Bitdefender®

# CE QUE VOUS DEVEZ SAVOIR SUR LES RANSOMWARES

## ET SUR LA FAÇON DONT BITDEFENDER VOUS PROTÈGE

Avec les cybercriminels qui génèrent des millions, voire des milliards de dollars, grâce aux demandes de rançons en ligne, les ransomwares sont unanimement considérés comme l'une des plus grandes menaces auxquelles les entreprises doivent faire face de nos jours.

Comble de l'ironie, la majeure partie de ces coûts n'est pas liée au montant de la rançon elle-même mais aux freins que les ransomwares font peser sur le développement des affaires des entreprises[1] - il n'est donc pas surprenant que seulement un tiers des entreprises pensent pouvoir vraiment se remettre d'une attaque de ransomware[2].

Bitdefender a suivi de près le développement des ransomwares, en prédisant leurs prochaines évolutions et en développant des technologies spécifiques pour leur éradication.

Dans ce livre blanc, vous apprendrez ce que vous devez savoir sur ce type de menace et quelles technologies Bitdefender utilise pour protéger votre entreprise contre l'un des plus grands fléaux en ligne auxquels elle est confrontée aujourd'hui.

[1] http://www.prnewswire.com/news-releases/report-identifies-ransomwares-biggest-cost-to-be-business-downtime-300236505.html

[2] https://www.hotforsecurity.com/blog/only-38-of-businesses-believe-they-will-recover-from-a-ransomware-attack-13625.html

# Qu'est-ce qu'un ransomware ?

Les malwares tentent de s'adapter à leur environnement pour survivre. Certains échouent, d'autres y parviennent. Ils peuvent alors se répandre et provoquer de véritables épidémies. En 2015, les ransomwares ont causé près de 400 millions d'euros de perte[3], confirmant leur réputation de cybermenace la plus sérieuse répertoriée à ce jour pour les particuliers et les entreprises.

De plus, 3 professionnels de sécurité sur 4 décrivent la réémergence des ransomwares comme la menace la plus importante des 12 derniers mois, selon une **enquête BlackHat**.

Le ransomware de dernière génération est un type de malware qui verrouille et, généralement, chiffre un système d'exploitation jusqu'à ce que l'utilisateur finisse par payer pour y avoir de nouveau accès. Le malware peut pénétrer un système via le téléchargement d'un fichier malveillant sur un site Web ou via une pièce jointe d'un e-mail, une vulnérabilité réseau ou même un SMS.

En quoi est-il différent des malwares traditionnels ?

- Il ne dérobe pas les données des victimes, mais les chiffre ;
- Il n'essaye pas de se cacher une fois les fichiers chiffrés, car sa suppression ne permettra pas la récupération des données perdues ;
- Il demande le paiement d'une rançon, généralement en devise virtuelle ;
- Il est relativement facile à créer : il existe de nombreuses crypto-librairies bien documentées.

## SOUS QUELLE FORME APPARAÎT-IL ?

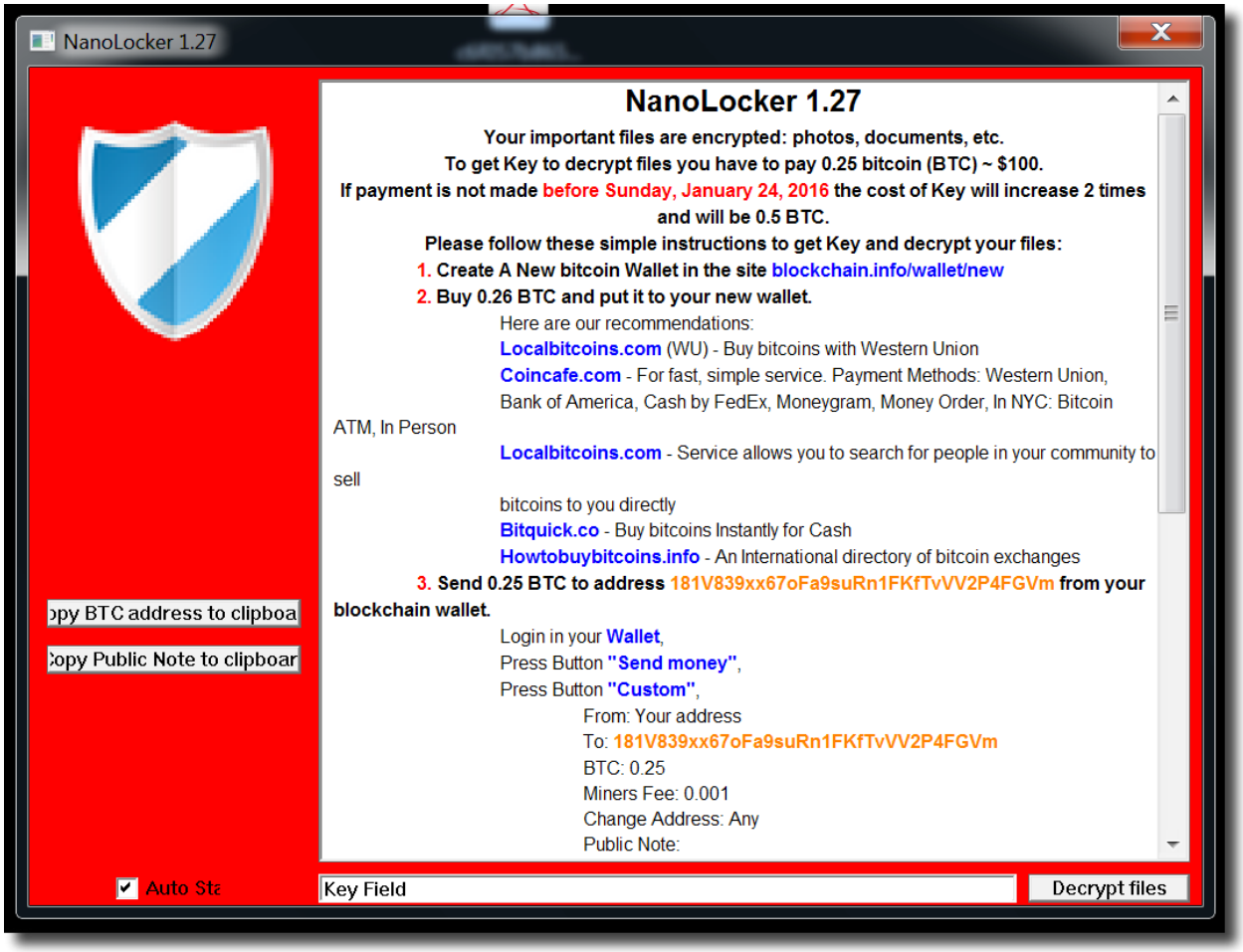
Il existe deux principaux types de ransomwares en circulation.

**Les Device Lockers.** Ce type de ransomware verrouille l'appareil et affiche une image en plein écran qui bloque son accès. Le message exige un paiement, mais les fichiers ne sont pas chiffrés. Il apparaît souvent sous la forme d'un message de la police et menace l'utilisateur d'une amende pour ses prétendues activités douteuses ou criminelles en ligne.


Source : theregister.co.uk - Certains hackers ont abandonné le crypto-ransomware. Désormais, ils verrouillent simplement votre appareil en espérant que vous payiez

[3] http://businessresources.bitdefender.com/hubfs/2016_-_FR_-_Files/Livre_Blanc_-_Les_ransomwares_une_affaire_personnelle.pdf

**Les Crypto-Ransomwares.** Les chiffreurs de fichiers sont bien plus évolués que le simple "verrouilleur d'écran", allant jusqu'à un chiffrement irréversible des dossiers et fichiers (documents professionnels et personnels, photos, vidéos, etc.).




Source : blog.malwareclipboard.com – Analyse du ransomware Nanolocker

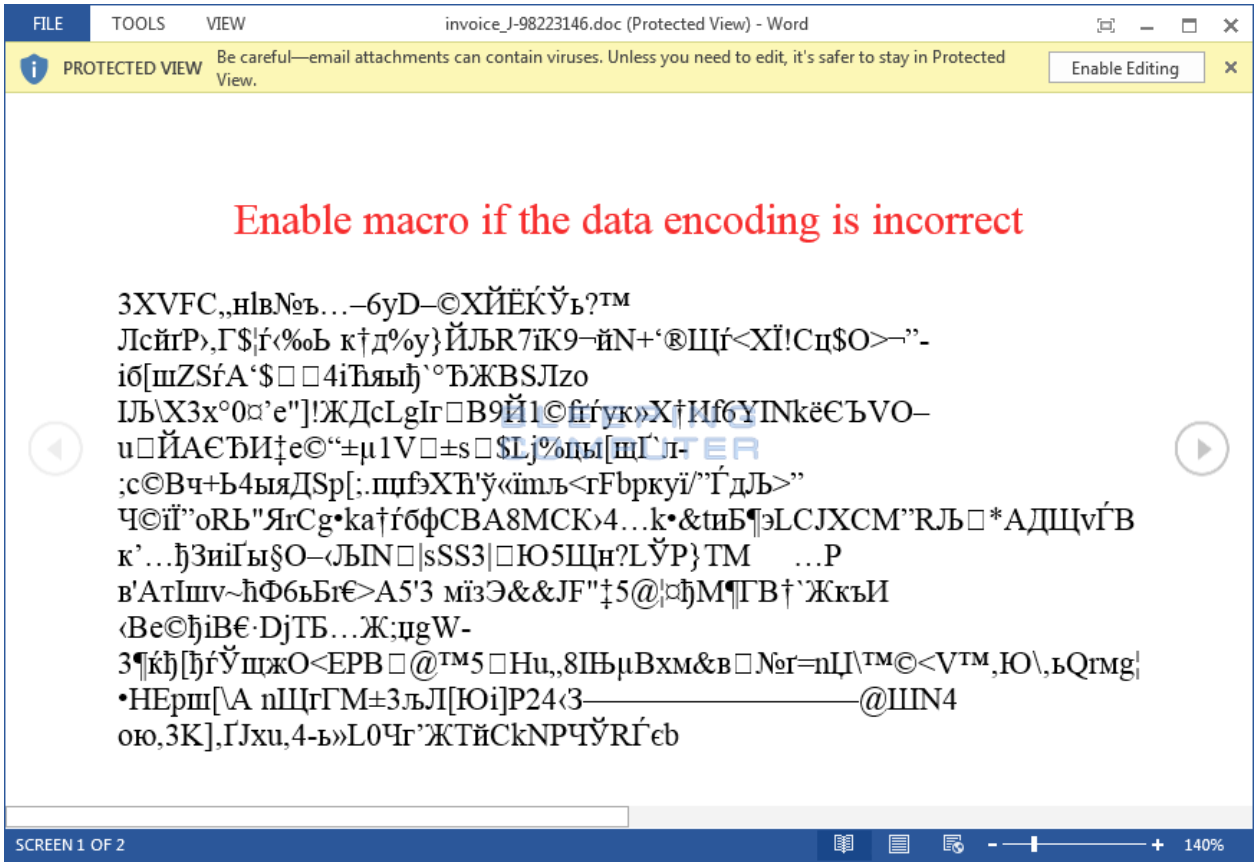
Ces deux types de malwares bloquent l'accès aux ressources de l'ordinateur, mais les verrouilleurs d'écran peuvent généralement être contournés via différentes techniques et outils de récupération, tandis que le chiffrement des crypto-lockers est bien plus difficile à contourner, ce qui rend leur pouvoir de destruction bien supérieur.

## CE QUE VOUS DEVEZ SAVOIR

Bitdefender suit de près l'évolution des ransomwares, en essayant d'en prédire les prochaines étapes et en développant des technologies de protection contre cette menace majeure.

Au cours des trois premiers mois de l'année 2016, le nombre de spams contenant des pièces jointes malveillantes a augmenté de 50%, selon les données des Bitdefender Labs. L'augmentation du nombre de pièces jointes infectées est liée à la prolifération des crypto-ransomwares. Locky et Petya, deux ransomwares particulièrement agressifs et en pleine expansion, infectent leurs victimes via des campagnes de spams massives diffusant des documents Word "déguisés" en factures et des liens Dropbox redirigeant vers des applications malveillantes. Ces deux nouveaux ransomwares se sont montrés particulièrement prolifiques : Locky, par exemple, a infecté plus de 400 000 postes de travail en seulement quelques heures[4].

[4] https://blog.knowbe4.com/its-here.-new-ransomware-hidden-in-infected-word-files




Un document infecté par Locky, envoyé en tant que pièce jointe dans un e-mail de spam. Une fois que la victime a activé les macros, ces dernières vont télécharger un fichier exécutable à partir d'un serveur distant et l'exécuter.

Source : blog.knowbe4.com

## LE RANSOMWARE SE RÉPAND DANGEREUSEMENT VERS DE NOUVELLES PLATEFORMES

Windows demeure la cible privilégiée des ransomwares, qui disposent de nombreuses variantes suivant différentes transformations pour faire face à l'évolution des lois et des mesures mises en place par les éditeurs de solution de sécurité pour contrer les effets des variantes les plus prolifiques, dont CryptoLocker, TorLocker, BitLocker entre autres.

Bitdefender dispose actuellement d'une base de données de plus de 2,8 millions d'échantillons de ransomwares et de trois technologies actives pour protéger les systèmes Windows contre cette menace.

Les ransomwares ne sont pas seulement prolifiques sous Windows, mais également sous Android, Linux et même macOS. Le système d'exploitation Android a été reconnu comme étant l'OS le plus susceptible de devenir la cible de la nouvelle génération de ransomwares mobiles, non seulement à cause de son pourcentage impressionnant de part de marché, qui s'élève à 82,2% au deuxième trimestre de 2015 d'après IDC[5], mais également parce qu'il représente plus de 1,4 milliard d'utilisateurs actifs sur 30 jours à l'échelle mondiale, selon le PDG de Google, Sundar Pichai[6].

Les statistiques internes de Bitdefender concernant Android, montrent que la famille du ransomware Android SLocker représente 4,35% des infections au cours du 3ème trimestre 2015 et 3,08% au cours du dernier trimestre 2015.

La toute dernière évolution des ransomwares montre qu'ils s'en prennent désormais aux systèmes d'exploitation Linux. Les serveurs Web sous Linux sont au cœur d'Internet, un grand nombre d'entre eux hébergeant même des dizaines de sites Web. Une infection réussie sur l'un d'entre eux, pourrait alors affecter de nombreuses victimes à la fois et donc permettre une augmentation des revenus générés par les rançons. L'une de nos prédictions pour 2016 concerne l'évolution croissante du ransomware sous Linux, faisant de lui l'une des menaces les plus sérieuses à ce jour.

**Bitdefender est le premier éditeur de sécurité à publier un outil de déchiffrement pour les victimes de ransomwares sous Linux - gratuitement.** Les chercheurs Bitdefender ont pu détecter des failles dans les algorithmes de chiffrement utilisés pour verrouiller les fichiers de chiffrement de Linux.Encoder.

[5] http://www.idc.com/prodserv/smartphone-os-market-share.jsp

[6] http://techcrunch.com/2015/09/29/android-now-has-1-4bn-30-day-active-devices-globally/

Bitdefender suit également de près l'évolution des ransomwares visant les Mac. En décembre 2015, Bogdan Dumitru, Directeur des Technologies chez Bitdefender, a annoncé qu'il s'attendait à l'apparition du premier ransomware Mac courant 2016[7]. Trois mois plus tard, une équipe de chercheurs de Palo Alto Network découvrait KeRanger, un ransomware infectant un client BitTorrent très prisé par les utilisateurs Mac. C'est le premier ransomware détecté sous macOS.

# COMMENT BITDEFENDER PROTÈGE LES ENTREPRISES CONTRE LES RANSOMWARES ?

Toutes les solutions professionnelles Bitdefender utilisent non pas une, mais deux couches de protection contre les ransomwares. Les deux technologies travaillent indépendamment. Ensemble, elles forment l'un des boucliers anti-ransomwares les plus puissants du marché.

Pour améliorer votre protection pour endpoint existante, vous pouvez aussi utiliser le vaccin anti-ransomware Bitdefender. Il fonctionne avec n'importe quelle solution de sécurité déjà installée.

**AVEC LES SOLUTIONS POUR ENTREPRISES BITDEFENDER**

Étape 1

**DÉTECTION PAR SIGNATURE**

FILTRE TOUS LES RANSOMWARES CONNUS

Étape 2

**RANSOMWARE ACTIVE THREAT CONTROL**

DÉTECTE DES COMPORTEMENTS DE TYPE RANSOMWARE DANS DES FICHIERS ET PROCESSUS INCONNUS

**AVEC UNE SOLUTION D'UN AUTRE ÉDITEUR DE SÉCURITÉ**

**VACCIN ANTI-RANSOMWARE**

EMPÊCHE LES RANSOMWARES QUI ONT CONTOURNÉ VOS DÉFENSES DE CHIFFRER LES FICHIERS ET DOSSIERS

- COMPATIBLE AVEC TOUTE SOLUTION EPP -

[7] http://businessinsights.bitdefender.com/predictions-for-2016

## UNE DÉTECTION BASÉE SUR LES SIMILITUDES DE SIGNATURES

# BLOQUE LA PLUPART DES RANSOMWARES

*Intégrée à toutes les solutions Bitdefender GravityZone*

## POURQUOI UNE DÉTECTION BASÉE SUR LES SIMILITUDES DE SIGNATURES ?

La détection basée sur les signatures est la première ligne de défense contre les attaques de ransomwares. Certes, elle ne suffit pas à se protéger totalement contre cette menace, mais elle joue néanmoins un rôle important au sein de toutes les solutions de sécurité pour lutter contre les ransomwares en entreprise.

**ELLE EMPÊCHE L'EXÉCUTION DE TOUTES LES FAMILLES DE RANSOMWARES CONNUES. Elle détecte et bloque tous les formes connues de ransomwares.**

**ELLE BLOQUE LES NOUVELLES VARIANTES DE RANSOMWARES. Les ransomwares sont polymorphes et créent des variantes différentes sur chaque appareil infecté. Pour contrer cette capacité, Bitdefender indexe les injecteurs à l'origine des infections plutôt que les fichiers.**

**ELLE STOPPE LES RANSOMWARES AYANT UN COMPORTEMENT SIMILAIRE AUX FAMILLES CONNUES. Grâce à sa technologie de détection des similitudes, Bitdefender peut détecter des ransomwares jusqu'alors inconnus, s'ils présentent des comportements similaires à ceux déjà répertoriés.**

**DÉJÀ 2,8 MILLIONS DE NOUVEAUX RANSOMWARES COMPTABILISÉS. Bitdefender a détecté plus de 2,8 millions d'échantillons uniques de ransomware sur ces deux dernières années seulement.**

## COMMENT CETTE DÉTECTION FONCTIONNE-T-ELLE ?

Les ransomwares sont polymorphes, ce qui signifie que chaque exemplaire est unique, personnalisé pour chaque victime. C'est la raison pour laquelle répertorier la signature de chaque souche ne serait pas logique dans le cas des ransomwares.

### Signature de l'injecteur

Pour optimiser cette méthode de détection traditionnelle, outre l'échantillon lui-même, Bitdefender signe également l'injecteur, bloquant le vecteur d'attaque avant que le ransomware n'atteigne réellement votre appareil.

*Qu'est-ce qu'un injecteur ?*

Durant une attaque, le ransomware en lui-même n'est pas le premier élément malveillant à atteindre votre appareil. Lorsque vous cliquez sur un lien ou fichier malveillant, ce qui est téléchargé en premier lieu est un injecteur - un petit logiciel qui agit comme un téléchargeur pour le véritable ransomware.

Un autre avantage de bloquer l'injecteur au lieu du ransomware lui-même, en plus d'anticiper l'infection, est qu'un injecteur peut être utilisé sur plusieurs appareils. Ainsi, chaque personne utilisant Bitdefender et qui est ciblé par cet injecteur spécifique sera complètement protégé contre les ransomwares diffusés par son intermédiaire.

### Similarité des signatures

Bitdefender détecte également les variantes de ransomwares déjà répertoriées, grâce à un algorithme appelé simhash, développé en interne. En utilisant simhash, les attaques de ransomwares similaires peuvent être bloquées, même si l'échantillon était inconnu jusqu'ici.

## LA TECHNOLOGIE BITDEFENDER RANSOMWARE ATC

# DÉTECTE DES RANSOMWARES INCONNUS

*Cette technologie qui complète le module d'analyse comportementale ATC (Advanced Threat Control)*

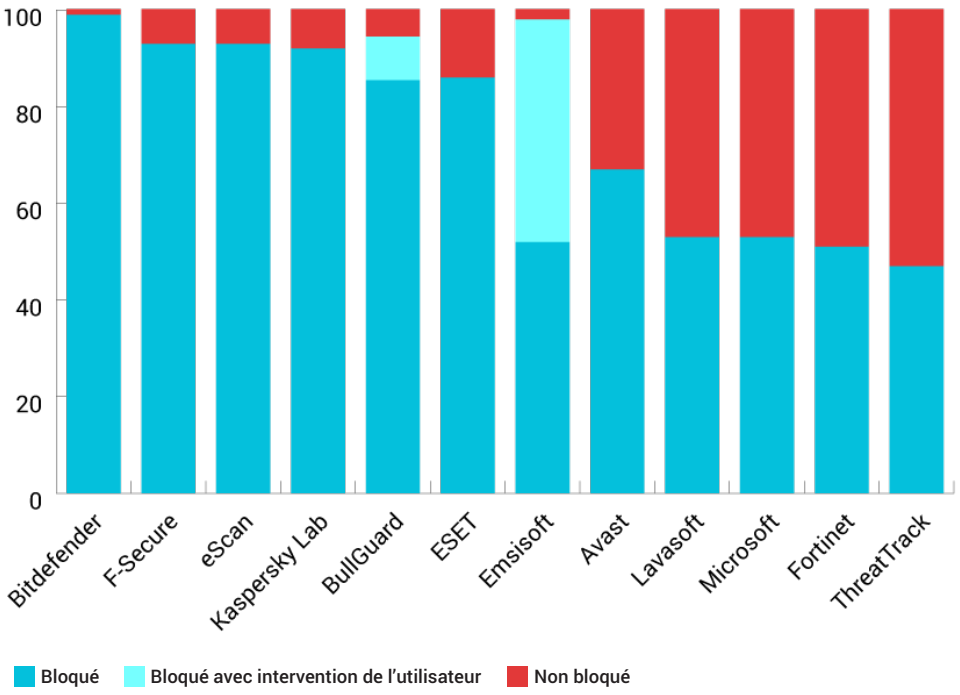
*Intégrée à toutes les solutions Bitdefender GravityZone*

### BITDEFENDER - LES MEILLEURS SCORES DE DÉTECTION DES MENACES INCONNUES

Bitdefender obtient un score presque parfait dans la détection des nouvelles menaces.

L'efficacité du moteur Bitdefender Advanced Threat Control est prouvée par des tests heuristiques ou comportementaux, tels que ceux réalisés par AV-Comparatives. Les tests indépendants comparent les résultats d'analyse de solutions antimalwares face à de nouveaux malwares ou des attaques de type Zero-day et classent leur performance en fonction de leur capacité à les bloquer. Parce que ces menaces sont nouvelles, les signatures traditionnelles sont inutiles. Les résultats de détection se fondent ainsi uniquement sur les résultats obtenus par les technologies heuristiques des différentes solutions.

Dans le test d'AV-Comparatives publié en 2015, Bitdefender a surpassé toutes les autres solutions en bloquant 99% des échantillons de malwares, le concurrent le plus proche n'en bloquant que 93%. Bitdefender a également obtenu plus de 97% de taux de détection au cours des trois dernières années, alors que la moyenne des acteurs du secteur pour ce test, passait de 84% à 75% sur la même période.




AV-Comparatives, test de détection comportementale/heuristique, 2015

## QU'EST-CE QUE LA TECHNOLOGIE RANSOMWARE ATC ?

Depuis septembre 2015, Bitdefender a étendu sa technologie heuristique brevetée, appelée ATC, pour détecter également les ransomwares inconnus. La technologie utilise des modèles comportementaux avancés pour détecter un ransomware, même s'il n'a pas été signé.

**INCROYABLEMENT EFFICACE CONTRE LES NOUVEAUX RANSOMWARES ISSUS DU BLACK MARKET. Cette technologie détecte les nouvelles familles de ransomwares qui peuvent être achetées et générées sur le Black Market - car elles présentent toutes des similitudes comportementales.**

**ELLE DÉTECTE DES TYPES DE RANSOMWARES INCONNUS. Les comportements des ransomwares sont similaires, même s'ils sont polymorphes. Une technologie comportementale puissante peut détecter de nouvelles variantes en utilisant des technologies heuristiques adaptées.**

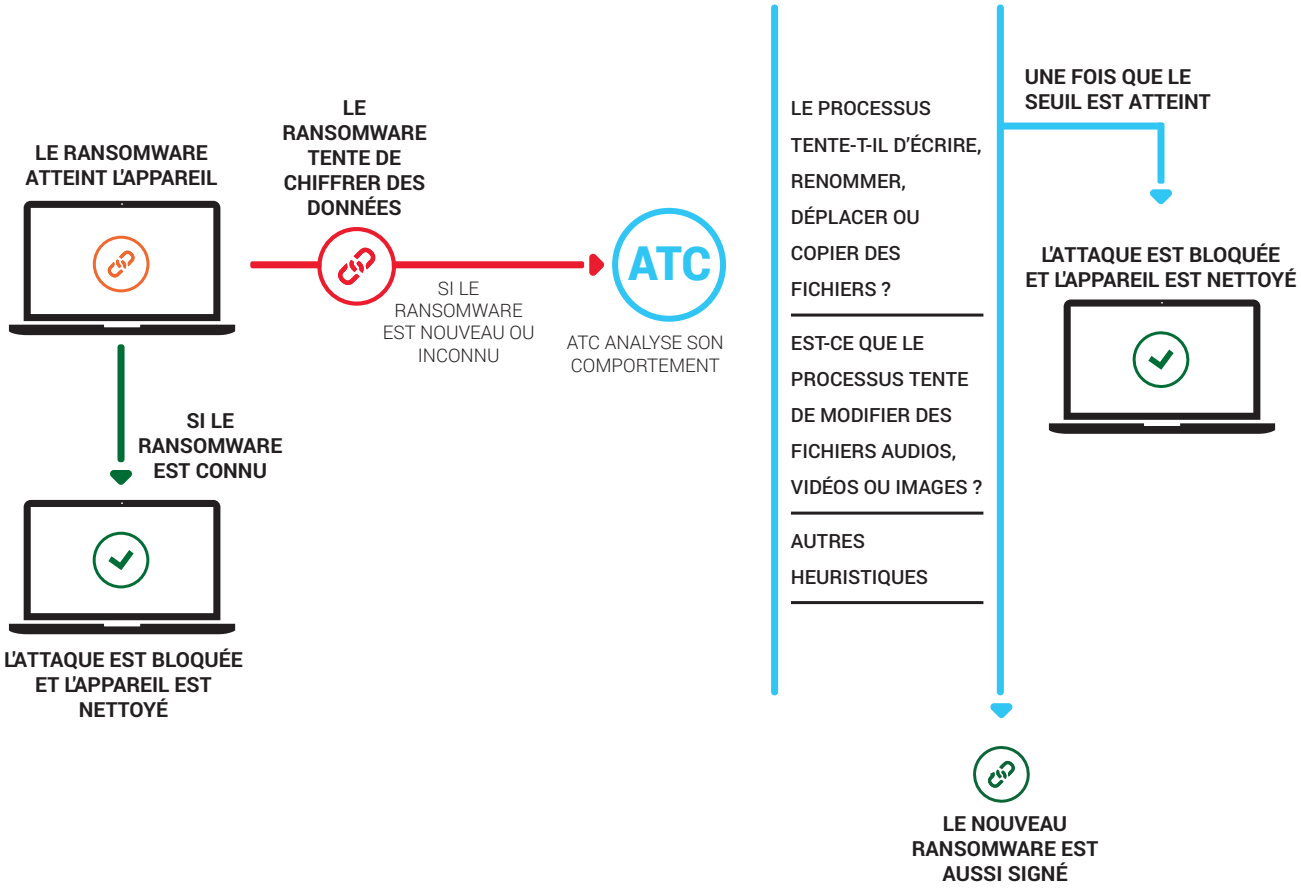
**ELLE FONCTIONNE AVEC DES TECHNOLOGIES DE DÉTECTION COMPORTEMENTALE COMPLEXES. Les nouvelles variantes de ransomwares sont incroyablement faciles à créer, c'est pourquoi la détection basée sur les signatures ne peut pas suivre le rythme. Pour pouvoir les détecter, une technologie doit pouvoir les détecter par leur comportement.**

**ELLE UTILISE LA TECHNOLOGIE ATC RECONNUE. Cette technologie s'est révélée particulièrement efficace pour la découverte de malwares inconnus. ATC permet à Bitdefender d'obtenir constamment les meilleures notes en matière de détection grâce à sa capacité à découvrir des menaces nouvelles.**

**ELLE PROTÈGE CONTRE LES RANSOMWARES SIGNÉS NUMÉRIQUEMENT. Même si un ransomware est signé numériquement, il présentera toujours un comportement malveillant et sera bloqué.**

## COMMENT FONCTIONNE CETTE TECHNOLOGIE ?

ATC n'a pas besoin de se baser sur les signatures, car elle détecte les ransomwares sur la base de leur comportement. Pour déterminer si un processus est une menace avant qu'elle puisse attaquer réellement, ATC surveille tous les processus actifs et définit un score à tout comportement suspect. Si un processus agit plusieurs fois de façon suspecte, il verra son score augmenter. Une fois que son score dépasse un certain seuil, ATC le signale à d'autres technologies pour qu'elles bloquent le processus.



Voici quelques actions surveillées par Bitdefender et pouvant indiquer un comportement de type ransomware :

LE PROCESSUS ESSAIE-T-IL D'ÉCRIRE, DE RENOMMER, DE DÉPLACER OU DE COPIER DES FICHIERS ? Le seul objectif d'un ransomware est de chiffrer vos fichiers. Ainsi, les actions les plus communément associées aux ransomwares sont d'écrire, de renommer, de déplacer ou de copier. La technologie Bitdefender ATC surveille en continu le comportement de tout programme qui tente de réaliser l'une de ces actions.

UN PROCESSUS ESSAIE-T-IL DE MODIFIER LES FICHIERS AUDIOS, VIDÉOS OU IMAGES ? Les ransomwares ciblent également des fichiers audios, vidéos ou images. Ainsi, ATC devient particulièrement suspicieux si un programme tente de réaliser l'une des actions citées plus haut sur un fichier de ces types.

Ce ne sont là que quelques exemples, Bitdefender Ransomware ATC réalise en continu plus d'une dizaine d'analyses pouvant indiquer la présence de ransomwares.

La détection ATC fonctionne localement et ne nécessite pas de connexion au Cloud Bitdefender. La technologie est autonome, car les paramètres de détection heuristique des ransomwares, définis par la technologie, fonctionnent de façon indépendante.

À mesure que la menace ransomware continue d'évoluer, Bitdefender améliore ses technologies heuristiques existantes et en ajoute de nouvelles, afin de garder constamment une longueur d'avance.

LE VACCIN ANTI-RANSOMWARE

# EMPÊCHE LES RANSOMWARES EXISTANTS DE CHIFFRER DES DONNÉES

## POURQUOI UN VACCIN ANTI-RANSOMWARE ?

Malgré les efforts des éditeurs de sécurité, les ransomwares parviennent parfois à pénétrer les couches de sécurité en place. Le vaccin anti-ransomware de Bitdefender est une dernière ligne de défense contre les ransomwares - si votre solution de sécurité n'a pas détecté ou bloqué la menace, le vaccin parvient à l'empêcher de chiffrer vos fichiers. Cette technologie est intégrée dans la gamme Bitdefender GravityZone et est également disponible gratuitement, en téléchargement, pour être exécutée en parallèle de toute autre solution de sécurité pour endpoint du marché. Pour qu'elle puisse fonctionner, elle doit être installée avant l'infection.

**PROTECTION PRÉVENTIVE CONTRE LES RANSOMWARES. La solution agit comme un vaccin qui empêche les modèles de ransomwares connus de chiffrer votre système.**

**ELLE FONCTIONNE CONTRE LES RANSOMWARES CONNUS ET INCONNUS. Le vaccin anti-ransomware de Bitdefender est capable de bloquer des nouveaux ransomwares en détectant des comportements connus, même s'ils utilisent des injecteurs inconnus.**

**ELLE EST COMPATIBLE AVEC N'IMPORTE QUELLE SOLUTION DE SÉCURITÉ. Le vaccin anti-ransomware de Bitdefender est compatible avec la protection pour endpoint que vous utilisez, quelle qu'elle soit, offrant ainsi un ultime rempart de sécurité au cas où vos autres niveaux de sécurité échouent à bloquer la menace.**

**ELLE ASSURE UNE DERNIÈRE LIGNE DE DÉFENSE. Le vaccin anti-ransomware de Bitdefender est l'ultime niveau de protection contre les ransomwares ayant contourné tous les autres filtres de sécurité.**

**ELLE N'A AUCUN IMPACT SUR LES PERFORMANCES. La technologie a été développée pour ne pas impacter les performances de votre endpoint.**

## COMMENT LE VACCIN FONCTIONNE-T-IL ?

Le vaccin anti-ransomware de Bitdefender fonctionne en exploitant les failles au sein de la méthode de propagation des ransomwares afin de les empêcher de chiffrer vos données, dans le cas où le malware a déjà pénétré votre appareil. La solution fonctionne en combinaison avec une solution de protection existante et agit comme une dernière ligne de défense contre les ransomwares qui parviennent à se glisser au-delà des autres niveaux de protection, même si l'injecteur est inconnu.

Le vaccin anti-ransomware de Bitdefender est actuellement disponible en téléchargement gratuit : https://labs.bitdefender.com/2016/03/combination-crypto-ransomware-vaccine-released/

# BITDEFENDER, UNE APPROCHE CIBLÉE CONTRE LES RANSOMWARES

- Les ransomwares sont l'une des menaces les plus graves que les entreprises ont eu à gérer à ce jour et une approche de sécurité ciblée est cruciale pour défendre votre business.
- Bitdefender n'a pas un, mais trois niveaux de protection pour combattre les ransomwares, qui sont intégrés à ses solutions dédiées aux entreprises. De plus, ils seront complétés dans un avenir proche.
- La technologie ATC, qui fournit une protection contre les nouvelles formes de ransomwares, participe activement aux excellents scores que Bitdefender obtient en matière de détection des menaces de type Zero-day. Bitdefender a également obtenu un score de détection des menaces inconnues de plus de 97% au cours des trois dernières années, alors que la moyenne du secteur pour ce test passait de 84% à 75% sur la même période.
- Bitdefender a détecté un total de 2,8 millions d'échantillons de ransomwares uniques pour ces deux dernières années seulement.
- Nous sommes le premier éditeur de sécurité à publier gratuitement un outil de déchiffrement pour les victimes de ransomwares sous Linux. Les Bitdefender Labs ont découvert des failles dans les algorithmes de chiffrement utilisés par Linux.Encoder pour verrouiller les fichiers.

Bitdefender propose des technologies de sécurité dans plus de 120 pays via un réseau de partenaires de premier plan, de distributeurs et de revendeurs à valeur ajoutée. Depuis 2001, Bitdefender produit régulièrement des technologies leaders du marché pour les entreprises et les particuliers et est l'un des plus grands fournisseurs de solutions de sécurité pour les technologies de virtualisation et cloud. Bitdefender associe ses technologies primées à des alliances et des partenariats commerciaux et renforce sa position sur le marché mondial via des alliances stratégiques avec des fournisseurs de technologies cloud et de virtualisation leaders dans le monde.



Plus de **500 millions d'utilisateurs**
sont protégés par les technologies Bitdefender

Bitdefender