

moz://a

(ne)bezpečnost na webu

Michal Vašíček



Stalo se

iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

- Killswitch pro ransomware WannaCry
- Stačilo zaregistrovat doménu
- Nespočet napadených institucí
 - FedEx
 - Národní zdravotnická služba UK
 - Nemocnice v Nitře
 - Deutsche Bahn
 - LATAM Airlines
 - Sberbank

Únos TLD

- Autoritativní nameservery .io nezaregistrované
- Matthew Bryant je kupuje
- Happyend

Těžba kryptoměn v prohlížeči

- Začal s tím The Pirate Bay (miner Coinhive)
- Výkon omezují na 30%
- Nelze ho vypnout
- Vynahrazuje reklamy
- Až přijde miner bez omezení výkonu?

WordPress ignoroval zranitelnost

- Možná SQL Injection ve WordPress pluginech
- Vývojáři vyrobili patch, který zranitelnost opravil „špatně“
- Výhružky na Twitteru
- Happyend



Stane se

Kryptografie ve Firefoxu

- Verze 57 - Firefox Quantum (za 10 dní)
- Knihovna HAACL*
- Formálně ověřená kryptografie
- Integrace do knihovny Network Security Services

TLS 1.3

- Nástupce TLS 1.2
- Zatím ve fázi draftu
- Mízí podpora pro MD5 a SHA-224 hashe
- Většina prohlížečů již podporuje
- Nginx 1.13, Apache nad OpenSSL 1.1.1

Let's Encrypt v Apache


- Podpora pro ACME protokol v modulu mod_md
- Nutná úprava mod_ssl
- Financuje Mozilla
- Jednoduchá konfigurace
 - SSLPolicy - úroveň zabezpečení
 - ManagedDomains - LE domény



Wildcard Let's Encrypt

- Příští rok s novou verzí ACME protokolu
- Očekávaný vzrůst webů s HTTPS
- Vzpomínáte na aféru SSLs?

Proč nepoužívat Let's Encrypt

	Let's Encrypt	PositiveSSL	Comodo EV
Platnost certifikátu	jen 3 měsíce	1-3 roky	1-2 roky
Podpora prohlížečů a zařízení	?	99,9%	99,9%
Podpora 256 bit ECC (silné šifrování)	✗	✓	✓
 https:// Zobrazuje zelený adresní řádek	✗	✗	✓
<u>Finanční záruka</u>	✗	✓ \$10,000	✓ \$1,750,000
Vhodný pro komerční či firemní web, eshop	✗	✓	✓
Podpora IDN (domény s diakritikou)	✗	✓	✓
Podpora wildcard (zabezpečí ∞ subdomén)	✗	✓	✗
Možnost získat před spuštěním serveru	✗	✓	✓
Ochrana proti vystavení pro podvodný web	✗	✓	✓
Prestížní značka certifikátu	✗	✓	✓
Neomezený počet vystavených certifikátů	✗	✓	✓
Možnost zneplatnění certifikátů	✗	✓ zdarma	✓ zdarma
Pečeť pro vyšší důvěryhodnost	✗	✓ statická	✓ dynamická
Stabilní ekonomický model CA	✗	✓	✓
Zákaznická podpora	✗	✓ 24H	✓ 24H



Vaše postřehy?

Díky!

@MekliCZ

mozilla.cz

a.openalt.cz/251