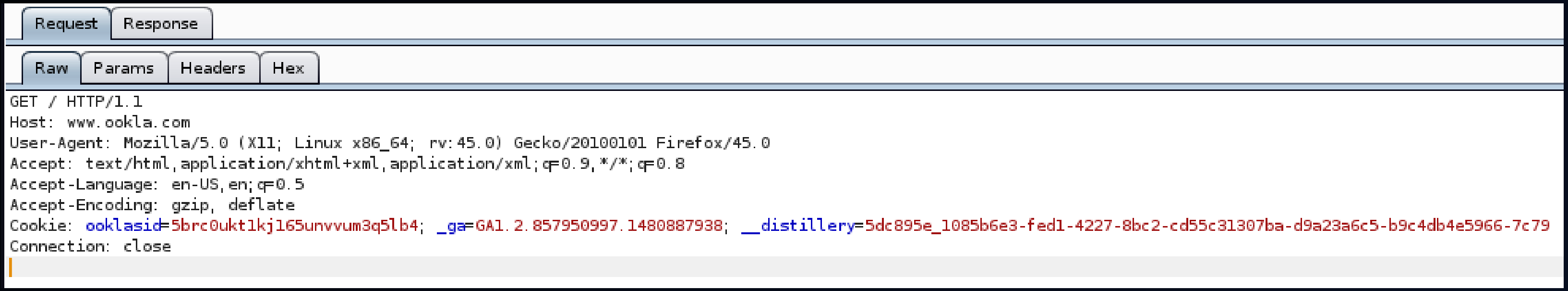
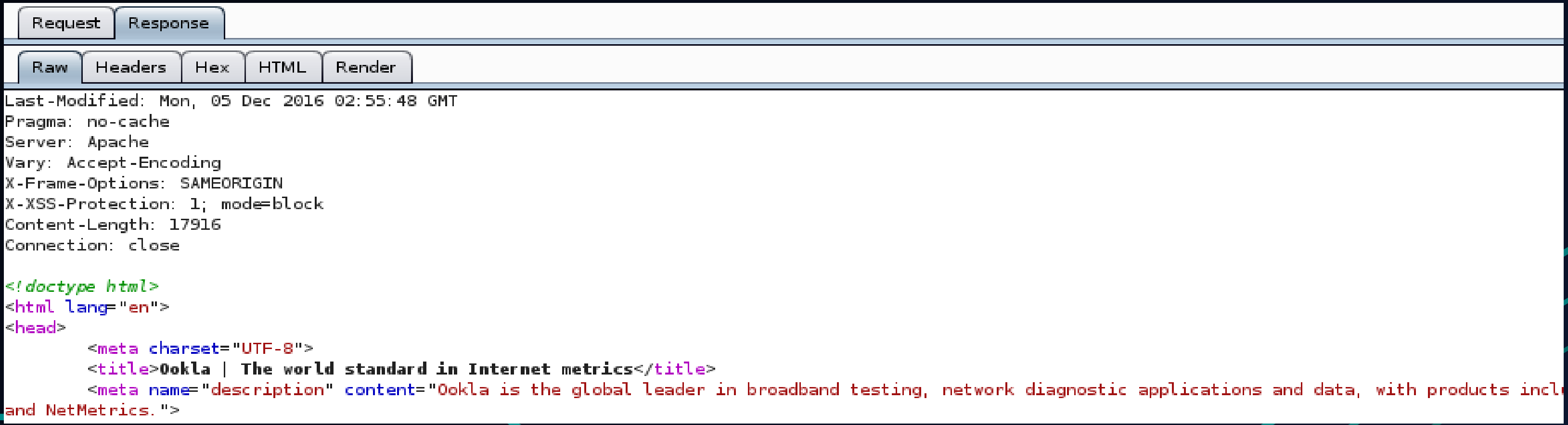


```
GET / HTTP/1.1
Host: www.ookla.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: ooklasid=5brc0ukt1kj165unvvum3q5lb4; _ga=GA1.2.857950997.1480887938; __distillery=5dc895e_1085b6e3-fed1-4227-8bc2-cd55c31307ba-d9a23a6c5-b9c4db4e5966-7c79
Connection: close
```

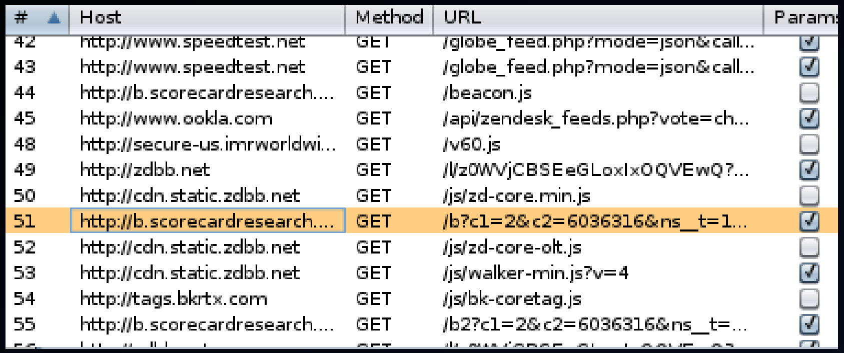
- Host systems sends information about OS and Browsing Client
- Session Cookie created



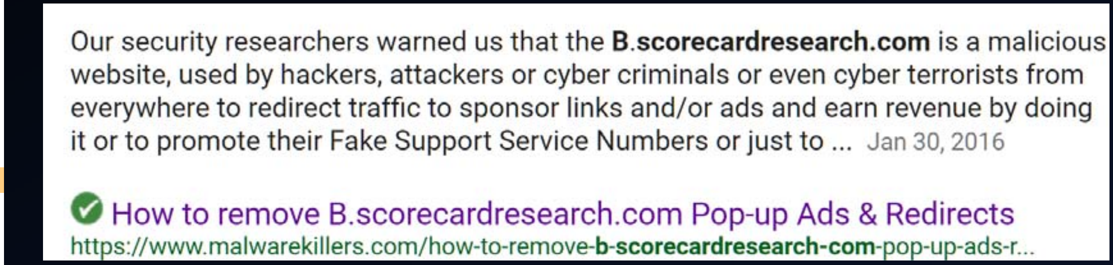
```
Last-Modified: Mon, 05 Dec 2016 02:55:48 GMT
Pragma: no-cache
Server: Apache
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Length: 17916
Connection: close

<!doctype html>
<html lang="en">
<head>
        <meta charset="UTF-8">
        <title>Ookla | The world standard in Internet metrics</title>
        <meta name="description" content="Ookla is the global leader in broadband testing, network diagnostic applications and data, with products incl
and NetMetrics.">
```

- Ookla responds with server type: Apache
- Also returned HTML document for rendering by web browser

Malicious host(s) found:



#	Host	Method	URL	Param
42	http://www.speedtest.net	GET	/globe_feed.php?mode=json&call...	☑
43	http://www.speedtest.net	GET	/globe_feed.php?mode=json&call...	☑
44	http://b.scorecardresearch....	GET	/beacon.js	□
45	http://www.ookla.com	GET	/api/zendesk_feeds.php?vote=ch...	☑
48	http://secure-us.imrworldwi...	GET	/v60.js	□
49	http://zdbb.net	GET	/l/z0WVjCBSEeGLoxIxOQVEwQ?...	☑
50	http://cdn.static.zdbb.net	GET	/js/zd-core.min.js	□
51	http://b.scorecardresearch....	GET	/b?c1=2&c2=6036316&ns_t=1...	☑
52	http://cdn.static.zdbb.net	GET	/js/zd-core-olt.js	□
53	http://cdn.static.zdbb.net	GET	/js/walker-min.js?v=4	☑
54	http://tags.bkrtx.com	GET	/js/bk-coretag.js	□
55	http://b.scorecardresearch....	GET	/b2?c1=2&c2=6036316&ns_t=...	☑

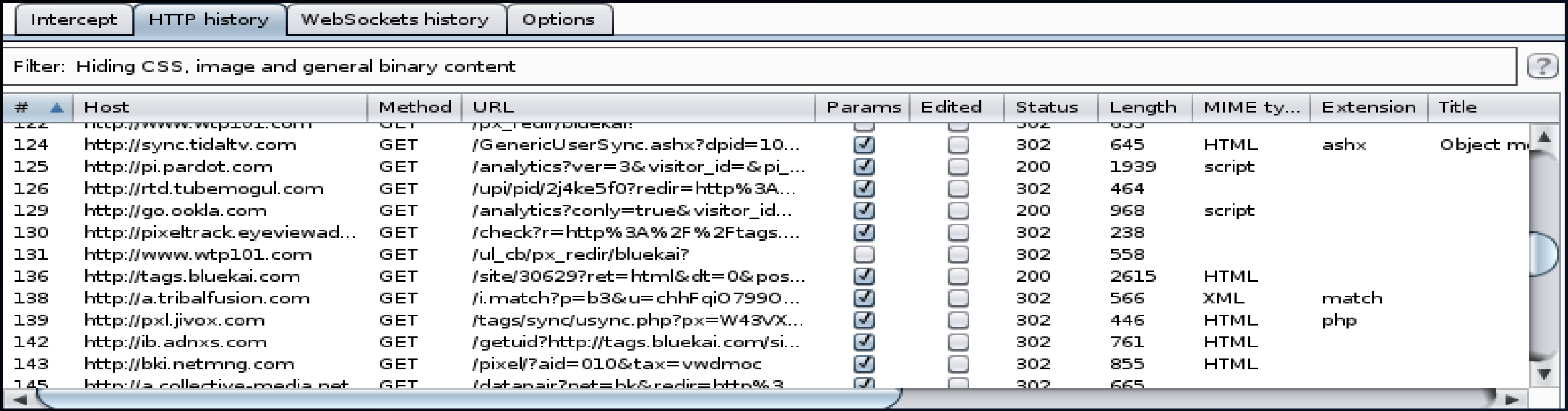


Our security researchers warned us that the **B.scorecardresearch.com** is a malicious website, used by hackers, attackers or cyber criminals or even cyber terrorists from everywhere to redirect traffic to sponsor links and/or ads and earn revenue by doing it or to promote their Fake Support Service Numbers or just to ... Jan 30, 2016

✓ How to remove B.scorecardresearch.com Pop-up Ads & Redirects
https://www.malwarekillers.com/how-to-remove-**b-scorecardresearch-com**-pop-up-ads-r...

- Research on some of the hosts like b.scorecardresearch.com shows the Ookla is loading potentially malicious content.
- Must be careful what you click on the website

Cookies and trackers:

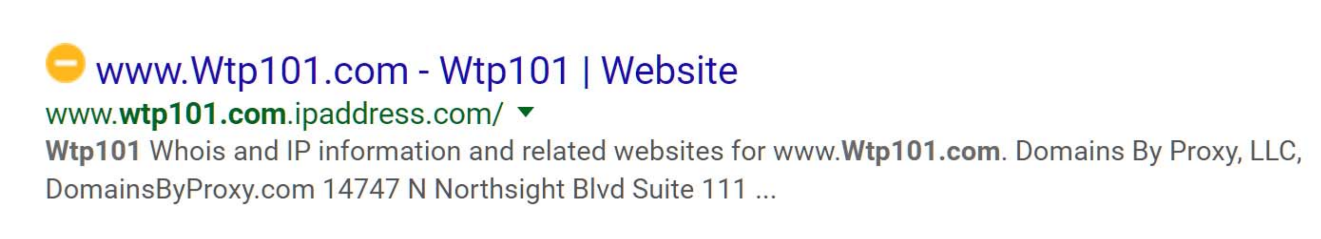


Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME ty...	Extension	Title
122	http://www.wtp101.com	GET	/px_redir/bluekai?	□	□	302	[illegible]			
124	http://sync.tidaltv.com	GET	/GenericUserSync.ashx?dpid=10...	☑	□	302	645	HTML	ashx	Object m
125	http://pi.pardot.com	GET	/analytics?ver=3&visitor_id=&pi_...	☑	□	200	1939	script		
126	http://rtd.tubemogul.com	GET	/upi/pid/2j4ke5f0?redir=http%3A...	☑	□	302	464			
129	http://go.ookla.com	GET	/analytics?conly=true&visitor_id...	☑	□	200	968	script		
130	http://pixeltrack.eyeviewad...	GET	/check?r=http%3A%2F%2Ftags....	☑	□	302	238			
131	http://www.wtp101.com	GET	/ul_cb/px_redir/bluekai?	□	□	302	558			
136	http://tags.bluekai.com	GET	/site/30629?ret=html&dt=0&pos...	☑	□	200	2615	HTML		
138	http://a.tribalfusion.com	GET	/i.match?p=b3&u=chhFqiO7990...	☑	□	302	566	XML	match	
139	http://pxl.jivox.com	GET	/tags/sync/usync.php?px=W43VX...	☑	□	302	446	HTML	php	
142	http://ib.adnxs.com	GET	/getuid?http://tags.bluekai.com/si...	☑	□	302	761	HTML		
143	http://bki.netmng.com	GET	/pixel/?aid=010&tax=vwdmoc	☑	□	302	855	HTML		
145	http://a.collective-media.net	GET	/datapair?net=bk&redir=http%3	☑	□	302	665			

- Site loads hundreds of adware and can potentially install software to the host computer if clicked.
- There’s also tracking hosts that tracks your movement on the website (probably used for analytics or worst, malicious)
- Some Ads can have you redirected to malicious websites (browser hijacking, etc)

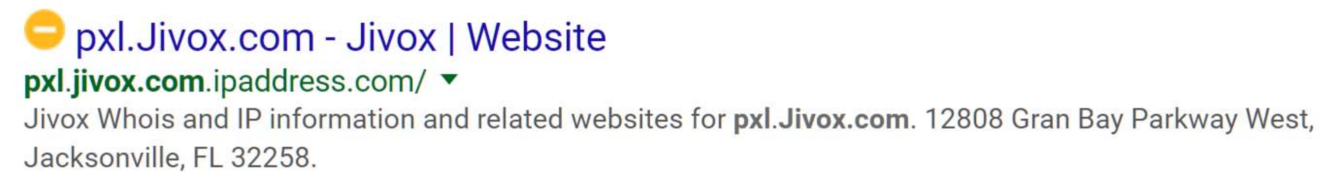
Cookies and trackers:



www.Wtp101.com - Wtp101 | Website

www.**wtp101.com**.ipaddress.com/ ▾

Wtp101 Whois and IP information and related websites for www.**Wtp101.com**. Domains By Proxy, LLC, DomainsByProxy.com 14747 N Northsight Blvd Suite 111 ...



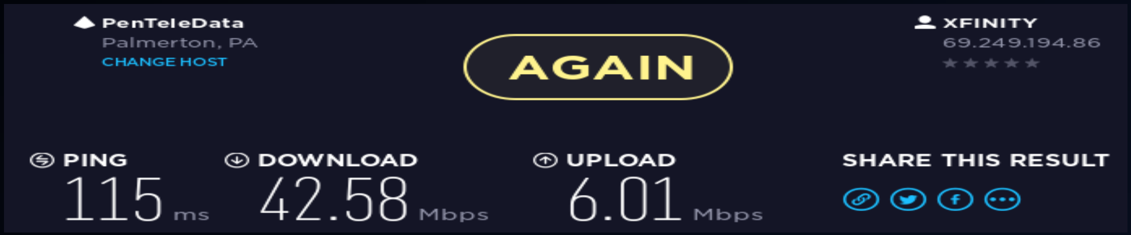
pxl.Jivox.com - Jivox | Website

pxl.jivox.com.ipaddress.com/ ▾

Jivox Whois and IP information and related websites for **pxl.Jivox.com**. 12808 Gran Bay Parkway West, Jacksonville, FL 32258.

- Personal anti-virus shows warnings for some of the hosts that Ookla loads.

Results of Speed test:



PenTeleData
Palmerton, PA
CHANGE HOST

AGAIN

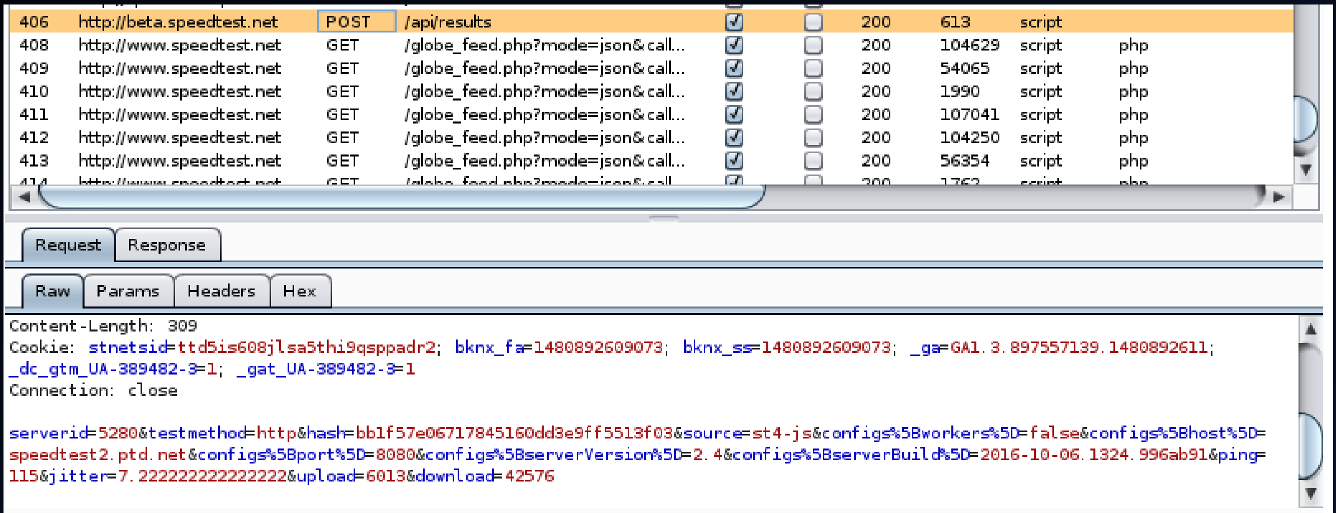
XFINITY
69.249.194.86
★★★★★

PING 115 ms

DOWNLOAD 42.58 Mbps

UPLOAD 6.01 Mbps

SHARE THIS RESULT



406	http://beta.speedtest.net	POST	/api/results	☑	□	200	613	script	
408	http://www.speedtest.net	GET	/globe_feed.php?mode=json&call...	☑	□	200	104629	script	php
409	http://www.speedtest.net	GET	/globe_feed.php?mode=json&call...	☑	□	200	54065	script	php
410	http://www.speedtest.net	GET	/globe_feed.php?mode=json&call...	☑	□	200	1990	script	php
411	http://www.speedtest.net	GET	/globe_feed.php?mode=json&call...	☑	□	200	107041	script	php
412	http://www.speedtest.net	GET	/globe_feed.php?mode=json&call...	☑	□	200	104250	script	php
413	http://www.speedtest.net	GET	/globe_feed.php?mode=json&call...	☑	□	200	56354	script	php
414	http://www.speedtest.net	GET	/globe_feed.php?mode=json&call...	☑	□	200	1762	script	php

```
Content-Length: 309
Cookie: stnetsid=ttd5is608jlsa5thi9qsppadr2; bknx_fa=1480892609073; bknx_ss=1480892609073; _ga=GA1.3.897557139.1480892611;
_dc_gtm_UA-389482-3=1; _gat_UA-389482-3=1
Connection: close

serverid=5280&testmethod=http&hash=bb1f57e06717845160dd3e9ff5513f03&source=st4-js&configs%5Bworkers%5D=false&configs%5Bhost%5D=
speedtest2.ptd.net&configs%5Bport%5D=8080&configs%5BserverVersion%5D=2.4&configs%5BserverBuild%5D=2016-10-06.1324.996ab91&ping=
115&jitter=7.2222222222222222&upload=6013&download=42576
```

- Hosts uses XMLhttprequest for the speed test
- Results are returned in a POST script