HTTPS zdarma a pro všechny

Ing. Tomáš Hála
Linux Teamleader
ACTIVE 24, s.r.o.
@tomashala

10. října 2015

LinuxDays 2015

A proč?

Proč bychom měli šifrovat i stránky, ke kterým se nepřihlašujeme?

Psali to na rootu. Před dvěma týdny a celkem zevrubně. Předpokládám, že jste všichni četli, tedy..

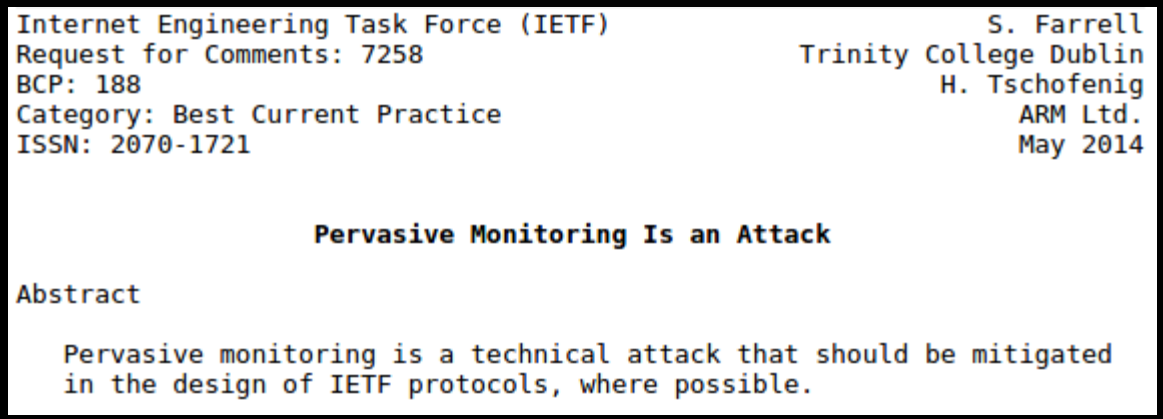
Děkuji za pozornost!

(Pokud jste to náhodou nečetli nebo chcete vědět více, poslouchejte dále a třeba se dozvíte něco nového.)

```
root@home:~# curl -I https://www.root.cz/
HTTP/1.0 301 Moved Permanently
Location: http://www.root.cz/
Content-Type: text/html
Content-Length: 156
```

Root sám před pár dny HTTPS zprovoznil. Zatím jen takto, ale dá se předpokládat, že brzy na něj přejde na ostro.

Dobře, tak co jsou ty důvody?



Internet Engineering Task Force (IETF) — S. Farrell
Request for Comments: 7258 — Trinity College Dublin
BCP: 188 — H. Tschofenig
Category: Best Current Practice — ARM Ltd.
ISSN: 2070-1721 — May 2014

Pervasive Monitoring Is an Attack

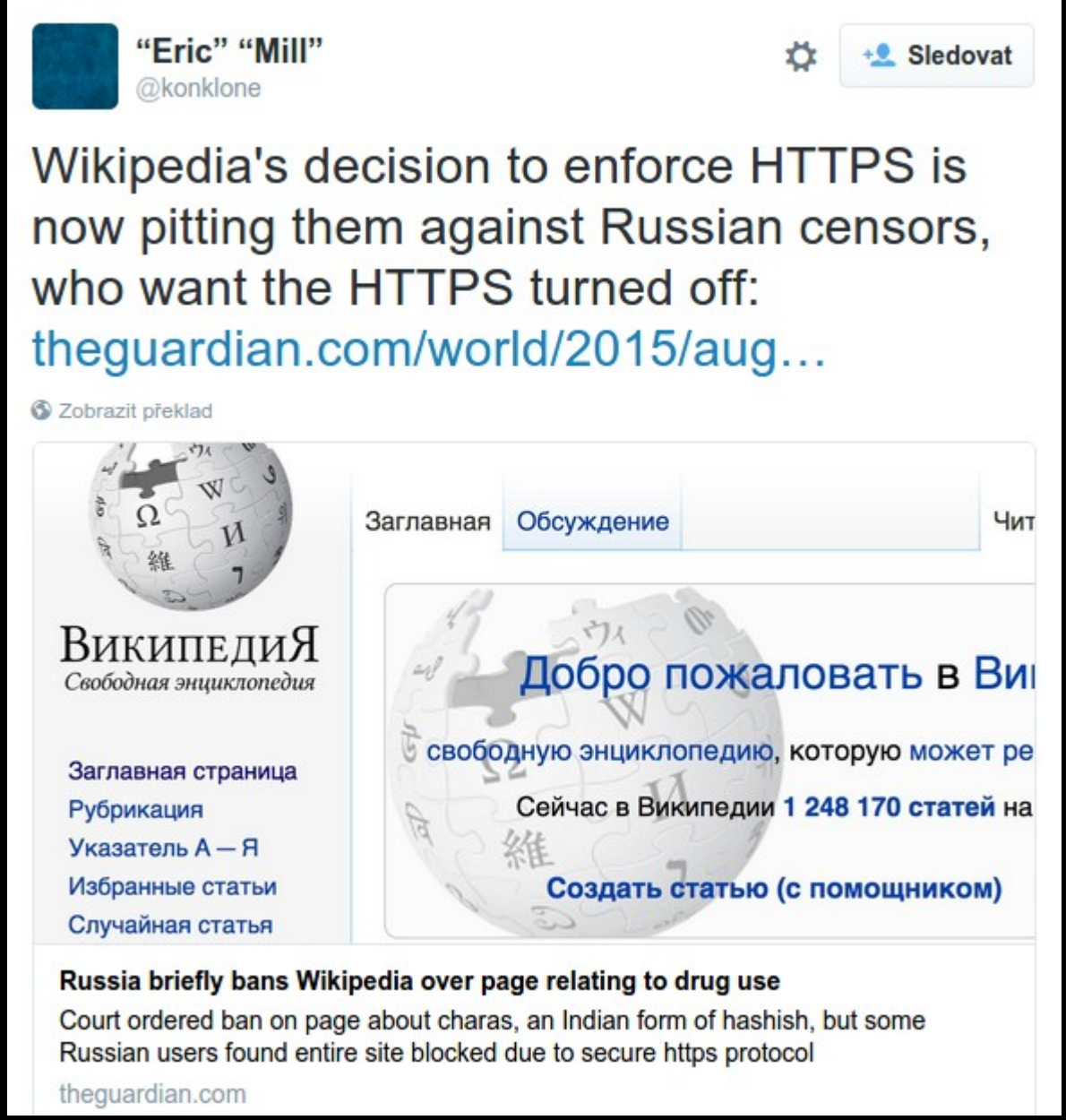
Abstract

Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible.

Dle RFC 7258 máme všudypřítomné sledování považovat za útok a snažit se mu bránit a omezovat možnosti odposlechu už v samotných přenosových protokolech.

Nečtu nic tajného, mně šmírování nevadí..

Ne každému to vadí, že je jeho aktivita na internetu sledována (např. zaměstnavatelem nebo reklamními agenturami). Jaké jsou tedy další důvody?



Wikipedia se po zavedeni HTTPS dostala do křížku s ruskými cenzory – nemohli zablokovat konkrétní stránku a žádali odstranění HTTPS. Úřady udržují seznamy stránek, na které všichni lokální poskytovatelé připojení blokují přístup.

Se zapnutým HSTS (více později) a preloadem v prohlížečích už ale vypnutí HTTPS není ani technicky možné a tedy není možné ani blokovat či modifikovat části obsahu.

To je Rusko, u nás přece cenzura nehrozí..

Dobře, zasahovat do obsahu stránek se mi nelíbí, ale u nás přece není cenzura jako v Rusku, my máme přístup na internet bez regulace státní správou.

Hlava II

Nepovolené internetové hry

§ 82

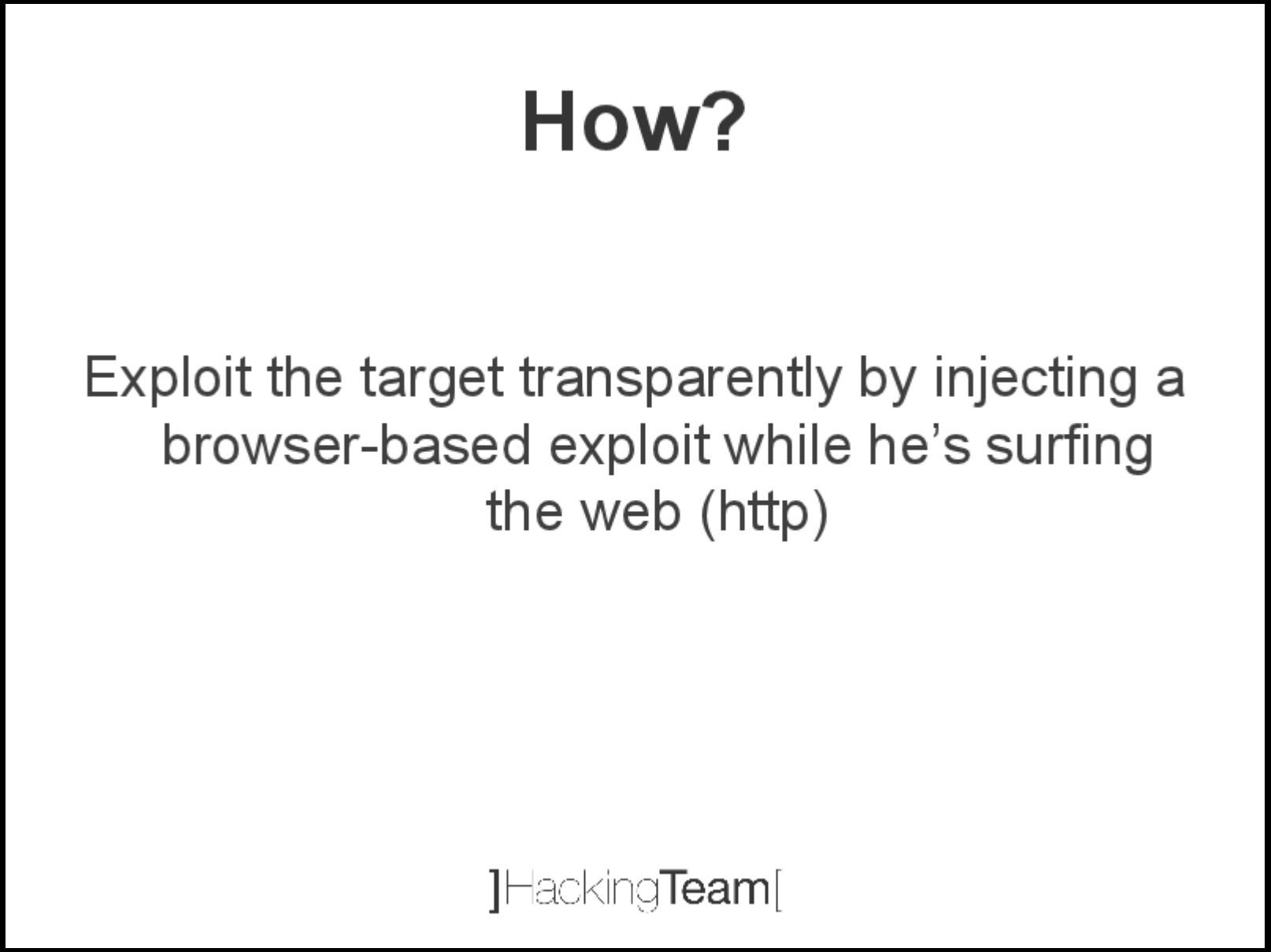
Blokace nepovolených internetových her

(1) Poskytovatelé připojení k internetu na území České republiky jsou povinni zamezit v přístupu k internetovým stránkám uvedeným na seznamu internetových stránek s nepovolenými internetovými hrami (dále jen „seznam nepovolených internetových her“).

Právě v těchto dnech projednávaný návrh novely zákona o hazardních hrách ale navrhuje přesně takový druh regulace a otevírá Pandořinu skřínku. Chceme, aby ministerstvo určovalo, jaké stránky si smíme prohlížet a jaké ne?

Hmm, a to je jako vše?

Jsou tedy šmírování a cenzura jediné důvody pro nasazování HTTPS?



Ve známé kauze HackingTeam se v plné nahotě ukázalo, jak se infikují počítače obětí malwarem – útočný kód se vkládá po cestě do jinak zcela legitimních webových stránek fungujících na nešifrovaném HTTP, když je oběť navštíví.

The Hacker News™
Security in a serious way

Hacking Team Flash Zero-Day Linked to Cyber Attacks on South Korea and Japan

Thursday, July 09, 2015 Wang Wei

Využívali k tomu např. 0-day zranitelnost ve Flash Playeru.

The Hacker News™
Security in a serious way

Second Flash Player Zero-day Exploit found in 'Hacking Team' Dump

Saturday, July 11, 2015 Swati Khandelwal

A ne jednu..

HACKBUSTERS

Hackbusters is an awesome IT Security Community. **Join** c

« Back to Articles

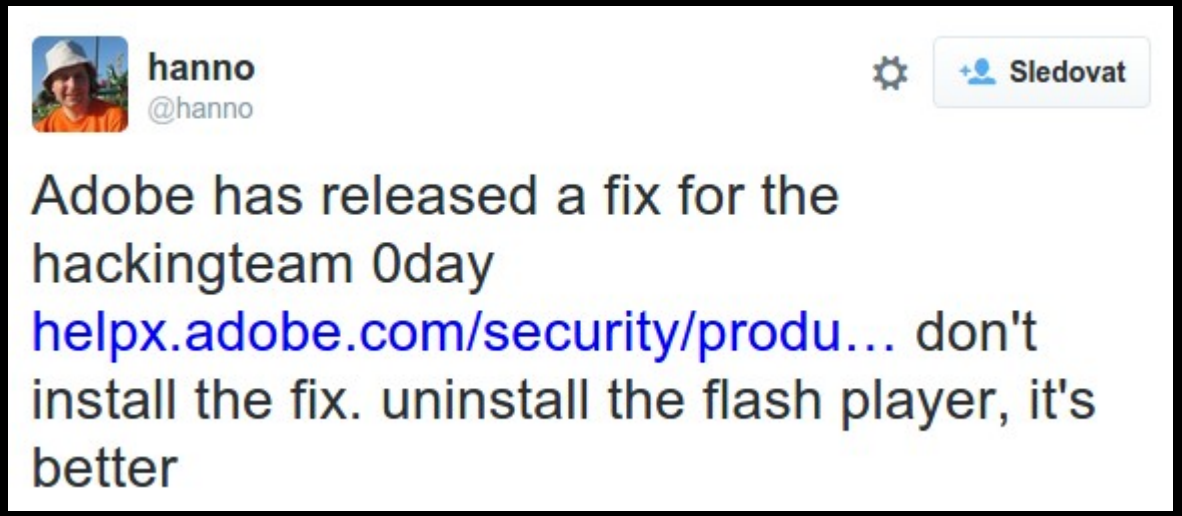
Hacking Team, the third Flash Zero-Day is out: CVE-2015-5123

securityaffairs.co - 3 months ago - by Pierluigi Paganini

Following the Hacking Team data breach, the security researchers discovered the third Adobe Flash Player zero-day vulnerability. **A third** Adobe Flash Player zero-day has been discovered since the HackingTeam breach. Thanks to the breach of the Hacking Team's private files, the third Adobe Flash zero-day has been made publicly accessible. *"After two Adobe Flash player zero-days disclosed in a row from the leaked data of Hacking Team, we discovered another Adobe Flash Player zero-day (assigned with CVE number, CVE-2015-5123) that surfaced from the said leak. Adobe has already released a security advisory after we reported the said zero-day. This vulnerability is rated as critical and can allow an attacker to take control of the affected system once successfully exploited. It affects all versions of Adobe Flash in Windows, Mac, and Linux." reported a blog post from Trend Micro.* This newly uncovered zero-day has a similar PoC as the one released immediately prior...(continued)

View Full Original Article

Ani ne dvě a samozřejmě ne jen ve Flashi. Měli připravené zranitelnosti prakticky pro jakoukoliv běžně používanou platformu na počítačích, tabletech nebo mobilech.

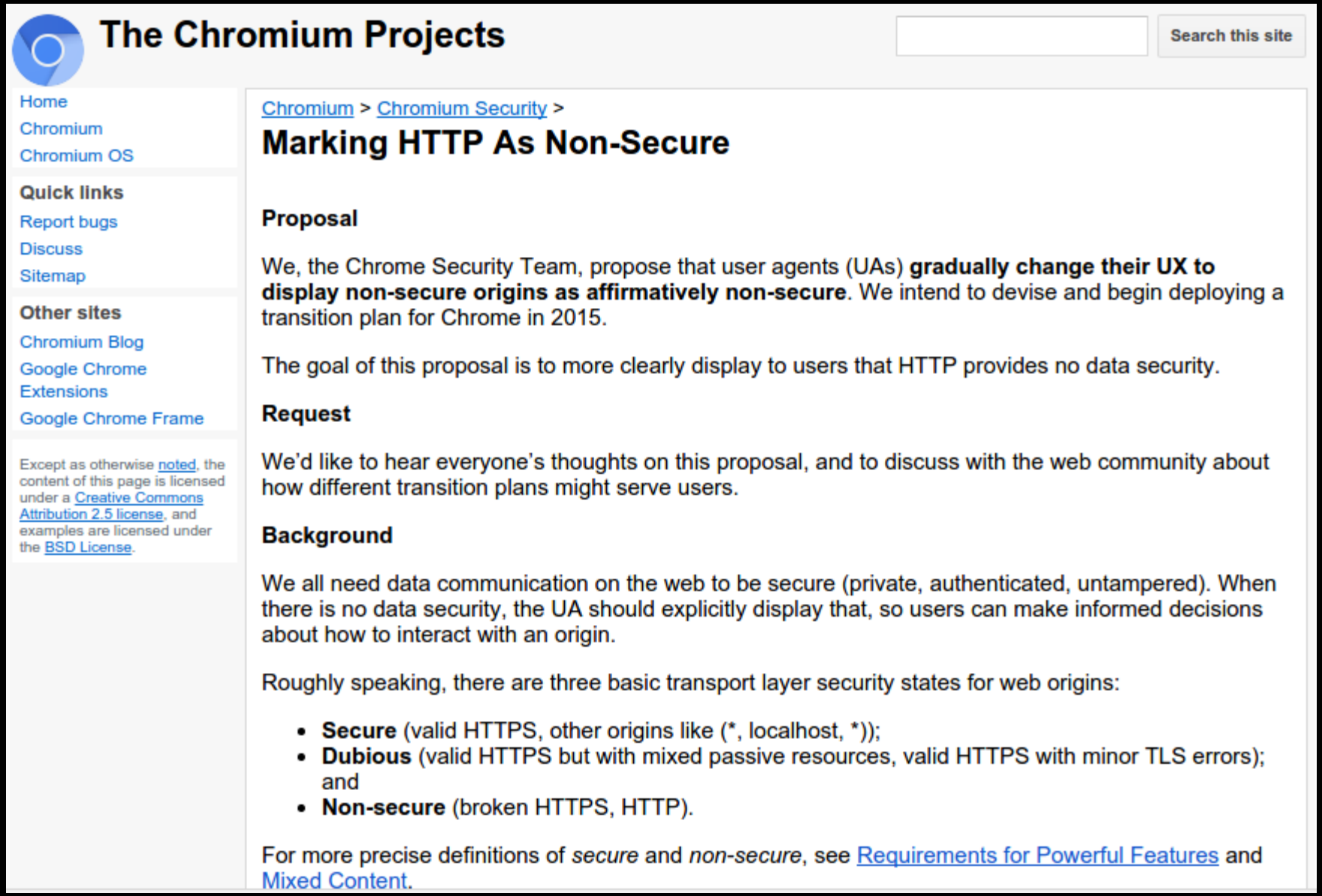


Když už jsme u toho Flashe, Adobe nalezené díry s odstupem času záplatuje, ale neinstalujte je – Flash prostě odstraňte. Vážné díry se v něm objevují stále dokola a je již přežitý. Stejně se v něm dnes zobrazuje zejména reklama.

Proč by po mně šel nějaký HackingTeam?

Malware ve svém mobilu/tabletu/počítači nechcete, ale proč by právě po vás šel nějaký HackingTeam nebo PČR, která používá jejich SW?
Nemusí, stačí že používáte Wi-Fi..

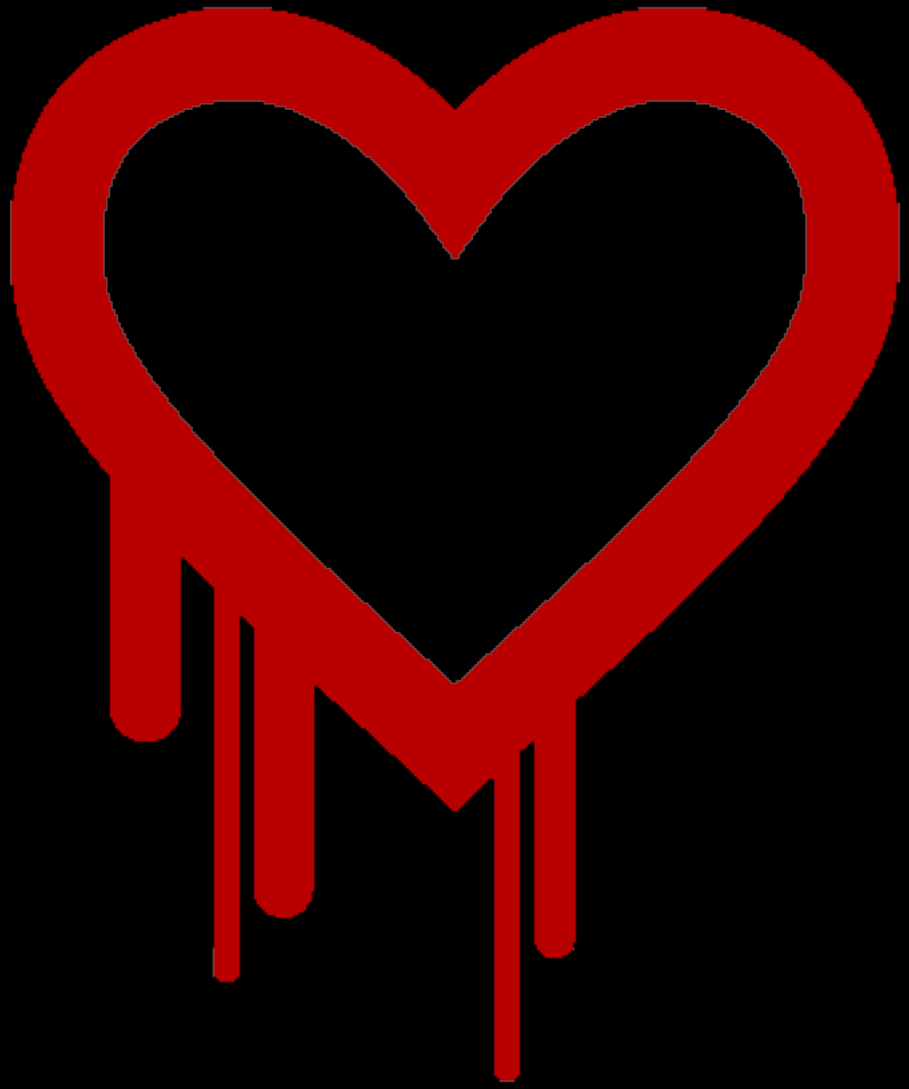
Tato krabička za $99 zjistí, k jakým Wi-Fi sítím je vaše zařízení ochotno se připojit a obratem takovou vytvoří. Na nic neklikáte, nic nepotvrzujete, stačí být jen v její blízkosti. Následně lze provádět všechny myslitelné MITM útoky.



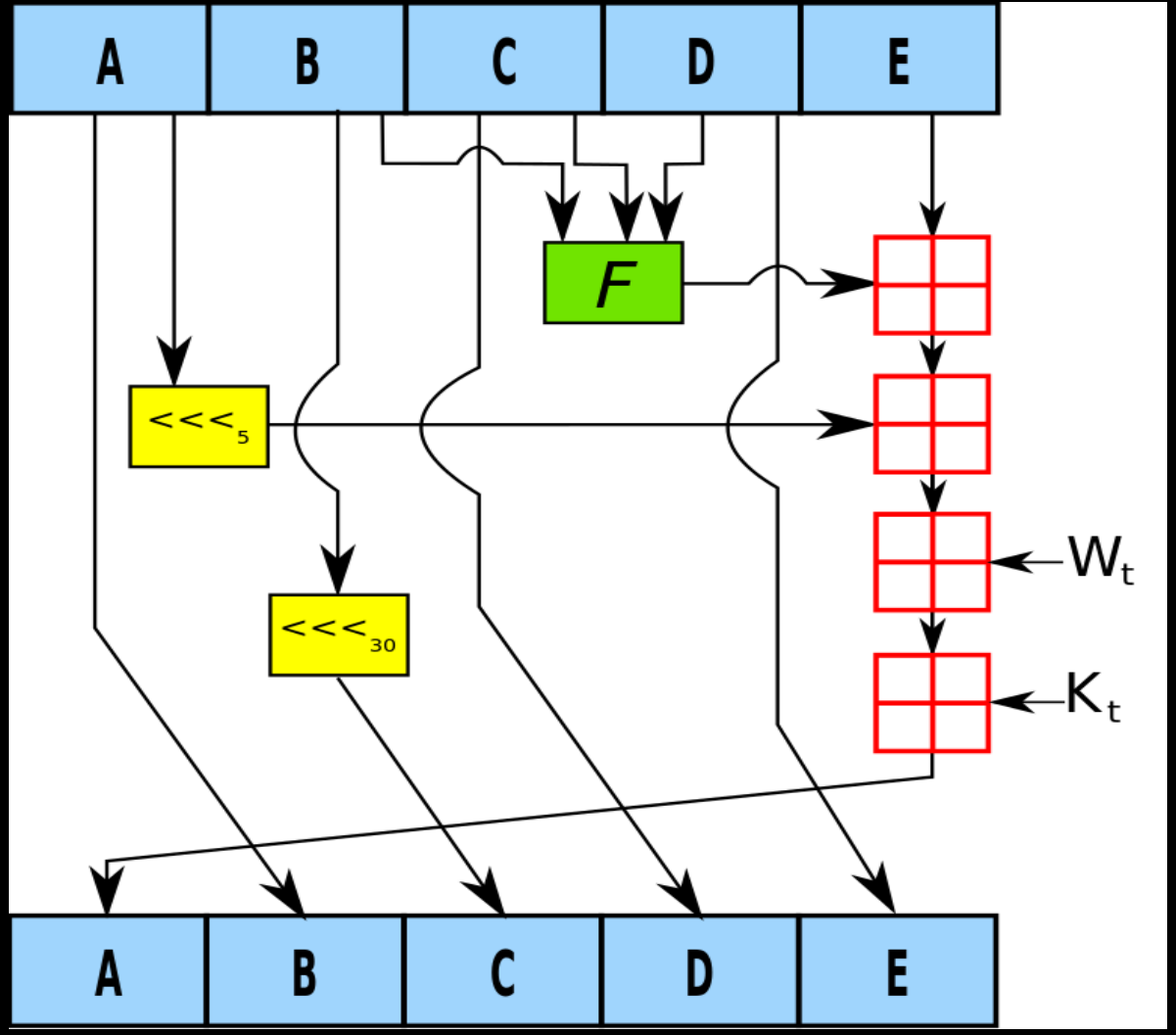
Řešením by bylo, kdyby prohlížeče používaly jen HTTPS. Chrome dnes zvýrazňuje weby, které mají na HTTPS slabý certifikát. Paradoxně ale neoznačuje weby, které nemají vůbec žádné zabezpečení. Zřejmě je to ale jen otázka času.

Vždyť SSL je také plné chyb..

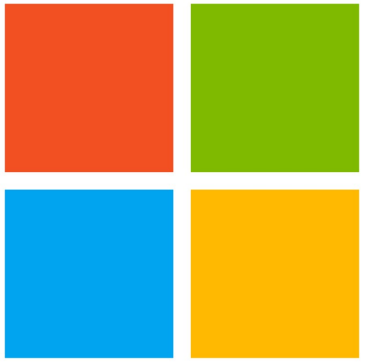
I v SSL implementacích, protokolech a šifrovacích algoritmech jsou chyby a slabiny. Pojďme se podívat na několik těch nedávných.



Bezprecedentní chyba HeartBleed v OpenSSL umožňovala vzdáleně získat fragmenty paměti serveru a tedy i privátní klíč komunikace a to bez jakékoliv stopě po této aktivitě. Kromě záplatování bylo nutné vyměnit certifikáty včetně klíčů.



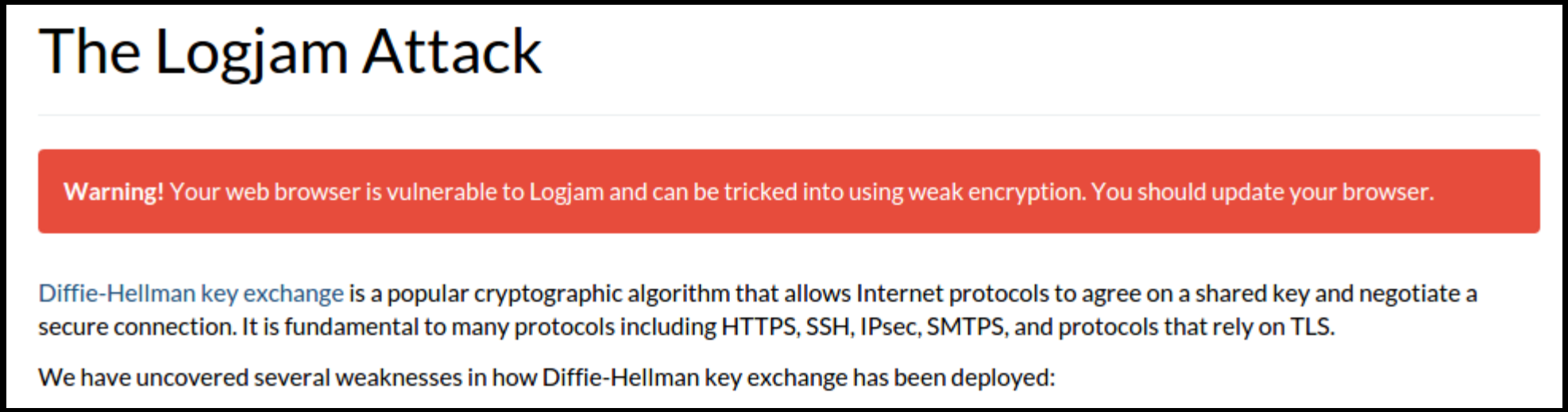
Algoritmus SHA-1, který byl nejrozšířenějším algoritmem pro ověřování SSL certifikátů, je dnes již slabý a nelze ho považovat za bezpečný. Nahrazuje se algoritmem SHA-256. Weby s SHA-1 certifikátem jsou označovány jako nezabezpečené. Kdo tedy po HeartBleed nasadil nový SHA-1 certifikát, mohl jej měnit znovu.



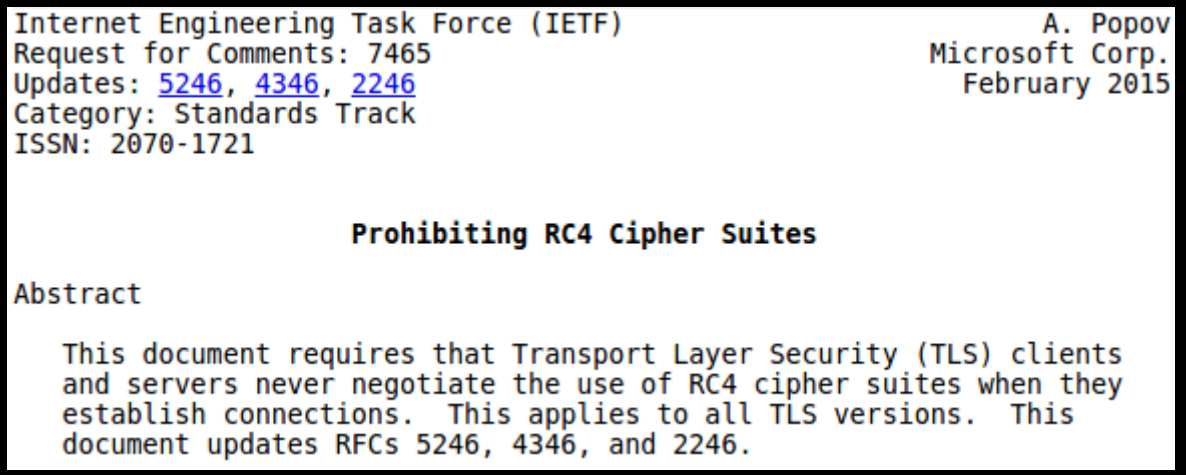
SChannel

Chyby se nevyhýbaly ani komerčním platformám. SSL implementace ve Windows (SChannel) obsahovala závažnou remote-code-execution chybu.

Chyba POODLE se netýkala implementace, ale samotného SSL 3.0 protokolu, který byl sice starý, ale stále hojně užívaný. Po zveřejnění se tato verze protokolu velice rychle přestala používat. (Kéž by stejně rychle zmizel Flash po kauze HackingTeam..)



Útok nazvaný Logjam využíval zranitelností v implementacích výměny klíčů metodou Diffie-Hellman. Kromě HTTPS se týká i protokolů jako SSH nebo různé VPN implementace. Bylo nutné aktualizovat SW tak, aby mohl používat delší a náhodně generované DH parametry.



Internet Engineering Task Force (IETF) — A. Popov
Request for Comments: 7465 — Microsoft Corp.
Updates: 5246, 4346, 2246 — February 2015
Category: Standards Track
ISSN: 2070-1721

Prohibiting RC4 Cipher Suites

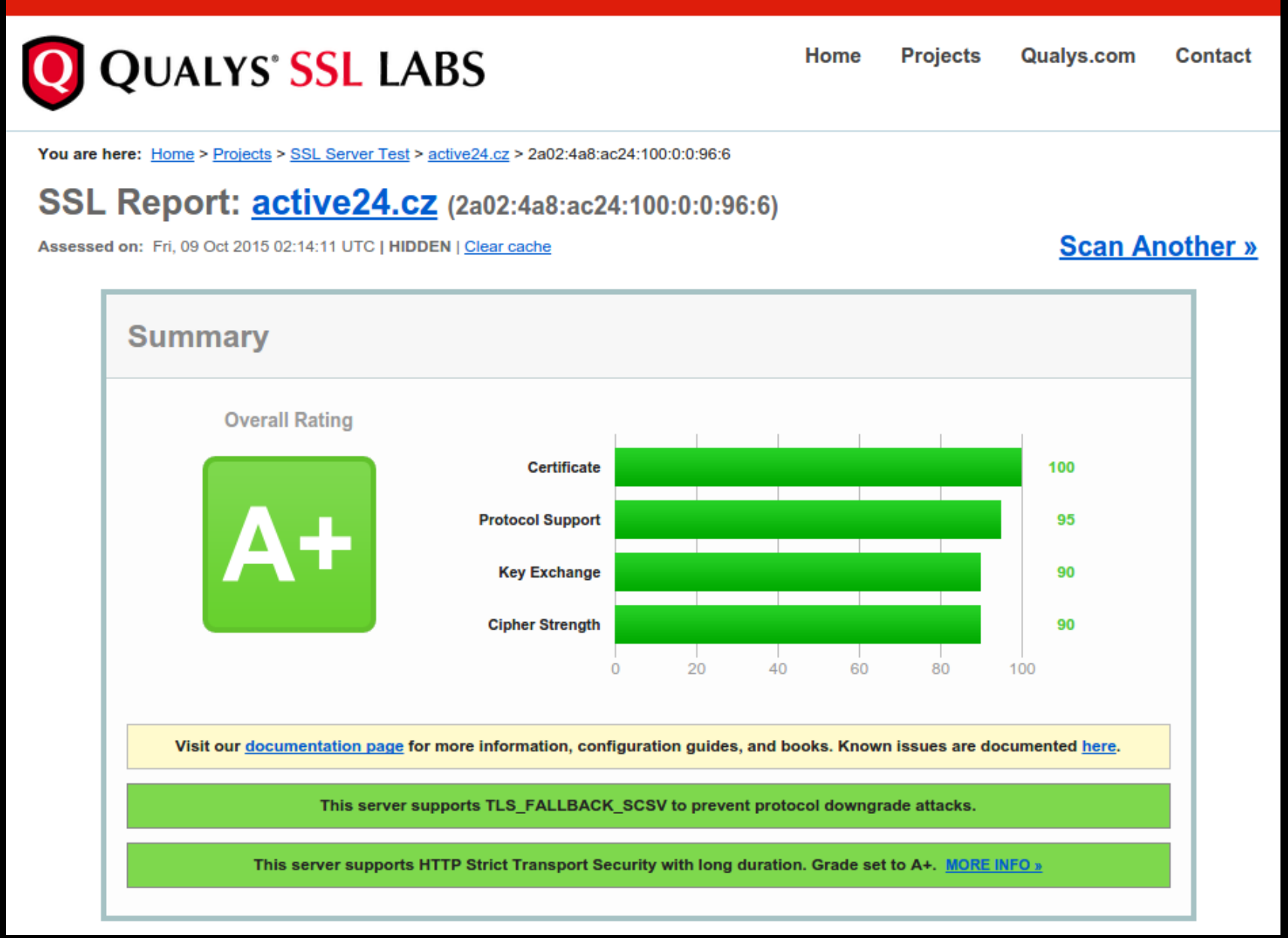
Abstract

This document requires that Transport Layer Security (TLS) clients and servers never negotiate the use of RC4 cipher suites when they establish connections. This applies to all TLS versions. This document updates RFCs 5246, 4346, and 2246.

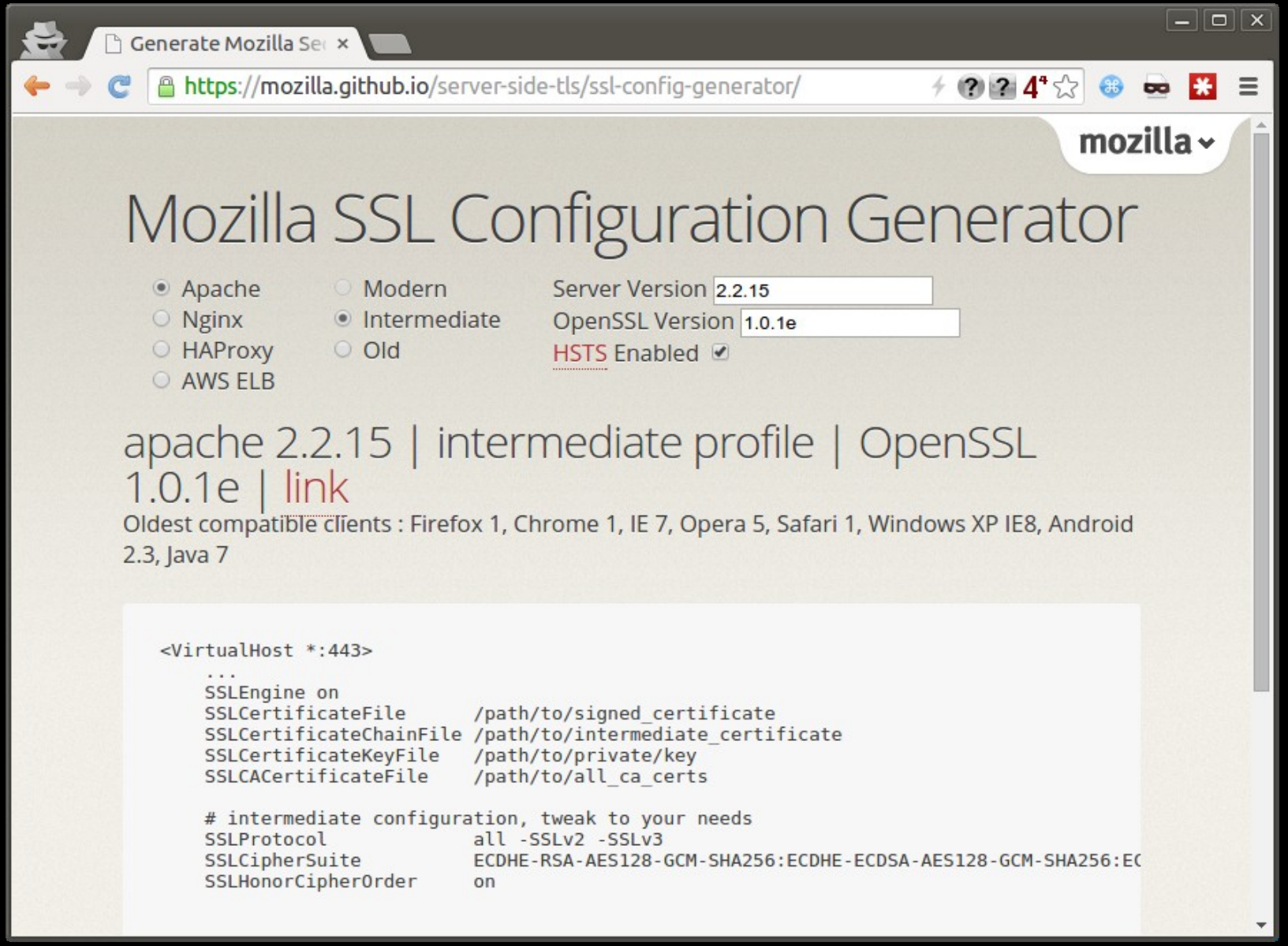
V hojně využívané šifrovací sadě RC4 bylo nalezeno několik slabin, a tak byla tato šifra označena jako slabá a nevhodná k zabezpečení komunikace.

OK, tak jak to správně nastavit?

Když je v SSL tolik chyb, jak to tedy nastavit a kde zjistím, že to mám nastaveno správně?



Velký pomocník je online nástroj ssllabs.com od Qualys. Známkuje nastavení šifer na vašem HTTPS podobně, jako se známkují pračky a ledničky v obchodech. Hodnocení je průběžně aktualizováno podle aktuálních znalostí. Jednou za čas se určitě sami otestujte.



Někdy může být složité na serveru konkrétní šifry správně nastavit.
Můžete proto použít tento nástroj, který vhodnou konfiguraci vygeneruje.

OK, mám A. Teď mohu být v klidu?

Takže když mám na SSL Labs známku „A“ a
veškerý HTTP provoz přesměrovávám na HTTPS,
tak už mi MITM útoky nehrozí?

Bohužel hrozí – problém je v tom úvodním přesměrování, které MITM může zachytit a udržet vás na nešifrovaném spojení. Říká se tomu SSL Stripping. Když zadáme adresu do prohlížeče, obvykle neuvádíme protokol a prohlížeč tedy použije HTTP. Na HTTPS nás přesměruje až následná odpověď serveru, kterou útočník může zachytit a modifikovat.

HSTS

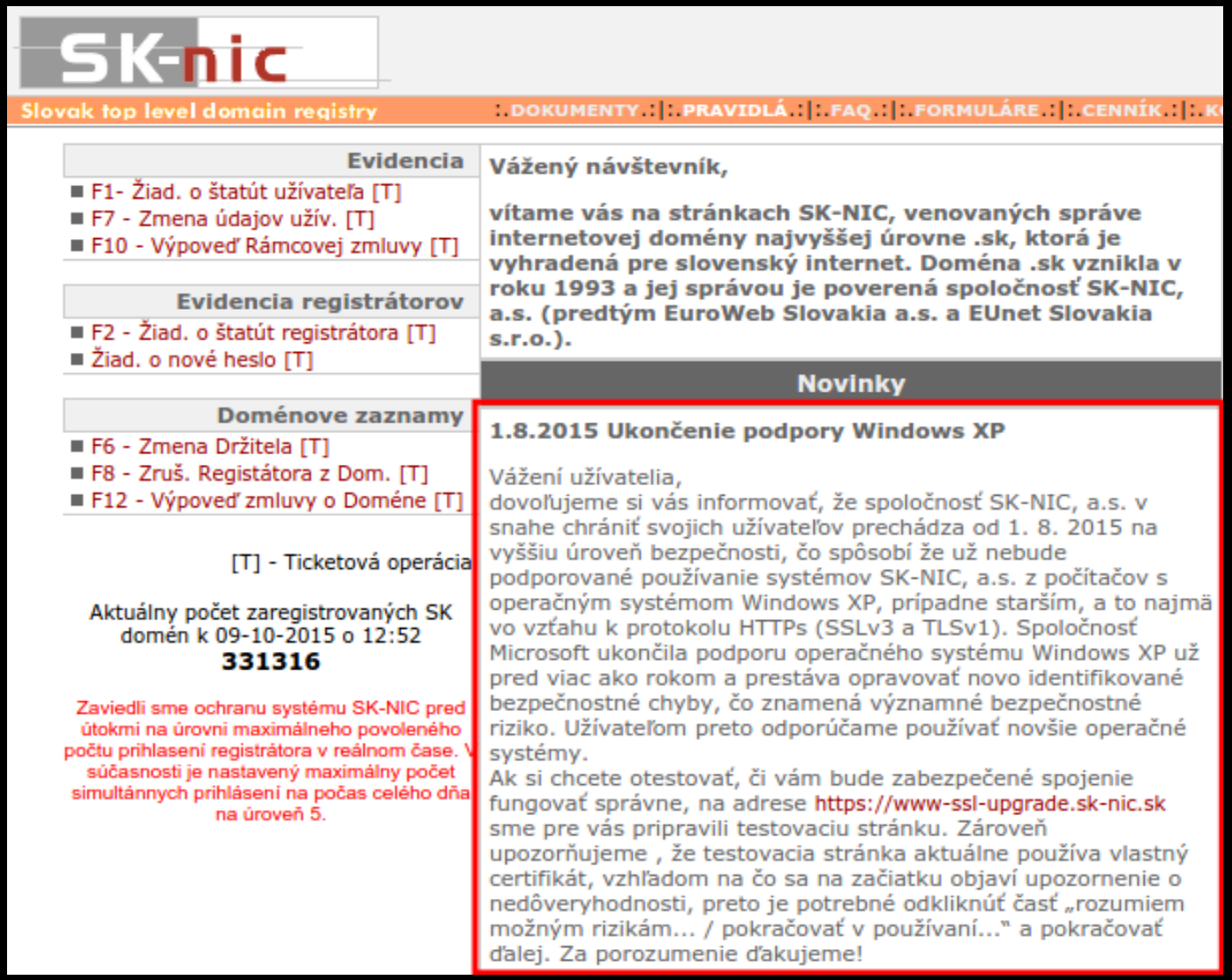
Řešením je HTTP Strict Transport Security, které vašemu prohlížeči říká, že má web načítat rovnou po HTTPS a na HTTP se vůbec nedotazovat. Tuto informaci si prohlížeč zapamatuje ihned po první návštěvě takto zabezpečeného webu. Pokud nastavíte, aby si to prohlížeče pamatovaly alespoň půl roku, SSL Labs vás odmění známkou „A+“.

Fajn, tak jdeme na A+

A jak tedy HSTS nastavit?

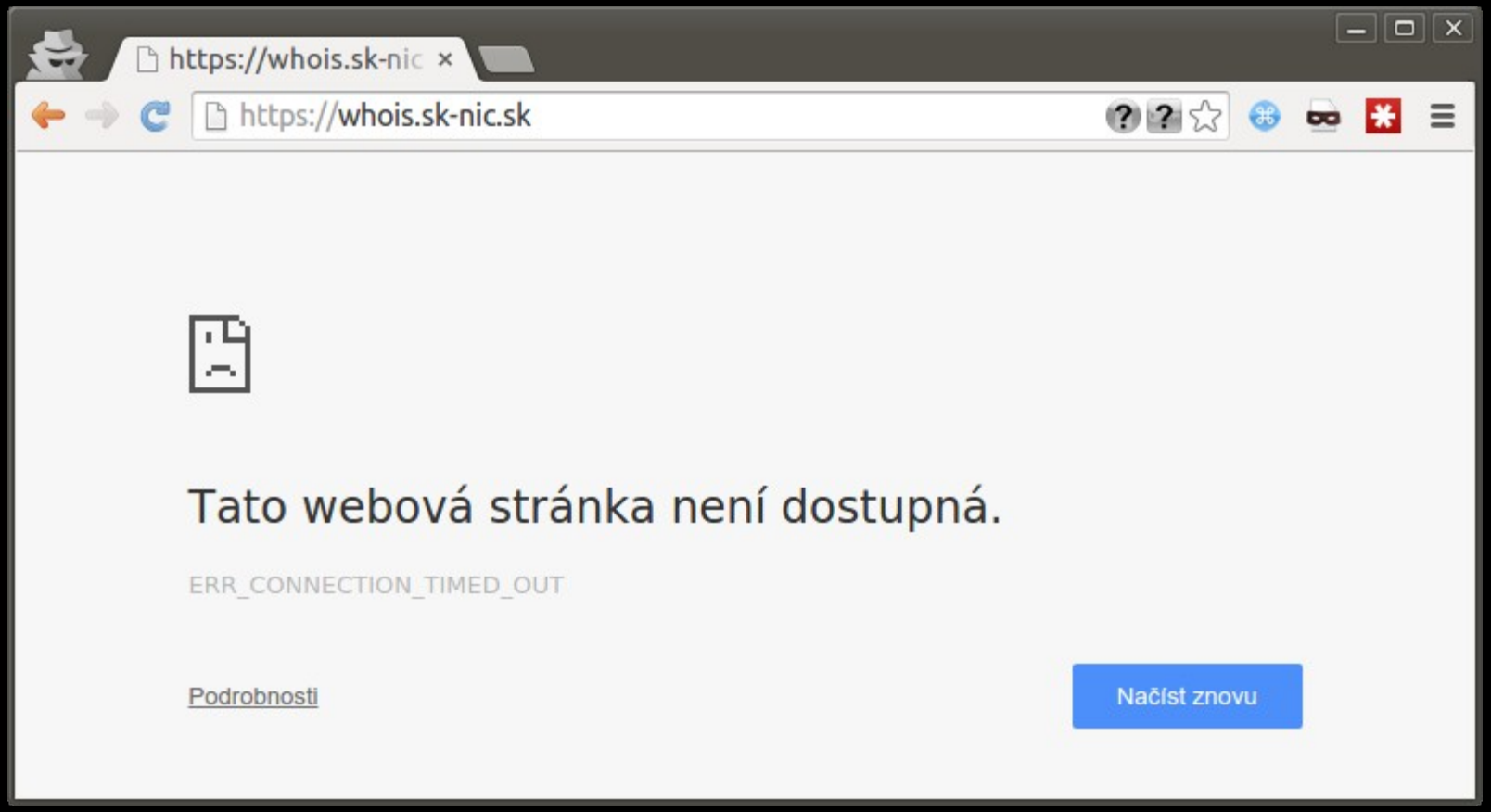
```
Strict-Transport-Security "max-age=15768000; IncludeSubdomains; Preload"
```

Pokud budete googlovat, jak HSTS nastavit, najdete pravděpodobně něco podobného tomuto. Ale velký pozor, takhle to nedělejte!



Např. v SK-NIC si chtěli také SSL lépe nastavit a zřejmě také googlovali. Nasadili pak HSTS včetně IncludeSubdomains, tedy na všech subdoménách pod sk-nic.sk.

Testovací doména s nevalidním certifikátem, kde si lidé měli novou konfiguraci otestovat, se tak stala nedostupnou. Se zapnutým HSTS již není možné hlášení o nevalidním certifikátu přeskočit!
Web se tak stává zcela nedostupný, dokud nedodáte validní certifikát.



Služba whois na doméně whois.sk-nic.sk se stala taktéž nedostupnou, protože vůbec na HTTPS neběží. HSTS vás na nezabezpečenou variantu webu nepustí.

Protocols	
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

Vzpomínáte, že oznamovali ukončení podpory pro Windows XP? Udělali to tak, že zakázali všechny protokoly kromě nejnovějšího TLS 1.2.

Android 2.3.7 No SNI [2]	Protocol or cipher suite mismatch		Fail[3]
Android 4.0.4	Protocol or cipher suite mismatch		Fail[3]
Android 4.1.1	Protocol or cipher suite mismatch		Fail[3]
Android 4.2.2	Protocol or cipher suite mismatch		Fail[3]
Android 4.3	Protocol or cipher suite mismatch		Fail[3]
Android 4.4.2	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) FS	256
Android 5.0.0	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Baidu Jan 2015	Protocol or cipher suite mismatch		Fail[3]
BingPreview Jan 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) FS	256
Chrome 43 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Firefox 31.3.0 ESR / Win 7	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Firefox 39 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Googlebot Feb 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
IE 6 / XP No FS [1] No SNI [2]	Protocol or cipher suite mismatch		Fail[3]
IE 7 / Vista	Protocol or cipher suite mismatch		Fail[3]
IE 8 / XP No FS [1] No SNI [2]	Protocol or cipher suite mismatch		Fail[3]
IE 8-10 / Win 7 R	Protocol or cipher suite mismatch		Fail[3]
IE 11 / Win 7 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
IE 11 / Win 8.1 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
IE 10 / Win Phone 8.0	Protocol or cipher suite mismatch		Fail[3]
IE 11 / Win Phone 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 11 / Win Phone 8.1 Update R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
Edge 12 / Win 10 (Build 10130) R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) FS	256
Java 6u45 No SNI [2]	Protocol or cipher suite mismatch		Fail[3]
Java 7u25	Protocol or cipher suite mismatch		Fail[3]

Výsledkem je celá plejáda klientů, kteří se na tento web už nepodívají.

```
Strict-Transport-Security "max-age=15768000; IncludeSubdomains; Preload"
```

Z SK-NIC si tedy příklad neberte. Jak nastavit šifry poradí dříve zmíněný Mozilla SSL Configuration Generator. A u HSTS začněte bez dlouhého max-age, bez IncludeSubdomains a bez Preload.

```
Strict-Transport-Security "max-age=900"
```

Začněte např. s 15 minutovým max-age, který lze v tomto čase zase vypnout, pokud se objeví nečekané potíže. Řešit budete muset zejména tzv. mixed-content, kdy stránka načítaná po HTTPS obsahuje prvky načítané po HTTP.

```
Strict-Transport-Security "max-age=86400"
```

Po odladění můžete čas zvýšit např. na 24 hodin a čekat, jestli vám někdo neohlásí problém, kvůli kterému byste museli HSTS ještě vypínat.

```
Strict-Transport-Security "max-age=604800"
```

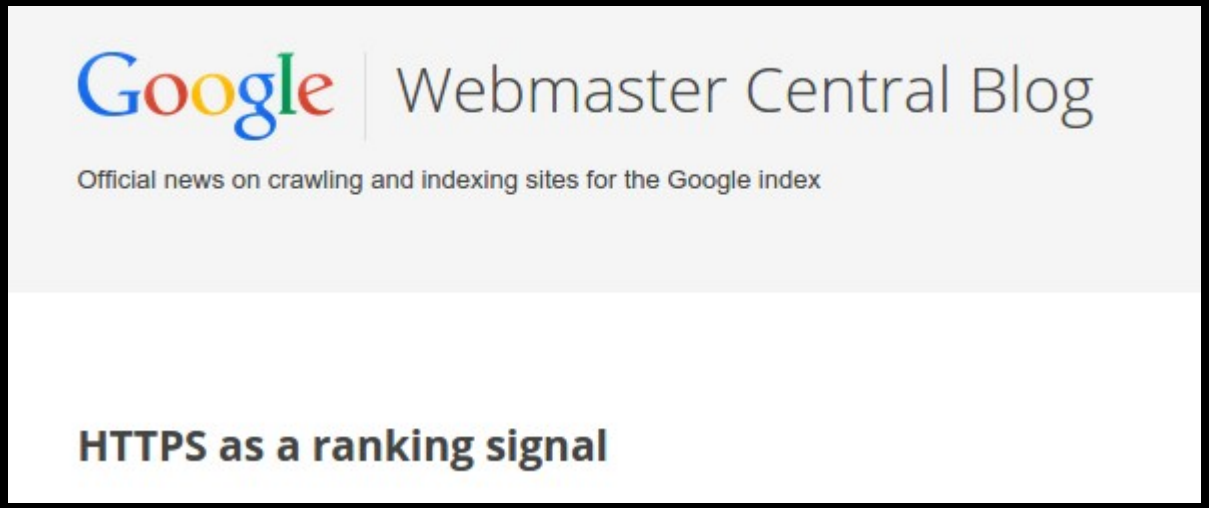
Pak zvyšte dejme tomu na týden a čekejte i několik týdnů, jestli nepřijde report chyby. Někdy to může trvat, než se problém od uživatelů dostane až k vám.

```
Strict-Transport-Security "max-age=15768000"
```

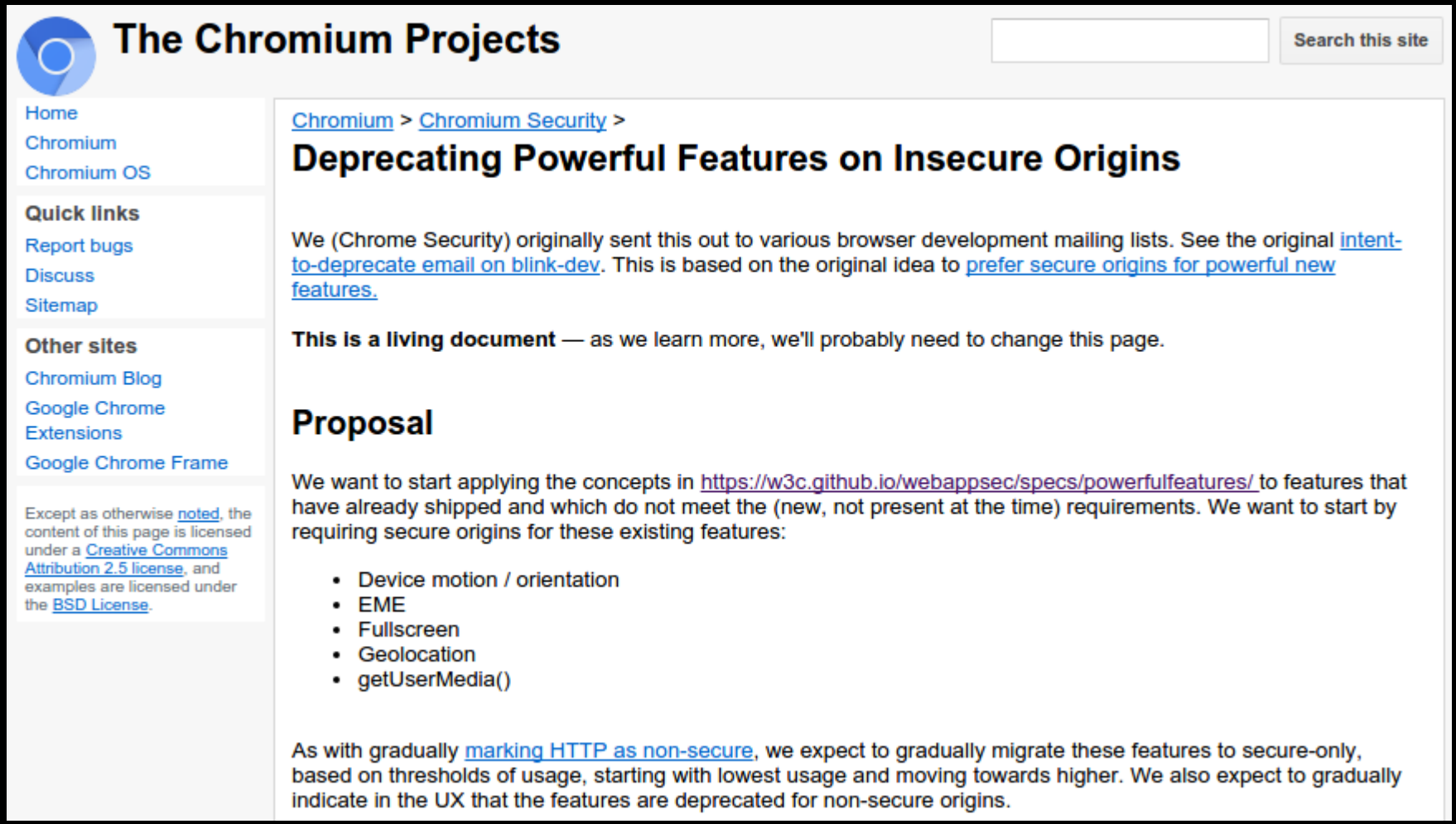
A když už to běží třeba měsíc bez potíží, nastavte teprve ten požadovaný půlrok a radujte se z „A+“ známky na SSL Labs.

IncludeSubdomains a Preload používajte až tehdy, když víte přesně, co děláte a že jste nezapomněli na žádnou subdoménu, které se to může týkat.

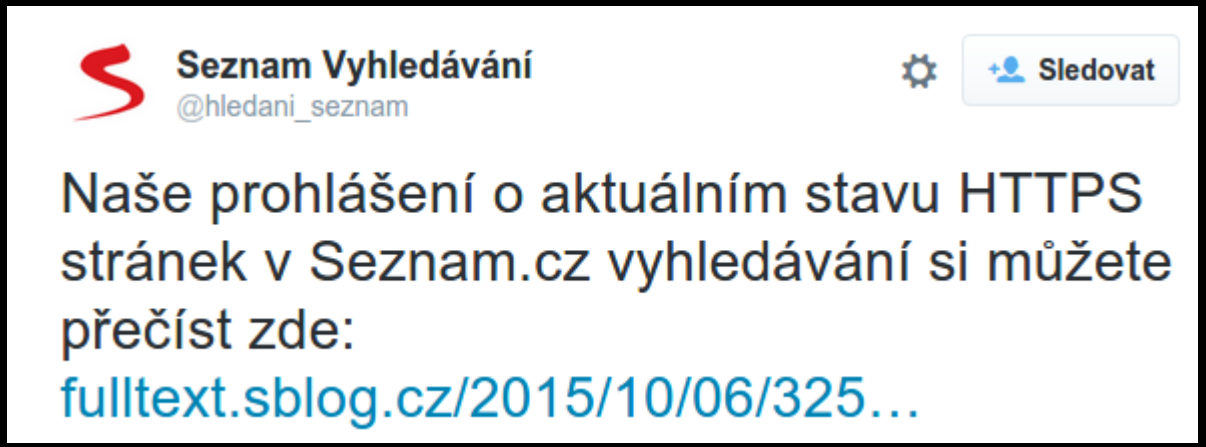
A když přejdu na HTTPS, nepropadnu se ve vyhledávačích?



Google vás za takový přechod naopak odmění mírným zvýhodněním webu. Ale spíše to ani nepoznáte – hlavním SEO signálem je stále obsah webu.



Kromě vyhledávání je dobré vědět, že bez HTTPS nebudete moci využívat některé služby Googlu ve své aplikaci, např. geolokaci. Seznam takových služeb se bude rozšiřovat.

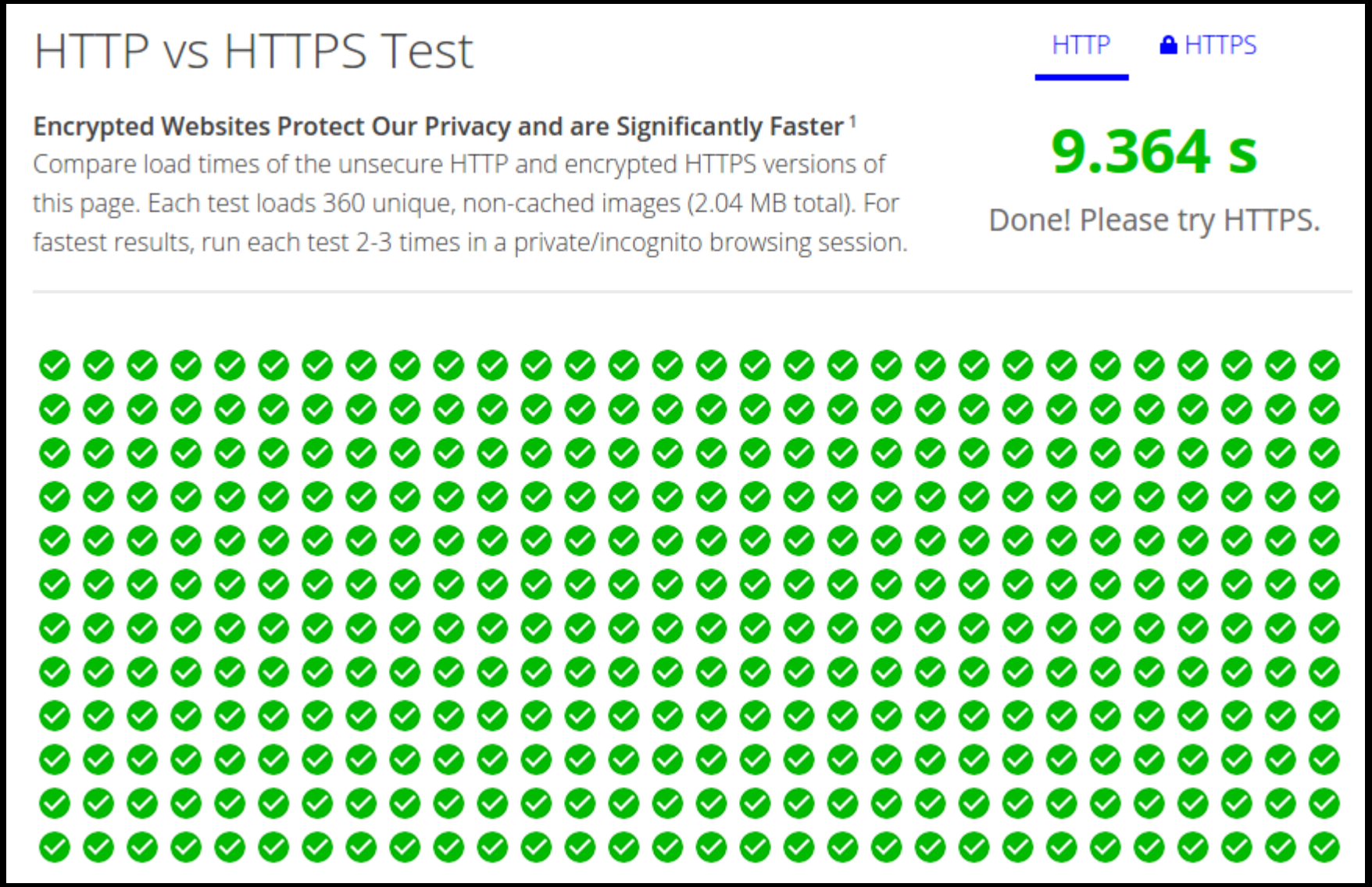


Seznam nedávno vydal prohlášení, že k webům na HTTP a HTTPS se již chová naprosto stejně a přechod z HTTP na HTTPS má stejný vliv, jako přechod na jinou doménu pomocí přesměrování. K dočasnému propadu tedy dojít může, ale pokud nejste životně závislí na výsledcích vyhledávání na Seznamu, s přechodem na ně nečekejte. U nových webů už není co řešit.

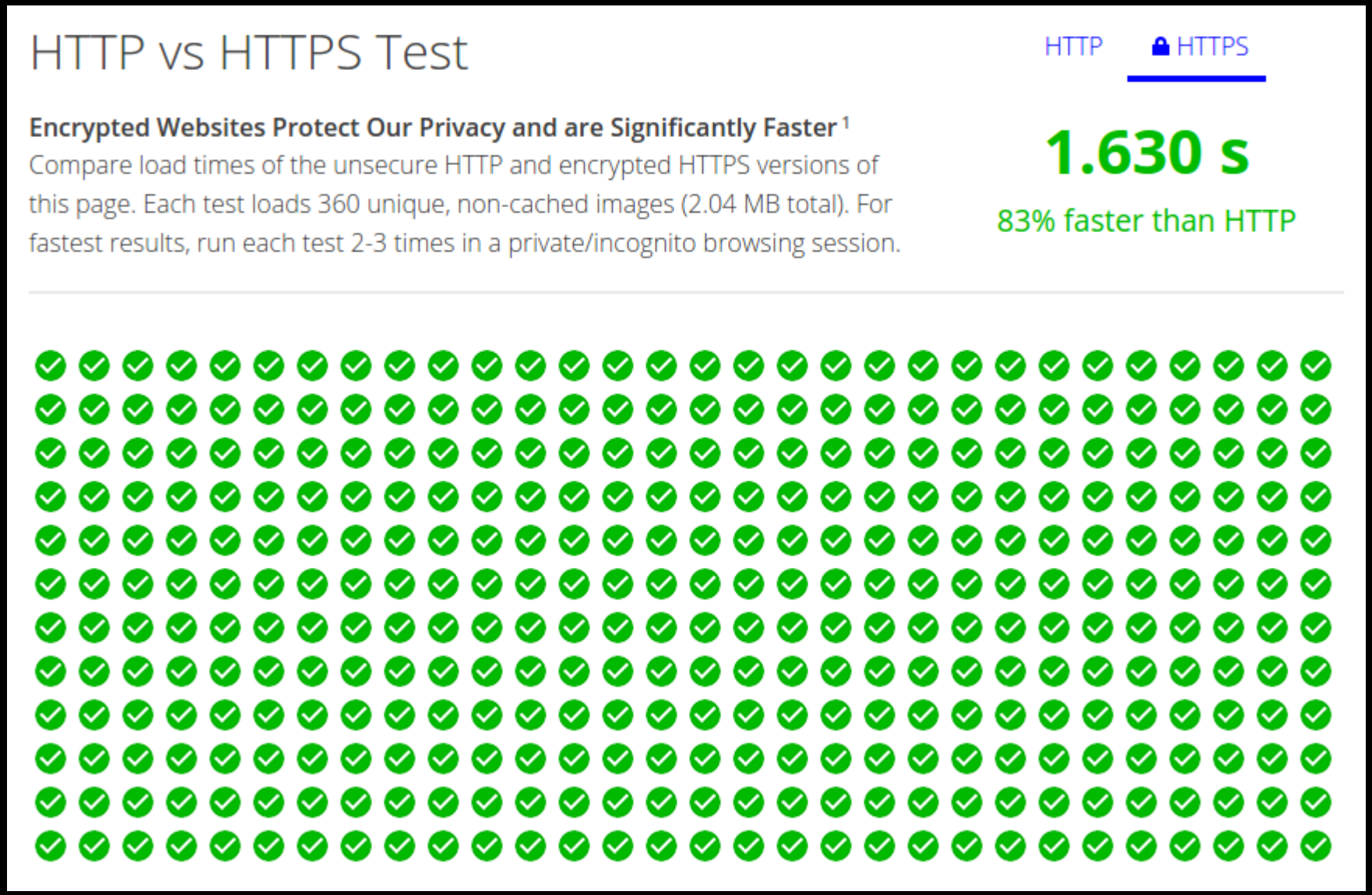
OK a kromě bezpečnosti má HTTPS nějaké výhody?

HTTP/2

Na HTTPS můžete využívat nový HTTP/2 protokol, který používá několik technik významně zrychlujících načítání stránek a to zejména na mobilech s pomalým připojením. Ačkoliv lze teoreticky HTTP/2 používat i nešifrovaně, v praxi to nikdo nedělá a prohlížeče i servery používají nový protokol jen na HTTPS.

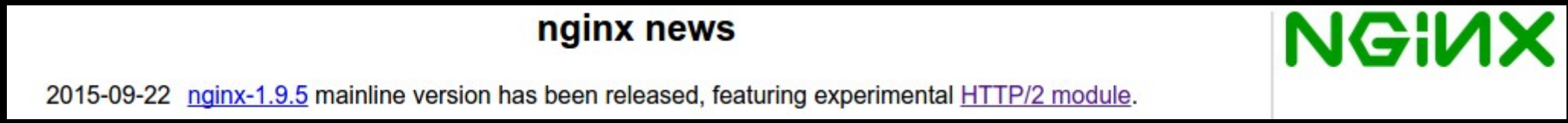


Takhle vypadá načítání mnoha malých obrázků po stávajícím HTTP/1.1

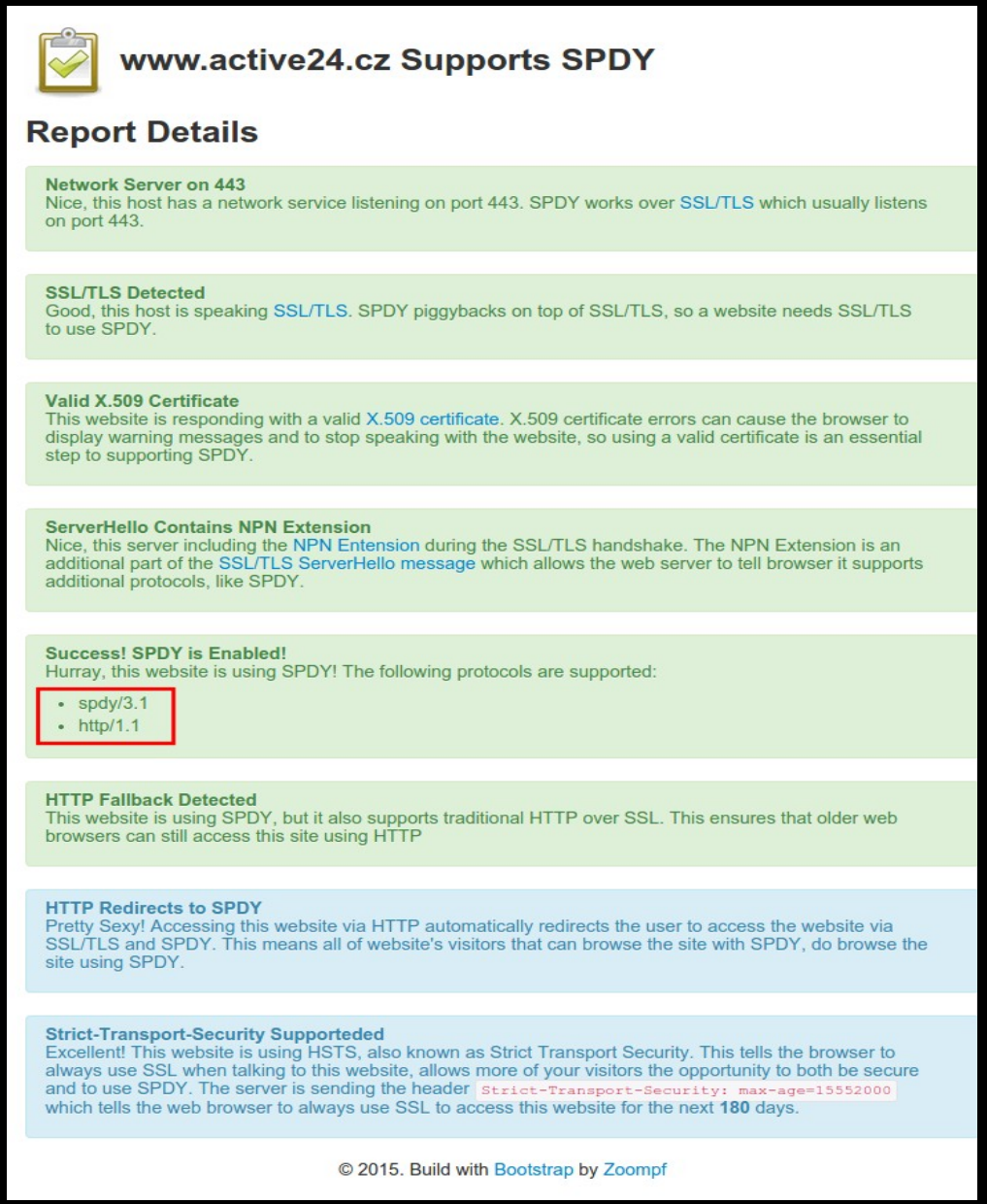


A takhle po HTTPS s HTTP/2.

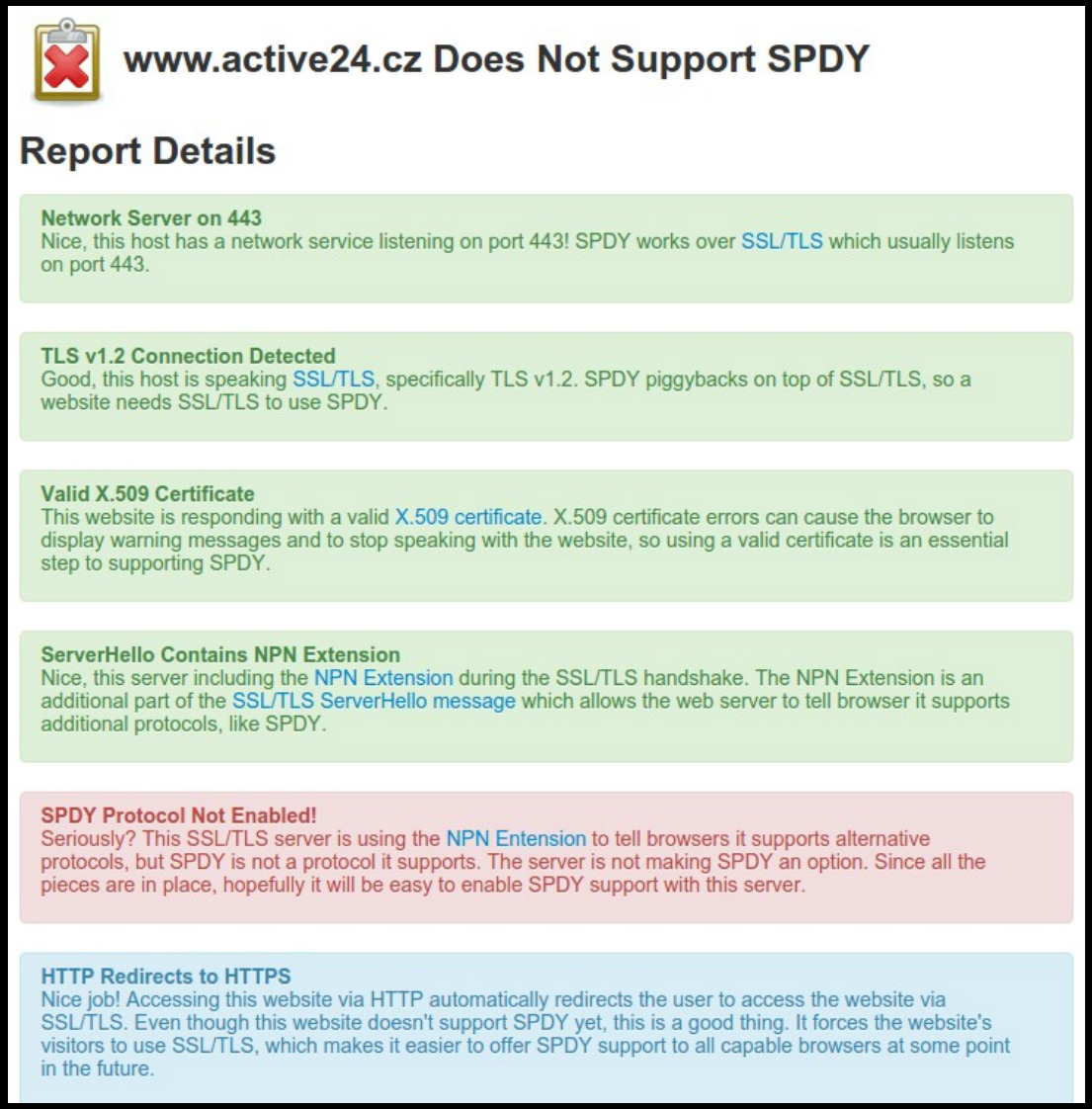
A on už to někdo podporuje?



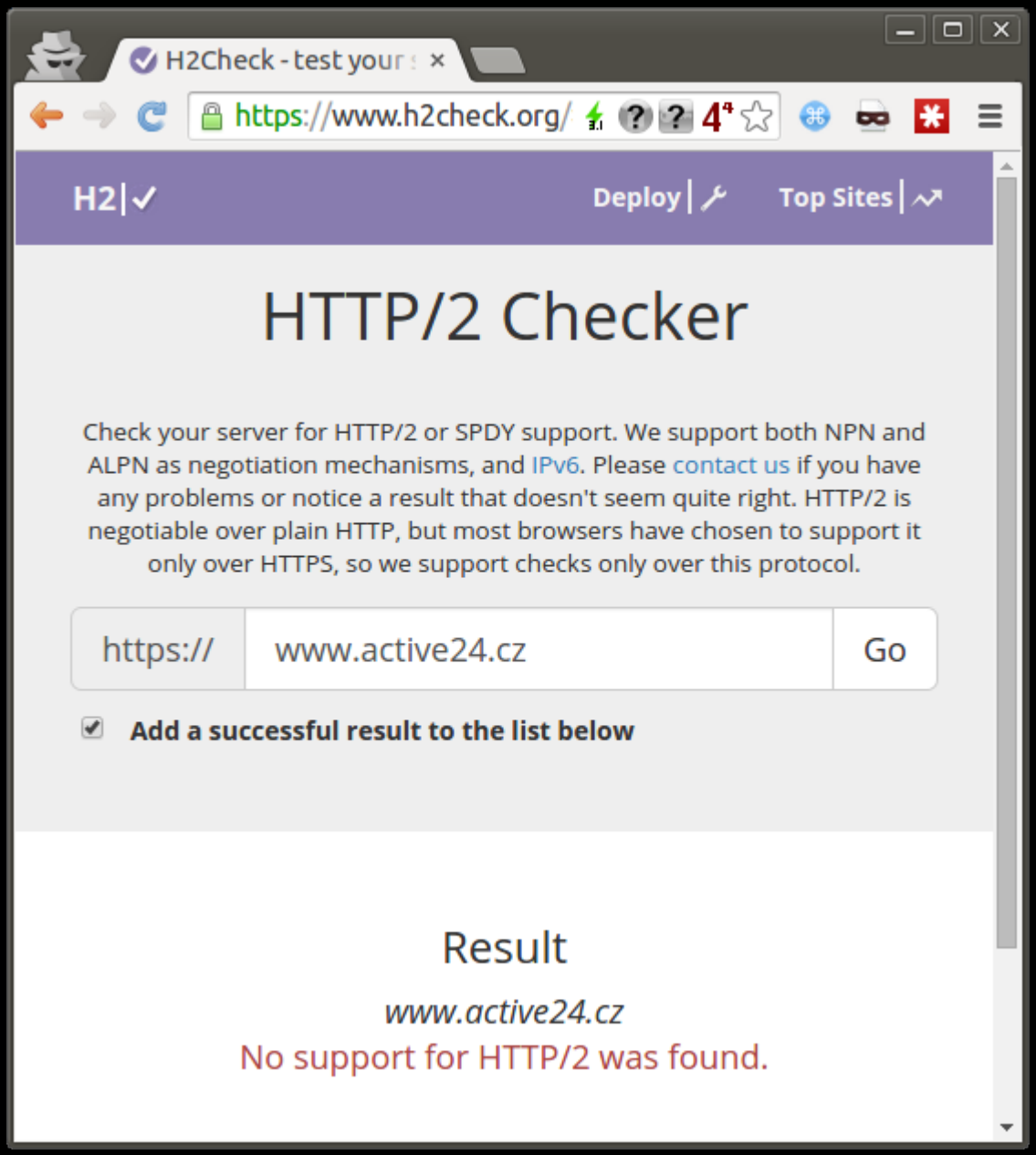
Prohlížeče to podporují už dávno, servery donedávna jen u velkých providerů jako Google či Twitter. Od konce září je ale podpora v serveru Nginx. Do Apache existuje zatím neoficiální modul.



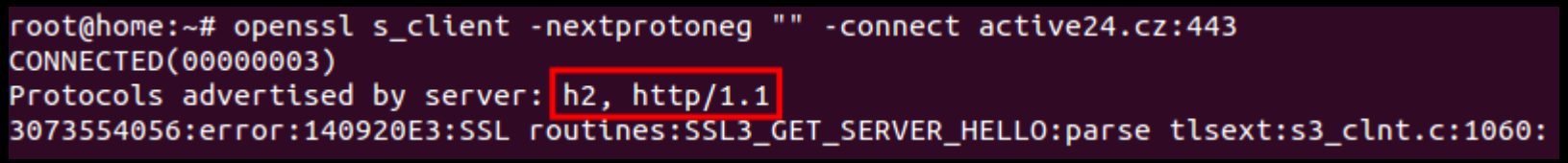
Takto jsme se chlubili podporu SPDY na konferenci Internet a Technologie 2015.



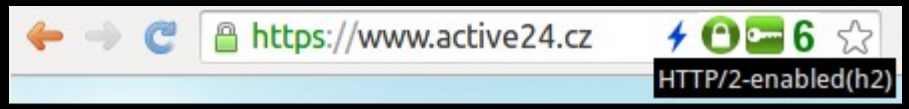
Dnes ten stejný test píše, že SPDY nepodporujeme. Je to vlastně pravda, protože podporujeme již jen HTTP/2.



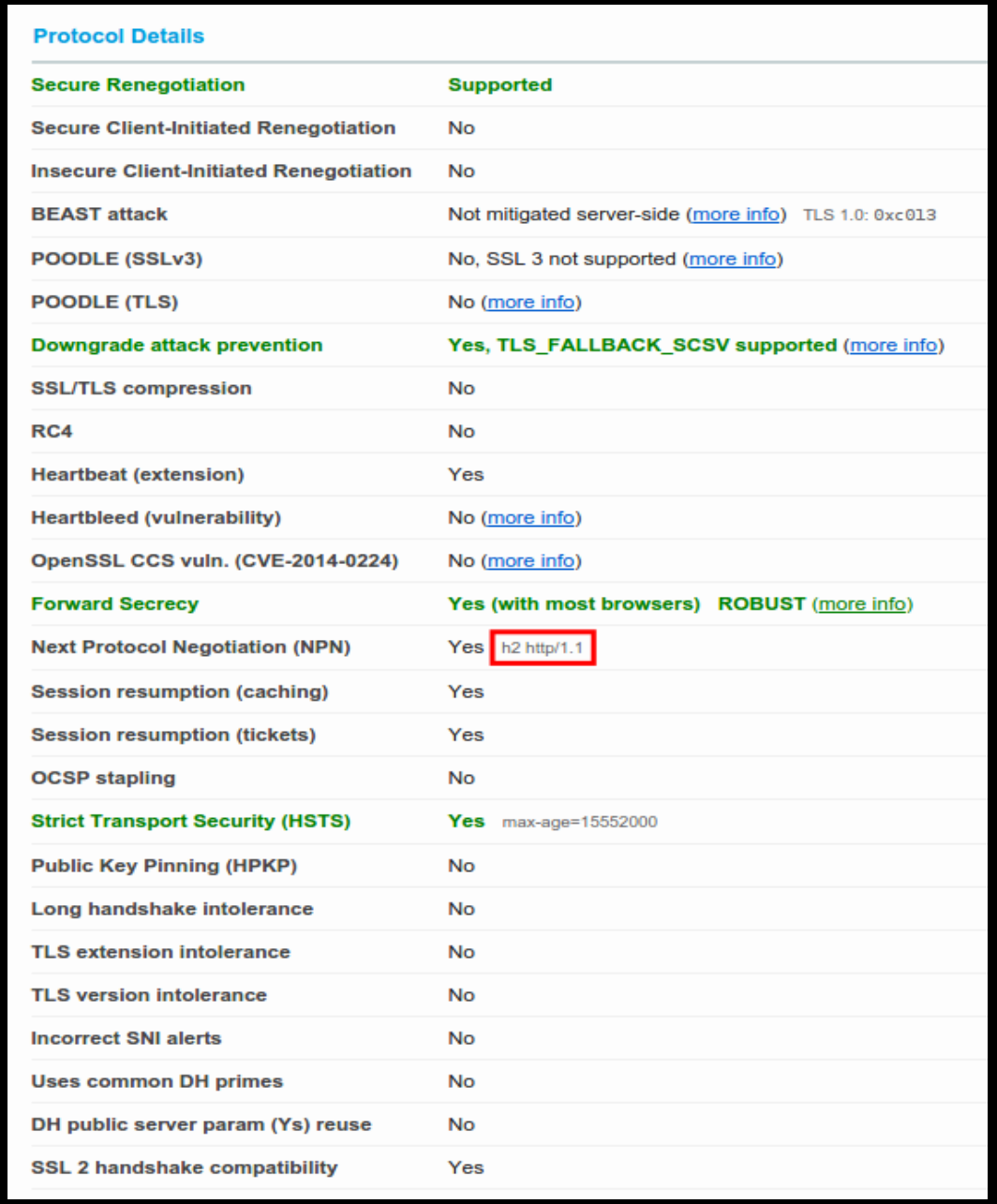
Horší je, že i HTTP/2 test ukazuje, že tento protokol nepodporujeme. To ale pravda není. Test jen bohužel nerozpozná poslední oficiální revizi tohoto protokolu, ale jen ty starší. Snad to brzy opraví.



Podporu HTTP/2 u nás tak můžete poznat např. takto pomocí OpenSSL klienta.



Nebo pomocí rozšíření „HTTP/2 and SPDY indicator“ v prohlížeči.



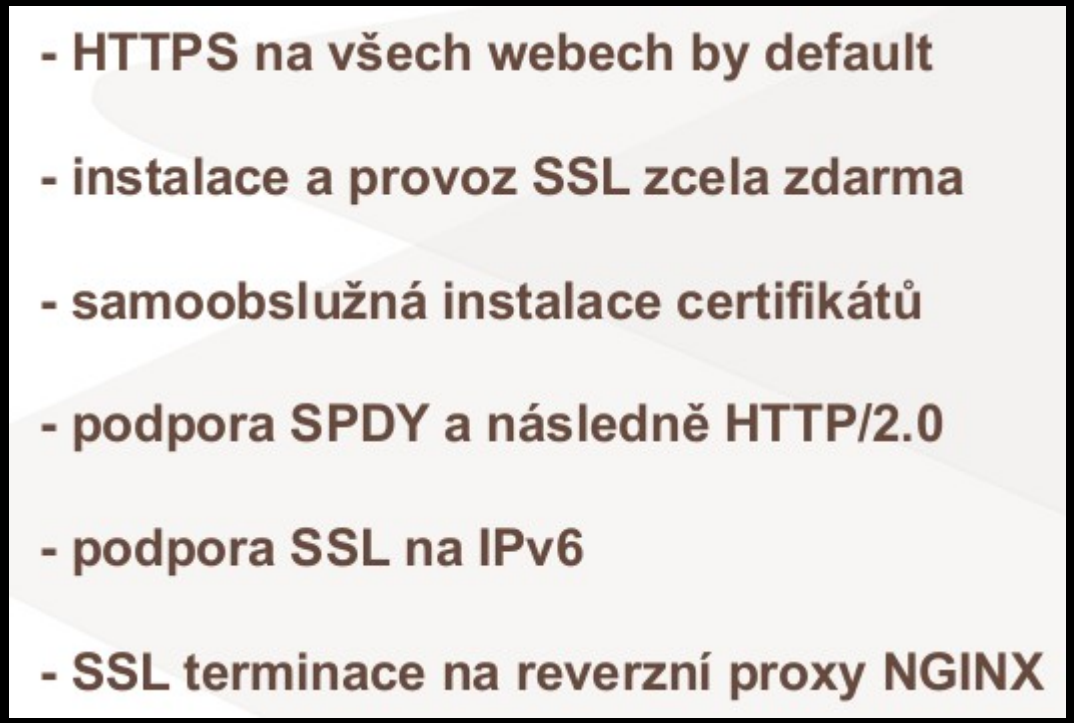
Protocol Details

Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc013
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	**Yes (with most browsers) ROBUST** (more info)
Next Protocol Negotiation (NPN)	Yes h2 http/1.1
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	**Yes** max-age=15552000
Public Key Pinning (HPKP)	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No
DH public server param (Ys) reuse	No
SSL 2 handshake compatibility	Yes

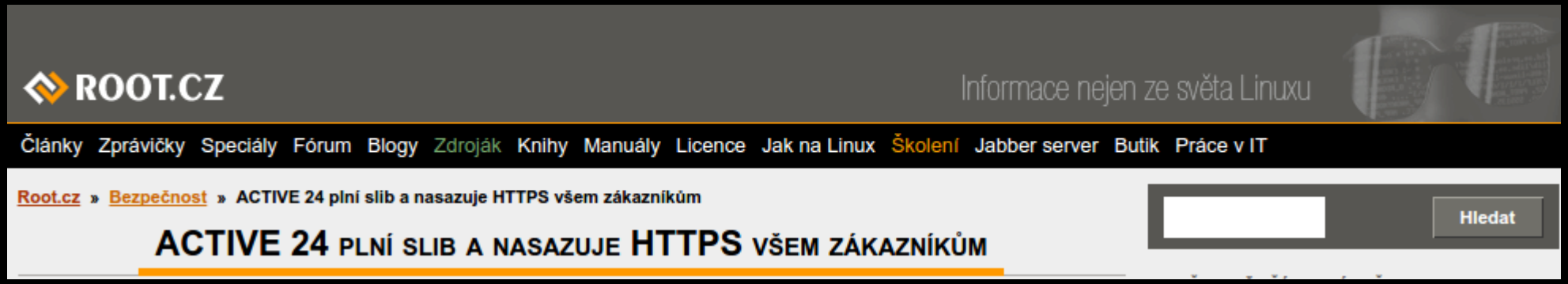
A nebo mnohokrát zmiňovaným SSL Labs testem.

Kolik mě to bude stát?

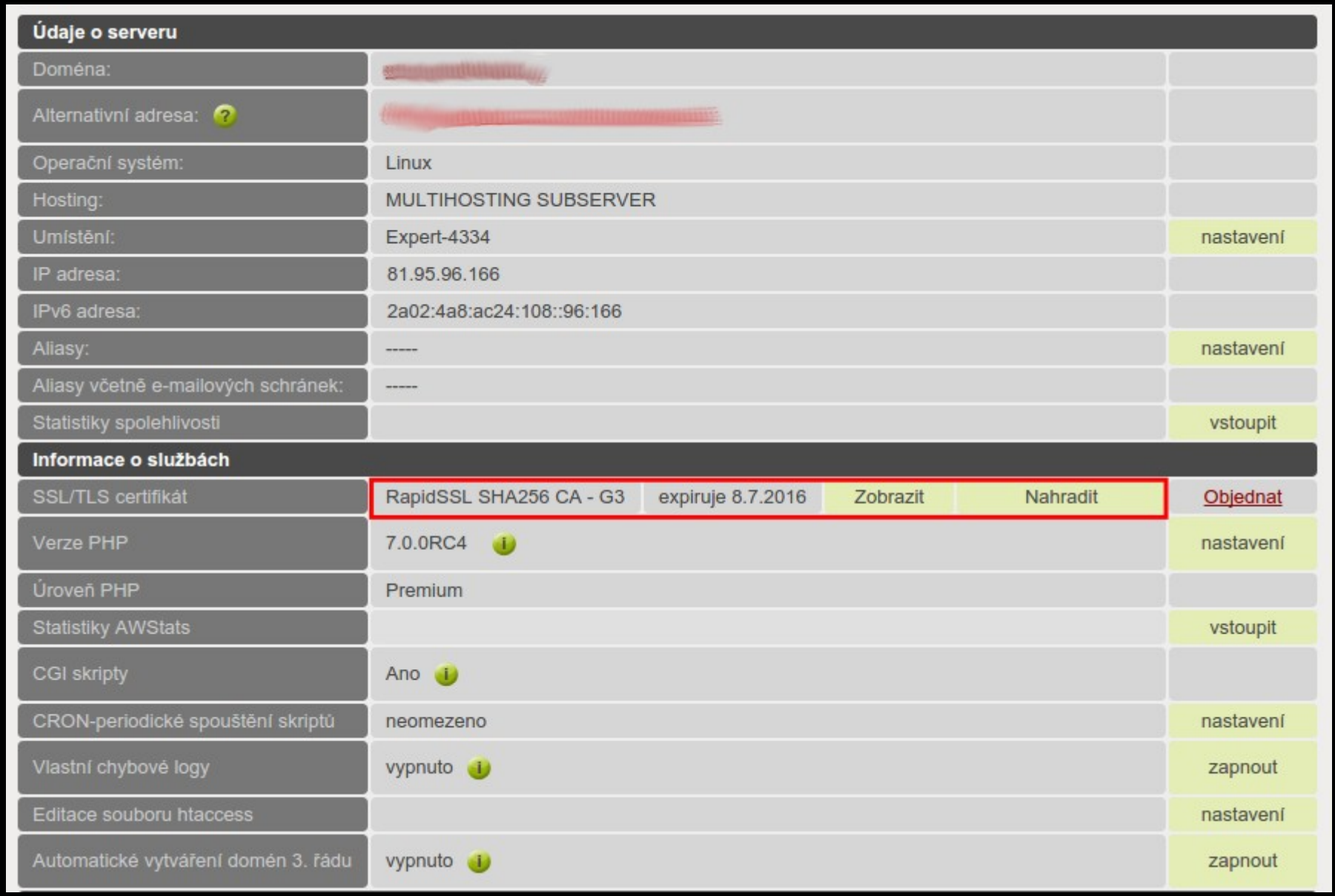
Bohužel záleží na tom, u koho budete HTTPS resp. HTTP/2 provozovat. Ve většině webhostingových společností je HTTPS stále příplatková služba.



V ACTIVE 24 věříme, že HTTPS má být zdarma dostupné všem v rámci základní služby a ne za příplatek jako opt-in služba. Toto jsme slibovali na konferenci Internet a Technologie 2015.



A co jsme slíbili, to také plníme. Každý web na našem Linux hostingu má HTTPS rovnou aktivní a to včetně HTTP/2 i na IPv6.



Údaje o serveru					
Doména:	[redacted]				
Alternativní adresa:	[redacted]				
Operační systém:	Linux				
Hosting:	MULTIHOSTING SUBSERVER				
Umístění:	Expert-4334				nastavení
IP adresa:	81.95.96.166				
IPv6 adresa:	2a02:4a8:ac24:108::96:166				
Aliasy:	-----				nastavení
Aliasy včetně e-mailových schránek:	-----				
Statistiky spolehlivosti					vstoupit
Informace o službách					
SSL/TLS certifikát	RapidSSL SHA256 CA - G3	expiruje 8.7.2016	Zobrazit	Nahradit	Objednat
Verze PHP	7.0.0RC4				nastavení
Úroveň PHP	Premium				
Statistiky AWStats					vstoupit
CGI skripty	Ano				
CRON-periodické spouštění skriptů	neomezeno				nastavení
Vlastní chybové logy	vypnuto				zapnout
Editace souboru htaccess					nastavení
Automatické vytváření domén 3. řádu	vypnuto				zapnout

Certifikáty si může zákazník sám aktualizovat dle potřeby přes naše zákaznické centrum. Buď si u nás CRT i koupí, nebo jen vygeneruje CSR a nebo uploaduje vlastní certifikát i s klíčem. Na takovém webu lze rovnou provozovat i poslední PHP 7.0.0 RC4 (default zůstává 5.6).

Validní certifikát lze dnes získat pro nekomerční účely zcela zdarma u Start SSL certifikační autority.

Nebo si počkejte na Let's Encrypt, kde už to bude zdarma pro všechny. Pokud se tyto certifikáty v praxi osvědčí, zákazníkům je rovnou zprostředkujeme.

A co když HTTPS i přesto všechno nechci?

Můžeme o tom diskutovat, můžeme s tím i nesouhlasit, ale to je tak všechno, co se proti tomu dá dělat…

Přechod z HTTP na HTTPS je realita, které se děje právě teď.
Má to své mouchy, které je potřeba řešit, ale přijměte to jako fakt.

Děkuji za pozornost!

www.active24.cz
@active24cz
@tomashala