LES RANÇONGICIELS

Octobre 2016

La technologie nous pousse souvent à évoluer. C'est aussi le cas pour des gens qui en profitent pour imaginer de nouvelles façons de s'attaquer à nos biens. Ils utilisent des logiciels malicieux, appelés *rançongiciels de chiffrement*, pour prendre en otage nos fichiers. Ils promettent ensuite de les « libérer » si nous acceptons de payer une rançon.

Ce document est conçu pour aider à combattre ces attaques. Il explique ce phénomène qui est souvent mal compris. On y retrouve aussi des trucs pour ne pas tomber dans les pièges que nous tendent ces pirates cachés derrière leur clavier.

Ça ressemble à quoi?

Nous pouvons diviser les rançongiciels en deux catégories : les rançongiciels sans chiffrement de fichiers et ceux avec chiffrement.

L'auteur du rançongiciel sans chiffrement de fichiers utilise la peur ou la honte. C'est une forme de chantage. Le moyen le plus classique consiste à afficher un message qui occupe tout l'écran. Aucun autre programme ne peut être exécuté sur l'ordinateur. Nous devons verser le montant de la rançon si nous voulons retrouver l'usage de notre poste de travail. Pour ce type de rançongiciel, le contenu du disque n'est pas touché. Éliminer le rançongiciel permet de retrouver l'usage de l'ordinateur.

Diverses stratégies sont utilisées pour nous convaincre de verser une rançon. On nous informe que refuser de débourser entraînera des conséquences plus graves. Par exemple, le rançongiciel « FBI » tente de nous convaincre que nous sommes l'auteur d'un crime. Une amende nous est imposée. Si nous ne payons pas, une peine d'emprisonnement sera appliquée. Dans certains cas, on utilise la caméra de l'ordinateur pour ajouter une photo de nous au message. Ceci ajoute une touche de réalisme.

Le rançongiciel avec chiffrement de fichiers rend impossible l'accès au contenu des documents en chiffrant les fichiers. Les comportements généralement observés sont :

- L'ajout d'un suffixe étrange aux noms des documents (exemple : [nom de document]infected.doc);
- L'ajout de nouveaux documents qui contiennent une demande de rançon;
- L'ouverture de plusieurs documents échoue et le système indique qu'ils sont corrompus.
- Une fenêtre peut également s'ouvrir, indiquant que nos fichiers ont été chiffrés.

Lorsque le rançongiciel a terminé son travail, une fenêtre s'affiche. On y mentionne que les fichiers ont été chiffrés.

DANS CE NUMÉRO

Du verbiage technique indique qu'aucun moyen technologique ne libérera les fichiers. Le seul moyen, selon le message affiché, est de verser le montant de la rançon. Le montant est souvent fixé en **Bitcoin**. Une limite de temps nous est impartie. Si le délai est dépassé, le montant de la rançon augmente ou les fichiers sont perdus.

Le **Bitcoin** est une monnaie virtuelle.

L'ordinateur demeure utilisable. Des instructions détaillées et du support sont offerts pour verser la rançon. Une fois la rançon versée, un outil qui permet de déchiffrer les fichiers est offert. Éliminer le rançongiciel sur le poste ne permet cependant pas de retrouver l'accès aux données.

LES RANÇONGICIELS NE DATENT PAS D'HIER…

Saviez-vous que le plus vieux rançongiciel a été créé en 1989? En voici un exemple qui fonctionnait sous le système d'exploitation DOS. À cette époque, les cybercriminels étaient davantage motivés par la gloire que l'argent.

Qu'est-ce que j'ai à perdre?

Nous pourrions croire que les rançongiciels de chiffrement s'en prennent uniquement aux informations des entreprises ou des organismes publics. Les rançongiciels s'intéressent aux fichiers qui représentent une valeur pour nous. Ils ne touchent pas seulement les textes ou les feuilles de calcul, mais tous les types de fichiers.

Notre comptabilité, les données liées à nos achats deviennent inutiles si elles sont chiffrées. La situation est pire si nous n'avons pas conservé une copie bien à l'abri des attaques.

Si nous nous faisons berner, nous perdons des fichiers qui sont plus difficiles à remplacer. Pensons aux premières images de notre fille, à celles du mariage de notre aîné. Et si c'était les vidéos d'anniversaire notre grand-mère centenaire ou les premiers pas –de notre petit-fils? Les rançongiciels ne font pas de différence entre un souvenir précieux et les données plus banales.

Savoir ce que nous risquons de perdre à cause des rançongiciels permet de réaliser que les efforts pour s'en protéger représentent bien peu. Effectuer des prises de copies de nos données nous prépare à réagir après une attaque. Mieux! Adopter quelques règles de conduite simples nous protège contre ces attaques. Ce sont ces petits gestes qui sauvent!

Comment ça s'attrape? Comment s'en protéger?

Un rançongiciel, tout comme d'autres codes malicieux, infecte un poste de travail et exécute une **charge utile**. Dans ce cas-ci, un programme chiffrera les fichiers de l'ordinateur sur notre disque ou sur le réseau local si notre poste y est connecté.

Une **charge utile** est la partie de code exécutable d'un virus qui est destiné à nuire.

Comment ça s'attrape?

- En profitant de failles que lui offre le poste où les composantes logicielles ne sont pas à jour;
- Avec l'aide de l'utilisateur du poste qui agit avec imprudence ou légèreté.

EXEMPLES DE COMPOSANTES LOGICIELLES

- Système d'exploitation (Windows, Linux, Mac OS X)
- Suite bureautique (Microsoft Office, LibreOffice, iWork)
- Autres logiciels et applications (antivirus, lecteur PDF)
- Modules enfichables au navigateur web (Flash Player, Adobe Reader, Java, Shockwave, etc.).

Souvent, les arnaqueurs utilisent le courriel pour tromper notre vigilance en piquant notre curiosité avec un :

- Lien vers un site web où nous pouvons, soi-disant, voir des photos inédites de vedettes ou d'autres personnalités;
- Document dont nous ne devrions pas être le destinataire et qui nous incite à l'indiscrétion : bon de livraison, rapport, etc.

Ces liens ou documents cachent du code malicieux qui servira à exploiter une faille du poste de travail.

Nous jouons un rôle de premier plan dans la stratégie de défense contre les rançongiciels.

Comment s'en protéger?

- En appliquant rapidement les plus récents correctifs disponibles pour toutes les composantes logicielles installées sur le poste;
- En tant qu'utilisateur, agir avec prudence et développer une conscience des dangers potentiels :
  - Détecter et identifier les courriels dont l'expéditeur nous est inconnu ou avec lequel nous ne communiquons pas habituellement;
  - Ignorer l'invitation à consulter un site web dont nous ignorons la nature;
  - Éviter d'ouvrir un document reçu en pièce jointe d'un courriel dont nous ne sommes pas le destinataire « conscient »;
  - Si nous nous trouvons en présence de courriels de ce genre, nous devons en informer le centre d'assistance et suivre ses instructions. L'analyse de ces courriels contribue à renforcer les mesures mises en place pour les bloquer.

Zut, mes fichiers sont chiffrés!

Quand nous perdons l'accès à nos fichiers parce qu'un rançongiciel les a chiffrés, plus rien ne va! Dans cette situation, réagir avec méthodologie peut permettre de réduire les dégâts et d'éviter une autre attaque.

Malgré nos efforts, un rançongiciel sévit sur notre ordinateur. Avec un peu de chance, le comportement de notre ordinateur indique que quelque chose ne va pas. Dans la majorité des cas, le rançongiciel a déjà chiffré nos fichiers et empêche leur utilisation. C'est un message de rançon qui nous indique le problème. Mais il est déjà trop tard. Le mal est fait.

La meilleure attitude à adopter est de prendre une grande respiration et de rester calme. Notre but est de restaurer nos fichiers. La démarche comporte trois étapes. En premier lieu, nous voulons faire cesser les actions du rançongiciel pour éviter qu'il récidive. Nous nous assurons ensuite d'éliminer toute trace du logiciel malveillant. Une fois l'ordinateur propre, nous pouvons restaurer nos fichiers.

Bloquer les actions du rançongiciel. Le premier objectif à atteindre dans notre bataille contre le logiciel malveillant est de l'empêcher de prendre d'autres fichiers en otage. Pour y arriver :

1. Nous débranchons le câble réseau;
2. Nous débranchons les disques et les clés USB.

RÉAGIR AUX RANÇONGICIELS AU TRAVAIL

Si nous constatons qu'un rançongiciel touche notre ordinateur au bureau, nous devons poser ces gestes :

1. Nous débranchons le câble réseau.
2. Nous arrêtons l'ordinateur.
3. Nous contactons immédiatement le centre d'assistance et nous suivons les consignes données par la personne qui nous assiste.

Nettoyer l'ordinateur. Malgré la frustration de perdre nos fichiers, nous devons enlever le rançongiciel. Notre but est de l'empêcher de recommencer. Si nous ne sommes pas à l'aise, nous demandons à une connaissance qui s'y connaît ou nous payons les services d'un technicien qualifié. Nous essayons plusieurs techniques, nous pouvons même en combiner plusieurs, jusqu'à ce que l'ordinateur soit « propre » :

- Démarrer l'ordinateur à partir d'un cédérom ou d'une clé USB et utiliser un logiciel spécialisé (exemple : « Windows Defender Offline »;
- Restaurer le système au démarrage de l'ordinateur;
- Désinfecter à l'aide d'un outil spécialisé. Le cédérom Malekal est un exemple d'outil qui peut s'avérer utile dans le cas de rançongiciels;
- Bien que cela demande plus de travail, la réinstallation complète constitue la meilleure solution pour s'assurer que l'ordinateur est à nouveau digne de confiance.

Restaurer les fichiers. Une fois que nous avons la certitude que l'ordinateur est bien nettoyé, il est temps de retrouver les fichiers touchés par l'attaque du rançongiciel.

La meilleure méthode consiste à récupérer les fichiers à partir d'une copie de sécurité qui a été effectuée avant l'action du rançongiciel. Pour garantir l'intégrité des fichiers à récupérer, la copie de sécurité doit avoir été conservée hors de l'ordinateur touché par l'attaque.

Il est aussi possible d'utiliser, en mode sans échec, un logiciel spécialisé comme celui publié par ESET ou TeslaDecoder.

Même si nous possédons les connaissances et les outils appropriés, se relever de l'attaque d'un rançongiciel de chiffrement est une expérience pénible. Effectuer régulièrement la prise de copies de sécurité de nos informations permet de s'en remettre plus facilement.

Ajuster son comportement en suivant quelques règles simples pour la navigation et la lecture du courrier électronique constitue le meilleur moyen d'éviter ce genre d'ennui. Ces mêmes gestes nous protégeront aussi contre la plupart des codes malicieux qui peuvent menacer nos informations. Comme pour notre santé, la prévention est plus agréable que de soigner un problème!

PAYER LA RANÇON, UNE BONNE IDÉE?

Le rançongiciel a pris nos données en otage et promet de nous en redonner l'accès si nous acceptons de payer un montant d'argent. Est-ce que payer permet de résoudre nos problèmes?

Non. Dans la plupart des cas, même si une rançon est payée, les malfaiteurs ne remettent pas la clé qui permet de redonner l'accès à nos informations. Nous avons aussi observé certains cas où une clé était fournie pour regagner l'accès aux données en échange du paiement. Quelques jours plus tard, les données avaient été de nouveau chiffrées et une seconde rançon était demandée.

Peut-être. Si tout a été essayé sans succès et que l'importance des fichiers chiffrés vaut le risque de payer, nous pouvons considérer le paiement comme une solution de dernier recours. Il faut par contre se faire à l'idée de perdre à la fois notre argent et nos fichiers.

Une affaire de gros sous

Tout comme d'autres activités criminelles, l'extorsion a pris le virage du monde numérique. On parle alors de cyberextorsion, dont la forme la plus connue est le rançongiciel de chiffrement.

La cyberextorsion, bien qu'elle ne soit pas un phénomène nouveau, est en pleine expansion. L'avènement de crypto-monnaies comme le Bitcoin et le coût relativement minime pour démarrer une campagne d'extorsion par rançongiciels ne sont pas étrangers à cette recrudescence. Comme les risques de se faire prendre sont faibles et que le retour sur l'investissement est élevé, cette activité est très attrayante pour les cybercriminels.

Le rançongiciel peut procurer aux cybercriminels un retour sur l'investissement de l'ordre de 1000 % à 2000 %.

Plusieurs groupes de cybercriminels motivés par les gains monétaires s'adonnent déjà à d'autres activités illicites. Les rançongiciels ne sont, pour eux, qu'une autre façon de générer des revenus.

Certains cybercriminels écrivent leur propre code. Cependant, la majorité choisit plutôt de se procurer un rançongiciel prêt à l'emploi. Il n'est pas rare que des **trousses d'exploitation** intègrent le rançongiciel parmi une panoplie d'autres outils de piratage prêts à l'emploi. Le cybercriminel doit parfois débourser une somme d'argent substantielle. À titre d'exemple, une trousse d'exploitation dans son intégralité (y compris le code source) peut se vendre entre 20 000 et 30 000 dollars sur le marché noir. Plusieurs opteront pour des locations de durées limitées (500 $ / mois).

Une **trousse d'exploitation** est un outil que les cybercriminels utilisent pour exploiter les vulnérabilités de notre système et l'infecter par des logiciels malveillants.

En 2015, des pertes de plus de 24 M$ ont été rapportées à la suite d'attaques de rançongiciels. De nombreuses victimes sont réticentes à signaler les cas d'extorsion par rançongiciel. Selon le FBI, les chiffres avancés ~~ne~~ présenteraient qu'une partie du phénomène.

Pour les trois premiers mois de 2016 seulement, les cybercriminels auraient extorqué 209 M$. Le FBI prévoit que l'extorsion par rançongiciel pourrait rapporter aux cybercriminels jusqu'à 1 G$ US d'ici la fin de l'année. En plus du paiement de la rançon, ce phénomène cause des pertes financières encore plus élevées.

Cette cyberextorsion vise les organisations de toutes tailles. Le montant d'une rançon peut s'élever à plus de 10 000 $.

Les rançongiciels rapportent de gros sous. Il est à prévoir que les cybercriminels continueront d'exploiter cette activité compte tenu du faible niveau de risque de se faire prendre et des profits qu'elle peut leur procurer.

Un utilisateur averti en vaut deux

Les antivirus sont la première ligne de défense contre les rançongiciels de chiffrement même s'ils ne sont pas toujours en mesure d'arrêter les attaques les plus sophistiquées. C'est pourquoi la prévention demeure un élément clé pour éviter d'être victime d'une infection par rançongiciel.

Les cybercriminels adaptent continuellement leurs tactiques pour propager les rançongiciels. Ces attaques prennent souvent la forme de faux hyperliens ou de pièces jointes malveillantes. Même les personnes les plus expérimentées ne sont pas toujours capables de reconnaître une attaque.

Nous devons être vigilants et nous assurer de connaître les symptômes observables d'une infection par rançongiciel de chiffrement.

Si on est au travail, il faut signaler rapidement au centre d'assistance toute anomalie ou tout symptôme qui laisse présager une infection par rançongiciel. En cas de doute, nous devons immédiatement éteindre l'ordinateur et noter l'heure et la date où le problème a été constaté.

Protéger ses données...

Le principal inconvénient d'un rançongiciel provient de la perte de données. Les cybercriminels exploitent le fait que certains documents sont irremplaçables pour nous. Le meilleur moyen de se prémunir contre ces pertes de données est de prendre régulièrement des copies de sauvegarde. Ces copies doivent toujours être conservées sur un support qui est hors d'atteinte des rançongiciels.

UN COMPORTEMENT SÉCURITAIRE

1. Prendre des copies régulières de nos fichiers et les garder hors de l'ordinateur.
2. S'assurer que tous les logiciels ont été mis à jour avec les plus récents correctifs de sécurité.
3. Utiliser des logiciels antivirus et antimaliciels;
4. Ne fréquenter que des sites de bonne réputation.
5. Ne pas ouvrir les fichiers joints aux courriels de source douteuse.
6. Ne pas cliquer sur les liens des courriels de source douteuse.
7. Appliquer ces mesures aux courriels inattendus qui proviennent de connaissances.

Le rançongiciel du futur

Le rançongiciel d'aujourd'hui est une menace qui touche les utilisateurs dans de nombreuses régions du monde, en particulier, ceux qui vivent dans les pays développés et qui font usage de haute technologie. Nous sommes de plus en plus connectés et notre dépendance à Internet ne cesse de s'accroître.

Il peut être délicat de faire des prédictions. Le rançongiciel est à l'image de notre monde. Il est en constante évolution tant du point de vue technologique que du point de vue social. Il est raisonnable d'affirmer que le phénomène des rançongiciels sera durable et qu'il continuera d'évoluer.

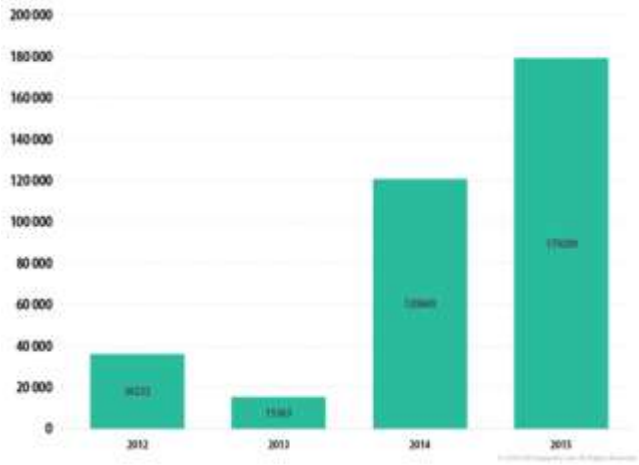
> Il faut s'attendre à voir apparaître des rançongiciels qui ciblent de nouvelles catégories d'appareils, là où ils n'ont jamais été observés jusqu'à maintenant.

Tout comme pour les maladies dans la vie réelle, les rançongiciels s'adaptent et évoluent en fonction de leur environnement. Certains survivent, d'autres disparaissent, alors que certains s'adaptent et prospèrent.

Le versement d'une rançon par la victime demeure la principale motivation des cybercriminels et ce, peu importe les innovations ou la technologie visée. Le meilleur moyen d'enrayer ce fléau est de ne pas payer la rançon demandée de manière à rendre cette activité beaucoup moins attrayante.

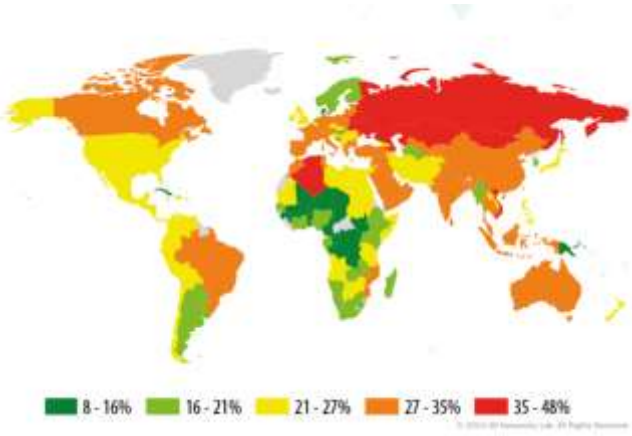
SAVIEZ-VOUS QUE?

En 2015, 179 209 utilisateurs ont vu leurs données être chiffrées par des rançongiciels et 20 % de ces chiffrements ont eu lieu dans le secteur corporatif.



Nombre de victimes attaquées par des rançongiciels de chiffrement

En 2015, 34,2 % des ordinateurs dans le monde ont été attaqués au moins une fois pendant que l'utilisateur était en ligne.



Pourcentage d'attaques par rançongiciels en ligne

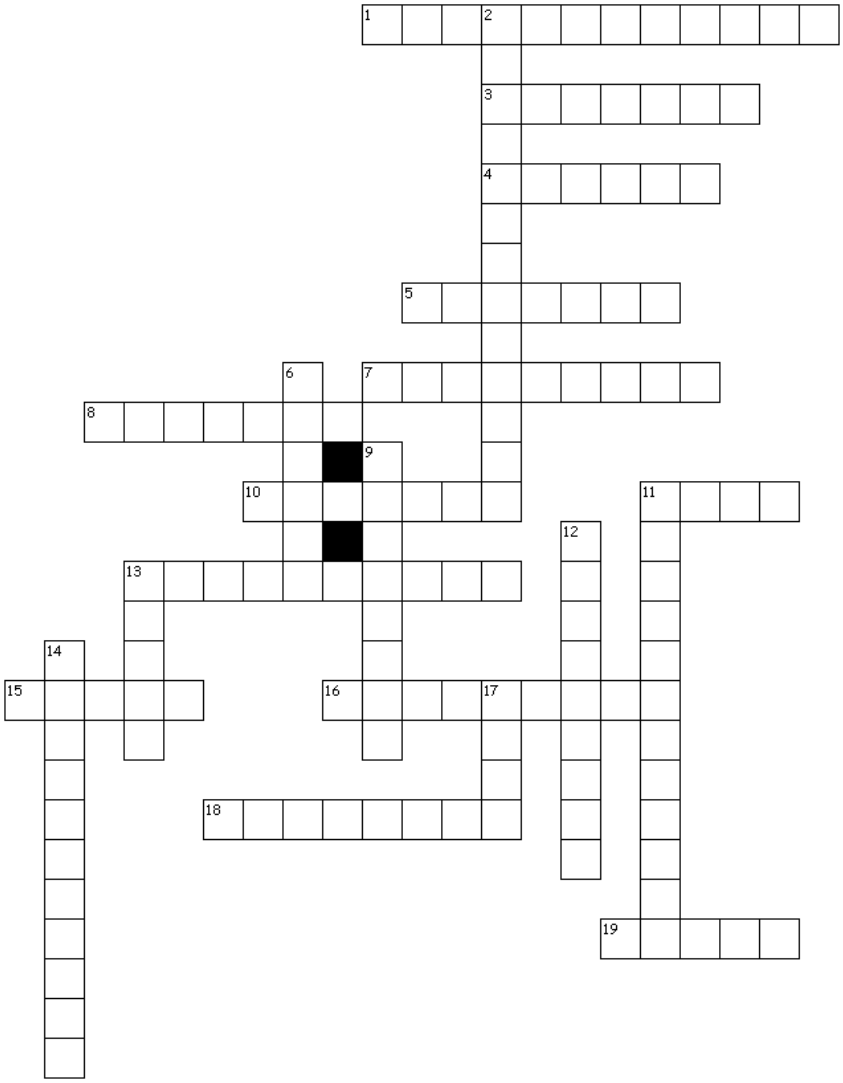
Mots croisés

Horizontal

1. Logiciel malveillant qui prend en otage les données personnelles.
3. Action pour empêcher le logiciel malveillant de prendre d'autres fichiers en otage.
4. Objectif du rançongiciel.
5. Qui affectent un élément du poste de travail.
7. Première ligne de défense contre les rançongiciels de chiffrement.
8. Monnaie virtuelle utilisée par les cybercriminels.
10. Outil spécialité de type Live CD utile pour la désinfection suite à une attaque de rançongiciel.
11. Ensemble de commandes formant un logiciel.
13. Élément clé pour éviter d'être victime d'une infection par rançongiciel.
15. Type de document pouvant être chiffré.
16. Récupérer des fichiers à partir d'une copie de sécurité.
18. Ordre de grandeur des pertes rapportées à la suite d'attaques de rançongiciel en 2015.
19. Retenu en échange d'une rançon.

Vertical

2. Individu qui commet des crimes à l'aide d'outils informatiques.
6. Spécialiste qui recherche des moyens de contourner les protections logicielles et matérielles.
9. Enlever le rançongiciel.
11. Synonyme d'attitude sécuritaire.
12. Acte criminel par lequel une personne oblige ou tente d'obliger une autre personne à accomplir un acte en usant de menaces.
13. Principal inconvénient d'un rançongiciel.
14. Procédé de cryptographie utilisé par un rançongiciel qui rend l'accès à un document impossible.
17. Le plus vieux rançongiciel, créé en 1989.



Références utiles

Saviez-vous que?
https://www.google.ca/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwirue6sz4LNAhVBHD4KHX0rBRwQFggeMAA&url=https%3A%2F%2Fsecurelist.com%2Ffiles%2F2015%2F12%2FKaspersky-Security-Bulletin-2015_FINAL_EN.pdf&usg=AFQjCNHchHHumH26Z8YLPTdthnyXsx5YJQ

Une affaire de gros sous
http://phys.org/news/2016-02-ransomware-precious.html
http://www.pymnts.com/news/security-and-risk/2016/fbi-ransomware-attacks-on-pace-to-be-1-billion-market/
https://heimdalsecurity.com/blog/ultimate-guide-angler-exploit-kit-non-technical-people/
https://heimdalsecurity.com/blog/exploit-kits-service-automation-changing-face-cyber-crime/

Zut, mes fichiers sont chiffrés!
http://windows.microsoft.com/fr-ca/windows/what-is-windows-defender-offline
http://www.malekal.com/malekal-live-cd/
http://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/
http://www.bleepingcomputer.com/forums/t/576600/tesladecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/

Le rançongiciel du futur
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf