

Phishing na české doméně

Martin Kunc • 04.10.2025

Our projects



Kdysi dávno v předaleké galaxii...

- červen 2022
- Zaznamenali jsme další phishing
- na doméně .cz (velmi neobvyklé!)
- vešel v platnost příspěvek na bydlení

„Příběhové postavy“ (1)

- mps.v.cz



**MINISTERSTVO PRÁCE
A SOCIÁLNÍCH VĚCÍ**

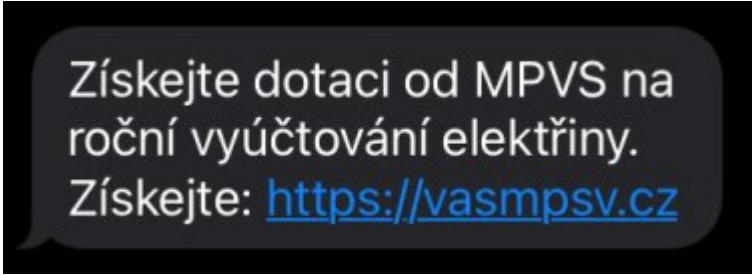
„Příběhové postavy“ 2

- BankID (kéž by lidé používali mojeID :))
- Oběti (občané)
- ... a podvodníci

Bank iD

Scénář

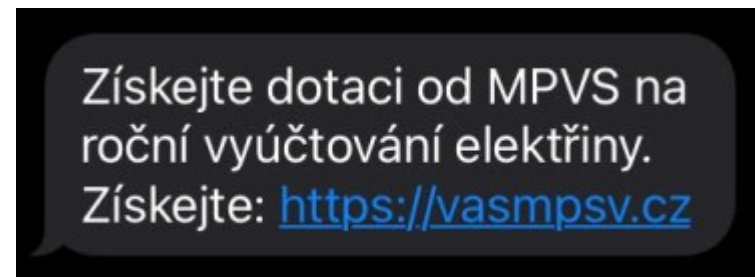
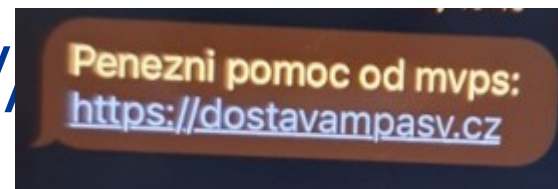
- Oběť dostane smsku:
- „Vyzvedněte si dotaci zde: <https://...>“

A screenshot of an SMS message displayed on a black background. The text is white and reads: "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>

Scénář

- Oběť dostane smsku:
- „Vyzvedněte si dotaci zde: [https://](https://dostavampasv.cz)“



Scénář

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>

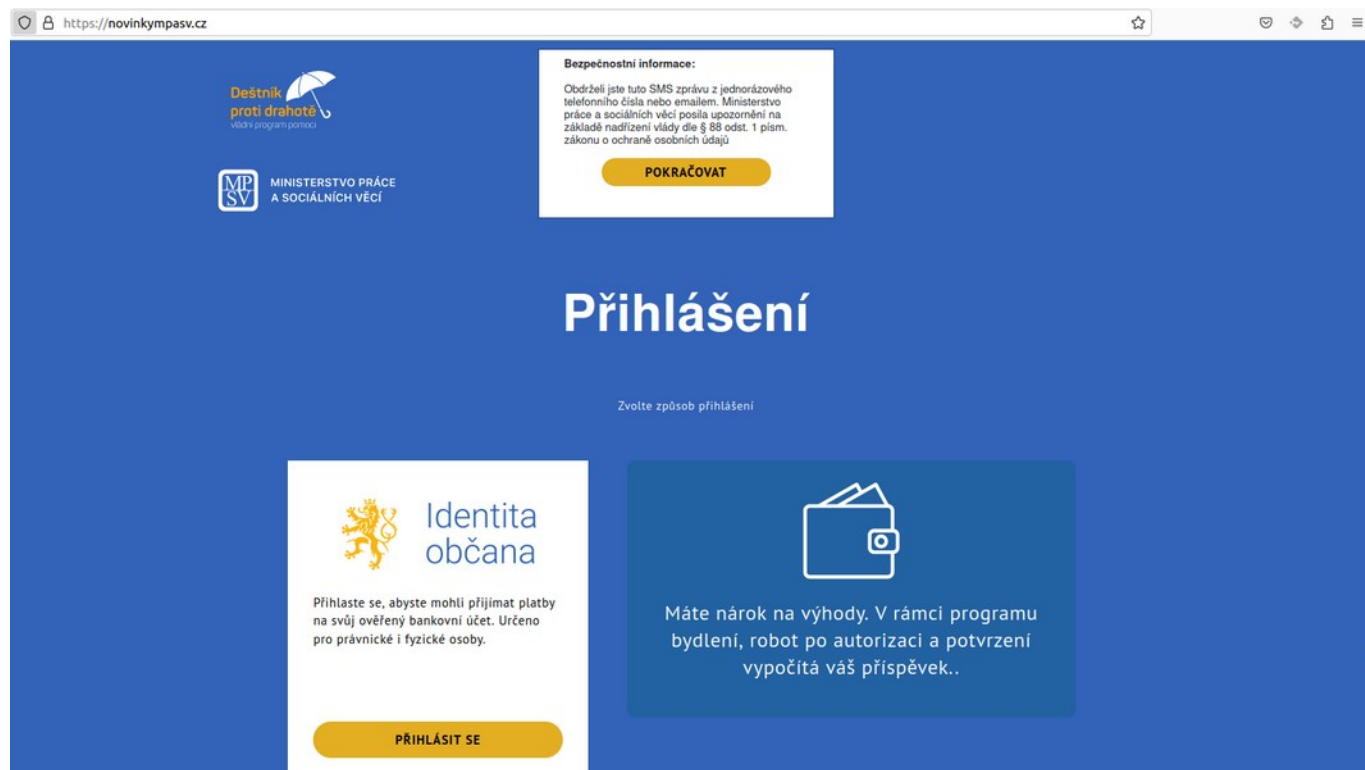
Hotovo. Příspěvek na bydlení
na vašem účtu: <https://24-mpsiv.cz>

Příspěvek na bydlení máte k
dispozici: <https://online-platbympsiv.cz>
SMS 17:20

Scénář - pokračování

- Uživatel otevře phishingovou stránku
- „Přihlašte se prosím pomocí BankID“ (pouze v pracovní době!)
- Útočník zneužije přihlašovací údaje a nechá si ověřit i druhý faktor

Příklady





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

Postupný nárůst

- 2022:
 - ~11 případů/domén za měsíc
- Únor 2023:
 - 72 domén
 - V tu chvíli už jsme případ řešili naplno

Oni se zlepšují a co my?

- Aktivní vyhledávání (oproti čekání na incident)
- Zdokonalování procesu na naší straně
- Zjišťovat a zaznamenávat detaily

Aktivní hledání

- Registr – „regulární výrazy“?
 - *mpvs* or *mpsv*
 - *mp-sv* or *mp-sv*
- Jediné spohlivé „Registration date: „LAST_WEEK“

Zdokonalování procesu

- Udržovaný seznam budoucích domén
- Pravidelné skenování (IP nikdy nezablokovali)
- Okamžité notifikace
 - S chutí jsme to řešili i nad rámec pracovní doby
 - Kudos pro Petra Špringera!
- Urychlení procesu na vyřazení domény

Zjišťovat a zaznamenávat detaily

- Weby byly aktivovány několik dní po registraci:
 - Nejprve directory listing
 - Po té nahráli zip (ozvěte se pokud chcete vzorky)
 - Rozbalili zip a stránka ožila

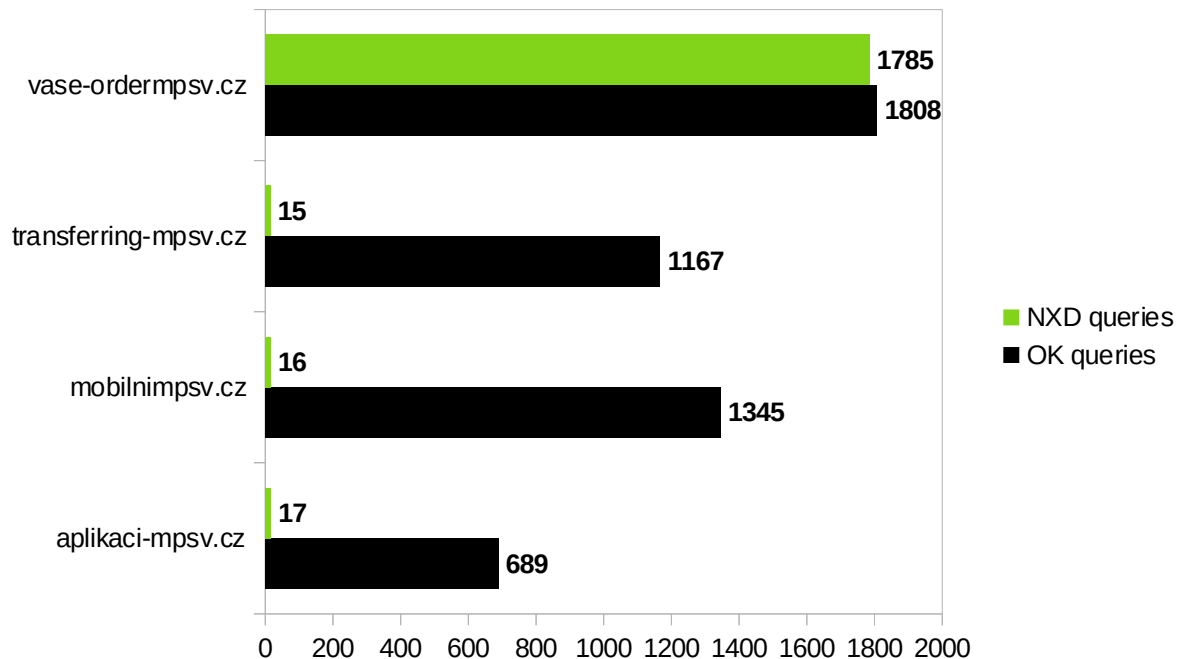
Zjišťovat a zaznamenávat detaily

- Certificate transparency je super věc!
- Nález subdomény – admin panel
 - přístupný bez hesla

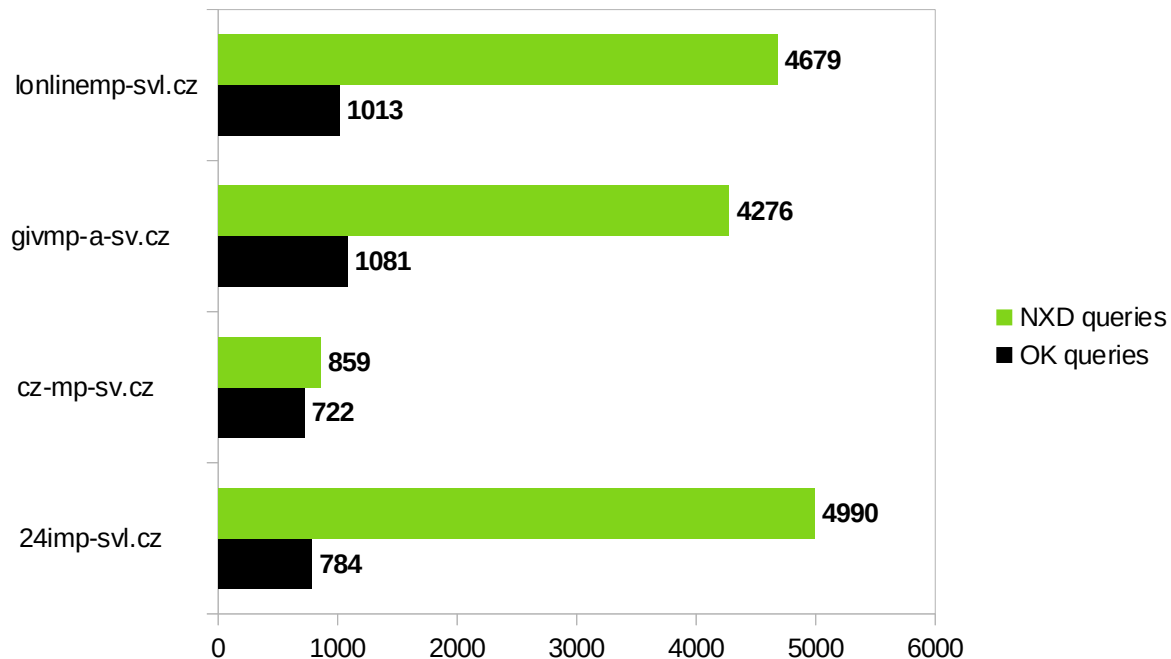
Vítězství!

- Pokusy ukončeny v březnu 2023
 - Po ~28 doménách (pamatujete na 72?)
- Od té doby nic srovnatelného
 - Čas od času snaha u jiných TLD

Počty 21.12.2022



Počty 2.2.2023



Nové podvody?

- Falešný bankéř
- Falešné investice (vč. napadených účtů přátel)
- Reverzní inzertní podvody
- „Hlasování v soutěži“ - Whatsapp

Co s nabitými zkušenostmi

- Deny listy
- DNS Patrol

Děkuji za pozornost!

Martin Kunc
martin.kunc@nic.cz