Trend Micro™

PROTÉGER VOTRE ORGANISATION CONTRE LES RANSOMWARE

Les ransomware (ou «rançongiciel») sont devenus une menace critique pour les entreprises et organisations de toutes tailles. Alors que les ressources et données d'entreprises sont plus que jamais ciblées par les cybercriminels, ces derniers veulent profiter des utilisateurs qui connaissent mal ces malware et leur comportement.

Il est nécessaire de maîtriser les risques que représentent ces menaces, afin d'éviter les indisponibilités systèmes, les pertes de productivité, l'impact délétère sur la réputation d'une marque et les conséquences juridiques liées à une attaque par ransomware.

VAINCRE LES RANSOMWARE AVEC TREND MICRO

Il n'y a pas de solution miracle face aux ransomware. Il faut, en effet, déployer, par étapes, plusieurs couches de sécurité pour maîtriser les risques.

Protection de l'email et du Web

Protection des endpoints

Protection du réseau

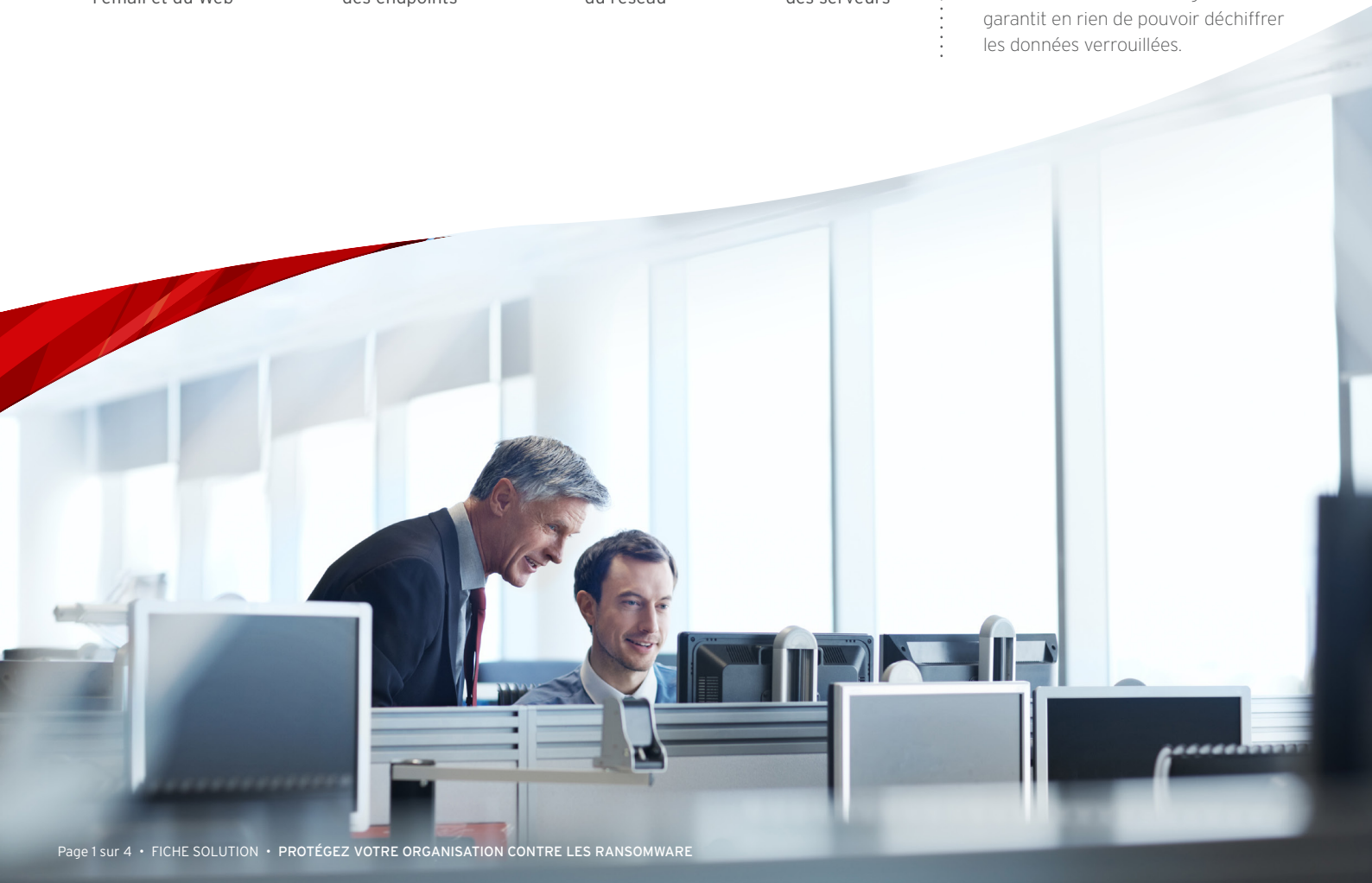
Protection des serveurs

Qu'est-ce qu'un ransomware ?

Le ransomware est un type de malware qui verrouille et chiffre les données et les systèmes, en empêchant d'y accéder. Les victimes sont invitées à régler une rançon aux instigateurs de l'attaque pour recouvrer cet accès.

Une infection par ransomware s'effectue généralement à l'aide d'un « Exploit Kit », via des techniques d'ingénierie sociale ou un email de spam massif. Il suffit que le destinataire ouvre un fichier joint vérolé ou clique sur une URL malveillante présente dans un email pour que le malware se télécharge sur son système.

La crainte de voir leurs données de valeur définitivement perdues peut inciter les victimes à régler la rançon, même si céder au chantage ne garantit en rien de pouvoir déchiffrer les données verrouillées.



PROTECTION DE L'EMAIL ET DU WEB

Tout démarre par vos utilisateurs. Ils sont les plus vulnérables face aux ransomware, lorsqu'ils se font piéger par un email de phishing ou cliquent sur une URL malveillante. Trend Micro a neutralisé plus de 99 millions de menaces par ransomware depuis octobre 2015, et 99 % d'entre elles étaient véhiculées par email ou un lien Web1. Vos utilisateurs ne seront plus victimes des ransomware si ces derniers sont stoppés en amont, dès la passerelle email ou web.

Votre email est sous Microsoft Office 365 ?

Certes, cette plateforme email dans le Cloud dispose déjà de ses outils de sécurité, mais vous restez vulnérable aux attaques par ransomware, via des emails de phishing ou des fichiers joints malveillants. Trend Micro peut vous aider à parfaire cette sécurité existante. **Trend Micro Cloud App Security** a neutralisé plus de 2 millions de menaces qui n'avaient pas été détectées par les fonctions de sécurité intégrées à Office 365. Ces fonctions sont ainsi renforcées des capacités anti-ransomware suivantes :

- Analyse antimalware et évaluation des risques liés à des fichiers.
- Analyse antimalware en sandbox.
- Détection des vulnérabilités de documents.
- Réputation Web.

Vous utilisez une passerelle email pour sécuriser votre messagerie sur site ?

Améliorez les taux de détection de ransomware de votre passerelle email. **Trend Micro™ Deep Discovery™ Email Inspector** utilise des techniques de détection évoluées pour identifier et neutraliser les emails de spear phishing souvent utilisés pour infecter des collaborateurs par ransomware. Fonctionnant en tandem avec votre passerelle de sécurité email et vos produits de sécurité serveur, Email Inspector détecte et neutralise les emails personnalisés de phishing (spear phishing), qui utilisent des fichiers joints et URL malveillants en tant que vecteur de propagation de ransomware. Les principaux atouts d'Email Inspector :

- Analyse en profondeur des fichiers joints aux emails et des URL, et notamment : documents et macros Office et PDF, fichiers compressés, exécutables, scripts, contenus multimédia, etc.
- Analyse granulaire des URL, et notamment les URL présentes dans le corps ou le sujet des messages et les URL présentes au sein de documents.
- Analyse de scripts suspects et détection des exploits zero-day pour détecter le comportement de ransomware (modification en masse de fichiers, chiffrement en cours, etc.)

Maîtrise des risques liés au trafic web

Au-delà de l'email, vos utilisateurs font face aux ransomware en cliquant sur des pages web malveillantes, créées intentionnellement ou après piratage de pages légitimes. **Trend Micro™ InterScan™ Web Security** protège vos utilisateurs sur le Web :

- Analyse des vulnérabilités zero-day et des navigateurs, souvent utilisées par les ransomware pour s'immiscer au sein de votre réseau.
- Intégration avec Trend Micro™ Deep Discovery™ à des fins d'analyse en sandbox.
- Réputation web en temps réel pour déterminer si une URL est connue en tant que source de ransomware.

[1] Trend Labs, avril 2016

Ransomware connus

PowerWare – Ce malware est capable de distinguer les disques logiques et les disques mappés à des réseaux partagés. Il met ainsi en péril la totalité d'un réseau et représente une menace majeure pour les entreprises.

PETYA – Supprime le MBR d'un système et empêche d'y accéder. Les systèmes infectés affichent une demande de rançon lors du démarrage et impossible d'aller plus loin. L'infection s'effectue via des services de stockage légitime dans le Cloud.

KeRanger – Un malware de chiffrement et également le tout premier crypto-ransomware pour Mac. S'installe via une application open-source de partage de fichiers. Les auteurs de ce malware ont utilisé un certificat développé pour application Mac pour contourner Apple Gatekeeper, cette fonction de sécurité qui permet aux utilisateurs de spécifier les sources à partir desquelles les applications peuvent être installées.

SAMAS (ou SAMSAM) – Le premier ransomware capable de chiffrer les fichiers sur l'ensemble du réseau, ciblant les bases de données et espaces de stockage d'une organisation. Les utilisateurs de SAMAS sont connus pour pouvoir localiser et supprimer manuellement les sauvegardes d'entreprise pour forcer les entreprises à régler une rançon.

Locky - Identifie et supprime les sauvegardes automatiques (shadow copies) des fichiers sous Windows.

MAKTUBLOCKER – La méthode de chiffrement de ce ransomware est classique, mais le vecteur d'infection est unique. Il débarque sous la forme d'un ransomware qui contient le nom et l'adresse email de l'utilisateur ciblé, ce qui inspire confiance. Le ransomware s'active après téléchargement des fichiers joints.

PROTECTION DES ENDPOINTS

Trend Micro a détecté 99 % des menaces par ransomware véhiculées par email ou URL. Mais il reste donc ce petit 1 % susceptible d'infecter un endpoint. **Trend Micro Smart Protection Suites** déploie un ensemble de technologies de différentes générations, en activant la technique la plus appropriée, au bon moment, pour optimiser la protection. Ces technologies sont les suivantes :

- **Un Machine Learning haute-fiabilité :** les fichiers sont analysés avant d'être exécutés et lors de leur exécution, afin d'affiner la détection. Des techniques de réduction de bruit (prévalence ou listes blanches) permettent de réduire le nombre de faux-positifs.
- **Analyse comportementale :** en cas de comportement suspect pouvant être associé à un ransomware, à l'image du chiffrement rapide de multiples fichiers, ce comportement peut être automatiquement neutralisé et le système piraté mis en quarantaine. Le ransomware est ainsi stoppé et ne peut plus se propager pour s'en prendre à vos données.
- **Contrôle applicatif :** des listes blanches sont créées de manière automatique et dynamique. Seules les applications légitimes (ce qui exclut donc les ransomware) sont autorisées à être exécutées.
- **Protection des vulnérabilités :** protège contre les ransomware qui tirent parti des vulnérabilités logicielles non patchées, qui sont des vecteurs d'attaques menées à partir d'Exploit Kits. Les plates-formes en fin de support comme Windows XP sont également protégées.

PROTECTION DU RÉSEAU

L'email et le Web constituent des vecteurs classiques par lesquelles les ransomware pénètrent au sein des organisations, mais d'autres protocoles réseau et méthodes d'attaques sont également utilisés par les ransomware. C'est la raison pour laquelle vous devez opter pour une stratégie de défense visant à empêcher les ransomware d'accéder à votre réseau et de se propager.

Trend Micro™ Deep Discovery™ Inspector est une appliance réseau qui détecte le trafic malveillant, les communications Command & Control, les comportements des assaillants, les exploits zero-day et toute autre activité associée à des tentatives de la part des ransomware de s'immiscer au sein de votre réseau. Deep Discovery peut empêcher les ransomware de se propager vers les endpoints et serveurs. La protection contre cette menace bénéficie :

- De technologies de détection évoluées pour l'ensemble du trafic réseau, des ports et plus de 100 protocoles réseau, afin d'identifier les ransomware et le comportement des attaques, à chaque étape de la tentative d'infection.
- D'analyses au sein d'une sandbox qui reprend les configurations de votre environnement informatique pour détecter les modifications et tentatives de chiffrement de fichiers, ainsi que les comportements malveillants associés aux attaques par ransomware.
- D'une intégration avec les passerelles de sécurité email et Web, les outils de sécurité serveur et email de Trend Micro, ainsi que les outils tiers, pour ainsi concrétiser une défense interconnectée contre les menaces déployées sur différentes couches de sécurité.

Protéger votre organisation contre les ransomware

- Processus automatisés de sauvegarde et de restauration
- Application des patchs logiciels dès leur disponibilité
- Sensibilisation des collaborateurs en matière de prévention des emails de phishing
- Accès limité et contrôlé aux données métiers critiques
- Protection en profondeur contre les ransomware pour renforcer le niveau de sécurité

PROTECTION DES SERVEURS

Les ransomware s'en prennent de plus en plus aux serveurs, comme le souligne l'exemple de **SAMSAM** qui utilise des vulnérabilités logicielles pour injecter des ransomware. Les conséquences d'attaques sur vos serveurs qui hébergent la majorité de vos données critiques peuvent être particulièrement lourdes.

Trend Micro™ Deep Security™ protège vos serveurs physiques, virtualisés ou cloud contre les ransomware grâce aux fonctionnalités suivantes :

- **Détection et prévention des activités suspectes :** lorsqu'un ransomware tente de s'introduire au sein d'un data center (via un utilisateur se connectant à un serveur de fichier vulnérable par exemple), Deep Security peut détecter les activités réseau suspectes et les neutraliser, tout en assurant une notification de cette problématique.
- **Protection des vulnérabilités :** protège les serveurs et applications contre les attaques par ransomware qui utilisent les vulnérabilités logicielles. Les plateformes en fin de support, somme Windows 2003, sont ainsi protégées.
- **Détection des mouvements latéraux :** si un ransomware pénètre au sein d'un data center, Deep Security permet également de minimiser son impact en le détectant et en neutralisant toute tentative de se propager à d'autres serveurs.

Lorsqu'un ransomware pénètre au sein d'une organisation, il peut accéder à toutes les données auxquelles accède un utilisateur piraté. L'impact peut être particulièrement lourd, avec de nombreuses heures-hommes consacrées à la récupération des fichiers, d'autant que cette récupération n'est pas garantie.

Alors que les ransomware évoluent, les organisations doivent pouvoir y faire face. Un partenariat avec Trend Micro apporte des solutions capables de prévenir et de neutraliser les dommages potentiellement causés par ces menaces dévastatrices.

Pour plus d'informations : **trendmicro.com/enterprise-ransomware**

À PROPOS DE TREND MICRO

Fort de 27 ans d'expérience, Trend Micro Incorporated (TYO: 4704; TSE: 4704) compte parmi les leaders mondiaux des solutions de sécurité. D'origine japonaise, l'entreprise continue d'innover afin de sécuriser les échanges d'informations numériques de ses clients. Nos solutions pour le grand public, les entreprises et les organisations gouvernementales, déploient une défense en profondeur permettant de protéger les informations sur les équipements mobiles, les endpoints, les passerelles, les serveurs et le Cloud.

TREND MICRO™

Securing Your Journey to the Cloud