kaspersky BRING ON THE FUTURE

Kaspersky Research Sandbox

Prendre une décision intelligente basée sur le comportement d'un fichier tout en analysant simultanément la mémoire du processus, l'activité réseau etc. est l'approche optimale pour comprendre les menaces sophistiquées, ciblées et personnalisées actuelles. Les technologies de sandboxing sont des outils puissants qui permettent d'enquêter sur l'origine d'un échantillon de fichier, de collecter des indicateurs de compromission basés sur l'analyse comportementale et de détecter des objets malveillants qui n'avaient jamais été vus auparavant.

Caractéristiques principales du produit

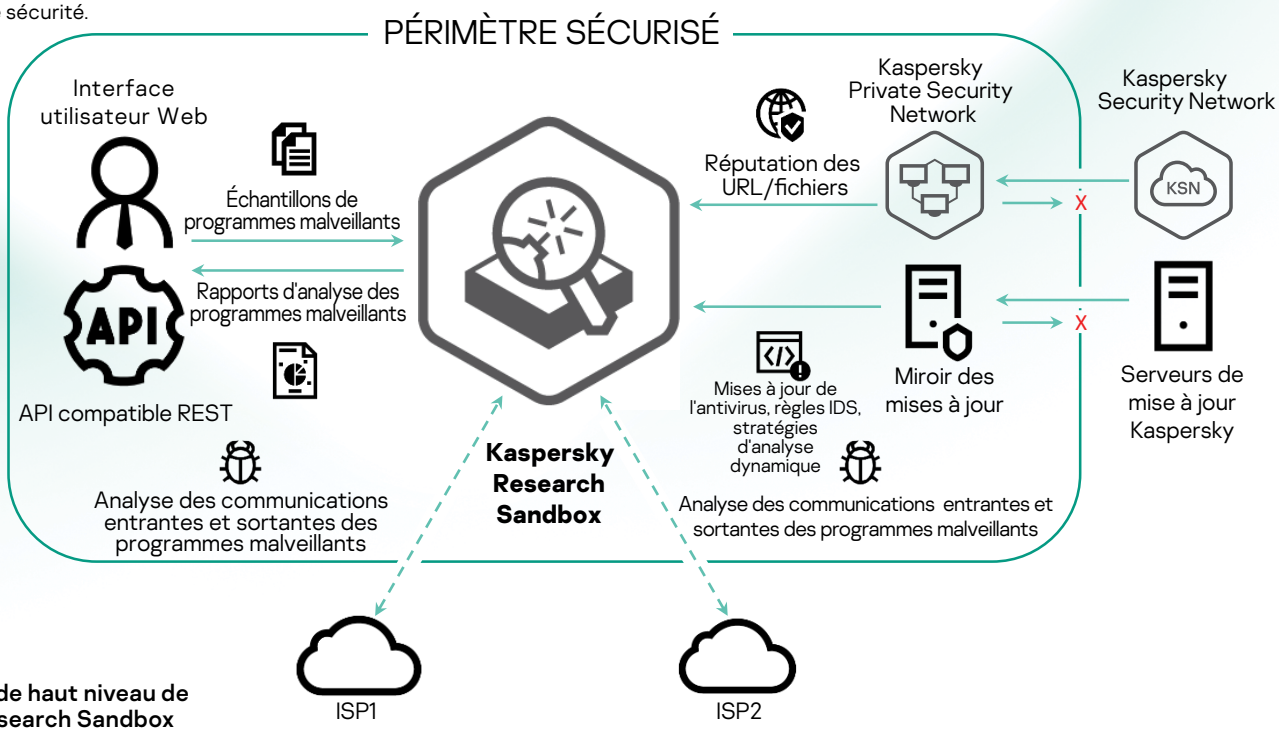
- Déploiement sur site permettant de ne pas exposer les données à l'extérieur de l'organisation
- Prise en charge de l'analyse de plus de cent types de fichiers
- Techniques anti-évasion avancées
- Émulation de l'activité des utilisateurs
- Images personnalisées permettant d'analyser les menaces dans divers systèmes d'exploitation et applications, et uniquement en fonction de ce qui s'applique aux environnements réels
- Analyse distincte de chaque processus pour détecter les activités suspectes et les connexions réseau associées
- Rapports d'analyse détaillés, incluant l'ensemble des activités du système, des fichiers extraits, des activités réseau (PCAP) et des graphiques visuels
- Prise en charge de l'intégration avec Kaspersky Private Security Network
- Soumission de fichiers manuelle et API compatible REST pour une intégration et une automatisation transparentes de vos opérations de sécurité.

Les programmes malveillants actuels ont recours à toute une série de méthodes pour éviter d'exécuter leur code si cela peut conduire à l'exposition de leur activité frauduleuse. Si le système ne respecte pas les paramètres requis, le programme malveillant s'autodétruira certainement, ne laissant aucune trace. Pour que le code malveillant s'exécute, l'environnement de sandboxing doit donc être capable d'imiter avec précision le comportement normal de l'utilisateur final.

Kaspersky Research Sandbox est un dérivé direct de notre ensemble de sandboxes interne, une technologie qui évolue depuis plus de dix ans. Elle intègre toutes les connaissances sur les comportements malveillants acquises par Kasperskypar le biais de notre recherche continue sur les menaces, ce qui nous permet de détecter plus de 350 000 nouveauxobjets malveillants chaque jour. Déployée sur site, cette technologie puissante empêche également l'exposition des données en dehors de l'entreprise.

Elle offre une approche hybride, en associant l'analyse comportementale et une fonctionnalité anti-évasion solide avec des technologies de simulation humaine. Kaspresky Research Sandbox permet également de personnaliser des images des systèmes à des fins d'analyse en les adaptant aux environnements réels, ce qui a pour effet de rendre la détection des menaces plus précise et d'augmenter la vitesse des enquêtes.

Le diagramme ci-dessous décrit l'architecture de haut niveau de Kaspersky Research Sandbox.



Architecture de haut niveau de Kaspersky Research Sandbox

Pour éviter de se faire repérer, un fichier malveillant peut commencer par rechercher s'il se trouve sur une machine virtuelle ou rester inactif pendant un certain temps jusqu'à ce que la sandbox ne soit plus en fonctionnement. Lorsque cela se produit, la technologie brevetée accélère le flux temporel à l'intérieur de la machine virtuelle afin de forcer le code malveillant à s'exécuter plus rapidement.

Il se peut que les programmes malveillants n'affichent pas leur comportement malveillant s'ils ciblent une application spécifique absente de la sandbox. Pour remédier à cela, les chercheurs doivent examiner les journaux, comprendre ce qui manque, l'ajouter à une machine virtuelle et recommencer ce processus. Ainsi, lorsque des programmes malveillants tentent d'accéder à une application, le système breveté bloque cette tentative. Au lieu d'attendre que l'exécution du fichier soit terminée, il interrompt le processus pour créer l'application et le contenu requis.

Les règles de détection décrivant comment réagir face à un événement spécifique ne sont pas installées à l'avance ni déployées à l'intérieur du moteur, mais elles peuvent être facilement mises à jour et ajoutées.

La solution Kaspersky Research Sandbox est basée sur une technologie propriétaire brevetée (brevet n° US10339301). En reproduisant les conditions exactes qui déclenchent l'exécution des programmes malveillants, elle permet aux chercheurs d'analyser un fichier suspect en une seule fois.

Le produit prend également en charge le déploiement sans système d'exploitation. La configuration matérielle dépend des performances requises et peut évoluer. Elle nécessite une connexion au réseau avec un débit de 100 Mbit/s pour chaque canal et au moins une connexion FAI indépendante (avec une recommandation de deux connexions ou plus pour la tolérance aux pannes). Le FAI doit être informé et prêt à recevoir du trafic malveillant.

Une fois l'analyse terminée, Research Sandbox fournit un rapport détaillé concernant le comportement et les fonctionnalités de l'échantillon étudié, ce qui vous aide à définir les procédures de réponse appropriées :

- **Résumé** : informations générales sur les résultats d'exécution d'un fichier.
- **Nom des détections effectuées par la sandbox** : liste des détections qui ont été répertoriées (à la fois pour l'antivirus et le comportement) durant l'exécution du fichier.
- **Règles du réseau déclenchées** : liste des règles SNORT du réseau qui ont été déclenchées par l'objet exécuté durant l'analyse du trafic.
- **Carte d'exécution** : représentation graphique de la séquence d'activités de l'objet (actions effectuées sur les fichiers, les processus et le registre, et activité du réseau) et des relations entre les activités. Le nœud racine de l'arbre représente l'objet exécuté.
- **Activités suspectes** : liste des activités suspectes répertoriées.
- **Captures d'écran** : ensemble des captures d'écran effectuées durant l'exécution du fichier.
- **Images PE chargées** : liste des images PE chargées détectées durant l'exécution du fichier.
- **Opérations sur le fichier** : liste des opérations sur le fichier qui ont été répertoriées durant l'exécution du fichier.
- **Opérations sur le registre** : liste des opérations effectuées sur le registre du système d'exploitation qui ont été détectées durant l'exécution du fichier.
- **Opérations sur les processus** : liste des opérations du fichier avec divers processus qui ont été répertoriées durant l'exécution du fichier.
- **Opérations synchronisées** : liste des opérations issues des objets de synchronisation créés (mutex, event, semaphore) qui ont été répertoriées durant l'exécution du fichier.
- **Fichiers téléchargés** : liste des fichiers qui ont été extraits du trafic réseau durant l'exécution du fichier.
- **Fichiers déposés** : liste des fichiers qui ont été sauvegardés (créés ou modifiés) par le fichier exécuté.
- **Requêtes HTTPS/HTTP/DNS** : listes des requêtes HTTPS/HTTP/DNS qui ont été répertoriées durant l'exécution du fichier.
- **Décharge de trafic réseau (PCAP)** : activité réseau pouvant être exportée au format PCAP.

Kaspersky Research Sandbox est l'instrument de choix pour détecter les menaces inconnues. Cette solution est plus mature et centrée sur les menaces avancées que toutes les autres.

Actualités dédiées aux cybermenaces : www.securelist.fr
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

Nous sommes reconnus. Nous sommes indépendants. Nous sommes transparents. Nous nous engageons à construire un monde plus sûr où 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.