Kaspersky Threat Lookup

kaspersky BRING ON THE FUTURE

Kaspersky Threat Lookup

La cybercriminalité ne connaît pas de frontières et les capacités techniques sur lesquelles elle s'appuie évoluent rapidement : nous assistons à des attaques qui sont de plus en plus sophistiquées, les cybercriminels ayant recours à des ressources du Dark Web pour menacer leurs cibles. La fréquence, la complexité et l'obfuscation des cybermenaces ne cessent de croître. Et les cybercriminels utilisent de nouveaux moyens pour affaiblir vos défenses. Chaînes de frappe complexes et TTP (Tactiques, Techniques et Procédures) personnalisées font désormais partie de leurs méthodes pour paralyser votre activité, dérober vos ressources et attaquer vos clients.

Kaspersky Threat Lookup fournit toutes les connaissances acquises par Kaspersky sur les cybermenaces et leurs liens, regroupées dans un service Web unique et efficace. Le but est de fournir à vos équipes de sécurité autant d'informations que possible, afin de contrer les cyberattaques avant qu'elles n'aient un impact sur votre entreprise. La plateforme récupère les dernières informations détaillées de Threat Intelligence sur les URL, les domaines, les adresses IP, les hachages de fichiers, les noms des menaces, les données statistiques/comportementales, les données WHOIS/DNS, les attributs de fichiers, les données de géolocalisation, les chaînes téléchargées, les horodatages, etc. Il en résulte une visibilité globale sur les menaces nouvelles et émergentes pour sécuriser votre entreprise et améliorer la réponse aux incidents.

Bénéfices

Informations de confiance : un des principaux atouts de Kaspersky Threat Lookup est la fiabilité de notre Threat Intelligence, ces informations sont enrichies d'un contexte exploitable, ce qui constitue un soutien pour des actions concrètes. Les produits de Kaspersky arrivent en tête dans les tests anti-malware[1] et démontrent la qualité inégalée de nos renseignements sur la sécurité en offrant les taux de détection les plus élevés, avec un nombre de faux positifs quasi nul

Recherche des menaces (Threat hunting) : faites preuve de proactivité dans la prévention, la détection et la réaction face aux attaques afin de minimiser leur impact et leur fréquence. Suivez et éliminez avec fermeté les attaques le plus tôt possible. Plus tôt vous détectez une menace, moins il y a de dommages et plus rapides sont les réparations ainsi que le retour à la normale des opérations de réseau

Investigations sur les incidents : un graphique de recherche dope les investigations sur les incidents en vous permettant d'explorer visuellement les données et détections stockées dans Threat Lookup. Il nous fournit une visualisation graphique de la relation entre les URL, les domaines, les IPs, les fichiers et d'autres contextes afin d'avoir une meilleure compréhension de la totalité d'un incident et d'identifier son origine

Recherche maître : cherchez de l'information parmi tous les produits actifs threat Intelligence et ressources externes (notamment OSINT IoCs, Dark Web et Surface Web) dans une seule puissante interface

Interface Web conviviale ou API compatible REST : vous pouvez choisir d'utiliser le service en mode manuel par l'intermédiaire d'une interface Web (avec un navigateur Web) ou d'y accéder via une simple API compatible REST

Large éventail de formats d'exportation :exportez les indicateurs de compromission (IOC) ou le contexte exploitable dans des formats de partage largement utilisés et mieux organisés, interprétables par une machine, tels que STIX, OpenIOC, JSON, Yara, Snort ou même CSV, afin de profiter pleinement des avantages de la Threat Intelligence, d'automatiser les processus d'opérations, ou de les intégrer dans des contrôles de sécurité tels que SIEM

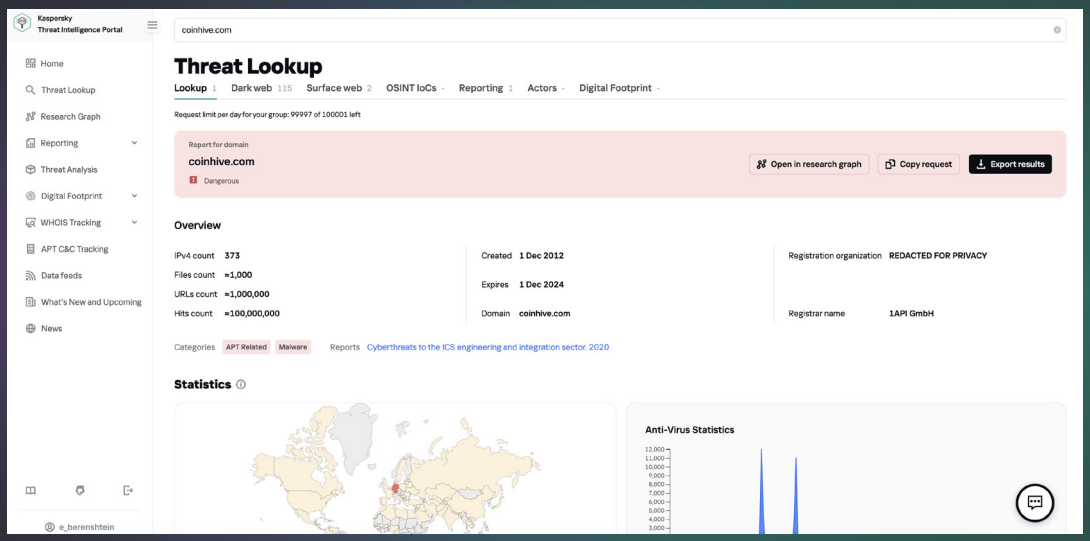
Avantages

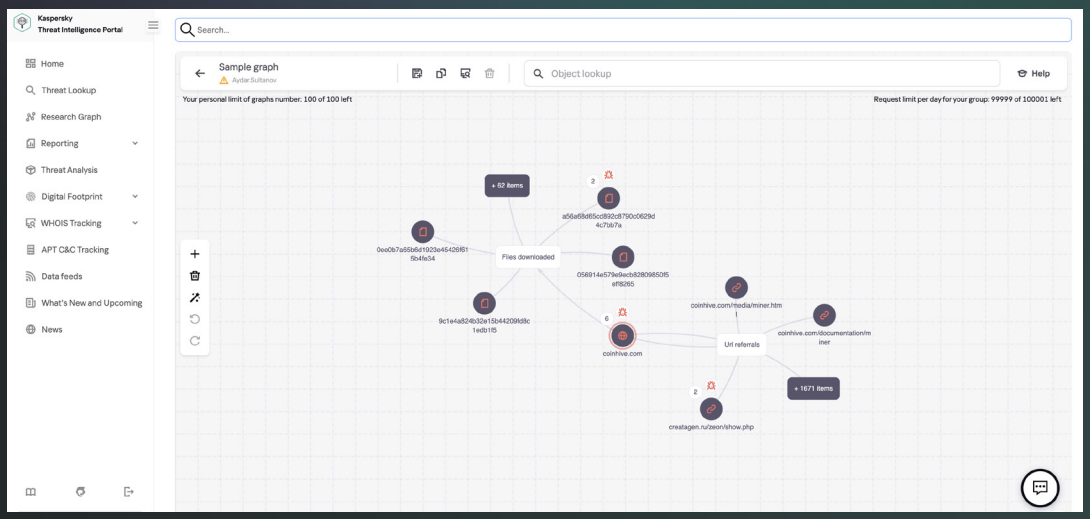
Examiner de manière approfondie les indicateurs de menace dotés d'un contexte hautement validé afin de hiérarchiser les attaques et de mettre l'accent sur l'atténuation des menaces les plus dangereuses pour votre entreprise

Diagnostiquer et analyser les incidents de sécurité sur les hébergeurs et le réseau plus efficacement, et hiérarchiser les signaux des systèmes internes contre des menaces inconnues

Doper vos capacités de réponse aux incidents et de recherche des menaces pour briser la chaîne de frappe avant que des données et des systèmes sensibles ne soient compromis

[1] kaspersky.fr/top3





Maintenant, c'est possible

Rechercher des indicateurs de menace via une interface Web ou une API compatible REST

Examiner les informations détaillées (certificats, noms couramment utilisés, chemins d'accès aux fichiers, URL associées) pour identifier de nouveaux objets suspects

Vérifier si l'objet en question est répandu ou unique

Comprendre dans quelle mesure un objet particulier doit être considéré comme malveillant

www.kaspersky.fr