



# Lookalike domény

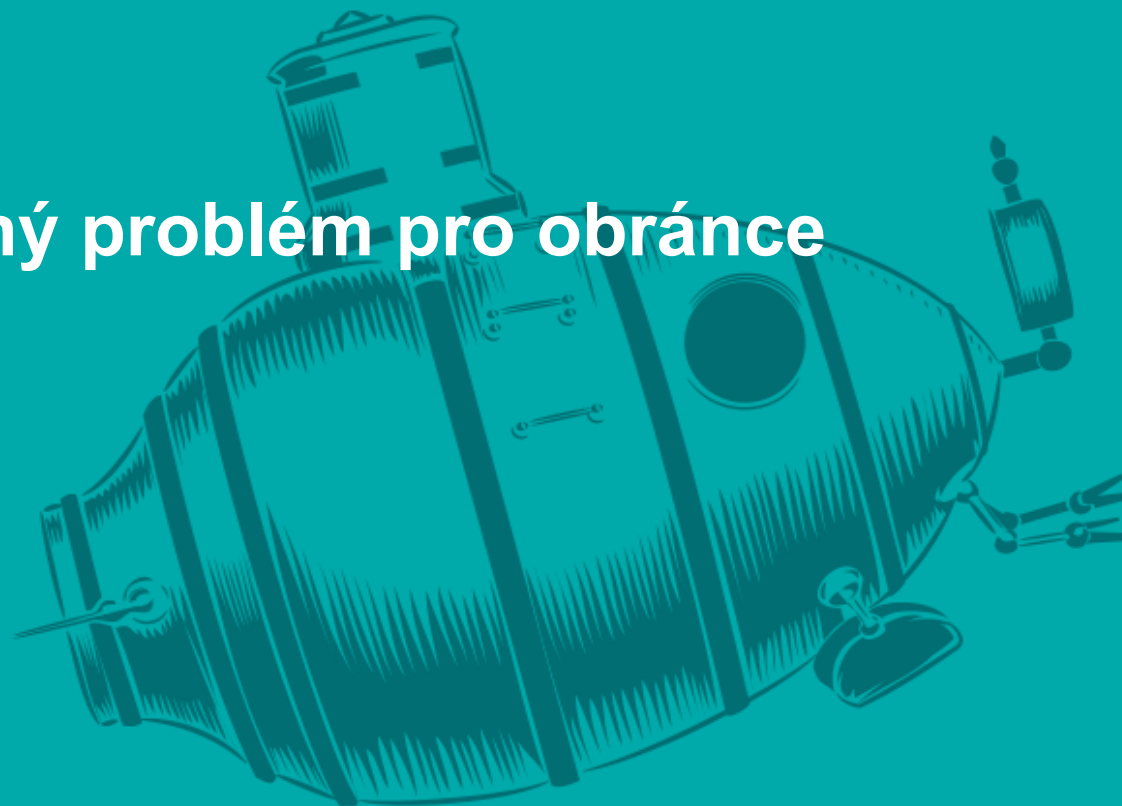
Mocná zbraň pro útočníky, citelný problém pro obránce

**Jan Kopřiva**

jan.kopriva@alef.com

 @jk0pr

ALEF CSIRT



**TLP: WHITE**

# Lookalike domény - označení říká vše

<https://www.paypal.com/>

- <https://www.paypal.com-en.cz/>
- <https://www.paypal.com/>
- <https://www.paypall.com/>
- <https://www.paypål.com/>
- <https://pa.ypal.com/>

# Proč jsou lookalike domény problém?

- V textu/odkazech jsou často nerozeznatelné od domén legitimních
- Jakoukoli „volnou“ je možné snadno získat
- Stejně tak je jednoduché získat důvěryhodný TLS certifikát

# K čemu je útočníci využívají?

- Odesílání phishingových e-mailů
- Hostování podvodných stránek

# K čemu je útočníci využívají?

- Zachytávání „překlepů“ a přesměrovávání na podvodné weby
- Falešné výsledky ve vyhledávačích

**iPrima** SERIÁLY A POŘADY FILMY PRO DĚTI TV PROGRAM ZPRAVODAJSTVÍ ČLÁNKY IPRIMA BEZ REKLAM VIDEOPŮČOVNA Přihlásit se

Domů » Finance » Kryptoměny

## Petr Kellner investuje 1,5 milionu eur do startupu a říká, že „zde se nachází budoucnost“

Velký počet Čechů si již přinesl domů miliony pomocí této „mezery v zákonech pro bohatství“, ale je to legitimní?

287 SDÍLENÍ Autor **Patrick Evans** PÁTEK, LEDEN 1, 2021 | AKTUALIZOVÁNO: LEDEN 2, 2021 **ZPRÁVY**

MOHLI JSTE VIDĚT V:

24 1 nova Prima

reklama  
**FIREMNÍ DÁRKY – NÁPADY A TIPY**  
Ještě není pozdě.  
CHCI VÍCE INFO

Nejnovější zprávy do e-mailu  
zadejte e-mail

reklama

# K čemu je útočníci využívají?

## **Lookalike domény pro Amazon (amazon.com)**

*amagon[.]com*

*amagzon[.]com*

*amažon[.]com (xn--amaon-7hb[.]com)*

*apmazon[.]com*

## **Lookalike domény pro Audible (audible.com)**

*aujdbible[.]com*

*audiblel[.]com*

## **Lookalike domény pro Google (google.com)**

*goozgle[.]com*

*goowle[.]com*

*googlen[.]com*

*googlpe[.]com*

*googvle[.]com*

*google[.]com (xn--gogle-vob[.]com)*

## **Lookalike domény pro Humble Bundle (humblebundle.com)**

*hublebundle[.]com*

*humbblebundle[.]com*

*humbleebundle[.]com*

*humblbundle[.]com*

*humblebunndle[.]com*

*humblebundlle[.]com*

*humblebunddle[.]com*

*humblebundlee[.]com*

*humblebundke[.]com*

*humblebunfle[.]com*

*humblebbundle[.]com*

*huumblebundle[.]com*

# Jak se proti lookalike doménám bránit?

- Vzdělávání
  - Nezbytné, ale pouze omezeně účinné
- Sledování nově registrovaných zájmových domén
  - Efektivní, ale ochrání jen „naší“ organizaci
- Technicky netriviální
  - <https://github.com/elceef/dnstwist>
  - <https://dnstwister.report/>

# Jak se proti lookalike doménám bránit?

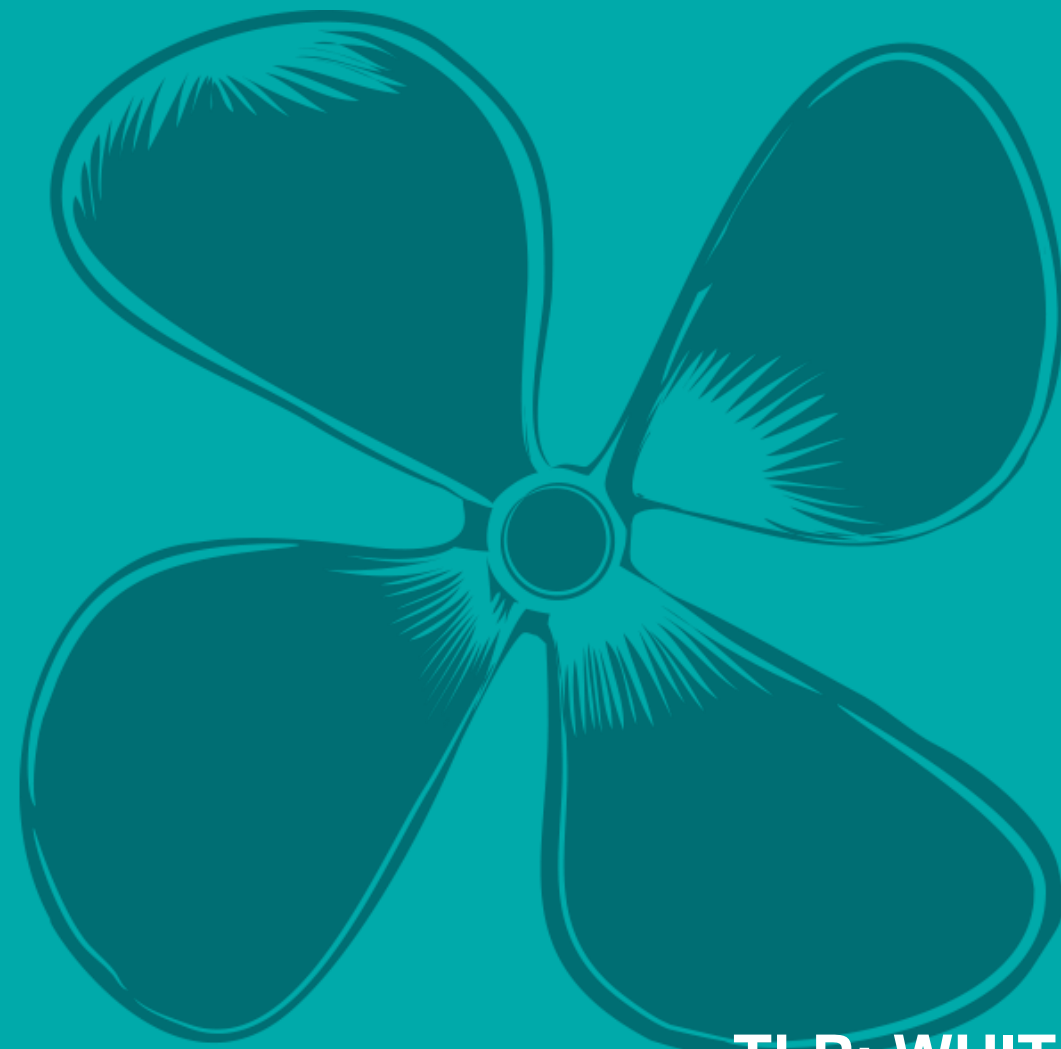
- Preventivní registrace zájmových domén z naší strany
  - Vhodné nastavit „blokační“ SPF záznamy
- Blokování e-mailů z domén bez MX záznamu
  - V současnosti standard

...a samozřejmě mnoho dalšího



**X ALEF**

**Děkuji Vám za  
pozornost**



**TLP: WHITE**