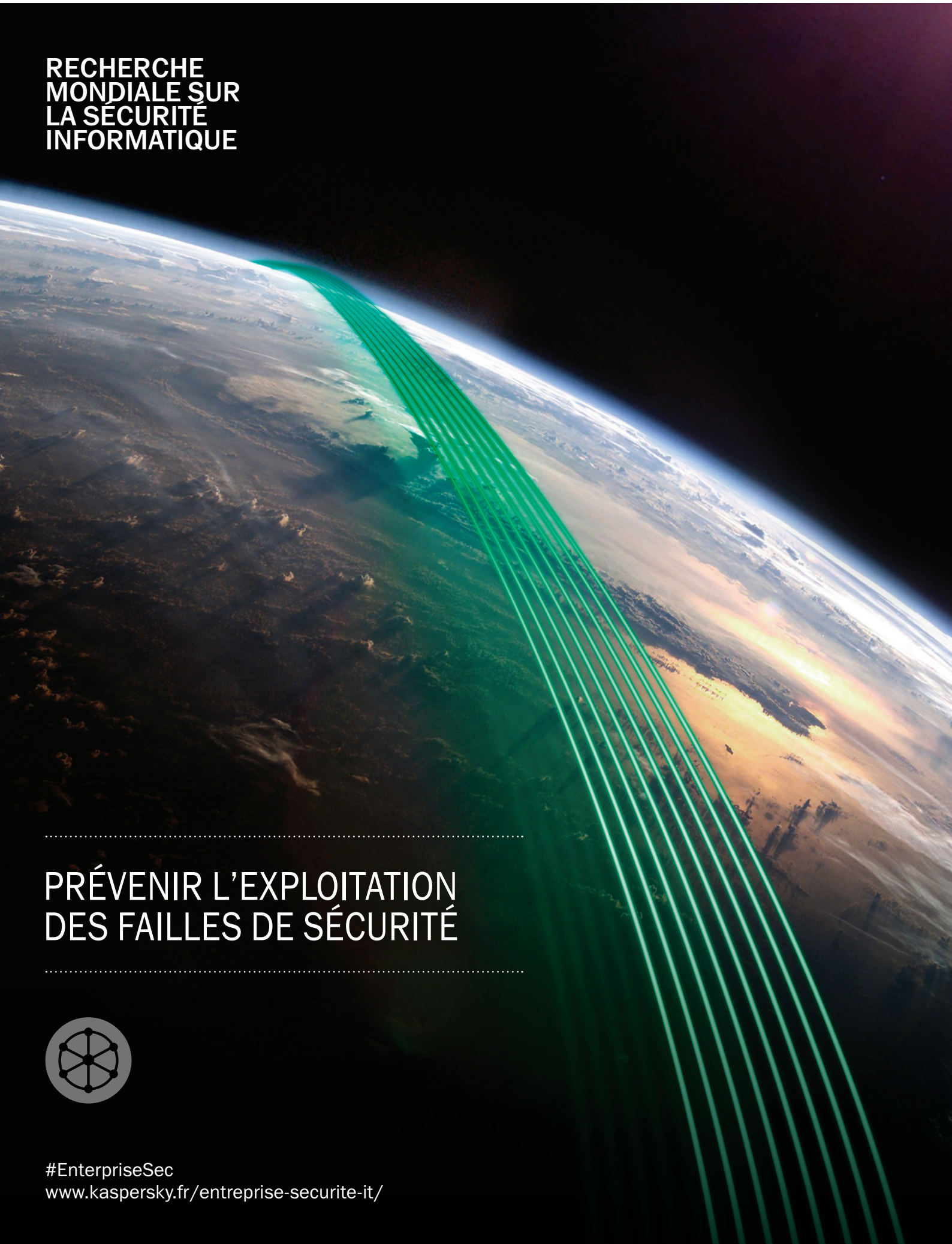
KASPERSKY lab

RECHERCHE MONDIALE SUR LA SÉCURITÉ INFORMATIQUE



PRÉVENIR L'EXPLOITATION DES FAILLES DE SÉCURITÉ

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

SOMMAIRE

LA NOUVELLE MENACE VENUE DE L'INTÉRIEUR

KASPERSKY LAB ESTIME QUE LA MEILLEURE FAÇON DE FAIRE FACE À CETTE MENACE, DONT L'ÉVOLUTION EST RAPIDE, CONSISTE À UTILISER UNE TECHNOLOGIE DÉDIÉE OFFRANT UNE COUCHE UNIQUE DE PROTECTION CONTRE L'EXPLOITATION DES FAILLES DE SÉCURITÉ DES APPLICATIONS LES PLUS POPULAIRES

En 2012, les applications tierces ont représenté 87 % des vulnérabilités.[1] Cette même année, Kaspersky Lab a enregistré plus de 132 millions d'applications courant un risque.

Les failles d'Oracle Java, d'Adobe Flash Player et d'Adobe Reader, ainsi que les faiblesses de Microsoft Office, sont les cibles préférées des criminels exploitant les failles de sécurité. Les chercheurs de Kaspersky Lab ont enregistré 8,54 millions d'attaques exploitant les failles de Java entre mars et août 2013, soit une augmentation de 52,7 % par rapport aux six mois précédents.

Kaspersky Lab estime que la meilleure façon de faire face à cette menace, dont l'évolution est rapide, est d'utiliser une technologie dédiée offrant une couche unique de protection contre l'exploitation des failles de sécurité des applications les plus populaires. En commençant par empêcher l'exécution de code malveillant, il est possible d'éviter que les applications et composants clés de l'entreprise ne fassent office de passerelle pour des attaques de plus grande envergure.

Notre couche de protection spécialisée trouve son origine dans une technologie développée par Kaspersky Lab appelée Prévention Automatique d'Exploitation des failles (AEP). Cette technologie permet de détecter et de protéger efficacement les systèmes et les données des entreprises contre l'exploitation de failles connues et inconnues.

1. Analyse des vulnérabilités de Secunia 2013, Secunia Research Lab, 14 mars 2013

LES PRINCIPALES FAILLES DE SÉCURITÉ POUR VOTRE ENTREPRISE

Le but de toute exploitation de faille de sécurité est de profiter des vulnérabilités des logiciels largement utilisés pour lancer divers types de codes malveillants. Les criminels se servent de diverses méthodes pour infecter un système à l'aide de cette technique, notamment :

- En attirant les internautes sur un site Web malveillant réalisé pour l'occasion ou un site Web légitime ayant été piraté et infecté par du code malveillant. Certains criminels ciblent des sites Web légitimes plébiscités par certains types d'internautes, par exemple les développeurs de grandes entreprises. Cette technique est appelée attaque de point d'eau (« watering hole attack »).
- En faisant télécharger ou ouvrir aux internautes un document spécialement conçu pour cet usage et paraissant (..) paraissant légitime. Il peut s'agir d'un document Office, d'un PDF, ou même d'une image apparemment inoffensive.
- Il est très facile d'introduire dans l'entreprise des supports de stockage amovibles (tels que des clés USB) sur lesquels se trouvent des programmes malveillants exploitant des failles. Plusieurs études récentes ont montré qu'après avoir trouvé une clé USB dans le parking de leur lieu de travail, les utilisateurs finaux la branchaient invariablement sur leur ordinateur, surtout si cette clé portait le logo de l'entreprise.[2]
- E-mails de phishing : ces attaques ciblées commencent généralement par un internaute ouvrant une pièce jointe malveillante spécialement conçue, semblant pourtant légitime au premier abord.
- Pour en savoir plus sur l'exploitation de failles ayant pour origine des supports amovibles : http://www.securelist.com/en/blog/208187475/Another_usb_media_infection

2. Bruce Schneier, « Yet Another "People Plug in Strange USB Sticks" Story » (Et encore une histoire de personnes qui branchent des clés USB suspectes), Schneier on Security

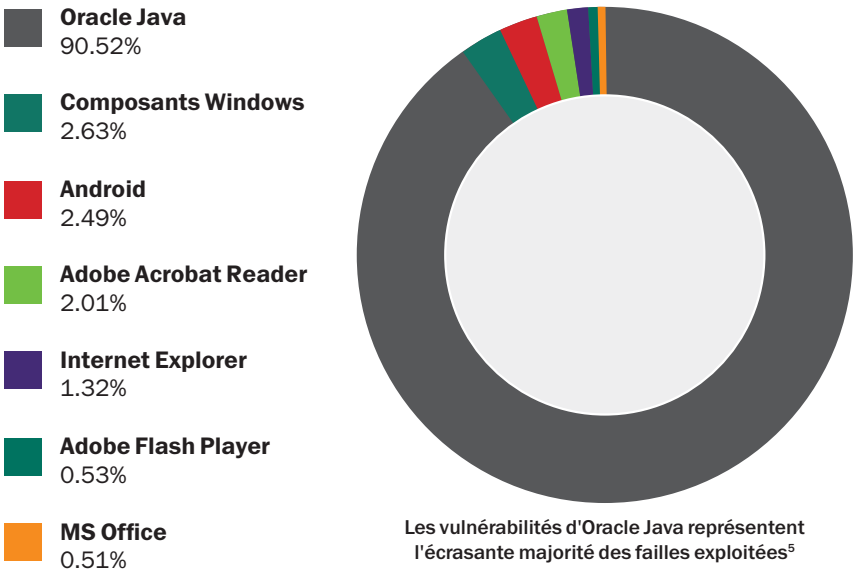
LA POPULARITÉ VOUS REND VULNÉRABLE : LES LOGICIELS LES PLUS ATTAQUÉS

6,3 % DES UTILISATEURS DE KASPERSKY LAB UTILISANT NOTRE SYSTÈME DE DÉTECTION DES MENACES BASÉ SUR LE CLOUD, KASPERSKY SECURITY NETWORK, UTILISENT TOUJOURS WINDOWS XP

Des bugs peuvent survenir dans le cadre de l'utilisation de presque n'importe quel programme, et certains d'entre eux permettent l'exécution non autorisée de code malveillant. Étant donné qu'en moyenne, environ 72 programmes sont installés sur l'ordinateur d'un utilisateur,[3] cela représente bon nombre de vulnérabilités dans l'entreprise. Mais en réalité, les criminels tendent à se focaliser sur les applications les plus utilisées, car cela leur assure un grand nombre de victimes potentielles. Après tout, il suffit d'un clic pour que l'attaque soit couronnée de succès.

Une étude de Kaspersky Lab indique qu'Oracle Java est le logiciel le plus ciblé par les exploitations de failles, représentant 90,52 % des tentatives d'exploitation des vulnérabilités en 2013. Ces vulnérabilités sont exploitées par des attaques éclair sur Internet. En outre, de nouvelles failles Java sont désormais incluses dans de nombreux packs d'exploitation.[4]

Les composants Windows représentent la seconde catégorie de vulnérabilités cibles préférées, notamment les fichiers de système d'exploitation Windows vulnérables, exception faite des fichiers Microsoft Office et Internet Explorer, que Kaspersky Lab a placés dans une catégorie à part. La plupart des attaques dont cette catégorie de composants est victime ciblent une vulnérabilité découverte dans le fichier win 32k.sys-CVE-2011-3402, utilisée pour la première fois dans le cadre de la fameuse faille d'exploitation Duqu.



Les vulnérabilités d'Oracle Java représentent l'écrasante majorité des failles exploitées[5]

Il n'est pas exclu que la liste de logiciels ciblés change au fil du temps. À titre d'exemple, Microsoft Office était la cible numéro un des attaques en 2010. Microsoft signant la fin du cycle de vie de Windows XP et d'Office 2003 à partir d'avril 2014, ce sera également la fin du développement de correctifs et de mises à jour de sécurité pour ces logiciels. Par conséquent, certaines organisations seront laissées pour compte avec de sérieuses faiblesses sur lesquelles les criminels lorgnent sans doute déjà. 6,3 % des utilisateurs de Kaspersky Lab utilisant notre système de détection des menaces basé sur le cloud, Kaspersky Security Network, utilisent toujours Windows XP.

3. Analyse des vulnérabilités de Secunia 2013
4. Rapport de Kaspersky Lab : Java Under Attack – The Evolution of Exploits in 2012-2013 (Les attaques contre Java : l'évolution des failles d'exploitation en 2012-2013), Securelist, 30 octobre 2013
5. http://www.securelist.com/en/images/vlill/stat_ksb_2013_04.png

MÉTHODES DE PROTECTION CONTRE L'EXPLOITATION DES FAILLES

MÊME SI LES MENACES PASSANT AU TRAVERS DES COUCHES DE SÉCURITÉ TRADITIONNELLES SONT PEU NOMBREUSES, IL PEUT S'AVÉRER VITAL D'AJOUTER UNE COUCHE DE SÉCURITÉ SUPPLÉMENTAIRE À L'ENTREPRISE, CAR L'EXPLOITATION D'UNE SEULE FAILLE PEUT PASSER AU TRAVERS DES MAILLES DU FILET ET CAUSER DE GROS DOMMAGES

Les solutions Kaspersky Lab utilisent plusieurs méthodes permettant de bloquer l'exploitation de failles. Par exemple, des signatures spéciales sont ajoutées aux programmes malveillants se servant de vulnérabilités, ce qui permet de détecter des fichiers malveillants (tels que des pièces jointes) avant même leur ouverture. La protection proactive, ainsi que d'autres technologies, permettent de détecter et de bloquer les programmes malveillants après l'ouverture d'un fichier vulnérable. Enfin, **l'analyse des vulnérabilités** permet de détecter facilement un logiciel vulnérable sur n'importe quel terminal. En outre, cette fonctionnalité est compatible avec la **gestion des correctifs** et d'autres fonctions de **gestion des systèmes**, ce qui permet d'appliquer automatiquement des mises à jour ou d'empêcher le chargement d'un logiciel non corrigé.

Bien entendu, la meilleure solution pour éviter la plupart des exploitations de failles consiste à régulièrement mettre à jour les composants systèmes de Windows et les autres logiciels installés.

Les techniques de protection au quotidien peuvent toutefois ne pas s'avérer efficaces dans certains cas. Cela est tout particulièrement vrai pour les vulnérabilités « zero-day » (failles logicielles non détectées ou tout récemment découvertes). Dans ce cas, les éditeurs de solutions de sécurité ont bien du mal à identifier les programmes malveillants ciblant les vulnérabilités « zero-day » à l'aide des méthodes utilisant des signatures. Des exploitations de failles complexes peuvent également utiliser diverses techniques pour contourner ou neutraliser les technologies de protection proactives. Même si les menaces passant au travers des couches de sécurité traditionnelles sont peu nombreuses, il peut s'avérer vital d'ajouter une couche de sécurité supplémentaire à l'entreprise, car l'exploitation d'une seule faille peut passer au travers des mailles du filet et causer de gros dommages. C'est là que la Prévention Automatique de l'Exploitation des failles (AEP) entre en scène.

PRÉVENTION AUTOMATIQUE DE L'EXPLOITATION DES FAILLES

La technologie de prévention automatique de l'exploitation des failles (AEP) cible tout particulièrement les programmes malveillants qui exploitent des vulnérabilités logicielles afin de s'implanter dans les réseaux et les terminaux de l'entreprise. La technologie AEP permet d'empêcher qu'un programme malveillant ne s'exécute, même si un utilisateur télécharge ou ouvre un fichier malveillant.

Kaspersky Lab a développé l'AEP en se fondant sur des analyses approfondies du comportement et des composants des exploitations de failles les plus répandues. Cela signifie que notre technologie peut détecter les comportements caractéristiques des exploitations de failles et les empêcher de se lancer.

Au cours de la phase de développement, les équipes R&D de Kaspersky Lab ont pris connaissance des logiciels et applications d'entreprise les plus fréquemment ciblés, ce qui leur a permis d'adapter la technologie AEP en conséquence. L'AEP fait désormais partie de l'antivirus et des solutions de sécurité Internet de Kaspersky Lab. La technologie AEP fonctionne en parallèle avec le module de **Surveillance du système** afin d'offrir une couche de sécurité supplémentaire présentant les fonctions suivantes :

CONTRÔLE DES APPLICATIONS POTENTIELLEMENT VULNÉRABLES

La technologie AEP se concentre tout particulièrement sur les applications les plus fréquemment ciblées, telles qu'Adobe Reader, Internet Explorer et Microsoft Office. Des contrôles de sécurité supplémentaires sont déployés dès que l'un de ces programmes tente d'exécuter un code ou un fichier exécutable inhabituel. Ces lancements seront parfois légitimes : par exemple, Adobe Reader peut lancer un fichier exécutable afin de rechercher des mises à jour. Certaines caractéristiques du fichier exécutable, ainsi que toute action qui y est associée, peuvent cependant indiquer la présence d'activité malveillante ce qui, par conséquent, rend l'examen supplémentaire nécessaire et utile.

SURVEILLANCE DES ACTIVITÉS ANTÉRIEURES AU LANCEMENT

La façon dont une application se lance ou un code s'exécute (ainsi que ce qu'il se passe juste avant) peut être révélatrice. Certains types de comportements indiquent clairement la présence d'activité malveillante. La technologie AEP peut tracer cette activité et identifier l'origine de la tentative de lancement du code. Elle peut provenir du logiciel lui-même, tout comme elle peut résulter de l'exploitation d'une faille de sécurité. Les données relatives aux comportements exploitations de failles les plus courantes permettent de détecter ce genre d'activité, même dans le cadre d'une vulnérabilité « zero-day ». Cela signifie que l'AEP n'a pas besoin de connaître la nature précise de la vulnérabilité exploitée pour déterminer la présence d'une activité malveillante.

LA MÉTHODOLOGIE D'ANALYSE ET DE SUIVI DE KASPERSKY LAB, AINSI QUE SES ÉTUDES APPROFONDIES ET CONTINUES SUR LES APPLICATIONS LES PLUS UTILISÉES EN ENTREPRISE, PERMETTENT DE FORTEMENT LIMITER LE NOMBRE DE FAUX POSITIFS

TRAÇABILITÉ DE L'ORIGINE DU CODE

Certains types d'exploitation de failles, notamment celles utilisées dans le cadre de « drive-by downloads » (exploitation de failles lancées via une page Web malveillante), doivent aller chercher leur charge sur un autre site Web avant de s'exécuter. L'AEP peut retracer l'origine de ces fichiers, identifier le navigateur précis qui a lancé le téléchargement et retrouver l'adresse Web distante des fichiers.

En outre, l'AEP peut, pour certains types de programmes, faire la distinction entre les fichiers générés avec le consentement de l'utilisateur et les nouveaux fichiers n'ayant pas reçu son autorisation. Lors d'une tentative de lancement d'un code suspect, ces informations peuvent permettre d'identifier exploitation de faille et de la bloquer.

BLOCAGE DE L'EXPLOITATION D'UNE VULNÉRABILITÉ CIBLE

L'AEP peut utiliser une technique appelée « Force Address Space Layout Randomization » (Forcer l'ASLR, qui est la distribution aléatoire de l'espace d'adressage) avec certains programmes et modules logiciels, empêchant le programme malveillant de trouver la vulnérabilité ou le code spécifique dont il a besoin pour s'exécuter.

La technologie ASLR a été incluse dans le système d'exploitation Windows de Microsoft depuis la version Vista. Cependant, certains programmes ne sont pas compatibles avec cette fonction par défaut. La technologie AEP de Kaspersky Lab étend la fonction d'ASLR aux programmes qui ne sont pas compatibles avec cette version par défaut, bloquant certains types d'exploitation de failles en les empêchant d'identifier l'emplacement du code dont elles ont besoin pour fonctionner (dans la mémoire par exemple). Il est plus probable que leurs efforts répétés visant à identifier l'emplacement du code nécessaire se traduisent par le blocage de l'application plutôt que par l'exécution du code malveillant.

COMMENT OBTENIR L'AEP

La technologie de Prévention Automatique d'Exploitation des failles (AEP) est disponible dans Kaspersky Endpoint Security for Business. Bien qu'elle soit activée par défaut, elle peut être désactivée si vous le souhaitez, seule ou avec l'intégralité du module de Surveillance du système (module qui surveille l'activité des programmes sur tout le système).
Par défaut, l'AEP bloque le lancement de tout code suspect. La méthodologie d'analyse et de suivi de Kaspersky Lab, ainsi que ses études approfondies et continues sur les applications les plus utilisées en entreprise, permettent de fortement limiter le nombre de faux positifs. Vous pouvez également exécuter cette fonction en mode interactif, en fonction de vos préférences.

LES AVANTAGES DE LA SÉCURITÉ INFORMATIQUE D'ENTREPRISE

La Prévention Automatique d'Exploitation des failles (AEP) réduit significativement le risque d'infection par des programmes malveillants ou des attaques ciblées par le biais d'exploitation de failles, même dans le cadre d'une vulnérabilité « zero-day ». Au cours des étapes approfondies de test, de recherche et de développement en interne de Kaspersky Lab, l'AEP a réussi à bloquer des programmes malveillants visant des vulnérabilités souvent utilisées dans Adobe Flash Player, QuickTime Player, Adobe Reader, Java et d'autres programmes.

Concernant la sécurité informatique, le mot d'ordre de Kaspersky Lab a toujours été d'offrir de multiples couches de protection, associées à l'efficacité de la surveillance des menaces afin d'anticiper la nature des menaces encore méconnues. La Prévention Automatique d'Exploitation des failles empêche l'exploitation de vulnérabilités, qu'elles soient connues ou non. Cela vient en complément des autres technologies de Kaspersky Lab, comme les filtres anti-programmes malveillants et anti-spam, en déployant un filet de sécurité pour capturer les codes plus complexes et perfectionnés qui peuvent parfois contourner les technologies traditionnelles de sécurité informatique.

L'exploitation du réseau Kaspersky Security Network et l'implication de nos équipes Global Research et Analysis Teams (GReAT) connues dans le monde entier nous permettent de bénéficier du plus large aperçu possible des millions de menaces présentes aux quatre coins du monde. Grâce à cette veille stratégique, nous sommes en mesure d'identifier et, la plupart du temps, de prévoir les incidents de sécurité de façon à aider les entreprises à se protéger plus efficacement et à réagir plus rapidement si leurs systèmes informatiques sont compromis. Nous concentrons nos efforts sur la résolution des problèmes de sécurité informatique à l'échelle internationale, de la protection des infrastructures critiques à la prévention des fraudes et aux services de veille en passant par la mobilité des entreprises et la sécurisation des environnements virtuels. Kaspersky Lab ne cesse d'anticiper et de prévenir les incidents menaçant la sécurité informatique des entreprises en réduisant les risques auxquels elles sont confrontées aujourd'hui et auxquels elles devront faire face à l'avenir.

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 16 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 300 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 2012. Ce classement a été publié dans le rapport IDC « Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares » (Sécurité des terminaux dans le monde : prévisions pour 2013-2017 et parts de marché des fournisseurs en 2012), document numéro 242618, août 2013. Ce rapport classait les éditeurs de logiciels selon leurs revenus provenant des ventes de solutions de sécurité des terminaux en 2012.