

# OPSEC for Red Teamers

Como ficar fora da cadeia?



\$ whoami  
Vinicius Vieira "@v1n1v131r4"

- SecOps Manager at Trustly
- Professor at FIAP University
- MSc. Emergent Technology | Pós Ethical Hacking
- CVE holder & Exploit Writer
- VulnHub & OffSec | DEF CON 5551
- Writer "OPSEC: Inteligência Cibernética na Prática"



# Agenda

- Intro
- OPSEC Fundamentals
- OPSEC Fails
- Advanced OPSEC Techniques
- Study Cases
- Practical Recommendations
- Conclusion



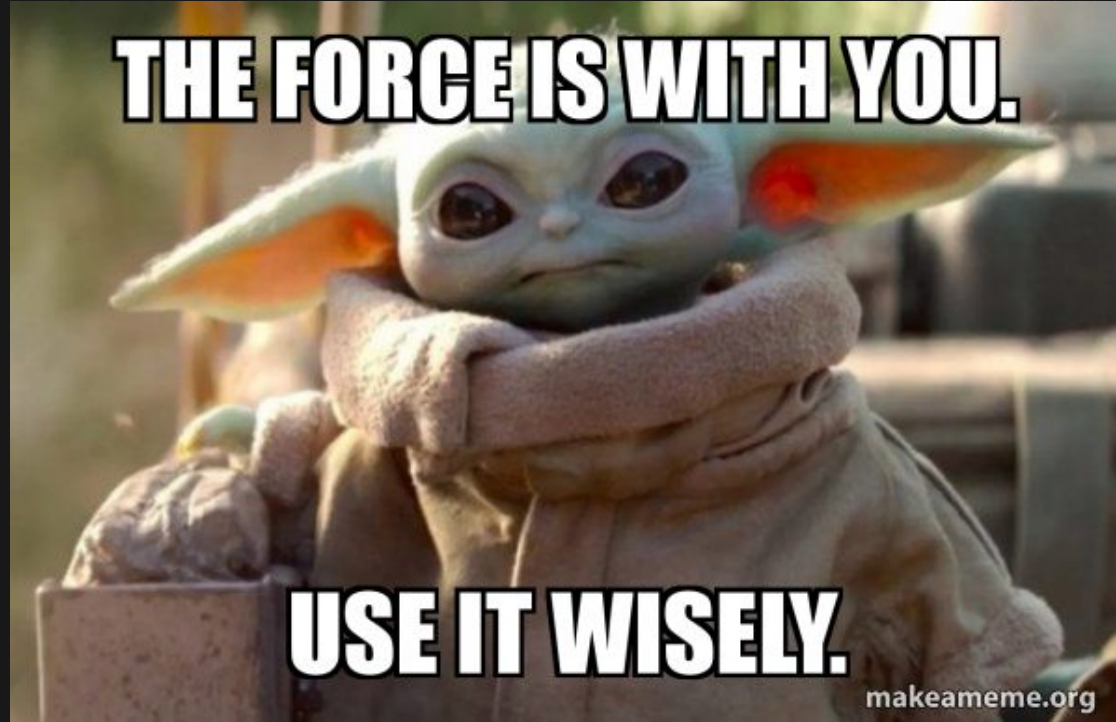
# Disclaimer

Os meus atuais empregadores não possuem relação direta e/ou indireta com o conteúdo aqui apresentado. Todo material foi desenvolvido por mim, baseado nas minhas experiências profissionais anteriores e/ou pesquisas sobre o assunto.

Logo, todo conteúdo apresentado nesta aula será exclusivamente para fins educativos e não deve ser usado para perpetração de crimes, sejam eles cibernéticos ou não.



# DISCLAIMER





# Intro

quais são as 5 principais perguntas que usuários te fazem sobre técnicas de Red Team?

Ótima pergunta. Com base nas interações mais comuns de usuários interessados em segurança ofensiva, aqui estão as **5 principais perguntas sobre técnicas de Red Team**:



# Intro

1. Como montar uma infraestrutura segura e anônima para operações de Red Team?
2. Quais são as melhores ferramentas e frameworks atuais para Red Teaming?
3. Como evitar detecção por EDRs e antivírus durante um exercício?
4. Como realizar ataques de phishing com maior taxa de sucesso em ambientes controlados?
5. Quais técnicas um Red Teamer pode usar para escalar privilégios e se mover lateralmente sem disparar alertas?



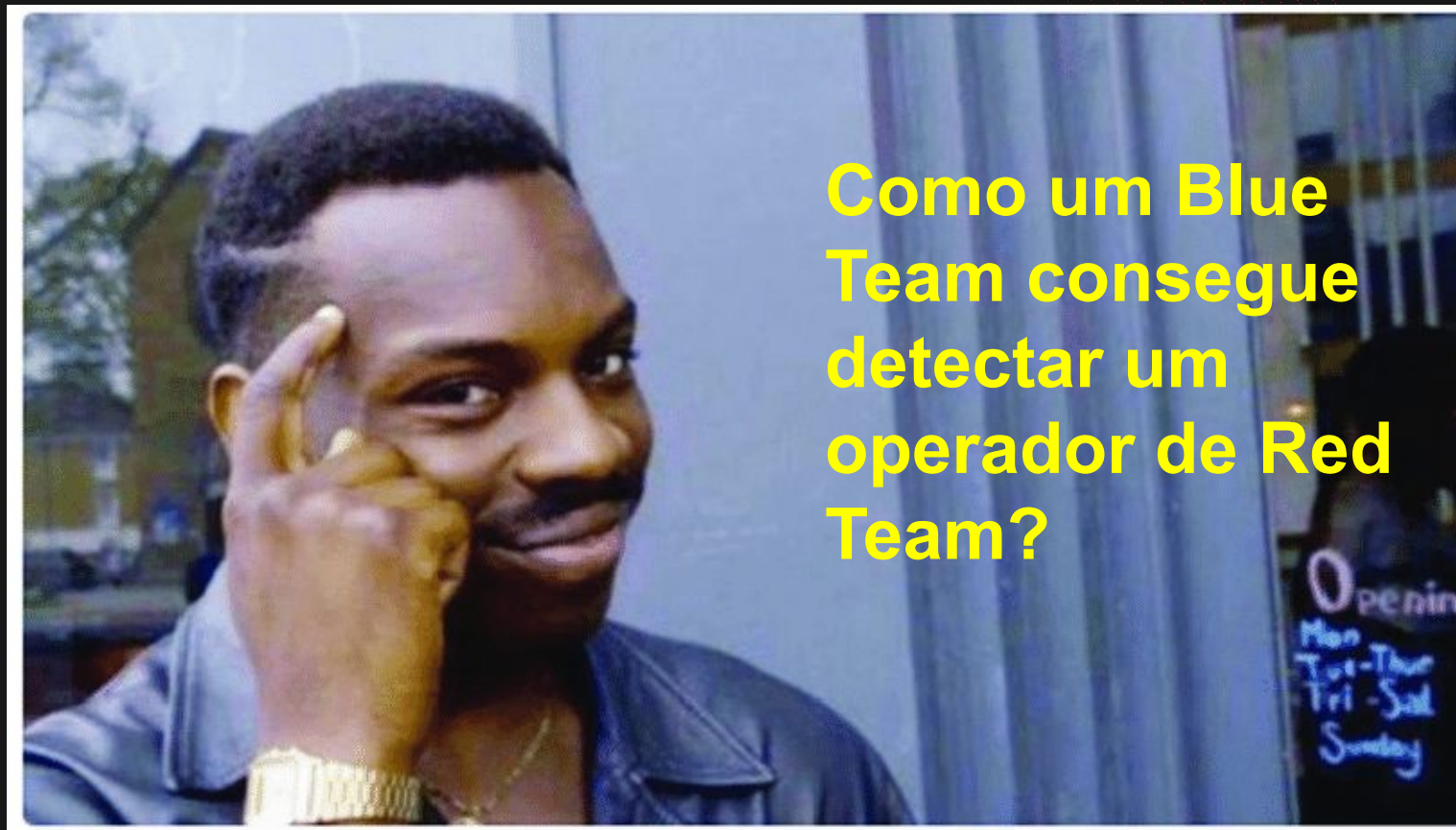
# Intro

1. Como montar uma infraestrutura segura e anônima para operações de Red Team?
2. Quais são as melhores ferramentas e frameworks atuais para Red Teaming?
3. Como evitar detecção por EDRs e antivírus durante um exercício?
4. Como realizar ataques de phishing com maior taxa de sucesso em ambientes controlados?
5. Quais técnicas um Red Teamer pode usar para escalar privilégios e se mover lateralmente sem disparar alertas?





# Intro



# Intro

- Assinaturas e Indicadores de Comprometimento (IoCs)
- Comportamentos Anômalos
- Detecção Baseada em Telemetria
- Análise de Tráfego e C2
- Monitoramento de Mudanças em Identidades e Privilégios

>>> Logs e Eventos de Segurança



# OPSEC Fundamentals

## 5 KEY STEPS OF THREAT MODELING PROCESS



# OPSEC Fails

- Configurações default
- Reutilização de Infraestruturas
- Reutilização de Contas
- Misturar ambiente pessoal/trabalho com operação
- Financial chain !!!



# Stay out of Jail

O que pode ajudar a identificar o autor de um tráfego de dados?

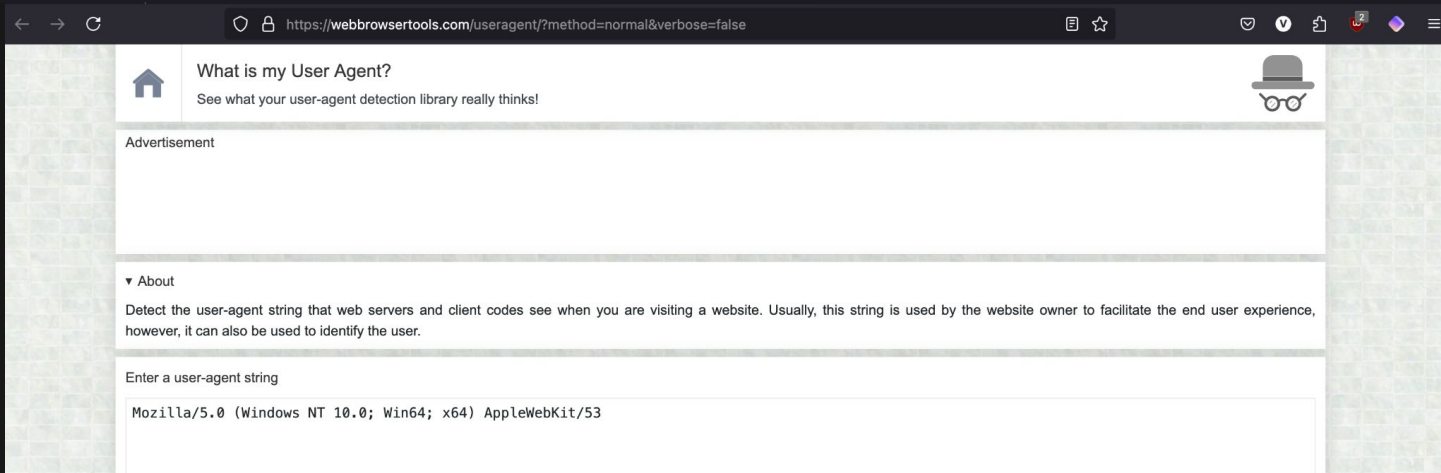
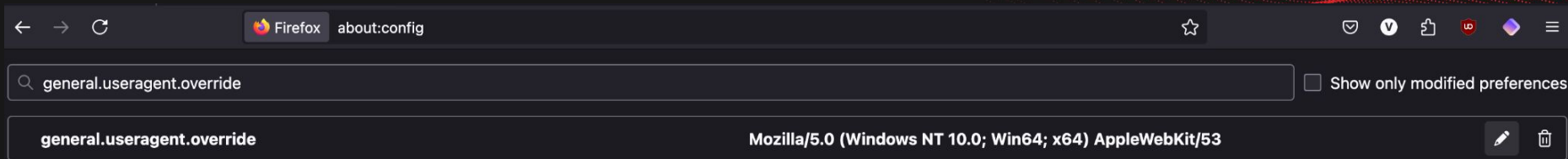
- IP
- User-Agent
- Cookies
- Fingerprinting
- Navegação prévia
- Análise circunstancial
- Correlação de tráfego
- Behaviour !!!





# Advanced Techniques - Default Confs

## Custom browser User-Agent



# Advanced Techniques - Default Confs

Wget, nmap, curl... custom User-Agent

```
# vim ~/.bashrc (ou ~/.zshrc)
```

```
export AGENT="Mozilla/5.0 (Windows NT 10.0; Win64; x64)"  
alias curl="curl -A '$AGENT'"  
alias wget="wget -U '$AGENT'"  
alias nmap="nmap --script-args=\"http.useragent='$AGENT'\""
```



# Advanced Techniques - Default Confs

about:preferences#privacy

## Firefox Data Collection and Use

We strive to provide you with choices and collect only the minimal data necessary to improve Firefox for everyone. [View Privacy Notice](#)

 You're no longer allowing Mozilla to capture technical and interaction data. All past data will be deleted within 30 days. [Learn more](#)

### ☐ Send technical and interaction data to Mozilla

This helps us improve Firefox features, performance, and stability. [Learn more](#)

#### ☐ Allow personalized extension recommendations

Get extension recommendations to improve your browsing experience. [Learn more](#)

#### ☐ Install and run studies

Try out features and ideas before they're released to everyone. [View Firefox studies](#)

### ☐ Send daily usage ping to Mozilla

This helps Mozilla to estimate active users. [Learn more](#)

### ☐ Automatically send crash reports

This helps Mozilla diagnose and fix issues with the browser. Reports may include personal or sensitive data. [Learn more](#)



# Advanced Techniques - Default Confs


about:preferences#privacy


## ☒ Strict

Stronger protection, but may cause some sites or content to break.

Firefox blocks the following:

- Social media trackers
- Cross-site cookies in all windows
- Tracking content in all windows
- Cryptominers
- Known and suspected fingerprinters

 You will need to reload your tabs to apply these changes.

 **Reload All Tabs**

### Heads up!

This setting may cause some websites to not display content or work correctly. If a site seems broken, you may want to turn off tracking protection for that site to load all content. [Learn how](#)



# Advanced Techniques - Default Confs

about:preferences#privacy

## DNS over HTTPS

Domain Name System (DNS) over HTTPS sends your request for a domain name through an encrypted connection, providing a secure DNS and making it harder for others to see which website you're about to access.

[Learn more](#)

Status: Off

Manage Exceptions...

Enable DNS over HTTPS using:

☐ Default Protection

Firefox decides when to use secure DNS to protect your privacy.

☐ Increased Protection

You control when to use secure DNS and choose your provider.

☐ Max Protection

Firefox will always use secure DNS. You'll see a security risk warning before we use your system DNS.

☒ Off

Use your default DNS resolver





# Advanced Techniques - Default Confs

WebRTC implement STUN (Session Traversal Utilities for Nat), a protocol that allows to discover the public IP address.

**WebRTC is a free, open project** that provides browsers and mobile applications with Real-Time Communications (RTC) capabilities via simple APIs. The WebRTC components have been optimized to best serve this purpose.

<https://browserleaks.com/>



# Advanced Techniques - Infra Reuse

VPN Fail safe

```
sudo openvpn --config <arquivo.ovpn> --script-security 2  
--down ./vpn-down.sh
```



# Advanced Techniques - Infra Reuse

```
#!/bin/bash
```

```
systemctl stop NetworkManager 2>/dev/null
```

```
killall -9 dhclient 2>/dev/null
```

```
for iface in $(ip -o link show | awk -F': ' '{print $2}' | grep -vE "^lo$"); do  
    ip link set dev "$iface" down  
done
```

```
ip route flush table main
```

```
iptables -F
```

```
iptables -X
```

```
iptables -t nat -F
```

```
iptables -t nat -X
```

```
iptables -t mangle -F
```

```
iptables -t mangle -X
```

```
iptables -P INPUT DROP
```

```
iptables -P FORWARD DROP
```

```
iptables -P OUTPUT DROP
```

```
iptables -A INPUT -i lo -j ACCEPT
```

```
iptables -A OUTPUT -o lo -j ACCEPT
```



# Advanced Techniques - Infra Reuse

## DNSEncrypt no Kali

```
sudo apt install dnscrypt-proxy  
sudo systemctl enable dnscrypt-proxy  
sudo systemctl start dnscrypt-proxy
```



# Advanced Techniques - Infra Reuse

Segmentação de Infraestrutura para Minimizar Correlações

Evite reutilizar IPs ou domínios em diferentes fases da operação. Por exemplo:

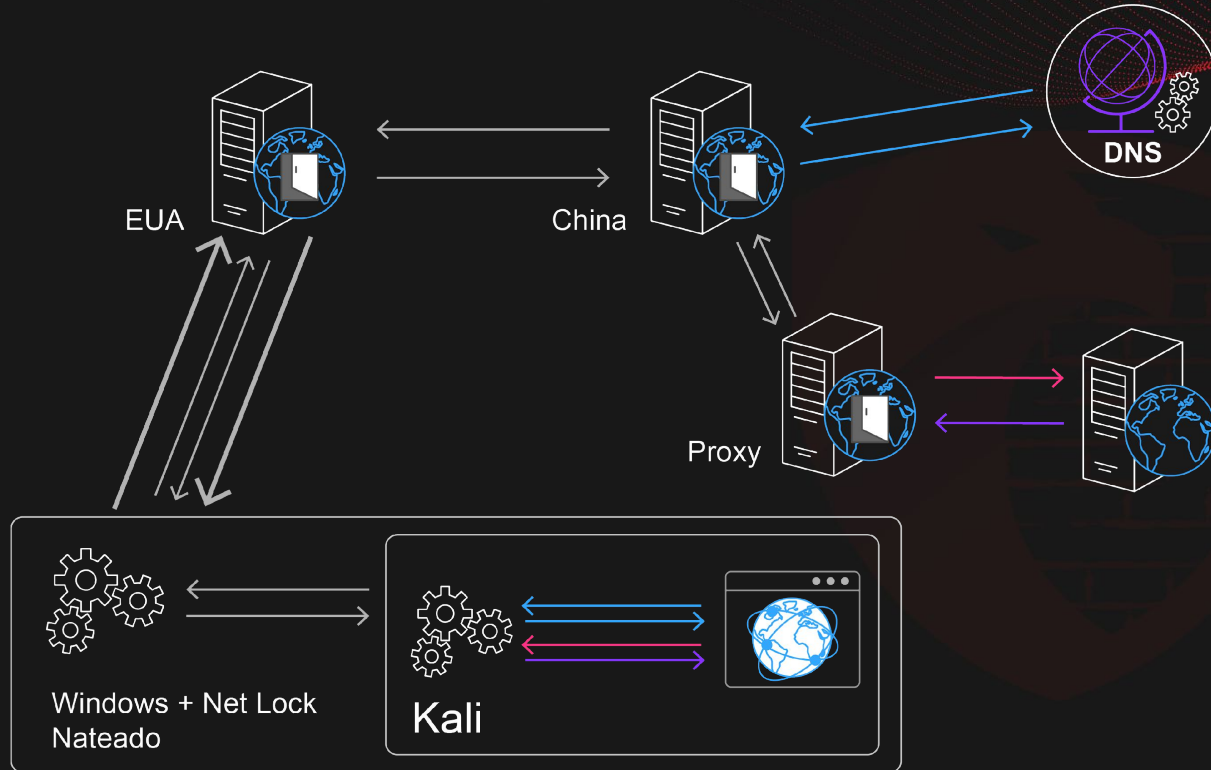
- **Domínio A:** Envio de e-mails de phishing
- **Domínio B:** Hospedagem de payloads
- **Domínio C:** Comunicação C2





# Advanced Techniques - Infra Reuse

## Modelo: Duplo Túnel VPN e Proxy



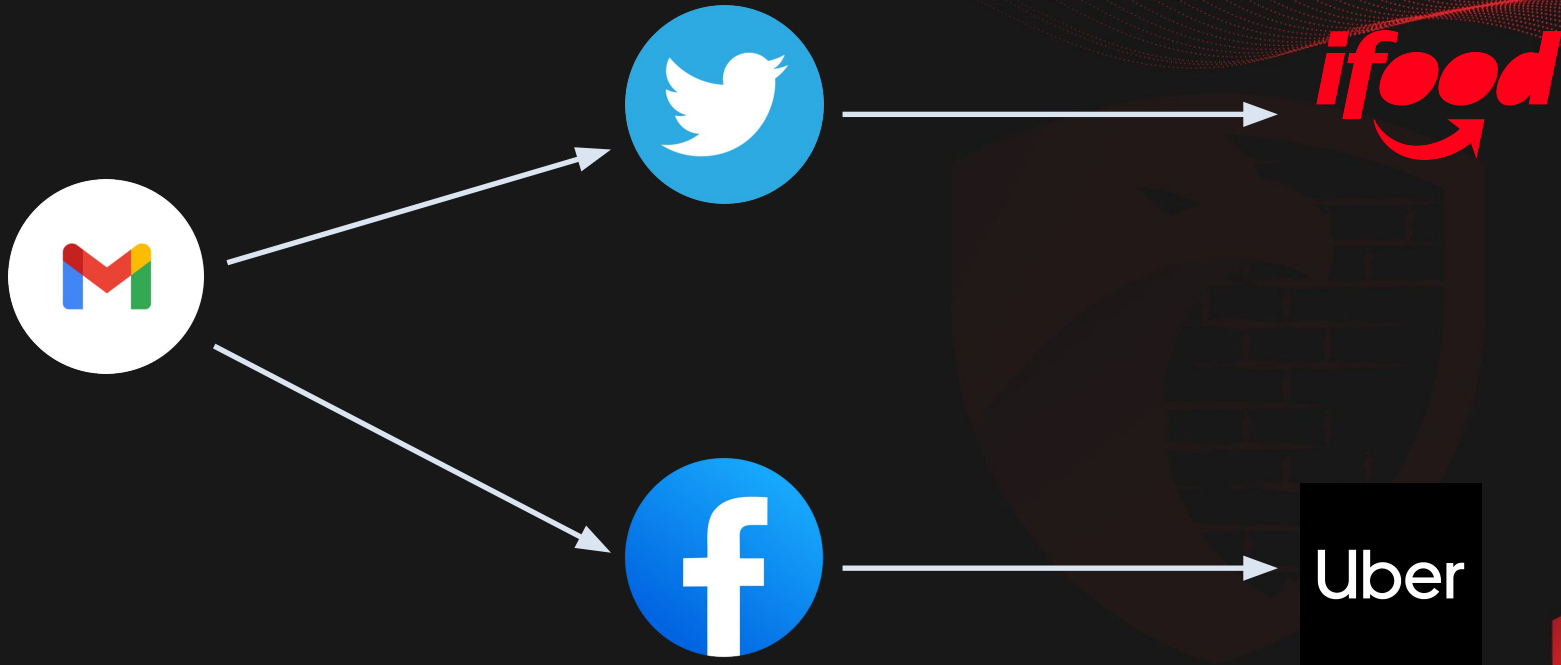
# Advanced Techniques - Infra Reuse

- Use uma VM para cada operação
- Use uma conexão (VPN, Proxy, TOR..) para cada operação
- Prefira ambientes Cloud/VPS que vc possa excluir o host após uso



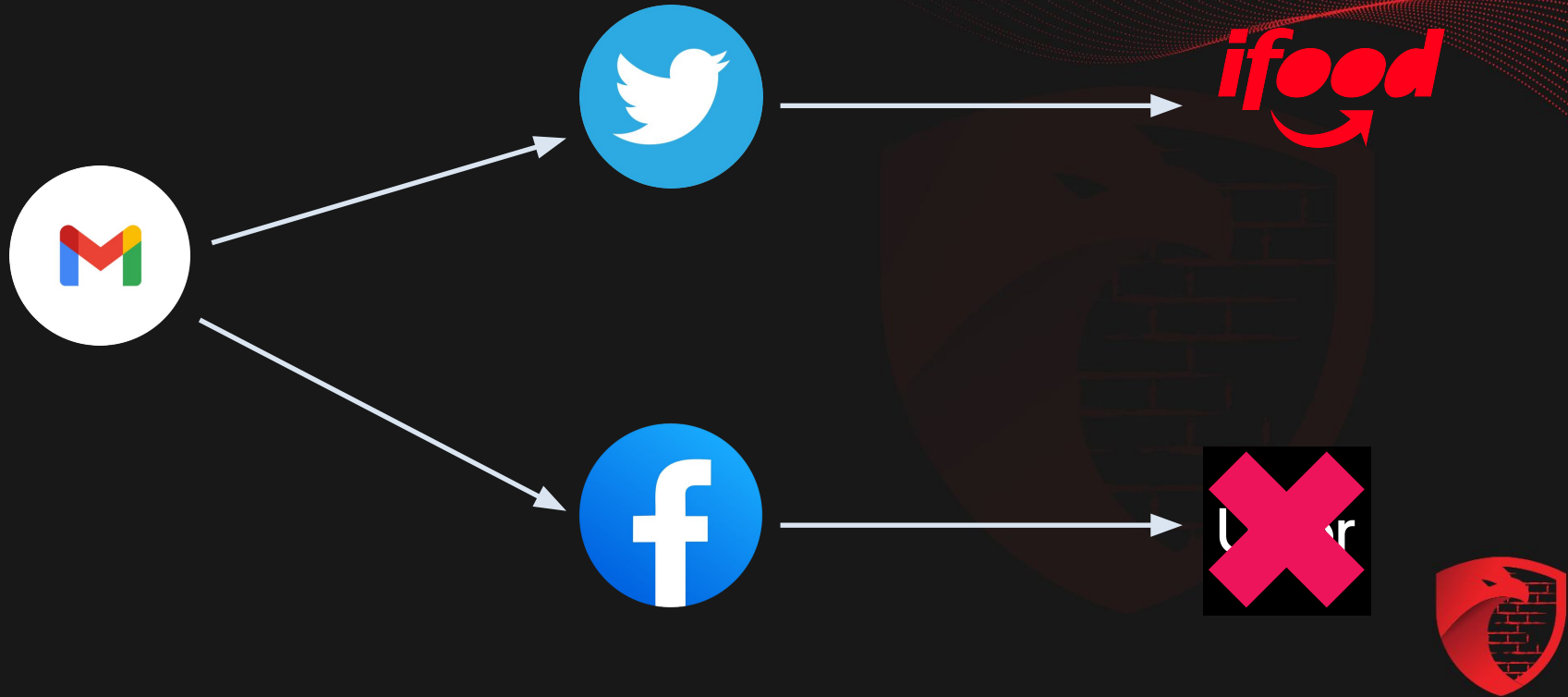
# Advanced Techniques - Account Reuse

Cadeia de anonimato



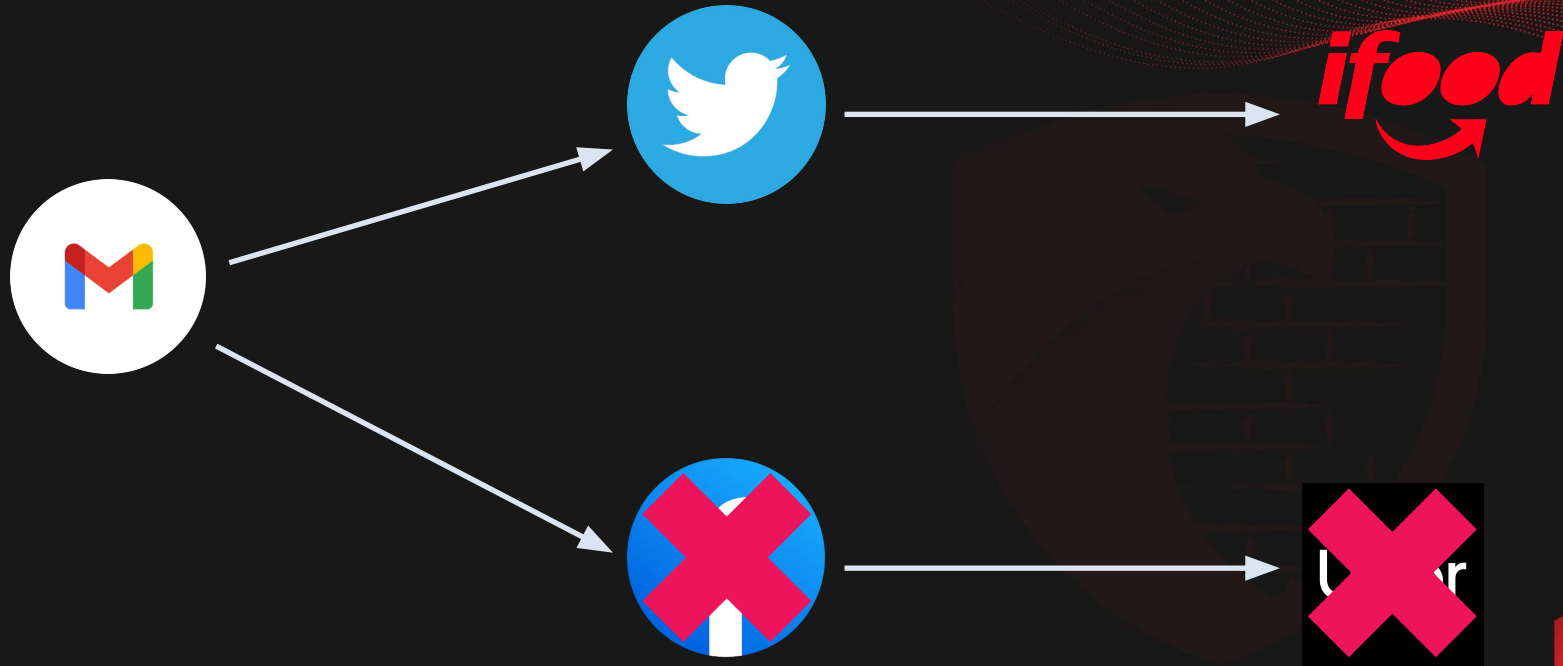
# Advanced Techniques - Account Reuse

Cadeia de anonimato



# Advanced Techniques - Account Reuse

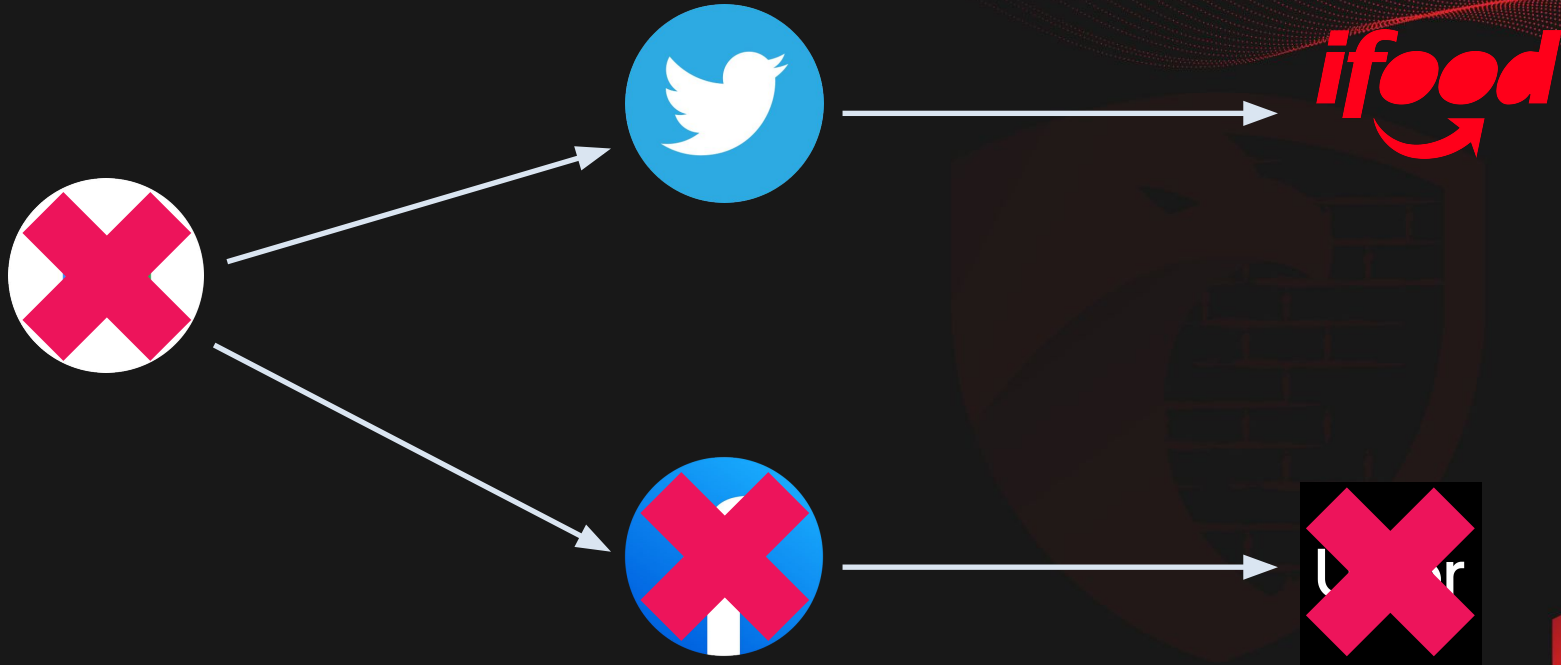
Cadeia de anonimato





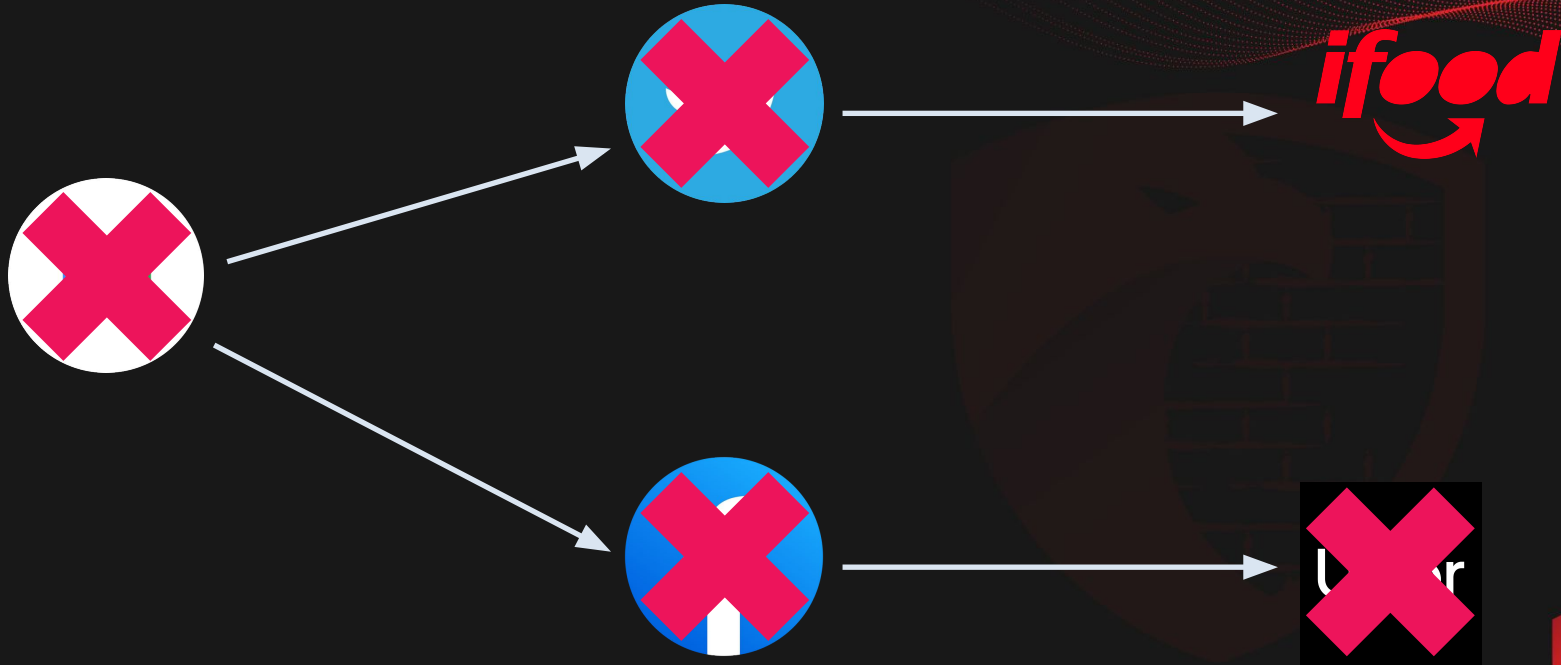
# Advanced Techniques - Account Reuse

Cadeia de anonimato



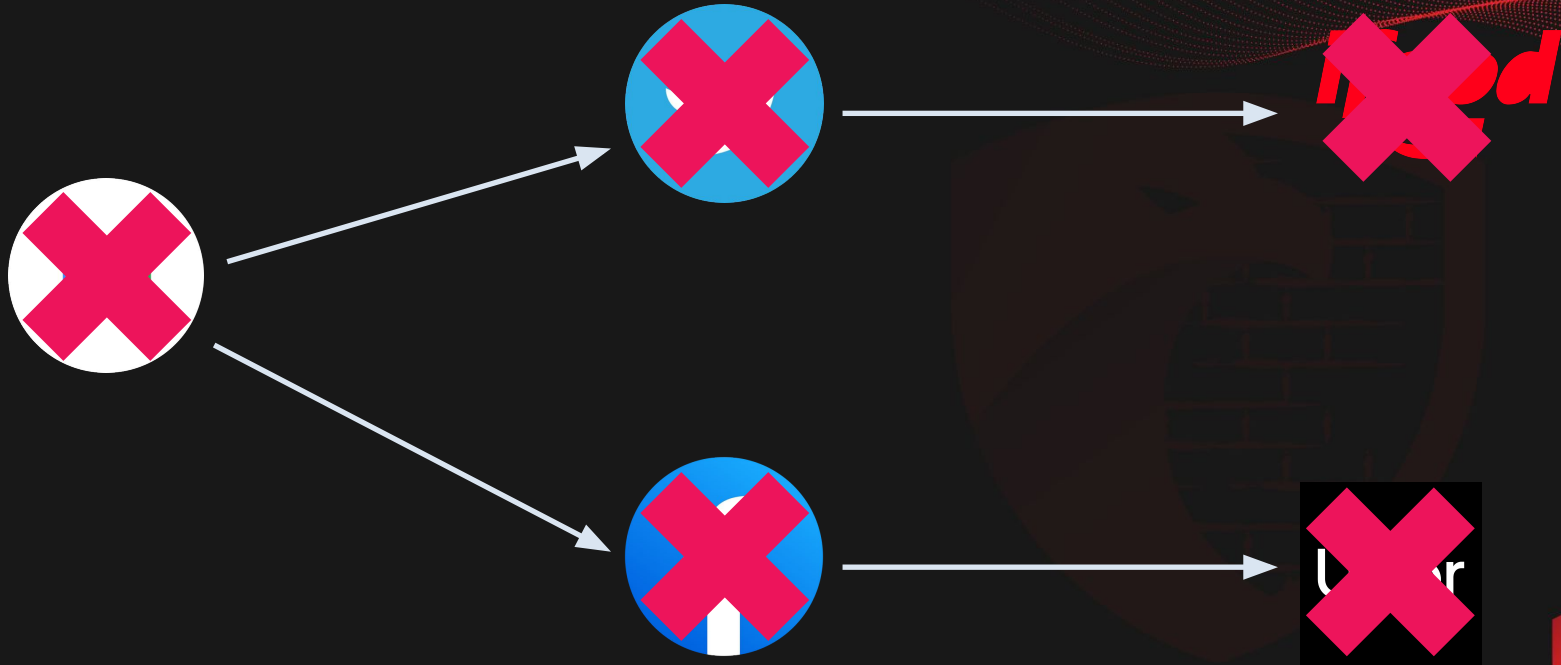
# Advanced Techniques - Account Reuse

Cadeia de anonimato



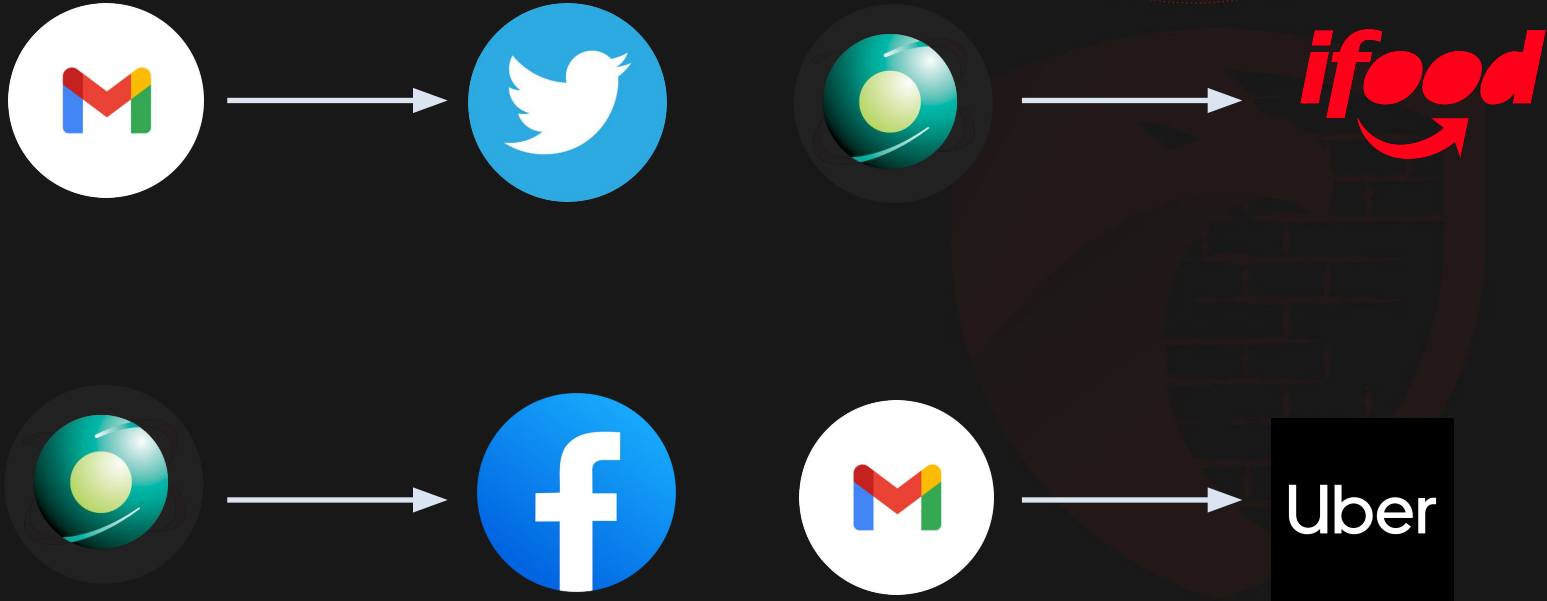
# Advanced Techniques - Account Reuse

Cadeia de anonimato



# Advanced Techniques - Account Reuse

Cadeia de anonimato

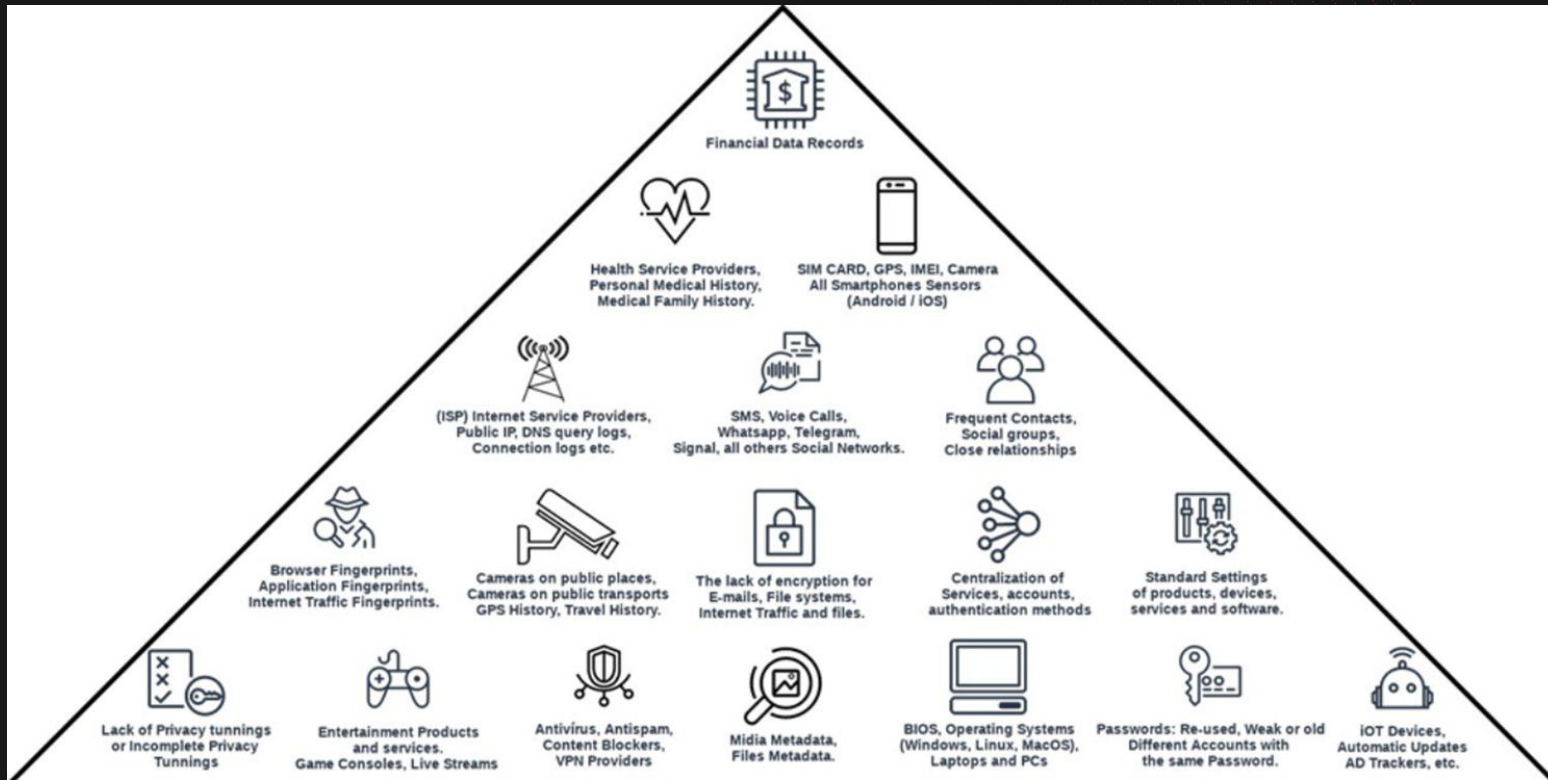


# Gold Tips for “Digital” OPSEC

- Seu computador "de trabalho" nunca deve ter nada pessoalmente relacionado à sua identidade real. Nunca!
- Prefira Sistemas Operacionais Open Source
- Use criptografia em seu disco.
- Use um firewall de host.
- Desabilite a inicialização via USB nas configurações da BIOS, e coloque senha nelas.
- Sempre use uma VPN. Sempre!
- Prefira salvar tudo em um USB ao invés da nuvem.
- Use um gerenciador de senhas e nunca salve as senhas no browser.
- Use o Whonix para as suas atividades na Dark Web. A VM deve ser salva em um USB/Micro SD e criptografada.
- Tenha o costume de limpar sua RAM antes de cada desligamento.
- Esteja ciente de outros dispositivos que você possa ter consigo que estejam revelando sua localização.
- Use criptografia PGP para envio de e-mail seguro.
- Use apenas teclados e mouses com fio.



# Financial Chain



Where does my Privacy fail? - The Gold mine for tracking, surveillance, and correlation attacks.

By: Rêner Alberto (aka Gr1nch) - Twitter: @Gr1nchDC - Email: rener.silva@protonmail.com - LinkedIn: <https://www.linkedin.com/in/reneralberto/en-us>  
DcLabs Security Team










# Financial Chain

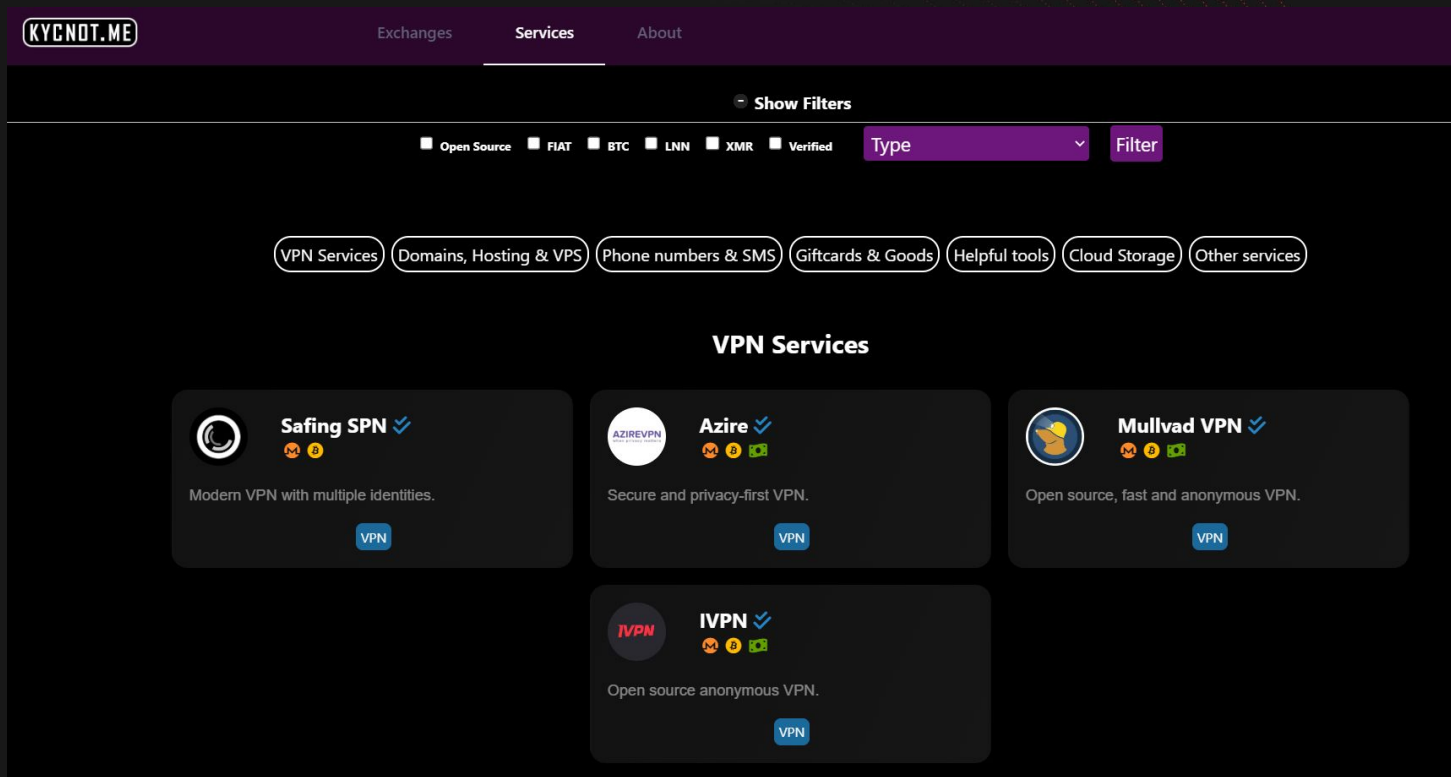
masterthecrypto

COMPARISON OF  
**ANONYMOUS**  
CRYPTOS

	PRIVATE	FUNGIBLE	DECENTRALIZED
 MONERO	✓	✓	✓
 bitcoin	✗	✗	✓
 CASH	?	?	✗
 DASH	✗	✗	✗
 VERGE	✗	✗	✓



# Financial Chain



The screenshot displays the KYCNOT.ME website interface. At the top, there is a navigation bar with the site logo and links for 'Exchanges', 'Services', and 'About'. Below this, a 'Show Filters' button is visible. A row of filter checkboxes includes 'Open Source', 'FIAT', 'BTC', 'LNN', 'XMR', and 'Verified'. A dropdown menu labeled 'Type' is set to 'Type', with a 'Filter' button next to it. A horizontal scrollable list of service categories is shown: 'VPN Services', 'Domains, Hosting & VPS', 'Phone numbers & SMS', 'Giftcards & Goods', 'Helpful tools', 'Cloud Storage', and 'Other services'. The 'VPN Services' section is highlighted, showing four service cards: 'Safing SPN' (Modern VPN with multiple identities), 'Azire' (Secure and privacy-first VPN), 'Mullvad VPN' (Open source, fast and anonymous VPN), and 'IVPN' (Open source anonymous VPN). Each card includes a logo, a name with a checkmark, a description, and a 'VPN' button. A decorative red dotted line graphic is on the right side of the page.


KYCNOT.ME Exchanges Services About


Show Filters


Open Source FIAT BTC LNN XMR Verified Type Filter


VPN Services Domains, Hosting & VPS Phone numbers & SMS Giftcards & Goods Helpful tools Cloud Storage Other services

### VPN Services

**Safing SPN** ✓  
Modern VPN with multiple identities.  
VPN

**Azire** ✓  
Secure and privacy-first VPN.  
VPN

**Mullvad VPN** ✓  
Open source, fast and anonymous VPN.  
VPN

**IVPN** ✓  
Open source anonymous VPN.  
VPN

<https://kycnot.me/>

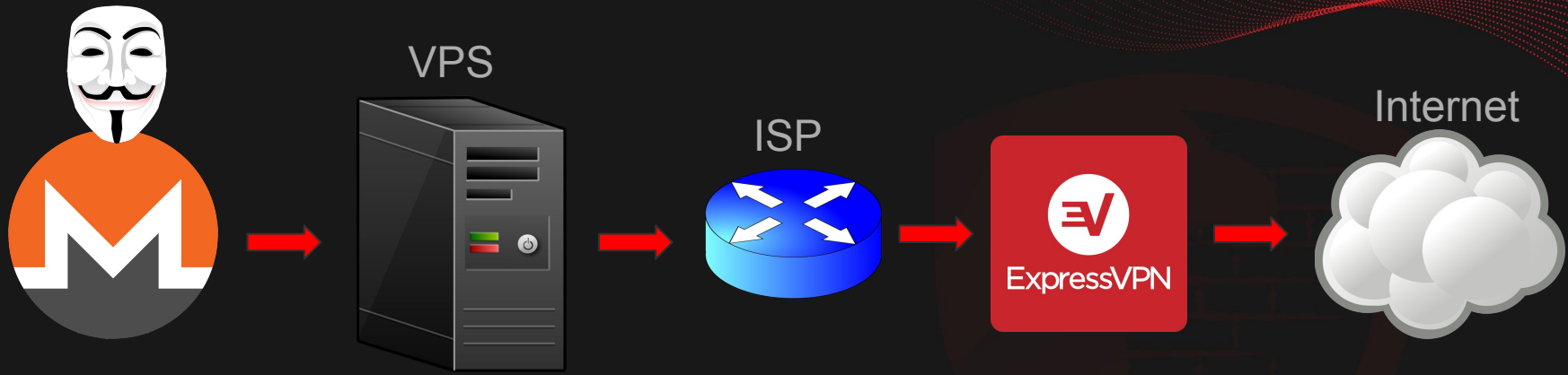


# Financial Chain

Financial Anonymity  $\neq$  Operational Security



# Financial Chain



# Financial Chain



# Financial Chain





# Financial Chain



# Financial Chain

[Products](#)[Industries](#)[Services](#)[Insights](#)[Company](#)[Log in](#)[Request a demo](#)

## Blockchain intelligence for investigations, risk, and security

From reactive to proactive, monitor fraud, pursue illicit activity, and detect and deter threat actors.

[Request a demo](#)

Receiving Exposure



Activity summary



[See more](#) ▾

# Qual o seu objetivo?

## 5 KEY STEPS OF THREAT MODELING PROCESS



# Good Sources

- Your VPS Provider Can Still Betray You, Monero or Not -

<https://youtu.be/OgzMrhcMcUM?feature=shared>

- OPSEC Fundamentals for Remote Red Teamers -

[https://www.blackhillsinfosec.com/webcast-opsec-fundamentals-for-remote-red-teams/?utm\\_source=chatgpt.com](https://www.blackhillsinfosec.com/webcast-opsec-fundamentals-for-remote-red-teams/?utm_source=chatgpt.com)



# Thank you!



[v1n1v131r4.com](http://v1n1v131r4.com)

[twitter.com/v1n1v131r4](https://twitter.com/v1n1v131r4)

[linkedin.com/in/v1n1v131r4](https://linkedin.com/in/v1n1v131r4)

