NE SOYEZ PAS PRIS EN OTAGE ! PROTÉGEZ VOTRE ENTREPRISE DÈS AUJOURD'HUI

POURQUOI CHOISIR LA PROTECTION KASPERSKY LAB CONTRE LES RANSOMWARES ?

LA PROBLÉMATIQUE

L'année 2016 a été l'année de la révolution des ransomwares qui ont ensuite poursuivi leurs méfaits dans le monde entier, ciblant les données, les appareils, les entreprises et les utilisateurs individuels. Elle a également été marquée par une augmentation des menaces liées aux programmes malveillants de crypto-verrouillage visant les entreprises, si bien que ces derniers sont devenus l'un des 3 problèmes de sécurité informatique les plus inquiétants pour les PME.

2016 EN CHIFFRES

20 % **DES SOCIÉTÉS DANS LE MONDE** ont été victimes d'un incident de sécurité informatique lié à une attaque par ransomware.*

42 % **DES PETITES ET MOYENNES ENTREPRISES** ont été attaquées par un ransomware au cours des 12 derniers mois.

UNE ENTREPRISE A ÉTÉ ATTAQUÉE par un ransomware toutes les **40 secondes**

C'EST LE COÛT MOYEN DES dommages causés par une attaque par programme malveillant de crypto-verrouillage sur une PME. **99 000 €**

67 % **C'EST LE NOMBRE APPROXIMATIF DE REPRÉSENTANTS DE PME** ayant déclaré une perte totale ou partielle des données de leur entreprise à cause d'un programme malveillant de crypto-verrouillage.

1 sur 5 **C'EST LA PROPORTION DE PME AYANT VERSÉ LA RANÇON QUI LEUR ÉTAIT DEMANDÉE**, mais n'ayant jamais récupéré leurs données.

1 445 434 **PC UTILISATEURS UNIQUES** ont été la cible de crypto-virus.

62 **NOUVELLES FAMILLES DE RANSOMWARES** ont fait leur apparition.

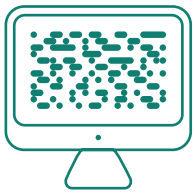
Enquête 2016 sur les risques liés à la sécurité informatique pour les entreprises

LA SOLUTION

En 2014, peu de temps après la propagation épidémique des attaques par ransomware, les produits Kaspersky Lab ont été améliorés et dotés de fonctionnalités de lutte contre les programmes malveillants de crypto-verrouillage. Depuis, notre gamme de technologies contre les ransomwares s'est considérablement développée pour faire face à cette menace en constante évolution.

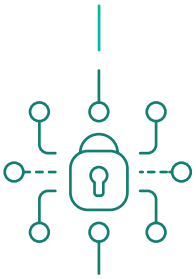
PROTECTION MULTICOUCHE DE KASPERSKY LAB

Les solutions de sécurité de Kaspersky Lab fournissent une protection multicouche contre les programmes malveillants de crypto-verrouillage, qui exploite des éléments et des technologies d'infrastructure pour bloquer les ransomwares.



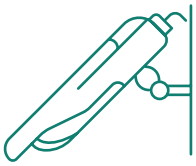
L'association de technologies de détection d'une grande précision basées sur l'utilisation d'une liste noire et d'une fonctionnalité d'apprentissage automatique proactif, qui exploitent les capacités de traitement du big data de Kaspersky Security Network (KSN), permet de proposer une identification fiable des programmes malveillants, ainsi qu'une protection efficace contre les menaces connues, inconnues ou avancées.

Les contrôles de sécurité, notamment les contrôles au démarrage des appareils, des applications et du Web, vous permettent de restreindre l'utilisation d'appareils et de sites Web non sollicités ou le lancement d'applications non autorisées ou non fiables, ce qui limite les possibilités d'attaques de la part de programmes malveillants, y compris des crypto-virus.



Il est possible de configurer le contrôle des privilèges des applications afin de limiter les droits d'accès des applications à certaines ressources, y compris aux fichiers système et utilisateur. Ainsi, le ransomware n'est pas en mesure de les chiffrer, car il ne possède pas les droits en « écriture ».

La technologie de protection automatique contre les Exploits surveille en permanence les programmes malveillants pour s'assurer qu'ils ne peuvent pas exploiter les vulnérabilités du système d'exploitation ou des applications fréquemment ciblées.



La surveillance du système suit les processus d'application et compare leur comportement à des schémas d'activités dangereuses connus. Cela permet de détecter et de bloquer les actions d'applications malveillantes. Lorsqu'une tentative de chiffrement est détectée, la surveillance du système créé une sauvegarde temporaire des fichiers consultés afin de supprimer toutes les actions malveillantes et de restaurer les informations.

La technologie de lutte contre les programmes de cryptage basée sur le serveur Kaspersky Lab entre en action lorsqu'une tentative de chiffrement est détectée sur un poste de travail infecté au niveau du réseau local : lorsqu'un crypto-virus tente de chiffrer des fichiers sur des ressources partagées, comme les serveurs d'une société, cette fonctionnalité bloque l'accès du poste de travail infecté aux ressources partagées afin d'interrompre le processus de chiffrement.

Les fonctions d'évaluation de la vulnérabilité et de gestion des correctifs de Kaspersky Endpoint Security Business contribuent à une sécurité renforcée, grâce à l'automatisation du processus d'atténuation des vulnérabilités logicielles. Ce dispositif limite la possibilité pour tous les types de programmes malveillants de parvenir à pénétrer au sein de votre réseau informatique.

UNE PROTECTION ÉPROUVÉE CONTRE LES RANSOMWARES

VALIDÉE PAR LES CLIENTS QUI L'ONT ADOPTÉE

COLLEZIONE, l'une des marques de mode leaders en Turquie utilise Kaspersky Endpoint Security for Business Advanced.

« Nous avons été particulièrement impressionnés par le fait que cette protection anti-ransomware se soit montrée efficace lors de tous nos tests », se souvient Gökhan Zengin, responsable informatique de Collezione.

JJW HOTELS, une société gérant des hôtels et centres de loisirs souvent récompensée, utilise Kaspersky Endpoint Security for Business Select.

D'après Tiago Reis, responsable de l'infrastructure informatique du groupe MBI International, « depuis que nous avons installé Kaspersky Lab, nous n'avons eu aucun problème lié aux ransomwares ou à d'autres types d'attaque ».

Outil Kaspersky contre les ransomwares

Site Entreprises Kaspersky Lab

Blog B2B de Kaspersky Lab