Kaspersky APT Intelligence Reporting

kaspersky BRING ON THE FUTURE

Kaspersky APT Intelligence Reporting

Les clients de rapports de surveillance des APT de Kaspersky accèdent 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 ne seront jamais rendues publiques. Les rapports contiennent un résumé analytique offrant des informations faciles à comprendre destinées aux cadres supérieurs ainsi qu'une description détaillée de l'APT, des règles Yara et des indicateurs IOC associés pour fournir aux experts en sécurité, aux analystes de programmes malveillants, aux ingénieurs en sécurité, aux analystes de la sécurité des réseaux et aux experts en matière d'APT des conseils exploitables afin d'assurer une protection supérieure.

Nos experts vous alerteront de suite s'ils constatent une modification dans les stratégies des groupes de cybercriminels. Vous aurez également accès à tous les rapports des bases de données d'APT de Kaspersky, un autre outil de recherche et d'analyse puissant venant compléter votre arsenal de sécurité.

Avantages

Enrichi avec les données

Toutes les TTP décrites dans les rapports sont cartographiées dans le cadre MITRE ATT&CK, améliorant ainsi la détection et la réponse grâce au développement et à la hiérarchisation des cas d'utilisation de surveillance sécurisée correspondants, ainsi qu'aux analyses d'écarts et aux tests des moyens de défense actuels contre les TTP pertinentes

Information sur les APT privées

Pour plusieurs raisons, toutes les menaces les plus graves ne sont pas révélées publiquement. Mais nous les partageons toutes avec nos clients

Accès privilégié

Recevez des descriptions techniques sur les dernières menaces pendant les enquêtes, avant leur révélation au grand public

Analyse rétrospective

Accès garanti à tous les rapports privés précédents durant toute la période de votre abonnement

Un accès aux données de l'entreprise...

Une documentation technique détaillée, avec une liste complète d'IOC, dans des formats standard tels qu'OpenIOC ou STIX, en plus de l'accès à nos règles YARA

Profils de criminels

Notamment le pays d'origine et la principale activité suspectés, familles de programmes malveillants utilisées, secteurs et régions visés, et descriptions de toutes les TTP utilisées dans le cadre MITRE ATT&CK

Une surveillance continue des campagnes d'APT

Accès aux informations exploitables au cours de l'enquête avec (information sur la distribution des menaces APT, les indicateurs IOC, les infrastructures de commande et de contrôle, etc.

API compatible REST

Intégration transparente et automatisation de vos flux de travail de sécurité

www.kaspersky.fr