Solutions de cybersécurité de
Kaspersky Lab pour les entreprises

KASPERSKY lab

Les technologies de protection de Kaspersky Endpoint Security

www.kaspersky.fr
#truecybersecurity

Les technologies de protection de Kaspersky Endpoint Security

Ce document porte sur les technologies de détection des menaces exploitées par Kaspersky Endpoint Security, la solution de Kaspersky Lab dédiée à la protection des terminaux dans les réseaux d'entreprise.

Historique du développement de la protection des terminaux

Alors qu'hier, le concept de terminal recouvrait uniquement les postes de travail et les serveurs, aujourd'hui il inclut les appareils mobiles ainsi que les environnements virtuels. Les infrastructures informatiques sont devenues plus complexes et remplissent un rôle bien plus important dans le maintien du fonctionnement des processus continus.

Les analyses du « big data », le stockage distribué des données et l'automatisation des processus sont autant de domaines qui nécessitent des approches modernes en matière de sécurité. Parallèlement à cela, les données confidentielles et les actifs financiers suscitent de plus en plus l'intérêt des cybercriminels. La majorité des menaces actuelles sont principalement des outils développés pour gagner de l'argent tout en provoquant de lourdes pertes financières chez la victime et en détériorant sa réputation.

Les développeurs de solutions de sécurité informatique désireux de proposer une protection efficace contre les attaques complexes qui constituent le défi d'aujourd'hui doivent faire preuve d'une expertise approfondie.

Voici une liste des caractéristiques que doit posséder toute solution moderne de protection des terminaux :

Les postes de travail constituent toujours le principal point d'entrée des menaces et leur besoin d'une protection de qualité ne cesse d'augmenter.

- impact minimal sur le système cible grâce au fonctionnement équilibré des technologies impliquées ;
- détection rapide : méthodes de pointe appliquées à la détection de toute activité anormale, y compris le recours à des services spécialisés dans le Cloud ;
- enquête automatisée sur les incidents détectés ;
- retour automatique du système à l'état antérieur aux actions malveillantes ;
- transfert des informations relatives aux incidents vers un système de gestion des événements et des informations (SIEM) pour la mise en rapport des événements ou vers d'autres solutions ;
- administration aisée : interface intuitive et fonctions préconfigurées ;
- administration centralisée ;
- contrôle de l'intégrité des technologies de protection interne ;
- services efficaces : assistance pour le produit, enquête, formation, etc.

Comme le montre clairement la liste ci-dessus, la protection moderne ne se limite plus à la mise en place d'un simple mécanisme de détection basée sur les signatures ; elle intègre un éventail de technologies performantes, ce qui renforce la nécessité d'une administration aisée.

Au-delà des exigences fonctionnelles, il existe un ensemble de facteurs importants à prendre en compte au moment de choisir ces outils de sécurité. Il faut comprendre les technologies exploitées au sein de la solution et les liens entre celles-ci. Il s'avère tout aussi important d'évaluer le savoir-faire et l'expérience de l'éditeur, sans oublier ses capacités à poursuivre ultérieurement le développement de ces technologies.

Technologies impliquant le machine learning

Les techniques de feature engineering appliquent le savoir des experts à la définition des attributs à utiliser dans les algorithmes de machine learning.

Le machine learning a fait des adeptes dernièrement et cette méthode a remporté un franc succès lorsque de gros volumes de données étaient impliqués. Toutefois, avant de pouvoir appliquer efficacement le machine learning à la détection des menaces, il faut pouvoir compter sur un volume considérable de savoir-faire et d'expérience dans le domaine de la sécurité de l'information, associé à des techniques de feature engineering.

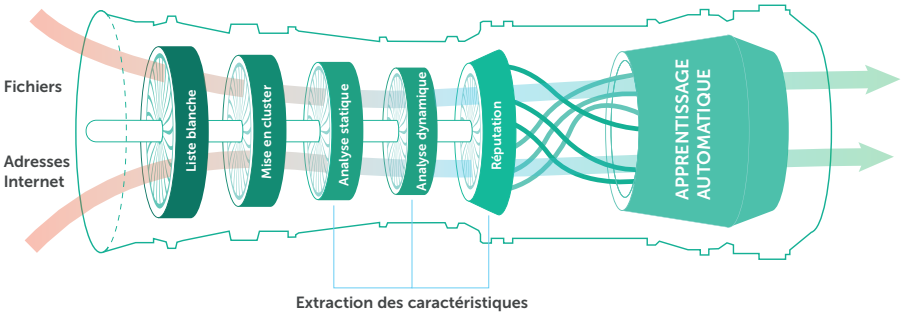
On entend souvent dire que le machine learning peut être appliqué aux données brutes dans le cadre de tâches de détection des menaces. En réalité, ce n'est pas vraiment le cas. Comme le dit l'adage des programmeurs : « mauvaises données au départ, mauvaises données à l'arrivée ». Il est primordial, dans le cadre de l'apprentissage, que les données soient soumises à un traitement préalable et à l'examen d'experts (feature engineering). Il serait naïf de croire qu'il est possible de créer des algorithmes efficaces sans l'intervention d'analystes de programmes

malveillants disposant d'une vaste expertise. En résumé, les analystes jouent un rôle de supervision : ils contrôlent et affinent le fonctionnement des algorithmes et interviennent dans la vérification des menaces les plus complexes que l'analyse automatique ne parvient pas toujours à gérer.

Grâce aux vingt ans de travaux de développement menés par son propre service de recherche, à l'analyse et aux données d'experts accumulées, Kaspersky Lab est en mesure de détecter automatiquement la très grande majorité des menaces à l'aide de méthodes de machine learning.

Le centre de traitement et d'analyse des menaces peut être décrit comme une « turbine » alimentée par des objets. Ces objets passent par différentes étapes de traitement et d'analyse qui font intervenir une palette de technologies, dont des algorithmes de machine learning. L'analyse des résultats ainsi obtenue sert de base à l'élaboration des règles de détection de menaces mises à la disposition des utilisateurs du Kaspersky Security Network.

Centre automatisé de traitement et d'analyse des menaces



Chaque jour, nos algorithmes de machine learning détectent et définissent plus de **310 000** menaces uniques. Grâce au travail accompli par Kaspersky Security Network, les technologies de sécurité appliquées aux terminaux peuvent bénéficier sur le champ de la majorité de ces informations.

La prévention des faux positifs figure également au cœur des préoccupations. C'est ainsi que les nouvelles règles sont vérifiées par rapport à une imposante base de données de fichiers sains.

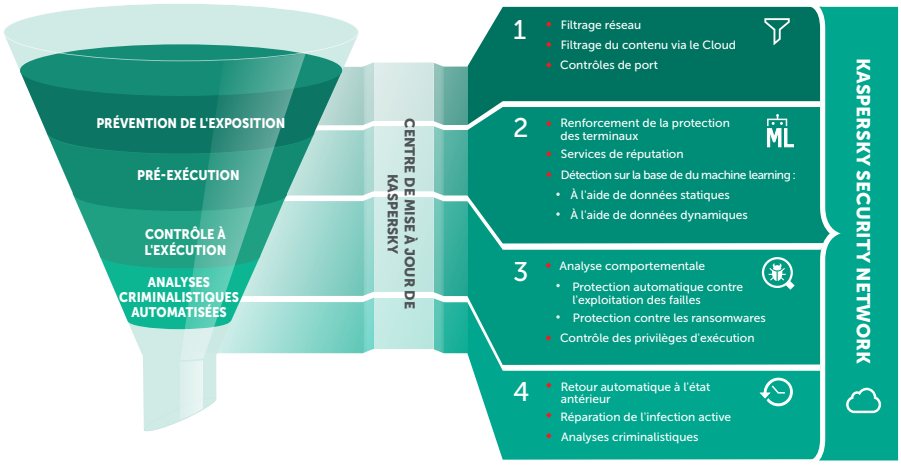
Kaspersky Endpoint Security

L'évolution des menaces qui ciblent les entreprises a donné naissance à une nouvelle génération de technologies de sécurité pour les terminaux. Kaspersky Lab a développé et mis en œuvre de nombreuses technologies dans ce domaine, notamment des technologies qui exploitent le machine learning. Grâce à elles, Kaspersky Lab a réussi à accélérer sensiblement la détection des menaces tout en réduisant l'impact global sur le système protégé. Kaspersky Endpoint Security (KES) est désormais un produit de sécurité très efficace destiné à la protection des terminaux dans les réseaux d'entreprises.

Séquence des technologies de protection

La logique qui sous-tend le fonctionnement de KES peut être scindée en quatre grandes étapes :

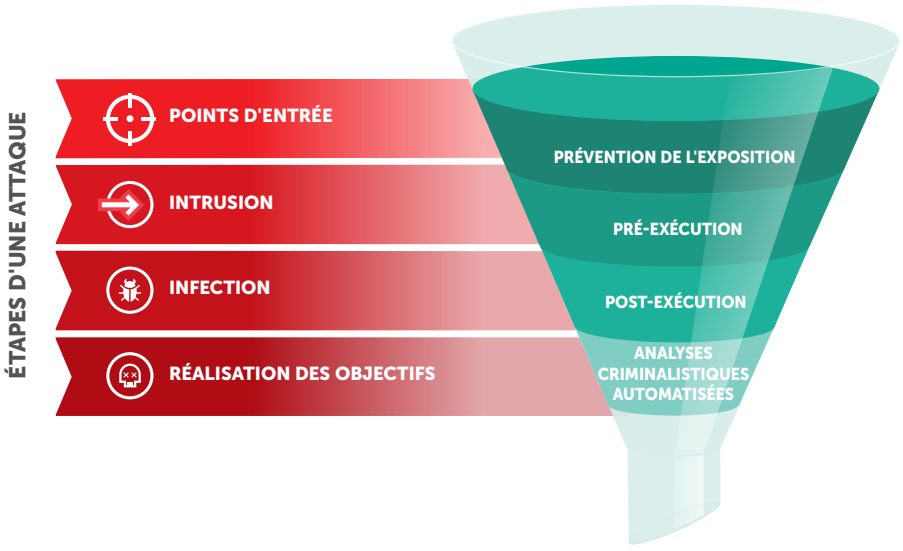
La séquence des technologies de protection de Kaspersky Endpoint Security



Chacune de ces étapes est représentées par un groupe de technologies de protection autonomes. En d'autres termes, chacune de ces technologies est capable de détecter et de bloquer une menace qui appartient à son domaine de compétence, alors que la séquence des étapes ci-dessus illustre les capacités de la solution prise dans son ensemble. Deux services Cloud spécialisés viennent renforcer ces technologies de sécurité.

- Le **centre de mises à jour** héberge les mises à jour incrémentielles et opportunes des composants de la protection, dont des bases de données spécialisées locales (comme la base de données des signatures, la base de données heuristique, la base de données des comportements, etc.). Le centre de mises à jour diffuse également les modifications opérationnelles introduites dans les paramètres des algorithmes de machine learning utilisés. Ceci confère au système une plus grande souplesse au moment de fournir la protection.
- **Kaspersky Security Network** est une infrastructure dans le Cloud qui garantit un accès en temps réel à diverses statistiques (notamment des statistiques sur la réputation, le contenu, le comportement, etc.). Il permet de réduire les durées de détection des menaces et préserve les ressources du nœud protégé.

La séquence d'application des technologies de protection ci-dessus est une réaction aux phases d'une attaque : chaque étape offre son propre niveau de sécurité requis pour déjouer la menace.



Nous allons à présent nous pencher sur chacune des étapes composant l'application des technologies de protection.

1. Prévention de l'exposition

De nos jours, les menaces se propagent par tous les canaux d'informations mis à leur disposition et il est dès lors essentiel que le périmètre du nœud protégé bénéficie d'une protection fiable.

La première étape consiste à filtrer toutes les informations entrantes.
Les technologies de blocage préventif se chargent de surveiller l'activité principale du nœud protégé, ce qui permet de détecter et de bloquer les menaces connues avant qu'il ne soit trop tard. Arrêtons-nous un instant sur les technologies de blocage mises en œuvre lors de cette première étape.

1.1. Protection contre les attaques réseau et pare-feu

Le **système de détection des intrusions (IDS)**, une sonde de réseau basée sur les signatures, assure la sécurité des connexions réseau. Dans le cadre de son fonctionnement, le système de détection des intrusions (IDS) exploite la technologie DPI (Deep Packet Inspection, inspection approfondie des paquets), ce qui permet à la sonde de réseau de contrôler tout le trafic en transit. Ce système est donc en mesure de détecter plusieurs événements réseau suspects et dangereux.

Voici quelques exemples d'événements réseau :

- balayage actif des ports ;
- tentatives de connexion à différents ports du système d'exploitation ;
- détection de communications réseau anormales, par exemple utilisation d'outils d'administration à distance, commandes envoyées depuis un serveur C&C (dans les cas impliquant des botnets).

Dès la détection d'un événement réseau dangereux, la sonde bloque la connexion à l'aide du pare-feu.

Un pare-feu est une technologie de blocage qui filtre l'activité réseau du nœud protégé sur la base de règles prédéfinies sur :

- le filtrage des paquets réseau et des flux de données ;
- l'activité des logiciels lors de l'interaction avec le réseau.

Ces paramètres sont définis par l'administrateur dans la stratégie de connexion réseau.

1.2 Filtrage Web

En 2016, 31,9 % des ordinateurs ont été exposés à une ou plusieurs attaques de malware pendant la navigation sur Internet.

Internet constitue une source de menaces. Il peut arriver que des individus malintentionnés piratent un nœud Internet de confiance afin d'y héberger un script malveillant ou d'y exploiter une faille zero-day, ce qui rend l'utilisation quotidienne de cette ressource dangereuse. Afin de garantir une utilisation conviviale et sûre d'Internet, KES intègre une technologie de filtrage Web composée de deux niveaux de protection.

Le premier niveau est associé au service Kaspersky Security Network (**KSN**) dans le Cloud. Il se charge du filtrage passif, à savoir l'indication en temps réel de la catégorie à laquelle une ressource Internet appartient ou de sa réputation. Cette opération se déroule avant que le navigateur ne commence à télécharger le contenu.

La base de données de réputation du KSN classe les adresses Internet dans l'une des catégories suivantes :

- adresse Internet malveillante : risque d'infection ;
- adresse Internet de phishing : intervient dans le vol d'informations personnelles ;
- adresse Internet inconnue : aucune information disponible sur la réputation ;
- adresse Internet sûre : ressource sans danger.

Le filtrage Web contribue grandement à la sécurité, bloque la majorité des sites Internet réputés dangereux et préserve les ressources du nœud protégé.

En 2016, 261 774 932 adresses Internet uniques ont déclenché des technologies de protection.

Le deuxième niveau repose sur la technologie d'analyse dynamique et assure le suivi du contenu téléchargé depuis toutes les ressources Internet inconnues. D'autres précisions sur les technologies de protection qui interviennent lors de la deuxième étape suivront ci-dessous.

1.3 Contrôle des périphériques connectés

Les appareils portables constituent une menace potentielle pour le nœud protégé. Le contrôle des périphériques identifie le type d'appareil connecté et invite l'utilisateur à confirmer que la connexion de celui-ci est autorisée.

Pour confirmer, l'utilisateur doit saisir le code affiché. Ce contrôle permet d'identifier les cas d'usurpation, par exemple lorsqu'une carte mémoire imite un clavier afin d'éviter l'analyse. Les cybercriminels adoptent cette méthode pour tromper les technologies de sécurité et s'introduire dans le périmètre protégé. Le contrôle des périphériques est étroitement lié aux technologies qui interviennent lors de l'étape de la prévention de l'exécution, là où les objets inconnus sont analysés.

2. Étape de prévention de l'exécution

Pour un cybercriminel, il est primordial de déjouer le filtrage, mais aussi de tromper les technologies de détection chargées d'identifier rapidement les programmes malveillants. Une infection n'est réussie que lorsque le code malveillant peut s'exécuter dans l'environnement de confiance. C'est la raison pour laquelle les cybercriminels ne cessent d'améliorer les techniques qui leur permettent de déjouer les techniques de détection.
Voici une liste des principales techniques :

- **Outils de compression** : le corps malveillant est compacté, ce qui complique la détection ;
- **Brouillage de code** : technique employée par des compilateurs spéciaux afin de compliquer le code au niveau de l'algorithme ;
- **Polymorphisme** : le code du programme malveillant est modifié pendant son exécution ;
- **Polymorphisme côté serveur** : un nouvel échantillon de code malveillant est généré par un serveur malveillant à chaque accès au serveur ;
- **Chiffrement** : le chiffrement à plusieurs niveaux permet de placer une partie du code hors de portée des mécanismes de détection. Cette technique est souvent utilisée conjointement avec le brouillage ;
- **Vulnérabilités, notamment les vulnérabilités zero-days** : l'exploitation des vulnérabilités d'un logiciel est une méthode d'infection efficace ;
- **Contournement des émulateurs** : un émulateur de lutte contre les programmes malveillants contrôle un fichier exécutable en l'exécutant dans un environnement isolé et en analysant sa logique de fonctionnement. Une analyse heuristique ou sur la base de signatures permet de détecter un code malveillant. Les pirates informatiques adoptent différentes méthodes pour modifier l'algorithme du code afin que l'émulateur ne puisse pas déterminer la logique.

L'adoption de deux ou plusieurs de ces méthodes est une pratique très fréquente chez les cybercriminels afin de s'introduire dans l'environnement d'un nœud protégé. La seule manière de contrecarrer ces pratiques passe par la mise en place d'une protection technologique globale, qui intègre les méthodes les plus récentes de contrôle et d'analyse des objets exécutables.

L'étape de prévention de l'exécution est l'une des plus actives étant donné l'imposant volume d'objets analysés en continu.

Examinons en détails les technologies employées à cette étape ainsi que les tâches réalisées.

2.1 Renforcement de l'environnement de confiance

Tout d'abord, un contrôle est mis en place au niveau de l'environnement de confiance. Cela permet d'atténuer les menaces potentielles en suivant et en éliminant les composants vulnérables du système d'exploitation et de logiciels de tiers.

Pour ce faire, l'objet est soumis à une évaluation de la vulnérabilité à l'aide de la base de données globale CVE (Common Vulnerabilities and Exposures). Il s'agit d'un processus automatisé, administré centralement via le composant Kaspersky System Management. Il signale rapidement les menaces identifiées dans le logiciel et les élimine en temps voulu grâce à la technologie de Patch Management.

D'après les statistiques de détection de l'année 2016, les vulnérabilités dans les logiciels constituent un point d'infection très utilisé.

Cette technologie de mise à jour garantit l'actualité du logiciel installé. Utilisées simultanément, deux technologies renforcent l'environnement protégé et réduisent considérablement la probabilité de l'exploitation de vulnérabilités.

Il convient de noter une autre technologie de blocage cruciale : le **Blocage par défaut**. Cette technologie adopte une autre démarche pour le contrôle du lancement des applications : tout ce qui n'est pas autorisé est interdit.

Dans le cadre d'un effort visant à améliorer la qualité de la détection des menaces et à minimiser les faux positifs, Kaspersky Lab a lancé le projet Technology Alliance, qui réunit les 500 plus grands éditeurs de logiciels ainsi que des développeurs de freeware indépendants. Cela permet à Kaspersky Lab de créer proactivement des listes blanches qui peuvent être exploitées par la technologie de blocage par défaut.

Cette solution permet à l'administrateur de définir les logiciels requis et suffisants pour réaliser les tâches quotidiennes au sein de l'entreprise.

Les avantages de la démarche Blocage par défaut sont les suivants :

- possibilité de bloquer les applications inconnues, y compris les nouvelles versions de programmes malveillants ;
- possibilité de bloquer l'installation et le lancement de logiciels interdits/sans licence sans aucun rapport avec les tâches à réaliser.

Cette technologie dispose d'un large éventail de catégories que l'administrateur peut attribuer aux logiciels (par exemple, éditeurs de confiance, comptes de confiance ajoutés manuellement, logiciel non autorisé ou sans licence, etc.). Le centre de traitement et d'analyse des menaces crée ces listes et les met à jour automatiquement. Cette procédure ne requiert aucune intervention humaine.

2.2 Services de réputation

Cette partie de Kaspersky Security Network garantit la détection rapide des menaces. Pour ce faire, le système repose sur des bases de données de réputation en ligne qui renferment des informations détaillées sur les objets. Ces bases de données sont enrichies en permanence d'informations spécialisées, dont des informations obtenues via les technologies de détection qui appartiennent à d'autres intervenants de l'infrastructure KSN par le biais du Cloud spécialisé de protection. Ces services de réputation offrent les avantages suivants :

- les verdicts sont émis sur le champ pour chaque objet ;
- ils ne reposent pas sur les ressources informatiques du terminal.

Après vérification, chaque objet se voit attribuer une catégorie :

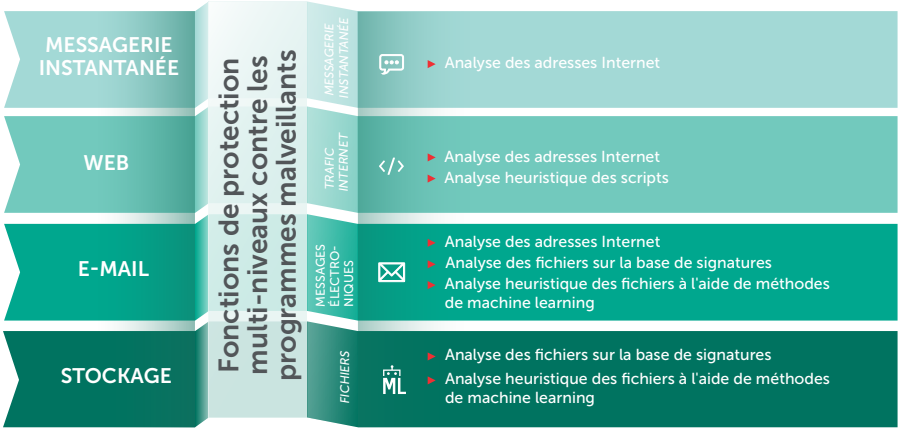
- **Malveillant** : le fichier contient un code malveillant.
- **Sain** : le fichier a été analysé et ne présente aucun danger.
- **Inconnu** : un nouveau fichier qui n'a jamais été analysé et qui représente un danger potentiel.

Tout fichier placé dans la catégorie « Inconnu » est automatiquement soumis à l'analyse grâce à des technologies de détection qui exploitent le machine learning (voir ci-après).

2.3 Protection à plusieurs niveaux

La dernière tâche de cette deuxième étape consiste à identifier les menaces complexes à l'aide de différentes technologies d'analyse. Elle repose sur un composant de protection à plusieurs niveaux qui inclut un ensemble de scénarios prédéterminés en fonction du type de point d'entrée de l'information.

La protection à plusieurs niveaux fonctionne de la manière suivante :



Chaque scénario possède son propre ensemble de technologies de détection. Toutefois, le cas échéant, ces technologies peuvent être utilisées simultanément afin de garantir le niveau de protection requis.

Filtrage Web - protection dynamique

Le filtrage Web intervient dans la phase active de détection des menaces au sein du contenu téléchargé. À l'étape initiale, les adresses Internet sont soumises à un contrôle statique afin d'identifier les catégories auxquelles chacune des ressources appartient. Lors de la deuxième étape, une analyse dynamique du code HTML est lancée dès que le téléchargement contrôlé débute.

Les technologies suivantes sont appliquées lors de l'étape active de la détection:

- **Analyse heuristique de l'adresse Internet**
  Une analyse de chaque adresse Internet intervient lors de son ouverture dans le navigateur du nœud protégé. Le code HTML est chargé dans un émulateur et un moteur d'analyse heuristique surveille son exécution. Ce procédé contribue à la détection des menaces dissimulées dans le code HTML et permet de bloquer l'ouverture des ressources Internet dangereuses.

- **Analyse heuristique des scripts**
  L'analyse des scripts dans les documents HTML fait l'objet d'une attention toute particulière. Cette analyse fait intervenir un émulateur capable de détecter des menaces complexes dans différents langages de scripts. Les niveaux passif (étape de filtrage initial) et actif (prévention des intrusions) du **Filtrage Web**, utilisés conjointement, garantissent la sécurité de la navigation pour l'utilisateur.

  Les technologies de **filtrage Web** interviennent également dans les contrôles de sécurité en cas d'utilisation de n'importe quel autre point d'entrée de l'information qui pourrait contenir une adresse Internet, par exemple dans des **e-mails ou des messageries instantanées**.

Statistiques 2016 : les technologies de filtrage Internet ont détecté 69 277 289 objets uniques, comme des scripts, des failles des fichiers exécutables, etc.

E-mail

Lors de la recherche de la présence éventuelle de menaces dans des e-mails, des technologies supplémentaires viennent appuyer l'**analyse heuristique des adresses Internet** pour analyser les fichiers en pièces jointes.

L'e-mail constitue un des points d'exposition les plus exploités par les cybercriminels. Il existe toute une branche de l'ingénierie sociale baptisée « phishing ciblé », qui choisit soigneusement la cible. Par exemple, on peut envisager l'envoi d'un e-mail spécial destiné à un utilisateur cible, qui va exploiter une faille dans des pièces jointes archivées. Les mots de passe d'accès aux archives figurent soit dans le corps du message, soit dans une image. Cette pratique impose certaines exigences aux outils de protection, à savoir la capacité d'ouvrir et d'analyser automatiquement des fichiers placés dans des archives.

Voyons à présent les technologies d'analyse des fichiers.

- **Analyse de fichiers basée sur les signatures**
  La technologie d'analyse basée sur les signatures intervient dans différents scénarios de protection lorsqu'il faut rechercher rapidement la présence éventuelle d'une menace dans un objet. Dans le cas des e-mails, cette méthode intervient dans l'analyse des fichiers en pièces jointes.

  La méthode qui repose sur les signatures possède certains avantages ; c'est la raison pour laquelle elle est appliquée en premier à l'analyse des fichiers. Voici ces principaux avantages :
  - rapidité de la détection ;
  - volume minime de faux positifs ;
  - peu de ressources requises sur le nœud protégé.

  La limite naturelle de cette méthode se situe au niveau du nombre de signatures qui existent dans la base de données (mise à jour en permanence). Pour cette raison, l'analyse basée sur les signatures fonctionne en parallèle avec l'analyse heuristique.

Une signature est un fragment de code qui permet d'identifier catégoriquement un objet malveillant.

- **Analyse des fichiers à l'aide des méthodes de machine learning**
  Nous allons examiner en détails ci-après l'analyse de fichiers à l'aide de du machine learning. Dans le cadre d'un scénario de protection des e-mails, la méthode de machine learning fournit la capacité unique de pouvoir décompacter les archives protégées par un mot de passe. Pour ce faire, elle extrait le mot de passe du corps du message (ce mot de passe est soit au format texte, soit sous la forme d'une image). Il s'agit d'une des techniques exploitées par les cybercriminels en vue de déjouer les technologies de détection : l'archive fait office de « coffre-fort » dont le contenu ne peut être soumis à une analyse. Afin de reconnaître le mot de passe fournit sous forme d'image, il faut utiliser un algorithme de machine learning. Une fois le mot de passe obtenu, il est saisi afin d'extraire le contenu de l'archive protégée par un mot de passe.

Stockage des fichiers

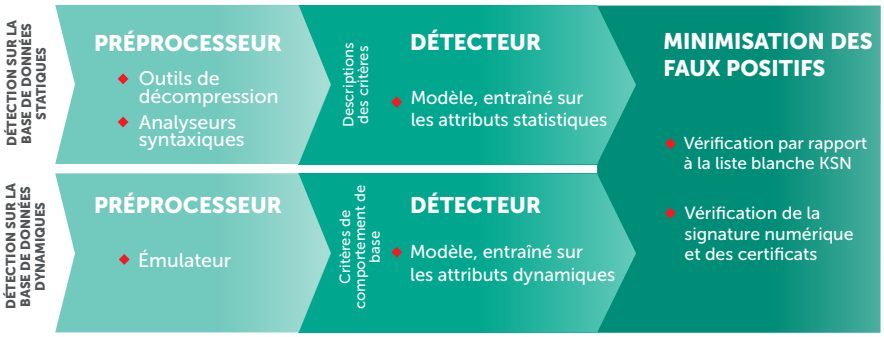
Tout fichier inconnu constitue une menace potentielle pour le nœud protégé et requiert une attention toute particulière de la part des technologies de protection.

Pour ce genre de situation, une protection à plusieurs niveaux propose un scénario complexe dans lequel le fichier est soumis à une analyse en profondeur à l'aide de méthodes de machine learning.

Il existe plusieurs technologies d'analyse de fichiers.

- **Analyse de fichiers basée sur les signatures**
  Les principaux avantages de cette méthode ont été cités dans la section consacrée aux e-mails. Dans le cadre de ce scénario, la technologie basée sur les signatures remplit la fonction d'un filtre élémentaire : elle fournit un verdict pour tous les fichiers connus et ne soumet que les fichiers inconnus à l'analyse à l'aide de méthodes de machine learning.

- **Analyse de fichiers à l'aide de méthodes de machine learning**
  Il s'agit de la technologie la plus avancée dans la protection à plusieurs niveaux. Elle soumet les fichiers à une analyse en profondeur afin de garantir une détection précoce des menaces. Cette technologie repose sur l'exécution de deux processus parallèles qui analysent le fichier au niveau des données statiques et dynamiques.



Ces deux processus sont scindés en trois étapes. Chacune d'entre elles fait intervenir des groupes spécifiques de technologies. L'utilisation conjointe des démarches statique et dynamique donne de bons résultats car elle permet de compenser les défaillances potentielles de chacune des approches individuelles :
- lorsque l'apprentissage du modèle repose sur des attributs statiques de programmes malveillants, certains fichiers se distinguent à peine des fichiers sains ;
- lorsque l'apprentissage du modèle repose sur des attributs dynamiques, certains programmes peuvent ne pas afficher un comportement malveillant. Il se peut que leur exécution requière un environnement particulier ou une ligne de commande dédiée.

Nous allons maintenant nous pencher sur les détails du fonctionnement de chacun de ces processus.

Les données statiques désignent les informations relatives à un objet qui ont été obtenues sans exécuter cet objet. Cette technologie se caractérise par un taux de généralisation et des performances élevés.

Détection sur la base des données statiques

Préprocesseur, technologies de préparation :

- **des outils de décompression** extraient le code compacté, ce qui permet aux analyseurs syntaxiques d'en extraire les métadonnées (les outils de compression, le brouillage de code et le chiffrement figurent parmi les méthodes traditionnellement utilisées par les cybercriminels pour éviter la détection) ;

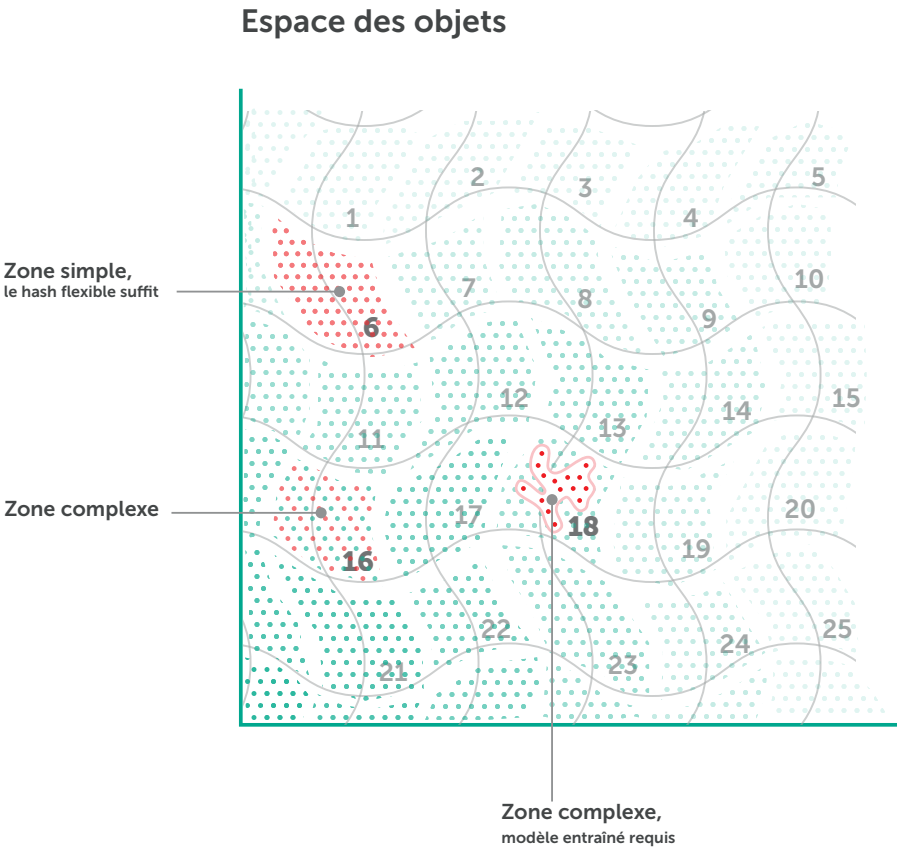
- **analyseurs syntaxiques** : outils qui permettent d'extraire différents ensembles de métadonnées.

La diversité des métadonnées a un impact direct sur la qualité de la détection. Pour cette raison, le préprocesseur contient une vaste bibliothèque d'analyseurs syntaxiques. Ceux-ci fournissent des descriptions informatives sur les attributs (comme les structures des fichiers exécutables, les caractéristiques statistiques des données et du code, les chaînes, etc.)

Le **détecteur** analyse les descriptions des attributs et transmet une décision sur le caractère malveillant ou non de chacun des objets analysés. Le détecteur fonctionne en deux étapes.

La première correspond au calcul d'un hash flexible qui permet de rechercher la présence de l'objet analysé dans la zone « sale ». Si la zone est simple (à savoir, elle contient des objets d'un seul type : tous « propres » ou tous « sales »), le

verdict peut tomber à cette étape. Un hash flexible tolère le polymorphisme et le brouillage de code, ce qui réduit sensiblement le volume de ressources requis sur le nœud protégé.



Le hash flexible repose sur des attributs, de telle sorte qu'il est identique pour un groupe de fichiers.

Une zone est une partie de l'espace des objets à laquelle un hash flexible ou un modèle entraîné correspondent.

Si la zone s'avère complexe (à savoir, elle contient à la fois des objets « sales » et des objets « propres »), l'objet passe à la seconde étape de l'analyse. Lors de la seconde étape, les descriptions d'attribut de l'objet sont évaluées par un module de classification dont la tâche consiste à trouver un modèle entraîné adéquat (spécialisé dans cette zone spécifique) parmi les nombreux modèles de la base de données et à l'appliquer. Le modèle entraîné formule la décision finale sur la nature malveillante ou non de l'objet.

Analyse d'un objet sur la base de données dynamiques

Le **préprocesseur** recueille des informations dynamiques telles que le comportement de l'objet, les secteurs de la mémoire qui contiennent du code exécutable, etc.

Les données dynamiques désignent les informations relatives à un objet, notamment les informations relatives à son comportement recueillies pendant son exécution ou l'émulation de celui-ci.

L'émulateur permet d'exécuter un fichier exécutable dans un environnement contrôlé qui imite en partie le système actuel. Les avantages sont l'impact minimal sur les ressources de l'ordinateur et sur la sécurité (le code analysé ne peut avoir un impact sur l'environnement de confiance). L'analyse dynamique génère une séquence enregistrée des actions du fichier exécuté, ainsi qu'un vidage de la mémoire et d'autres objets (par exemple, des fichiers) créés pendant l'exécution. Toutes les données citées constituent les attributs de base du comportement.

Le vidage de la mémoire permet d'accéder au code original (non compacté) et de détecter les données qui pourraient signaler la nature malveillante du fichier.

Le **détecteur** identifie les scénarios de comportement malveillant et prend une décision sur le caractère malveillant ou non de chacun des objets analysés.

Le détecteur utilise une bibliothèque de scénarios malveillants compilée par le centre automatisé de traitement et d'analyse des menaces de Kaspersky Lab.

Un scénario malveillant désigne une séquence d'actions pour la réalisation d'une attaque.

Statistiques 2016 : la protection à plusieurs niveaux a signalé 4 071 588 objets uniques malveillants et potentiellement indésirables.

Le centre possède d'immenses collections de fichiers malveillants et sains qu'il traite en permanence pour extraire les attributs de comportement de base utilisés dans l'entraînement des modèles. Les modèles se transforment en scénarios de comportement et le détecteur les reçoit sous la forme de mises à jour incrémentielles. Cette démarche réduit considérablement la durée d'attente requise pour les mises à jour et la taille de celles-ci. Elle préserve l'efficacité du fonctionnement du détecteur.

Un faux positif est une erreur de jugement du détecteur qui considère un objet comme étant malveillant alors que cet objet est sain.

Minimisation des faux positifs

Après chaque décision prise par le détecteur, une vérification confirme qu'il ne s'agit pas d'un faux positif. La probabilité d'un faux positif est très faible, mais un tel événement peut avoir de graves conséquences.

Lorsqu'un objet est considéré comme malveillant, les vérifications minimales suivantes permettent de réduire le risque de faux positif :

- Le service Cloud KSN reçoit une demande qui contient le numéro du modèle entraîné ou du scénario de comportement qui a émis la décision sur la menace identifiée. (KSN contient des informations relatives aux modèles et aux scénarios de comportements valides, si bien qu'il peut vérifier si le modèle/le scénario a été révoqué.)
- Les listes blanches du service Cloud KSN reçoivent une demande afin de pouvoir exclure tout faux positif du détecteur. (Les listes blanches désignent une vaste collection de fichiers identifiés comme sains. Cette collection est mise à jour en continu via le centre automatisé de Kaspersky Lab.)
- Un service Cloud de classification de certificats reçoit une demande afin de vérifier la réputation du certificat utilisé pour signer le fichier.

S'agissant de la deuxième étape, il convient de noter qu'il existe un cache KSN local permettant d'éviter les demandes répétitives au sujet d'objets qui ont déjà été analysés. Ceci permet de préserver les ressources du nœud protégé.

3. Contrôle de l'exécution

En 2016, des attaques de crypteurs ont été bloquées sur les ordinateurs de 1 445 434 utilisateurs uniques.

En 2016, Kaspersky Lab a détecté plus de 54 000 nouvelles modifications de crypteurs et 62 nouvelles familles.

Bien que la deuxième étape contienne une analyse statique et une analyse dynamique, certaines menaces peuvent malgré tout passer au travers des mailles du filet. Ainsi, des crypteurs à plusieurs composants qui utilisent un logiciel de chiffrement légitime peuvent passer inaperçus car aucun des composants individuels pris séparément ne constitue une menace.

L'objectif de la troisième étape est de détecter tout comportement malveillant au sein de l'environnement de confiance. Lors de l'analyse, le comportement global de tous les composants actifs est pris en compte, y compris celui des applications de confiance ou des applications douteuses, sans oublier les composants système. Ce type d'analyse permet d'identifier les menaces complexes à plusieurs composants.

Les vulnérabilités zero-day sont des erreurs de code qui n'ont pas encore été corrigées et qui permettent aux cybercriminels de compromettre un système à l'aide de fonctions de l'application non documentées.

L'analyse comportementale porte sur le comportement réel et non sur une représentation présumée (émulée) d'actions analysée à l'étape de la prévention de l'intrusion.

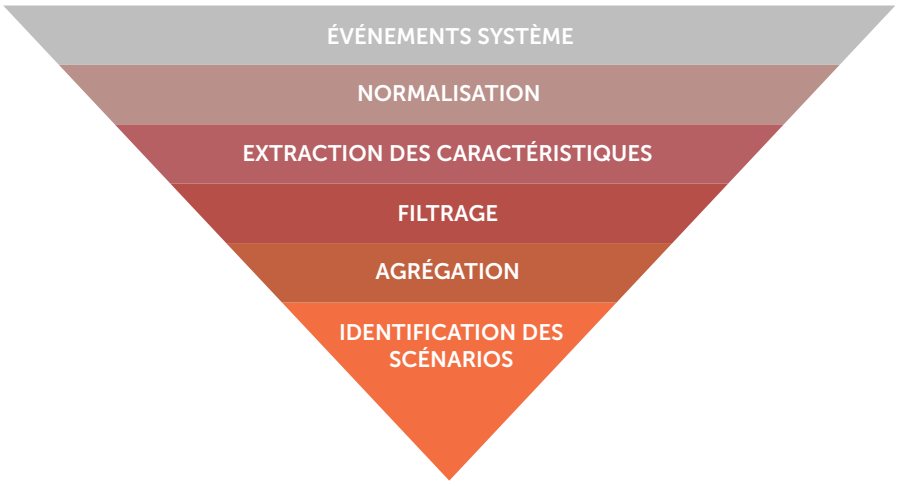
Un autre exemple serait celui de la prévention de l'exploitation des failles. Ce cas correspond à la détection d'un comportement malveillant au sein d'une application de confiance.

Par exemple, à l'ouverture d'un document Word contenant une faille, la technologie AEP (Automatic Exploit Prevention, protection automatique contre l'exploitation des failles) détecte le comportement malveillant et le bloque. Cette technologie est efficace et bloque les menaces complexes, y compris les failles pour les vulnérabilités zero-day.

3.1 Analyse comportementale

Cette technologie analyse le comportement de tous les composants actifs au sein de l'environnement de confiance du nœud protégé. Elle offre les niveaux d'analyse suivants :

Analyse comportementale



- Événements système : surveillance des principaux événements système comme la création de processus, les modifications de valeurs de clé de registre, les modifications des fichiers, etc ;
- Normalisation : organisation des événements entrants au sein d'un format commun pour la suite du traitement ;
- Extraction des caractéristiques : ajout d'informations complémentaires pour certains événements, par exemple le fichier modifié est-il ou non un fichier exécutable ;
- Filtrage, agrégation et identification des scénarios : ces étapes correspondent à l'identification de combinaisons et de séquences importantes d'événements, ce qui donne le scénario de comportement. Le centre automatisé de Kaspersky Lab crée la bibliothèque des scénarios malveillants qui sert de référence au traitement et à l'analyse des menaces.

3.2 Contrôle des privilèges

Le contrôle des privilèges s'opère parallèlement à l'analyse comportementale, sur la base des stratégies et de la catégorie de l'application.

Le contrôle consiste à surveiller les activités de l'application et à imposer des restrictions sur la base des propriétés de cette dernière : popularité à travers le monde, réputation de l'éditeur, risque de détection, etc. Grâce à ce contrôle, une application ne peut réaliser des actions non contrôlées dans l'environnement protégé comme réaliser des communications réseau ou d'autres activités du genre.

Les restrictions élémentaires pour différentes catégories d'applications sont générées par le centre automatisé de traitement et d'analyse des menaces de Kaspersky Lab.

Par exemple, les applications Microsoft ou d'autres bien connues sont soumises à une stratégie de contrôle faible. En revanche, le système de contrôle des privilèges applique une stratégie plus stricte aux applications moins connues et ce, en raison des risques et du niveau de danger que l'application peut présenter.

Le contrôle des privilèges fonctionne avec les listes de blocage par défaut des applications de confiance (le cas échéant), ce qui garantit une sécurité en temps réel. Il est possible de gérer les restrictions centralement au niveau du réseau de l'entreprise ou de configurer la protection des données personnelles sur une base individuelle.

4. Mesures correctives après une infection

Une infection est l'exécution d'un code malveillant au sein d'un environnement de confiance. Après l'infection, le processus exécuté cherche à atteindre les objectifs définis par les cybercriminels et déclenche une séquence d'événements. En général, ce genre de situation se présente en cas d'installation d'une solution de sécurité sur un nœud dont l'infection est connue ou lors de la détection d'une activité potentiellement dangereuse au niveau de l'analyse comportementale. Prenons, à titre d'exemple, un chiffrement de fichier lancé par un processus légitime sur un disque local du nœud de protection.

En 2016, 22,6 % des utilisateurs attaqués par des crypteurs appartenaient au secteur professionnel.

Dans ce cas, la quatrième étape de la protection démarre. Cette étape correspond à la réponse d'urgence à la menace.

Chaque fois que les technologies d'analyse comportementale bloquent une activité potentiellement dangereuse, il faut exécuter un plan d'action afin de rétablir l'état antérieur de l'environnement de confiance.

4.1 Retour automatique à l'état antérieur aux actions

Le retour automatique à l'état antérieur aux actions annule la moindre modification introduite par le processus bloqué. Il déroule la séquence d'actions et rétablit l'état antérieur de la structure. Ce processus bénéficie de l'aide de technologies de l'étape d'**analyse comportementale**, qui fournissent un historique détaillé des actions réalisées par chaque processus en particulier.

Une séquence d'événements peut contenir les éléments suivants :

- branches du registre du système d'exploitation ;
- fichiers exécutables créés par le processus (scripts ou fichiers binaires) ;
- fichiers modifiés, par exemple les fichiers chiffrés par le cryptovirus.

4.2 Réparation de l'infection active

Dans certains cas complexes (par exemple, un code malveillant s'est injecté dans un processus système dans lequel il est impossible d'intervenir sans risque de nuire à la stabilité du système d'exploitation), il faut faire appel à la technologie de traitement d'une infection active. Cet outil est capable de restaurer en toute sécurité les fichiers infectés, notamment les composants du système d'exploitation. En cas de traitement actif, l'ordinateur protégé redémarre. Les composants infectés du système sont remplacés par des composants propres. Pour ce faire, la technologie compte sur sa capacité à rechercher les fichiers originaux requis pour la restauration. Le système retrouve alors son état stable.

En 2016, 4 071 588 programmes uniques, malveillants et potentiellement dangereux ont été signalés. (Il est généralement admis que le nombre de programmes uniques correspond au nombre de verdicts uniques.)

4.3 Analyses criminalistiques

L'analyse de chaque incident lié à la sécurité de l'information requiert sa propre base de preuves. Dans la mesure où les technologies de protection récoltent un large éventail de données, il est possible d'analyser les incidents et d'adopter des mesures de prévention pour la sécurité de l'information.

Mesures de sécurité inhérentes

Pour garantir la fiabilité de son propre fonctionnement, la solution possède des outils qui lui permettent de contrôler sa propre sécurité. L'intégrité de la protection est ainsi garantie, notamment la protection contre les tentatives de désactivation.

Ces outils d'autodéfense interceptent et bloquent les opérations dangereuses sur les ressources de l'environnement de confiance, quels que soient les privilèges de l'utilisateur. Ceci permet de résoudre la question des vulnérabilités qui pourraient permettre à un programme malveillant d'obtenir des privilèges d'administrateur.

Gestion

La console Kaspersky Security Center a été développée en pensant à la souplesse de la gestion de la sécurité. Elle fournit des informations détaillées sur l'état de la sécurité du terminal et sur la stratégie de sécurité centralisée. Kaspersky Security Center est donc le centre névralgique de la gestion de la sécurité du réseau d'entreprise et des rapports sur l'ensemble des menaces.

Il convient également de citer les fonctionnalités étendues disponibles dans Kaspersky Systems Management. Cet élément améliore la sécurité du réseau d'entreprise grâce aux caractéristiques suivantes :

- l'évaluation des vulnérabilités et la gestion des correctifs ;
- les inventaires matériel et logiciel ;
- le déploiement flexible d'applications et de systèmes d'exploitation ;
- la distribution logicielle ;
- l'intégration SIEM ;
- le contrôle des accès dans les réseaux d'entreprise complexes.

Solutions de cybersécurité de
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