kaspersky BRING ON THE FUTURE

Kaspersky Threat Attribution Engine

Le suivi, l'analyse, l'interprétation et la lutte contre les menaces informatiques, en perpétuelle évolution, représentent un travail considérable. La Threat Intelligence offre une valeur réelle qui va au-delà du battage médiatique actuel provoqué par une nouvelle tendance dans le secteur de la sécurité de l'information. L'attribution des menaces, quant à elle, est probablement le point d'intérêt et de discorde le plus important à ce sujet.

Caractéristiques principales du produit

- Fournit un accès instantané à un répertoire de données sur des centaines d'échantillons et acteurs APT
- Permet une hiérarchisation automatique ou manuelle efficace des menaces et un triage des alertes
- Permet d'ajouter des acteurs et des échantillons privés pour un produit évolutif qui apprendra à détecter les échantillons qui sont similaires aux fichiers de votre collection privée
- Permet de télécharger manuellement des échantillons et une API ouverte pour l'intégration avec des flux de travail automatisés
- Peut être déployé dans des environnements sécurisés, isolés par un espace d'air (air-gapped) virtuel, afin de protéger vos systèmes et vos données et de répondre à l'ensemble des exigences en matière de conformité.
- Maintient le respect absolu de la vie privée et la confidentialité de toutes les soumissions afin d'éviter d'exposer des informations sensibles

La raison en est évidente. Le délai moyen d'intervention après la détection de menaces très sophistiquées est généralement trop long, en raison de la complexité des processus d'enquête et de reverse engineering. Dans de nombreux cas, il n'en faut pas plus aux attaquants pour atteindre leurs objectifs. Une attribution correcte et rapide permet non seulement de réduire le temps de réponse aux incidents de plusieurs heures à quelques minutes, mais aussi de réduire le nombre de faux positifs.

Identifier une attaque ciblée, établir le profil des attaquants et créer des facteurs d'attribution pour les différents acteurs de la menace est un travail long et minutieux qui peut prendre des années. La création d'une attribution fonctionnelle nécessite également une grande quantité de données accumulées depuis des années ainsi qu'une équipe de chercheurs hautement qualifiés et expérimentés en termes d'investigation. Les chercheurs suivent l'activité des différents groupes et alimentent la base de données avec des éléments d'information. Ces bases de données constituent alors une ressource précieuse pouvant être partagée sous forme d'outil.

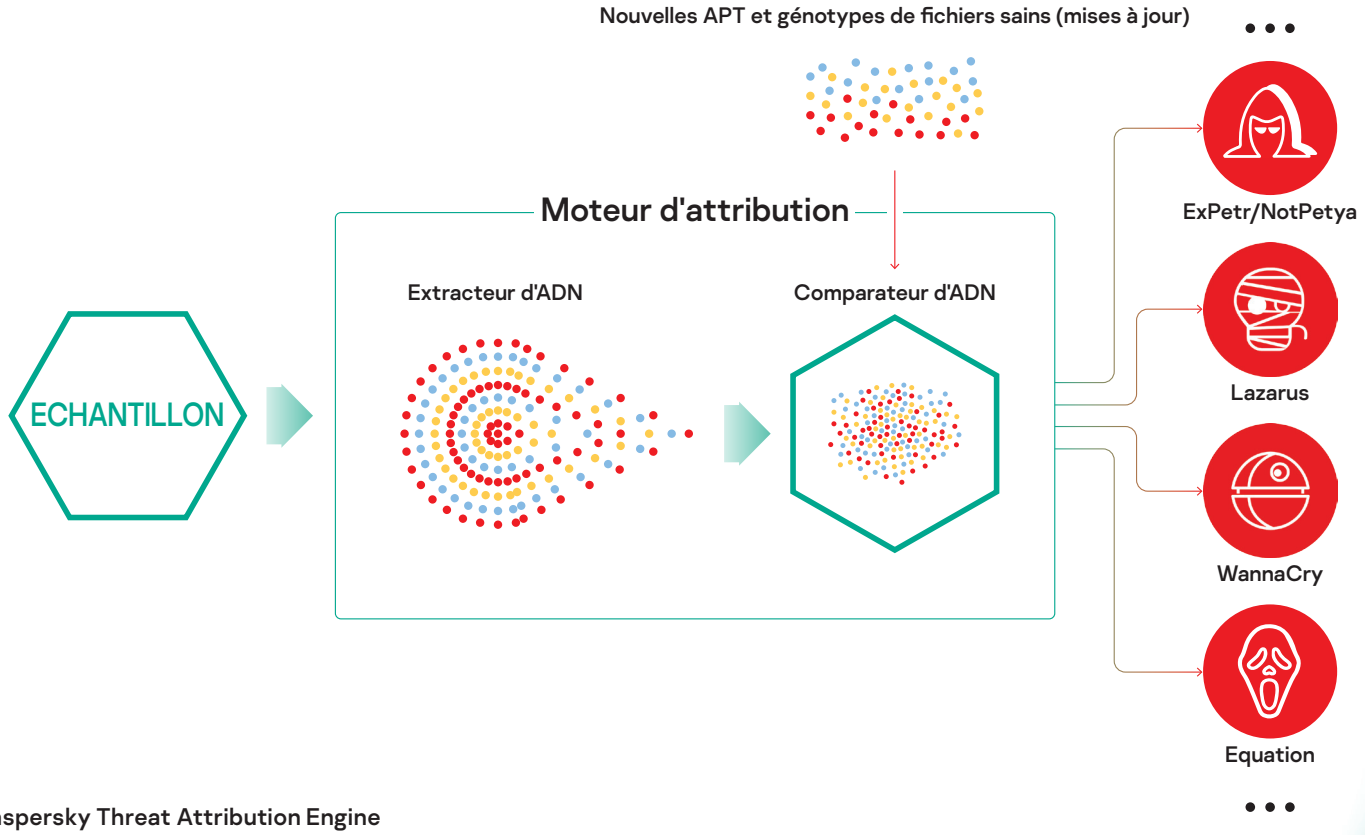
Kaspersky Threat Attribution Engine intègre une base de données d'échantillons de programmes malveillants APT et de fichiers sains collectés par les experts Kaspersky au cours des 22 dernières années. Nous effectuons le suivi de plus de 600 acteurs et campagnes APT et publions chaque année plus de 120 rapports de surveillance des menaces APT. Nos recherches alimentent continuellement une vaste collection d'APT de plus de 60 000 fichiers. Elles améliorent la détection des fausses bannières et rendent l'attribution aussi précise que possible grâce aux outils automatisés.

Le produit permet une approche unique pour comparer la similarité des échantillons tout en garantissant un taux de faux positifs nul. Il peut rapidement faire le lien entre une nouvelle attaque et des logiciels malveillants APT connus, des attaques ciblées antérieures et des groupes de hackers. Ainsi, il est plus facile de repérer les menaces sérieuses parmi les incidents moins graves et de prendre des mesures de protection opportunes pour empêcher un attaquant de s'infiltrer dans le système.

Comment ça fonctionne ?

Kaspersky Threat Attribution Engine analyse la « génétique » des logiciels malveillants pour trouver des similitudes de code avec des échantillons d'APT préalablement étudiés et des acteurs connexes, le tout de manière automatisée. Il compare les « génotypes », c'est-à-dire des petits morceaux binaires de fichiers décomposés, avec la base de données d'échantillons de logiciels malveillants APT. Ensuite, il propose un rapport sur l'origine des logiciels malveillants, les acteurs de la menace et la similarité des fichiers avec les échantillons APT connus. De plus, les équipes de sécurité peuvent ajouter des acteurs et des objets privés à la base de données du produit et lui apprendre à détecter les échantillons qui sont similaires aux fichiers de votre collection privée. Avec Threat Attribution Engine, le processus d'attribution ne prend que quelques secondes par rapport aux années requises dans le passé.

Le produit peut être déployé dans un environnement sécurisé, à l'abri des regards indiscrets, empêchant toute tierce partie d'accéder aux informations traitées et aux objets soumis. Il existe une interface API pour connecter le moteur à d'autres outils et frameworks afin de mettre en œuvre l'attribution dans l'infrastructure existante et les processus automatisés.



Kaspersky Threat Attribution Engine

Des informations détaillées sur l'acteur APT concerné se trouvent dans les rapports de surveillance des APT de Kaspersky[1]. En tant qu'abonné aux rapports de surveillance des APT de Kaspersky, vous accédez à tout moment à nos enquêtes et découvertes, y compris aux données techniques complètes sous plusieurs formats, sur chaque APT, dès sa découverte, ainsi que sur toutes les menaces qui restent dissimulées.

Kaspersky Threat Attribution Engine étend et renforce encore le portefeuille de Kaspersky pour les agences nationales de cybersécurité et les centres d'opérations de sécurité (SOC) commerciaux en les aidant à mettre en place un processus efficace de gestion des incidents.

Kaspersky Attribution Engine améliore considérablement les opérations de sécurité en aidant à :

- attribuer rapidement des fichiers à des acteurs connus de l'APT pour révéler les motivations, les méthodes et les outils qui se cachent derrière les cyberincidents ;
- évaluer rapidement si vous êtes la cible d'une attaque ou une victime secondaire afin de mettre en place des procédures de confinement et d'intervention appropriées ;
- assurer une atténuation efficace et opportune de la menace selon une Threat Intelligence exploitable sur la famille APT fournie dans le rapport de surveillance des APT de Kaspersky.

1 Un abonnement à Kaspersky APT Intelligence Les rapports doivent être achetés séparément

Actualités sur les cybermenaces : www.securelist.com
Actualités dédiées à la sécurité informatique : business.kaspersky.com
Sécurité informatique pour les PME : kaspersky.fr/small-to-medium-business-security
Sécurité informatique pour les entreprises : kaspersky.fr/enterprise-security

www.kaspersky.fr

Reconnu. Indépendant. Transparent. Nous nous engageons à construire un monde plus sûroù la technologie améliore notre vie. C'est pourquoi nous la sécurisons, afin que le monde entier dispose des possibilités infinies qu'elle nous offre. Adoptez la cybersécurité pour un avenir plus sûr.

Pour en savoir plus, rendez-vous sur kaspersky.fr/transparency

Proven. Transparent. Independent.