



HLÁŠENÍ PHISHINGOVÝCH URL

Jiří Ráž
CESNET

únor 2023
seminář o bezpečnosti sítí a služeb



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

■ dokuwiki Bureaucracy Plugin

- Jednoduchý formulář pro hlášení
- Implementace do stávající infrastruktury
- Kontrola syntaxe
- Vygeneruje tabulku

Formulář pro hlášení phishingového URL

- dobře si rozmyslete co hlásíte, všechny zprávy obsahující uvedené URL budou automaticky označeny jako spam 🚫 (a my se dozvíme, že to nahlásil Jiří Ráž)
- prosím, hlášte pouze phishingová URL, reklamní a jiná sem nepatří
- pokud URL končí e-mailovou adresou nebo obsahuje další parametry, odstraňte je a nahlašte URL bez toho například:

```
https://f000.backblazeb2.com/file/indiscribablev6v8dichotominpiredfor/chel
```

```
https://f000.backblazeb2.com/file/indiscribablev6v8dichotominpiredfor/chel
```

- snažte se o co nejspesifitější definici, ale v případě potřeby „<https://domena.cz>“ zablokuje i všechny její subdomény (protokol se ignoruje a následně se aplikuje fulltext match)
- URL reportujte také na [PhishTank](#) a [Google safebrowsing](#)
- v případě dotazů pište na [CESNET Masters](#)

Phishingové URL k nahlášení:

URL *

- [Již nahlášená phishingová URL](#)

■ 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://wjjhcn.s3.us-west-004.backblazeb2.com/fn.html
25.01.2023 21:41	Miroslav Sochor	http://cz.cesksystem.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/zaaaa/beta2.html
23.01.2023 10:22	Miroslav Sochor	http://www.owa4340.c1.biz
15.01.2023 15:39	Pavel Vachek	https://qassaadmoreedhgmyinmerfvdbggghjklotyhnbsaqewe.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/QmZ3LAWK8goAqXE2q39EvjcxrST8UvkHxftbHEZL8k4Ged

■ Spamassassin cronjob

■ Hlídá změny

■ Aktualizuje lokální kopii

■ Restartuje spamassassin

uri shortcircuit	CERTS_202301261304_PHURL CERTS_202301261304_PHURL	/wjhhn\.s3\.us\-west\-004\.backblazeb2\.com\/fn\ spam
uri shortcircuit	CERTS_202301252141_PHURL CERTS_202301252141_PHURL	/cz\.ceskysystem\.authorityrate\.co\.in\ spam
uri shortcircuit	CERTS_202301251630_PHURL CERTS_202301251630_PHURL	/p\-mpsv\.online\ spam
uri shortcircuit	CERTS_202301242121_PHURL CERTS_202301242121_PHURL	/s3\.ap\-northeast\-2\.wasabisys\.com\/zaaaas\ spam
uri shortcircuit	CERTS_202301231022_PHURL CERTS_202301231022_PHURL	/www\.owa4340\.c1\.biz\ spam
uri shortcircuit	CERTS_202301151539_PHURL CERTS_202301151539_PHURL	/qassaaddmoreedhgmyinmerfvdbggghjklotyhnbsaqewe\ spam
uri shortcircuit	CERTS_202301121408_PHURL CERTS_202301121408_PHURL	/qwert\.dedyn\.io\ spam
uri shortcircuit	CERTS_202301101802_PHURL CERTS_202301101802_PHURL	/ipfs\.io\/ipfs\/QmZ3LAWK8goAqXE2q39EvjcxrST8Uvkf spam
uri shortcircuit	CERTS_202212300930_PHURL CERTS_202212300930_PHURL	/infoefocusiric\.github\.io\/portfolio\/mik_webm\ spam
uri shortcircuit	CERTS_202212221106_PHURL CERTS_202212221106_PHURL	/queballthemammoth\.s3\.ir\-thr\-at1\.arvanstoraç spam
uri shortcircuit	CERTS_202212221101_PHURL CERTS_202212221101_PHURL	/www\.asaas\.com\/register\/dispositive\-remove\ spam
uri shortcircuit	CERTS_202212191440_PHURL CERTS_202212191440_PHURL	/ipfs\.io\/ipfs\/QmQLmGmx2PtvUQ3yxus25qNzJFyYXv9v spam
uri shortcircuit	CERTS_202212141628_PHURL CERTS_202212141628_PHURL	/williewontie\.com\/audit\ spam
uri shortcircuit	CERTS_202212121545_PHURL CERTS_202212121545_PHURL	/online\.applications\.rest\/x2Xh25WRB1HSG616XNBaç spam
uri	CERTS_20221121014	/account\ director\ rest\ developer\ app /



- **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?

