



CONVISO

IT SECURITY

# HTML5 Seguro ou Inseguro?

Wagner Elias

Gerente de Pesquisa e Desenvolvimento

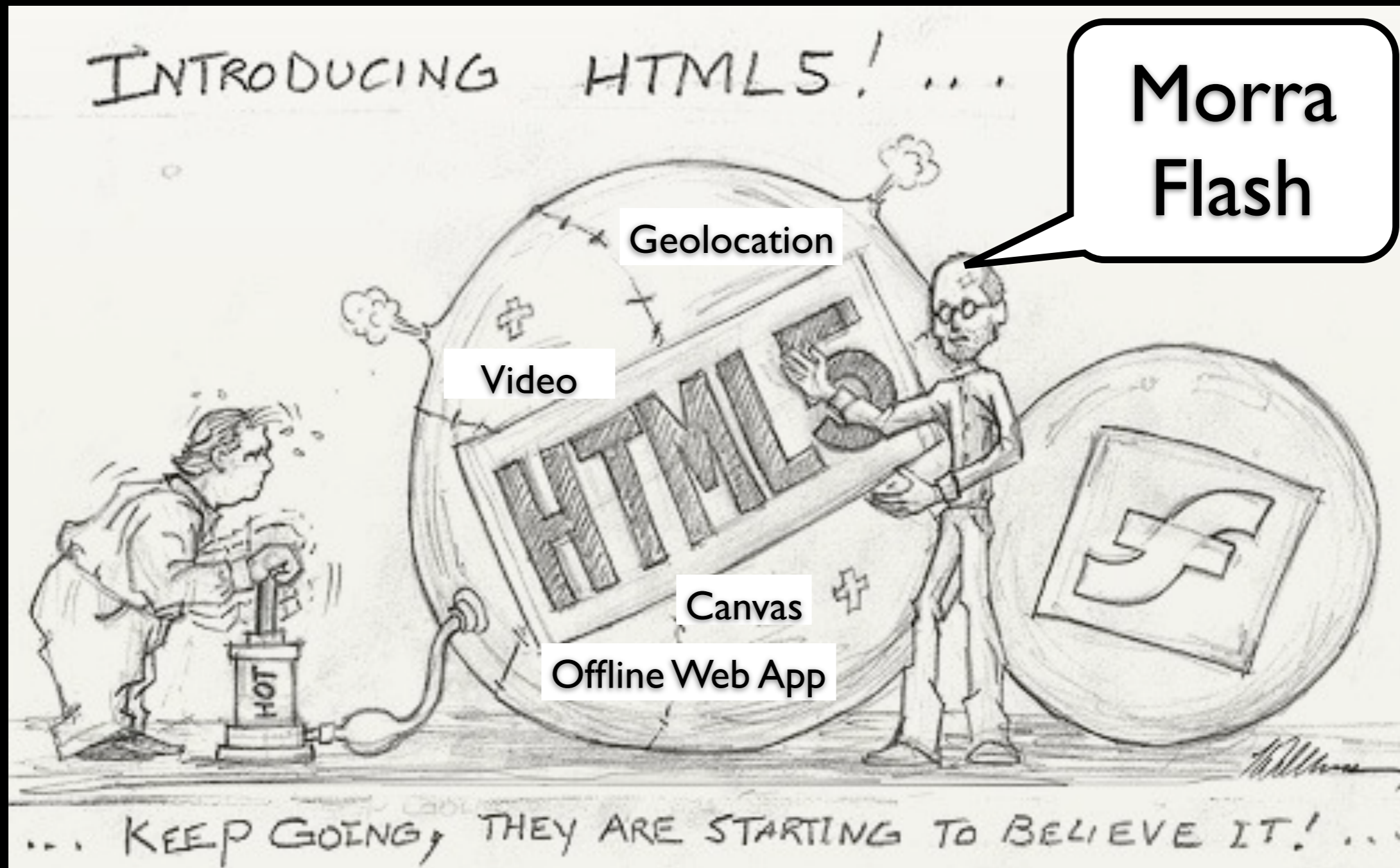
# Agenda

- **HTML5**
  - O que é?
  - Quem usa?
- **Alguns Recursos**
  - localStorage
  - WebSocket
- **Ele pode ser um big brother**
  - Navigator
  - Geolocation
- **Uma nova e eficaz abordagem para Botnets**
  - Geolocation
  - WebSocket
  - LocalStorage
- **Explorando**
  - Client-Side SQLi
  - Stored XSS
- **Conclusão**



# HTML5

# O que é?



# Quem usa?



# <HTML 5>

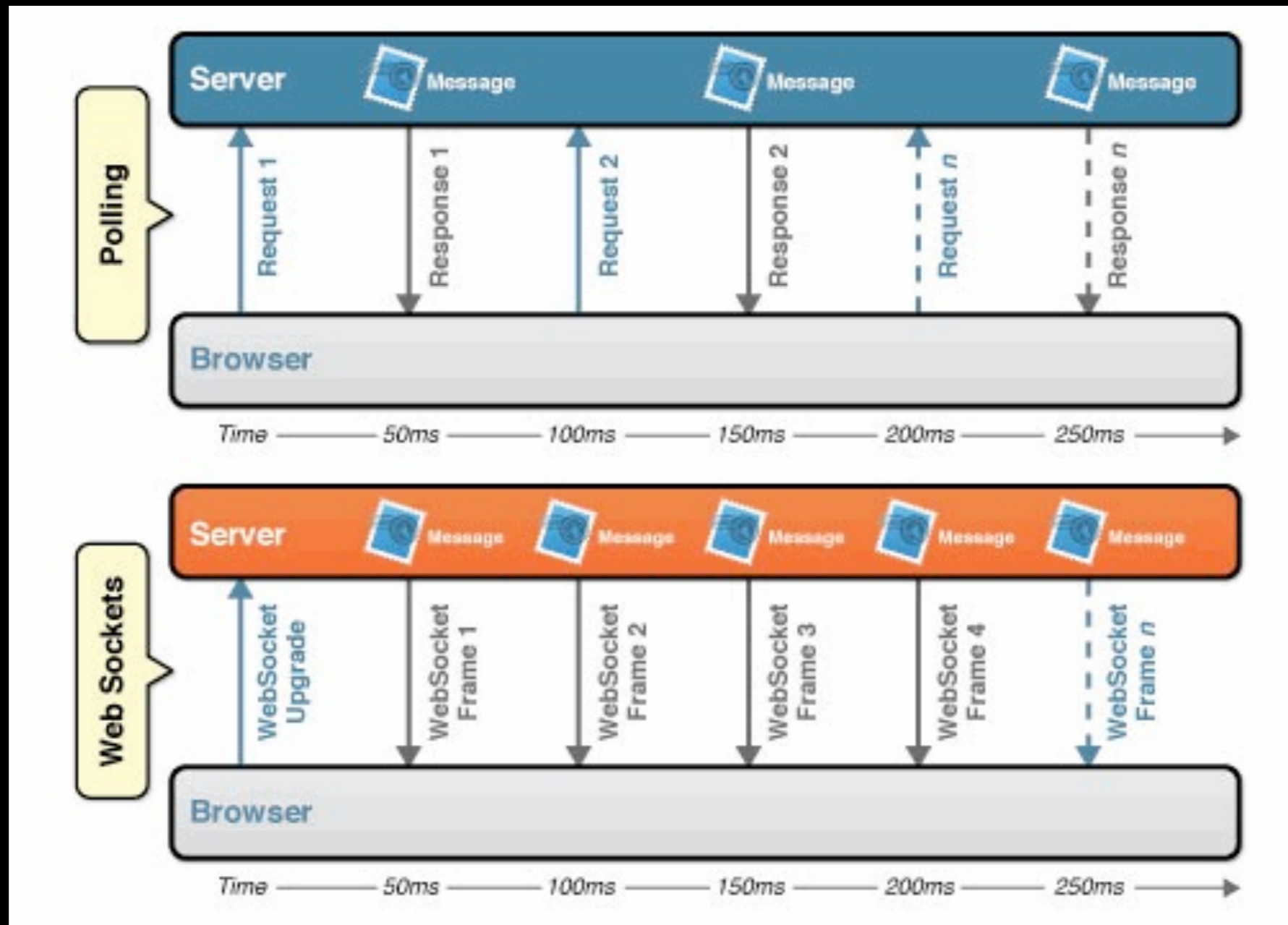


## Alguns Recursos

# localStorage



# Websockets

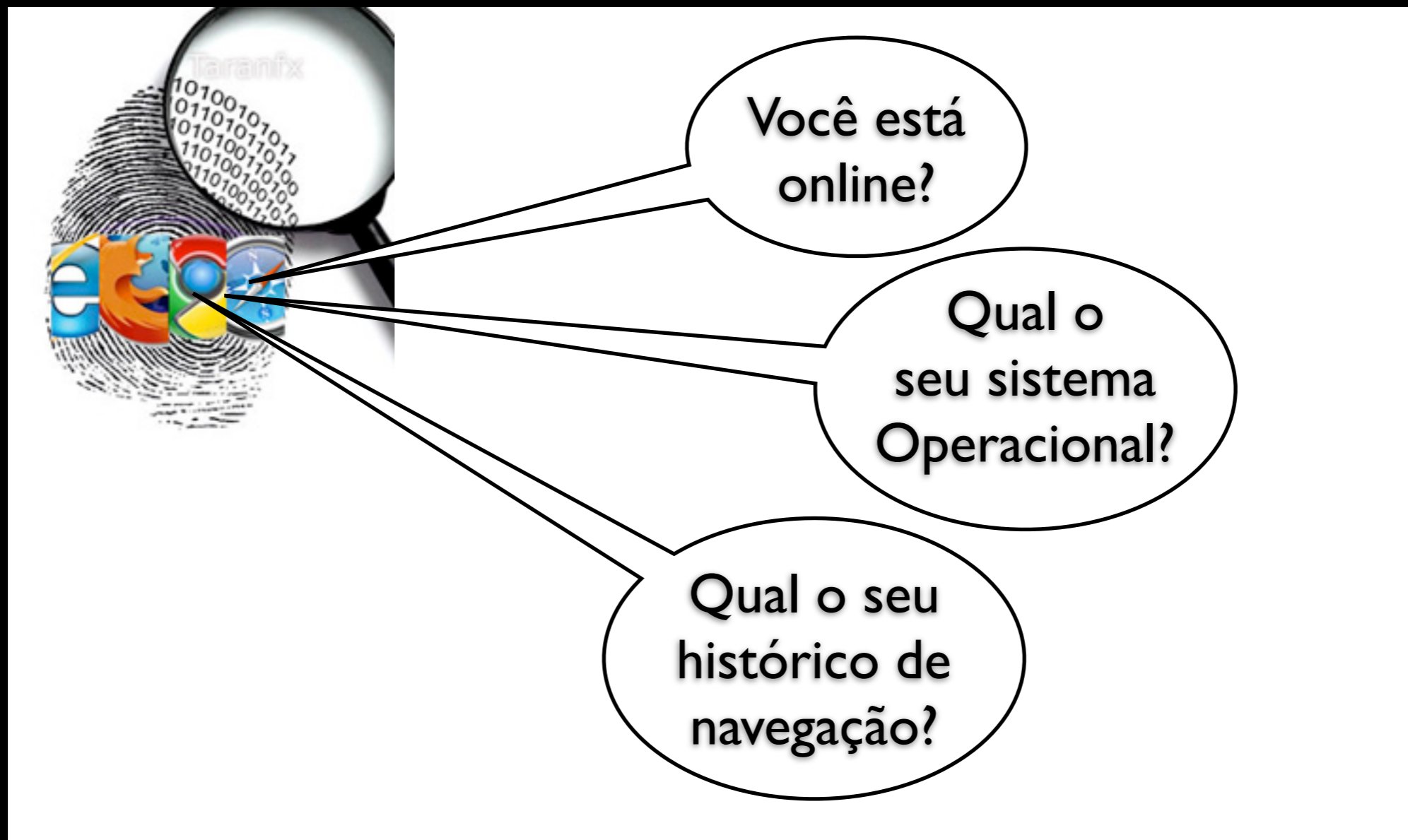






Ele pode ser um Big Brother

# Navigator



# Geolocation

The website "http://html5demos.com" would like to use your current location.

Request permission only once every 24 hours

Don't Allow Allow

**geolocation**

Finding your location: **found you!**

Vicente Nobrega

R. Heitor Peixoto

R. Basilio da Cunha

R. Gaspar Fernandes

R. Santa Flora

R. Porto Milião

R. Marajá

R. Monteiro

R. Pereira da

R. Itália Fausto

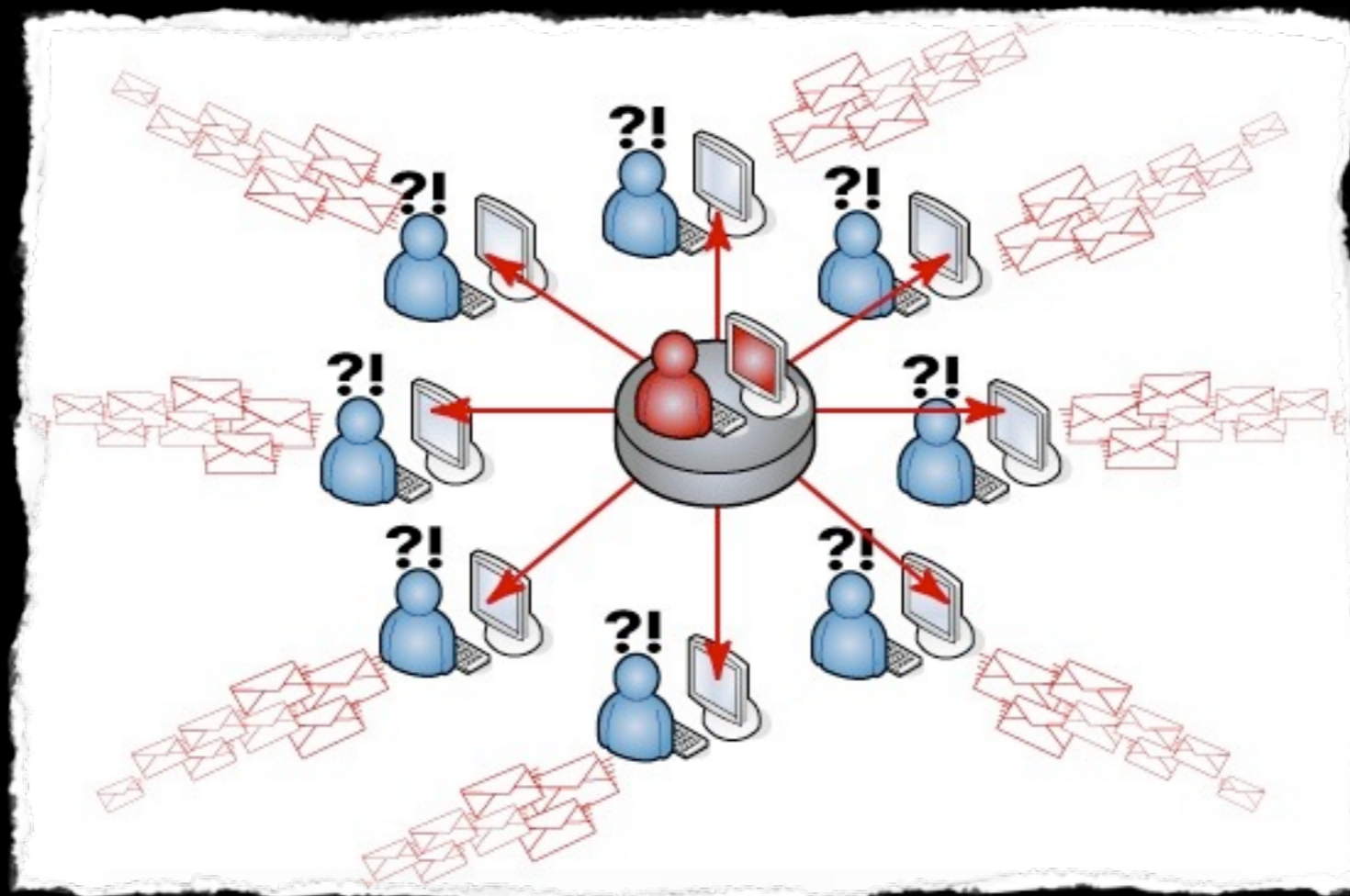
R. Raguena Cabral

R. Eiras Garcia

R. Covello

Map data ©2010 MapLink - [Terms of Use](#)

HTML5 demos / @rem built this / [view source](#)



# Uma nova e eficaz abordagem para Botnets

# Abordagem segmentada por região com Geolocation




# Usando WebSocket pode se ter uma comunicação entre os nós da Botnet rápida e menos barulhenta

SHODAN ws:// Search

» Top countries matching your search


<a href="#">Japan</a>	1
<a href="#">France</a>	1
<a href="#">Singapore</a>	0
<a href="#">Marshall Islands</a>	0
<a href="#">Honduras</a>	0

**95.141.97.244**  
Added on 09.11.2010  
  
95-141-97-244.stella-net.net

HTTP/1.0 101 Web Socket Protocol Handshake  
Upgrade: **WebSocket**  
Connection: Upgrade  
**WebSocket-Origin:** 192.168.0.43:9490  
**WebSocket-Location:** ws://192.168.0.43:9490/  
**WebSocket-Protocol:** sample

**163.43.160.56**  
Added on 05.11.2010  


HTTP/1.0 200 OK  
Upgrade: **WebSocket**  
Connection: Upgrade  
connection: close  
content-type: text/plain

LocalStorage e/ou Web Database permite armazenar código e estende os ataques a dispositivos móveis (Um foco do HTML5)





# Client-Side Exploit



# Client-Side SQLi



CONVISO  
IT SECURITY

## HTML5 Web Database - Client-Side SQLi demo


ID to test1: 8791101477490688

Tweet ID:

Tweeter	Tweets
<a href="#">Gregory D. Evans by Ligatt</a>	#pochtml5 Eu o maior hacker do mundo recomendo a H2HC... ;)
<a href="#">Willian Caprino</a>	#pochtml5 @welias falando sobre web2.0 na H2HC... Again!... ;)

\* PoC baseado no apresentado no AndLabs: <http://www.andlabs.org/html5/csSQLi.html>

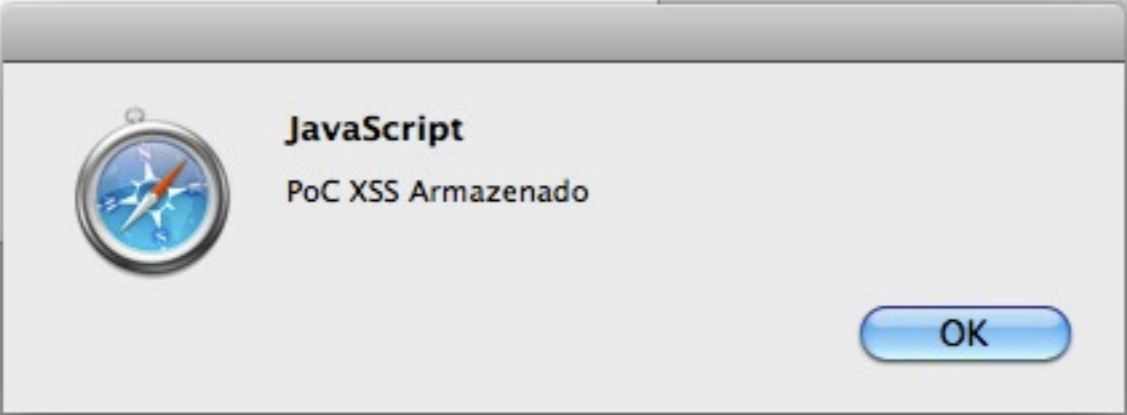
# Stored XSS

 CONVISO  
IT SECURITY

## HTML5 localStorage - Demo

Value: `<h1 onmouseover="alert('PoC XSS Armazenado')">Own3d!</h1>`

Name:

 JavaScript  
PoC XSS Armazenado  
OK

### Items

Name	Value
Stored XSS	<b>Own3d!</b>



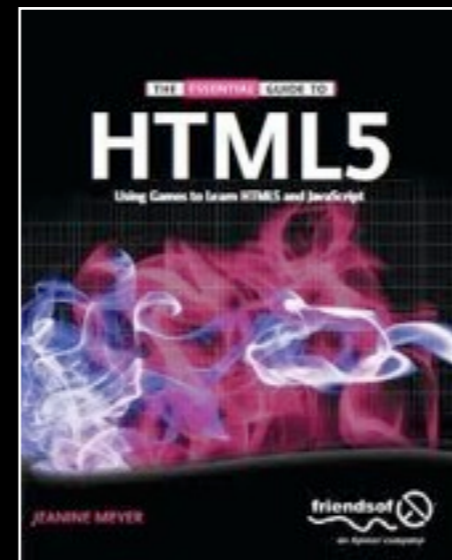
# Conclusão

# Conclusão

- Um avanço para aplicações web, mas ainda é cedo para adotá-lo. O próprio w3c pediu cautela
- Um novo desafio para ferramentas e profissionais que testam aplicações web
- Alguns recursos serão alvo de ataques e ações criminosas

# Referências

- <http://HTML5Rocks.com>
- <http://html5demos.com/>
- <http://websockets.org/>
- <http://dev.w3.org/html5/websockets/>



# Obrigado...



- **Blog:** <http://wagnerelias.com>
- **E-mail:** [welias@conviso.com.br](mailto:welias@conviso.com.br)
- **Twitter:** @welias