

TLP: CLEAR

DEFEND
DETECT
RESPOND

RANSOMWARE x BLUE TEAMS

UMA GUERRA CIBERNÉTICA SEM FIM

ZOZIEL FREIRE



ENCRYPTING



DATA LOCKED



PAY OR LOSE



NO ESCAPE



YOU HAVE
BEEN HACKED



RANSOMWARE

YOUR FILES ARE ENCRYPTED

TIME LEFT:

47:59:59

PAY OR LOSE



CONHECER
O INIMIGO



FORTALECER
DEFESAS



DETECTAR
AMEAÇAS



INVESTIGAR
E ANALISAR



RESPONDER
RAPIDAMENTE



PROTEGER
SEMPRE

Disclaimer

Nada do que apresento aqui representa a posição da minha empresa. Todas as opiniões e análises são de minha exclusiva responsabilidade.

Propósito

Apresentar um pouco da evolução dos malwares e das defesas de segurança, evidenciando a adaptação constante entre atacantes e defensores.

Whoami ?

Whoami ?

- Profissional +16 anos de experiência em TI
- Pesquisador em segurança nos ecossistemas: Windows Linux e Apple
- Apaixonado por Análise e Desenvolvimento de Malware
- Organizador Apple Red Team Village
- Fã de Chaves e Chapolin 😊



Contribuições para Comunidade

TLP: CLEAR

hackbahia



NerdZão



cajusec
SECURITY CONFERENCE



Tópicos

- Do Vírus ao Ransomware
- O que é um Ransomware?
- Evolução: Ataque x Defesa
- Tipos de Ataques
- Evolução dos CSIRTs
- Estudos de Casos
- Conclusão



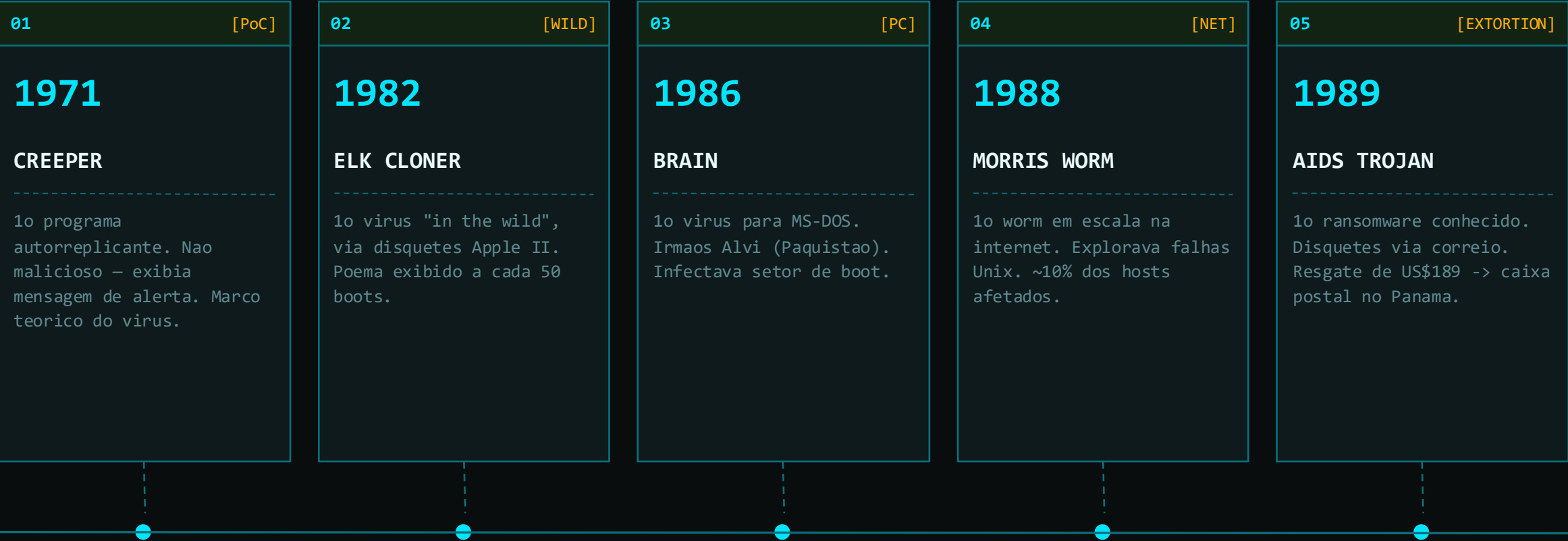
Do Virus ao Ransomware

>

DO PRIMEIRO VÍRUS AO PRIMEIRO RANSOMWARE_

TLP:CLEAR

// a evolução essencial do malware





O que é um ransomware?

O que é Ransowmare?

O ransomware é um tipo de ataque malicioso no qual os invasores criptografam os dados de uma organização, os vazam e exigem pagamento para restaurar o acesso ou impedir a exposição.

Modus Operandi

Modus - 1

Criptografia

Extorsão

Modus - 2

Criptografia

Extorsão

Exposição

Modus - 3

Criptografia

Extorsão

Exposição

Notificação Regulatório

Nota de Invasão

TLP: CLEAR



ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
<https://tox.chat/download.html>
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.

Wana Decrypt0r 2.0 3C4AE9B7

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT+5. Make sure to pay.



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)

encrypted



All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail: Ransomware2020@cock.li

Write this ID in the title of your message **4647FDEA-2930**

In case of no answer in 24 hours write us to this e-mail: Ransomware2021@cock.li

Our online operator is available in the messenger Telegram: [@Resp0nse](https://t.me/Resp0nse)

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 4Mb (non archived), and files should not contain valuable information.

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.

helpdecrypt@msgsafe.io



YOUR FILES ARE ENCRYPTED

Don't worry, you can return all your files!

If you want to restore them, follow this link: email helpdecrypt@msgsafe.io YOUR ID **C279F237**

If you have not been answered via the link within 12 hours, write to us by e-mail: helpdecrypt@msgsafe.io

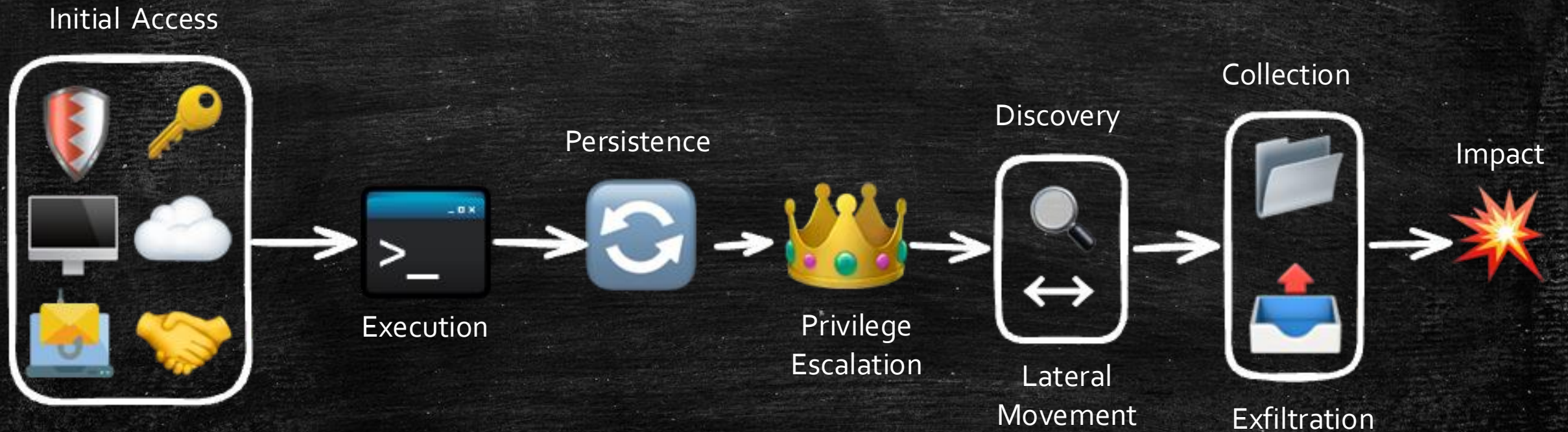
Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

AKIRA

Well, you are here. It means that you are as an unscheduled forced audit of your price to make it all go away. Do not you can do is to follow our instructions will minimize the damage that might. The functionality of this blog is to enjoy the juiciest information that you are unable to recover without our of final storage nor deleted by anyone.

Ransomware Kill Chain



Impactos

- Interrupção das operações
- Perdas financeiras
- Perda ou vazamento de dados
- Danos à reputação
- Consequências legais e regulatórias
- Redução da produtividade
- Custos de recuperação
- Impacto na continuidade do negócio



Evolução: Ataque x Defesa

UMA GUERRA SEM FIM

TLP:CLEAR

Evolução do ataque vs. evolução da defesa, década a década

● Marcos de ataque

● Resposta defensiva



- Vírus de disquete (Brain, Elk Cloner)
- Worms de rede local (Morris, 1988)
- Vírus de macro embrionários
- Phreaking e acesso não autorizado
- AIDS Trojan 1º Ransomware



- Worms por e-mail (ILOVEYOU, Melissa)
- Worms automatizados (SQL Slammer)
- Botnets surgem (Zeus, Conficker)
- Ataques web (SQL Injection, XSS)
- Phishing bancário se populariza



- Malware em infra crítica (Stuxnet)
- Ransomware moderno (CryptoLocker)
- Worm + exploit vazado (WannaCry)
- APTs e ataques direcionados
- Supply chain attacks (SolarWinds)



- Ransomware-as-a-Service (LockBit)
- Dupla/tripla extorsão de dados
- Ataques a identidade e nuvem
- IA generativa em phishing/deepfake
- Zero-days explorados em escala

ATÉ 1990



- Antivírus por assinatura (McAfee, Norton)
- Firewall de pacote simples
- Criptografia básica (PGP, DES)
- TCP Wrappers / controle Unix
- IDS acadêmico incipiente (Snort, 1998)

2000 – 2009



- NGFW (stateful inspection)
- IDS/IPS comerciais (Snort, Sourcefire)
- SIEM surge (correlação de logs)
- VPN corporativa (IPSec/SSL)
- Pentest evolui (Nessus, Metasploit)

2010 – 2019



- EDR substitui o antivírus
- Threat Intel Platforms (IOC feeds)
- SOAR (automação de resposta)
- MITRE ATT&CK como framework
- ML/UEBA na detecção de anomalias

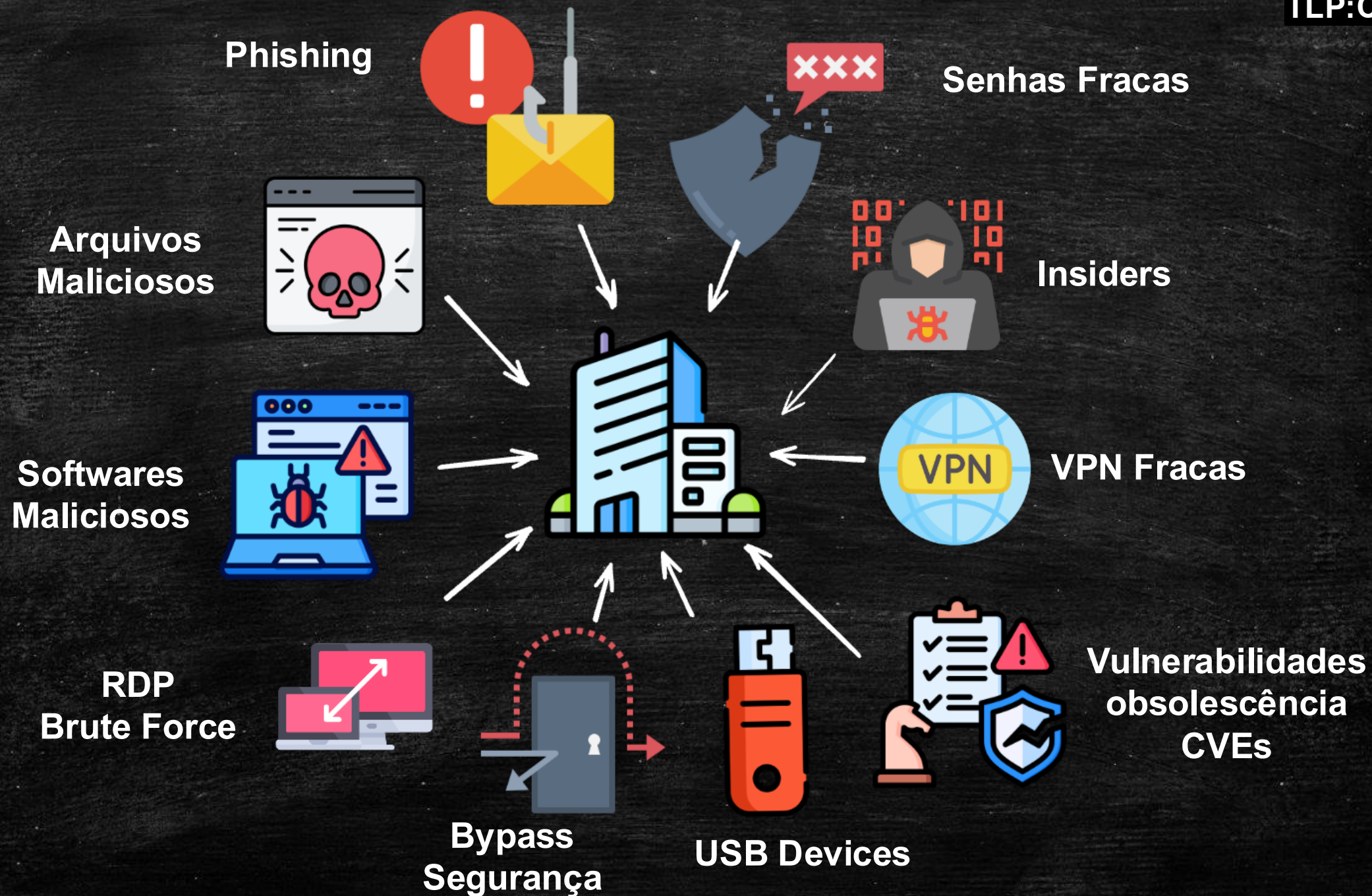
2020 – 2029



- XDR unificado (endpoint/rede/cloud)
- Zero Trust como padrão
- IA generativa no SOC (copiloto)
- CNAPP (segurança cloud-native)
- ITDR (ameaças à identidade)



Tipos de Ataques



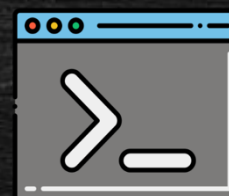
Exemplo de estágios de um Ataque

Recebimento de e-mail de phishing com documento anexado



O documento é aberto e executa macros diretamente no disco / memória

Execução de comandos via macros



Execução de PowerShell via linha de comando
Memória ou Disco

Criptografia de Dados via Script



Exibição da nota de resgate

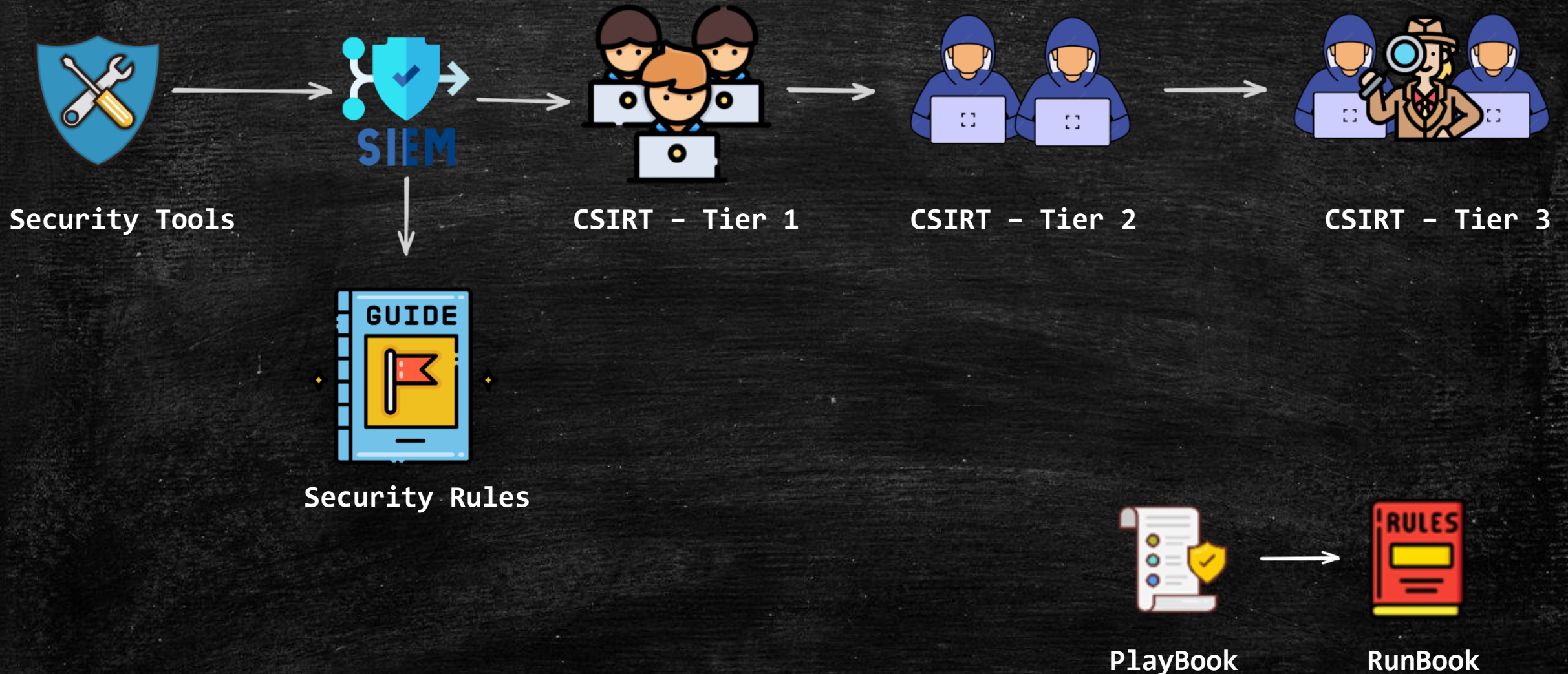
Evolução dos CSIRTs



Do Antivírus a Inteligência Artificial

Fluxo Tradicional

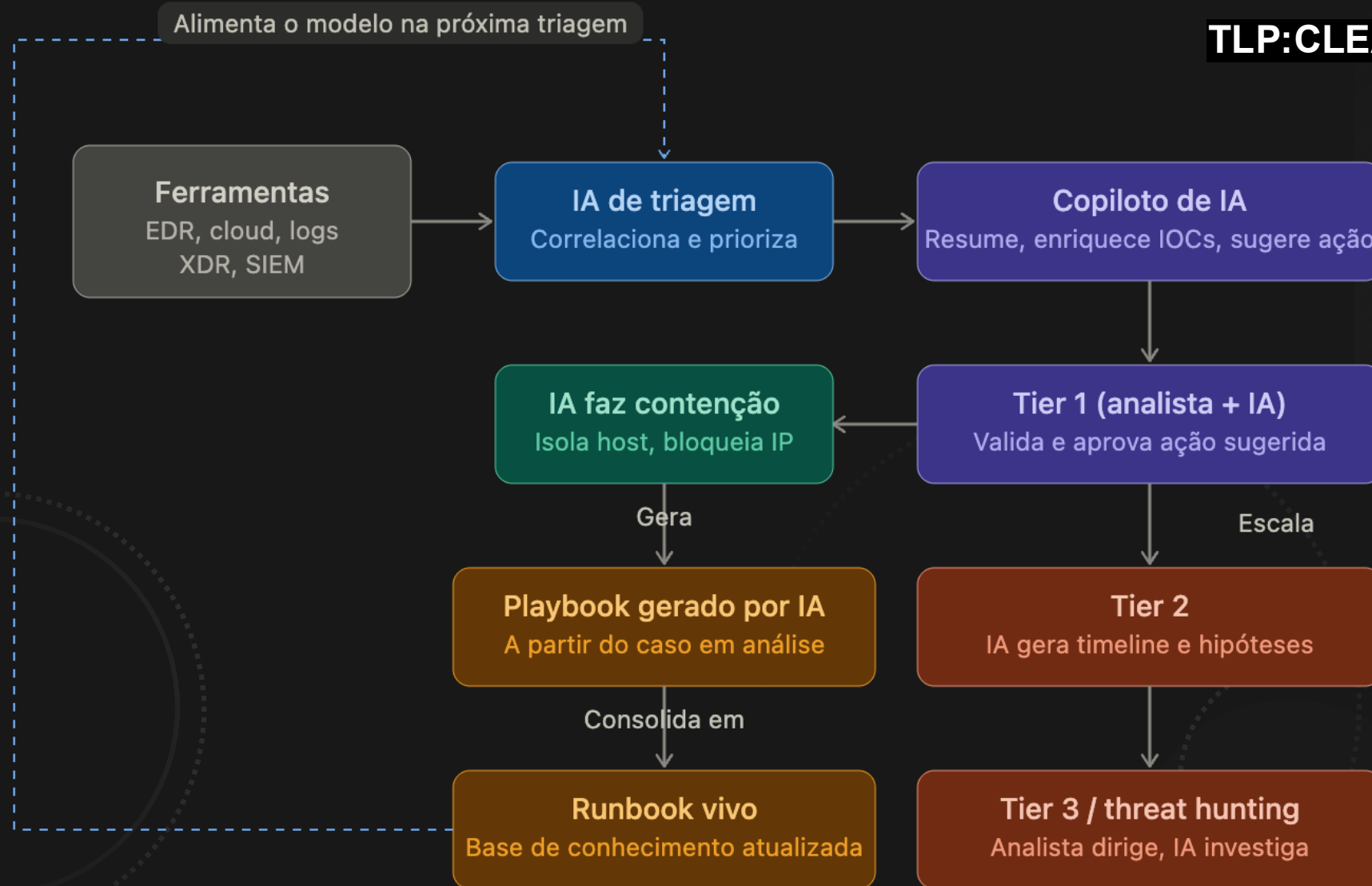
TLP:CLEAR



CSIRT - Computer Security Incident Response Team

Fluxos Futuros

TLP: CLEAR



SOC: Security Operations Center

IA atua como copiloto em cada tier, não substitui o analista humano

BLUE TEAM

DEFEND • DETECT • RESPOND • RECOVER

CONCLUSÃO & RECOMENDAÇÕES



Controles Importantes

TLP: CLEAR

- Antivírus / EDR
- SIEM
- XDR
- Firewall NGFW
- IDS / IPS
- Scanner de Vulnerabilidades
- IAM
- PAM
- MFA
- DLP
- WAF
- Segurança de E-mail
- Backup e Recuperação
- Gestão de Patches

Controles Importantes

TLP:CLEAR

- SOAR
- CASB
- SASE
- Threat Intelligence
- Threat Hunting
- Foreense Digital
- Pentest
- Criptografia e Gestão de Chaves
- GRC (Governança, Risco e Compliance)
- War Games
- Threat Simulations

Estaremos Seguros? Não!

A AI vai resolver tudo?

Não, mas vai ajudar!

Perguntas?

Contatos

Telegram: @pun1sh3rx0
[linkedin.com/in/zozielfreire](https://www.linkedin.com/in/zozielfreire)

Obrigado!

