KASPERSKY lab

# NE RIEN LAISSER AU HASARD : COMBATTRE LES RANSOMWARES SUR LES STATIONS DE TRAVAIL ET LES SERVEURS

www.kaspersky.fr

*Les ransomwares sont l'une des catégories de logiciels malveillants qui se développent le plus. Les pirates n'ont même pas besoin de voler et revendre les données dont vous ou votre entreprise dépendez. Ils se contentent de les chiffrer et demandent une rançon. Au fil des années, les ransomwares sont passés de simples verrouilleurs d'écran qui demandaient de l'argent aux victimes à une immense vague de logiciels beaucoup plus dangereux. Dans votre lutte contre les programmes malveillants de type CryptoLocker, vous ne pouvez pas vous permettre de laisser quoi que ce soit au hasard.*

# POURQUOI LES RANSOMWARES SONT-ILS SI PROBLÉMATIQUES ?

Comment fonctionnent-ils et pourquoi sont-ils si nocifs ? La catégorie « programmes malveillants » repose maintenant sur des **malwares de chiffrement**, des chevaux de Troie qui s'infiltrent dans votre système lorsque vous ouvrez une pièce jointe malveillante dans un e-mail ou suivez sans le savoir un lien vers un site Web spécial. Le module chiffre ensuite discrètement les données qu'il trouve et qui pourraient avoir de la valeur pour vous. Cela peut inclure vos photos personnelles, archives, documents, bases de données, graphiques, etc. Les programmes malveillants de type CryptoLocker demandent ensuite un paiement (souvent une somme considérable) pour déchiffrer ces fichiers à nouveau.

L'anonymat est très important pour les pirates. Le paiement peut donc être sollicité via Bitcoin et les serveurs de commande et de contrôle des pirates peuvent être dissimulés dans le réseau Tor, qui est anonyme. Si du trafic est intercepté entre le cheval de Troie et son serveur, l'utilisation de modèles cryptographiques non conventionnels tels que Tor ou des algorithmes de chiffrement courants rendent le déchiffrage de fichiers impossible (Trojan-Ransom.Win32.Onion, par exemple, utilise toutes ces techniques).

De nos jours, certains programmes malveillants de type CryptoLocker demandent à recevoir un paiement non seulement pour déchiffrer les données des utilisateurs mais également pour des « services » supplémentaires. Par exemple, le pirate peut mettre la barre encore plus haut en effectuant un chantage : « Payez ou nous pourrons nous retrouver dans l'obligation d'envoyer tout votre historique de navigation à tous vos contacts. »

# À QUEL POINT LES RANSOMWARES SONT-ILS RÉPANDUS ?

| Ransomwares détectés (en utilisant Kaspersky Security Network) | |
|---|---|
| 2014 | 121 238 |
| 2015 | 448 430 |
| Total | 554 267 |

En 2015, le nombre total d'attaques par des ransomwares que nous avons détectées via notre Kaspersky Security Network était presque quatre fois plus élevé qu'en 2014, avec près de **quatre-cent cinquante mille détections**. Il en existe de nombreux types et familles différentes, tels que CryptoWall, TeslaCrypt, TorrentLocker et Locky. CTB-Locker, ACCDFISA et GpCode font partie des plus connus. Les données provenant de Kaspersky Security Network (ci-dessous) donnent une idée de l'échelle des différentes attaques par des ransomwares dans l'Union européenne en 2015 :

| Verdict de Kaspersky Lab | Utilisateurs uniques (KSN) | Utilisateurs uniques (KSN) combinés | Autres alias connus pour ce programme malveillant |
|---|---|---|---|
| Trojan-Downloader.JS.Cryptoload<br>+ Trojan-Ransom.Win32.Bitman | 80 017<br>1 163 | 81 180 | TeslaCrypt |
| Trojan-Ransom.NSIS.Onion<br>+ Trojan-Ransom.Win32.Onion | 16 491<br>8 571 | 25 062 | CTB-Locker |
| Trojan-Ransom.Win32.Cryptodef | 7 346 | 7 346 | CryptoDefense (premières versions), CryptoWall (dernières versions) |
| Trojan-Ransom.Win32.Snocry | 4 998 | 4 998 | |
| Trojan-Ransom.Win32.Cryakl | 4 955 | 4 955 | |
| Trojan-Ransom.Win32.Crypren | 1 681 | 1 681 | |
| Trojan-Ransom.Win32.Shade | 1 390 | 1 390 | |
| Trojan-Ransom.Win32.Crypmod | 1 173 | 1 173 | |
| Trojan-Ransom.Win32.Rack | 717 | 717 | TorrentLocker |
| Trojan-Ransom.Win32.CryFile | 395 | 395 | |

**Locky**, qui est susceptible d'avoir été utilisé lors de la récente attaque ransomware contre le Hollywood Presbyterian Memorial Hospital, est apparu mi-février 2016 et est déjà l'un des principaux ransomwares en circulation.

**TeslaCrypt** : des échantillons ont d'abord été détectés en 2015 et ce ransomware ne cesse d'évoluer pour éviter d'être détecté. Dans les médias, TeslaCrypt a beaucoup été décrit comme la « malédiction » des gamers parce qu'il cible de nombreux types de fichiers liés à des jeux vidéo (sauvegardes, profils d'utilisateur, etc.). Ce cheval de Troie cible les États-Unis, l'Allemagne, l'Espagne et d'autres pays.

# SOLUTIONS DE SÉCURITÉ INFORMATIQUE

Malgré tous les mécanismes avancés mis en place dans les programmes malveillants actuels, vous pouvez limiter considérablement les menaces que présentent les ransomwares pour vous et votre entreprise. La stratégie anti-ransomware de Kaspersky Lab utilise un certain nombre de contremesures pour les programmes malveillants de type CryptoLocker.

Votre **solution de sécurité doit être active** à tout moment et doit disposer d'autant de niveaux de protection que possible. Elle **doit également être à jour**.

Actuellement, il est impossible de déchiffrer des fichiers correctement chiffrés par des programmes malveillants modernes de type CryptoLocker. Le seul moyen de protéger vos données en cas d'attaque réussie est donc d'effectuer une sauvegarde de vos fichiers. Mais une **sauvegarde générale** (par exemple avec Acronis ou d'autres produits spécialisés), même effectuée régulièrement, ne suffit pas car les fichiers récemment modifiés restent non protégés et la sauvegarde risque d'être écrasée par les fichiers chiffrés.

## Solutions hébergées sur l'hôte

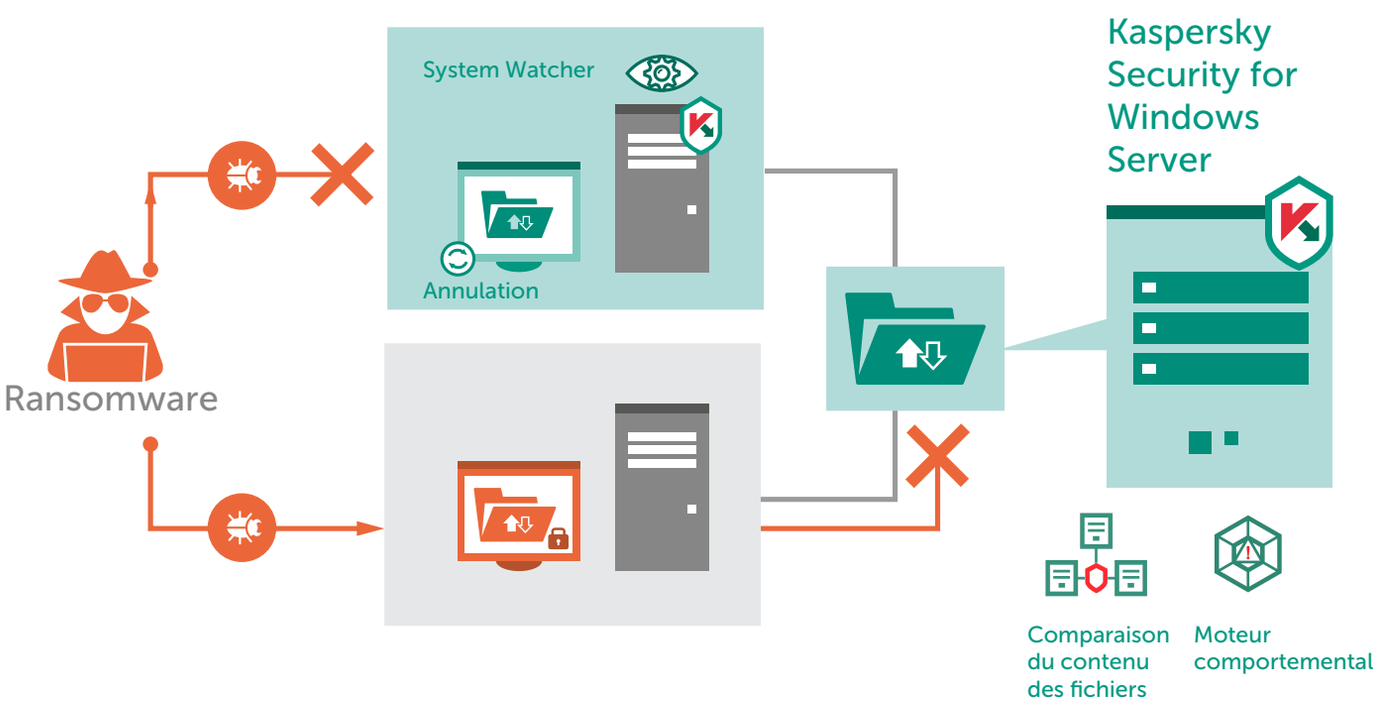
C'est l'une des raisons pour lesquelles les produits Kaspersky Lab intègrent la technologie Kaspersky System Watcher. Kaspersky System Watcher est une solution hébergée sur l'hôte qui analyse les données d'événements pertinentes du système, y compris les informations relatives à la modification des fichiers. Lorsqu'elle détecte qu'une application suspecte tente d'ouvrir les fichiers personnels d'un utilisateur, elle effectue immédiatement une copie de sauvegarde locale protégée de ces derniers. Si l'application s'avère être un programme malveillant de type CryptoLocker (ou autre type de programme malveillant), Kaspersky System Watcher annule automatiquement les modifications non sollicitées. Vous recevez simplement des notifications vous indiquant ce qu'il se passe. Il n'y a pas d'interruption ou d'action à mener.

Kaspersky System Watcher protège les données des utilisateurs et empêche les cybercriminels de gagner de l'argent en recevant des rançons qui alimentent leur secteur et permettent de créer encore plus de programmes malveillants.
Autre approche de Kaspersky Lab, hébergée sur hôte et permettant de limiter les risques liés aux programmes malveillants de type CryptoLocker : la création de règles de contrôle au démarrage des applications, qui empêchent le lancement d'applications non autorisées.

## Solution anti-ransomware sur serveur

Au sein du périmètre de sécurité, certains hôtes utilisent des dossiers SMB/CIFS partagés sur des serveurs d'entreprise. Tous les hôtes ne disposent pas d'une version activée de System Watcher. Certains peuvent même ne pas être protégés ou l'être par un autre logiciel qui ne dispose pas d'une fonctionnalité anti-ransomware. Si c'est le cas, tout malware de chiffrement entrant dans le système via un e-mail ou un navigateur vulnérable affectera également les dossiers partagés sur les serveurs d'entreprise. Dans ce scénario, seul un **logiciel de sécurité côté serveur** peut protéger les données.

La fonctionnalité anti-ransomware de Kaspersky Lab n'est pas fournie uniquement pour les terminaux : elle l'est également pour les serveurs Windows. Notre solution Kaspersky Security for Windows Server comprend un nouveau niveau de protection spécialement développé pour se protéger contre les malwares de chiffrement. Elle surveille les dossiers de données sélectionnés (y compris les partages de fichiers) et **compare les contenus de chaque fichier avant** et après toute tentative d'accès. Bien sûr, les programmes malveillants de type CryptoLocker modifient considérablement le contenu des fichiers, puisqu'ils sont chiffrés ! Ce mécanisme détecte donc presque toujours la présence de ransomware et bloque leur exécution.




En plus de sa fonction de **détection**, Kaspersky Security for Windows Server dispose d'un mécanisme de prévention. Bien que les protocoles SMB/CIFS ne puissent nous fournir d'information concernant le processus sur l'hôte du ransomware, nous pouvons obtenir l'adresse IP de cet hôte. La technologie **Host Blocker** peut ensuite empêcher cet hôte infecté de mener d'autres actions dans les dossiers partagés.

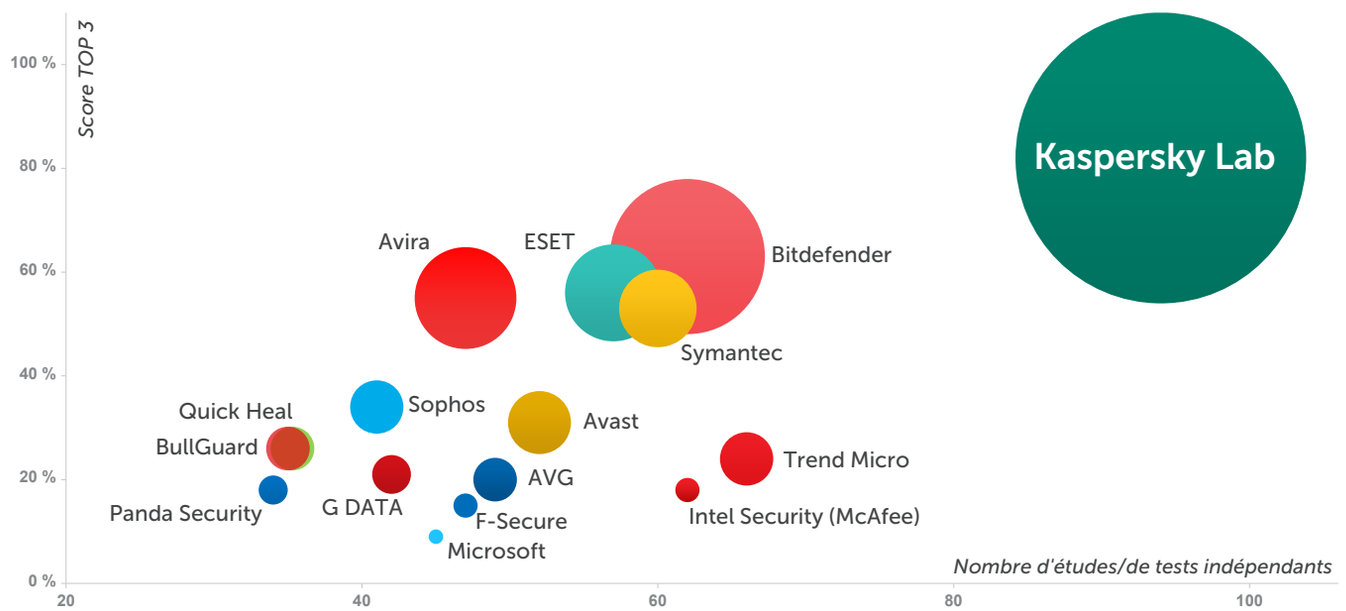
Certaines organisations peuvent décider, à juste titre, de chiffrer des dossiers sur certains serveurs dans le cadre de leur propre politique de sécurité. Kaspersky Security for Windows Server permet à l'administrateur d'ajouter des exceptions pour les répertoires dans lesquels ce chiffrement est mis en place.

# Ne rien laisser au hasard – se protéger contre les ransomwares avec Kaspersky Lab

De nouvelles menaces ne cessent d'émerger et Kaspersky Lab s'engage à suivre le rythme en fournissant une protection multi-niveaux pour protéger ses clients.
Nous sommes en mesure de limiter les problèmes générés par les ransomwares autant sur les stations de travail (Kaspersky System Watcher) que côté serveur (technologie anti-ransomware intégrée à Kaspersky Security for Windows Server).

Kaspersky Lab renouvelle constamment son arsenal de technologies grâce à sa veille stratégique éprouvée. Nous prouvons également nos déclarations concernant notre performance en présentant les résultats de tests indépendants et l'avis de cabinets d'analyse (TOP3).

**En 2015, les produits Kaspersky Lab ont fait l'objet de 94 études et tests indépendants. Nos produits ont reçu 60 premiers prix et ont figuré 77 fois parmi les trois premiers.**




1

Consultez toutes les informations concernant l'indicateur TOP3 ici
[www.kaspersky.fr/top3](www.kaspersky.fr/top3)