Acronis Active Protection

Protégez-vous contre les pertes de données dues aux attaques par ransomware

Disponibilité permanente de vos données dans un paysage des menaces en constante évolution

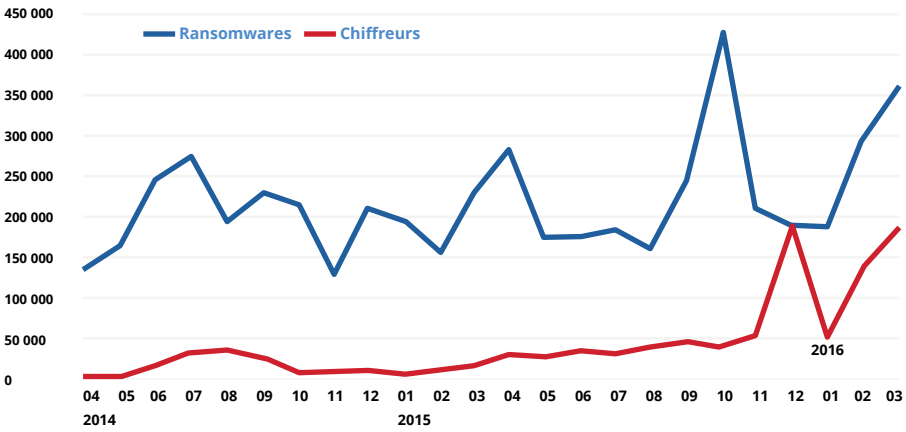
D'après Osterman Research, 47 % des entreprises ont déjà été la cible d'attaques par ransomware. Il ne fait d'ailleurs aucun doute que les attaques du ransomware WannaCry en mai 2017 ont probablement fait grimper ces statistiques partout dans le monde. Malheureusement, le ransomware a encore de beaux jours devant lui.

À l'avenir, il est bien possible que les auteurs d'attaques par ransomware menacent tout simplement d'altérer les données de documents pris au hasard pour mettre leur victime dans l'embarras. Mais que savez-vous réellement des ransomwares ?

Qu'est-ce qu'un ransomware ?

Un ransomware, ou logiciel de demande de rançon, est un type de logiciel malveillant qui bloque l'accès à l'équipement qu'il infecte, ou à tout ou partie des informations qu'il contient. Pour pouvoir à nouveau disposer de l'équipement ou des données, la victime doit s'acquitter d'une rançon, souvent libellée dans une monnaie électronique courante. On distingue essentiellement deux types de ransomware : les bloqueurs d'écran (qui bloquent l'accès au système d'exploitation ou au navigateur au moyen d'une fenêtre pop-up) et les ransomwares de chiffrement. Ce terme s'applique également aux chevaux de Troie de type « Trojan-Downloader » qui servent à télécharger un ransomware de chiffrement une fois la machine infectée. De nos jours, le terme ransomware est devenu synonyme de ransomware de chiffrement.

Les graphiques ci-dessous illustrent bien l'essor du ransomware. Les acteurs de la lutte antimalware, notamment le FBI et d'autres organismes similaires, s'accordent à dire que ce type de menace continuera à proliférer, en particulier dans le monde des petites et moyennes entreprises.



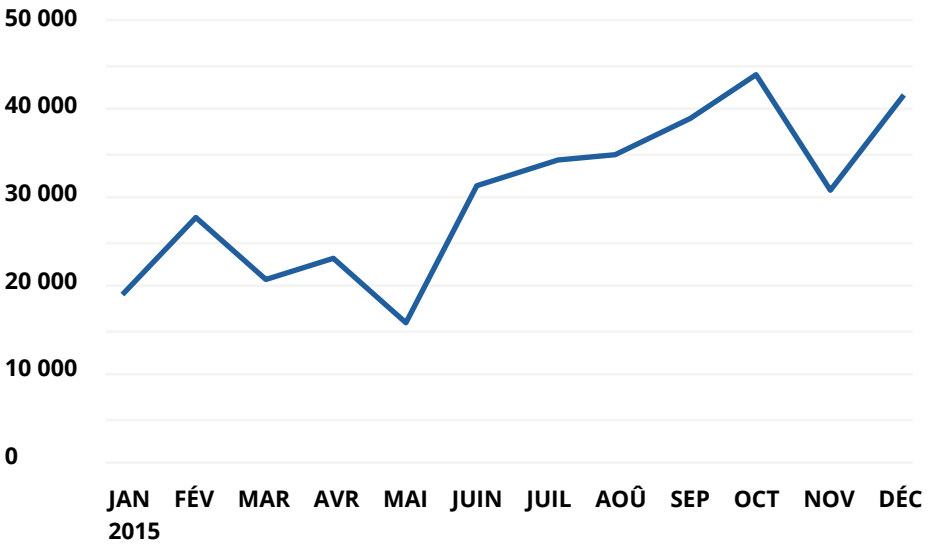
Données tirées d'un rapport récent de Kaspersky Lab (https://securelist.com/files/2016/06/KSN_Report_Ransomware_2014-2016_final_ENG.pdf)

PRINCIPAUX POINTS À RETENIR

Acronis Active Protection est une technologie de protection des données de nouvelle génération qui s'appuie sur l'expertise d'Acronis en matière de sauvegardes :

- Elle assure une protection en temps réel des sauvegardes contre les ransomwares. Ainsi, vous ne perdez pas de données en cas d'attaque.
- Elle protège vos données, vos fichiers de sauvegarde et l'application de sauvegarde elle-même, même en cas de nouvelle variante de ransomware encore non identifiée.
- Elle est simple à utiliser : intuitive et entièrement transparente, elle fonctionne pratiquement de manière automatique.

Acronis Active Protection ajoute une couche de protection des données renforcée, de façon à les prémunir contre les ransomwares actuels et les variantes à venir.



Données tirées d'un rapport récent de Symantec (https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf)

ACRONIS ACTIVE PROTECTION™ : UNE RÉPONSE EFFICACE AUX ATTAQUES PAR RANSOMWARE

Acronis Active Protection est une technologie avancée conçue pour les systèmes d'exploitation Windows. Acronis envisage d'étendre cette technologie aux équipements Android et éventuellement à d'autres systèmes d'exploitation mobiles et de bureau.

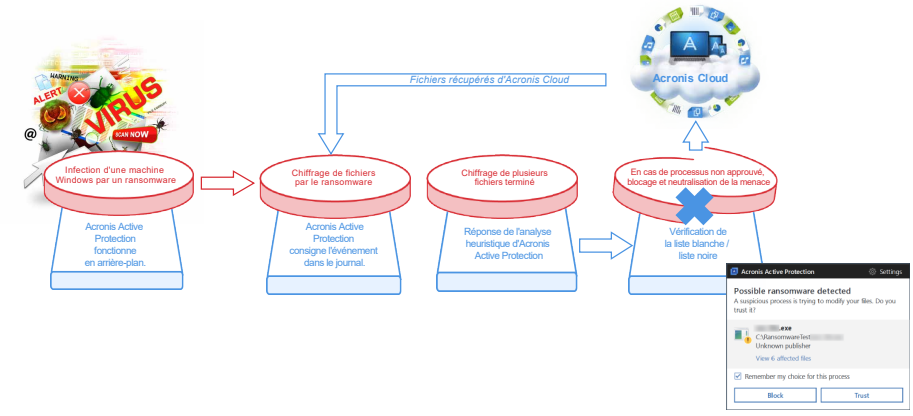
Acronis Backup 12.5 et la technologie Acronis Active Protection, en attente de brevet, constituent le fondement d'un plan robuste de continuité des activités.

Il est important de bloquer une attaque par ransomware à un stade précoce. Ce type d'attaque doit être mis en échec au niveau du poste de travail, de préférence avant que le ransomware ait pu chiffrer des fichiers. Il est donc essentiel de bien cerner la menace et d'implémenter des solutions permettant à l'équipe de sécurité de réagir rapidement à une attaque par ransomware, sans perturber le fonctionnement des postes de travail, du réseau ou des utilisateurs connectés au réseau. Il s'agit là d'une condition essentielle pour les utilisateurs en entreprise, mais aussi pour les particuliers.
Acronis a la solution pour combattre efficacement les ransomwares.

Cette technologie est disponible dans les produits Acronis grand public (et le sera ensuite dans les produits pour entreprises), en combinaison avec un logiciel antimalware si vous le souhaitez.

La détection heuristique

Acronis Active Protection repose sur une approche heuristique dont vous avez peut-être entendu parler dans le contexte des solutions antimalware. La détection heuristique est à la fois plus moderne et sophistiquée que celle basée sur les signatures. Une signature ne peut déceler qu'un seul échantillon, tandis que l'analyse heuristique est capable de détecter plusieurs centaines



d'échantillons de fichiers appartenant à une famille de logiciels malveillants (aux comportements et séquences d'actions similaires). L'analyse heuristique comportementale consiste à comparer une séquence d'actions exécutée par un programme (plus précisément, des événements liés au système de fichiers) avec une séquence d'événements référencée dans une base de données de modèles de comportements malveillants.
Cette analyse est associée à une liste blanche et à une liste noire de divers programmes. La vérification de la liste blanche est importante. En effet, si les analyses heuristiques sont à même de détecter de nouvelles menaces, elles se fondent sur l'expérience et les données comportementales ; il faut donc les contrôler pour éviter les faux positifs. Les produits dotés d'Acronis Active Protection consultent donc la liste blanche et la liste noire lorsqu'ils détectent des processus suspects. Parallèlement, lorsqu'un utilisateur bloque un ransomware potentiel, ce dernier est ajouté à la liste noire, ce qui empêchera le lancement du programme malveillant lors du prochain redémarrage du système.
Ce principe a toute son importance, car il évite à l'utilisateur d'avoir à bloquer à nouveau le ransomware. Pour compromettre des sauvegardes, il semblerait logique que les pirates prennent directement pour cible Acronis True Image lui-même. Nous avons toutefois doté l'agent Acronis d'une fonctionnalité d'autoprotection, si bien qu'aucun processus du système, à l'exception du logiciel Acronis, ne peut modifier les fichiers de sauvegarde. Nous avons également implémenté des mécanismes d'autodéfense fiables qui neutraliseront toute attaque et empêcheront les cybercriminels d'interrompre l'action du logiciel Acronis ou de modifier le contenu des fichiers de sauvegarde.
De plus, Acronis Active Protection surveille le secteur de démarrage principal du disque dur installé sur la machine Windows de l'utilisateur et n'autorise aucune modification apportée par des utilitaires non répertoriés dans la liste blanche.

Acronis Active Protection fonctionne-t-il avec tous les types de fichiers ?

Absolument. Toutefois, une protection des données continue et active contre trois principaux vecteurs de menaces est nécessaire.

1. Attaques par ransomware ciblant des fichiers

En règle générale, on remédie à une telle attaque en se servant des fichiers sauvegardés précédemment pour restaurer les données compromises. Ce type d'attaque est désormais plus facile à contrer et ne se produira probablement jamais à grande échelle si vous possédez un produit doté de la technologie Acronis Active Protection. La restauration de fichiers chiffrés vers la dernière version se fait automatiquement (moyennant confirmation de l'utilisateur), car la technologie opère en temps réel. Imaginez une situation où une sauvegarde est planifiée pour minuit, mais l'ordinateur fait l'objet d'une attaque par ransomware à 11 h. Si l'utilisateur se contente de récupérer les fichiers d'une sauvegarde en ligne, il perd onze heures de travail. Grâce à la surveillance continue de l'activité des processus décrite ci-dessus, aucune donnée ne sera perdue en cas d'attaque par ransomware.

2. Attaque par ransomware d'un fichier de sauvegarde local

Dans ce cas de figure, Acronis Active Protection surveille activement tous les disques locaux pour empêcher la modification de fichiers de sauvegarde par un processus malveillant.

3. Modification de sauvegardes dans le Cloud par des processus malveillants

Les fichiers sauvegardés dans Acronis Cloud Storage bénéficient d'une protection exceptionnelle contre toute modification directe par un code malveillant, grâce à un chiffrement robuste de bout en bout et à la restriction des modifications de fichier au seul logiciel agent Acronis autorisé.

Type de comportement	Explication	Réponse d'Acronis Active Protection
Écrasement sur place	Le ransomware ouvre et modifie les fichiers de données sur place.	Le pilote transmet des notifications d'accès aux fichiers et des données heuristiques au service et effectue une copie sur écriture des activités suspectes. Le service détecte le cas, bloque le ransomware et le pilote restaure la dernière version du fichier à partir de son propre cache.
Modification du nom	Le ransomware ouvre, renomme et modifie des fichiers de données.	La procédure est la même que celle décrite ci-dessus.
Création d'un nouveau fichier	Le ransomware crée un nouveau fichier, copie le contenu original, modifie le nouveau fichier et supprime le fichier original.	La procédure est la même que celle décrite ci-dessus.
Écrasement du secteur de démarrage principal	Le ransomware ouvre le lecteur physique et écrase le secteur de démarrage principal, le système redémarre et le disque dur ou la table de fichiers maîtres sont chiffrés au redémarrage (Chkdsk masqué).	Le pilote surveille les opérations d'écriture/SCSI à destination de la table de fichiers maîtres via le système de fichiers RAW et avertit le service, qui vérifie le processus et prend une décision.
Écrasement sur place, modification du nom ou création d'un nouveau fichier avec injection dans les processus corrects connus	Le ransomware effectue l'injection dans un processus correct connu et exécute des actions malveillantes comme décrit précédemment.	Le pilote envoie des notifications de tentatives d'injection au service, qui demande au pilote de surveiller le processus sans effectuer de copie sur écriture. Si des comportements suspects sont détectés, le système peut inviter l'utilisateur à récupérer des fichiers à partir du Cloud.

Les attaques par ransomware et nos moyens de défense

Examinons le tableau ci-dessus illustrant les techniques et méthodes utilisées par un ransomware pour exécuter ses actions malveillantes.

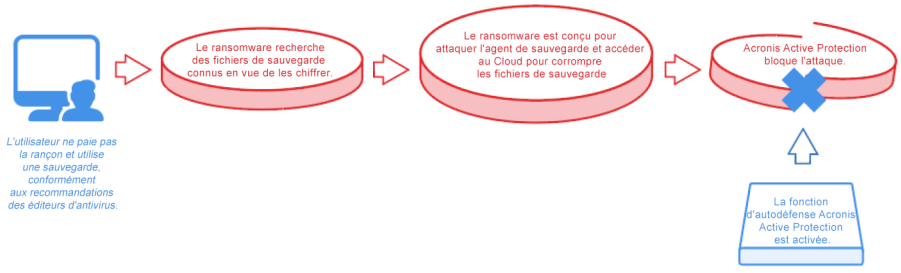
Pourquoi notre technologie est-elle plus efficace qu'un antivirus associé à un logiciel de sauvegarde ?

La réponse est simple : deux produits opérant de manière individuelle ne protégeront pas vos données contre les ransomwares, car ils ne sont pas en mesure de communiquer. Dans une configuration traditionnelle, lorsqu'une attaque échappe à la vigilance d'une solution antimalware, les données affectées sont perdues, parce que la solution antimalware n'effectue pas de sauvegarde des fichiers dans le Cloud et que la solution de sauvegarde ne détecte pas les logiciels malveillants. Lorsqu'Acronis Active Protection est associé à Acronis Cloud via un agent de terminal Acronis, les données originales peuvent être restaurées à partir de caches locaux, de sauvegardes locales ou encore de sauvegardes dans le Cloud. La menace la plus grave liée au ransomware est ainsi éliminée.
Les logiciels de demande de rançon peuvent passer à travers les mailles du filet des logiciels antimalware parce que les cybercriminels ciblent prioritairement ces programmes. Les pirates étudient les principales solutions antimalware pour identifier les failles dans leurs technologies de détection ou leur architecture logicielle et parvenir à les contourner. Comme nous l'avons dit précédemment, la détection basée sur les signatures présente peu d'intérêt de nos jours puisqu'il suffit de chiffrer le logiciel malveillant pour échapper à la détection. Or, bon nombre de packages logiciels antivirus gratuits continuent à utiliser cette approche. C'est bien pour cette raison que les éditeurs de logiciels antimalware recommandent aux utilisateurs d'effectuer des sauvegardes. Dans le même temps, toutes les solutions de sauvegarde dans le Cloud offrent une protection contre un vecteur d'attaque simple : l'endommagement des données sur une machine locale. Mais aucune solution n'offre de protection contre les attaques ciblant un logiciel de sauvegarde.

Acronis Active Protection offre une protection contre les menaces émergentes

Pourquoi les cybercriminels ciblent-ils les sauvegardes ? Parce qu'ils y voient une menace à court terme pour leur mode opératoire. Des projets tels que https://www.nomoreransom.org/prevention-advice.html encouragent les utilisateurs à respecter deux principes simples d'une importance primordiale : effectuer des sauvegardes et ne jamais payer de rançon.
Force est de constater que les escrocs s'en prennent déjà aux fichiers de sauvegarde. La tactique s'avère toutefois insuffisante dans la plupart des cas, car nombre de solutions de sauvegarde offrent un stockage dans le Cloud. Pour compromettre une sauvegarde dans le Cloud, les cybercriminels doivent obtenir des identifiants pour obtenir l'accès au Cloud, chose dont sont incapables les ransomwares classiques.

Les cybercriminels en viennent donc à analyser la façon dont les données sont transférées dans le Cloud : elles passent par un agent installé sur l'équipement. D'un point de vue technique, les possibilités ne manquent pas pour injecter du code malveillant dans l'agent local et compromettre les données de sauvegarde dans le Cloud. Un produit Acronis doté de la technologie Active Protection est le seul logiciel de sauvegarde capable de mettre en échec ce type d'attaque émergente.



Acronis

Des résultats validés par des laboratoires indépendants

Le laboratoire indépendant AV-TEST a mis à l'essai quatre nouveaux programmes. Il est parvenu à la conclusion suivante : « Le test montre clairement qu'une protection efficace contre les malwares doit inclure le déploiement d'un logiciel de sauvegarde. [La technologie Acronis Active Protection] était la seule solution de sauvegarde testée capable de bloquer les attaques par ransomware. »

Le laboratoire indépendant MRG Effitas en est arrivé à la même conclusion, après n'avoir identifié « aucune vulnérabilité » dans le cadre de ses tests sur les solutions Acronis.

Pour en savoir plus sur ces tests indépendants, consultez les communiqués de presse et le blog d'Acronis.

Pour plus d'informations, visitez notre site : **www.acronis.com**.