

Fighting Phishing in Czech Constituency

Martin Kunc • 9. 6. 2025

Our projects



Who we are

- CZ.NIC – .cz domain registry, also operates:
- CSIRT.CZ – National CSIRT
- Martin Kunc – me (Security Analyst)

Story time

- June 2022
- Yet another phishing
- on .cz (unusual!)
- Housing allowance came into place

„Movie characters“ (1)

- mpsv.cz (the official site)
- „Ministry of Labour and Social Affairs“



**MINISTERSTVO PRÁCE
A SOCIÁLNÍCH VĚCÍ**

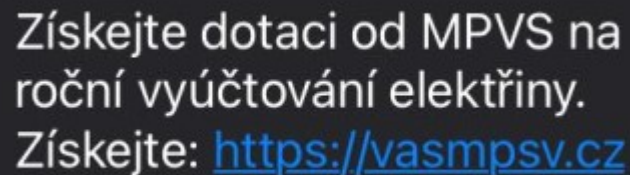
„Movie characters“ 2

- BankID (if only people used our mojID)
- Victims (citizens)
- ... and the bad guys

Bank iD

Scenario

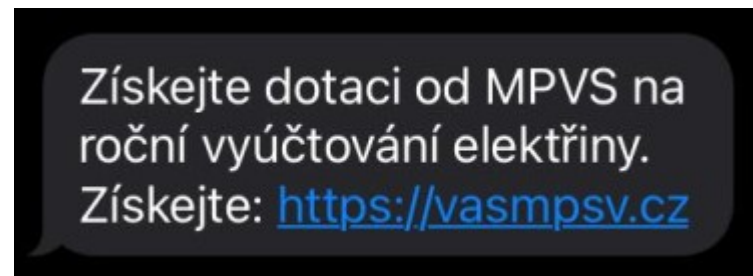
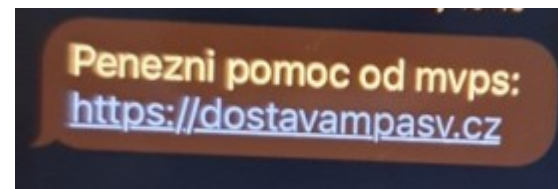
- Victim gets SMS message
- „Get money here: <http://...>“

A screenshot of an SMS message on a dark background. The text is in white and blue. It says: "Získejte dotaci od MPVS na roční vyúčtování elektřiny. Získejte: <https://vasmps.v.cz>".

Získejte dotaci od MPVS na
roční vyúčtování elektřiny.
Získejte: <https://vasmps.v.cz>

Scenario

- Victim gets SMS message
- „Get subsidy here: <http://...>“



Scenario

Příspěvek na služby,
který máte k dispozici
od mpsv: <https://web-mpsiv.cz>

Platba z mpsv je k dispozici
na váš účet. Dostávat:
<https://online-platbympsiv.cz>
SMS 16:53

MPSV informuji
Příspěvky na bydlení
Získat:
<https://aktivovat-idmpsiv.cz>

Dobrý den, dostáváte
dotaci na úhradu elektřiny.
Příjem průkazu: <https://vasmpsiv.cz>

Benefit z mpsv je k dispozici na
vašem účtu: <https://onlines-mpsiv.cz>

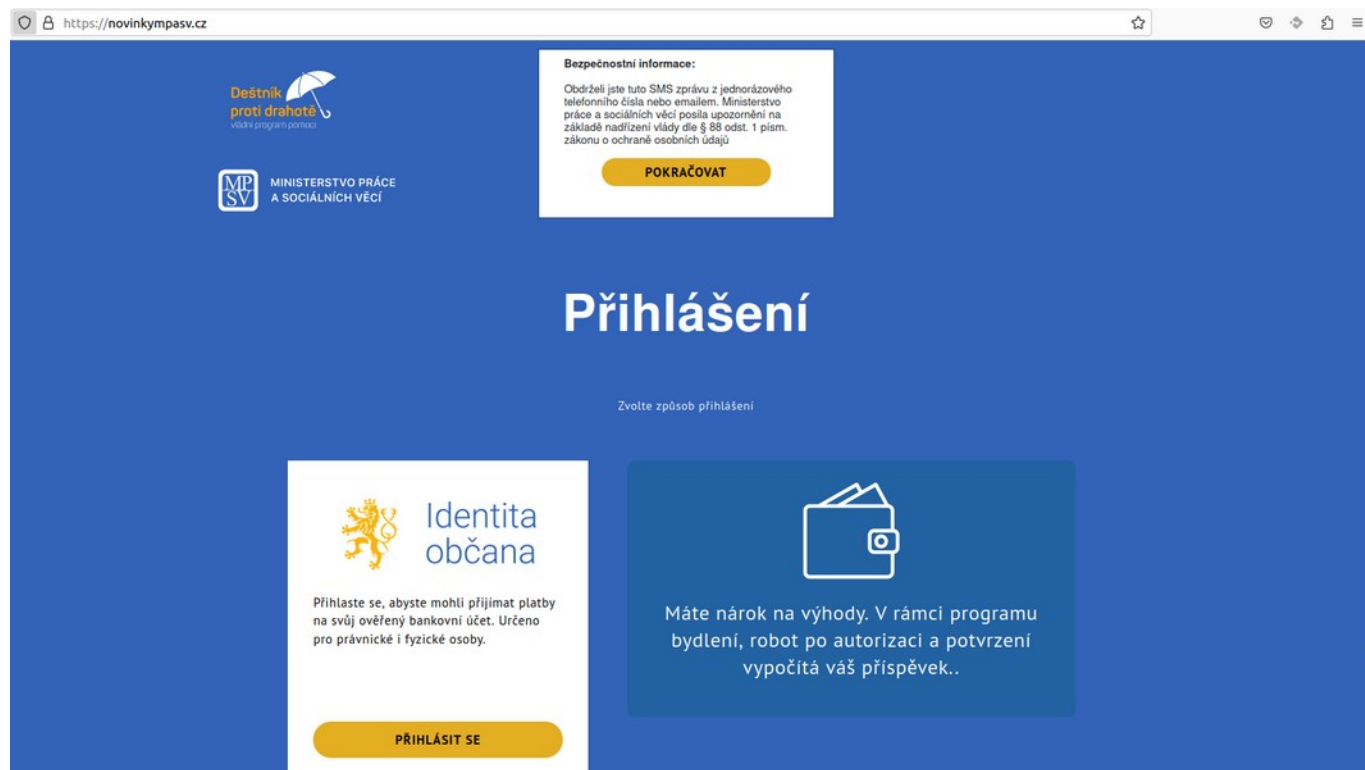
Hotovo. Příspěvek na bydlení
na vašem účtu: <https://24-mpsiv.cz>

Prispevek na bydleni mate k
dispozici: <https://online-platbympsiv.cz>
SMS 17:20

Scenario cont.

- Landing phishing site
- „Please login using BankID“ (only in business hours)
- Attacker uses credentials and 2FA and gets the money

Examples





Bankovní IDentita České spořitelny

Odpovídáme za to, že přihlášení za účelem Vašeho ověření je bezpečné. Třetí strana nemůže získat přístup k Vaším přihlašovacím údajům.



Pokračovat

Nepamatuji si uživatelské jméno

Upping the game

- 2022:
 - ~11 cases/domains per month
- February 2023:
 - 72 domains
 - at that time we were fully after them

They improved what can we do?

- Active searching
- Improve the process
- Study and make notes!

Active searching

- Registry – „regexes“?
 - *mpvs* or *mpsv*
 - *mp-sv* or *mp-sv*
- **** it! „Registration date: „LAST_WEEK“

Improve the process

- Having list of „future“ phishing domains
- Scan those periodically (no-one cared)
- Send notification
 - We were happy to act outside regular hours (felt personal)
 - Thanks Petr!
- Shorten the time for takedown

Study and make notes

- Website emerged several days after registration
- Directory listing emerged first
- Zip file in it (let me know if you want free samples!)
- Unpacked zip files – the site was up

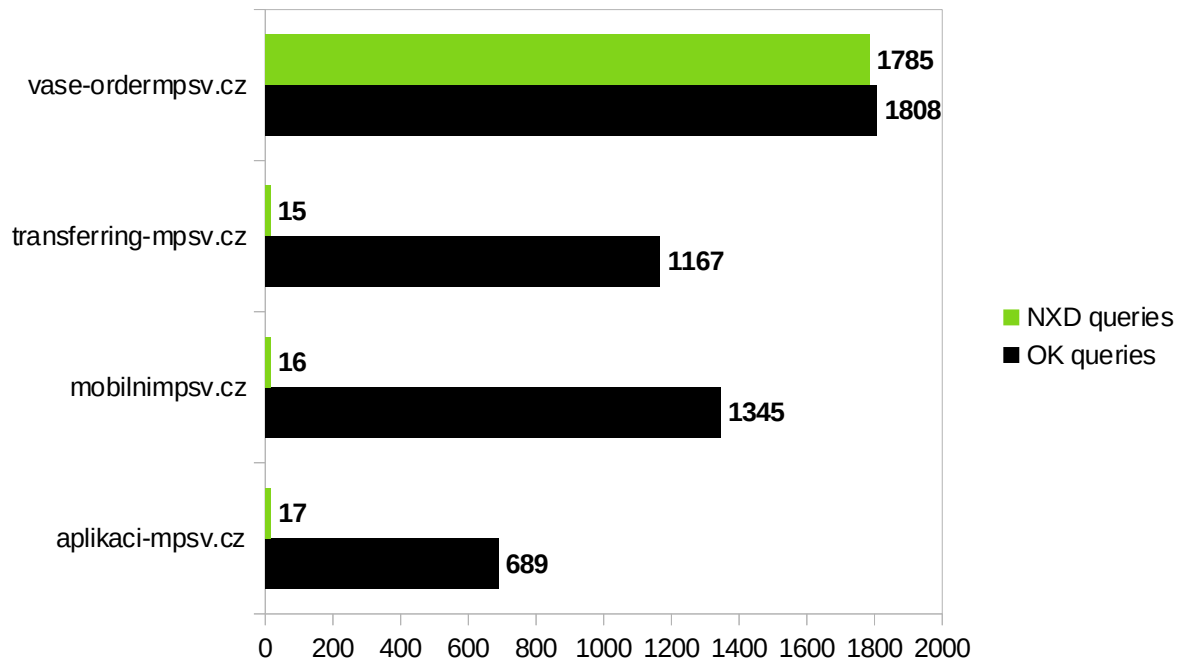
Study and make notes 2

- Certificate transparency is a thing!
- Find subdomain – find an admin panel
 - no password needed

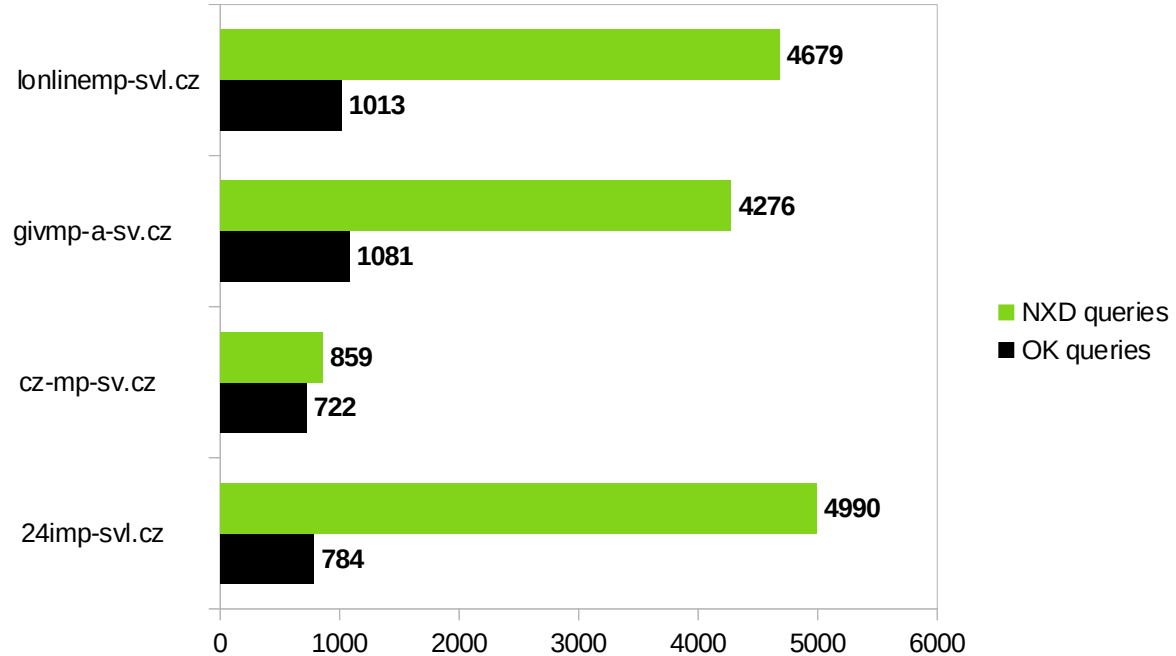
Victory!

- Stopped March 2023
 - After ~28 domains (remember 72?)
- Nothing comparable since
 - Occasional tries with other TLDs

Numbers 21.12.2022



Numbers 2.2.2023



Behind the scenes

- Article 17 („disrupts cyber security“)
- out-of-zone:
 - status: The domain is administratively kept out of zone
- Public list of blocked domains

Thank you for watching!

Martin Kunc
martin.kunc@nic.cz