|  |
| --- |
| CESI EXIA |
| Projet Cybersécurité |
| Projet d’étude de 4ème année |

|  |
| --- |
| Nicolas Carpentier – Nicolas Huet Emmanuel Real – Guillaume Real  12/04/2018 |

Table des matières

[1 Rappel du besoin 1](#_Toc510773697)

[2 Liste des tâches 1](#_Toc510773698)

[2.1 Décryptage des fichiers 1](#_Toc510773699)

[2.2 Livrables administratifs 1](#_Toc510773700)

[2.3 Livrables d’implémentations 2](#_Toc510773701)

[2.4 Questions 2](#_Toc510773702)

[3 Répartitions des tâches 2](#_Toc510773703)

# Rappel du besoin

L’entreprise Motuc a subi une cyber-attaque ce qui met en péril le fonctionnement de cette dernière. Tous les fichiers de l’entreprise ont été cryptés, rendant le SI HS, et le ransomware a envoyé un mail. Ce dernier contient des pistes sur la méthode à utiliser pour décrypter les fichiers.

Pour que Motuc puisse continuer son activité, cette dernière nous à solliciter afin de trouver le moyen de décrypter tous ces fichiers et de lui fournir un logiciel permettant de l’appliquer. De plus, elle nous a également demandé de lui proposer un PRA et un PCA pour qu’elle soit préparée à d’éventuelles futures attaques du même type.

La seconde demande requiert que nous réalisions certaines analyses, telle qu’une analyse des risques, avant de pouvoir proposé un PRA et PCA viable.

# Liste des tâches

## Décryptage des fichiers

* Déchiffrement du Rébus
* Trouver la clé de décryptage (en utilisant le brute force)
* Fournir et expliquer le logiciel de décryptage

## Réalisation du PCA & PRA et des analyses conjointes

* Modélisation du SI avec BPMN
* Analyse des Sinistres
* BIA
* Analyse des Risques
* PRA et PCA

# Répartitions des tâches

|  |  |
| --- | --- |
| **Nicolas Carpentier** | * Analyse des Sinistre * BIA * Analyse des Risque |
| **Nicolas HUET** | * Explication du logiciel de décryptage * Trouver la clé de décryptage |
| **Emmanuel REAL** | * Réalisation du PCA & PRA |
| **Guillaume REAL** | * Modélisation du SI en BPMN |
| **GROUPE** | * ??? |

# Décryptage des fichiers

## Déchiffrement du rébus

Le ransomware a envoyé un mail qui contenait le rebus ci-dessous. Une fois déchiffré, il nous donne le message suivant :

|  |  |  |
| --- | --- | --- |
|  | Flèche : courbe légère | Je viens d'appliquer un algorithme de cryptage XOR à tous vos fichiers.  Je vous laisse une semaine pour trouver la clé de 6 charactère alpha-minuscule maximum.  Le texte est codé est lettre par lettre avec la clé charactère par charactère. |
| **Rebus** |  | **Signification** |

Si ce le contenu du message est véridique, alors l’algorithme utilisé est simplement une application de l’opération XOR sur chaque lettre des fichiers. Cet algorithme est de type symétrique, c’est-à-dire que l’encryptage et le décryptage utilise la même clé.

Ce message nous renseigne également sur la clé utilisé lors de l’encryptage, elle serait potentiellement composée de 1 à 6 lettre alphabétique en minuscule. Avec ces infos, il nous ai possible d’implémenter une première solution pour trouver la clé utiliser et ainsi décrypter les fichiers.

## Trouvé la clé en utilisant la méthode brute force

La première étape est donc de trouvé la clé d’encryptage pour pouvoir ainsi décrypter les fichiers par la suite.

Les informations que nous avons sont les suivantes :

* L’opération utilisé lors de l’encryptage est le XOR
* La clé contient entre 1 et 6 lettre alphabétique en minuscule

Avec le peu d’information que nous avons, la méthode, semblant être la plus efficace pour trouver la clé, à utiliser serait d’effectuer un décryptage avec toutes les clés possibles et voir si nous obtenons des mots compris dans un dictionnaire.

Si après décryptage notre programme détecte la présence d’un mot cela signifie que nous avons potentiellement trouvé la clé. Nous allons donc stocker toutes les clés permettant d’obtenir un mot compréhensible par l’homme pour ensuite faire une dernière vérification et ainsi trouvé la bonne clé.

Pour résumé, nous allons d’en un premier temps limité le nombre de clé à vérifier grâce à notre programme et notre dictionnaire de mots pour ensuite vérifier, par nous-même, le résultat du décryptage avec les clés restantes.