# Como o seu navegador se tornou um malware socialmente aceito

Guilherme Baptista

CryptoRave 2019, Brasil.

# Agenda

- Navegadores e os 4 níves da internet;
- Malwares, trackers, publicidade e JavaScript;
- Proteções conhecidas;
- Novos níveis de proteção;
- Como fazer parte;
- Demonstração ao vivo.

# Quais são os navegadores mais populares no Brasil?

http://gs.statcounter.com/browser-market-share/all/brazil

# 80%

# Google Chrome

# 5%

# Mozilla Firefox

# 5%

# Apple Safari

# 2%

# Opera

# 1%

# Microsoft Edge e Internet Explorer

Quase

# 90%

da internet é acessada por navegadores de

***"código aberto".***

# BSD ~ MIT

## Chromium

(Google Chrome)

# MPL

## Mozilla Firefox

# E por quê isso importa?

# A importância do software livre

Código aberto

**não**

significa software livre.

# As 4 liberdades

de um software livre.

# 0

# Usar para qualquer propósito.

# 1

# Estudar e adapdar para as suas necessidades.

# 2

# Redistribuir cópias livremente.

# 3

# Modificar e distribuir as modificações.

Gratuito

**não**

significa livre.

Google Chrome é

# gratuito.

Não é livre.

Chromium é

# livre.

Mozilla Firefox é

# livre.

Cenário promissor em direção à

# liberdade.

# É o suficiente?

# Os 4 níveis da internet

# Nível 1

## Transferência de dados entre computadores.

# Transferência de arquivos

http://site.com.br/Documento.txt

# Documento.txt

*DOCUMENTO PÚBLICO*

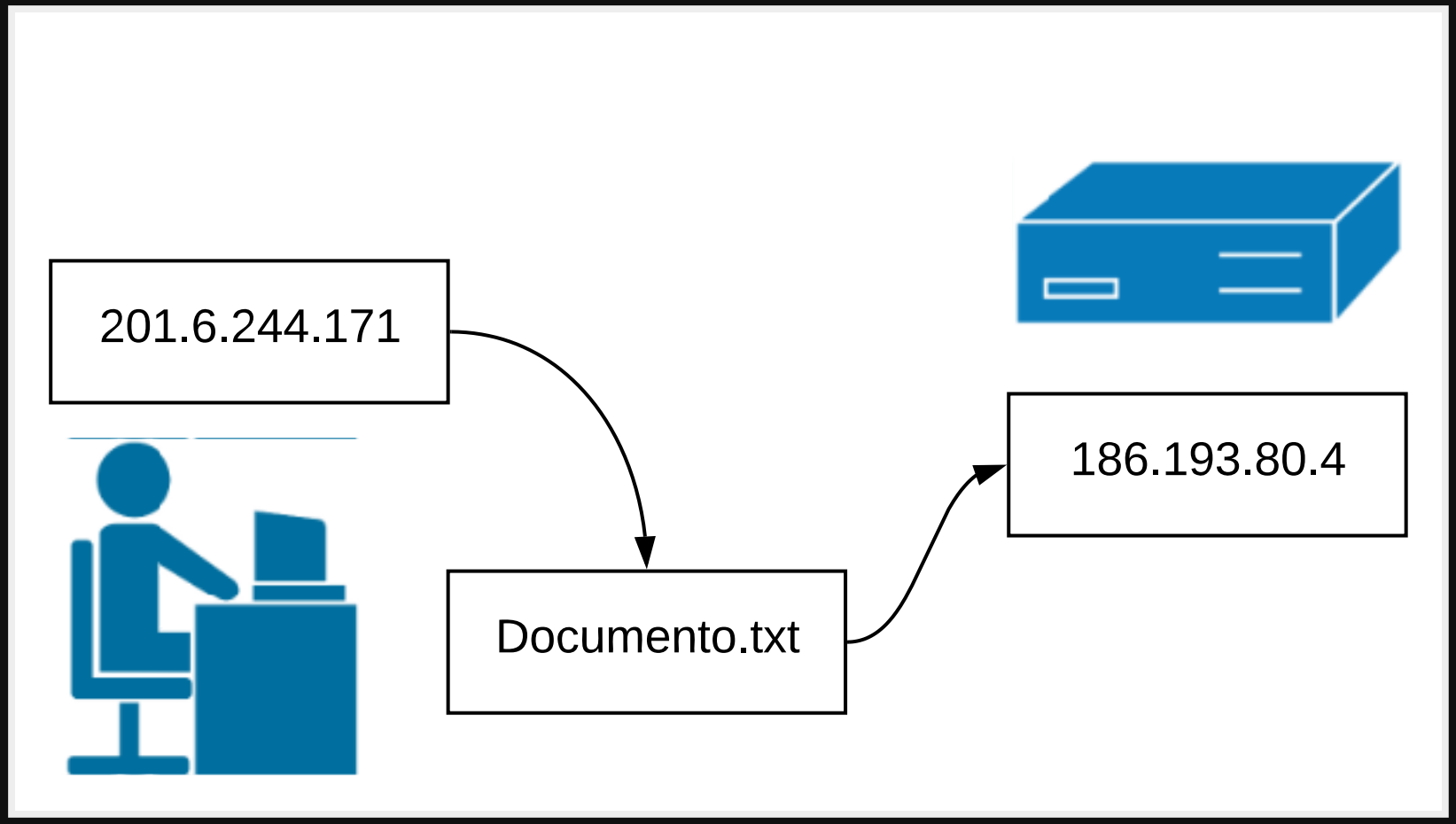
*Este é um exemplo de documento com texto puro.*

```
wget http://site.com.br/Documento.txt

--2019-05-01 18:55:51--  http://site.com.br/Documento.txt
Resolving site.com.br (site.com.br)... 192.241.176.17
Connecting to site.com.br (site.com.br)|192.241.176.17|:80...
Connected.
HTTP request sent, awaiting response... 200 OK
Length: 1782 (1,7K) [text/plain]
Saving to: ‘Documento.txt’

Documento.txt 100%[=====>]   1,74K  --.-KB/s    in 0s

2019-05-01 18:55:51 (83,0 MB/s)
‘Documento.txt’ saved [1782/1782]
```


201.6.244.171
186.193.80.4
Documento.txt

# Editor de textos:

*DOCUMENTO PÚBLICO*

*Este é um exemplo de documento com texto puro.*

# 2014

## Marco Civil da Internet

## Subseção I

# Da Guarda de Registros de Conexão

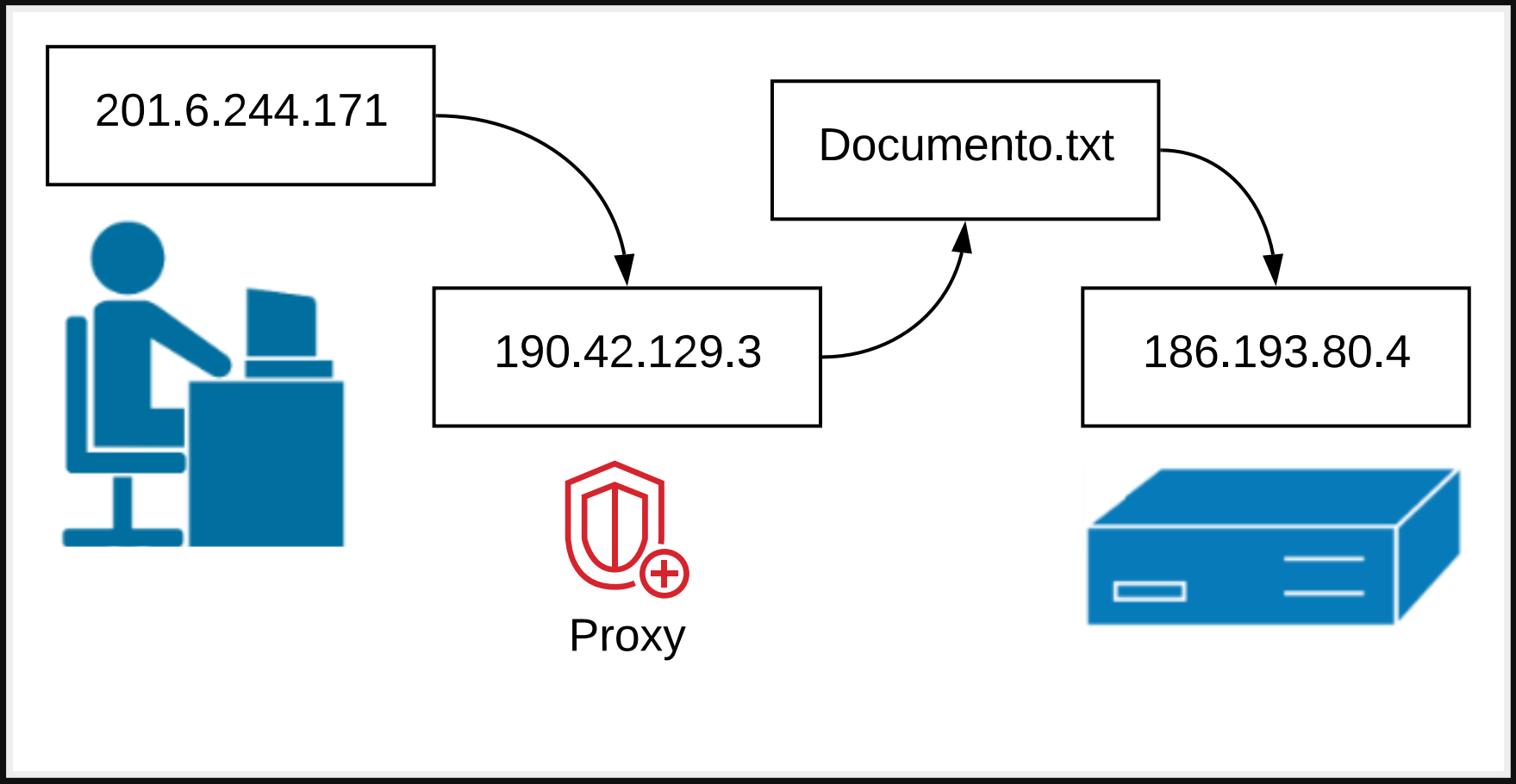
# Resumindo

Se a justiça liberar, o seu provedor precisa dizer:

- Qual documento você acessou;
- Qual dia e hora;
- Onde você estava quando acessou.

# Tem como evitar?

# Servidores proxy


201.6.244.171
Documento.txt
190.42.129.3
186.193.80.4
Proxy

# Anonymous

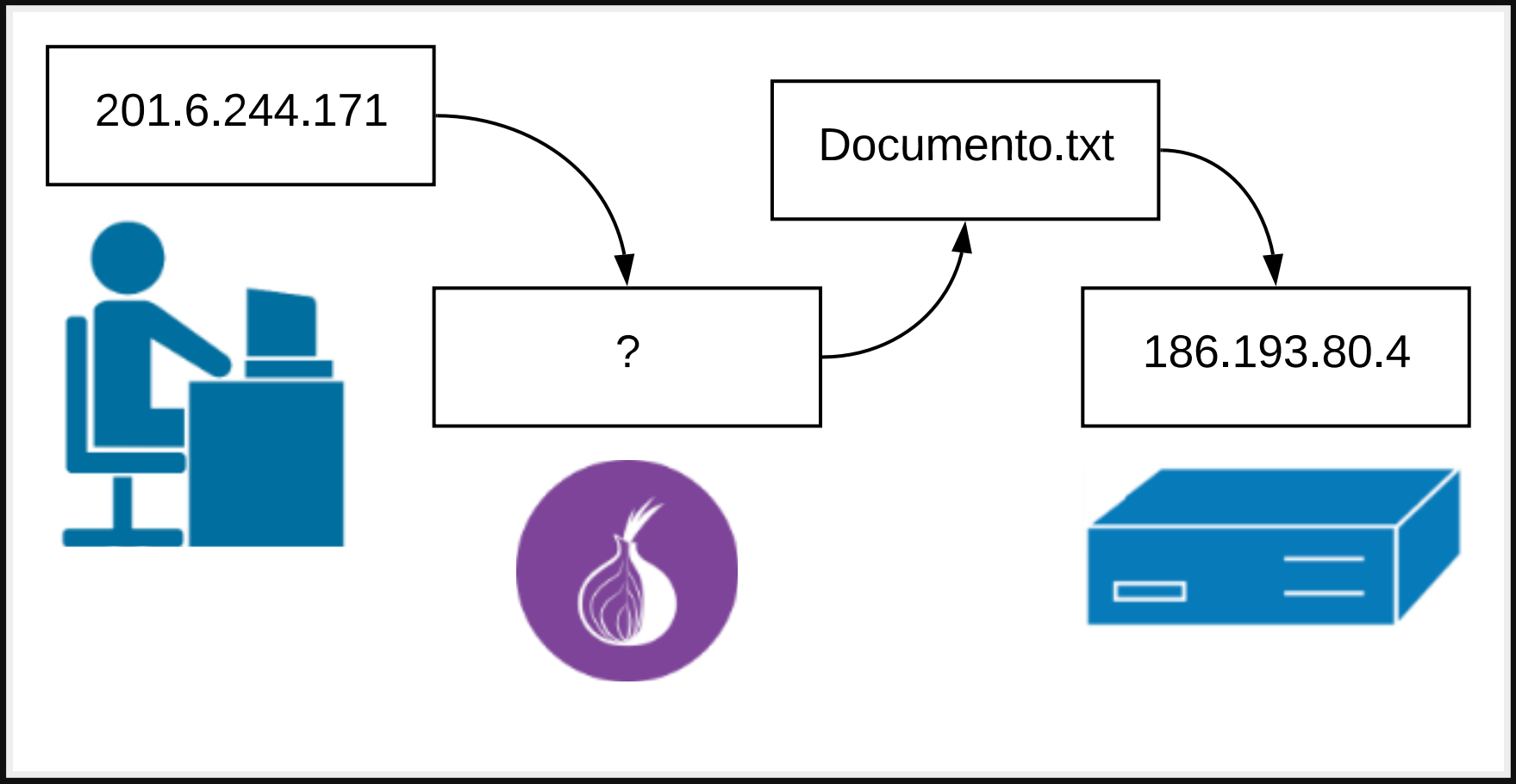
## LulzSec

# Hidemyass

foi obrigado a liberar os dados e

**duas pessoas foram presas pelo FBI.**

# Tor


201.6.244.171
Documento.txt
?
186.193.80.4

# Nível 2

## HTML e Hyperlinks

1980

# WWW

# 1992

foi lançado o primeiro site HTML da internet.

```
<title>Summary -- /WWW</title>

<h1>WorldWideWeb - Summary</h1>

The <a name="6" href="TheProject.html">WWW</a> project merges...

<p>
The project is based...

</p><h3>Reader view</h3>
The WWW world consists of documents, and links...
```

```
<h1>Exemplo de Documento</h1>

<p>
  Este é um documento web simples para demonstrar
  como a internet funciona. Ele não possui:
</p>
<ul>
  <li>Estruturas complexas</li>
  <li>Imagens ou animações</li>
  <li>
    Recursos que dependam de um navegador
    para serem totalmente compreendidos
  </li>
</ul>
```

# wget?

http://site.com.br/Documento.html


HTML

# Exemplo de Documento

Este  um documento web simples para demonstrar como a internet funciona. Ele n  possui:

* Estruturas complexas
* Imagens ou animaM-ues
* Recursos que dependam de um navegador para serem totalmente compreendidos

# Nível 3

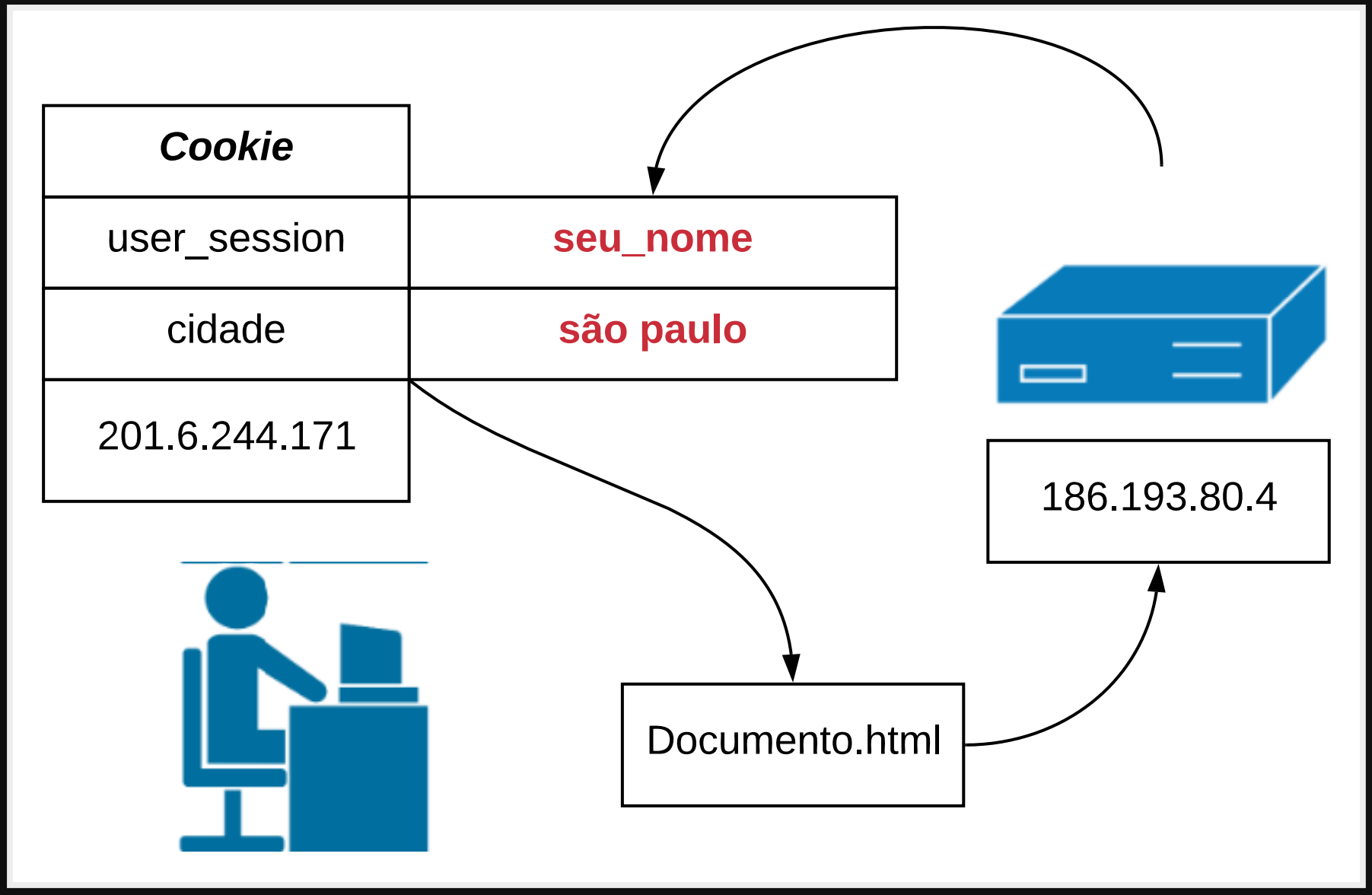
## Headers e cookies

| | |
|---|---|
| Accept | **text/html,image/webp** |
| Accept-Language | **en-US,en** |
| User-Agent | **Chrome/74.0.3729.108** |
| 201.6.244.171 | |

186.193.80.4

Documento.html

# Cookies?


Cookie
user_session
seu_nome
cidade
são paulo
201.6.244.171
186.193.80.4
Documento.html

```
<h1>Exemplo de Documento</h1>

<p>
  Este é um documento web simples para demonstrar
  como a internet funciona. Ele não possui:
</p>
<ul>
  <li>Estruturas complexas</li>
  <li>Imagens ou animações</li>
  <li>
    Recursos que dependam de um navegador
    para serem totalmente compreendidos
  </li>
</ul>
```

# Exemplo de Documento

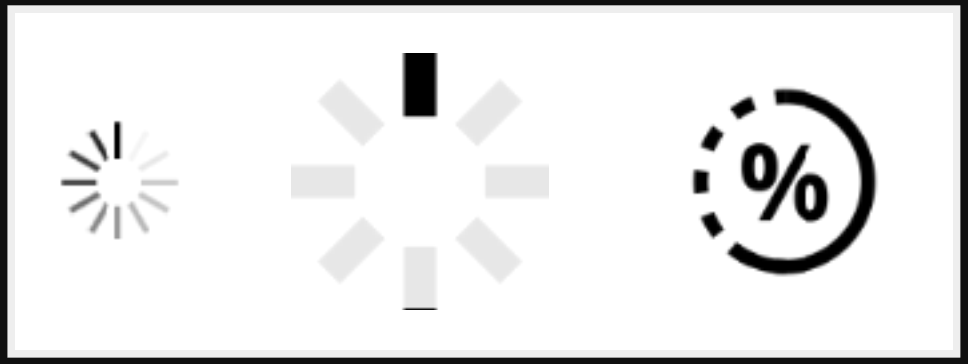
Este é um documento web simples para demonstrar como a internet funciona. Ele não possui:

- Estruturas complexas
- Imagens ou animações
- Recursos que dependam de um navegador para serem totalmente compreendidos

# Nível 4

## JavaScript e AJAX


WELCOME TO CASINO DEL RIO - Micr
File Edit View Favorites Tools Help
Back
Address http://www.casinodelrio.com/
SEARCH
SideFind
sideFind powered by IST
casino
Find
www.888.com
CASINO ON NET
Click
http://ads1.revenue.net - ExclusiveRewards - Microsoft Internet Explorer
CONGRATULATIONS!
You've been chosen to receive a
FREE* Gateway Desktop Computer!
Intel Pentium 4 Processor 2.66 GHz
256MB DDR-SDRAM, 80GB HD, 48x CD-RW
19-inch Color CRT Monitor (18-inch viewable)
Click Here to Claim Your FREE* Desktop Computer!
FREE!
Gateway
by ExclusiveRewards
*with participation in our program
Address http://www.poker-on-net.com/index.htm?SR=916066
TopSearches
Microsoft Internet Explorer
Click OK to download our free software while browsing the site
OK
Cancel
Go
Links
Practical
SideFind
sideFind powered by IST
casino
Find
www.888.com
CASINO ON NET
Click
Casino On Net - Up to 200$
Welcome Bonus
Since 1996, over 8,000,000
people have experienced Casino
POKER ON-NET
Download
Getting Started
Features
Contact Us
Help
> Current Events
Finale
GAMES
WHITE PAGES
Blackjack
Roulette
Slot Machine
Click Here!



# Malware

# Código ou programa:

- Malicioso;
- Nocivo;
- Mal-intencionado.

Entra no

**computador alheio**

para causar danos ou

**roubo de informações**

(confidenciais ou não).

# O meu navegador faz isso?

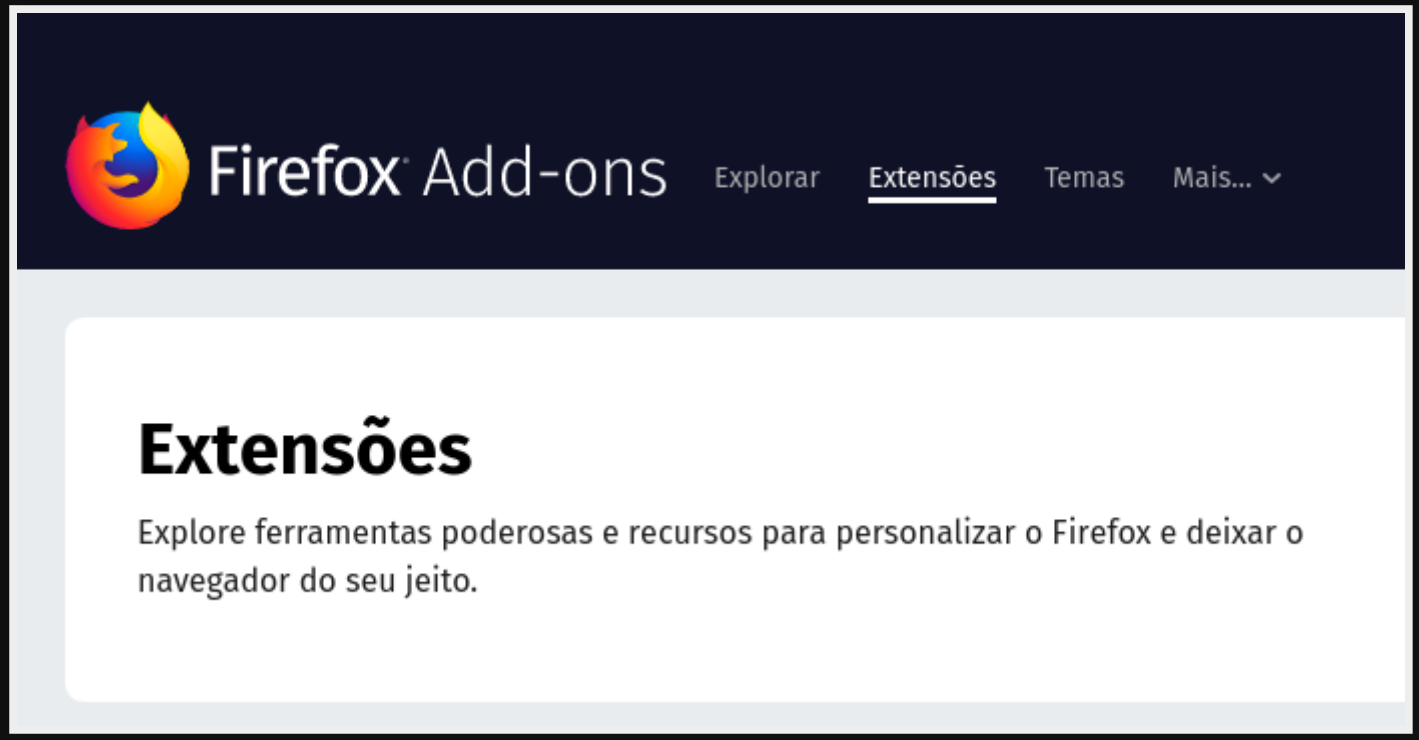
# Mais do que isso:

Ele é uma porta de entrada para que qualquer site possa fazer isso.

# Tem como se proteger?

# Sim!

# Extensões


Firefox Add-ons
Explorar
Extensões
Temas
Mais...
Extensões
Explore ferramentas poderosas e recursos para personalizar o Firefox e deixar o navegador do seu jeito.

# Proxy

https://hide.me

https://hidester.com

https://www.hidemyass.com

https://www.hotspotshield.com

# Camuflar o seu verdadeiro IP

# Por quê?

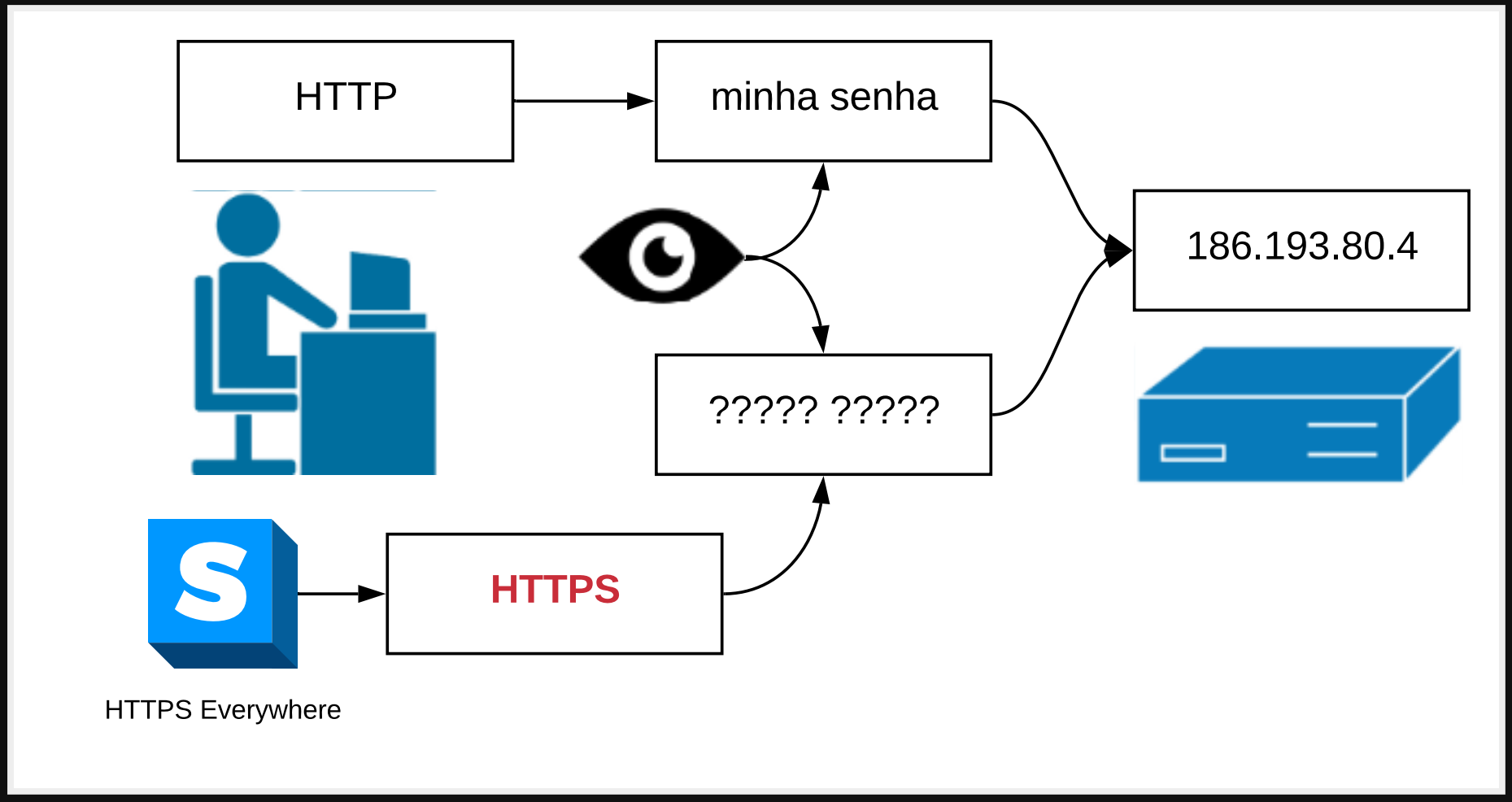
# Seu IP verdadeiro não fica registrado como quem acessou algum documento.

# Conteúdo bloqueado para IP's brasileiros.

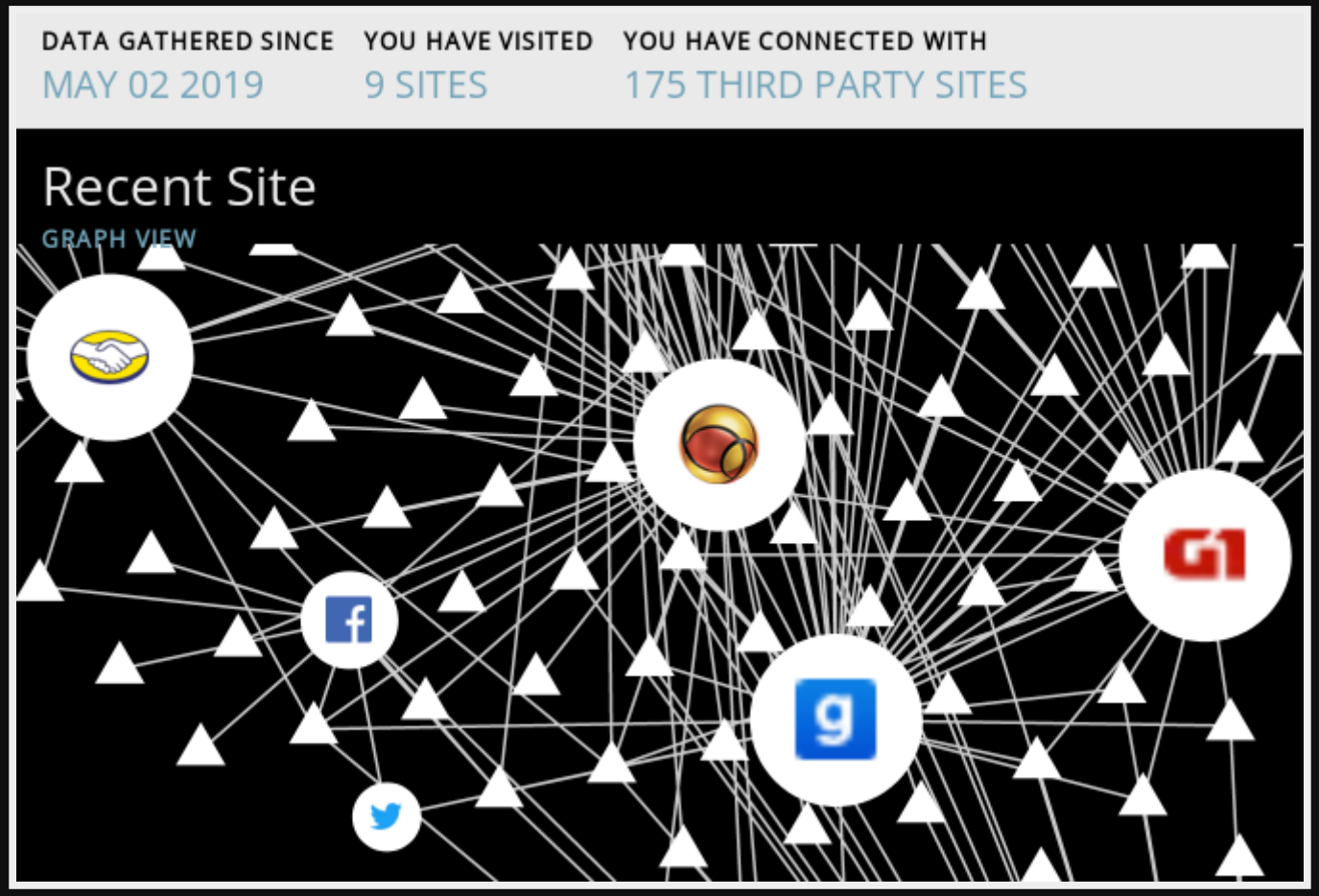
# Sites que tentam cobrar por conteúdo aberto.

Prática comum em grandes jornais.

# HTTPS Everywhere


HTTP
minha senha
186.193.80.4
????? ?????
HTTPS
HTTPS Everywhere

# Trackers




# Firefox Lightbeam

# Bloqueio de trackers

## uBlock Origin

## Disconnect

## Privacy Badger

## Ghostery

# Publicidade

# Quanto da sua internet é consumida por publicidade?

*The New York Times*

# Sites de notícias acessados por celulares.

*theblaze.com*

# 11.9 segundos

com publicidade;

# 7 segundos

com conteúdo.

*thedailybeast.com*

# 11.3 segundos

com publicidade;

# 5 segundos

com conteúdo.

*boston.com*

# 30.8 segundos

com publicidade;

# 8.1 segundos

com conteúdo.

*boston.com*

# mais de 15 MB

com publicidade.

Da sua franquia 3G.

# E nos sites mais acessados do Brasil?

*mercadolivre.com.br*

# 21%

com trackers e publicidade;

# 0,4 MB

de trackers e publicidade.

*globo.com*

# 63%

com trackers e publicidade;

# 1,7 MB

de trackers e publicidade.

*uol.com.br*

# 67%

com trackers e publicidade;

# 7,1 MB

de trackers e publicidade.

# Bloqueio de publicidade

## Adblock Plus

## Adblock_

## uBlock Origin

# Impacto do uso de extensões no mercado de navegadores.

# Tor Browser

- NoScript;
- HTTPS Everywhere.

# Opera

- VPN integrada;
- Bloqueador de anúncios.

# Brave

- Bloqueador de anúncios;
- Bloqueador de trackers;
- HTTPS upgrades.

# É o suficiente?

Infelizmente

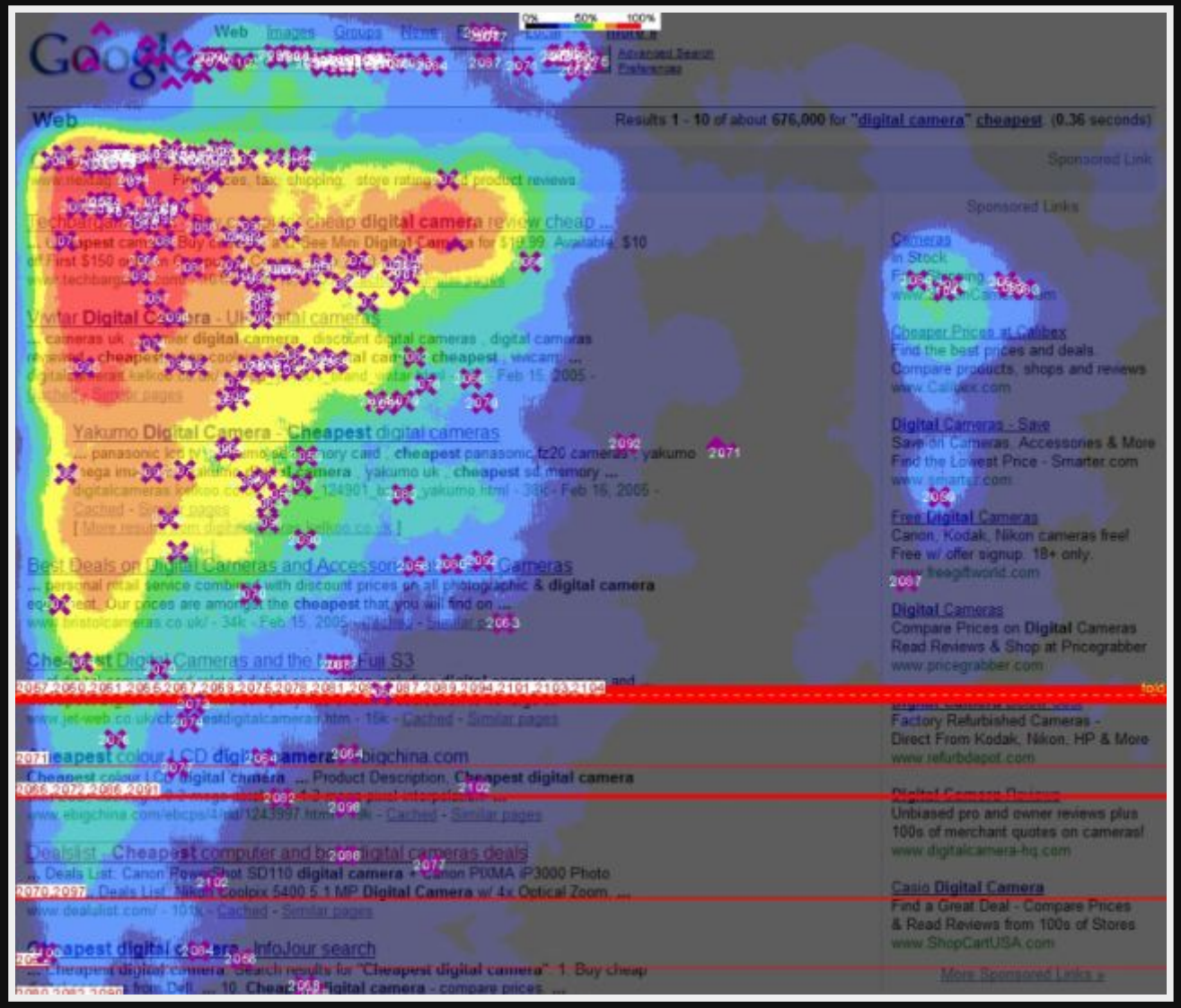
# não.

# JavaScript

# addEventListener

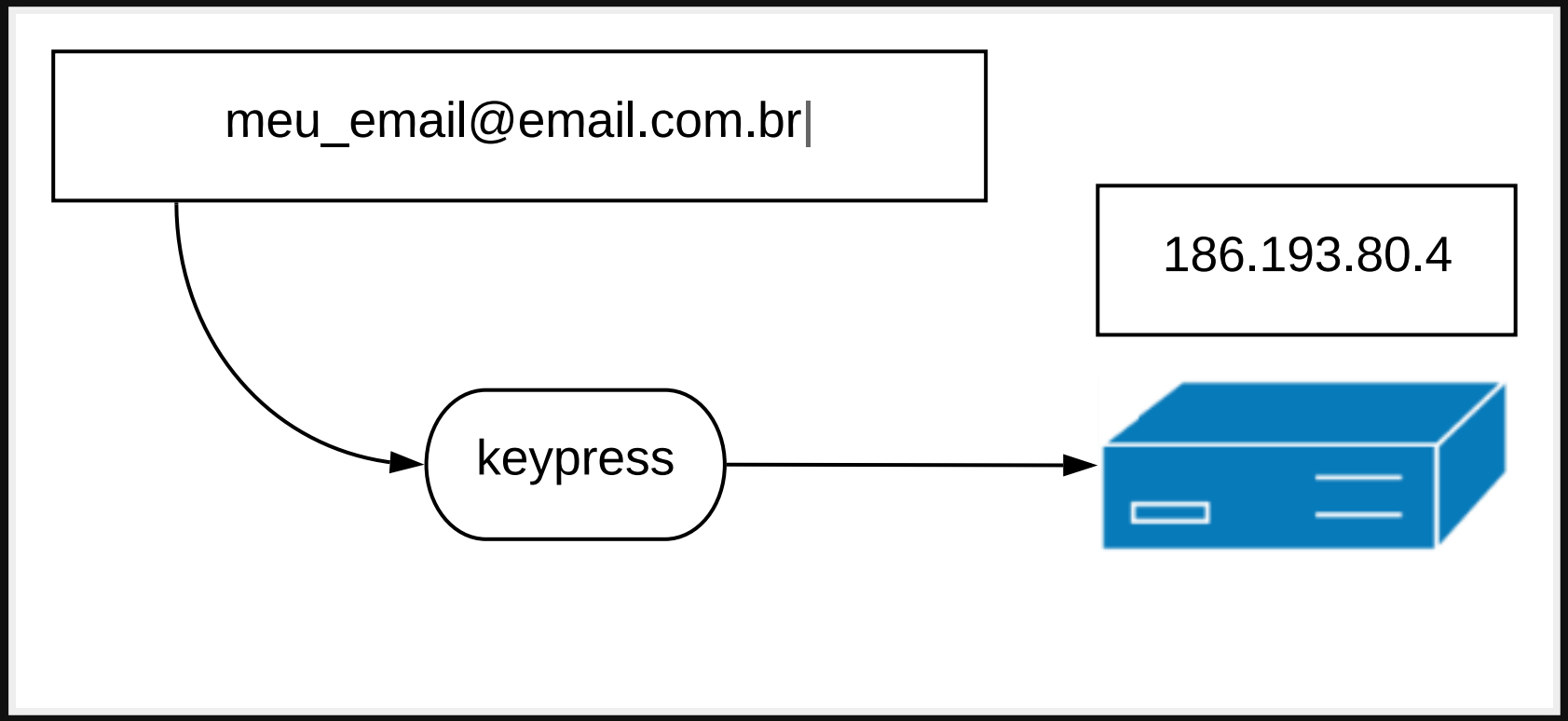
Olhar o ponteiro do seu mouse é como observar o movimento dos seus olhos:

```
someImage.addEventListener('mousemove', function(_event) {
  sendReport('the user is moving the mouse over the image');
});
```


Google
Web
Results 1 - 10 of about 676,000 for "digital camera" cheapest (0.36 seconds)
Sponsored Links
Cameras
Cheaper Prices at Calbex
Find the best prices and deals
Compare products, shops and reviews
Digital Cameras - Save
Free Digital Cameras
Canon, Kodak, Nikon cameras free!
Digital Cameras
Compare Prices on Digital Cameras
Read Reviews & Shop at Pricegrabber
Factory Refurbished Cameras -
Direct From Kodak, Nikon, HP & More
Unbiased pro and owner reviews plus
100s of merchant quotes on cameras!
Casio Digital Camera
Find a Great Deal - Compare Prices
& Read Reviews from 100s of Stores
More Sponsored Links »

# Começou a digitar algo e mudou de ideia?

```
someTextInput.addEventListener('keypress', function(_event) {
  sendEmail('send the typed email!');
});
```


meu_email@email.com.br
186.193.80.4
keypress

# Tá "escrolando" a página?

```
document.addEventListener('wheel', function(_event) {
  sendReport('scrolling...');
});
```

# Web APIs

# *A maioria dos sites não precisam vibrar*

https://arxiv.org/abs/1708.08510

# 74

padrões de Web APIs implementados nos

# navegadores modernos.

Apenas

**11**

pedem sua permissão pra executar.

# vibrate(200);

*Vibrar por 200ms.*

https://googlechrome.github.io/samples/vibration/

# getCurrentPosition();

*Qual a sua localização GPS?*

# Fingerprinting

# getBattery()

*Tem bateria? É um notebook?*

# getGamepads();

*Quantas portas USB's? Tem algo conectado?*

# NavigatorID;

*Qual o navegador?*

# Service Workers

# Web Workers

Realizar tarefas em background.

**about:debugging#workers**

Firefox

**chrome://inspect/#service-workers**

Chromium

# Mineração de criptomoedas.

***"Site do Governo de SP usou computador de visitante para minerar moeda virtual"***

https://g1.globo.com/tecnologia/noticia/site-do-governo-de-sp-usou-computador-de-visitante-para-minerar-moeda-virtual.ghtml

***"Governo de SP está minerando criptomoedas no seu computador sem você saber"***

https://www.tecmundo.com.br/seguranca/124000-governo-sp-minerando-criptomoedas-computador-voce-saber.htm

# *"Site do governo do RJ e outras 7 páginas brasileiras mineram criptomoedas"*

https://olhardigital.com.br/noticia/site-do-governo-do-rj-e-outras-7-paginas-brasileiras-mineram-criptomoedas/72292

# Como o seu navegador se tornou um malware socialmente aceito?

# Abrindo uma porta para qualquer site fazer o que quiser.

# Escondendo de você o que os sites estão fazendo.

# Implementando APIs perigosas sem perguntar ou informar as pessoas.

# Com os usuários não se importando com o que acontece em seu próprio computador.

# Tem como evitar?

# Desabilitar o JavaScript do seu navegador.

E não conseguir utilizar nenhum site.

# Minimizar o impacto

**NoScript**

**ScriptSafe**

**uMatrix**

# 2017

# Web API Manager

https://github.com/snyderp/web-api-manager

(não mantida)

Web Workers

Service Workers

Ambient Light Sensor

Battery Status

DeviceOrientation

Gamepad

Proximity

Screen Orientation

Vibration

WebUSB

Speech

Beacon

# 79

# itens que podem ser bloqueados

## Janeiro de 2018

# Luminous

Bloqueador de eventos JavaScript

https://gbaptista.github.io/luminous/

# Entrando em um site com um combo de 3 extensões:

- HTTPS Everywhere;
- uBlock Origin;
- ScriptSafe.

# 6

requisições influenciadas pela

# HTTPS Everywhere.

# 75

requisições bloqueadas pela

# uBlock Origin.

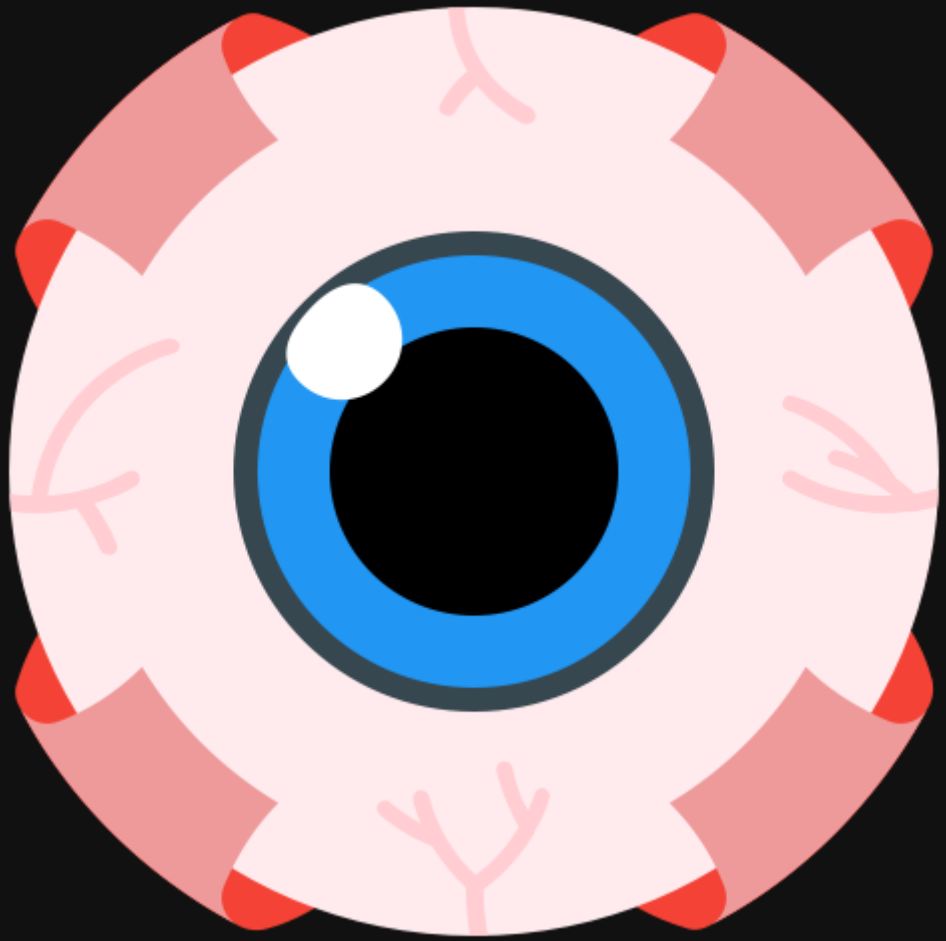
# 4

execuções bloqueadas pela

# ScriptSafe.

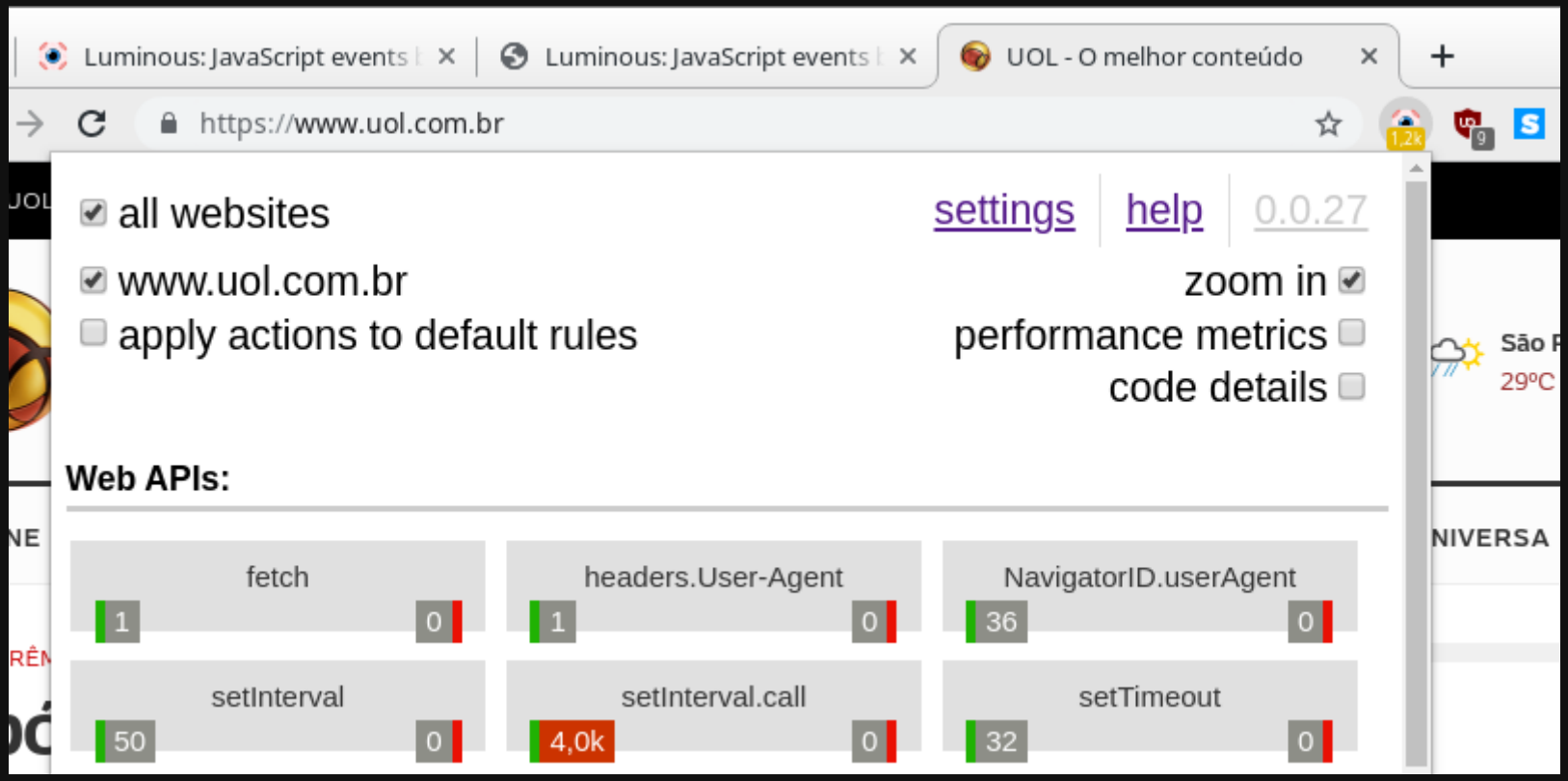
Adicionando a

# Luminous...



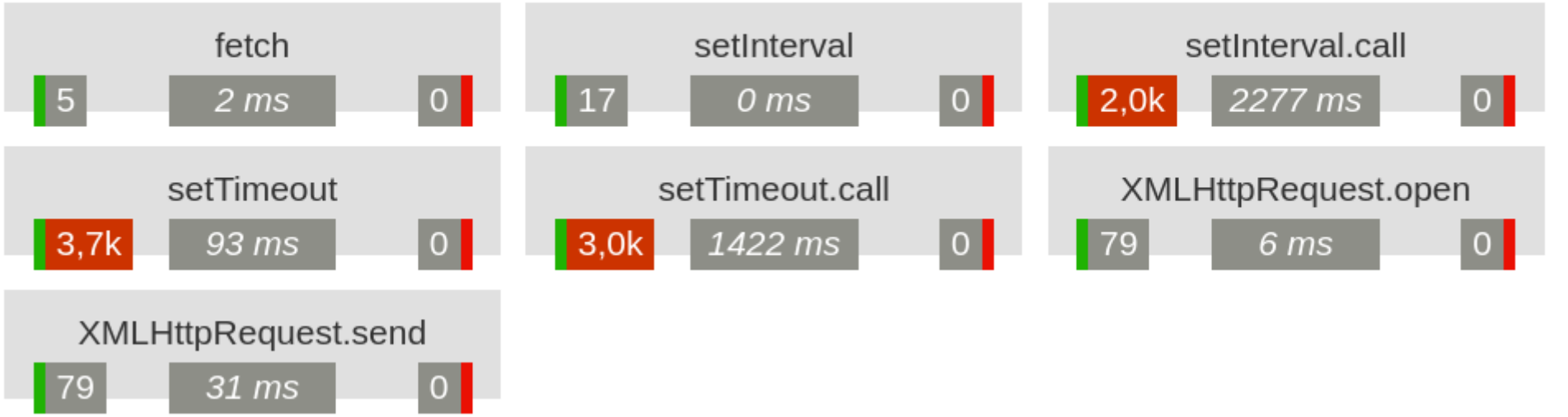
# 7,6 mil

execuções de JavaScript detectadas.


Luminous: JavaScript events
Luminous: JavaScript events
UOL - O melhor conteúdo
https://www.uol.com.br
all websites
settings
help
0.0.27
www.uol.com.br
zoom in
apply actions to default rules
performance metrics
code details
Web APIs:
fetch
1
0
headers.User-Agent
1
0
NavigatorID.userAgent
36
0
setInterval
50
0
setInterval.call
4,0k
0
setTimeout
32
0

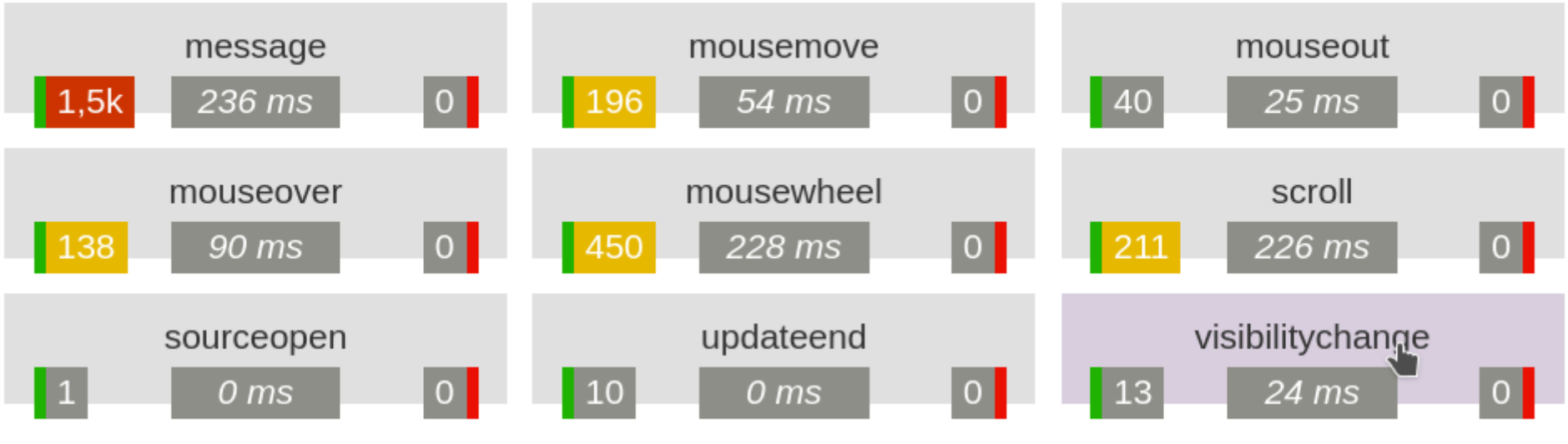
# Códigos consumindo sua CPU

## Web APIs:


fetch
5
2 ms
0
setInterval
17
0 ms
0
setInterval.call
2,0k
2277 ms
0
setTimeout
3,7k
93 ms
0
setTimeout.call
3,0k
1422 ms
0
XMLHttpRequest.open
79
6 ms
0
XMLHttpRequest.send
79
31 ms
0

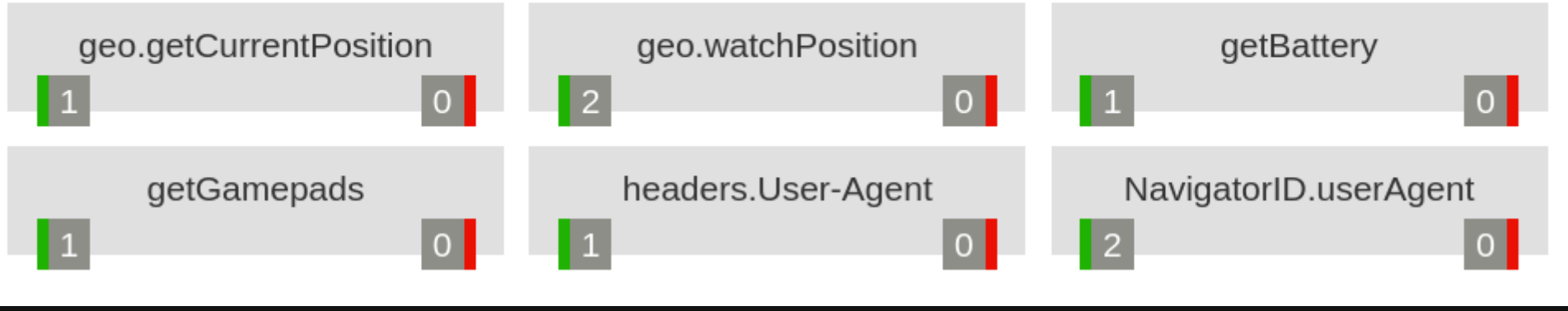
# Códigos monitorando sua atividade

## triggered events (handleEvent):



# Fingerprinting

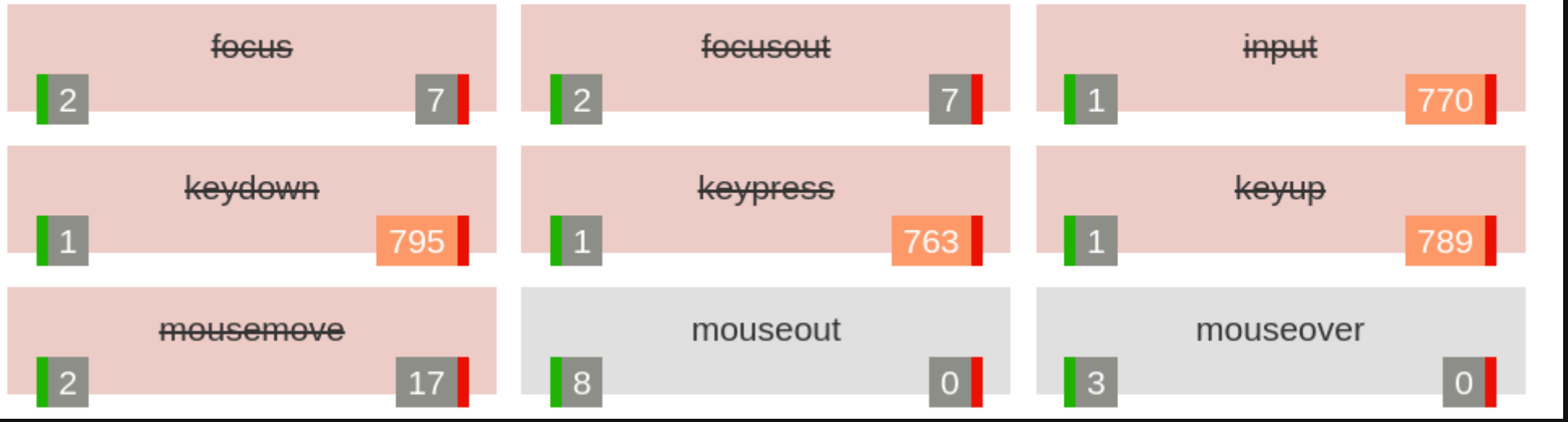
## Web APIs:


geo.getCurrentPosition
1
0
geo.watchPosition
2
0
getBattery
1
0
getGamepads
1
0
headers.User-Agent
1
0
NavigatorID.userAgent
2
0

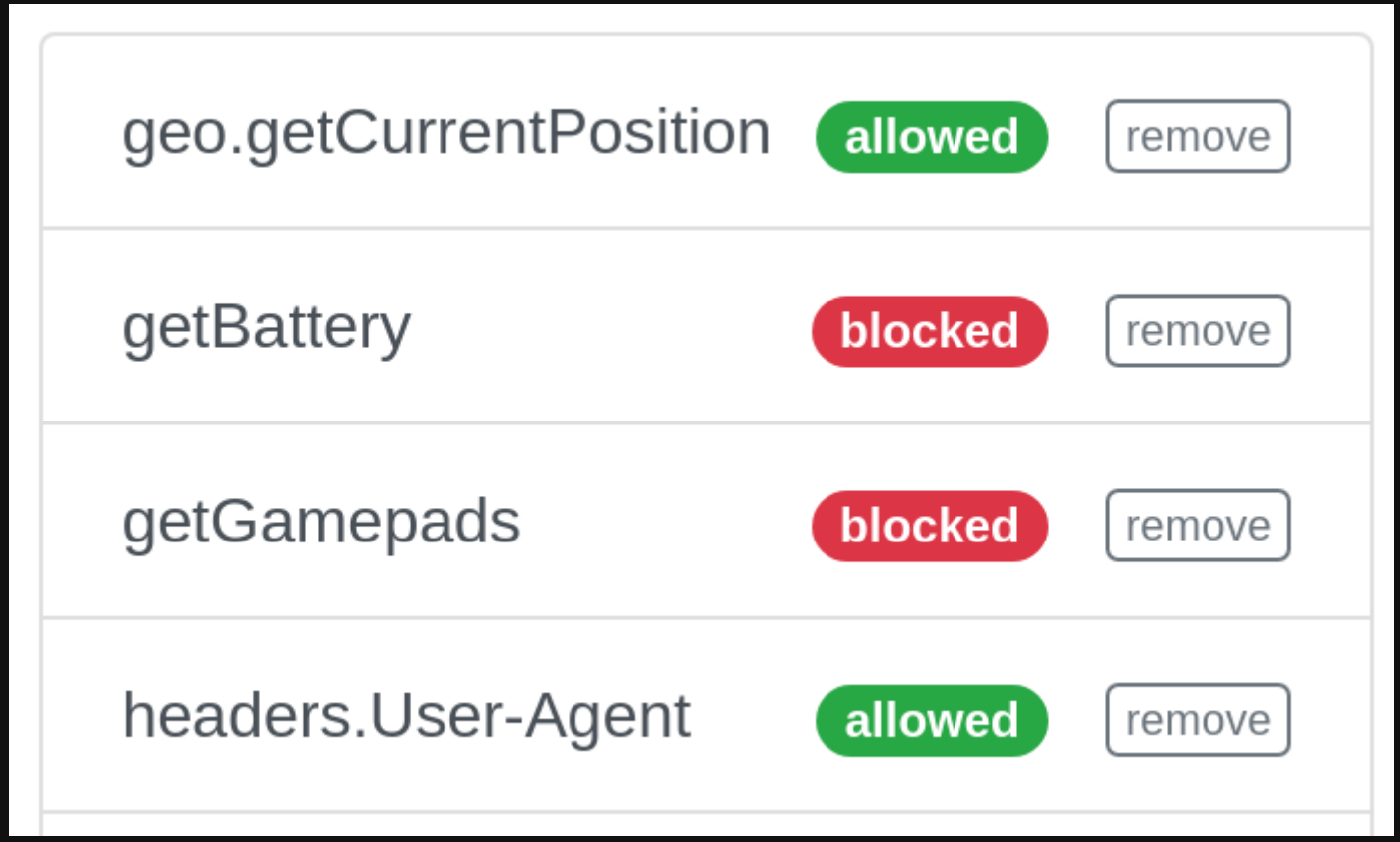
# Como bloquear algo indesejado?

É so clicar.

## triggered events (handleEvent):



# Configurações globais e por site específico.


geo.getCurrentPosition
allowed
remove
getBattery
blocked
remove
getGamepads
blocked
remove
headers.User-Agent
allowed
remove

# Relatórios

Qual site que

você

acessa mais executa JavaScript?

all

| | | |
|---|---|---|
| www.facebook.com | 4,9 k | 2,47 s |
| www.globo.com | 2,3 k | 643 ms |
| translate.google.com | 1,6 k | 145 ms |

# Qual código JavaScript é mais executado nos sites que

# você

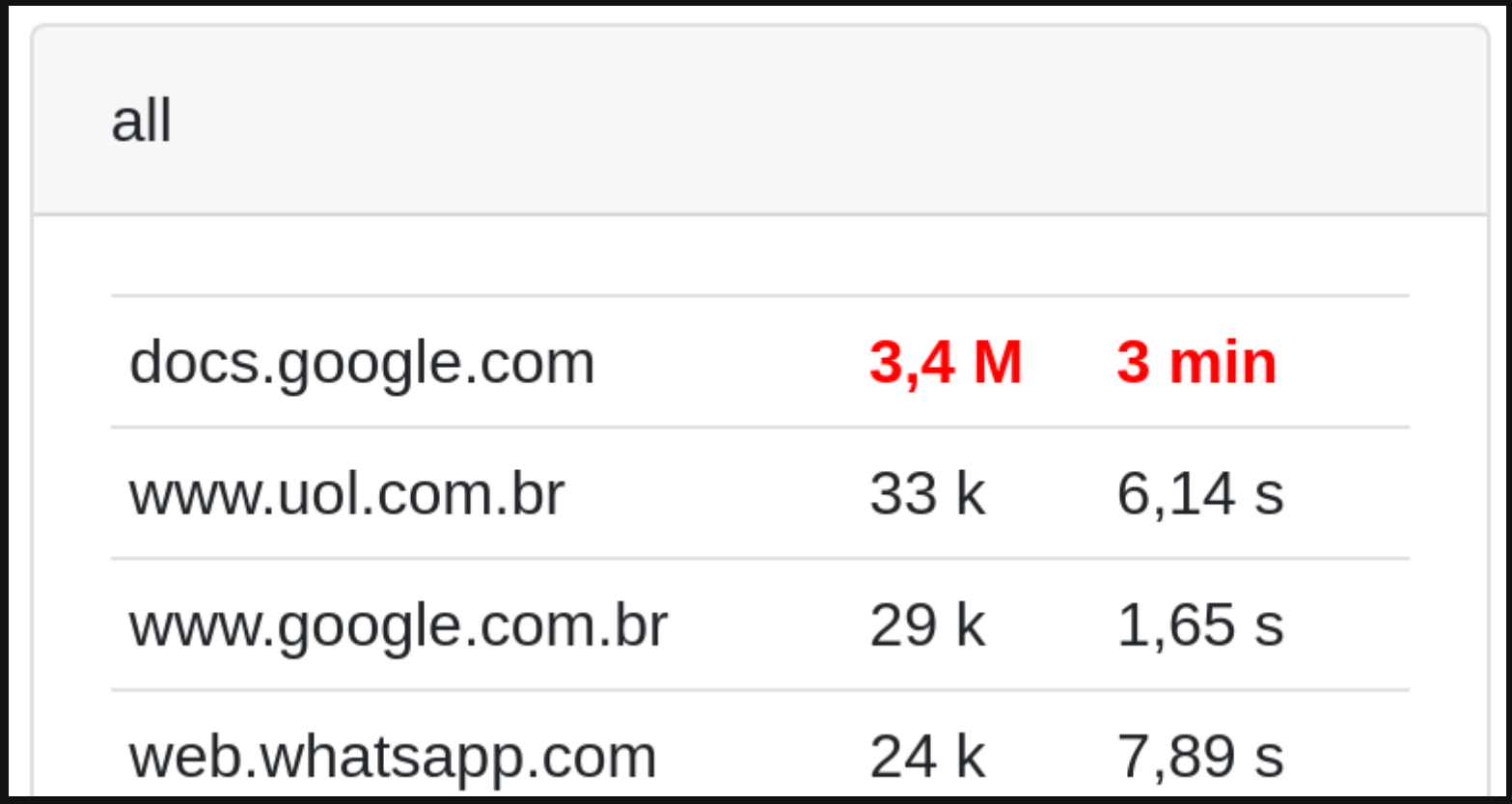
# visita.

| | | |
|---|---|---|
| setInterval.call | 2,2 k | 1,01 s |
| setTimeout | 2,1 k | 98 ms |
| setTimeout.call | 1,6 k | 3,08 s |
| keydown | 1,1 k | 1,37 s |
| scroll | 1 k | 342 ms |

Depois de alguns

# minutos

utlizando...


all

| | | |
|---|---|---|
| docs.google.com | **3,4 M** | **3 min** |
| www.uol.com.br | 33 k | 6,14 s |
| www.google.com.br | 29 k | 1,65 s |
| web.whatsapp.com | 24 k | 7,89 s |

# Quem está por trás de todas essas ferramentas de proteção?

# EFF

# Electronic Frontier Foundation

## EFForg/https-everywhere

## EFForg/privacybadger

Mais de

**800**

pessoas que escreveram mais de

# meio milhão

de linhas de código.

EFForg/privacybadger

**49%**

do código foi escrito por

# 1 pessoa.

snyderp/web-api-manager

**63%**

do código escrito por

# 1 pessoa.

gbaptista/luminous

# 71%

do código escrito por

# 1 pessoa.

disconnectme/disconnect

**73%**

do código escrito por

# 1 pessoa.

gorhill/uMatrix

**74%**

do código escrito por

# 1 pessoa.

gorhill/uBlock

**86%**

do código escrito por

# 1 pessoa.

hackademix/noscript

# 95%

do código escrito por

# 1 pessoa.

andryou/scriptsafe

# 96%

do código escrito por

# 1 pessoa.

Tirando os 2 projetos da

# Electronic Frontier Foundation

da conta.

# 6%

das pessoas são responsáveis por

# 70%

do código.

Mais de

# 3 milhões e meio

de linhas de código escritas por

# 12 pessoas

em 9 projetos diferentes.

# 2013

**Google: + 47 mil pessoas;**

**Apple: + 80 mil pessoas;**

**Microsoft: + 90 mil pessoas.**

# 12 pessoas

# Sozinhos não chegamos a lugar nenhum.

# Cada pessoa conta.

# Muito.

# Como você pode ajudar?

# Use as ferramentas.

https://addons.mozilla.org/firefox
https://chrome.google.com/webstore/category/exter
https://addons.opera.com

# Conte para outras pessoas.

# Ensine outras pessoas.

# Escreva sobre.

# Investigue os sites com as ferramentas.

# Denuncie sites com comportamentos suspeitos.

# Reporte problemas:

https://github.com/gbaptista/luminous/issues

(de maneira produtiva)

***"Essa ferramenta é uma $%#*!. Nunca achei que eu fosse odiar algo com tanto força."***

(Babel)

***"Não está funcionando na versão X, como é a versão mais segura, é uma VERGONHA não funcionar."***

(Luminous)

# Issues produtivas

- Qual o problema?
- Por quê é importante para você, como isso afeta a sua vida?

*"Minha filha gosta desse joguinho e ele para de funcionar com a extensão."*

*"Eu preciso usar esse site no trabalho e ele para de funcionar."*

- Como eu posso reproduzir o problema? Alguma teoria do motivo?
- Printscreens ou filmagens da tela.

# Deixe uma avaliação nas stores

- Conte como a extensão te ajudou;
- Estrelinhas.

# Mão na massa.

# Traduzir para outros idiomas.

gbaptista / **luminous**

Code | Issues 16 | Pull requests 2 | Projects 0 | Wiki

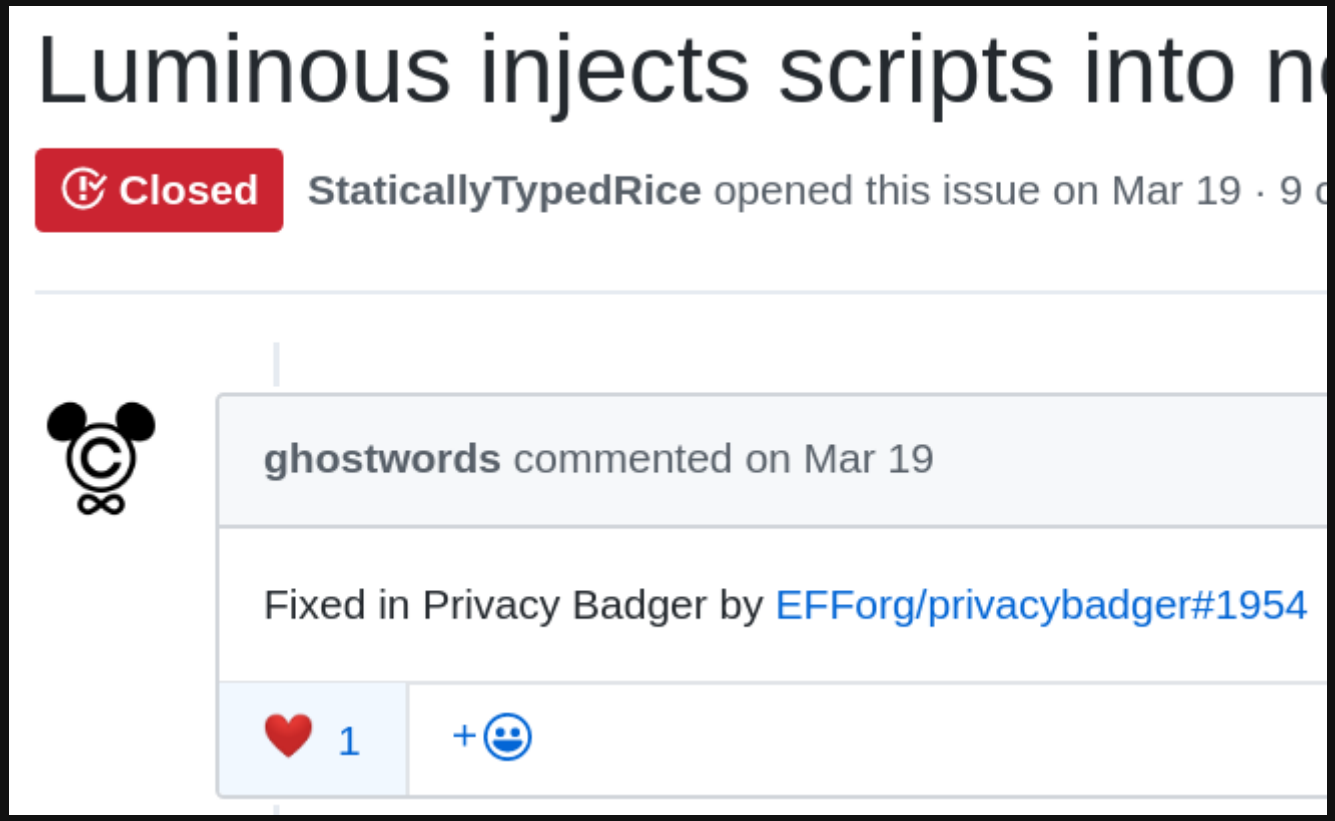
# Added Spanish Language #7

**Merged** **gbaptista** merged 11 commits into `gbaptista:master` from `SeppNel:master`

Conversation 1 | Commits 11 | Checks 0 | Files changed 6

# UX, UI, código, desempenho e dicas.

# Colaboração


Luminous injects scripts into n
Closed
StaticallyTypedRice opened this issue on Mar 19 · 9 c
ghostwords commented on Mar 19
Fixed in Privacy Badger by EFForg/privacybadger#1954
1

Estamos

# juntos

buscando o mesmo objetivo.

Não deixe o seu navegador agir como um malware que permite que qualquer site faça o quiser.

# Faça parte da resistência.

**O navegador é seu;**
**O computador é seu;**
**O celular é seu;**
**A energia elétrica é sua;**
**É a sua privacidade.**

# Estamos com tempo?

# Obrigado!

**https://github.com/gbaptista/luminous**

**https://github.com/gbaptista**

*(que foi comprado pela Microsoft)*

**guilhermebaptistasilva [at] gmail.com**

*(que vai ser usado pela Google pra vender banner)*