Kaspersky Research Sandbox

kaspersky BRING ON THE FUTURE

Technologie Sandboxing

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 (IoC) basés sur l'analyse comportementale et de détecter des objets malveillants qui n'avaient jamais été vus auparavant.

Kaspersky Research Sandbox

Prendre une décision intelligente basée sur le comportement d'un fichier ou d'une URL 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 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.

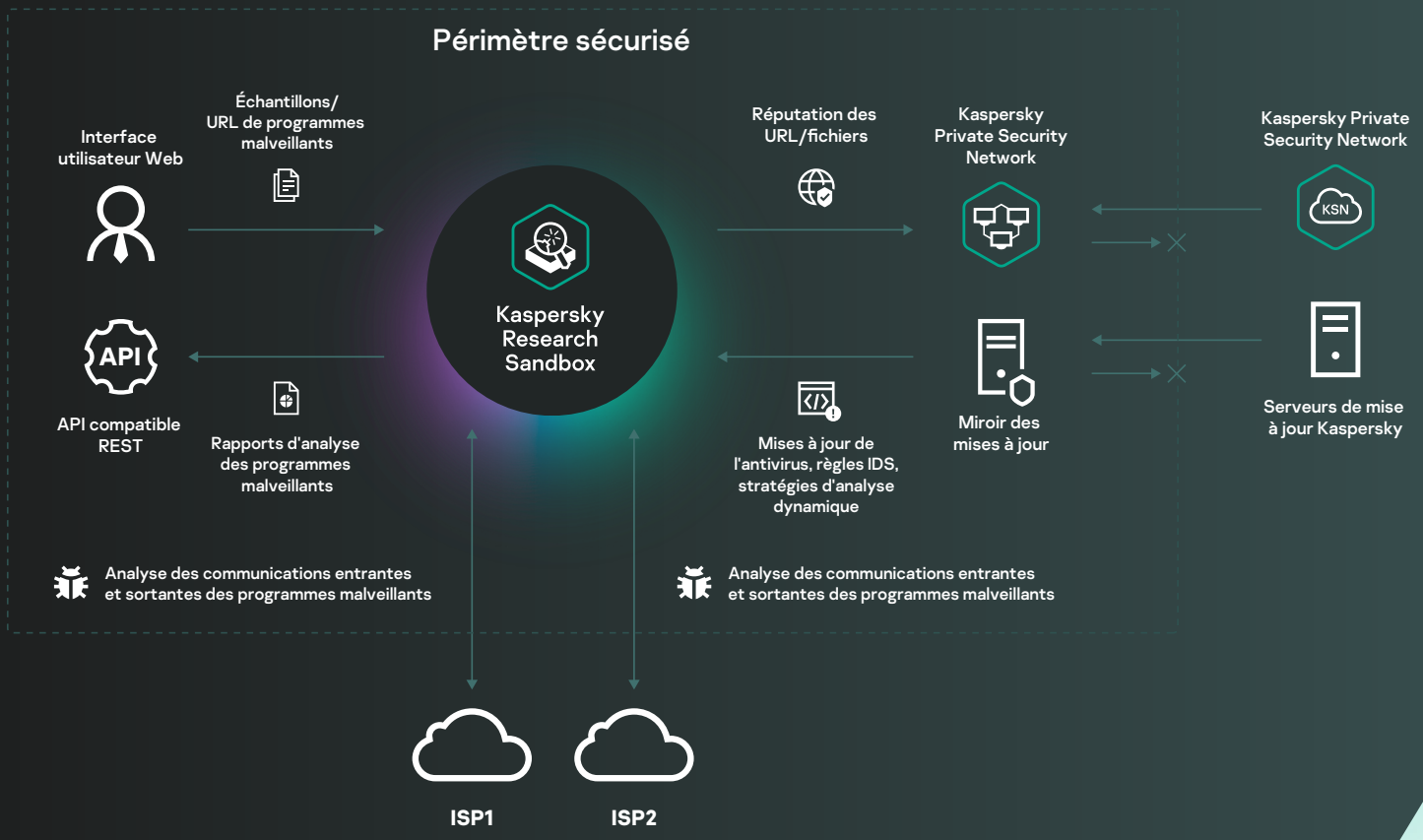
Kaspersky Research Sandbox est un dérivé direct de notre ensemble de sandboxes interne, une technologie qui évolue depuis plus de dix ans. Elle intègre toutes les connaissances sur les comportements malveillants acquises par Kaspersky par le biais de sa recherche continue sur les menaces, ce qui permet de détecter plus de 350 000 nouveaux objets 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. Kaspersky 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.

Caractéristiques principales du produit

- Analyse d'objets automatisée dans les environnements Windows, Linux et Android
- Les images personnalisées permettent d'effectuer une analyse des menaces sur les systèmes d'exploitation et les environnements Windows (uniquement ceux qui s'appliquent à des environnements réels)
- Le score de menaces basé sur les mesures et les données obtenues lors de l'exécution du fichier indique le niveau de danger de l'objet analysé
- Déploiement sur site permettant de ne pas exposer les données à l'extérieur de l'organisation
- Technologies avancées d'anti-évasion et de simulation humaine
- Envoi manuel de fichiers/d'URL et API RESTful
- Prise en charge de l'analyse de plus de 100 types de fichiers avec des rapports d'analyse détaillés
- Il est possible d'ajouter des règles Suricata personnalisées pour analyser le trafic réseau et de les utiliser avec les règles Suricata prêtes à l'emploi fournies
- Le produit prend en charge les déploiements sans système d'exploitation et peut être évoluer facilement selon les performances requises

Architecture de haut niveau de Kaspersky Research Sandbox



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.

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

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. Dans ce cas, 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. 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.

Rapports d'analyse des programmes malveillants

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 l'exécution d'un fichier/les résultats de navigation vers une URL

Noms des détections

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 Suricata 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 et des relations entre elles.

Activités suspectes

Liste des activités suspectes répertoriées.

Captures d'écran

Ensemble des captures d'écran effectuées durant l'exécution du fichier ou la navigation vers l'URL.

Images PE chargées

Liste des images PE chargées qui ont été détectées durant l'exécution du fichier ou de la navigation vers l'URL.

Opérations sur le fichier

Liste des opérations sur le fichier qui ont été répertoriées durant l'exécution du fichier ou la navigation vers l'URL.

Opérations sur le registre

Liste des opérations effectuées sur le registre du système d'exploitation qui ont été détectées durant l'exécution du fichier ou la navigation vers l'URL.

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 enregistrées durant l'exécution du fichier ou la navigation vers l'URL.

Téléchargement de fichiers

Liste de fichiers qui ont été extraits du trafic réseau durant l'exécution du fichier ou la navigation vers l'URL.

Fichiers déposés

Liste des fichiers qui ont été enregistrés (créés ou modifiés) pa le fichier exécuté.

HTTPS/HTTP/DNS/IP/ TCP/UDP, etc.

Sessions réseau/détails des demandes qui ont été enregistrées durant l'exécution du fichier ou la navigation vers l'URL.

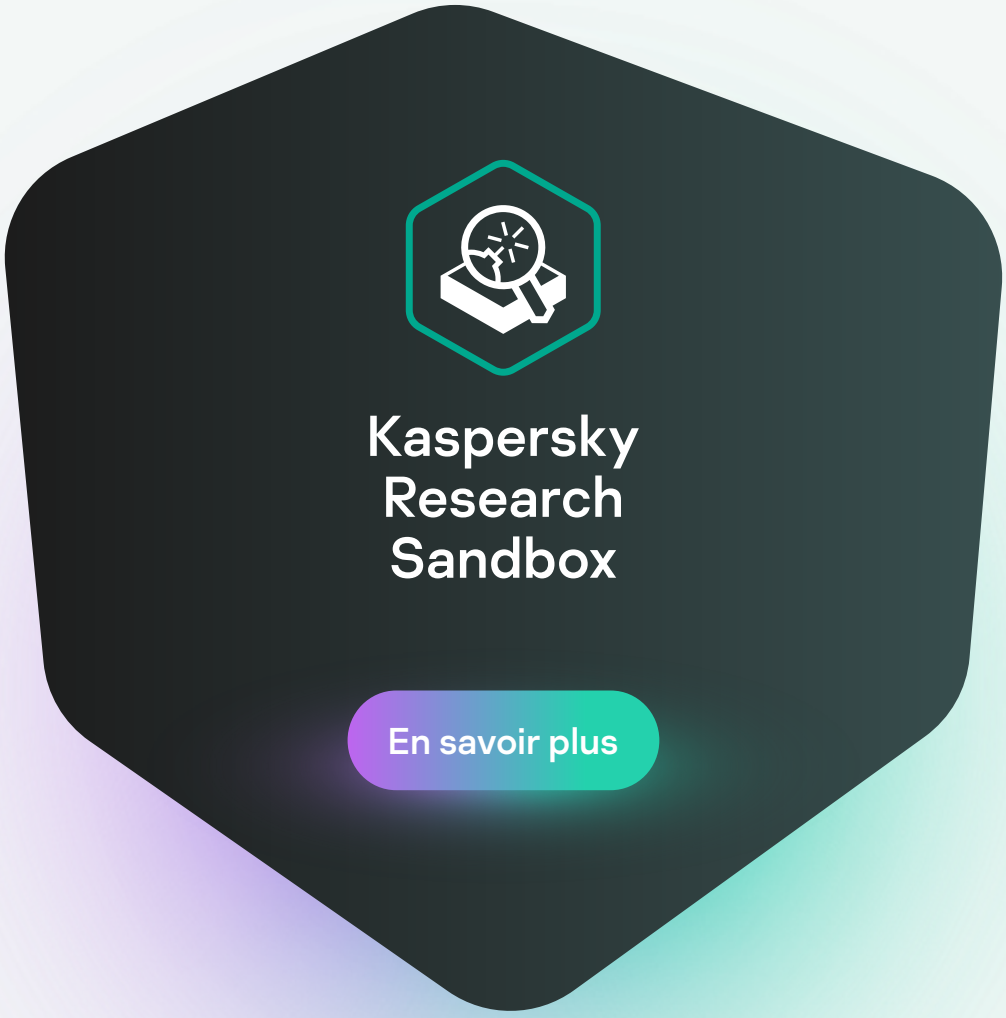
Décharge de trafic réseau (PCAP)

Activité réseau pouvant être exportée au format PCAP.

Matrice MITRE ATT&CK

Toutes les activités de traitement identifiées et enregistrées pendant l'émulation sont présentées sous la forme d'une matrice MITRE ATT&CK.

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.



www.kaspersky.fr