



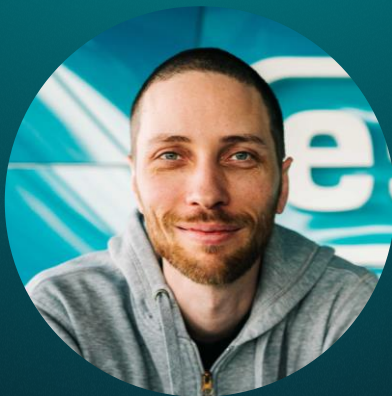
Digital Security  
Progress. Protected.

# Novinky z Labu: Deepfaky, fake captcha a evergreeny

Ondrej Kubovič

ESET Špecialista na digitálnu bezpečnosť

**(eset):research**



## Ondrej Kubovič

ESET Špecialista na digitálnu bezpečnosť

X: @OndrashMachula

BSK: ondrashkubovic.bsky.social

**1 Chaos na infostealer scéně**

**2 Digitální lovci pokladov**

**3 Je to appka, stránka alebo nový útok?**



**4 Investujte ako slávni a bohatí, skončíte s Nomani**

# 1 Chaos na infostealer scéně

2 Digitální lovci pokladov

3 Je to appka, stránka alebo nový útok?

4 Investujte ako slávni a bohatí, skončíte s Nomani

## Redline vs. Lumma



2020



2022

## Redline vs. Lumma



2020

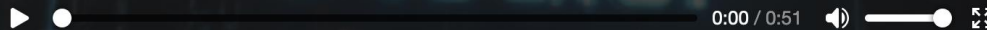
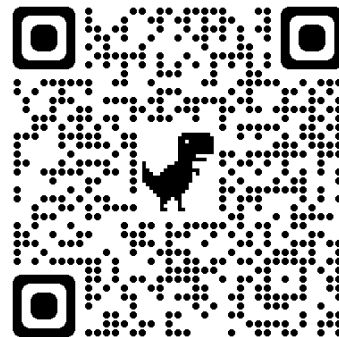


2022

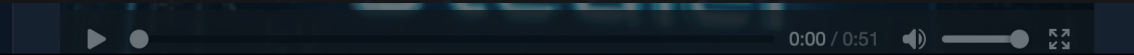
# OPERATION MAGNUS

On the 28th of October 2024 the Dutch National Police, working in close cooperation with the FBI and other partners of the international law enforcement task force *Operation Magnus*, disrupted operation of the Redline and META infostealers.

Involved parties will be notified, and legal actions are underway.



# OPERATION MAGNUS



## ESET RESEARCH

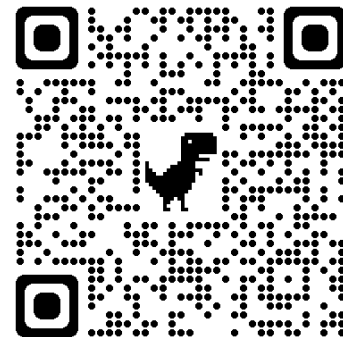
# Life on a crooked RedLine: Analyzing the infamous infostealer's backend

Following the takedown of RedLine Stealer by international authorities, ESET researchers are publicly releasing their research into the infostealer's backend modules

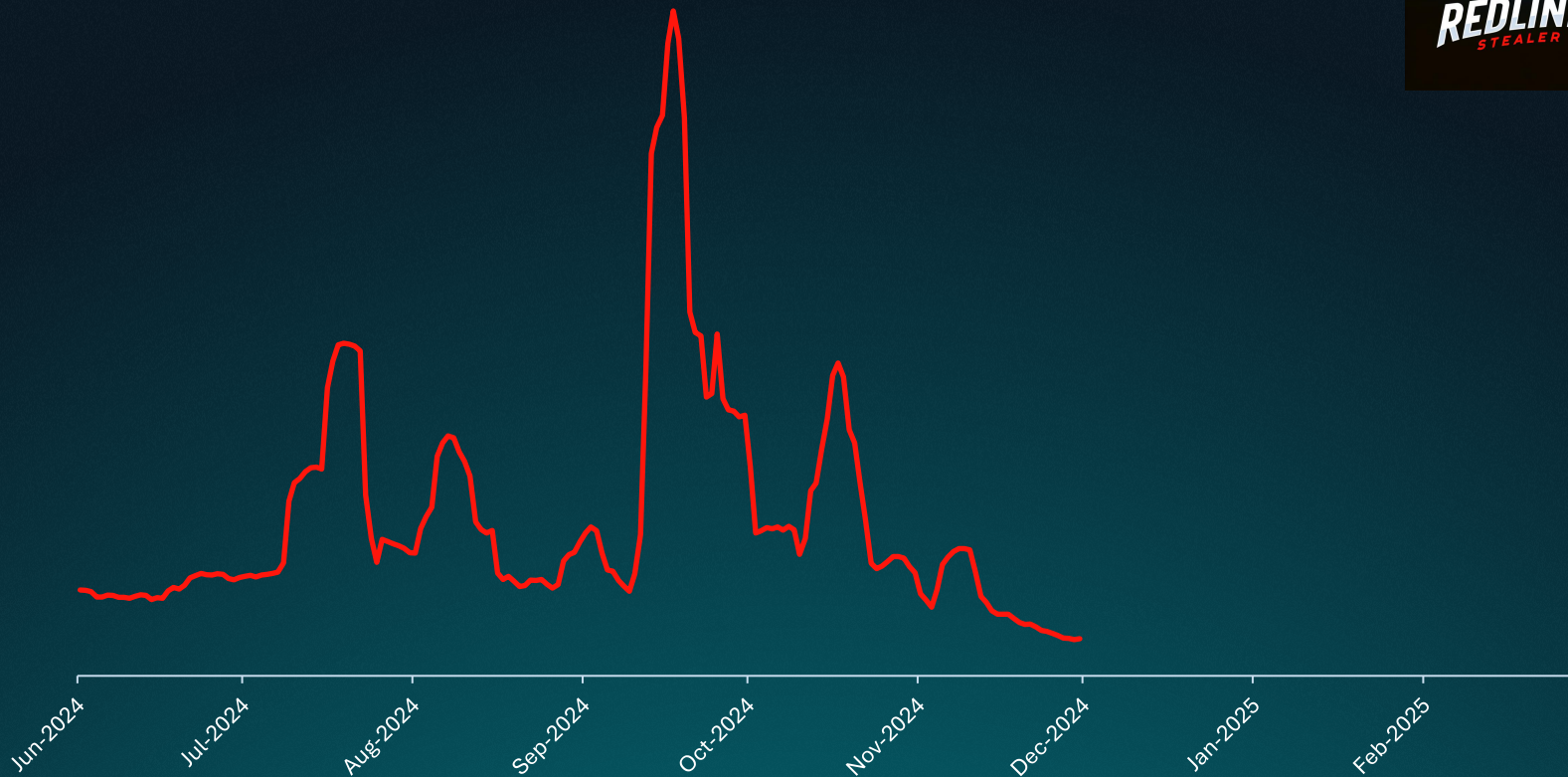


Alexandre Côté Cyr

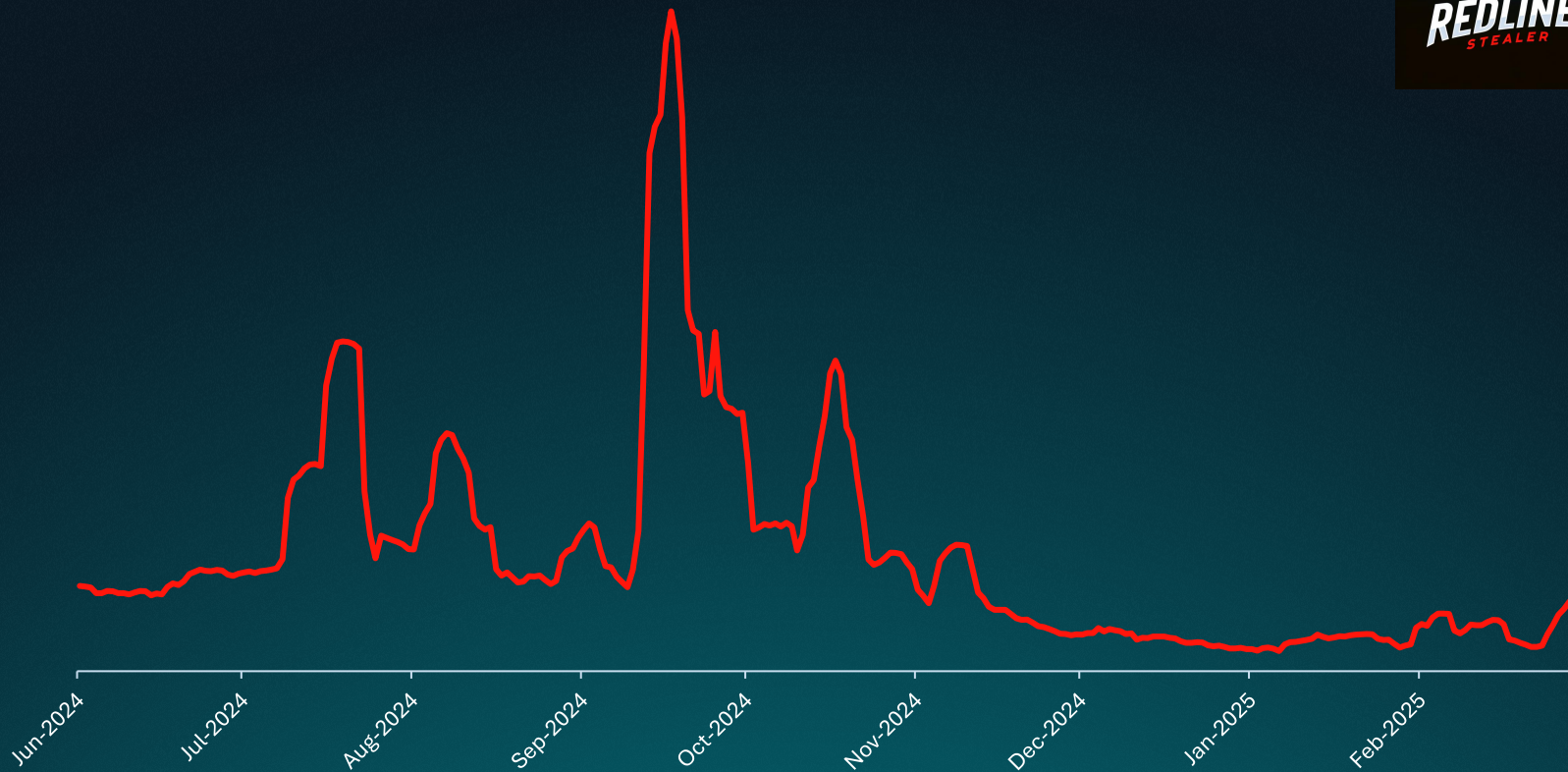
08 Nov 2024 • 24 min. read



# Prežil RedLine zásah polície?



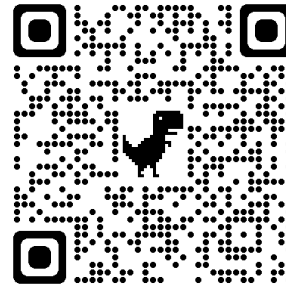
# Prežil RedLine zásah polície?



# ESET Online Scanner for Redline and META

This page is also available in [English](#)

It is important to note that our regular ESET solutions already detect forms these or malware.



## ESET Online Scanner for Redline and META

ONE-TIME SCAN

### System requirements

#### Supported operating systems :

Microsoft Windows 11/10/8.1/8/7

*MacOS, Android and IOS are not supported*

#### Required disk space

350MB (minimum), 400MB (optimum)

#### The Required Memory:

500MB of 50

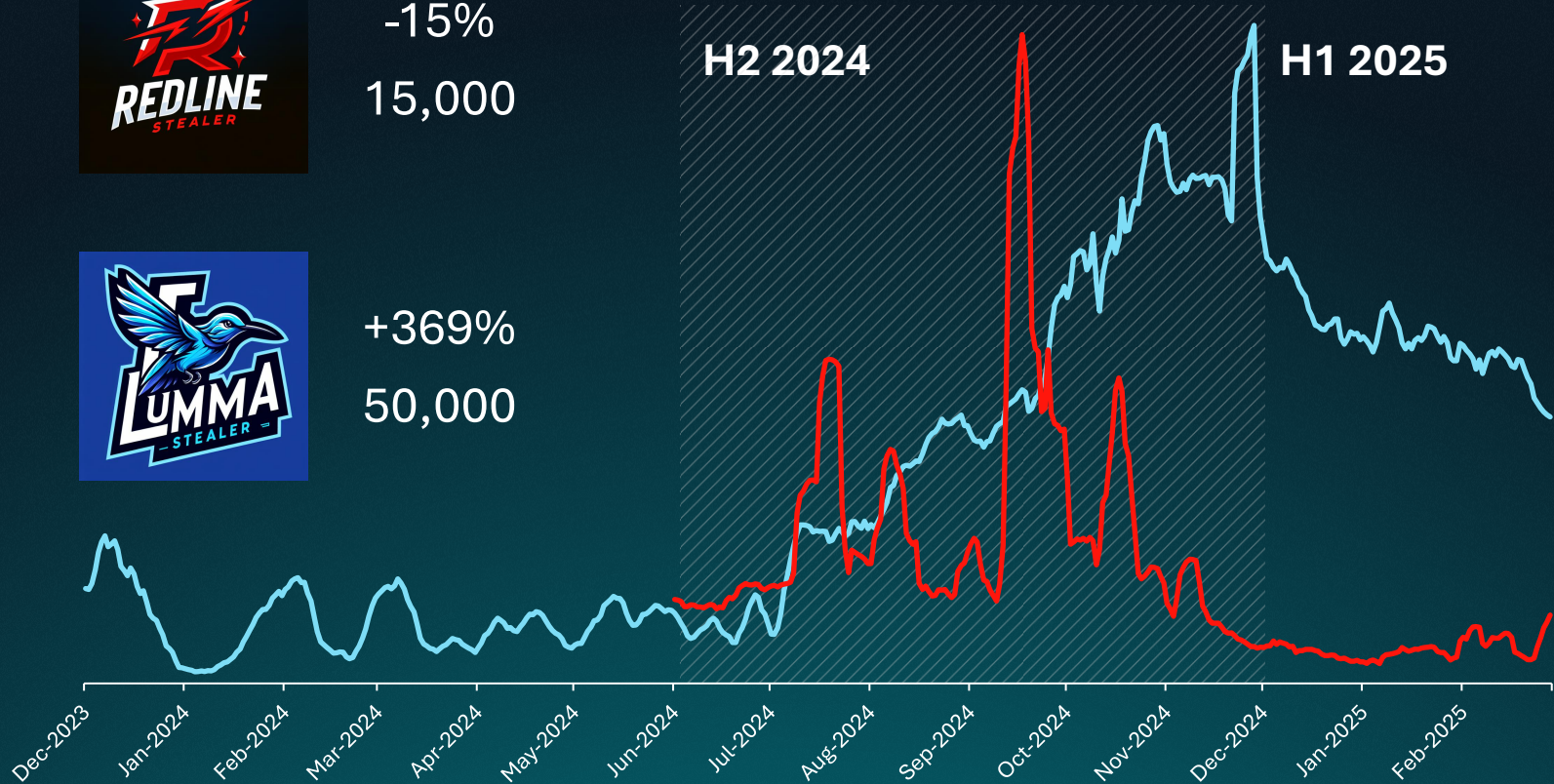
# Redline vs. Lumma (global)



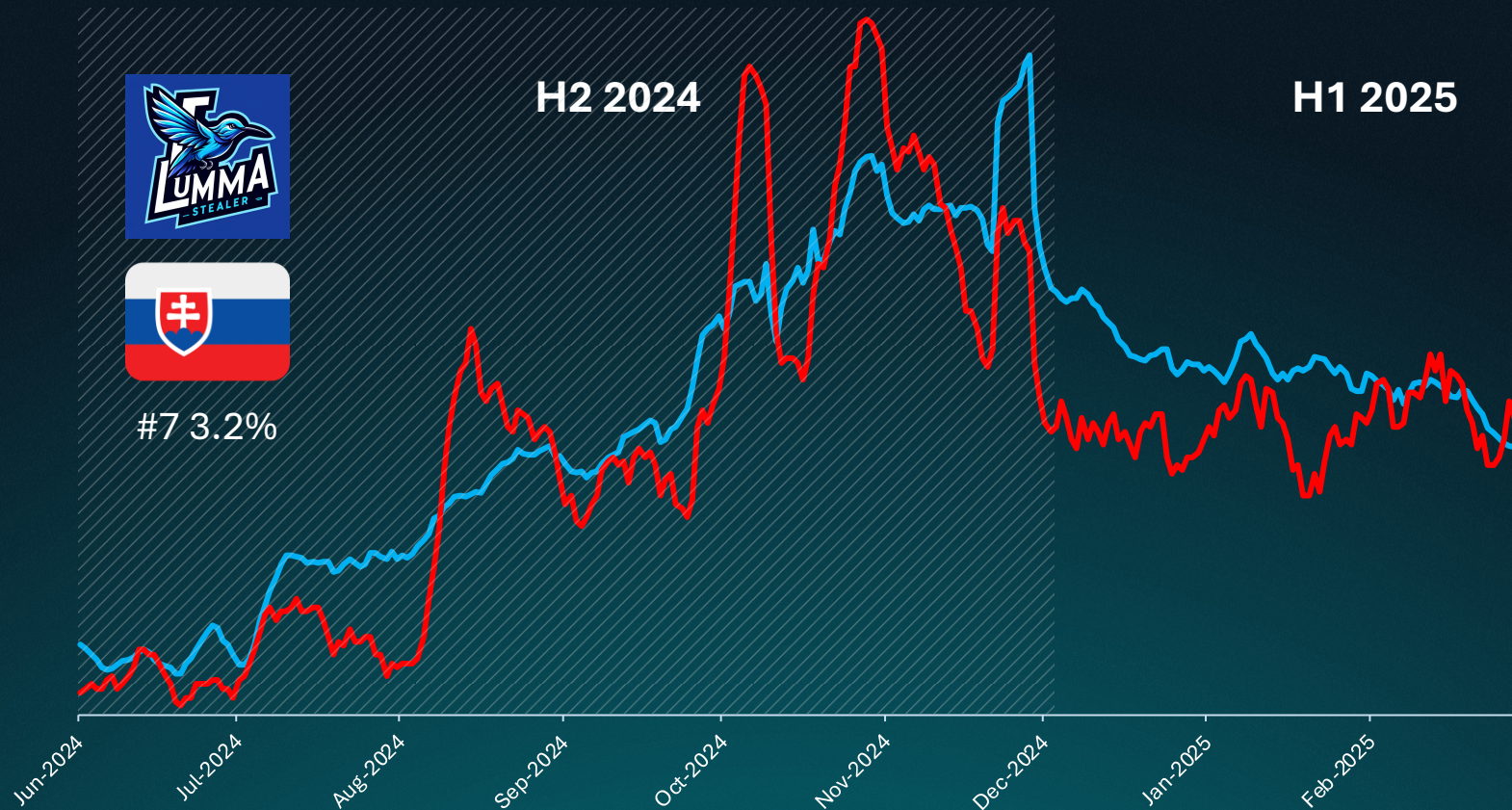
-15%  
15,000

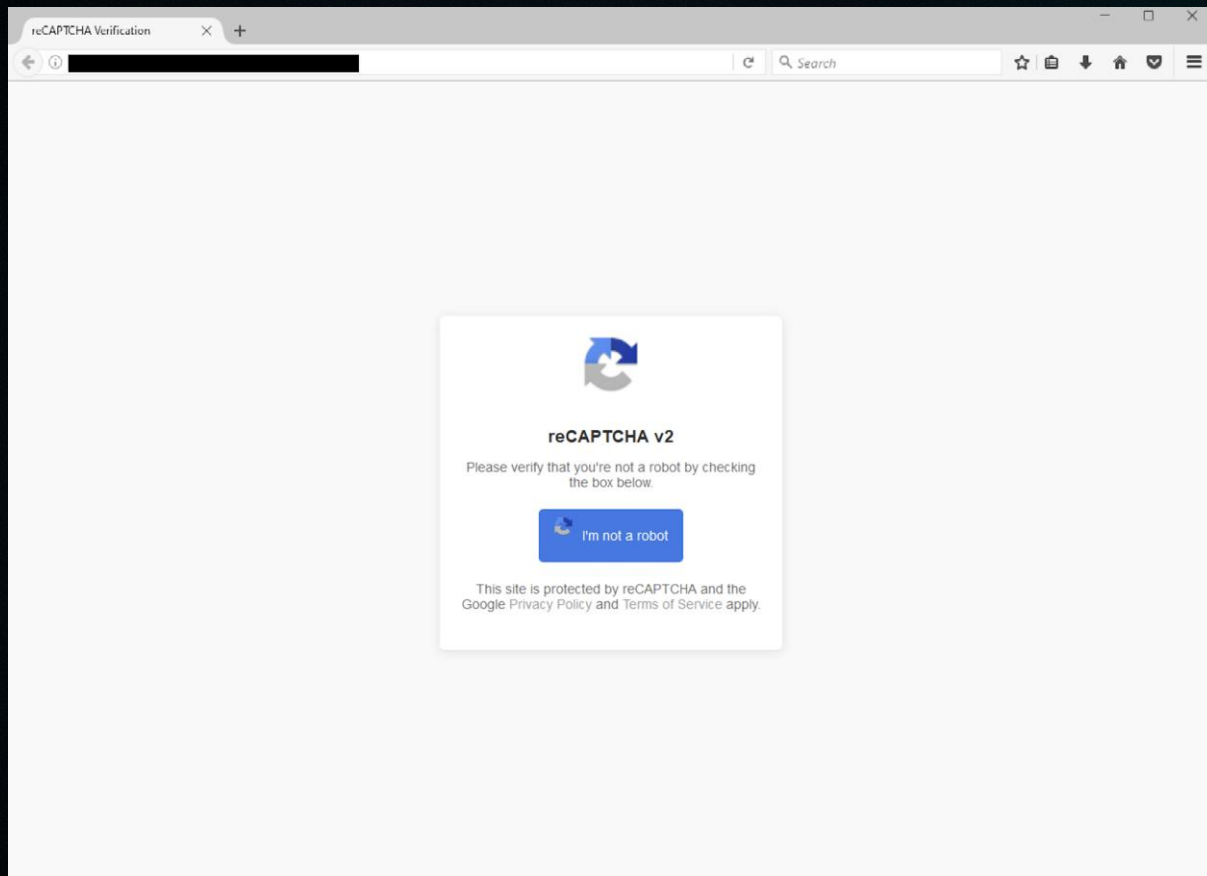


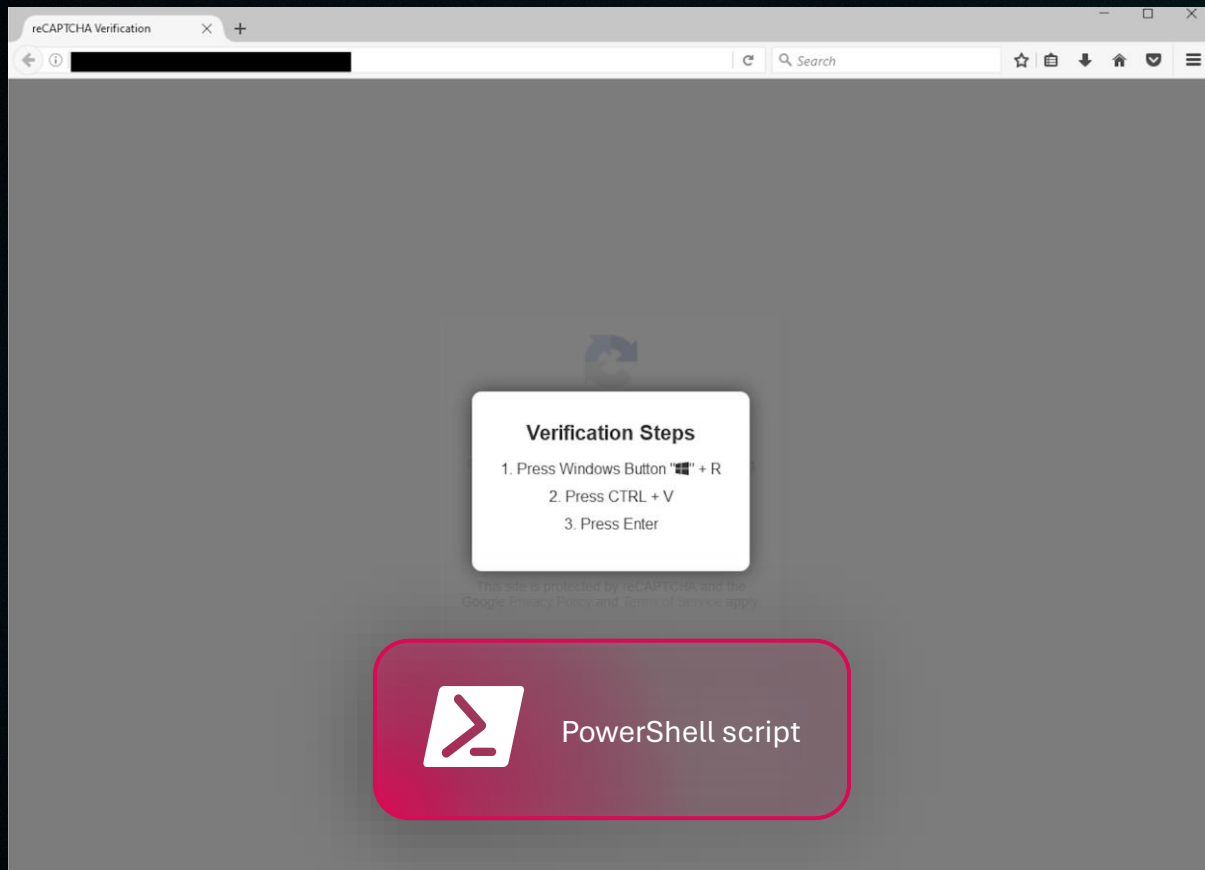
+369%  
50,000



# Lumma (global vs. Slovensko)

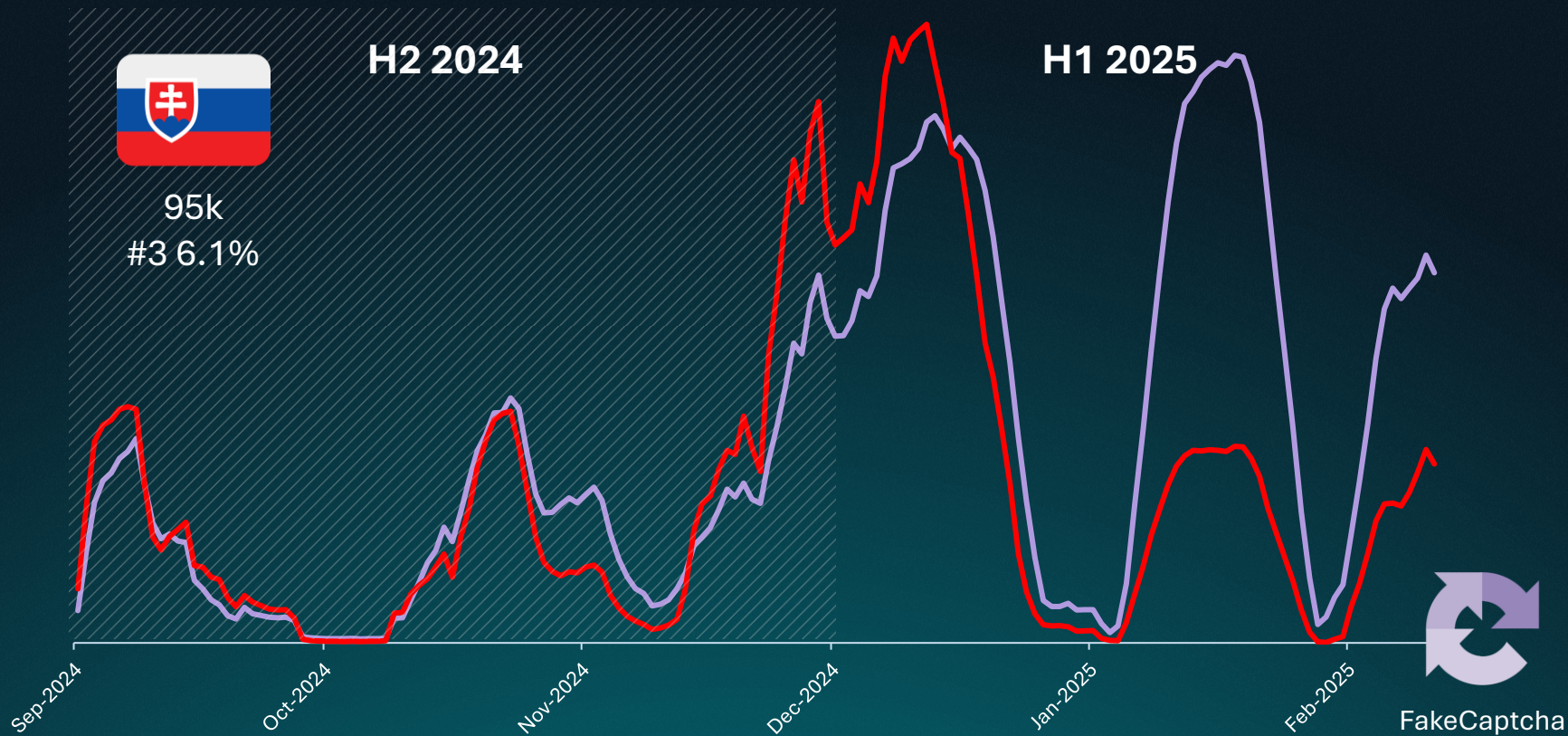








# FakeCaptcha (global vs Slovensko)



# AgentTesla zosadený starým konkurentom



H1 v H2 2024

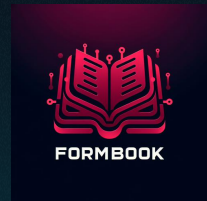
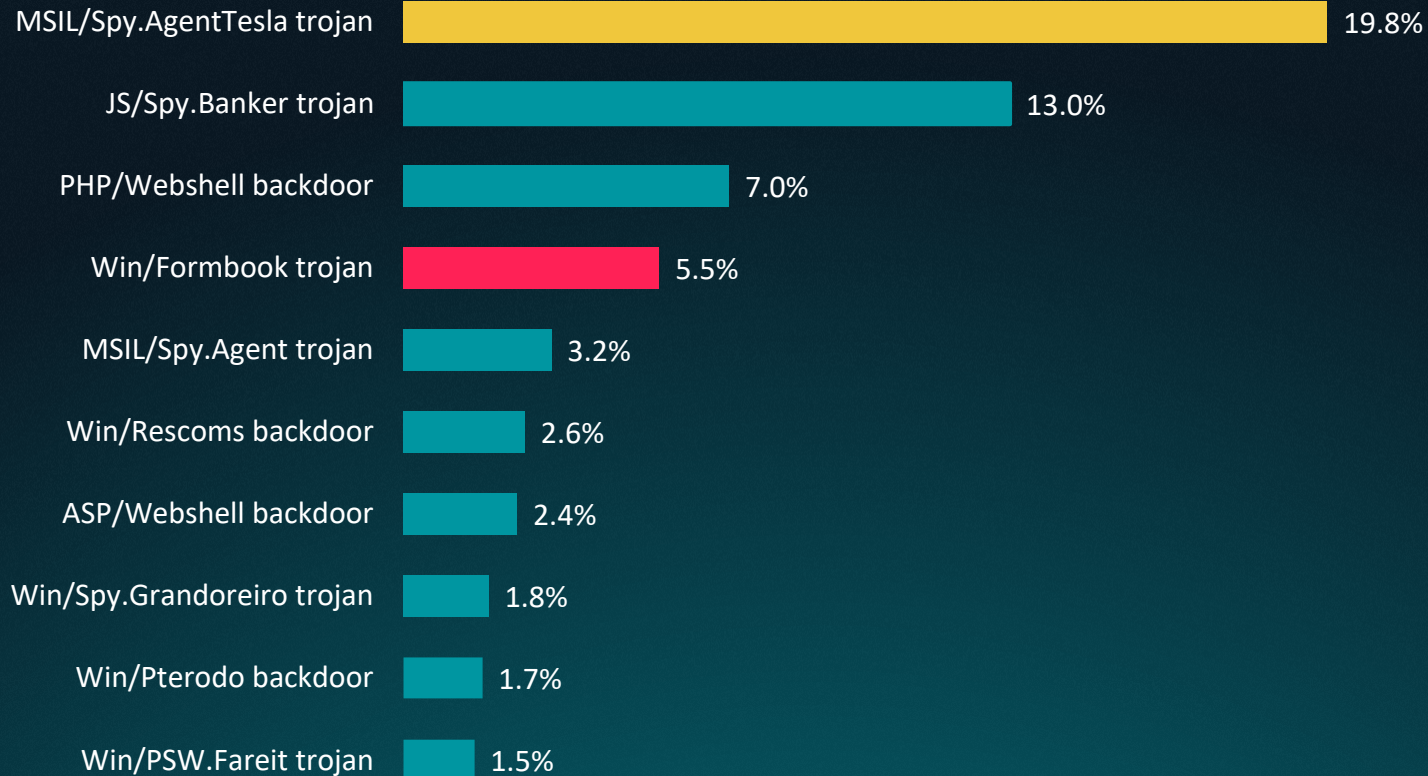
-26%



H1 v H2 2024

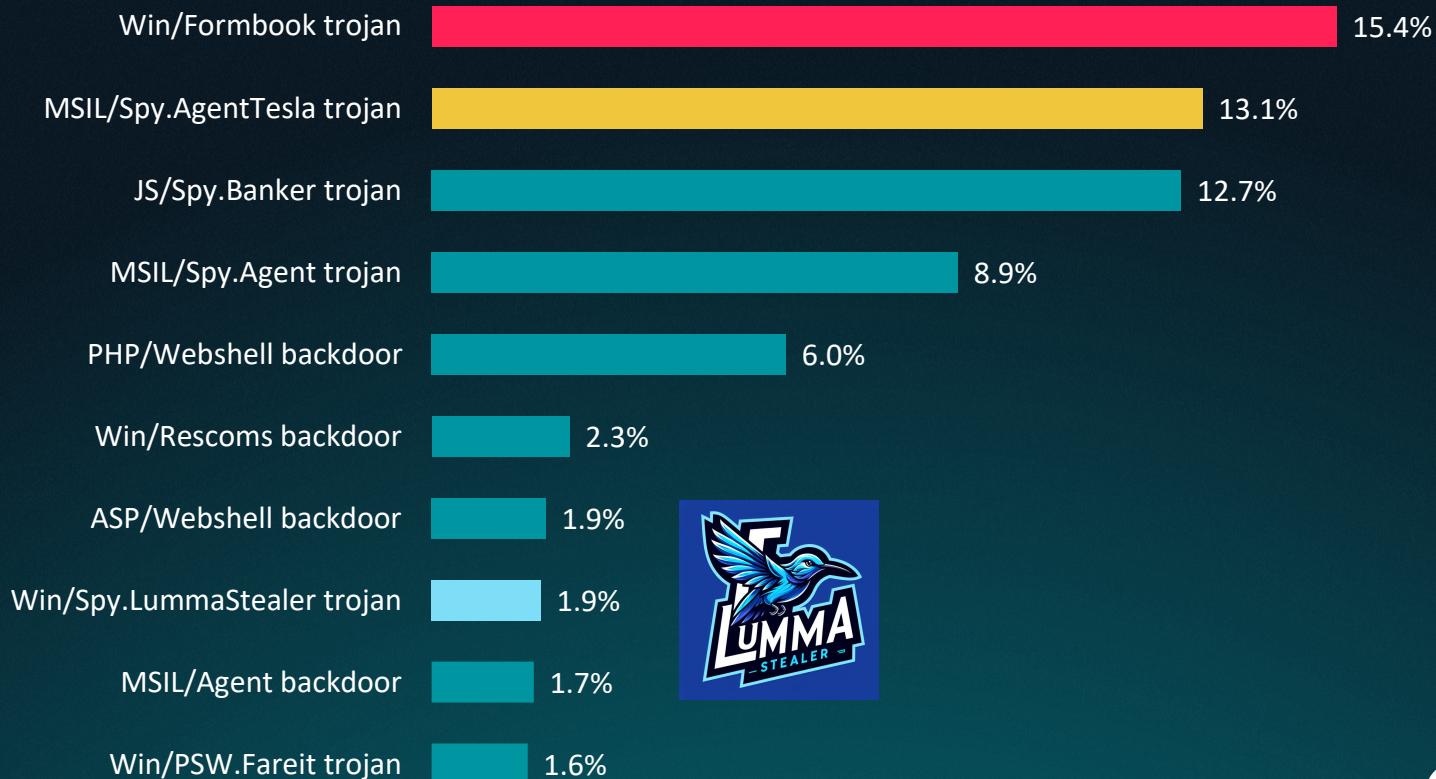
+213%

# AgentTesla zosadený starým konkurentom



H1  
2024

# AgentTesla zosadený starým konkurentom



H2

2024

# Formbook rastie...opäť raz

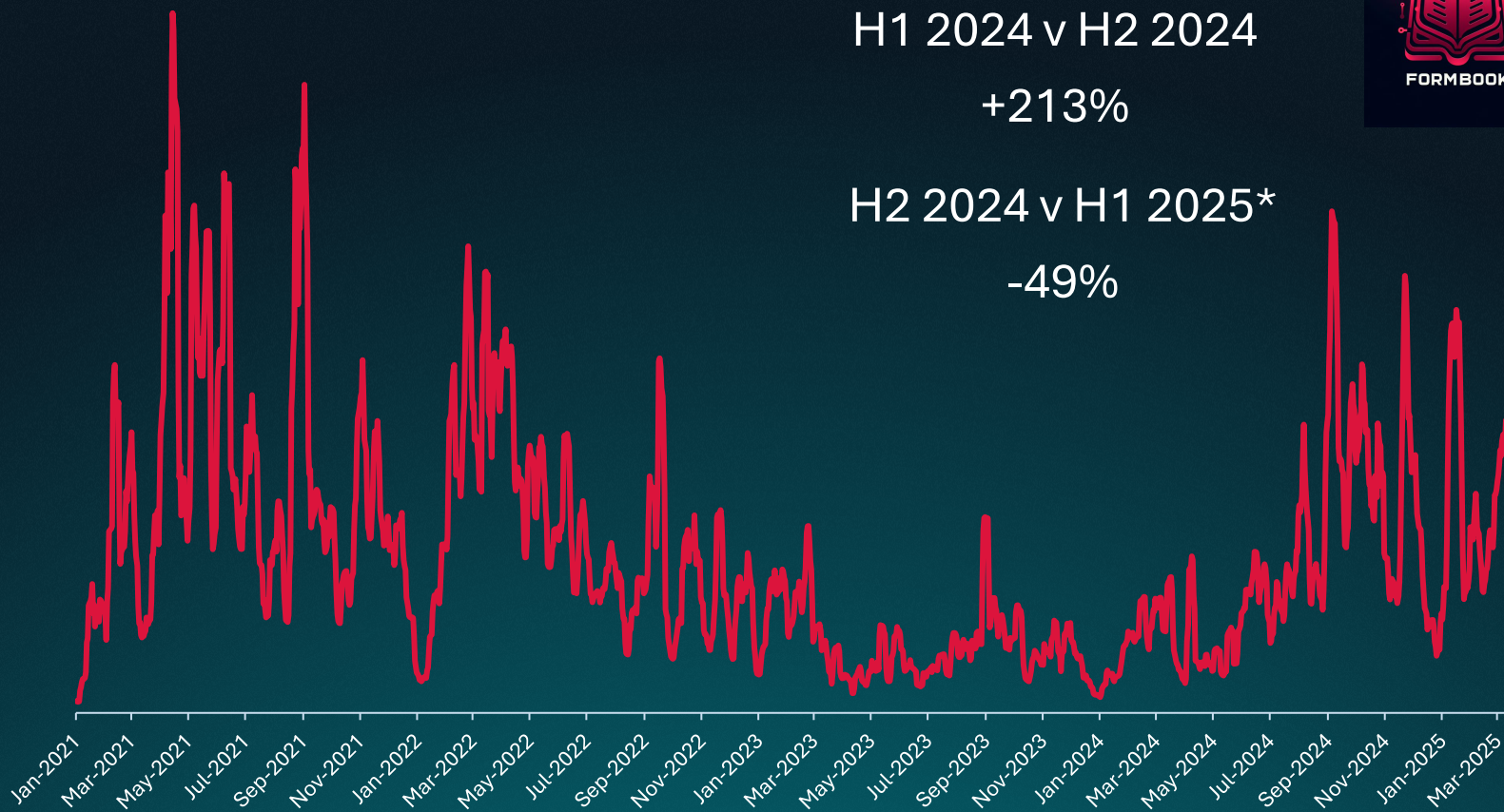


H1 2024 v H2 2024

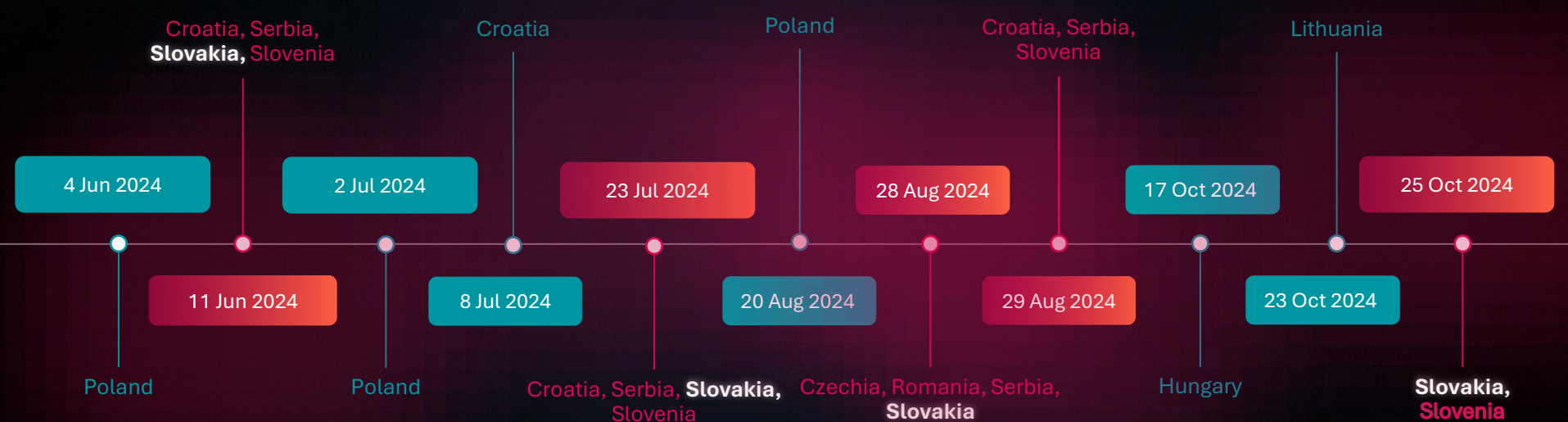
+213%

H2 2024 v H1 2025\*

-49%



# ModiLoader, AceCryptor poštar pre Formbook



# 1 Chaos na infostealer scéně

2 Digitální lovci pokladov

3 Je to appka, stránka alebo nový útok?

4 Investujte ako slávni a bohatí, skončíte s Nomani

1 Chaos na infostealer scéně

## 2 Digitální lovci pokladov

3 Je to appka, stránka alebo nový útok?

4 Investujte ako slávni a bohatí, skončíte s Nomani

# 2024 "made crypto great again"



Kryptostealery všade kam až oko dovidí

macOS



Windows

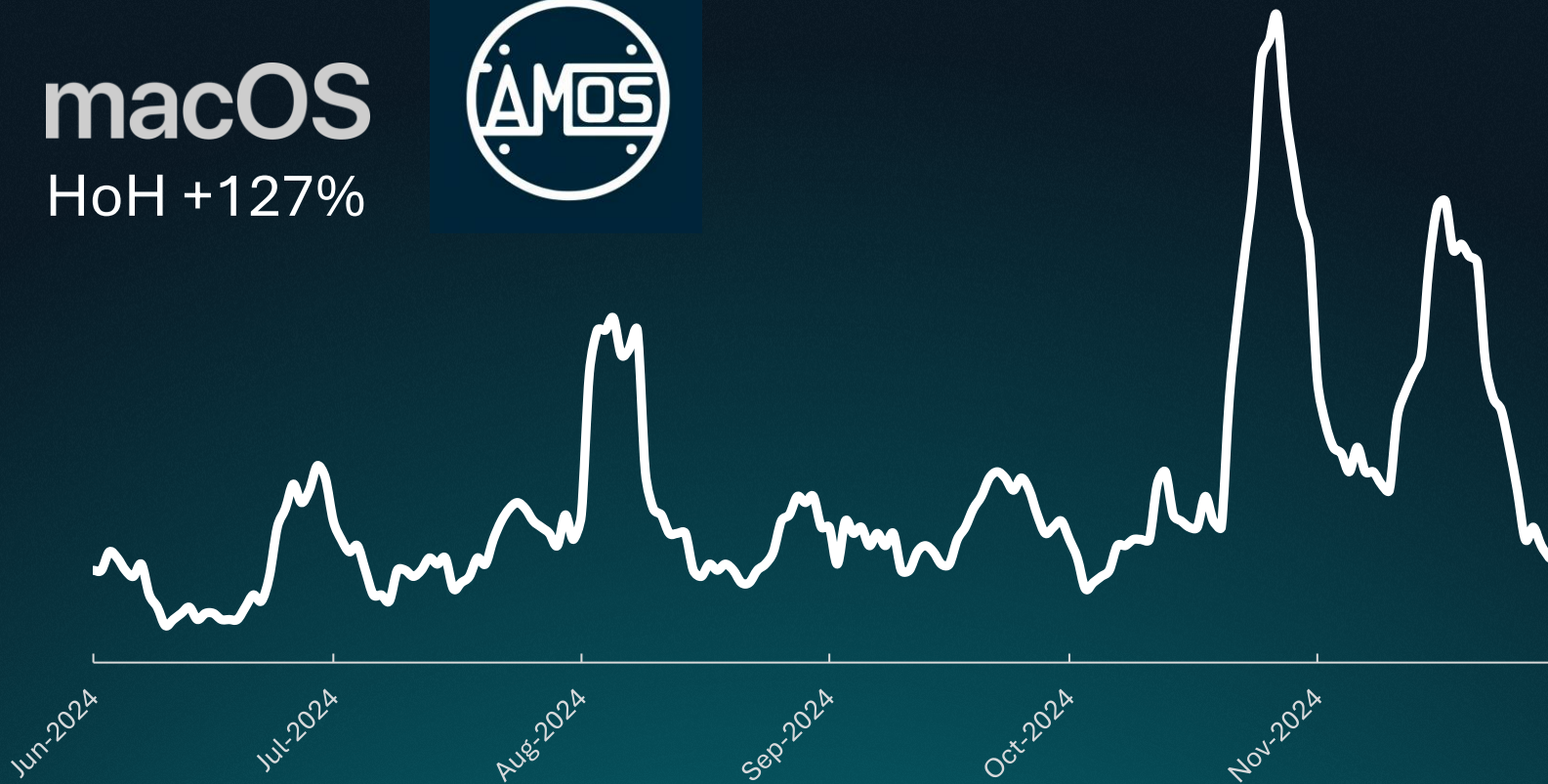
Android



# Dramatický nárůst macOS kryptostealerov

macOS

HoH +127%





April 25

**ATOMIC MACOS STEALER**

SYSTEM:

- Keychain (Export all passwords from apple keychain)
- SystemInfo (Full information about system)
- FileGrabber (Desktop, Documents)
- MacOS Password

BROWSERS:

- Chrome (Autofills, Passwords, Cookies, Wallets, Cards)
- Firefox (Autofills, Cookies)
- Brave (Cookies, Passwords, Autofills, Wallets, Cards)
- Edge (Cookies, Passwords, Autofills, Wallets, Cards)
- Vivaldi (Cookies, Passwords, Autofills, Wallets, Cards)
- Yandex (Cookies, Autofills, Wallets, Cards)
- Opera (Cookies, Passwords, Autofills, Wallets, Cards)
- OperaGX (Cookies, Passwords, Autofills, Wallets, Cards)

WALLETS + PLUGINS:

- Electrum
- Binance
- Exodus
- Atomic
- Coinomi
- Over 60 plug-ins like MetaMask, Phantom and others

FEATURES:

- Web-Panel
- Brute MetaMask (Seed/Private Key)
- Crypto-Checker
- Beautiful dmg-installer
- Logs in telegram (logs + notification)

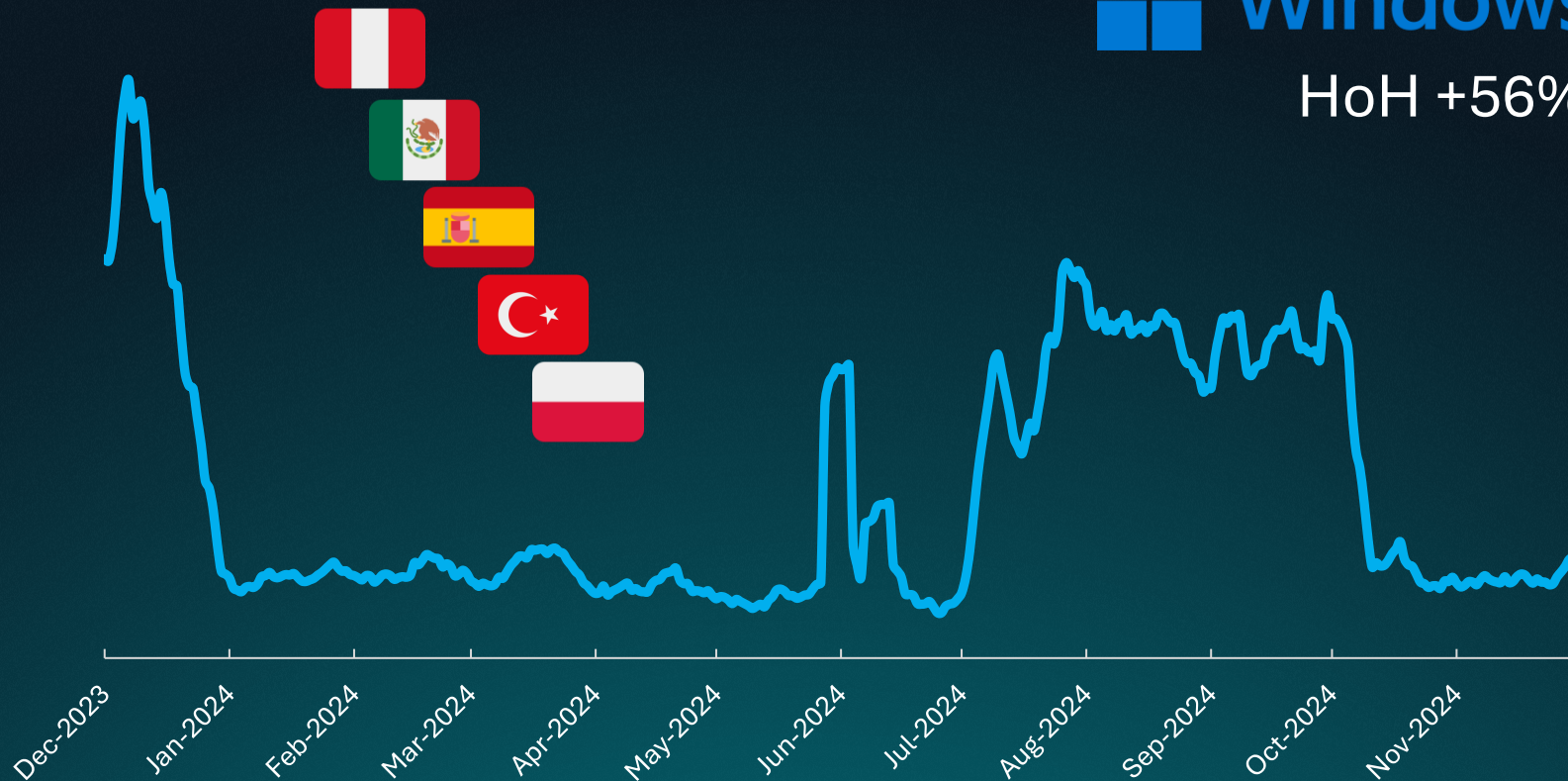
Current price: 1000\$/month



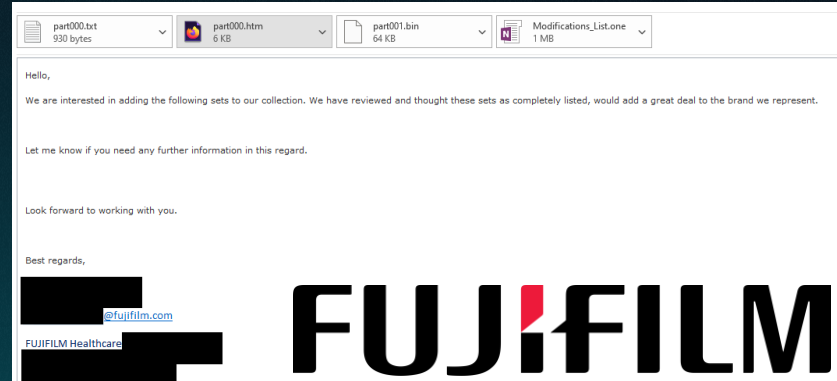


# Kryptostealery pre Windows

 **Windows**  
HoH +56%



# Kryptostealery pre Windows



# Kryptostealery pre Android rásť tiež

## Android

HoH +20%



Jun-2024

Jul-2024

Aug-2024

Sep-2024

Oct-2024

Nov-2024

1 Chaos na infostealer scéně

## 2 Digitální lovci pokladov

3 Je to appka, stránka alebo nový útok?

4 Investujte ako slávni a bohatí, skončíte s Nomani

1 Chaos na infostealer scéně

2 Digitální lovci pokladov

**3 Je to appka, stránka alebo nový útok?**

4 Investujte ako slávni a bohatí, skončíte s Nomani

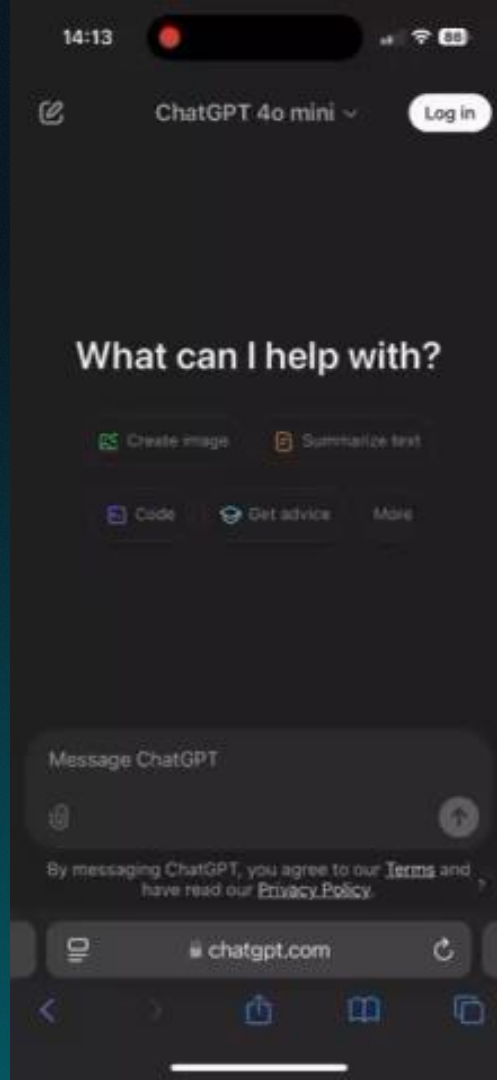


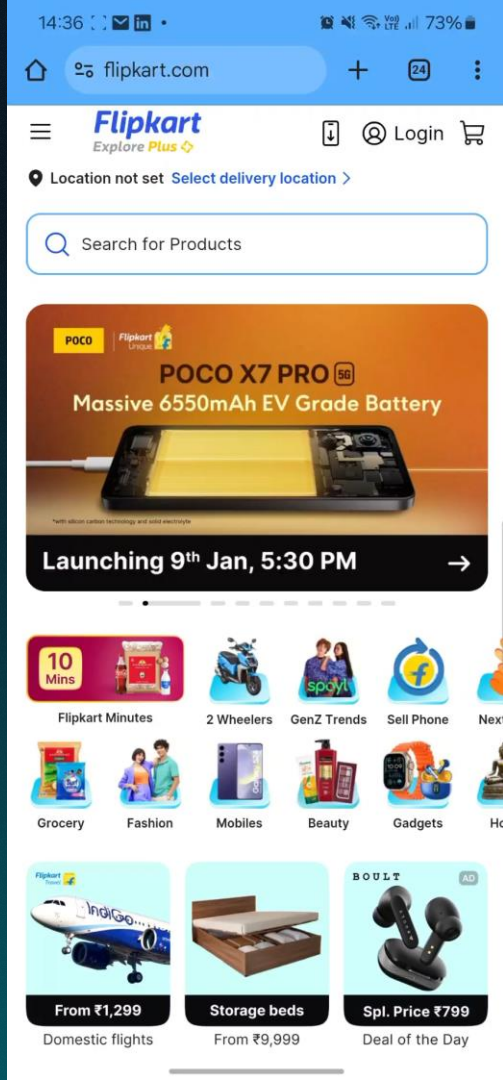
Progressive Web Application



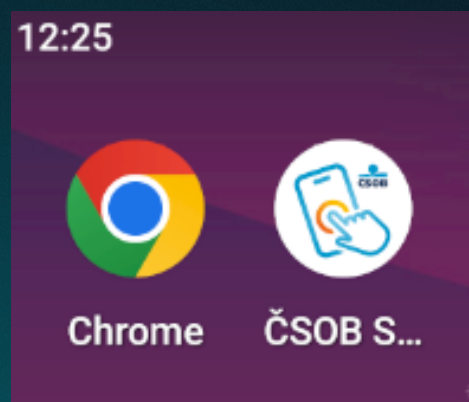
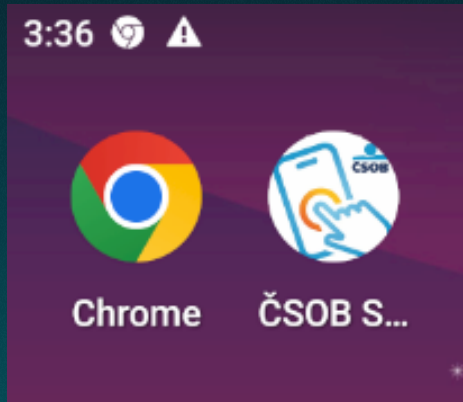
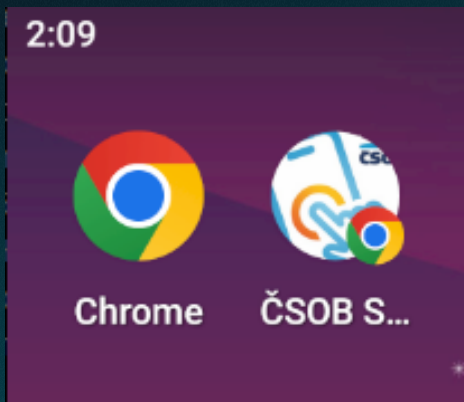
Web Android Package Kit

# PWA

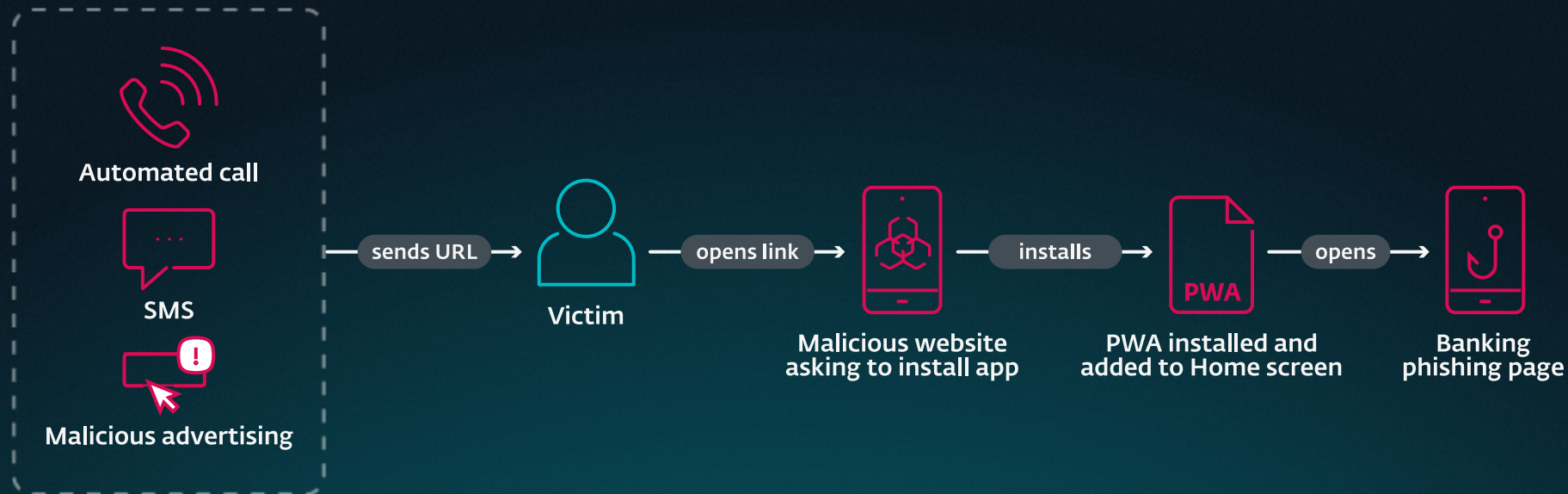




# PWA



# Ako sa šíri táto nová hrozba?



V úterý 12. března od 23:59 aplikace ČSOB Smart bude nedostupná. Pokud ji ještě neprovedete aktualizaci, udělejte to nyní!

Aktualizovat



## Je potřeba aktualizace aplikace ČSOB Smart

Velikost: 32 MB

Verze aplikace je zastaralá a brzy přestane fungovat! Pro pokračování v používání ČSOB Smart doporučujeme nainstalovat nejnovější verzi aplikace.



Aktualizovat



Otevřeno online



Mobilní aplikace a Kate

11:26

george-bank-cz.online

V úterý 21. listopadu od 23:59 budou nedostupné aplikace George a George klíč. Nahradí je naše nová aplikace George ID. Pokud ji ještě nemáte staženou, udělejte to právě teď!



## Je potřeba aktualizace aplikace „George Česko“

Velikost: 46 MB

Verze aplikace je zastaralá a brzy přestane fungovat! Pro pokračování v používání „George“ doporučujeme nainstalovat nejnovější verzi aplikace.



AKTUALIZOVAT

se a autorizovat operace přímo z aplikace George ID.

Zjistěte více

play-secure.pro



Google Play



ČSOB Smart nový

Československá obchodní banka, a.s.

4.8 star  
3 tis. recenzí

100 tis.+  
Stažení

Everyone

Nainstalovat



Informace o aplikaci

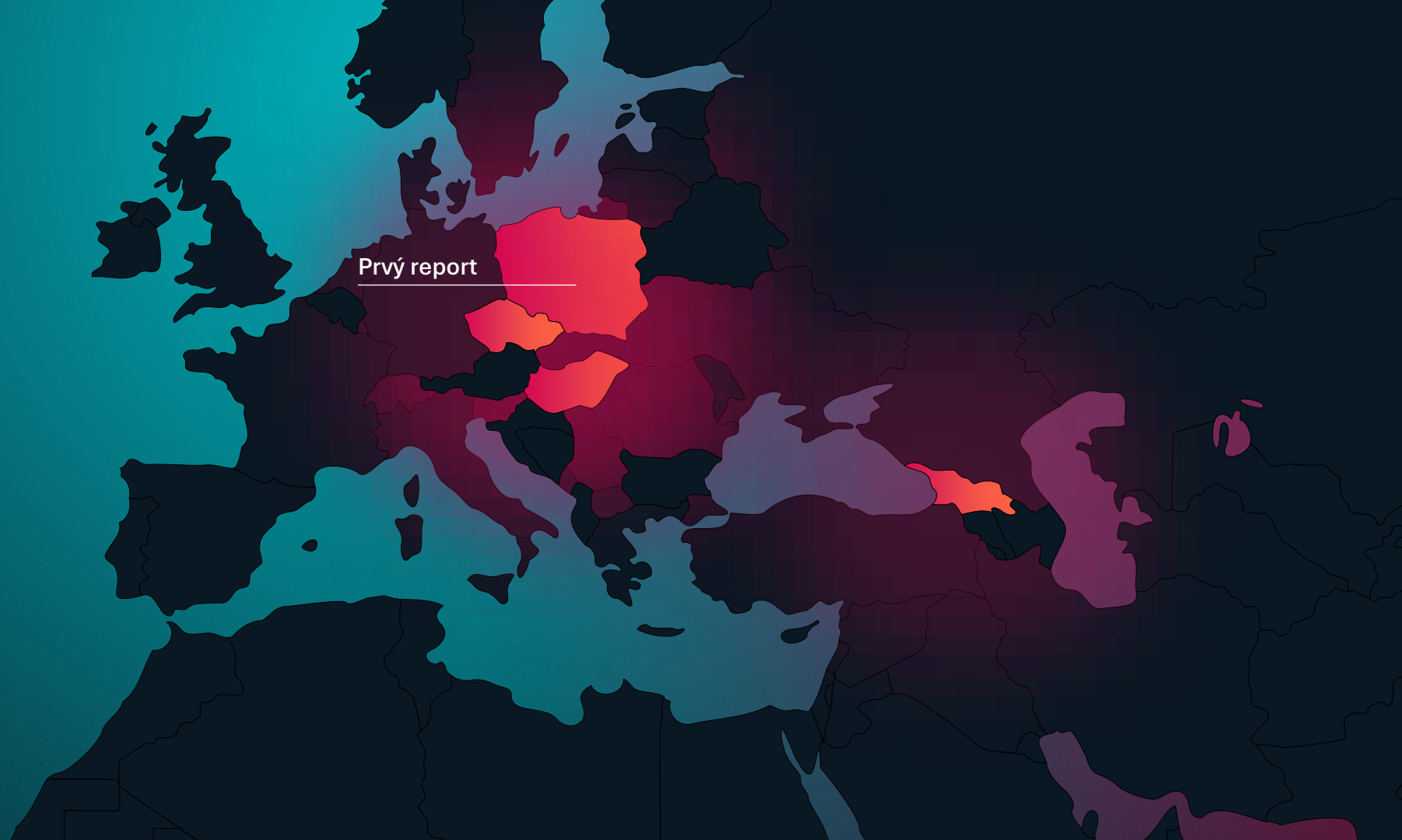
Všechny výhody ČSOB Smart nyní v nové aplikaci "ČSOB Smart nový"

Využívejte první nové funkce a účastněte se nových akcí pouze v aplikaci ČSOB Smart nový!

Pomozte nám otestovat nové funkce aplikace a získejte za to

INTERNAL

Prvý report



1 Chaos na infostealer scéně

2 Digitální lovci pokladov

**3 Je to appka, stránka alebo nový útok?**

4 Investujte ako slávni a bohatí, skončíte s Nomani

1 Data Feeds

2 Digitálni lovci pokladov

3 Je to appka, stránka alebo nový útok?

**4 Investujte ako slávni a bohatí, skončíte s Nomani**

# 1











Profile Name

2d · 

 6

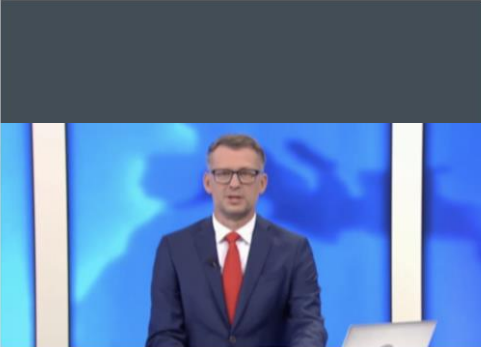




World Report

Sponsored · 

IMG\_0499.MP4



**ALFONZ SURAN**

Finančný program s umelou inteligenciou, ktorý vyvinuli poprední vedci o ekonomickej budúcnosti, je teraz dostupný pre každého. 

SME.SK

Prečítajte si viac

Learn more



Contacts





John Doe



Jane Smith



Mike Johnson



Sarah Lee



David Kim



Emily White



Chris Brown



Alex Green



Olivia Black



Noah Grey



Isabella Blue



Liam Gold



Mia Silver



Benjamin Bronze



Charlotte Iron



Lucas Steel



Aria Copper



Leo Nickel



Sophia Zinc



William Tin



Evelyn Lead



James Silver



Maria Gold



Robert Bronze



Linda Iron



Michael Steel



Anna Copper



Thomas Nickel



Elizabeth Zinc



Christopher Tin

Privacy · Terms · Advertising · Ad Choices · Cookies · More · Meta © 2024



# 1



# 2





# Daňové príjmy obyvateľov Slovenska na základe nariadenia Ladislava Kamenického

Pred 39 minútami

**Andrea Polláková**, digitálna producentka/reportérka  
andrea.pollakova@freemail.sk



Ladislav Kamenický minister financií Slovensko Foto: 123RF

Každý má nárok na platby do výšky 2500 eur mesačne, zdôraznil Minister financií.

V rozhovore s ministrom financií Ladislavom Kamenickým sme sa ho opýtali, ako môže každý, kto žije v Slovensku, získať sociálne dávky.

**Jozef Hübel:** "Ďakujem, že ste prišli, pán Minister financií Ladislav Kamenický. A že všetci občania budú oficiálne dostávať až 2500 eur mesačne. Ako to funguje?"

**Ladislav Kamenický:** "Zdravím. Od prvého dňa, keď som sa stal ministrom financií, som chcel zlepšiť daňový systém. Samozrejme, nezbavíme sa daní úplne, ale všetci obyvatelia budú mať možnosť získať z nich dividendy. Odtiaľ budú peniaze daňových poplatníkov pracovať v prospech našich občanov a každý sa bude môcť sám rozhodnúť, ako ich použije."

**Jozef Hübel:** "Mám tomu rozumieť tak, že ide vlastne o odškodnenie od štátu?"



**Ladislav Kamenický:** "Presne tak. Predpokladali sme platby až do výšky 2500 eur na osobu mesačne. Pre niektorých ľudí to bude malá suma, ale väčšine ľudí to vykompenzuje ich dane a ešte viac."

**Jozef Hübel:** "Odkiaľ štát berie peniaze na takéto odškodnenie?"

**Ladislav Kamenický:** "Keď sa peniaze daňových poplatníkov dostávajú do rozpočtu krajiny, časť z nich sa vynakladá na štátne potreby: platenie sociálnych

**Jozef Hübel:** "Doslova som zarobil 14 eur za 20 minút bez toho, aby som vytiahol telefón z vrecka. Neuveriteľné! Môžete našim divákom povedať, ako môžu zarobiť to isté?".

**Ladislav Kamenický:** "Vážení diváci! Ako vášmu ministrovi financií mi záleží na blahu vás všetkých. Preto ak nás dnes sledujete alebo čítate, zaregistrujte sa v našom projekte [Nearest Edge](#). Stačí, ak zanecháte svoje telefónne číslo a kontaktné údaje, aby vám manažér mohol zavolať späť. A nezabudnite zdvihnúť telefón, pretože miesto v štátnom programe je obmedzené. Potom vám pomôžu s nastavením programu a aby ste mohli začať zarábať, budete musieť vykonať prvý vklad vo výške 250 eur. To vám umožní vďaka daňovej reforme zarobiť až 2500 eur mesačne".

### AKO ZAČAŤ ZARÁBAŤ S NEAREST EDGE:

Navštívte [oficiálnu webovú stránku](#) Nearest Edge a vyplňte registračný formulár.

Počkajte, kým vám zavolá zástupca a pomôže vám nastaviť účet cez telefón.

Doplňte si zostatok ľubovoľnou sumou od 250 EUR.

Výhry si môžete vybrať na ľubovoľnú kartu alebo si ich ponechať na účte a zarobiť ešte viac.

**Dôležité informácie:** podľa ministra financií Ladislava Kamenického zostáva na nástupišti približne 800 miest. Aj keď ste sa ešte nerozhodli, či chcete od vlády dostávať mesačnú kompenzáciu vo výške 2500 eur, dôrazne vám odporúčame vyplniť registračný formulár a rezervovať si účet.

NAVŠTÍVTE OFICIÁLNU  
STRÁNKU

Komentáre

# Nearest Edge

## Odomknite tajomstvá krypto víťazstva pomocou pokročilých investičných techník!

Udržať si náskok v rýchlom svete obchodovania s kryptomenami si vyžaduje hlboké pochopenie sofistikovaných investičných metód. Bohužiaľ, mnohým investorom sa nedarí rozvíjať tieto kľúčové kompetencie. V Nearest Edge vyplníame túto medzeru vo vedomostiach poskytovaním prvotriedneho vzdelávacieho obsahu. Prostredníctvom našej platformy tiež poskytujeme prístup k množstvu vybraných nástrojov tretích strán, čím rozširujeme výskumnú zdatnosť obchodníkov s digitálnymi menami.

### Create an account

 +421 ▼[LEARN MORE](#)

\* By submitting you confirm that you've read and accepted the [privacy policy](#) and [terms of conditions](#).

\*\* By submitting this form, I agree to receive all marketing material by email, SMS and telephone.

\*\*\* All Trading carries risk.



Slovak



1



2



3



# 3

Miestny jazyk

”Dobré rady” na začiatok

Individuálne poradenstvo

Investičná platforma

Stačí “len” 250€

Obrovský zisk rýchlo

Intenzívne telefonáty

Citové vydieranie

Pozor! Žiadajú vzdialený prístup



# 1



# 2



# 3



# 4



# 4

Quantum Bumex  
Bit 9.1 Maxair  
Immediate 0.1 Alrex  
Neoprofit  
Immediate 4.1 Daypro  
Immediate Imovax 400  
Immediate Peak  
Immediate Altex  
Immediate Smarter



# COIN INSIDER

[COIN NEWS](#) [GUIDES](#) [EXCHANGES](#) ▼ [COINS](#) ▼

[Home](#) > [Reviews](#) > [Nearest Edge Review 2024: Is It Legit Or A Scam?](#)

## Nearest Edge Review 2024: Is It Legit Or A Scam?

95%

Coin Insider | Oct 24, 2024



- ✓ Licensed CySec Brokers
- ✓ 24/5 Broker Support
- ✓ Full User Risk Control Tools
- Requires Quick Phone Call To Verify Account

|                                   |       |       |
|-----------------------------------|-------|-------|
| Sign Up Process & Getting Started | 4.9/5 | ★★★★★ |
| Deposits & Withdrawals            | 4.7/5 | ★★★★★ |
| Ways To Trade & Assets            | 4.6/5 | ★★★★★ |
| Security And Regulation           | 4.6/5 | ★★★★★ |
| Customer Support                  | 4.9/5 | ★★★★★ |

### Verdict:

Following comprehensive research conducted for Coin Insider, my findings substantiate Nearest Edge as a credible automated trading solution. The platform demonstrates remarkable utility for market participants across all expertise levels seeking to amplify their trading performance.



Nearest Edge™

### Rating



95%

Excellent  
TESTED & VERIFIED

### Try Nearest Edge

## FREE ACCOUNT MANAGER



IRONSAI

Account ID  
18526046Currency  
EURType  
Real

EN



Trade

1 Hour

Candles

Indicators

Tools

Multiscreen

Cleaning

ACCOR, 1H

Equity  
€0.00Free margin  
€0.00Used margin  
€0.00Open P/L  
€0.00Balance  
€0.00Margin level  
---Credit  
€0.00

Social

Signals



Search

Join

Top ranked

Spotlight

Stream



Name

P/L (%)

Copiers



Avatarsystem225

148%

7



Avatarsystem247

132%

2



FutureRate255

125%

4



Trendyindex238

124%

7



Avatarsystem388

119%

0



VIPTiger872

118%

1

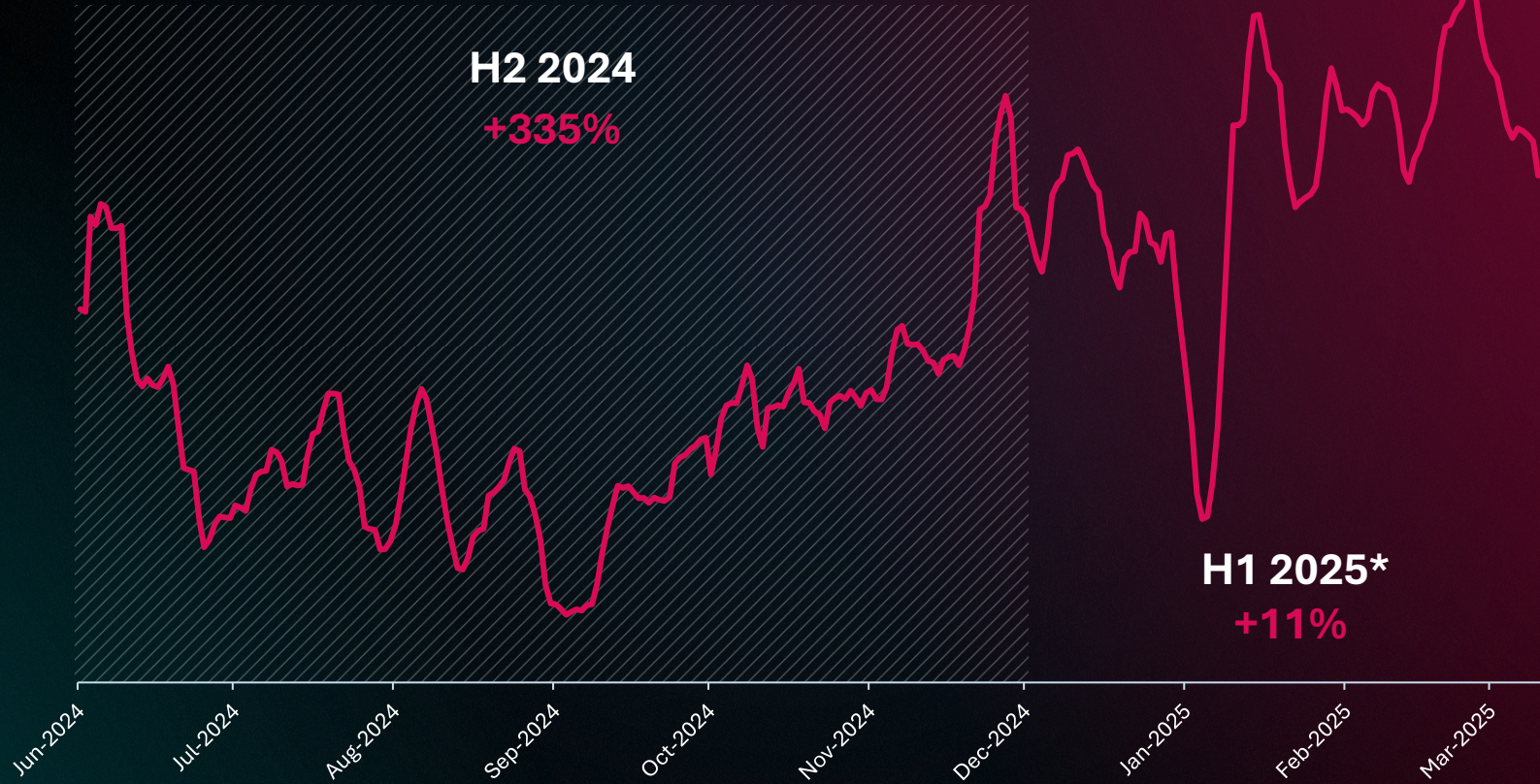


Avatarsystem239

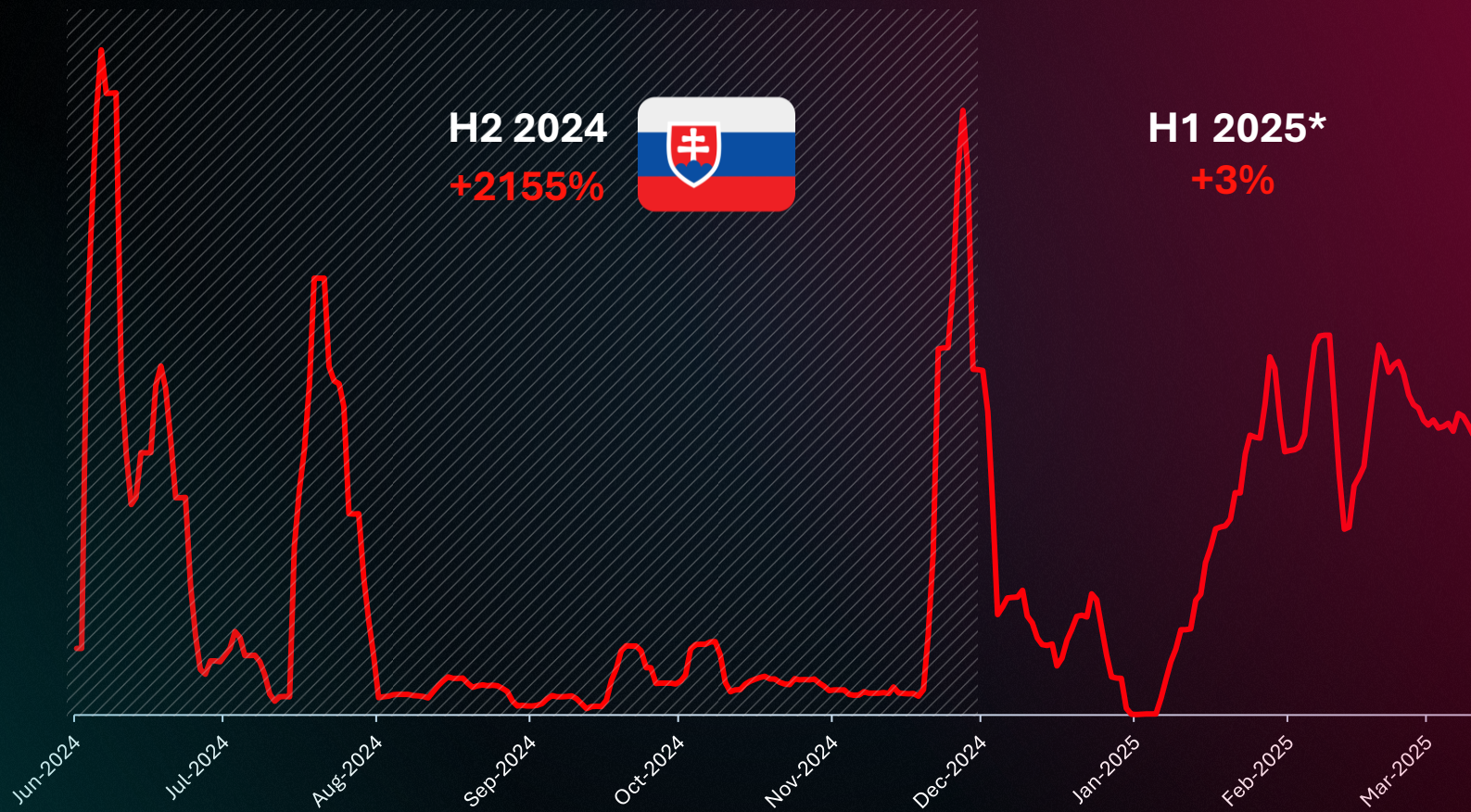
118%

1

# HTML/Nomani detection trend



# HTML/Nomani detection trend



# Čo si všímať?



**Nízka kvalita  
video**



**Zlá audio-video  
synchronizácia**



**Jazyk a prejav sú  
neprirodzené**



**Vzdialený  
prístup**



## Ondrej Kubovič

ESET Špecialista na digitálnu bezpečnosť

X: @OndrashMachula

BSK: ondrashkubovic.bsky.social

[www.eset.com](http://www.eset.com) | [www.welivesecurity.com](http://www.welivesecurity.com) | [@ESETresearch](https://twitter.com/ESETresearch)

# Thank you!

