cesnet

HLÁŠENI PHISHINGOVÝCH URL

Jiří Ráž
CESNET

únor 2023
seminář o bezpečnosti sítí a služeb

cesnet

HLÁŠENÍ PHISHINGOVÝCH URL

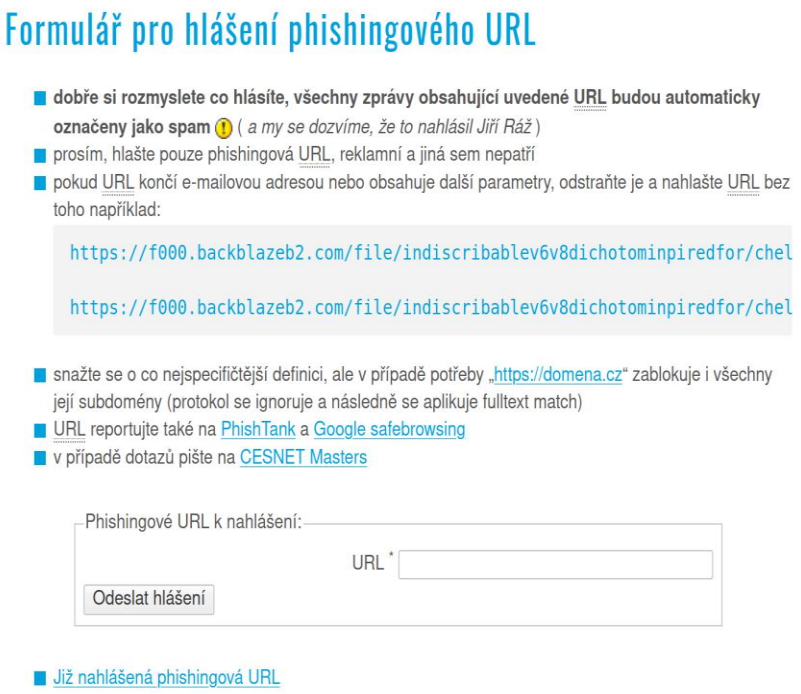
ČAS JE PROTI NÁM

- URL se mění
- Komplikovaný proces blokování
- Potřeba urychlit celý proces
- Minimalizovat zapojení různých správců
- Jednoduché na používání
- Přístup jen pro csirt

cesnet

HLÁŠENÍ PHISHINGOVÝCH URL
FORMULÁŘ

- **dokuwiki Bureaucracy Plugin**
  - Jednoduchý formulář pro hlášení
  - Implementace do stávající infrastruktury
  - Kontrola syntaxe
  - Vygeneruje tabulku



- dokuwiki cronjob
  - Hlídá změny ve stránce
  - Ošetření speciálních znaků
  - Vygeneruje txt soubor s pravidly
  - Soubor je vystaven na webu
  - Přístup jen pro vybrané IP

Nahlášená phishingová URL

Neupravujte stránku ručně! *Pro nahlášení nového URL použijte Formulář pro hlášení phishingového URL*

Datum	Jméno a příjmení	Nahlášené URL
26.01.2023 13:04	Jiří Ráž	https://wjjhhn.s3.us-west-004.backblazeb2.com/fn.html
25.01.2023 21:41	Miroslav Sochor	http://cz.ceskysystem.authorityrate.co.in/
25.01.2023 16:30	Miroslav Sochor	https://p-mpsv.online/
24.01.2023 21:21	Pavel Vachek	https://s3.ap-northeast-2.wasabisys.com/zaaaas/beta2.html
23.01.2023 10:22	Miroslav Sochor	http://www.owa4340.c1.biz
15.01.2023 15:39	Pavel Vachek	https://qassaaddmoreedhgmyinmerfvdbgghjklotyhnbsaqewe.000webhostapp.com/u
12.01.2023 14:08	Pavel Vachek	https://transport20.dedyn.io/secure.php
12.01.2023 14:08	Pavel Vachek	https://qwert.dedyn.io/
10.01.2023 18:02	Pavel Vachek	https://ipfs.io/ipfs/QmZ3LAwK8goAqXE2q39EvjcxrST8UvkHxfbtHEZL8k4Ged

HLÁŠENÍ PHISHINGOVÝCH URL

NASAZENÍ

- Spamassassin cronjob
  - Hlídá změny
  - Aktualizuje lokální kopii
  - Restartuje spamassassin

```
uri             CERTS_202301261304_PHURL        /wjjhhn\.s3\.us\-west\-004\.backblazeb2\.com\/fn\
shortcircuit    CERTS_202301261304_PHURL        spam

uri             CERTS_202301252141_PHURL        /cz\.ceskysystem\.authorityrate\.co\.in/
shortcircuit    CERTS_202301252141_PHURL        spam

uri             CERTS_202301251630_PHURL        /p\-mpsv\.online/
shortcircuit    CERTS_202301251630_PHURL        spam

uri             CERTS_202301242121_PHURL        /s3\.ap\-northeast\-2\.wasabisys\.com\/zaaaas\/be
shortcircuit    CERTS_202301242121_PHURL        spam

uri             CERTS_202301231022_PHURL        /www\.owa4340\.c1\.biz/
shortcircuit    CERTS_202301231022_PHURL        spam

uri             CERTS_202301151539_PHURL        /qassaaddmoreedhgmyinmerfvdbgghjklotyhnbsaqewe\.(
shortcircuit    CERTS_202301151539_PHURL        spam

uri             CERTS_202301121408_PHURL        /qwert\.dedyn\.io/
shortcircuit    CERTS_202301121408_PHURL        spam

uri             CERTS_202301101802_PHURL        /ipfs\.io\/ipfs\/QmZ3LAwK8goAqXE2q39EvjcxrST8UvkH
shortcircuit    CERTS_202301101802_PHURL        spam

uri             CERTS_202212300930_PHURL        /infoefocusiric\.github\.io\/portfolio\/mik_webm\
shortcircuit    CERTS_202212300930_PHURL        spam

uri             CERTS_202212221106_PHURL        /queballthemammoth\.s3\.ir\-thr\-at1\.arvanstorag
shortcircuit    CERTS_202212221106_PHURL        spam

uri             CERTS_202212221101_PHURL        /www\.asaas\.com\/register\/dispositive\-remove\/
shortcircuit    CERTS_202212221101_PHURL        spam

uri             CERTS_202212191440_PHURL        /ipfs\.io\/ipfs\/QmQLmGmx2PtvUQ3yxus25qNzJFxYXv9v
shortcircuit    CERTS_202212191440_PHURL        spam

uri             CERTS_202212141628_PHURL        /williewontie\.com\/audit/
shortcircuit    CERTS_202212141628_PHURL        spam

uri             CERTS_202212121545_PHURL        /online\.aplications\.rest\/x2Xh25WRB1HSG616XNBag
shortcircuit    CERTS_202212121545_PHURL        spam
```

HLÁŠENÍ PHISHINGOVÝCH URL

ZÁVĚR

- **Blokování URL je mnohem rychlejší**
  - Do deseti minut je blokováno na všech serverech
- **Historie hlášení**
  - Máme přehled kdo kdy a co zablokoval
- **Nahlášených URL 293**
  - Za rok 2022
- **Počet zachycených zpráv 10 284**
  - Za rok 2022 Data z 5 serverů, u dvou jen za 6 měsíců

cesnet

DĚKUJI ZA POZORNOST

MÁTE NĚJAKÉ DOTAZY?