h e g

Haute école de gestion
Genève

Etude des Ransomware : Vecteur d'attaque, fonctionnement, économie et réponse légal

Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES

par :

Leutrim Misini

Conseiller au travail de Bachelor :

David BILLARD

Genève, le 20 octobre 2017

Haute École de Gestion de Genève (HEG-GE)

Filière informatique de gestion

Hes·so GENÈVE
Haute Ecole Spécialisée de Suisse occidentale

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre de Bachelor of Science HES-SO en informatique de gestion.

L'étudiant atteste que son travail a été vérifié par un logiciel de détection de plagiat.

L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 20 octobre 2017

Leutrim Misini

Remerciements

Je tiens tout d'abord à remercier monsieur David Billard qui a accepté de suivre mon travail et qui s'est toujours montré à l'écoute de mes requêtes.

Je remercie également les personnes qui m'ont aidé à relire mon travail et qui m'ont donné leurs avis et leurs conseils.

Finalement je tiens à remercier ma famille et mes amis pour leur soutien et leur compréhension durant mes indisponibilités tout au long de ce travail.

Résumé

Le ransomware est un logiciel malveillant qui empêche la victime d'accéder à ses données. Pour ce faire, il y a plusieurs manières de procéder, par exemple en chiffrant les données ou en bloquant l'accès de l'ordinateur.

Ces manœuvres ont pour but d'obtenir le paiement d'une rançon. Une fois payée, la victime pourra accéder à ses données. Cependant payer la rançon ne garantit pas le retour des données. Ce type de logiciel est en constante évolution, il se professionnalise et infecte toujours plus de personnes.

Nous allons commencer par nous informer sur cette menace et parler de l'actualité autour des ransomwares. Nous poursuivons ensuite sur les principaux vecteurs d'attaques pour comprendre comment le ransomware arrive sur nos machines.

Nous continuions sur le fonctionnement du ransomwares avec divers exemples tels que LOCKY ou RAA. Ensuite, nous allons expliquer comment l'économie des ransomwares fonctionne. Pour conclure, nous proposerons des outils et techniques pour se défendre et réagir au ransomware.

Table des matières

Liste des figures

1. Introduction

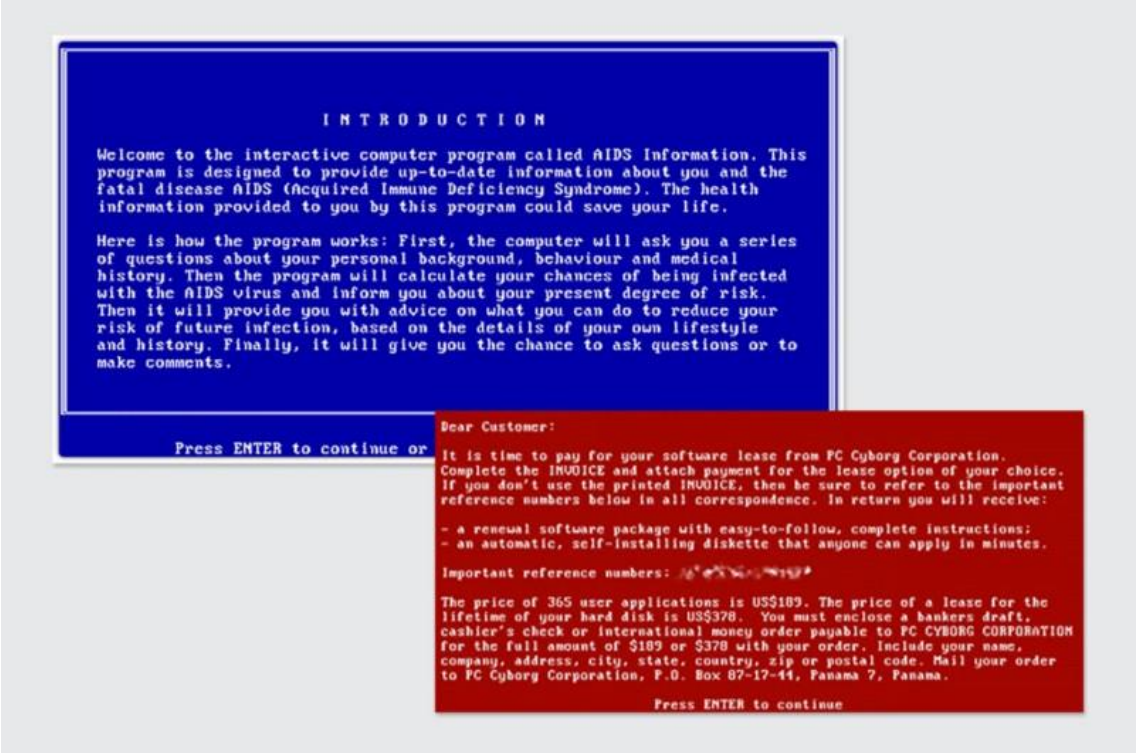
1.1 Historique

1.2 Le 1er ransomware

Ces derniers années les ransomwares ont fait la une des actualités du monde entier, mais ce genre logiciel ne date pas d'hier. Le premier type de ransomware est apparu en 1989. Il s'agit du Trojan AIDS aussi appelé PC Cyborg. A cette époque, le sida faisait la une des journaux du monde entier. C'est à ce moment-là que le docteur Joseph Popp profite de la situation et distribue environ 20 000 disquettes à des patients, des particuliers mais aussi des institutions médicales.

Cette disquette contient un programme de renseignements sur le sida. Mais elle contenait également un ransomware qui, après quelques jours, chiffrait les fichiers de l'ordinateur pour ensuite, demander une rançon de 189 dollars. Afin de récupérer les fichiers chiffrés.

Figure 1 : Le 1er ransomware : PC Cyborg



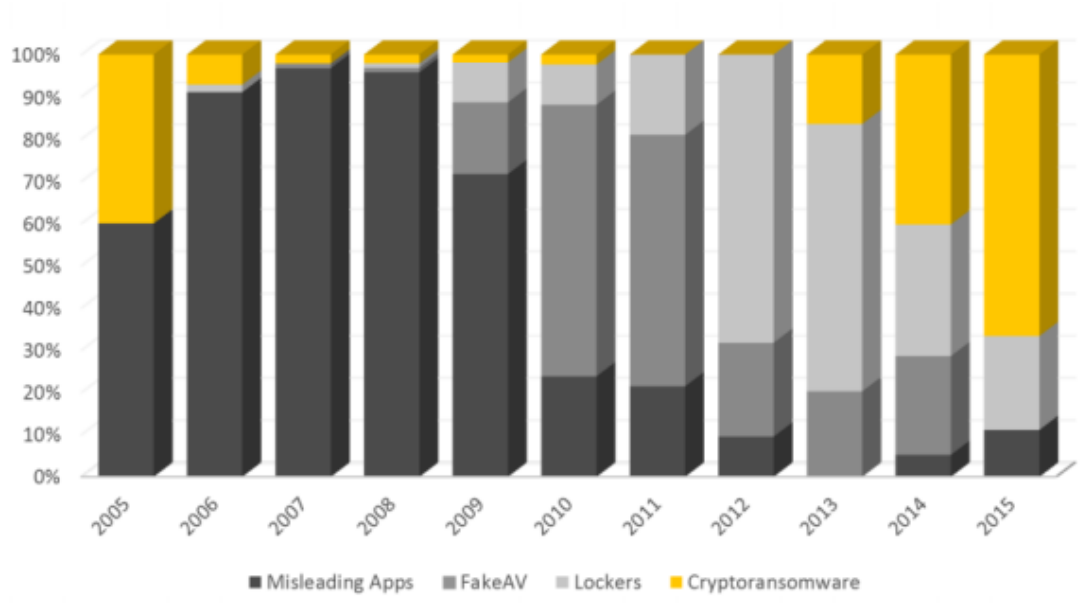
(https://medium.com/un-hackable/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b)

1.3 Année 2000

Après la première attaque de PC cyborg en 1989, les attaques de ransomware sont restées inaperçues jusqu'au milieu des années 2000. L'une des raisons est que les hackeurs écrivaient leur propre code de cryptage, ce qui était assez simple à décrypter et donc facile à contrer. Mais tout a changé quand ils ont commencé à s'appuyer sur des bibliothèques de cryptages qui sont quasiment impossibles à déchiffrer sans la clé de déchiffrement. Les premiers ransomware à utiliser des techniques de chiffrements sont arrivé 2005 (par exemple Gpcode utilisait le cryptage RSA 1024 bits).

Au fil des années, il y a deux types de ransomwares qui se sont démarqués. Le ransomware chiffrant et le bloqueur. Ces deux types de ransomware seront détaillés plus tard mais pour faire simple : le ransomware chiffrant crypte les fichiers et dossiers de l'ordinateur alors que le ransomware bloqueur verrouille les appareils. Tous les deux demandent une rançon pour permettre à la victime de récupérer le contrôle de ses données ou de son appareil.

Figure 2 : Evolution des logiciels d'extorsion



(http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf)

En analysant ce graphique qui représente le marché des logiciels d'extorsion, on peut constater que les tendances changent rapidement. Cela vient du fait que les hackeurs cherchent avant tout du profit. On peut constater que les ransomwares chiffrant sont les plus viables de nos jours.

1.4 L'explosion du ransomware

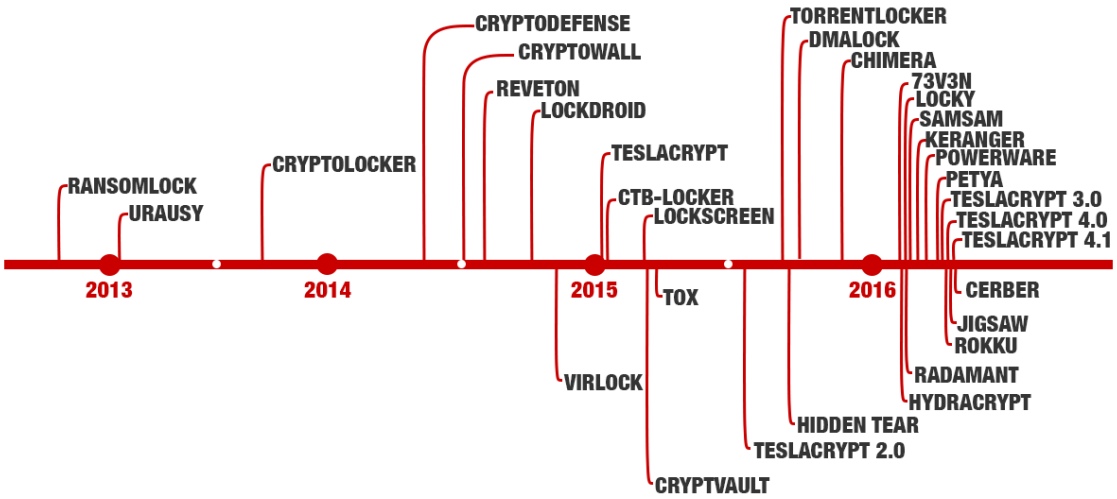
Les ransomwares ont pris une tout autre dimension et tout cela a commencé avec la popularisation du Bitcoin qui permet aux hackeurs d'être très difficile (pour ne pas dire) à tracer. De plus, les algorithmes de chiffrement sont devenus de plus en plus complexes, ce qui les rend quasiment impossible à déchiffrer sans connaitre la clé.

À tout cela s'ajoute que les ransomwares deviennent « professionnels », c'est-à-dire que les hackeurs proposent des marches à suivre pour guider les victimes lors du paiement. Certains même déchiffrent un fichier pour montrer à la victime que la clé fonctionne réellement. Cela pousse les victimes à payer la rançon étant donné qu'ils ont la certitude que les hackeurs peuvent débloquer les fichiers.

Pour les entreprises, payer la rançon est souvent l'option la moins couteuse. Donc si les entreprises ont la certitude de retrouver leurs fichiers an payant ils n'hésiteront pas.

À cause de tous ces éléments qui rendent les ransomwares viables et très attractifs niveaux financiers, leur nombre ont tout simplement explosé comme l'indique le graphique.

Figure 3 : L'explosion du nombre de ransomwares



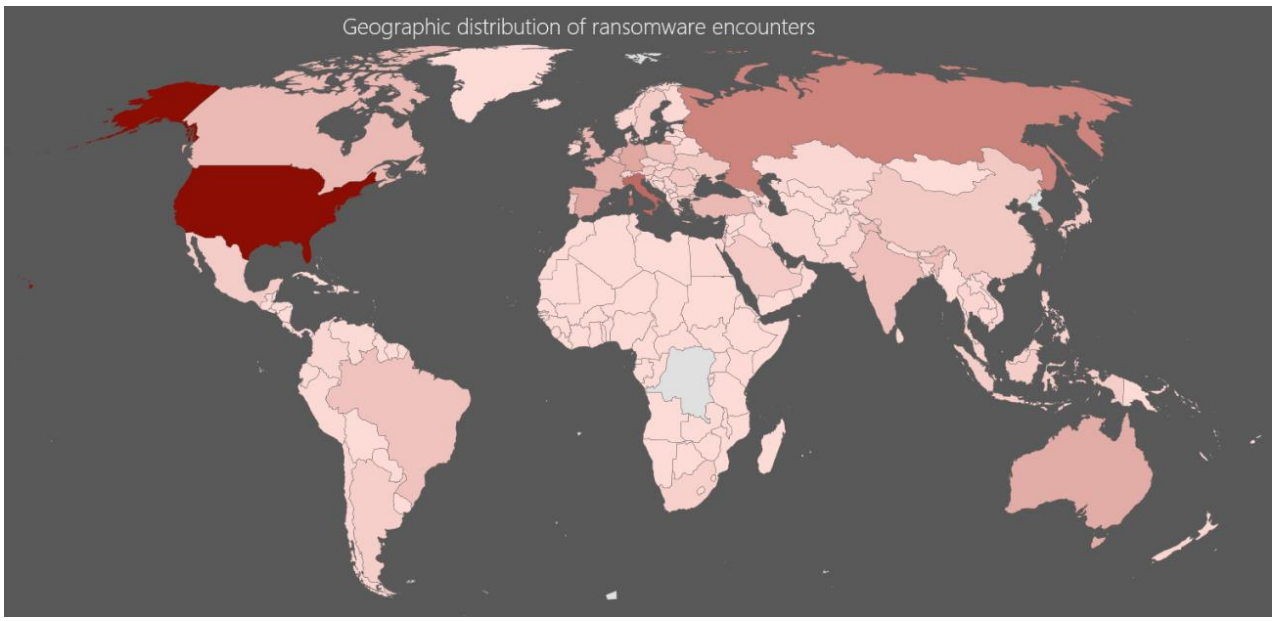
(https://www.endgame.com/blog/technical-blog/your-package-has-been-successfully-encrypted-teslacrypt-41a-and-malware-attack)

1.5 Les pays touché

Comme on peut le voir les endroits les plus touchés sont pour la plupart des pays développé. L'endroit où le ransomware est le plus répandu est aux États-Unis avec 460 000 ordinateurs infectés. Suive ensuite l'Italie et de la russe, qui avec 252 000 et 192 000 infections de ransomware sont au deuxième et troisième rang.

De plus, comme on peut le voir avec cette carte aucun pays n'est à l'abri d'une attaque de ransomware.

Figure 4 : Pays les plus touchés par les attaques de ransomware en 2016



(https://blogs.technet.microsoft.com/mmpc/2017/02/14/ransomware-2016-threat-landscape-review/)

1.6 Attaques ransomwares qui ont été médiatisées

Aujourd'hui, les attaques de ransomwares font la une des journaux du monde entier. L'impact des ransomwares est devenu trop important pour qu'ils restent inaperçus. Prenons l'exemple des hôpitaux qui sont devenus des cibles intéressantes pour les hackeurs.

Les conséquences d'une attaque de ransomware sont lourdes pour un hôpital. Ce n'est plus qu'une question de perdre une photo de famille mais de patients qui voient leurs rendez-vous annulés ou qui sont obligés d'être envoyés vers d'autres hôpitaux. Les hôpitaux sont donc rapidement forcés à payer la rançon en espérant retrouver leurs données.

Articles sur les attaques d'hôpitaux :

- Hôpital de Los Angeles (Lien)
- Hôpitaux en Allemagne (Lien)

Les hôpitaux ne sont pas les seules institutions qui ont été victimes d'attaques de ransomwares. Les médias, les commissariats et même les universités, personne n'est à l'abri d'une attaque de ransomware.

Articles sur les différentes attaques :

- Université of Calgary (Lien)
- Commissariat de police (Lien)
- Média New York Times, BBC (Lien)

Les établissements se retrouvent bloqués avec des fichiers inutilisables. Ils ne peuvent simplement plus travailler et donc bien trop souvent ces attaques se terminent par le paiement de la rançon pour récupérer les fichiers cryptés.

1.7 Qui sont les cibles ?

Quelles sont les meilleures cibles pour les ransomwares ? Les particuliers ? Les institutions ? Quelles sont les raisons ?

Tout d'abord il faut savoir que personne n'est à l'abri contre les ransomwares : les particuliers, les entreprises ou encore des institutions publiques. N'importe qui peut en être la cible d'une attaque. Mais les hackeurs ont appris à mieux cibler leurs attaques.

Les raisons qui poussent les hackeurs à attaquer des particuliers sont nombreuses. Les particuliers ne font quasiment jamais de sauvegarde de leurs données. Ils manquent de connaissances en sécurité informatique ce qui les rend faciles à manipuler (par exemple ils ne font pas attention à ce qu'ils vont cliquer). Ils ne gardent pas leurs logiciels à jour. Ils utilisent des antivirus gratuits qui sont moins performants, Ils pensent que les antivirus les protègent de toutes les menaces. Les protections de bases ne sont pas mises en place (proxy, pare-feu,…).

Tous ces éléments rendent les particuliers vulnérables à une attaque de ransomware. Bien sûr, Il est évident que ces critiques ne s'appliquent pas à tout le monde et heureusement d'ailleurs. Mais il faut savoir qu'une seule petite faille peut permettre au ransomware d'infecter une victime.

En ce qui concerne les entreprises, les raisons d'attaques sont aussi nombreuses. Tout d'abord les entreprises ont de l'argent et qu'une attaque de ransomware cause beaucoup de problèmes à l'entreprise. Il y a aussi le facteur humain qui est encore sous-évalué, les hackeurs utilisent des techniques d'ingénierie sociale pour tromper les collaborateurs de l'entreprise. Les hackeurs peuvent utiliser les ransomwares pour attaquer les ordinateurs, les serveurs et même les fichiers sur les systèmes de partage. Les petites entreprises ne sont pas préparées à faire face à des attaques de ransomware. De plus, les entreprises préfèrent ne pas signaler une infection de ransomware par peur des conséquences sur l'image de l'entreprise.

En effet un tel incident peut avoir de graves conséquences sur une entreprise. Celles-ci peuvent être financières mais cela peut aussi rompre la confiance qu'ont les clients, fournisseurs ou partenaires avec l'entreprise. Par exemple qui voudrait déposer son argent dans une banque qui a été victime d'un ransomwares?

En ce qui concerne les institutions publiques les raisons ressemblent celles des entreprises à quelques exceptions près. Les institutions publiques ont aussi des collaborateurs qui sont rarement sensibilisés aux risques de l'ingénierie sociale qui est utilisé avec habilité par les hackeurs. Les hackeurs peuvent voir le fait de réussir une attaque contre une cible connu médiatiquement comme un accomplissement personnel. Mais le plus gros problème reste que les institutions publiques utilisent généralement des logiciels et des équipements qui ne sont pas à jours, donc leurs systèmes informatiques ont des failles qui n'ont pas été corrigé.

Comme on peut le voir les hackeurs peuvent s'attaquer à n'importe qui. Tout dépend des ressources et motivations du hackeur.

Figure 5 : Dommage causé par les ransomwares

(https://heimdalsecurity.com/blog/cyber-security-threats-types/)

On peut constater que 70% des entreprises paient les rançons ce qui est un énorme pourcentage. Mais comme nous l'avons dit plus haut, il est impossible pour une entreprise de travailler sans ses données. Du coup si elles n'ont pas de plan de secours, elles sont obligées de payer pour espérer récupérer les données. Une autre information importante est que l'un des vecteurs d'attaques les plus utilisés pour diffuser les ransomwares est l'envoi de email malveillant notamment le hameçonnage.

.

2. Vecteur d'attaque

On vient de voir l'impact que pouvaient avoir les ransomwares sur les entreprises, les particuliers ou les institutions. Mais comment les ransomwares arrivent sur vos ordinateurs. Il y a beaucoup de façons d'être infecté par un ransomware. Les principaux sont les suivants :

2.1 Ingénierie social

Ce moyen est surement le plus malhonnête de tous, il consiste à convaincre une personne de nous révéler une information confidentielle ou à mener la victime à exécuter des actions. Pour cela on compte sur la bonne foi ou la serviabilité de la personne.

Vous n'êtes pas sans savoir qu'en informatique la plus grande faille reste l'humain. On a beau avoir la sécurité la plus élaborée possible, il suffit qu'un collaborateur donne une information (sans pour autant que cela soit intentionnel) pour mettre en danger tout le système.

L'ingénierie sociale se passe en quatre étapes. La première étape est la récolte d'information. Cette phase consiste à rassembler des informations sur la future victime. Comme par exemple la structure de l'entreprise où elle travaille, les projets en cours, processus métiers et les logiciels utilisés. Tous ces éléments permettent d'établir une relation de confiance avec la victime lors de l'attaque.

La seconde étape est le prétexte. Après avoir récolté assez d'information il est temps pour l'attaquant de faire un scénario fiable vis-à-vis de la victime. Les informations qu'il a récolées vont lui permettre de paraître crédible devant la victime.

La troisième étape est d'utiliser le prétexte que le hackeur mit en place pour mener la victime à exécuter certaines actions ou à divulguer des informations confidentielles sur l'entreprise.

La dernière étape consiste à l'hackeur de ne laisser aucune information qui pourrait remonter à sa réelle identité.

Exemple d'un scenario d'ingénierie social :

L'attaquant se renseigne sur une entreprise, il s'informe sur le fonctionnement de l'entreprise, la hiérarchie de l'entreprise, les modèles utilisés pour les adresses e-mails ainsi que sur les projets en cours et sur quelques logiciels qui sont utilisés dans l'entreprise. Ensuite il va également s'informer sur un collaborateur en particulier de l'entreprise. Il s'informe sur le déroulement d'une journée classique pour lui et il peut également chercher ses hobbys via les réseaux sociaux.

Une fois les informations récoltées l'attaquant prépare un scénario.

L'attaquant se fait passer pour un employé du département informatique. Il prépare un email avec le même modèle qu'utilise l'entreprise cible. Il demande à la victime si elle peut télécharger et installer un correctif d'un logiciel utilisé quotidiennement car il n'a pas réussi à le déployer à distance. L'attaquant demande en quelques sorte une faveur, qui dans des circonstances normales pourraient être totalement plausible.

Malheureusement, si le collaborateur télécharge et installe le logiciel, il se retrouve piégé et il sera fautif d'avoir fait entrer le ransomware dans l'entreprise. Tout cela est possible car le collaborateur a été naïf et a voulu être serviable. Pour lui il venait simplement en aide à un collègue.

2.2 Emails

Encore une fois avec cette méthode on vise l'humain. Il y a plusieurs types d'emails qui peuvent infecter l'utilisateur :

2.2.1 L'hameçonnage

Le phishing (autre nom de l'hameçonnage) ressemble à l'ingénierie sociale. Comme pour celle-ci, le but est de se faire passer pour une personne/entité pour récupérer des informations confidentielles ou à mener la victime à exécuter des actions (par exemple cliquer sur un lien de téléchargement).

2.2.2 E-mail avec une pièce jointe malveillante

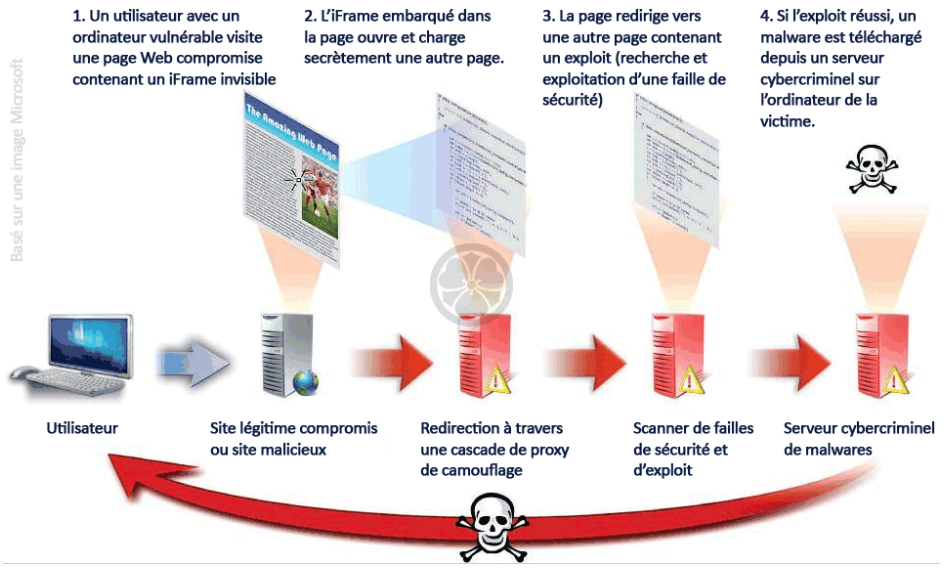
Envoyer des e-mails infectés est l'une des méthodes les plus répandues et les plus efficaces pour diffuser les ransomwares. Si la victime ouvre la pièce jointe cela peut infecter directement le système.

2.3 Drive-By-Download

Il s'agit d'un téléchargement et installation automatique sur un ordinateur. Le ransomware est téléchargé sur l'ordinateur sans demander l'avis de l'utilisateur. Il n'a même pas besoin de cliquer sur un lien.

En effet, les publicités ou pop-up de certain site web peuvent détecter des failles présentes sur l'ordinateur (généralement des vulnérabilités du navigateur ou des mauvais paramétrages de sécurité) et lancer automatiquement l'installation du ransomwares.

Figure 6 : Déroulement du drive-by download



(http://assiste.com/Drive_by_download.html)

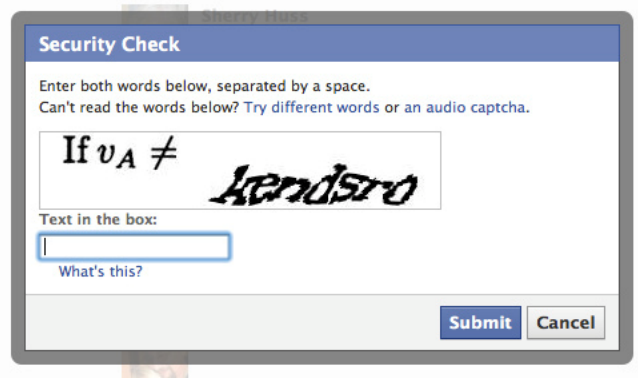
2.4 Menace interne

La menace intérieure comme son nom l'indique est que le danger vient de l'intérieur de l'entreprise comme par exemple une clef USB infecté d'un employé qui permet au ransomwares de circuler dans le système.

2.5 CAPTCHA

Un captcha est simplement un test qui permet de distinguer un humain d'un ordinateur sur le web. Certains hackeurs ont décidé d'utiliser cette méthode pour persuader la victime que le site qu'il visite est sure. Une fois le CAPTCHA tapé et validé cela lance directement le téléchargement du ransomware.

Figure 7 : Exemple de CAPTCHA



https://c1.staticflickr.com/7/6175/6208205466_73e2c190bb.jpg

2.6 Faille de sécurité

Les failles de sécurité sont simplement des erreurs que les programmeurs n'ont pas remarquées lors du développement du logiciel. Bien sûr, il a des erreurs qui sont sans importance et qui non aucune conséquence grave. Mais il y en a d'autres qui peuvent mettre en danger tout le système de l'utilisateur. Lorsqu'un hackeur découvre ce genre de faille de sécurité, il va pouvoir accéder a l'ordinateur et d'installer le ransomware. Par exemple, le ransomware WannaCry a utilisé une faille CVE-2017-0145(MS17-010) impactant l'ensemble des versions de Windows. Donc le ransomware pouvait être diffusé en passant par cette faille même si l'ordinateur est à jour. Généralement les failles sont rapidement corrigées mais souvent le mal est déjà fait.

3. Fonctionnement

Le principe de base d'un ransomware est de verrouiller le système de la victime jusqu'à que celui-ci paie une rançon qui lui permettra de reprendre le contrôle de son ordinateur ou de ses données.

3.1 Types de ransomwares

Il y a plusieurs types de ransomwares ceux qui bloquent l'écran de l'ordinateur, ceux qui chiffrent les données, ceux qui bloquent le démarrage du système et ceux qui visent les mobiles.

Les premières versions de ransomwares étaient ceux qui bloquent l'écran. En effet, cette méthode-là consistait à verrouiller l'écran de l'ordinateur jusqu'à que la victime paie la rançon. Il n'y avait aucun chiffrement de données. Du coup, il suffit de trouver un moyen de supprimer le ransomware de l'ordinateur pour récupérer les données. Après cette première vague passée, les ransomwares ont évolué et sont devenus plus variés.

Une des évolutions du ransomware est le ransomware chiffrant. Le fonctionnement de cette méthode est qu'une fois installé il chiffre les données des lecteurs réseaux, des ordinateurs ou encore des serveurs. Il y a certain qui cherche même les clés USB connectées.

Les ransomware chiffrant sont efficaces car souvent les données privées sont uniques. Donc une fois chiffré il est impossible pour la victime de récupérer avec une simple remise à zéro du système d'exploitation.

Pour chiffrer, il y a deux manières. La manière symétrique qui emploie le même mot de passe pour chiffrer et pour déchiffrer. Du coup, cette manière est plus facile à casser vu qu'elle utilise le même mot de passe. Il suffit à la victime de retrouver le mot de passe utilisé pour récupérer ses données.

Les problèmes commencent quand le ransomware utilise la façon asymétrique. Dans cette méthode il y a une clé publique qui est partagée et qui permet de chiffrer les données. Il y a aussi une clé privée, qui elle n'est pas partagée et qui est utilisée pour déchiffrer les données. La clé privée ne sera divulguée qu'une fois la rançon payer.

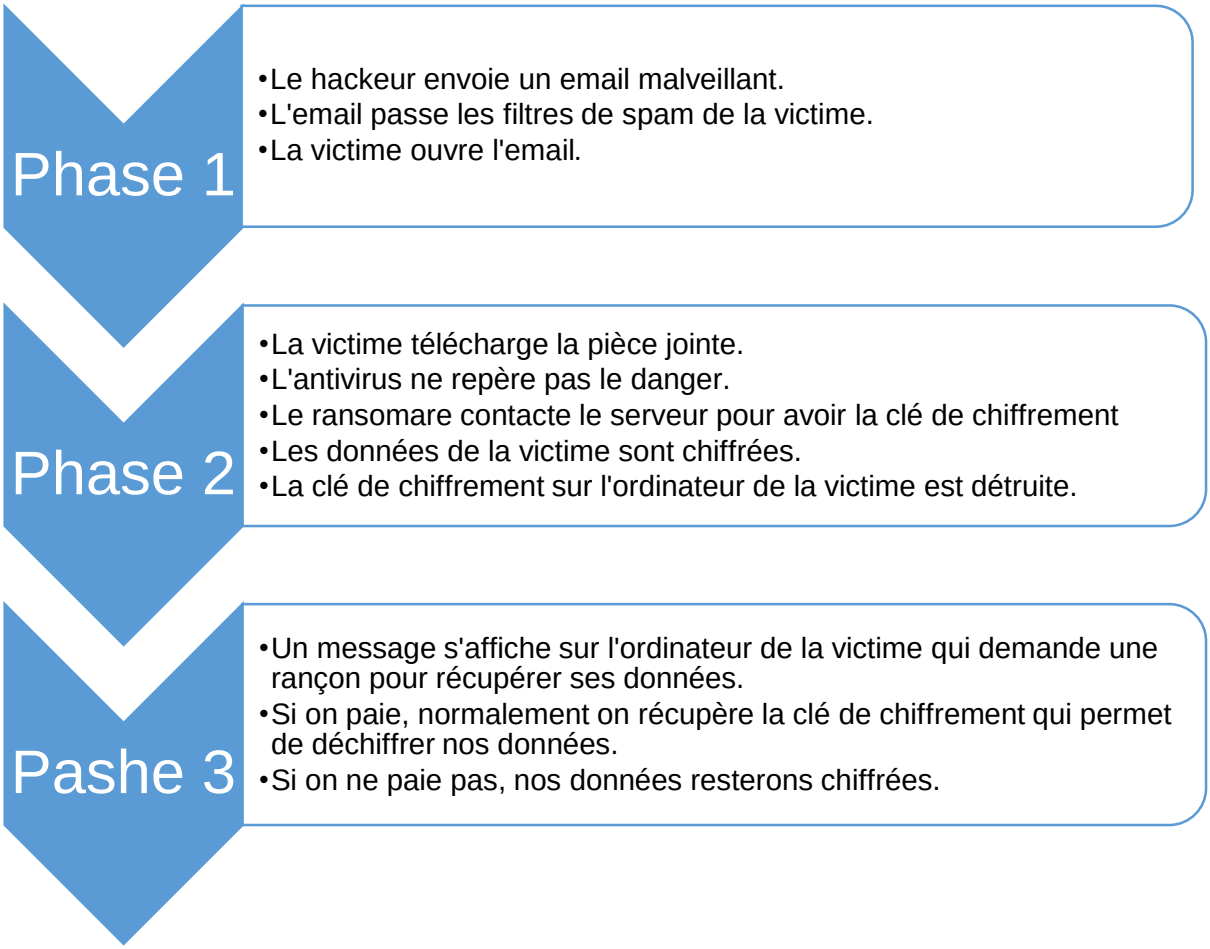
Une fois les données chiffrées, un message à l'écran s'affiche dans laquelle il y a le montant que la victime devra payer si elle veut récupérer ses données. Généralement, on demande à la victime de payer en bitcoin (crypto-monnaie), puisqu'il est très difficile à d'identifier à qui appartient les adresses de bitcoin. .

De plus, il est possible que le ransomware affiche un décompte avant qu'il ne détruise la clé privée (qui permet de déchiffrer) ou qu'il demande une plus grosse somme. Si la clé privée est détruite il est quasiment impossible de déchiffrer les données crypté.

D'ailleurs il y a des méthodes pour supprimer le ransomware de votre ordinateur mais, il faut savoir que même en le retirant de votre ordinateur, les données chiffrés ne seront pas déchiffrés. Pour cela il faut la clé privée.

Si la victime paie la rançon, elle recevra la clé privée (bien sûr n'est pas garanti à 100%). Avec cette clé la victime pourra récupérer le contrôle de son ordinateur et déchiffrer ses données.

Figure 8 : Schéma d'une attaque classique d'un ransomware



Les ransomwares qui bloquent le démarrage s'attaquent directement au disque dur, plus précisément le Master Boot Record(MBR). Le MBR c'est ce qui permet au système d'exploitation de démarrer. Le ransomware modifie cette zone pour empêcher le processus normal de démarrer. À la place du démarrage classique on a une demande de rançon qui s'affiche sur l'écran.

Évidemment, il est aussi possible que ces ransomwares chiffrent les données. Le fait de bloquer le démarrage ne les empêchent pas forcément de chiffrer les données de la victime.

En ce qui concerne les ransomware mobiles ils fonctionnent comme ceux qui bloquent l'écran de l'ordinateur. Ils bloquent l'interface de chaque application qui rend inutilisable l'utilisation du mobile pour la victime.

D'ailleurs, les ransomwares de chiffrement ne sont pas vraiment utilisés sur les mobiles car le système d'exploitation et les applications font des sauvegardes régulières dans le cloud. Ce qui veut dire que les fichiers sont sauvegardés et qu'il n'y a donc pas d'intérêt à payer la rançon.

3.2 Analyse ransomware

De manière générale, les ransomwares n'utilisent pas de faille du système à proprement parler. Les attaquants trompent les victimes comme on a pu le constater dans la partie « vecteur d'attaque ».

Évidemment, si le système visé a des failles qui ne sont pas corrigées ou ne sont pas encore repérées, les hackeurs ne vont pas se gêner pour les exploiter et pour diffuser leur ransomware à travers cette faille. Comme par exemple le ransomware wannacry qui avait exploité une faille de Windows (référencée CVE-2017-0145) pour se propager.

La manière de procéder de chaque ransomware est programmée différemment. Mais ils sont tous conçu pour ne pas être détectés par l'antivirus.

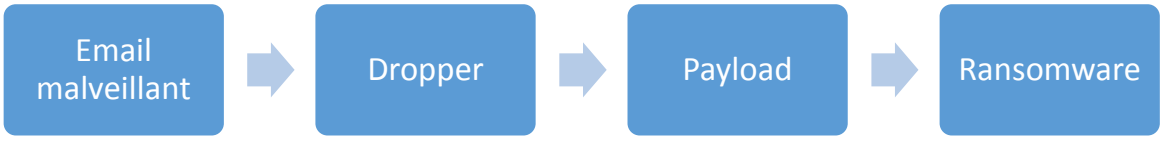
3.2.1 Dropper

Il y a plusieurs manières pour rendre indétectable le ransomware. L'une d'entre elles est le dropper. Il s'agit d'un algorithme qui va délier un programme à un autre.

En d'autres termes il y aura un dropper et un payload (le ransomware). Le dropper est chargé de lancer l'installation du ransomware sur le système. Il va séparer le ransomware de l'installeur. Pour faire simple le dropper agit comme un programme d'installation du ransomware.

Le dropper s'active lorsque la victime croit télécharger ou lancer le fichier/programme qu'il a reçu en pièce jointe. Le dropper lance furtivement l'installeur du ransomware à l'insu de la victime. Autrement dit, le dropper est un moyen de lancer l'attaque, il n'est pas en lui-même un danger mais il permet de traverser les couches de sécurités d'un ordinateur.

Figure 9 : Schéma démontrant la séparation du ransomware



3.2.2 Obfuscation

Une autre technique est « l'obfuscation ». C'est-à-dire rendre le code source incompréhensible pour l'être humain ou pour un décompilateur. Voici quelques exemples « d' obfuscations » utilisées par les malwares pour dissimuler le code :

Figure 10 :Exemple d'obfuscation

Obfuscation Example	Explanation

public class HelloWorld {
 	
public static void main(String[] args) {
System.out.println("Hello World!");
}
}
	Normal code for "Hello World!"

public class HelloWorld {
 	
public static void main(String[] args) {
System.out.println("48656c6c6f20576f726c6421");
}
}
	Data Obfuscation with Hex
	Hex encoding turns "Hello World!" into 48656c6c6f20576f726c6421.

public class HelloWorld {
 	
public static void main(String[] args) {
System.out.println("48","65en","6c","6c(fd","6f","2054","57g","6f5h","72__t","6c","64'h","21"
);
}
}
	Data fragmentation
	Adding "" around each digit and then packing it with other additional characters - in decoding only the first two bytes are read.

public class HelloWorld {
 	
cHVibGljIHN0YXRpYyB2b2lk main(String[] args) {
System.out.println("48","65en","6c","6c(fd","6f","2054","57g","6f5h","72__t","6c","64'h","21"
);
}
}
	Code Obfuscation with Base64
	Using Base64 to encode 'public static void' into cHVibGljIHN0YXRpYyB2b2lk hides the variables that determine how the "Hello World!" script is run.

https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Code-obfuscation.pdf (page 5)

Comme on peut le constater le hello world est devenu incompréhensible au fur et à mesure de « l'obfuscation ». Si on arrive à rendre aussi compliqué un simple Hello world imaginer le résultat avec un code plus compliqué. Il est évident qu'un humain n'a aucune chance de le comprendre rapidement.

De plus, le fait de transformer le code permet de dissimuler les signatures ou les comportements suspects. Du coup, cela permet de passer au travers certains niveaux de protection d'antivirus. Mais il y a aussi d'autres raisons à utiliser « l'obfuscation ». L'une d'entre elles est que le cout financier pour une telle manœuvre est faible. D'autant plus qu'elle est facile à mettre en place pour quelqu'un qui a un minimum d'expérience.

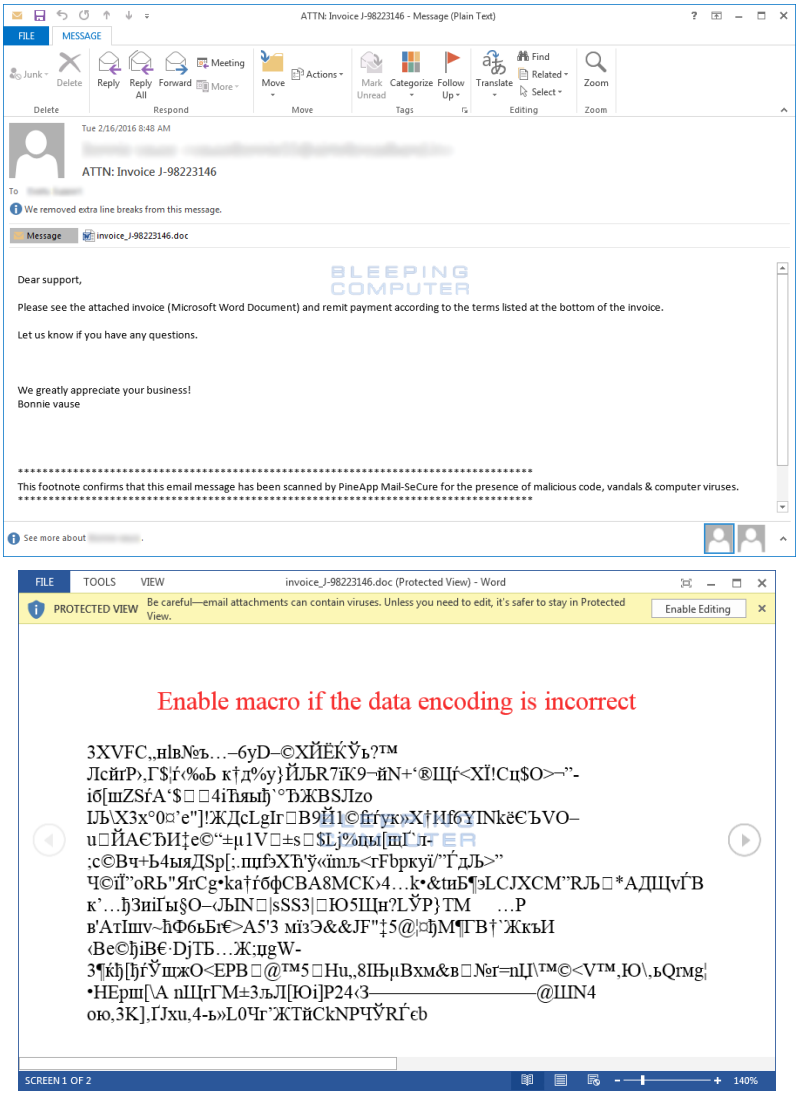
D'ailleurs, « l'obfuscation » est aussi utilisée dans le cadre de la sécurité de la propriété intellectuelle, Cette technique permet de contrer le reverse engineering (une technique pour reconstituer le code source à partir de sa forme compilée).

Maintenant que nous avons vu le fonctionnement général du ransomwares nous allons nous intéresser à certains en particulier :

3.3 LOCKY

Le ransomware LOCKY utilise l'ingénierie sociale pour infecter les victimes. La victime reçoit un mail qui lui demande de payer une facture. Généralement, le texte du message est rédigé dans la langue de la victime ce qui pousse à croire en la solvabilité de l'expéditeur. De plus, la pièce jointe est un format .doc qui est une extension connue. La victime n'a pas de raison de ne pas l'ouvrir. Une fois le fichier Word téléchargé et ouvert le texte est illisible. Du coup on demande à la victime d'activer les macros pour lire le texte.

Figure 11: Exemple d'email et de fichier Word



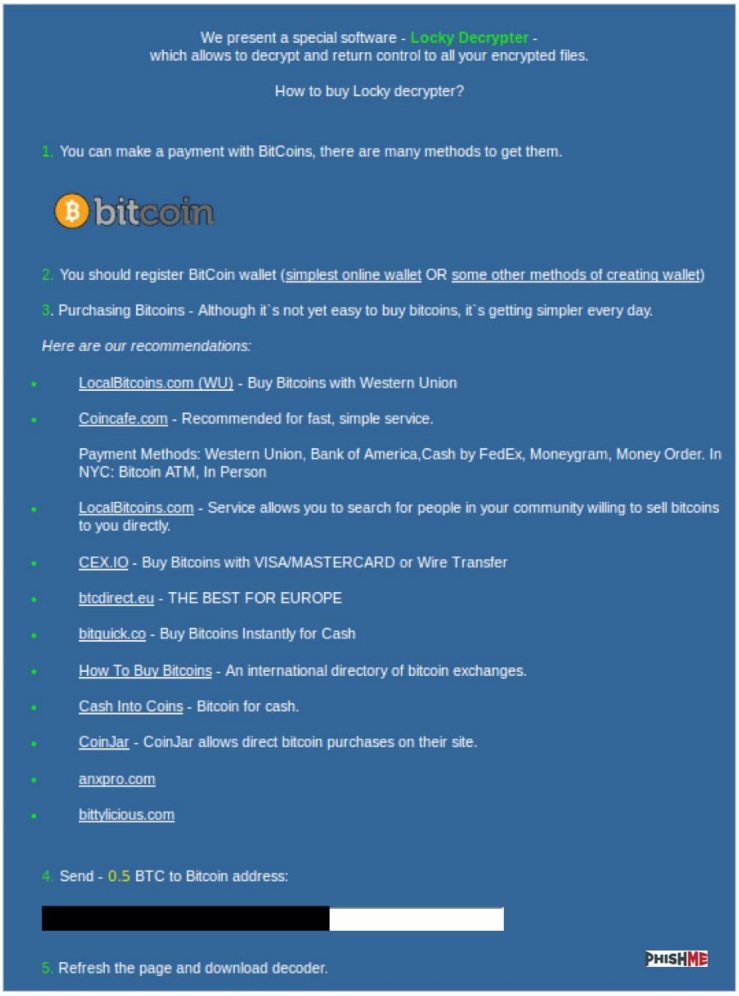
(https://www.bleepingcomputer.com/news/security/the-locky-ransomware-encrypts-local-files-and-unmapped-network-shares/)

(https://www.bleepstatic.com/images/news/ransomware/locky/word-document.png)

Une fois les macros activées, le ransomware commence à chiffrer tous les fichiers. Locky supprime également les sauvegardes que Windows a faites. Du coup cela rend impossible la restauration de l'ordinateur à une date antérieure.

Une fois cette opération terminée, l'écran de Windows est remplacé par la demande de rançon qui nous dit à la victime d'aller sur un lien. Ce lien va lui expliquer comment acheter des bitcoins et lui donner l'adresse à laquelle il devra verser la somme. Après avoir réglé la somme il pourra normalement télécharger le déchiffreur nommé Locky Decrypter et récupérer le contrôle de notre ordinateur ainsi que ses données.

Figure 12: Exemple de lien pour Locky Decrypter



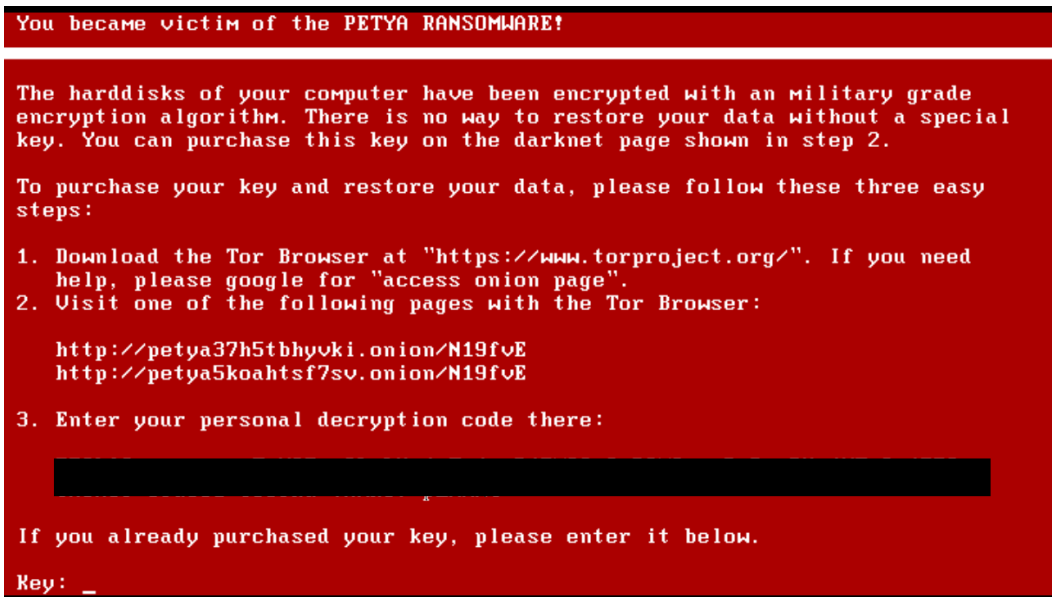
(https://korben.info/wp-content/uploads/2016/03/figure-6-4.png)

3.4 PETYA

Le ransomware PETYA a été découvert en 2016. Il s'attaque immédiatement à auxc disques durs. Il remplace la zone d'amorçage par un programme qui va chiffrer l'intégralité des disques durs puis va réclamer une somme en bitcoins.

La différence entre peyta et les autres ransomwares c'est que PEYTA bloque l'accès à tout le disque dur directement. En 2017, des entreprises de grande envergure telles que BNP Paribas ou la SNCF ont été touchée par PETYA-

Figure 13 : Ecran affiché après une attaque de Petya



(http://www.futura-sciences.com/tech/definitions/securite-petya-16559/)

3.5 ZCRYPTOR

ZCRYPTOR est un ransomware classique il fonctionne comme les autres. Il a cependant une particularité à ne pas négliger. Ce ransomware se propage aussi via les clés USB et les disques durs. Une fois qu'il a infecté un ordinateur via les moyens traditionnels (ingénierie sociale, email, spam,…), Il détecte s'il y a des supports informatiques (clés USB, disques durs) qui sont connectés à l'ordinateur. S'il en trouve il va copier les fichiers et les rendre invisibles à l'utilisateur.

Ensuite, dès que le support est connecté sur un nouvel ordinateur. Le ransomware va l'infecter.

Figure 14 : La page qui s'affiche lorsqu'on se fait attaquer par zCryptor

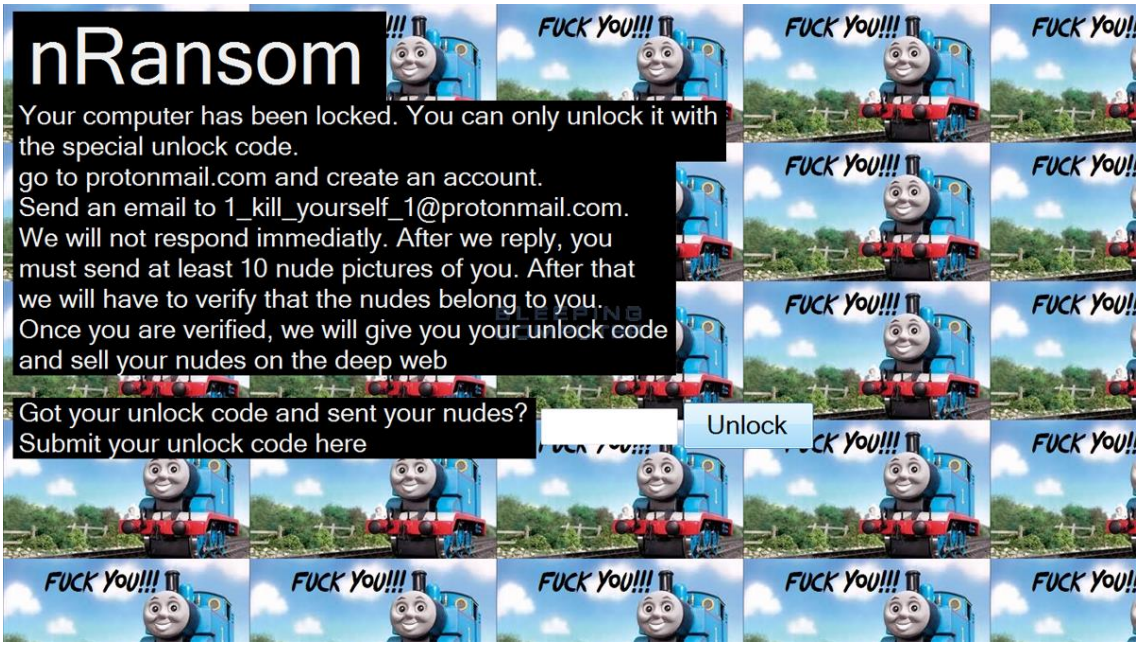
http://www.zdnet.fr/actualites/zcryptor-un-ransomware-aux-allures-de-ver-39837604.htm

3.6 nRansom

Voici un ransomware très particulier. Quand les autres ransomwares demandent des sommes d'argent celui la demande des photos de la victime dans la tenue d'Adam. Après quelques analyses du code il s'avère que nRansom n'est pas vraiment un ransomware.

Il s'agit d'un bloqueur qui verrouille seulement l'écran. Il ne chiffre pas les données. nRansom est avant tout une blague il suffit d'aller dans le processus et de tuer pour ne plus en entendre parler.

Figure 15 : Ecran afficher par nRansom



https://www.bleepingcomputer.com/news/security/nransom-joke-locker-demands-nude-pics-as-payment-/

3.7 RAA (JS/RANSOM-DLL)

RAA (JS/RANSOM-DLL) est un ransomware pas comme les autres. En effet, RAA est écrit entièrement en JavaScript (un langage de programmation). L'un des avantages d'utiliser JavaScript est que Windows n'affiche pas ces extensions par défaut. Une pièce jointe qui devrait s'afficher « facture.js » s'affichera « facture ». Donc les victimes ne se préoccupent pas de l'extension vu qu'elle n'est pas visible.

RAA (JS/RANSOM-DLL) n'a pas besoin de télécharger de ransomware sur le serveur. Dès que le ransomware a infecté la victime il est prêt à chiffrer les données et demander une rançon.

Premièrement, RAA (JS/RANSOM-DLL) lance un fichier leurre qui contient un message qui sert surtout à détourner attention. Pendant ce temps, le ransomware fait un appel au serveur pour demander une clé de chiffrement. Le serveur fournit une clé de chiffrement aléatoire AES ainsi qu'un identifiant (clé publique). Dès que les données sont chiffrées la victime devra mentionner l'identifiant pour payer la rançon ainsi il pourra récupérer la clé AES correspondante pour le déchiffrage.

La clé de chiffrement AES n'est pas gardée en mémoire par RAA (JS/RANSOM-DLL), dès que le chiffrement est fini, elle est supprimée, ainsi il n'y a plus que le serveur qui a une copie de la clé pour le déchiffrage. Une fois le chiffrement terminé, il y aura comme pour les autres ransomware une marche à suivre qui va nous expliquer comment récupérer les données.

RAA (JS/RANSOM-DLL) installe aussi un voleur de mots de passe. Le nom de code de ce virus est Troj/Fareit-AWR. Il est stocké dans le répertoire Mes Documents avec le nom suivant : st.exe

3.8 TORRENTLOCKER / Cryptowall / Critroni / TorLocker/…

Tous ces ransomwares fonctionnent quasiment de la même manière. Ils cryptent les données de la victime avec des algorithmes de chiffrement et demandent un paiement en crypto-monnaie. Tout cela pour dire qu'il y a plein de ransomware et que ce genre de virus ne fait que de s'améliorer et de se multiplier.

4. Economie

4.1 Le paiement des rançons

Comment peut-on demander une rançon sur internet sans être retrouvé ? Ou encore pourquoi ne trace-t-on pas les virements d'argent pour retrouver le hackeur ?

Les ransomware actuel utilisent la crypto-monnaie plus précisément le Bitcoin pour payer les rançons. Mais avant d'utiliser la crypto-monnaie les ransomware demandaient de régler la rançon avec d'autres méthodes de paiement.

Au début les victimes de ransomware pouvait payer les rançons en envoyant un SMS via un code comme par exemple ceux qu'on peut utiliser pour payer un ticket de bus TPG. Les victimes pouvaient également verser la somme de la rançon vers un porte-monnaie électronique comme par exemple paypal.

Les autorités policières et les experts en sécurité ont trouvé une solution lors du changement des dispositions réglementaires des paiements électronique (On vérifie beaucoup plus d'éléments). Utiliser les porte-monnaie électroniques est devenu moins rentable et beaucoup plus risqué pour les ransomwares qui ont vu leur nombre baisser à ce moment.

Il y a quelques années, la crypto-monnaie a commencé à se populariser chez les particuliers mais aussi chez les cybercriminels. Une des crypto-monnaies les plus populaires est le bitcoin.

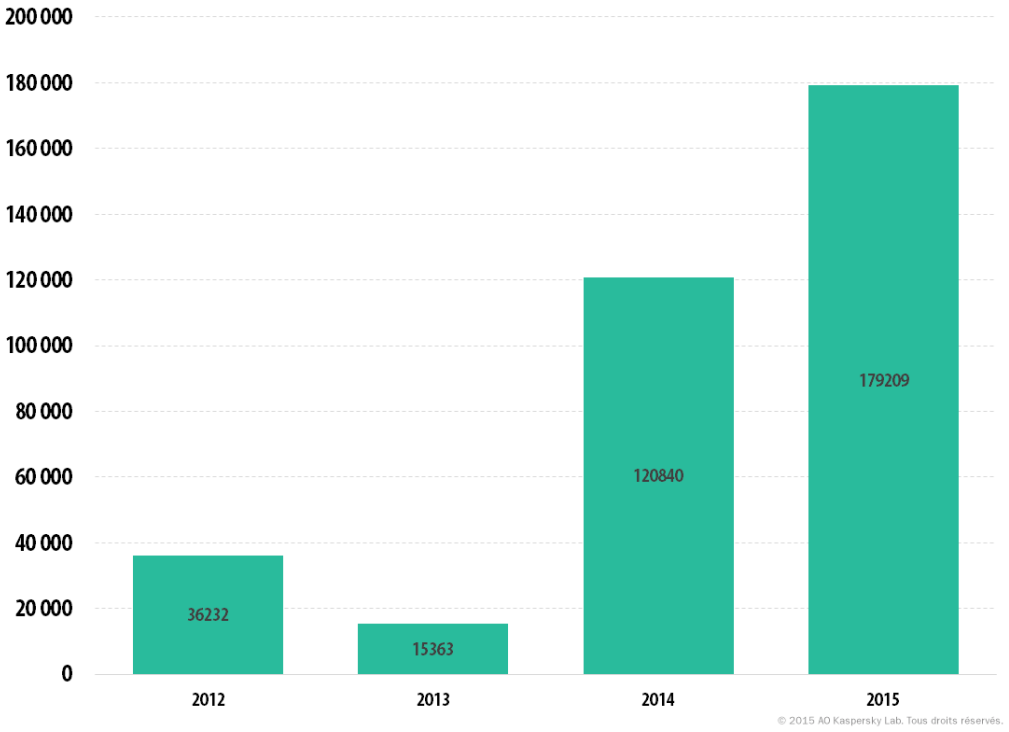
Il s'agit d'une monnaie électronique (il n'existe pas de billets ou de pièces) inventé par Satoshi Nakamoto en 2008. Elle a la particularité de ne dépendre d'aucune banque centrale ou d'autorité centrale. Le bitcoin est donc décentralisé. Sa valeur est évaluée par l'offre et la demande des sites internet qui servent de lieux d'échanges au bitcoin. Ce qui veut dire que chaque transfère se fait directement entre utilisateurs sans passer par une autorité tierce. Le prix du bitcoin est très volatile par exemple si on doit payer 1 bitcoin (1 btc = 4900 euros), demain un bitcoin pourrait valoir 5500 ou 4500 euros. Tout dépend de l'offre et la demande.

Les transactions de bitcoin utilisent le chiffrement asymétrique. Il y a une clé privée et une clé publique. La clé privée sert de mot de passe et permet de signer les messages de transaction. La clé publique est le numéro de compte de l'utilisateur c'est-à-dire le portefeuille.

Ensuite, une adresse est créée à partir de la clé publique qui elle-même est créée à partir de la clé privée. Cette adresse permet de recevoir des paiements. Les utilisateurs peuvent utiliser une nouvelle adresse pour chaque nouveau paiement. Cela permet de séparer les transactions de telle sorte qu'ils ne soient pas possibles de les associer. Donc si une personne vous envoie des bitcoins, elle ne peut pas voir vos autres adresses. Les adresses ne peuvent pas être associées.

Pour toutes ces raisons le bitcoin est devenu omniprésent dans le monde des cybercriminels.

Figure 16 Nombre d'utilisateurs attaqué par un ransomware



(https://securelist.fr/bulletin-de-kaspersky-sur-la-securite-en-2015-principales-statistiques-pour-2015/63269/)

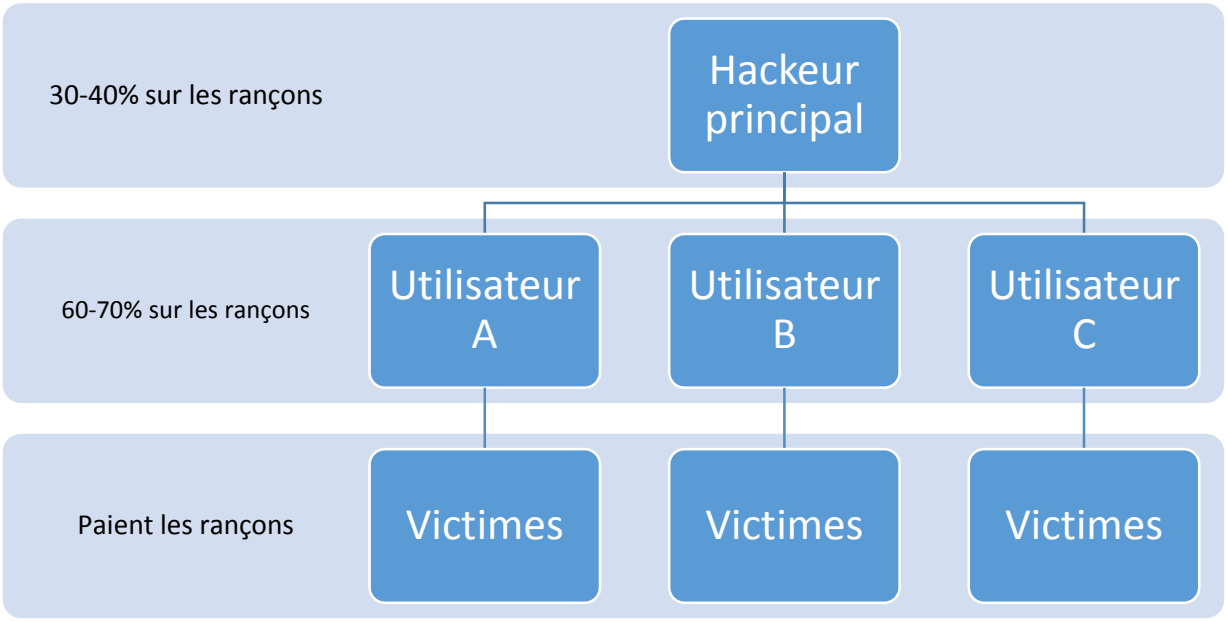
On peut constater que le nombre d'attaques a baissé en 2013 grâce aux dispositions pris par les autorités. Mais qu'avec la croissance du bitcoin le nombre d'attaques a explosé.

4.2 Les ransomware comme un service (RaaS)

Le concept est relativement simple : un hackeur principal met à disposition une plate-forme pour pouvoir créer un ransomware personnalisé. Là où cela fait peur c'est que n'importe qui peut utiliser cette plate-forme, peu importe le niveau technique. Il suffit à la personne de payer (des fois gratuit) le service et elle pourra paramétrer son ransomware à sa guise et le télécharger. Les paramètres que la personne peut modifier son : le montant de la rançon(en fonction du pays), les fichiers cibles à chiffrer, le type de chiffrage, etc.

L'hackeur qui a mis à disposition la plate-forme prend un pourcentage sur les rançons récupérées par chaque personne qui utilise son service. Ce modèle est de plus en plus amélioré, certaines plates-formes mettent à disposition des outils pour suivre leurs attaques ou encore de aider à la diffusion du ransomware.

Figure 17 Schéma de fonctionnement des RaaS



(https://kivulabs.com/ransomware-as-a-service-raas/)

5. Réponse légale

Maintenant qu'on sait comment un ransomware arrive dans système et comment il fonctionne, il est temps de voir comment se protéger contre les attaques et quelles mesures prendre après une infection.

5.1 Comment se protéger ?

5.1.1 Sensibilisation

L'attaque chez un particulier ou dans un établissement d'un ransomware commence souvent par une erreur de la personne qui se trouve entre la chaise et l'ordinateur. Il faut donc sensibiliser les personnes aux risques associés aux attaques d'ingénierie sociale. Il faut éviter les sites douteux, ne pas ouvrir les emails malveillants, ne pas activer les macros et ne pas cliquer sur des liens suspects. Ce sont des règles qui paraissent basiques mais on s'aperçoit qu'elles ne sont pas évidentes pour tout le monde. Il faut apprendre aux personnes à se comporter prudemment sur internet.

En ce qui concerne les entreprises, elles commencent enfin à prendre conscience de l'importance et de l'impact que peut avoir une attaque d'ingénierie sociale. C'est pour cela que les entreprises commencent à mettre en place des audits et des tests d'intrusion dans lesquelles il faudra tester les collaborateurs dans des situations à risques. Comme par exemple la réaction face à des emails ou à la demande d'informations confidentielles par téléphone. Ces tests servent à former les collaborateurs afin qu'ils puissent reconnaitre le risque et à être prêt pour le jour où une vraie attaque aura lieu.

5.1.2 Sauvegarde

Un des moyens les plus simples pour contrer les ransomware est de faire des sauvegardes régulières des données dans un support externe tel qu'un disque dur externe ou dans le cloud. Cette méthode va limiter l'impact qu'aura le ransomware vu qu'il suffira d'isoler et de nettoyer l'ordinateur infecté. Ensuite, il restera plus qu'à restaurer les fichiers à partir de la sauvegarde. On n'aura pas besoin de payer la rançon car on a déjà une copie des données.

5.1.3 Installer une solution anti-Ransomware

Il existe des outils anti-ransomware qui permettent d'éviter d'être infecté par certains ransomwares. Ce genre de logiciel comporte généralement deux fonctionnalités : une qui vérifie la réputation des fichiers et des sites internet. S'il s'avère que les sites ou fichiers sont déjà répertorier comme malveillant le logiciel prévient l'utilisateur. L'autre fonction est un système « watcher » qui surveille le comportement des logiciels inconnus et une fois une action inconnue détectée il la notifie à l'utilisateur. Certains outils vont plus loin en réalisant des sauvegardes de fichiers ouverts par des logiciels inconnus. Ainsi, même si nos fichiers sont chiffrés l'anti-ransomware aura fait des copies.

Voici des exemples d'anti-ransomware :

- Anti-Ransomware Tool Bitdefender
- Anti-Ransomware Tool for business de Kaspersky Lab
- CrypthoPrevent
- HitmanPro.Alert
- Malwarebytes anti-Ransomare
- Trend Micro Anti-Ransomware
- WinPatrol

Malheureusement, ces solutions ne fonctionnent pas contre tous les ransomwares. En effet, il y a une vaste panoplie de version de ransomware et beaucoup ne sont pas détectés par les anti-Ransomware.

5.1.4 Mettre à jour

Il faut toujours maintenir son système d'exploitation, son antivirus et toutes les applications installées à jour. Les hackeurs utilisent des failles pour installer automatiquement le ransomware.

Faire les mises à jour régulièrement permet de réduire un maximum le risque qu'un hackeur puisse utiliser une faille qui est généralement corrigée rapidement une fois découverte.

5.1.5 Précautions à mettre en place

Il y a quelques précautions qu'il faut mettre en place pour repérer certains sites ou fichiers malveillants.

5.1.5.1 Afficher l'extension des noms de fichiers

Windows n'affiche pas les extensions par défaut. Les attaquants peuvent utiliser les extensions pour cacher un fichier malveillant. Par exemple un fichier nommé facture.js va s'afficher facture.

Le ransomware RAA (JS/RANSOM-DLL) utilise cette méthode.

5.1.5.2 Paramétrer/Personnaliser son navigateur internet

Une des premières choses à faire est d'installer et d'activer un bloqueur de publicité lorsqu'on visite des sites internet inconnus. Cela permet d'éviter les publicités malveillantes. Quand on visite un site régulièrement et qu'il est fiable, il est conseillé de désactiver le bloquer étant donné que les publicités permettent au site de se rémunérer.

Exemples de bloqueur de pub :

- AddBlock
- AdThwart
- uBlock

Dans le même registre que le premier conseil, il y a des extensions qui permettent de bloquer JavaScript. JavaScript est un langage de programmation qui s'interprète par le navigateur. Les attaquants peuvent utiliser ce langage pour réaliser des attaques. Comme pour le bloqueur de pub il est conseillé de laissé actif JavaScript que sur des sites internet fiables.

Exemples de bloqueur de javascript :

- NoScript.
- Quick JavaScript Switcher

Pour éviter les sites malveillants, il y a des extensions qui ont été réalisé pour déterminer si le site visité est sécurisé et fiable.

Exemple d'extension

- Web of trust
- HTTPS EveryWhere

5.1.6 Installation d'application

Voilà un conseil qui est valable autant sur un ordinateur que sur un mobile. Il faut toujours passer par le site officiel ou les magasins officiels lorsqu'on veut installer une application. Si on installe une application par une source inconnue c'est la porte ouverte à tous les malwares.

5.1.7 D'autres conseils pour les entreprise

Tous les conseils cités plus hauts sont applicables pour les entreprises mais il y a d'autres précautions pour se protéger :

- Il faut que les collaborateurs aient les droits les plus faibles possibles.
- Mettre en place un proxy pour contrôler l'accès internet de l'entreprise.
- Bloquer les programmes de téléchargement peer to peer.
- Former les collaborateurs pour être préparer en cas d'attaques informatique
- Contrôler les supports externes que les collaborateurs utilisent sur les machines de l'entreprise.
- Segmenter le réseau de sorte que différentes zones du réseau soient isolées des autres afin éviter que l'infection se propage.
- Sensibiliser les collaborateurs sur les nouvelles menaces.

5.2 En cas d'infection que faire ?

5.2.1 Marche à suivre

La première chose à faire est de déconnecter la machine infectée de tous les réseaux. Cela permet d'éviter que le ransomware se propage sur d'autres ordinateurs ou serveurs.

Une fois la machine infectée isolée, le plus simple reste de restaurer le système à une date antérieure à celle de l'infection et ensuite lancer une analyse complète du système pour vérifier qu'il n'y a plus de problème.

Malheureusement, certains ransomwares suppriment les sauvegardes qui permettent la restauration du système. Dans ce cas, il faut d'abord supprimer le ransomware de la machine. Normalement en exécutant une analyse avec un antivirus performant on devrait s'en débarrasser.

Mais le gros problème est que nos fichiers restent toujours chiffrés même en ayant supprimé le ransomware. Il faut la clé de déchiffrement pour récupérer nos fichiers.

Plusieurs entreprises de sécurité ont développé des outils de déchiffrement qui permettent justement de récupérer les fichiers chiffrés.

- Free Ransomware Decryptors par Kaspersky (lien)
- Free Ransomware Decryption par Avast (lien)

Malheureusement les ransomwares évoluent rapidement et il est fort possible que les clés de déchiffrement que vous trouvez sur ce genre d'outil ne fonctionnent pas.

5.2.2 Le projet No More Ransom

Une initiative de National High Tech Crime Unit, European CyberCrime, KasperskyLab et McAfee a vu le jour dont le but est simplement d'informer le public sur le danger des ransomware et d'aider les victimes à récupérer leurs données. Cette initiative a aidé environ 4500 personnes.

Le projet continu de croitre, il suffit de regarder le nombre de partenaires qui ne fait qu'augmenter. Bien sûr cette croissance permet d'augmenter le nombre de nouveaux outils que met à disposition No More Ransom pour aider les victimes des ransomware.

No More Ransom propose des outils de déchiffrement personnaliser pour chaque ransomware.

Cette initiative n'aucun but commercial, elle veut simplement inverser la tendance et faire cesser cette pratique.

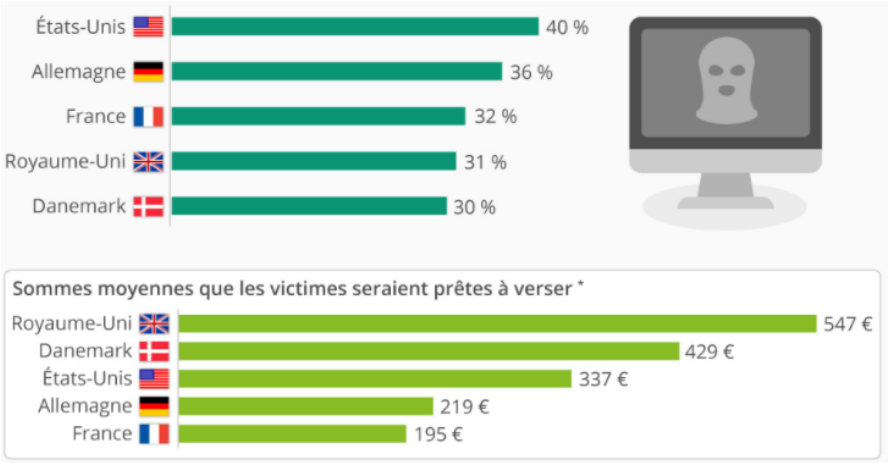
5.2.3 Faut-il payer la rançon ?

Le fait de payer la rançon ne garantit pas la réception de la clé qui permet de déchiffrer nos données.

Si on paie on devient une cible encore plus intéressante pour les attaquants qui pourront se dire que c'est une cible facile. À cela s'ajoute le fait que payer la rançon finance directement les ransomwares qui vont continuer à se développer.

Mais si on a déjà tout tenté pour récupérer nos données (différents outils de déchiffrements) et que les données qui sont chiffrées sont très importantes (moralement ou financièrement). Il est toujours possible payer la rançon pour espérer retrouver les données.

Figure 18 : Sondage sur les utilisateurs prêts à payer une rançon



(https://fr.statista.com/infographie/7303/les-internautes-face-a-la-menace-des-logiciels-de-rancon/)

Comme on peut le constater près d'un tiers des pays sondés, sont prêts à verser la rançon pour récupérer leurs données. Les utilisateurs du Royaume-Uni sont prêts à débourser environ 547 euros en moyenne. Si 20 personnes décident de payer une rançon cela fait une somme de 10 940 euro.

5.2.4 Porter plainte

Malgré le nombre grandissant d'attaques de ransomwares, les victimes signalent rarement les attaques aux autorités. Selon un rapport de Datto (entreprise de sécurité) moins d'une attaque sur quatre sont signalées aux autorités.

Une statistique qui s'explique par le fait que dénoncer une telle attaque aux autorités est un coup dur pour l'image d'une société. Mais, il ne faut pas oublier que l'attaque par ransomware est un crime.

En Suisse il est conseillé de signaler l'incident au Service national de coordination de la lutte contre la criminalité sur internet(SCOCI) et de le signaler auprès de la police.

5.3 Anecdote

Des chercheurs ont développé un ransomware « pédagogique » dans le but de donner un moyen de simuler une attaque de ransomware et de tester les méthodes de protection à des entreprises et particuliers.

Ils ont publié le code source sur GitHub. Malheureusement, de nombreux hackeurs ont utilisé et modifié le code source pour créer leurs propres ransomware.

6. Conclusion

6.1 Synthèse de la recherche sur les ransomwares

Dans ce travail de Bachelor, nous avons revu l'histoire et l'évolution des ransomwares. Tout a commencé avec le virus nommé PC Cyborg, qui est donc le premier ransomware à avoir été documenté. Il était distribué sur des disquettes et déjà à l'époque l'attaquant utilisait la sensibilité et la naïveté des personnes pour le diffuser.

Les attaques de ransomwares ont commencé à évoluer dans tous les compartiments, le code des ransomware est devenus plus élaboré et les manières les diffuser sont devenu plus méthodique. Tout cela dans le but de gagner de l'argent.

Les ransomwares sont passés à des méthodes où ils chiffrent les données de la victime avec des bibliothèques de cryptage. À cela s'ajouter la popularisation de la crypto-monnaie et la professionnalisation des procédures de paiements de rançon. Le nombre de ransomware a tout simplement explosé.

On a pu voir que les attaques de ransomware peuvent toucher n'importe quel pays et que personne n'est vraiment à l'abri. Les entreprises, les institutions et les particuliers sont tous des cibles potentielles.

On a analysé les vecteurs d'attaques et on a pu constater que les méthodes les plus utilisées sont les emails et l'ingénierie sociale. Les victimes ne sont pas assez formées pour décerner les emails malveillants ou les attaques d'ingénierie sociale.

Malheureusement ce ne sont pas les seules méthodes pour diffuser les ransomwares. Cette menace peut se propager via des sites malveillants ou simplement par des clés USB infectées. Mais il est aussi arrivé qu'un ransomware se propage à cause d'une faille de sécurité (wannaCry).

Ensuite on a vu les différents types de ransomwares et leurs fonctionnements. Les ransomware utilisent différentes manières pour échapper à la détection de l'antivirus comme par exemple « l'obfuscation » ou le « dropper ».

Les différents types de ransomware qu'on a vu sont les chiffreurs, les bloqueurs, les mobiles ou encore ceux qui bloquent le démarrage du système.

Celui qui est le plus en vogue c'est le ransomware chiffrant. En effet, ce type de ransomware est le plus compliqué à nettoyer même après l'avoir supprimé de l'ordinateur, les données restent chiffrées.

Pour récupérer les données il faut soit chercher des outils de déchiffrement ou soit payer la rançon et espérer que les hackeurs donnent la clé pour déchiffrer les données.

On a pu constater que les ransomwares sont très diversifiés. Il y a une grosse panoplie de ransomwares, ce qui les rend très difficiles contrer étant donné qu'il faut trouver un déchiffreur pour chacun d'entre eux. Cela encourage les victimes à finalement payer les rançons.

Les paiements des rançons se font généralement via les bitcoins qui permettent au hackeur d'être quasiment intraçables. Cela en fait la monnaie courante pour payer les rançons.

Les hackeurs ont poussé le vice plus loin en produisant des ransomwares comme des services. Avec cette méthode tout le monde pourrait acheter un ransomware et l'utiliser sans pour autant avoir de compétences techniques.

Pour se défendre contre les ransomwares, on a vu que cela passait d'abord par une sensibilisation des personnes. Les victimes doivent en savoir plus sur les ransomwares. Il faut mettre en place des précautions pour se préparer et minimiser l'impact des attaques de ransomwares.

La meilleure chose à faire, selon plusieurs rapports de sécurité, c'est de faire des sauvegardes régulières des données pour rendre le chiffrement des données inutiles puisqu'il existe une copie des données.

Si malheureusement il n'y a pas de copie des données, il est tout de suite plus compliqué de les retrouver. Pour commencer on peut essayer de chercher les outils de déchiffrement que proposent les entreprises de sécurité.

Si les outils de déchiffrement ne fonctionnent pas, on peut payer la rançon et espérer recevoir la clé de déchiffrement. Toutefois il ne faut pas oublier de signaler aux autorités l'attaque.

S'il faut retenir une chose dans cette recherche c'est : sensibiliser les gens :

- Informer et éduquer sur l'ingénierie sociale
- Expliquer comment naviguer prudemment sur internet
- Faire attention aux informations qu'
- Apprendre à reconnaître un risque
- S'informer sur les nouvelles menaces

6.2 Point de vue personnel

J'ai choisi ce travail de recherche pour différentes raisons. Tout d'abord il s'agit d'un sujet d'actualité, tous les médias parle de ransomware. Mais la vrai raison est qu'un membre de ma famille a été victime d'une attaque d'un ransomware et il m'avait sollicité pour de l'aide, avec la fameuse répliques « tu fais des études en informatiques tu peux m'aider à dépanner mon ordinateur ». Il était infecté par un ransomware qui chiffrait les données et il avait environ 1000 photos de famille, amis, etc. Donc il voulait récupérer ces photos.

Heureusement, le ransomware n'avait pas supprimé les sauvegardes de restauration Windows. Du coup, il m'a suffi de restaurer l'ordinateur à l'état dans lequel il se trouvait avant le ransomware et de procéder ensuite à une analyse avec un antivirus pour vérifier que tout allait bien.

Quand j'ai demandé comment il avait été infecté par ce ransomware, il m'a simplement dit qu'il avait ouvert une pièce jointe et que l'antivirus ne l'avait pas prévenu du danger du fichier.

Cet évènement ma fait prendre conscience que les ransomwares sont un danger à ne pas négliger que soit pour un particulier ou une entreprise et qu'il fallait absolument que je me renseigne sur ce sujet. Ce travail de recherche était l'occasion pour moi d'en apprendre plus.

Avec à cette recherche sur les ransomwares, j'en suis venu à la conclusion que pour les éliminer. Il fallait absolument passer par une éducation, formation et sensibilisation des gens sur la sécurité informatique.

Bibliographie

ABRAMS, Lawrence, 2017. NRANSOM JOKE LOCKER DEMANDS NUDE PICS AS PAYMENT. *Bleeping computer* [en ligne].22 septembre 2017. [Consulté le 10.10.2017]. Disponible à l'adresse :

https://www.bleepingcomputer.com/news/security/nransom-joke-locker-demands-nude-pics-as-payment-/

ANTONIN, Nadia, 2017.LE BITCOIN : UNE MONNAIE VIRTUELLE AU SERVICE DE LA CYBERCRIMINALITE. *Andese* [en ligne].24 mai 2017. [Consulté le 5.09.2017]. Disponible à l'adresse :

http://www.andese.org/chronique-de-nadia-antonin/404-le-bitcoin-une-monnaie-virtuelle-au-service-de-la-cybercriminalite.html

ARSENE, Liviu, ALEXANDRA, Gheorge, 2016. RANSOMWARE A VICTIMS'S PERSPECTIVE. *BitDefender* [en ligne].Janvier 2016. [Consulté le 10.08.2017]. Disponible à l'adresse :

https://download.bitdefender.com/resources/files/News/CaseStudies/study/59/Bitdefender-Ransomware-A-Victim-Perspective.pdf

ASECURITYSITE. RANSOMWARE AND CODE OBFUSCATION . *Asecurity site* [en ligne]. [Consulté le 8.25.2017]. Disponible à l'adresse :

https://asecuritysite.com/subjects/chapter87

ASSISTE, 2017. DROPPER. *Assiste* [en ligne].18 juin 2013. 27 juillet 2017. [Consulté le 13.09.2017]. Disponible à l'adresse :

http://assiste.com/Dropper.html

ASSISTE, 2017. DRIVE-BY DOWNLOAD. *Assiste* [en ligne]. 02 juillet 2013. 27 juillet 2017. [Consulté le 30.09.2017]. Disponible à l'adresse :

http://assiste.com/Drive_by_download.html

AVAST BLOG, 2016. INSIDE PETYA AND MISCHA RANSOMWARE *Avast* [en ligne]. 20 septembre 2016. [Consulté le 5.10.2017]. Disponible à l'adresse :

https://blog.avast.com/inside-petya-and-mischa-ransomware

BARJON, Anthony, 2015. ANALYSE D'UN RANSOMWARE : CRYPTOLCOKER. *Lexsi* [en ligne].2 mars 2015. [Consulté le 25.09.2017]. Disponible à l'adresse :

https://www.lexsi.com/securityhub/analyse-dun-ransomware-cryptolocker/

Bitcoin [en ligne]. [Consulté le 31.08.2017]. Disponible à l'adresse :

https://bitcoin.org/fr/

BITCOIN680, 2014, Bitcoin en 15 minutes *Bitcoin680* [en ligne]. 23 mars 2014 [Consulté le 10.10.2017]. Disponible à l'adresse :

https://bitcoin680.wordpress.com/2014/03/23/une-transaction-expliquee/

BITDEFENDER, 2015. RANSOMWARES, MIEUX VAUT PERDRE SES DONNEES OU SONT ARGENT ? . *Bitdefender* [en ligne].26 mai 2015. [Consulté le 22.08.2017]. Disponible à l'adresse :

https://www.bitdefender.fr/blog/Ransomwares-mieux-vaut-perdre-ses-donnees-ou-son-argent-Partie-1-1585.html

BONVOISIN, Guillaume, 2017.RANSOMWARE : 8 MESURES POUR SE PROTÉGER ET RÉCUPÉRER SES FICHIERS. *cnet* [en ligne].30 Juin 2017. [Consulté le 28.09.2017]. Disponible à l'adresse :

http://www.cnetfrance.fr/produits/ransomware-8-mesures-pour-se-proteger-et-recuperer-ses-fichiers-39836850.htm

CANNELL, Joshua, 2013. OBFUSCATION : MALWARE'S BEST FRIEND. *Malqarebytes labs* [en ligne]. 31 mars 2016. [Consulté le 12.09.2017]. Disponible à l'adresse :

https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Code-obfuscation.pdf

CERT-FR, 2017. PROTECTION CONTRE LES RANÇONGICIELS. *CERT-FR* [en ligne].27 juin 2017. [Consulté le 11.09.2017]. Disponible à l'adresse :

https://www.cert.ssi.gouv.fr/information/CERTFR-2017-INF-001/

CERT-UK, 2014. CODE OBFUSCATION. *Cert.UK* [en ligne]. 2014. [Consulté le 11.09.2017]. Disponible à l'adresse :

https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Code-obfuscation.pdf

CISCOFRANCE, 2016, Les ransomware vus par les hackers [enregistrement vidéo], *Youtube* [en ligne].7 décembre 2016. [Consulté le 10.10.2017]. Disponible à l'adresse :

https://www.youtube.com/watch?v=ZLAT2pggbNQ

CUCU, Paul, 2017. HOW 4 TYPE OF CYBER THREATS BREAKS YOUR ONLINE SECURITY. *Heimdal security* [en ligne]. 10 mai 2017. [Consulté le 27.09.2017]. Disponible à l'adresse :

https://heimdalsecurity.com/blog/what-is-ransomware-protection/

DAGOUAT, Charles, 2017. SYNTHESE DES ELEMENTS DISPONIBLES CONCERNANT #WANNACRY. *Xmco* [en ligne].17 mai 2017. [Consulté le 15.09.2017]. Disponible à l'adresse :

http://blog.xmco.fr/synthese-des-elements-disponibles-concernant-wannacry/

DATTO, 2016. DATTO'S STATE STATE OF CHANNEL RANSOMWARE REPORT 2016. *Datto* [en ligne].2016. [Consulté le 22.08.2017]. Disponible à l'adresse:

http://cdn2.hubspot.net/hubfs/241394/DattoStateOfTheChannelRansomwareReport2016.pdf

DESAI, Deepen, 2017. WANNACRY 2.0 RANSOMWARE ATTACKS CONTINUE… . *Zscaler* [en ligne].15 mai 2017. [Consulté le 22.08.2017]. Disponible à l'adresse :

https://www.zscaler.com/blogs/research/wannacry-20-ransomware-attacks-continue

DROZHZHIN, Alex, 2016. L'HISTOIRE DU RANSOMWARE ET SON EVOLUTION EN FAITS ET CHIFFRES. *Kaspersky secure list* [en ligne]. 24 juin 2016. [Consulté le 6.09.2017]. Disponible à l'adresse :

https://www.kaspersky.fr/blog/ransomware-blocker-to-cryptor/5777/

DUCKLIN, Paul, 2016. RANSOMWARE THAT'S 100% PURE JAVASCRIPT, NO DOWNLOAD REQUIRED . *Naked security sophos* [en ligne].20 juin 2016. [Consulté le 5.09.2017]. Disponible à l'adresse :

https://nakedsecurity.sophos.com/2016/06/20/ransomware-thats-100-pure-javascript-no-download-required/

FONTAINE, Pierre, LE BOURLOUT,Eric, 2014. LE POINT SUR BITCOIN EN DIX QUESTIONS ET REPONSES… . *01NET* [en ligne].21 MARS 2014. [Consulté le 10.09.2017]. Disponible à l'adresse :

http://www.01net.com/actualites/le-point-sur-bitcoin-en-dix-questions-et-reponses-615790.html

FRANCIS, Ryan, 2016. THE HISTORY OF RANSOMWARE. *CSO* [en ligne].20 juillet 2016. [Consulté le 31.08.2017]. Disponible à l'adresse :

https://www.csoonline.com/article/3095956/data-breach/the-history-of-ransomware.html#slide1

GARNEAVA, Maria, MAKRUSHIN, Denis, 2015. BULLETIN DE KASPERSKY SUR LA SECURITE EN 2015. PRINCIPALES STATISTIQUES POUR 2015. *Kaspersky secure list* [en ligne]. 15 décembre 2015. [Consulté le 20.09.2017]. Disponible à l'adresse :

https://securelist.fr/bulletin-de-kaspersky-sur-la-securite-en-2015-principales-statistiques-pour-2015/63269/

GOUSSARD, Lionel, 2017. MENACES INTERNES ET CYBERSECURITE : BIEN PLUS QUE DE SIMPLES ERREURS HUMAINES. *JDN* [en ligne]. 24 mars 2017. [Consulté le 20.09.2017]. Disponible à l'adresse :

http://www.journaldunet.com/solutions/expert/66623/menaces-internes-et-cybersecurite---bien-plus-que-de-simples-erreurs-humaines.shtml

K, Michel, 2016. LES RANSOMWARES, EXPLICATIONS ET CONTRE-MESURES. *Le blog du hacker* [en ligne]. 23 novembre 2016. [Consulté le 5.09.2017]. Disponible à l'adresse :

https://www.leblogduhacker.fr/ransomwares-explications-contre-mesure/

KORBEN,2016. LOCKY – TOUT CE QU'IL Y A A SAVOIR SUR LE MALWARE DU MOMENT. *Korben* [en ligne]. 8 mars 2016. [Consulté le 07.09.2017]. Disponible à l'adresse :

https://korben.info/locky-quil-y-a-a-savoir-malware-moment.html

LARGENT, William, 2016. RANSOMWARE: PAST,PRESENT, AND FUTUR. *Talos* [en ligne].11 Avril 2016. [Consulté le 25.08.2017]. Disponible à l'adresse :

http://blog.talosintelligence.com/2016/04/ransomware.html#ch1

LELLOUCHE, Nicolas, 2017.LES DEMANDES DE RANCONS INFORMATIQUES EN TRÈS NETTE HAUSSE EN 2017. *Le figaro*[en ligne].05 septembre 2017.11 septembre 2017. [Consulté le 1.10.2017]. Disponible à l'adresse :

http://www.lefigaro.fr/secteur/high-tech/2017/09/05/32001-20170905ARTFIG00087-les-demandes-de-rancons-informatiques-en-tres-nette-hausse-en-2017.php

LE GROS, Clara, 2017. TOP 3 DES PRINCIPAUX VECTEURS D'ATTAQUE INFORMATIQUE EN ENTREPRISE. *Astrakhan innovation management* [en ligne].16 mai 2017. [Consulté le 5.09.2017]. Disponible à l'adresse :

http://lelab.astrakhan.fr/vecteurs-attaque-informatique/

LEVEILLE, Marc-Etienne, 2014. TORRENT LOCKER RANSOMWARE IN A CUNTRY NEAR YOU. *Enjoy Safer Technology* [en ligne]. décembre 2014. [Consulté le 29.09.2017]. Disponible à l'adresse :

https://www.welivesecurity.com/wp-content/uploads/2014/12/torrent_locker.pdf

MALEKAL_MORTE, 2014. Crypto-ransomware / rançongiciels chiffreurs de fichiers. *Malekal's forum* [en ligne]. 18 novembre 2014. [Consulté le 22.08.2017]. Disponible à l'adresse :

https://forum.malekal.com/viewtopic.php?t=49834&start=

MELANI, 2017. RANCONGICIEL. *Melani* [en ligne].5 juillet 2017. [Consulté le 13.09.2017]. Disponible à l'adresse :

https://www.melani.admin.ch/melani/fr/home/themen/Ransomware.html

MSFT-MMPC, 2017. RANSOMWARE : A DECLINING NUISANCE OR AN EVOLVING MENACE ?. *Msft-MMPC*[en ligne].14 février 2017. [Consulté le 13.09.2017]. Disponible à l'adresse :

https://blogs.technet.microsoft.com/mmpc/2017/02/14/ransomware-2016-threat-landscape-review/

NO MORE RANSOM [en ligne]. [Consulté le 20.08.2017]. Disponible à l'adresse :

https://www.nomoreransom.org/fr/index.html

PATTERSON, Richard, 2017. CYBER SECURITY AND INTERNET FREEDOM STATISTICS BY COUNTRY. WHICH ARE MOST AND LEAST SAFE ?. *Comparitech* [en ligne]. 13 février 2017. [Consulté le 10.09.2017]. Disponible à l'adresse :

https://www.comparitech.com/blog/information-security/cyber-security-statistics/

ROUSSEAU, Amanda, 2016.YOUR PACKAGE HAS BEEN SUCCESFULLY ENCRYPTED :TESLACRYPT 4.1 AND THE MALWARE ATTACK CHAINE. *Endgame* [en ligne].19 Avril 2016. [Consulté le 28.08.2017]. Disponible à l'adresse :

https://www.endgame.com/blog/technical-blog/your-package-has-been-successfully-encrypted-teslacrypt-41a-and-malware-attack

RIPOLL, Mickael, 2017. RANSOMWARE-AS-A-SERVICE (RAAS). *Digitemis* [en ligne]. 25 avril 2017. [Consulté le 5.09.2017]. Disponible à l'adresse :

https://www.digitemis.com/2017/04/25/ransomware-as-a-service/

SAVAGE, Kevin, COOGAN, Peter, LAU, Hon, 2015. THE EVOLUTION OF RANSOMWARE. *Symantec* [en ligne].6 Août 2015. [Consulté le 20.08.2017]. Disponible à l'adresse :

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

SIMONE, Alina, 2015. THE STRANGE HISTORY OF RANSOMWARE. *Medium* [en ligne]. 26 mars 2015. [Consulté le 10.10.2017]. Disponible à l'adresse :

https://medium.com/un-hackable/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b

SINITSYN, Fedor, IVANOV, Anton, 2016. KASPERSKY SECURITY BULLETIN 2016. LA REVOLUTION DU RANSOMWARE. *Kaspersky secure list* [en ligne]. 8 décembre 2016. [Consulté le 22.08.2017]. Disponible à l'adresse :

https://securelist.fr/kaspersky-security-bulletin-2016-story-of-the-year/65780/

SOPHOS,2016. COMMENT BIEN SE PROTEGER CONTRE LES RANSOMWARES ? *Sophos* [en ligne]. mars 2016. [Consulté le 10.09.2017]. Disponible à l'adresse :

https://www.sophos.com/fr-fr/medialibrary/Gated%20Assets/white%20papers/fr/sophos-ransomware-protection-wpfr.pdf?la=fr-FR?cmp=701j0000001YAKMAA4

SOPHOS,2016. LES RANSOMWARES DANS VOS EMAILS ET L'AUGMENTATION DES JAVASCRIPT MALVEILLANTS ! . *Sophos* [en ligne]. 6 mai 2016. [Consulté le 22.08.2017]. Disponible à l'adresse :

https://news.sophos.com/fr-fr/2016/05/06/ransomwares-emails-augmentation-javascript-malveillants/

SNOW, Jon, 2016.TOUT CE QUE VOUS DEVEZ SAVOIR SUR LES RANSOMWARES. *Kaspersky Blog* [en ligne].7 Novembre 2016. [Consulté le 23.08.2017]. Disponible à l'adresse :

https://www.kaspersky.fr/blog/ransomware-faq/6276/

SNOW, Jon, 2016. PROJET NO MORE RANSOM : PLUS FORT QUE JAMAIS !. *Kaspersky Blog* [en ligne].15 décembre 2016. [Consulté le 22.08.2017]. Disponible à l'adresse :

https://www.kaspersky.fr/blog/nomoreransom-grows-even-bigger/6458/

UNUCHEK, Roman, SINITSYN, Fedor, 2017. DéVELOPPEMENT DES MENACES INFORMATIQUES AU 2E TRIMESTE 2017 STATISTIQUES. *Kaspersky secure list* [en ligne]. 15 AOUT 2017. [Consulté le 5.09.2017]. Disponible à l'adresse :

https://securelist.fr/it-threat-evolution-q2-2017-statistics/66408/

XMCO, 2013. LE BITCOI, UNE MONNAIE VIRTUELLE INTRACABLE. *Xmco* [en ligne].06 décembre 2013. [Consulté le 23.09.2017]. Disponible à l'adresse :

http://blog.xmco.fr/20131206le-bitcoin-une-monnaie-virtuelle-intracable/

ZAHARIA, Andra, 2017. WHAT IS RANSOMWARE AND 15 EASY STEPS TO KEEP YOUR SYSTEM PROTECTED. *Heimdal security* [en ligne].15 mai 2017. [Consulté le 23.09.2017]. Disponible à l'adresse :

https://heimdalsecurity.com/blog/what-is-ransomware-protection/

ZDNET, 2016. ZYCRPTOR : UN RANSOMWARE AUX ALLURES DE VER. *Zdnetr* [en ligne].31 mai 2016. [Consulté le 23.09.2017]. Disponible à l'adresse :

http://www.zdnet.fr/actualites/zcryptor-un-ransomware-aux-allures-de-ver-39837604.htm