaques à se propager et à réduire leur impact.

Détection : comme le montrent les études de Kaspersky Lab sur les menaces APT, les attaques sophistiquées peuvent passer inaperçues pendant des années. On estime qu'une attaque sur une entreprise passe inaperçue pendant plus de 200 jours en moyenne[1]. Or, plus l'incident est découvert tôt, mieux c'est. Les technologies de détection qui sont complétées par une analyse des menaces performante améliorent l'identification : à l'heure où les menaces évoluent rapidement, la meilleure stratégie de détection repose souvent sur la capacité à déceler les comportements et séquences d'événements indiquant qu'une violation a eu lieu.

Réponse : une protection d'entreprise efficace est capable de réagir à une violation et d'en limiter les effets. À un premier niveau, cela peut passer par une politique d'action/réaction appliquée aux procédures qui peut être automatisée, tels que l'application de correctifs. À un autre niveau, cela peut passer par l'analyse post-violation ou le recours à des équipes spécialisées dans la réponse aux incidents dont la mission consiste à stopper, limiter et étudier les attaques, les violations et les autres incidents de sécurité.

Pour être véritablement efficaces, toutes ces capacités doivent s'associer en prenant la forme d'un système multi-niveaux. L'architecture de sécurité complète et adaptable d'une entreprise doit être basée sur la veille stratégique, axée sur les menaces, globale et centrée sur la stratégie. Kaspersky Lab est exceptionnellement bien placée pour fournir une plate-forme de sécurité d'entreprise adaptable. Voyons maintenant pourquoi.

[1] https://www.siliconrepublic.com/enterprise/2014/04/11/advanced-cyberattacks-can-go-undetected-for-typically-229-days

NOTRE EXPERTISE AU SERVICE DE VOTRE ENTREPRISE

Kaspersky Lab bénéficie d'une expérience de longue date dans l'identification de menaces sophistiquées, notamment les suivantes :

- Carbanak : le plus grand cyberbraquage de banque au monde
- Dark Hotel : qui cible les voyageurs d'affaires occupant des postes élevés
- The Mask/Careto : qui a ciblé des entreprises, des administrations et des fonds de placement privés, entre autres
- Wild Neutron : qui cible notamment des entreprises internationales
- Icefog : qui a attaqué la chaîne d'approvisionnement des entreprises
- Red October : qui a exploité des systèmes d'entreprise pour mener à bien des opérations massives de surveillance

Plus d'un tiers de nos employés travaillant dans la recherche et le développement se concentrent uniquement sur la conception de technologies visant à neutraliser et anticiper les menaces en constante évolution que les équipes dédiées de veille stratégique et d'analyse de Kaspersky Lab étudient au quotidien.

Kaspersky Lab a pu, grâce à notre compréhension du fonctionnement interne d'attaques extrêmement sophistiquées, développer un portefeuille stratégique multi-niveaux de technologies et services de sécurité 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 de réduction des menaces que n'importe quelle autre entreprise de sécurité informatique.

PRÉVISION

Les capacités de prévision et les stratégies de réduction qui sont construites autour d'elles sont au cœur de l'ensemble des activités de Kaspersky Lab, de notre équipe dédiée Global Research and Analysis Team (GReAT) jusqu'au Kaspersky Security Network (KSN) en passant par notre portefeuille de services de veille stratégique :

Kaspersky Security Network : élément majeur de la plate-forme multi-niveaux de Kaspersky Lab, Kaspersky Security Network est une architecture complexe basée dans le cloud dédiée au recueil et à l'analyse des informations sur les menaces provenant de millions de systèmes dans le monde.

En tant que laboratoire mondial de recherche de menaces basé sur le cloud, KSN détecte, analyse et gère les menaces inconnues ou avancées, ainsi que les sources d'attaque en ligne en quelques secondes et intègre ces informations directement dans les systèmes des clients. Pour les entreprises ayant des problèmes de confidentialité des données très spécifiques, Kaspersky Lab a développé l'option Kaspersky Private Security Network.

Services de veille stratégique : rares sont les organisations qui disposent des ressources nécessaires pour développer les niveaux élevés de veille stratégique requis pour suivre l'évolution constante des menaces sophistiquées. C'est pourquoi Kaspersky Lab a développé un vaste portefeuille de services de veille stratégique.

Sensibilisation et formation : des principes de base de la cybersécurité aux formations avancées sur le cyberdiagnostic, l'analyse des programmes malveillants et le reverse engineering, Kaspersky Lab fournit un ensemble complet de programmes de formation et de sensibilisation à destination des entreprises, sur site et en ligne. En plus des jeux interactifs, des évaluations des compétences et de la promotion de la cybersécurité, des cours de 2 à 5 jours abordant les sujets suivants sont disponibles :

- **Sensibilisation à la cybersécurité :** compréhension des menaces, utilisation de la technologie en toute sécurité.
- **Principes généraux du cyberdiagnostic :** mise en place d'un laboratoire de cyberdiagnostic, reconstruction des incidents, outils.
- **Analyse des programmes malveillants et reverse engineering :** création d'un environnement sécurisé d'analyse des programmes, analyse express.
- **Cyberdiagnostic avancé :** analyse approfondie des systèmes de fichiers, récupération des fichiers supprimés, reconstruction de la chronologie des incidents.
- **Analyse avancée des programmes malveillants et reverse engineering :** analyse des shellcodes, programmes malveillants autres que Windows, utilisation des bonnes pratiques mondiales.

Évaluation de la sécurité :

- **Tests de pénétration :** compréhension de la protection des infrastructures du point de vue du cybercriminel, tout en garantissant la conformité avec les normes de sécurité telles que la norme PCI DSS.
- **Tests de sécurité des applications :** analyse des applications Web (y compris les services bancaires en ligne et les applications où le WAF est activé), applications mobiles, clients lourds.

Surveillance des menaces :

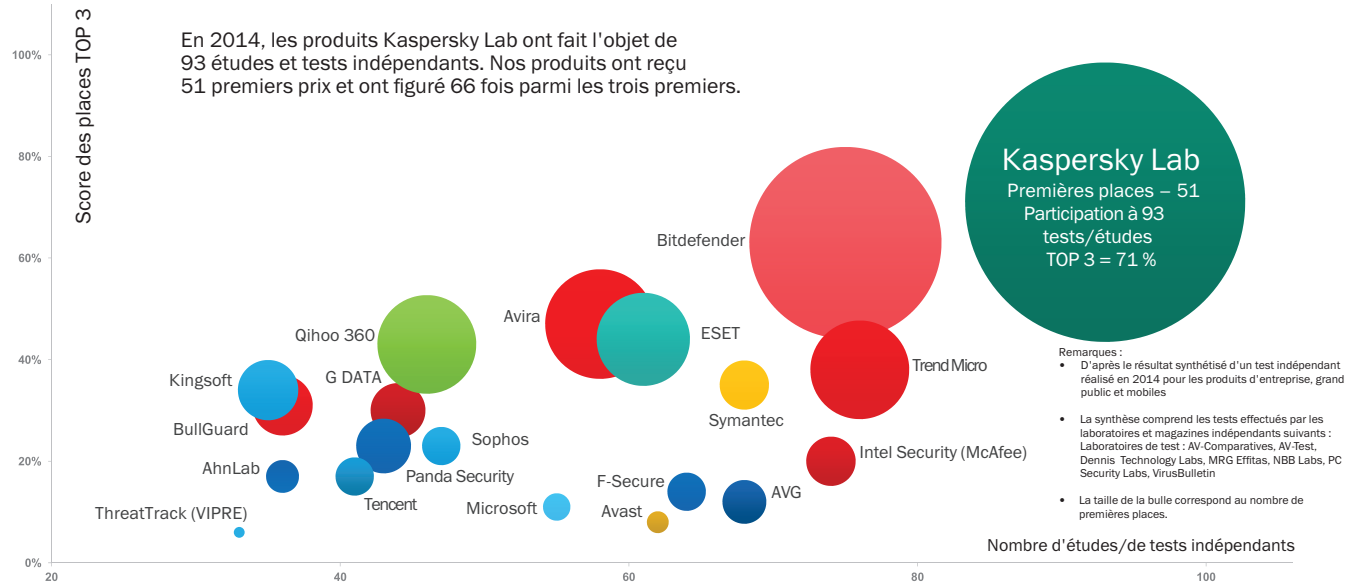
- Système d'alerte précoce, étayé par l'expertise de l'équipe GReAT et soutenu par KSN : flux d'informations sur les menaces, suivi d'activité des botnets et rapports de surveillance. L'accès rapide aux fichiers de configuration liés aux menaces APT et aux échantillons de programmes malveillants ainsi que l'intégration à SIEM (HP Arcsight) aident les entreprises à développer une vision complète des informations sur les menaces.

PRÉVENTION

Kaspersky Lab détecte 325 000 nouveaux programmes malveillants *chaque jour*. 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. 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 études indépendants, obtenant 51 fois la première place et figurant parmi les trois meilleurs dans 71 % des cas, un chiffre record.[2] Ce n'est que l'une des raisons pour lesquelles les OEM (parmi lesquels Microsoft, Cisco Meraki, Juniper Networks et Alcatel Lucent) font confiance à Kaspersky Lab pour leur fournir la sécurité qu'ils intègrent ensuite à leurs propres produits.

[2] Pour en savoir plus sur les tests et les indicateurs, consultez : http://media.kaspersky.com/en/business-security/TOP3_2013.pdf
Le nouveau lien du rapport actualisé est le suivant : http://media.kaspersky.com/en/business-security/TOP3_2014.pdf.

KASPERSKY LAB PROPOSE LA MEILLEURE PROTECTION DU SECTEUR*



Notre portefeuille de solutions de sécurité pour les entreprises associe des programmes de lutte contre les logiciels malveillants à plusieurs technologies pour réduire les surfaces d'attaque en offrant une combinaison unique de technologies axées sur la veille stratégique.

Les menaces connues, inconnues et avancées sont évitées à l'aide de plusieurs niveaux de protection, notamment les suivants :

Prévention des intrusions : analyse l'ensemble du trafic réseau à l'aide de signatures connues pour détecter et bloquer les attaques réseau, notamment le balayage des ports et les attaques par déni de service. Kaspersky DDoS Protection (KDP) est une solution qui apporte un niveau de protection supplémentaire contre les attaques par déni de service (DDoS). Il s'agit d'une solution complète et intégrée de prévention et de réduction des DDoS, qui intègre des analyses en continu et des rapports post-attaques.

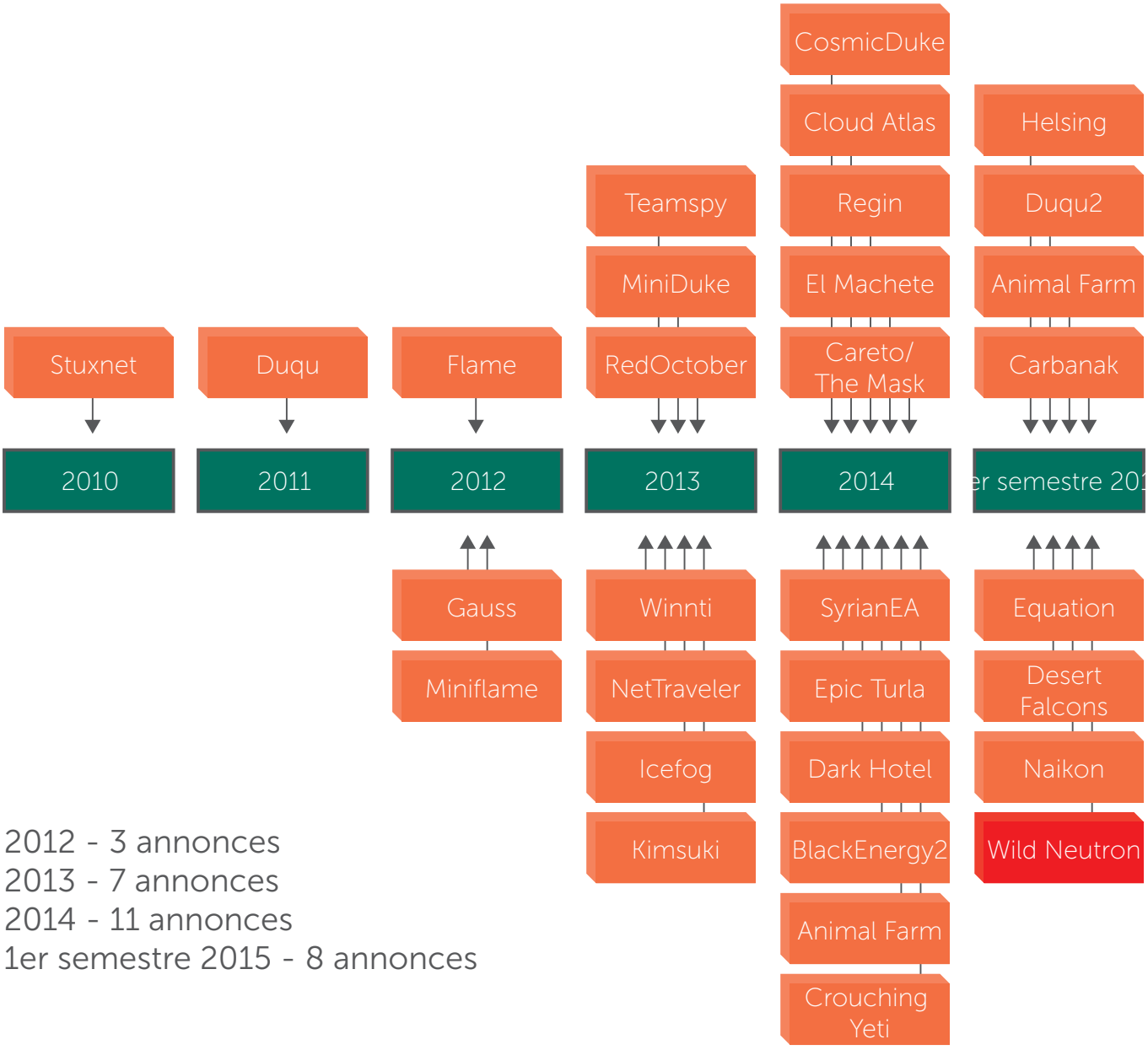
Protection contre le phishing heuristique : permet d'empêcher certaines des techniques d'attaques de phishing les plus récentes en recherchant des preuves supplémentaires d'activité suspecte. Cette technologie surpasse les approches traditionnelles axées sur les bases de données de phishing. Contrôle des applications et liste blanche dynamique : le contrôle des applications bloque ou autorise les applications déterminées par l'administrateur. Il repose sur la liste blanche dynamique, la liste de catégories de logiciels et d'applications de confiance actualisée en permanence par Kaspersky Lab.

HIPS – Système de prévention des intrusions de l'hôte : permet de contrôler le comportement des applications et de restreindre l'exécution de programmes potentiellement dangereux sans affecter les performances des applications sûres qui sont autorisées.

DÉTECTION

L'expertise inégalée de Kaspersky Lab en matière de détection des menaces les plus sophistiquées au monde alimente directement les capacités de détection des menaces de notre entreprise. Depuis 2008, nos chercheurs ont découvert quelques-unes des attaques multi-composants les plus sophistiquées jamais vues. Ces connaissances et ces informations sont directement appliquées au développement de nos produits. En plus de notre capacité à détecter des attaques sophistiquées ciblant les entreprises, Kaspersky Lab a utilisé les connaissances acquises en identifiant les auteurs de menaces financières d'envergure telles que Carbanak pour développer des solutions entièrement axées sur la détection de la fraude financière.

ANNONCES D'APT PAR KASPERSKY LAB



2012 - 3 annonces
2013 - 7 annonces
2014 - 11 annonces
1er semestre 2015 - 8 annonces

RÉACTION

Dans une architecture de sécurité adaptable, la capacité à réagir aux menaces est aussi importante que la capacité de prévision et de prévention de ces menaces, car elle permet à l'entreprise de réaliser à la fois des gains de temps et d'argent. Il convient également d'être conscient que l'optimisation de la détection a pour conséquence directe l'optimisation de la capacité de réaction. Kaspersky Lab relève ce défi aussi bien au niveau de la technologie que des services :

System Watcher : la technologie unique de surveillance proactive de Kaspersky Lab est capable de réagir aux événements système complexes tels que l'installation de pilotes et de détecter les comportements suspects.

Services d'investigation : permettent de résoudre les incidents de sécurité en direct avec l'aide de Kaspersky Lab. De l'analyse des programmes malveillants au cyberdiagnostic en passant par l'établissement de rapports et la réponse aux incidents, nos clients disposent des outils nécessaires pour tirer les enseignements des incidents tout en réduisant l'impact d'une attaque et en restaurant les systèmes endommagés.

UNE PROTECTION D'ENTREPRISE PROACTIVE, RÉACTIVE ET BASÉE SUR LA VEILLE STRATÉGIQUE

Dire que les programmes malveillants se sont multipliés est un euphémisme : les menaces avancées échappent aux techniques de blocage traditionnelles, des kits de programmes malveillants prêts à l'emploi sont en vente sur Internet pour trois fois rien et des outils capables de créer automatiquement plusieurs variantes personnalisées d'un programme malveillant ne sont que la partie émergée d'un immense iceberg de programmes malveillants.

Face à des menaces de plus en plus sophistiquées et complexes, il est nécessaire d'adopter une approche de sécurité multi-niveaux adaptable, dans laquelle plusieurs technologies intégrées sont combinées pour garantir une détection et une protection complètes contre les programmes malveillants connus, inconnus et sophistiqués et les autres menaces ciblant les entreprises.

L'expérience inégalée de Kaspersky Lab en matière d'identification des menaces les plus sophistiquées combinée à ses technologies et services de pointe nous permettent d'être particulièrement bien placés pour offrir la protection complète et adaptable dont les entreprises ont besoin. Tandis que Kaspersky Security Network s'appuie sur les informations en temps réel générées par plus de 60 millions de nœuds dans le monde entier, les membres de notre équipe d'experts Global Research and Analysis (GReAT) apportent un ensemble unique de compétences et d'expertise à nos recherches sur les menaces, en développant des solutions capables de lutter contre des menaces de plus en plus complexes et sophistiquées.

PARTENAIRE DE CONFIANCE DES ENTREPRISES, DES ADMINISTRATIONS ET DES RÉGULATEURS

En sa qualité de société privée, Kaspersky Lab est libre d'investir massivement dans la recherche et le développement, sans avoir à se préoccuper des contraintes à court terme du marché. Près de la moitié de nos 3 000 employés dans le monde travaillent dans nos laboratoires de recherche et de développement, où ils se concentrent sur la conception de technologies innovantes, l'étude des cyberguerres, du cyberespionnage et de tous les types de menaces et techniques.

Cet accent mis sur la R&D interne de qualité a permis à Kaspersky Lab d'être reconnu comme un leader dans le secteur des technologies de sécurité informatique. Ce n'est que l'une des raisons pour lesquelles plus de 100 grands OEM (parmi lesquels Microsoft, Cisco Meraki, IBM, Juniper Networks et Alcatel Lucent) font confiance à Kaspersky Lab pour leur fournir la sécurité qu'ils intègrent ensuite à leurs propres produits.

C'est aussi pour cela que nous sommes un partenaire de choix pour les administrations, les autorités de police et les grandes entreprises du monde entier. Des organismes internationaux respectés, dont INTERPOL, Europol et de nombreux CERT, ont fait de Kaspersky Lab un collaborateur et consultant permanent. En plus de dispenser régulièrement des formations aux employés d'INTERPOL et aux agents de police de nombreux pays, nous avons soutenu le lancement du laboratoire de cyberdiagnostic d'INTERPOL.


Twitter.com/
KasperskyFrance


Facebook.com/
KasperskyLabFrance


Youtube.com/
KasperskyFrance

Kaspersky Lab,
Moscou, Russie
www.kaspersky.fr

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

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

KASPERSKY lab