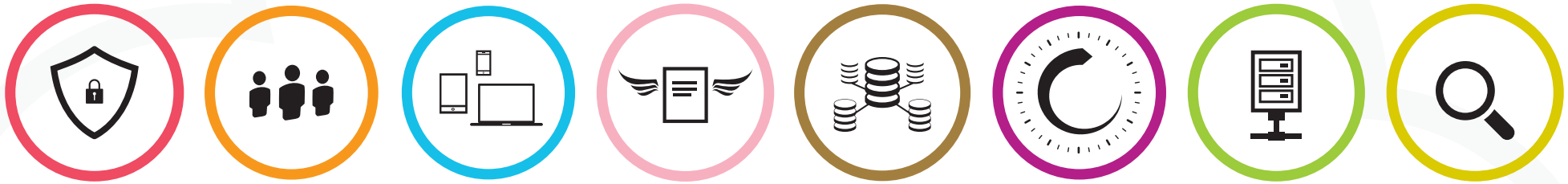
LIVRE BLANC

Rançongiciel : Entre Mythes et Réalités



Tout savoir pour faire face
et survivre à ce fléau

PREAMBULE

Les rançongiciels sont des programmes malveillants permettant aux cybercriminels d'infecter les équipements informatiques.

Une fois exécutés, les fichiers contaminés sont illisibles et les victimes sont alors sollicitées au travers d'un message pour s'acquitter d'une rançon dans l'espoir d'obtenir la clé de chiffrement leur permettant de récupérer leurs fichiers.

L'accès facilité à toutes les ressources utiles pour mener ces cyber-attaques (fichiers, codes malveillants, infrastructures), même pour un non initié, la forte rentabilité de l'activité (plusieurs milliers d'euros par heure de revenus pour les cybercriminels) auxquels s'ajoute une relative impunité, ont créé le terreau fertile pour la prolifération de ces nouveaux virus. Ils représentaient 20% des ransomwares en 2014 et 80% en 2015 !

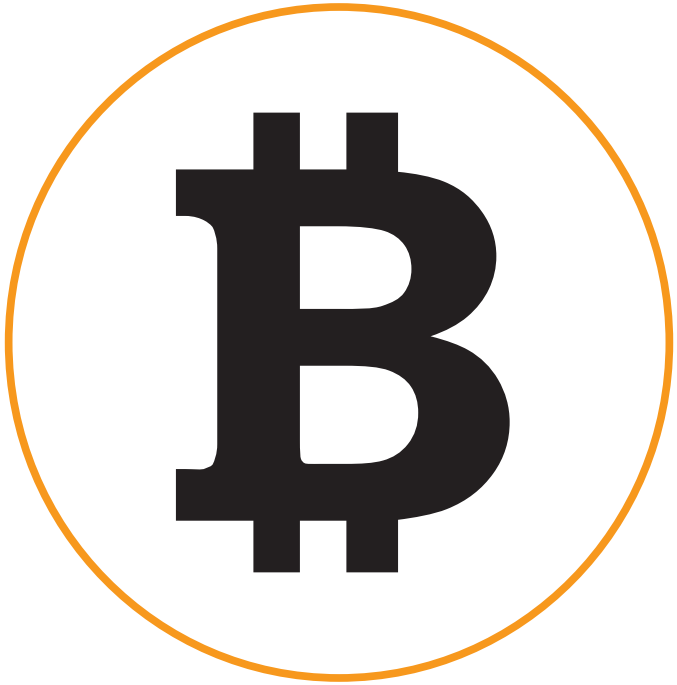
Une organisation professionnelle sur deux a ainsi été la cible d'une attaque en Europe en 2016(1) et deux tiers des attaques ont été dirigées vers les PME(2).

Dans ce contexte, la politique de l'autruche peut s'avérer désastreuse. En effet, **la question n'est pas de savoir si on va être attaquée, mais quand, et quel est le niveau de vulnérabilité de son organisation en cas d'infection.**

Dans ce guide, nous vous expliquerons comment fonctionne un rançongiciel, comment il se propage, quelles dispositions prendre pour minimiser les risques d'infection, quelles mesures prendre en cas de contamination.

Sommaire

UN RANCONGICIEL, COMMENT CA MARCHE ?



Il existe plusieurs familles de rançongiciels et chacune affiche de multiples variantes. La plupart utilise l'algorithme de chiffrement AES, mais d'autres méthodes sont utilisées.

Pour permettre aux victimes de déchiffrer les fichiers, les cybercriminels proposent à ces derniers de s'acquitter d'une rançon, laquelle sera exigée soit en monnaie électronique via la création d'un compte Bitcoin, soit via l'achat d'un coupon sur un site en ligne (Paysafecard…) qui sera monétisé par le cybercriminel pour assurer son revenu.

COMMENT SE DIFFUSENT LES RANCONGICIELS ?

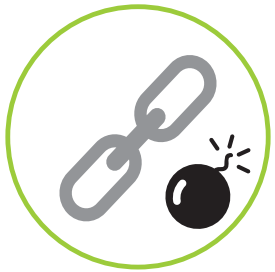
Les modes de contamination les plus courants

Le courriel piégé

Un courriel vous invite à ouvrir une pièce jointe (prétendue facture, bon de livraison…).

La raison est que ce mode de propagation nécessite un niveau d'ingénierie très simple d'adresse mails qui constituent autant de victimes potentielles.

Pour renforcer la pression sur la victime, il n'est pas rare que le message soit « prétendument » signé d'un organisme officiel : Police, Impôts, Banque, Fournisseur d'énergie ou de Telecoms… ou que l'émetteur appartienne au même domaine (@ nomdevotresociete.com) que votre adresse électronique.



Le lien piégé

Le lien piégé, passant généralement par des bannières publicitaires ou des boutons cliquables, est un leurre utilisé par le cybercriminel pour piéger sa victime.

La première phase consiste à identifier les sujets qui intéressent la victime (en étudiant par exemple son compte facebook) dans le but de lui présenter une publicité attractive en relation avec ses centres d'intérêts.

La banner présenté a bien entendu été préalablement piégé à l'aide d'un code malveillant dont le but est de réorienté la victime vers un site sur lequel est déposé le rançongiciel et de déclencher son activation via le click de souris réalisé sur le banner.

Les logiciels gratuits

Offrir une version gratuite d'un logiciel est une autre technique employée par les cybercriminels pour diffuser les rançongiciels. Pour infecter un équipement, rien de plus simple que de proposer à l'utilisateur de le faire lui-même en téléchargeant un logiciel, une application, un économiseur d'écran ou un jeux gratuits.

Méfiez-vous des prétendus philanthropes, rien n'est gratuit en ce bas monde. Lorsqu'on vous propose une solution gratuite, il y a fort à parier que ce soit vous le produit !

COMMENT SE DIFFUSENT LES RANCONGICIELS ?

Les modes de contamination les plus courants

Le point d'eau ou Watering hole

Le nom de l'attaque de point d'eau fait référence à la technique de chasse de certains fauves qui préfèrent attendre leurs proies à un point de passage obligé (en l'occurrence à un point d'eau pour s'abreuver) que d'aller chasser.

Une première phase consiste à identifier les sujets qui intéressent la victime (en étudiant son compte facebook par exemple) et à placer un code malicieux sur un site en rapport avec le sujet d'intérêt identifié.

Lorsque la victime vistera ce site, le code exploitera une faille de type zéro day de son équipement afin d'y infiltrer un cheval de troie.

L'accès à ce point d'eau est considéré comme un trafic légitime (via les ports 80, 443 ou 53) et passe donc inaperçu puisque la connexion a été initiée par un équipement interne au réseau.

Généralement, **le cheval de troie infiltré infecte l'ensemble des machines et serveurs de la société** permettant ainsi aux cybercriminels d'avoir accès à toutes les données informatiques des équipements (contacts, fichiers etc..), mais également de prendre le contrôle de la machine pour effacer toute trace des accès frauduleux.

Les méthodes utilisées dans ce cas sont connues sous le nom d'Exploit Kit dont le plus célèbre est incontestablement Angler kit qui utilise des codes HTML et JavaScript afin d'identifier le navigateur web de l'utilisateur et rediriger la requête tapée dans la barre de navigation vers un site infecté.

Cette technique s'applique également aux bannières publicitaires derrière lesquelles est embusqué le code malveillant qui s'active lorsque l'on clique sur le bouton nous invitant à agir (en savoir plus, j'en profite…).

COMMENT SE DIFFUSENT LES RANCONGICIELS ?

Schéma explicatif

SPAM

Activation du code malveillant à l'ouverture de la pièce jointe

Site Web infecté

Bannière pub infectée

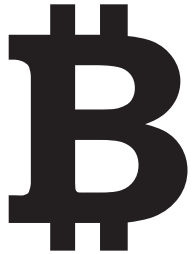
Activation du code malveillant au clique ou lors de la connexion

Poste de la victime

Chiffrement des données :

Plusieurs méthodes :

- Récupération d'une clé de chiffrement sur un serveur distant en utilisant la connexion internet (serveur de commande et de contrôle)
- Génération d'une clé de chiffrement pour chaque fichier trouvé
- Clé de chiffrement embarquée dans le code



Affichage d'une boite de dialogue affichant une demande de rançon réglable en Bitcoins ou en Coupons

ATTENTION

Que vous payez ou non cette rançon, vous n'êtes pas assuré de récupérer la clé de chiffrement et vos fichiers peuvent rester définitivement inexploitables

QUELS RISQUES ENCOURENT UNE ENTREPRISE VICTIME D'UN RANSOMWARE ?

Les ransomwares circulent via internet. Ils sont donc susceptibles d'infecter tout type d'équipement connecté (PC, Mac, Machines virtuelles, Tablettes, Smartphones).

Si l'équipement est connecté sur un réseau local, le crytovirus pourra se propager et infecter toutes les stations de travail du réseau, y compris le serveur de fichiers, aucun droit d'administration n'étant requis pour effectuer les opérations prévues par le ransomware.

Interruption de l'exploitation

Tout équipement contaminé devient immédiatement inexploitable,
les données qu'il héberge sur son disque dur étant devenues illisibles.

Risque élevé de perte de données

Le paiement de la rançon ne garantit en rien le déchiffrement des données.

Certains criminels ont, en effet, pour seule intention d'escroquer financièrement leurs victimes et ne prévoit aucun processus de déchiffrement après encaissement. Certains cryptovirus s'avèrent également incapables de déchiffrer les données du fait de bugs présents dans leur code.

Coût financier

Si l'entreprise ne dispose pas d'un logiciel de sauvegarde professionnel, **les fichiers chiffrés peuvent avoir été malencontreusement copiés sur le dispositif de sauvegarde** (Un Nas par exemple) lors de la dernière sauvegarde.

Dans ce cas, la restauration va s'avérer impossible.

Le montant moyen peut atteindre 3.000€ en PME et des centaines de miliers d'euros pour les grandes entreprises.

Si l'organisation est dotée d'une solution professionnelle de sauvegarde, les équipements infectés seront restaurés à partir des fichiers intègres de la dernière sauvegarde.
Au coût de restauration ou de reconstitution viendra s'ajouter le montant de la rançon éventuellement payée. On estime qu'une victime sur trois s'acquitte de la rançon demandée.

QUELLE POLITIQUE ADOPTER POUR SE PRÉMUNIR ?

1. La sensibilisation et l'éducation des collaborateurs

Le but aujourd'hui est de limiter les risques de contamination par négligence.

De nombreux guides pratiques sont disponibles en ligne afin de sensibiliser les personnes désireuses de vous prémunir. Abonnez-vous à des bulletins emailing dédiés et diffusez ces informations à tous vos collaborateurs.

La pédagogie constitue sans nul doute possible le premier maillon de toute politique de sécurité.

QUELLE POLITIQUE ADOPTER POUR SE PRÉMUNIR ?

2. Les solutions préventives

Antivirus / Antimalwares

Ils ont pour objet de détecter et bloquer l'infiltration de virus / malwares préalablement répertoriés. Les dernières générations protègent de nombreuses menaces connues (keyloggers, backdoors, chevaux de troie…) auxquelles s'ajoutent, pour les plus sophistiqués, la détection des attaques de type phishing, ingénierie sociale, vol d'identité, et déni de service.

Attention, les antivirus fonctionnent comme les vaccins.
Ils ne sont efficaces que contre les virus connus et affichent leur limite lors de l'apparition de nouveaux rançongiciels ou de nouvelles variantes. Il faut absolument les mettre à jour régulièrement.

Antispam

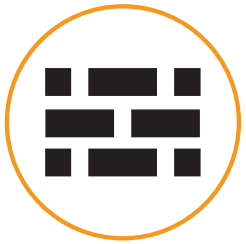
La très grande majorité des rançongiciels sont véhiculés par des campagnes d'emails.

Les antispam ont pour objet d'éviter les messages non sollicités d'émetteurs inconnus, ce qui constitue un premier rempart contre les vagues d'attaques massives et non ciblées.

Les Mises à jour

Quand une faille a été utilisée par un cybercriminelle et que cette vulnérabilité est repérée par l'éditeur, il embarque une réparation (un patch) dans la mise à jour suivante.

Il est donc nécessaire de maintenir son système à jour.



Pare-feu (Firewalls et New Generation FireWall)

Les pares-feux ont pour mission de séparer votre réseau informatique de l'internet en monitorant et filtrant, via des règles préétablies, le trafic entrant et sortant sur le réseau informatique.

Ils vous mettent à l'abri des sites internet malicieux.

Malheureusement, ils ne peuvent rien contre les sites légitimes mais infectés.

Politique de Gestion des mots de passe

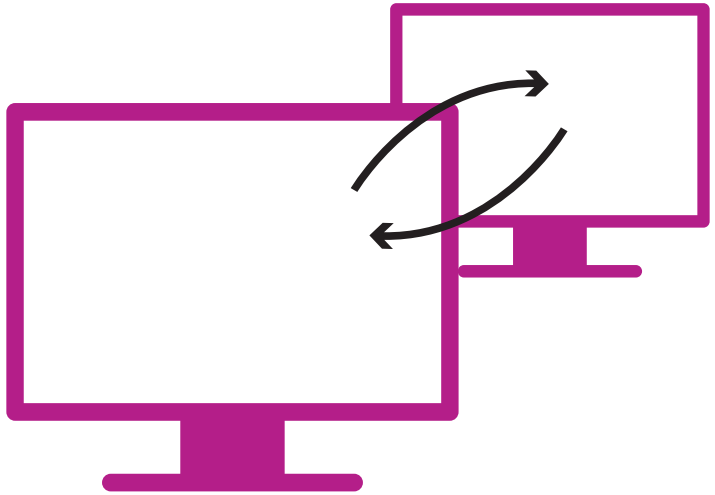
Les mots de passe sont rarement modifiés par les collaborateurs et, plus grave, souvent communs à toutes leurs applications, privées comme professionnelles.

Deviner le mot de passe d'un utilisateur à partir des activités d'un utilisateur sur les réseaux sociaux n'est pas une tâche difficile pour un hacker professionnel.

Pour vous prémunir, vous pouvez utiliser des solutions professionnelles de gestion de mot de passe au sein de votre organisation.

QUELLE POLITIQUE ADOPTER POUR SE PRÉMUNIR ?

3. Les solutions curatives



Quand les mesures préventives se sont avérées inefficaces et que le rançongiciel est dans la place, la solution ultime demeure une solution de sauvegarde professionnelle embarquant un plan de reprise d'activité après sinistre.

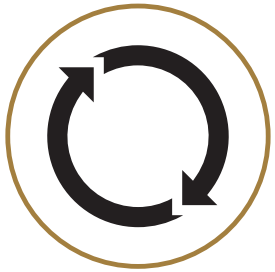
Les solutions professionnelles conservent vos fichiers dans un format crypté, ils ne peuvent donc pas être cryptés à nouveau.

Seule une solution professionnelle vous garantit la restauration de la dernière version intègre de vos fichiers.

QUELQUES CONSEILS UTILES POUR PREVENIR UNE ATTAQUE RANCONGICIELLE

Ne pas ouvrir les documents en pièces jointes d'un message électronique non sollicités

Désactiver l'exécution automatique des macros dans les suites bureautiques



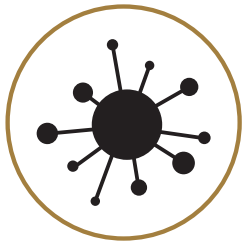
Maintenir à jour le système d'exploitation et l'antivirus de vos postes de travail, ainsi que votre navigateur internet

Optez pour un logiciel de sauvegarde proposant la fonctionnalité permettant de sauvegarder plusieurs versions d'un même fichier.

Souscrivez à une assurance Cybercriminalité qui vous couvrira en cas de survenance d'un sinistre

Couverture de : Votre responsabilité suite à la perte ou au détournement de données, les frais de notification aux propriétaires des données, les honoraires d'une société spécialisée pour identifier et colmater la faille de sécurité, les frais des tentatives de restauration des données perdues, les frais de remise en ligne d'un site internet endommagé, la perte de revenus consécutive à une cyber attaque, les honoraires de communication de crise, le montant de la rançon ou d'intermédiation avec les criminels, et les honoraires des consultants spécialisés en cas d'extorsion.

Que faire en cas d'attaque ?



Isolez le parasite

Si vous avez malencontreusement cliqué sur le lien et téléchargé un Ransomware, nous vous recommandons d'**éteindre immédiatement le poste infecté et de le déconnecter du réseau.**

L'objectif est de **bloquer le travail du parasite et si possible sa diffusion sur le réseau ou à vos contacts contenus dans votre messagerie.**

Recherchez et supprimez tous les messages similaires dans les boîtes de messagerie des utilisateurs connectés à votre réseau informatique.

Procédez enfin à une réinstallation complète du poste infecté et à la restauration des fichiers à partir d'une sauvegarde réputée saine.

Alertez les autorités

Vous pouvez adresser directement un courrier au Procureur de la République du Tribunal de Grande Instance dont relève votre siège social. Vous pouvez également envoyer un courrier électronique au Ministère de l'Intérieur.

Ces démarches permettent non seulement de mesurer l'ampleur des dommages causés mais surtout **de dégager votre responsabilité en cas de poursuites judiciaires** éventuelles de tiers.

Déposez également une plainte auprès de la police. Idéalement, cela doit être fait au commissariat de la ville où le crime a été commis. Cette plainte sera produite comme preuve auprès de créanciers éventuels.

Pour signaler un courriel malveillant ou une escroquerie :

Info escroqueries : 0811 02 02 17

(Prix d'un appel local)

www.internet-signalement.gouv.fr

Annexe

PANORAMA DES RANÇONGICIELS LES PLUS CONNUS

BETABOT – CERBER

Le cheval de Troie BETABOT et le rançongiciel CERBER sont deux acteurs bien connus du paysage cybercriminel :
le premier s'emploie à **dérober les mots de passe** stockés sur les équipements infiltrés, le second les **infecte et crypte les données** qui y sont stockées **afin de rançonner les victimes**.

Cette fois, ils s'associent afin d'accroître la rentabilité des campagnes malveillantes menées par des cybercriminels.

Au produit de la vente des mots de passe dérobés sur le dark net, (approximativement 170€ au cours du marché actuel), s'ajoute le fruit de la rançon, 1 bitcoin, soit 646€, payée dans plus d'un tiers des cas en milieu professionnel.

CRYPTOWALL

Celui-ci **affecte les utilisateurs de Windows** et c'est l'un des logiciels escrocs les plus populaires à l'heure actuelle.

Il peut entrer dans votre système si vous visitez des sites web malveillants ou si vous cliquez sur un message imitant une mise à jour de plugin.

CryptoWall est un surdoué prometteur ayant inspiré de nombreux fans tels que Cryptorbit, CryptoDefense, CryptoWall 2.0 et CryptoWall 3.0.

CRYPTOLOCKER

L'éditeur d'antivirus Kaspersky estime qu'il procure **90M€ de revenus tous les 100 jours à la communauté de cybercriminels qui l'exploite.**

Il est la **star incontestée du milieu...**

Apparu il y a plus de vingt ans dans sa forme originale, il a inspiré de multiples variantes utilisables aussi bien en version spam que kit d'exploit. **Il encrypte les fichiers présents sur la machine infectée mais aussi les disques durs externes attachés ou les serveurs de fichiers (NAS) trouvés sur le réseau.** Il limite son action aux fichiers issus des suites bureautiques (Microsoft Office ou Open Document) ainsi qu'aux fichiers au format image.

CTB-LOCKER

Le roi de l'affiliation préfère **sous-traiter la diffusion de ses codes malveillants** à des partenaires complices en échange d'un partage des revenus. Une stratégie très efficace **pour toucher une cible élargie et planétaire en un temps record.**

Il utilise une technique d'encryption appelée Elliptic Curve Cryptography.

Sa cible de fichiers est plus large que celle des cryptolockers.

Annexe

PANORAMA DES RNÇONGICIELS LES PLUS CONNUS

LOCKY

Locky préfigure la nouvelle génération des rançongiciels. Son ingénierie en apparence très simple, une pièce jointe infectée dans un spam, s'avère redoutablement **efficace puisqu'il infecte un très large spectre de format de fichiers.**

Il a acquis ses lettres de noblesse dans la communauté interlope début 2016 en attaquant un très grand nombre d'organisations professionnelles à l'échelle internationale.

Il fait un retour remarqué au second trimestre 2017 en exploitant une faille zéro day de microsoft qui le rend quasi indetectable par les antivirus du marché, lesquels ont tardé à patcher leurs codes.

KERANGER

Ce rançongiciel peu connu cible spécifiquement les applications **Mac OSX** jusqu'ici relativement préservées de la cybercriminalité.

Il s'installe en même temps que Transmission 2.9 (logiciel BitTorrent) **et commence à crypter les données du postes infectés après 3 jours d'incubation, via une connexion anonymisée Tor sur un serveur distant.**

KeRanger, toujours en développement, tente aussi de chiffrer les fichiers de sauvegarde Time Machine, rendant alors toute restauration de données impossible, **d'où la nécessité pour les PME sous Mac OSX d'opter pour une solution de Sauvegarde et de Restauration Informatique Professionnelle.**

TESLACRYPT

TeslaCrypt exploite tout particulièrement une faille de la suite Adobe en s'appuyant sur Angler et le chiffrement AES.

Diffusé à très large échelle sous forme d'email infecté il fait preuve de compassion à l'égard des victimes en leur offrant comme réconfort une large variété d'options pour régler l'addition (Bitcoin, coupon…).

TORRENTLOCKER

Non seulement TorrentLocker crypte les données pour vous rançonner mais il en profite pour récupérer votre carnet d'adresses afin d'infecter les contacts via votre messagerie.

TorrentLocker utilise des techniques d'attaques ciblées qui n'ont rien à envier aux meilleurs société de marketing : géomarketing, message personnalisé…

Ce livre blanc a-t-il été utile pour compléter vos connaissances ?

Pour évaluer les capacités des différentes solutions à satisfaire vos besoins,
un outil d'aide à la décision est mis à votre disposition en annexe de ce livre blanc

Téléchargez aussi :
le livre blanc sur les bonnes pratiques de la sauvegarde informatique en PME

A propos de Wooxo

Wooxo est un éditeur français de solutions spécialisé dans la protection et l'exploitation sécurisées du patrimoine professionnel et figure dans le TOP 100 des Editeurs verticaux du Classement EY-L'Express.
Il propose une suite logicielle modulaire articulée autour des trois besoins fondamentaux des PME :

YOO BACKUP — Sauvegarde et Restauration

YOO SYNC — Synchronisation et Partage de Fichiers

YOO FIND — Moteur de Recherche Documentaire

Les solutions Wooxo sont proposées en Cloud Pro, Cloud Hybride ou Cloud Privé.

WOOXO
IT security for business continuity

Membre du Pôle Mondial de Compétitivité des Solutions Communicantes Sécurisées (Rousset – 13),
Wooxo a été reconnu entreprise innovante en 2011, a remporté le Trophée TIC de la Meilleure Application Cloud de l'année 2012
et a été nommée Entreprise d'Avenir au Trophée EY (Anciennement Ernst and Young) 2013 et 2014