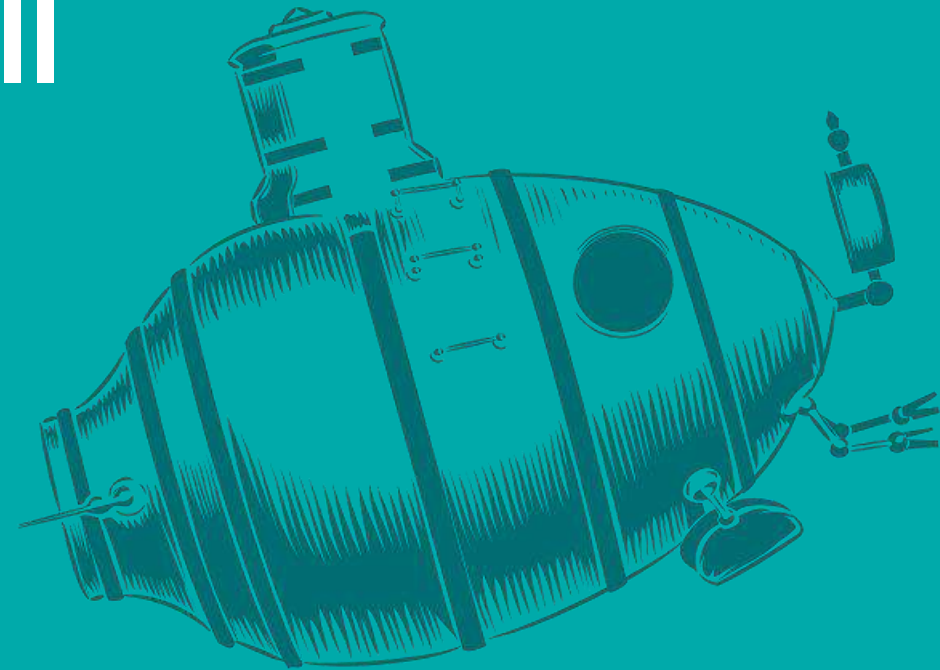


ALEF

(Ne)veselé historky z KB III

Michal Zedníček
ALEF NULA



Disclaimer:

1. Události popsané v této prezentaci ve své podstatě nejsou k smíchu a útočníci pravděpodobně postupují mimo zákony ČR.
2. Všechny popsané útoky byly vedeny na mojí identitu, pro jejich testování nebyla užita žádná jiná identita.

Případ č. 1

LIDÉ A HRUBÉ TELEFONICKÉ NALÉHÁNÍ



Základ story

1. Příběh: mám někde zapomenuté investiční crypto
2. Cíl: snaha přimět mě kliknout na odkaz (někde nějaký)

Obsah sociální inženýrství:

- Žijeme ve světě duality (dobré/špatné, světlé/temné ...) = touha/odpor
- Běhání za touhou = mrkvička v budoucnosti = až budu takový, bude to skvělé ...

TELEFONÁT 1 (T0)

1. **Kontakt:** zahraniční číslo (EU)
2. **Jazyk:** SK
3. **Strategie:** euforie
4. **Taktika:** jemná manipulace do crypto wallet
5. **Replika:** ukončil jsem telefon
6. **Reakce:** nic

TELEFONÁT 2 (T0 + 7D)

1. **Kontakt:** zahraniční číslo (EU)
2. **Jazyk:** SK
3. **Strategie:** nátlak
4. **Taktika:** vyhrožování, že o všechno přijdu, pokud to neudělám do XY
5. **Replika:** ukončil jsem telefon
6. **Reakce:** nic

TELEFONÁT 3 (T0 + 8D)

1. **Kontakt:** zahraniční číslo (SK)
2. **Jazyk:** SK
3. **Strategie:** nátlak
4. **Taktika:** osobní zesměšňování
5. **Replika:** ukončil jsem telefon
6. **Reakce:** 8 pokusů o kontakt ze stejného čísla během 3 minut, nic jsem nevzal

TELEFONÁT 4 (T0 + 9D)

1. **Kontakt:** CZ číslo
2. **Jazyk:** SK
3. **Strategie:** nátlak
4. **Taktika:** osobní zesměšňování
5. **Replika:** chtěl jsem IČO, kontakt na ředitele a odkaz na firmu
6. **Reakce:** ukončili hovor

TELEFONÁT 5 (T0 + 8D)

1. **Kontakt:** CZ číslo
2. **Jazyk:** SK
3. **Strategie:** nátlak
4. **Taktika:** osobní zesměšňování
5. **Replika:** ukončil jsem telefon
6. **Reakce:** 17 pokusů o kontakt ze různých čísel během 5 minut, nic jsem nevzal

BREAK1

Aktivita 1: Konzultace s operátorem

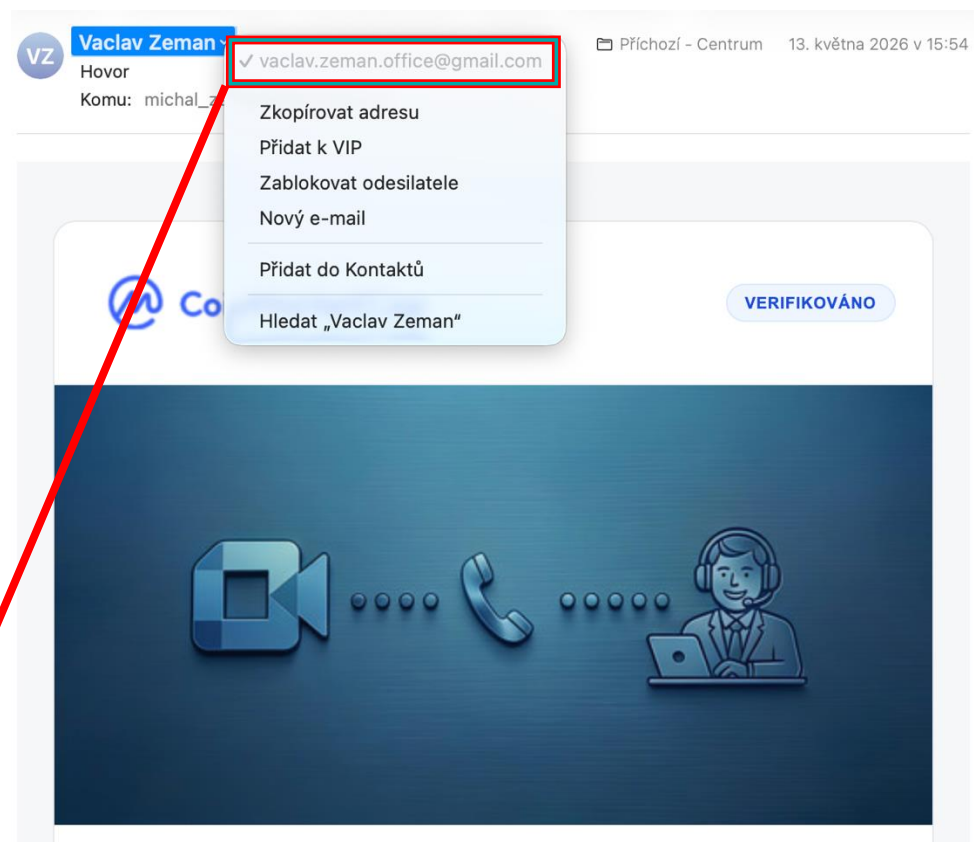
Aktivita 2: Zablokování všech použitých čísel

TELEFONÁT 6 (T0 + 8D)

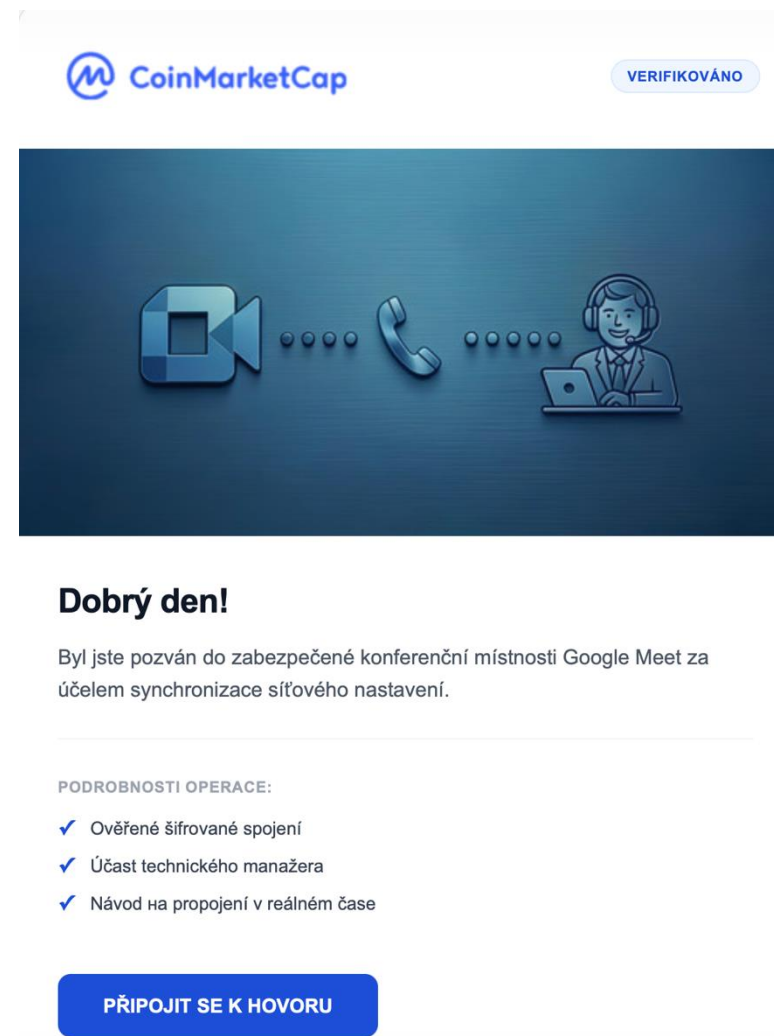
1. **Kontakt:** CZ číslo
2. **Jazyk:** CZ
3. **Strategie:** mentor
4. **Taktika:** jemná manipulace do crypto wallet
5. **Replika:** nadšení, že budu mít peníze 😊
6. **Reakce:** dostal jsem odkaz call a na stažení „klíče“ 😊
7. **Reakce2:** dali jsme si Whatsapp call

BREAK2

Dark side:

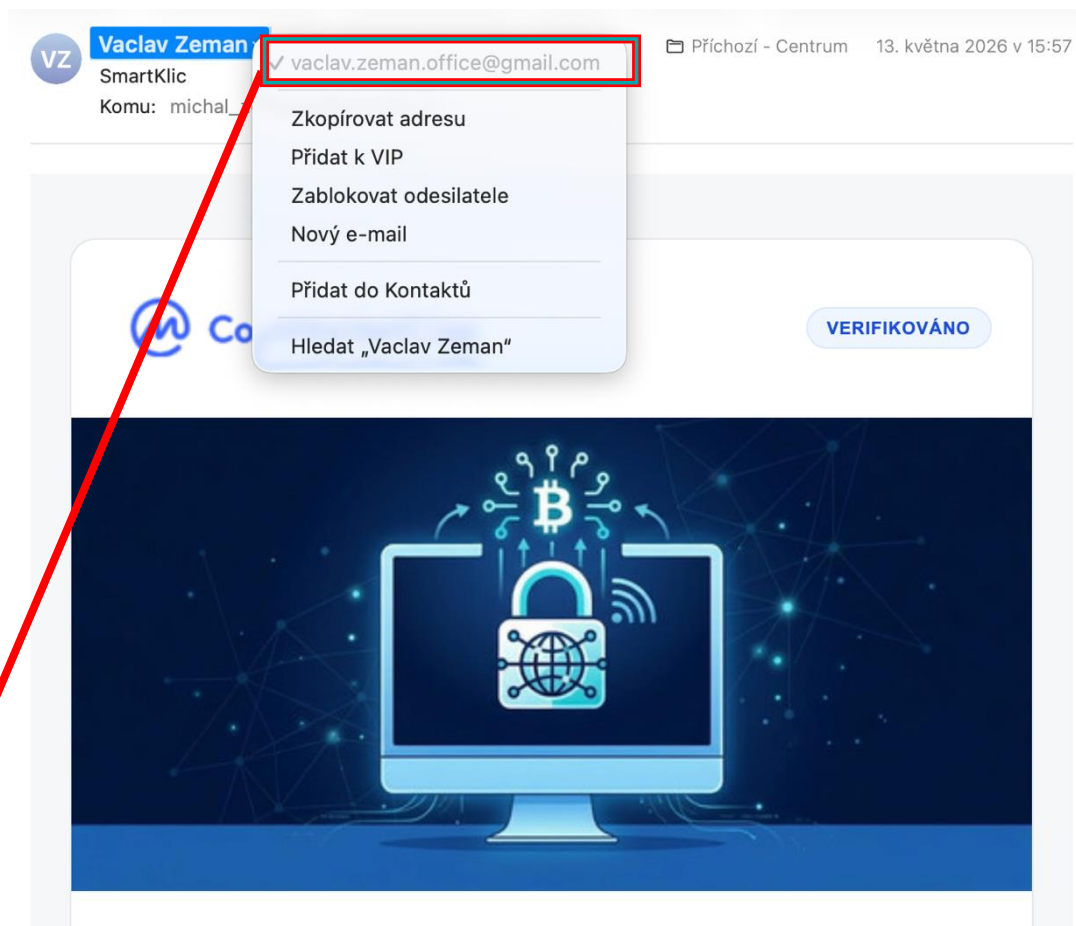


vaclav.zeman.office@gmail.com



BREAK2

Dark side:



vaclav.zeman.office@gmail.com

A promotional banner for CoinMarketCap. The top left features the CoinMarketCap logo. The top right has a 'VERIFIKOVÁNO' (Verified) badge. The main visual is a computer monitor displaying a padlock icon with a Bitcoin symbol above it, set against a dark blue background with network lines. Below the image, the text reads 'Dobrý den!' (Good day!). This is followed by a paragraph: 'Připojujeme smart klíč pro stabilní provoz služeb, bezpečnou synchronizaci a spolehlivou práci.' (We attach a smart key for stable service operation, safe synchronization and reliable work.). Below this is a section titled 'PODROBNOSTI OPERACE:' (OPERATION DETAILS:), followed by a list of four bullet points with checkmarks: 'Stabilní chod sítě a uzlů' (Stable network and node operation), 'Správné směrování a synchronizace dat' (Correct routing and data synchronization), 'Ochrana proti výpadkům a „rozpojení“' (Protection against outages and 'disconnection'), and 'Jednotný standard přístupu pro účastníky' (Uniform access standard for participants). At the bottom right, there is a blue button with the text 'PŘIPOJIT SMART KLIČ' (ATTACH SMART KEY).

BREAK2

Dark side:



BREAK3

Dark side:

SmartKlíč
Oficiální připojení k síti

CoinMarketCap

Jediný klíč k vašemu investičnímu účtu

SmartKlíč je oficiální instalační aplikace pro bezpečné připojení k kryptoměnové infrastruktuře a investičnímu účtu.

Stáhnout teď

Získat nejnovější verzi

- Co to je**
Toto je oficiální klíč, který zajišťuje bezpečnost vašich prostředků na vašem investičním účtu.
- Správa účtu**
Přehled investičního účtu, zůstatků a historie operací.
- Kryptoměny**
Odesílání, výběry a práce s propojenou peněženkou.
- Bezpečnost**
Podpisování operací bezpečně v aplikaci bez sdílení privátních klíčů.

© 2026 SmarkKlíč • Oficiální instalační balíček

BREAK3

Dark side:

EXE souboru „CoinMarketCap.exe“ (určeného pouze pro Windows)

- upravený open-source nástroj RustDesk
- ihned po spuštění spustí powershell script (vyčte z RustDesku přihlašovací údaje a odešle je útočnickovi na jeho vlastní Discord server.
- malware umožní ihned po spuštění útočnickovi ovládat počítač oběti
- komunikace na IP adresy spojované se rodinou malwaru SkulD ((malware založený na volně dostupném projektu na Githubu - <https://github.com/hackirby/skuld/>)

BREAK3

Dark side:

- Steals logins, cookies, history, and download lists from 10 Gecko browsers.
- [clipper](#): Replaces the user's clipboard content with a specified crypto address when copying another address.
- [commonfiles](#): Steals sensitive files from common locations.
- [discodes](#): Captures Discord Two-Factor Authentication (2FA) backup codes.
- [discordinjection](#):
 - Intercepts login, register, and 2FA login requests.
 - Captures backup codes requests.
 - Monitors email/password change requests.
 - Intercepts credit card/PayPal addition requests.
 - Blocks the use of QR codes for login.
 - Prevents requests to view devices.
- [fakerror](#): Trick user into believing the program closed due to an error.
- [games](#): Extracts Epic Games, Uplay, Minecraft (14 launchers) and Riot Games sessions.
- [hideconsole](#): Module to hide the console.
- [startup](#): Ensures the program runs at system startup.
- [system](#): Gathers CPU, GPU, RAM, IP, location, saved Wi-Fi networks, and more.
- [tokens](#): Extracts tokens from 4 Discord applications, Chromium-based browsers, and Gecko browsers.
- [uacbypass](#): Grants privileges to steal user data from others users.
- [wallets](#): Steals data from 10 local wallets and 55 wallet extensions.
- [walletsinjection](#): Captures mnemonic phrases and passwords from 2 crypto wallets.

TELEFONÁTY 7 – (T0 + dosud)

1. **Kontakt:** všechna možná EU čísla vč. CZ
2. **Jazyk:** nejvíce SK, sekundárně CZ, UK
3. **Strategie:** mentor nebo vyhrožování
4. **Taktika:** všechno možné, vč. vyhrožování Policií
5. **Replika:** všechno možné vč. mňoukání
6. **Reakce:** po důsledném blokování čísel výrazné omezení volání

Závěr



1. **DĚJE SE TO – NIKDY nepřestávejte myslet a BLOKUJTE volající čísla**
2. Když Vám bude chtít někdo dát peníze, **VŽDY to bude TRANSPARENTNÍ cestou a bude to „Někdo“**
3. **MODLETE SE, aby se někdo odpovědný konečně zamyslel, jak je možné, že do mobilní datové a hlasové sítě pouštíme neznámou identitu bez autentizace**

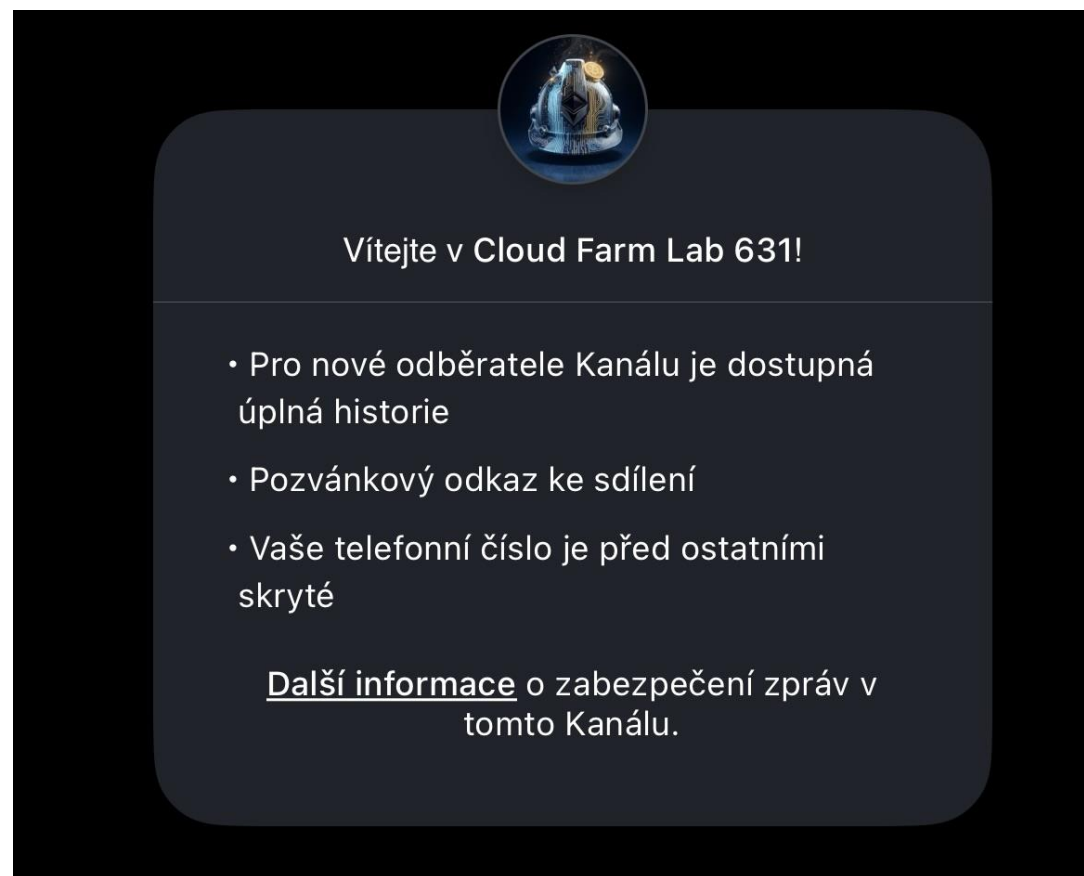
Případ č. 2

AI a SYNDROM VAŘENÉ ŽÁBY



KROK1

Nevím, jak mě dostali, ale stal jsem se členem skupiny „CLOUD FARM LAB 631“ v aplikaci Viber



KROK1

Představení leaderů „CLOUD FARM LAB 631“

a. Emma de Suyrot (správce kanálu)

Ve veřejně dostupných materiálech Binance je uváděna jako graphic designer v rámci programu Binance Accelerator Program (BAP), což je program pro mladé talenty a absolventy.

Odkazy:

BINANCE:

<https://www.binance.com/en/blog/all/6771140985933048651>

LINKEDIN:

<https://www.linkedin.com/in/emmadesuyrot/>

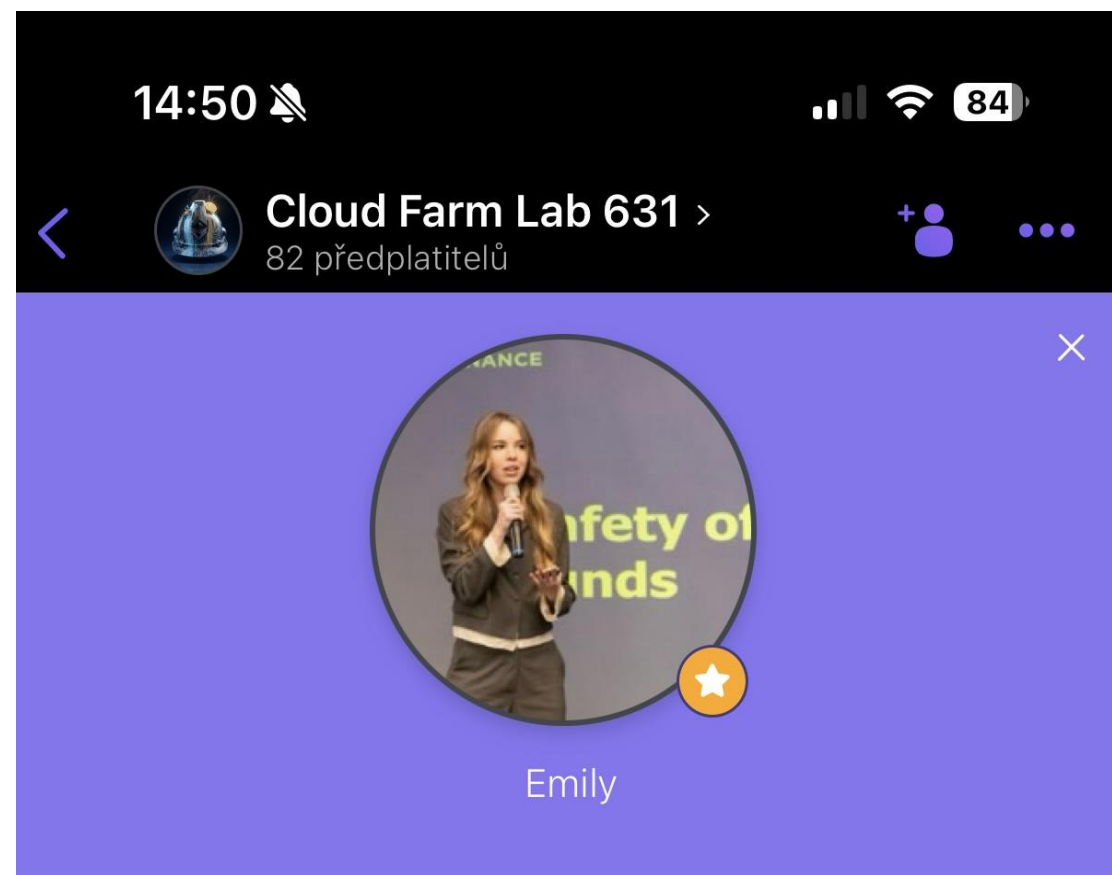


KROK1

Představení leaderů „CLOUD FARM LAB 631“

b. Emily (členka týmu pro propagaci)

Super věrohodnost, že? 😊



KROK1

Představení leaderů „CLOUD FARM LAB 631“

c. „Profesor“ Joshua Eaton (analytik Binance)

Skutečně existuje, pracoval v
Binance, ovšem jako Advisor

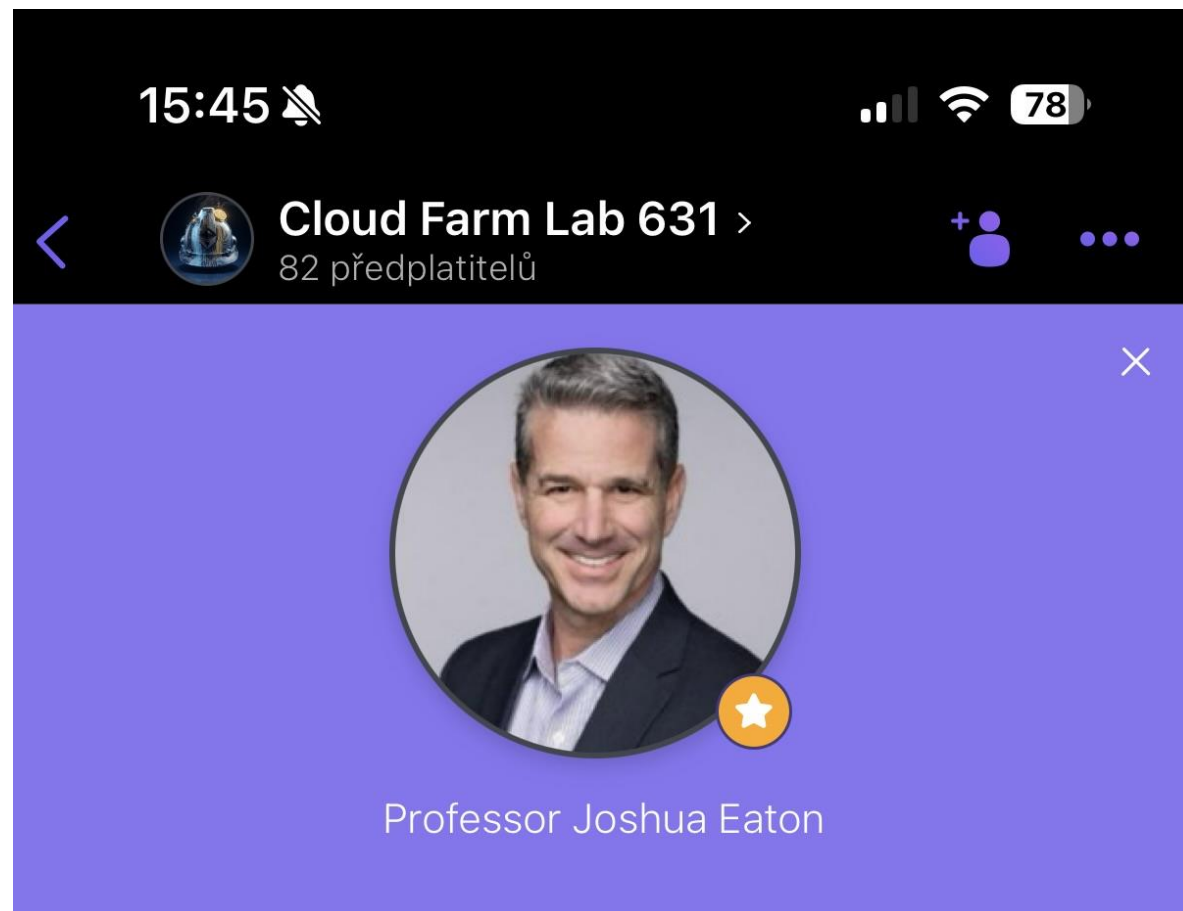
Odkazy:

BINANCE:

<https://www.binance.com/en/blog/leadership/421499824684903840>

LINKEDIN:

https://www.linkedin.com/in/joshua-b-eaton?utm_source=share_via&utm_content=profile&utm_medium=member_ios



KROK2

Začaly mi chodit zprávy o výnosnosti projektu „DeFi Farm“ od uživatelů, kteří byli do tohoto projektu zapojeni

82 ČLENOVÉ 😊

Semtam do diskuse zasahovali Emily nebo profesor Joshua Eaton (ten zejména předkládal různé studie podporující výhodnost DEFI Farm)



KROK3

Přestalo mě bavit neustálé pípání zpráv a pokusil jsem se odhlásit.
Zaujala mě zprvu nenápadná lišta



KROK4

1. Skupina získala můj zájem:

- **Ověřil jsem hlavní zúčastněné**
- **Ověřil jsem projekt**
- **Ověřil jsem organizaci**
- **Prohlédl jsem si konverzaci detailněji**

2. Začal jsem studovat taktiku ...

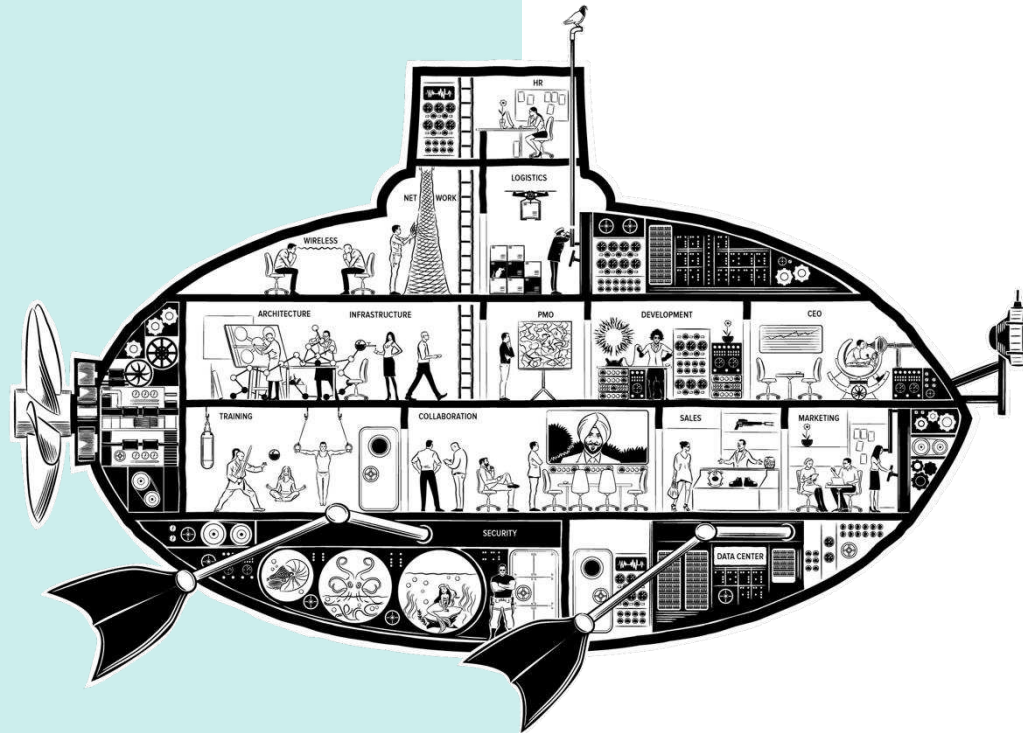
3. ...a vypnul jsem tu fake lištu 😊

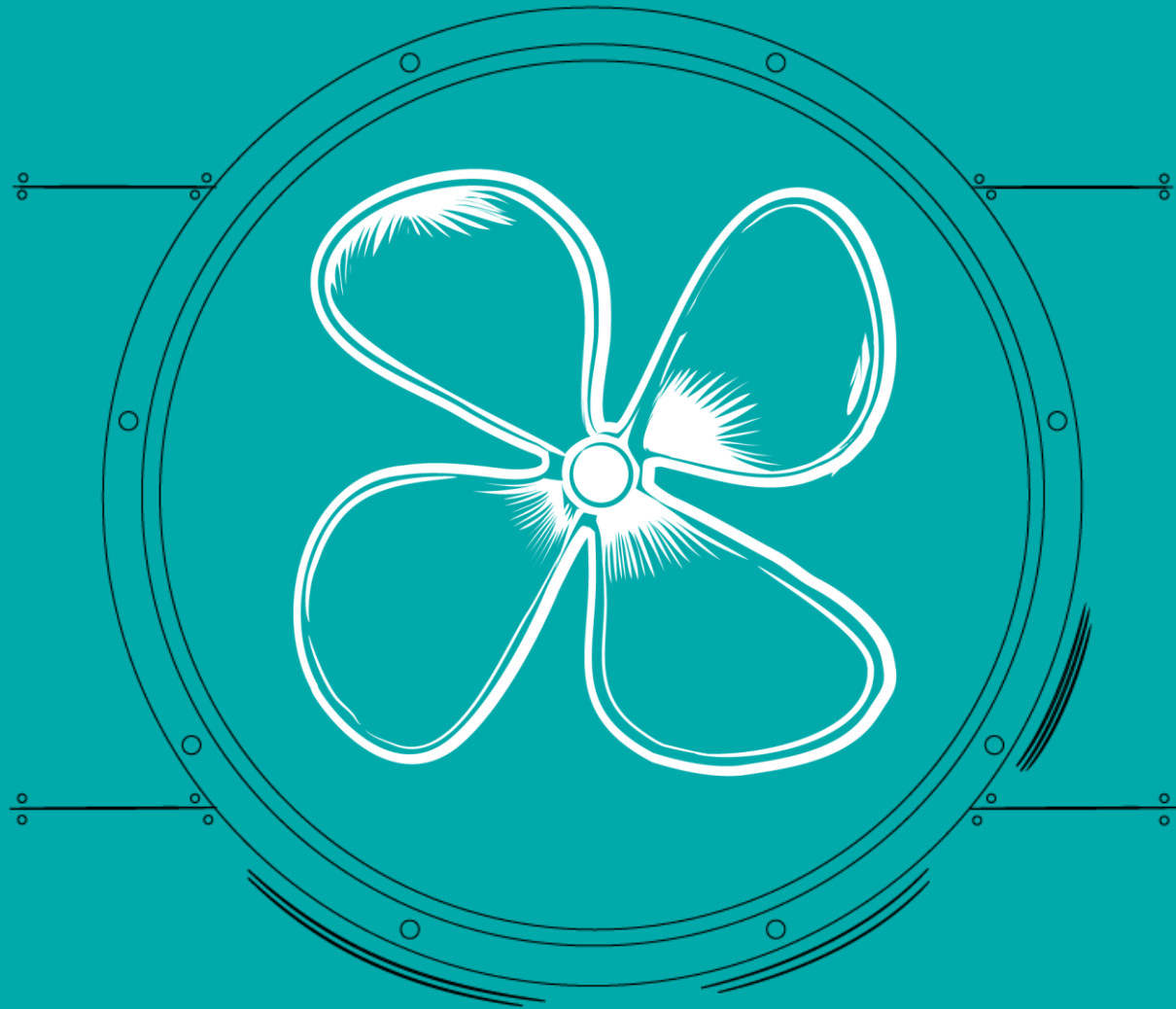
Závěr



1. Velice nenásilná taktika, bez přímého oslovení
2. Když se nehlásíte do Viber, omezí po čase zprávy. Jakmile se přihlásíte, zesílí aktivitu
3. Trpělivost a nepáchání nátlaku, čekají, až se uvaříte a sami požádáte o přístup s dychtivostí
4. Budou Vám ukazovat fake wallet, kde budete bohatí, a dál Vás manipulovat k investicím na posílení fake wallet. Dokud to nebudete chtít vybrat ... 😊

OUR KNOWLEDGE IS YOUR FUTURE





Thank you for your attention!