

Forum:[Hack Forums](#)

Thread: [HF phishing site](#)

KILLM3 - June 4, 2012, 12:54 pm

DO NOT VISIT THE FOLLOWING SITE AND INPUT INFORMATION.

[deleted]

Avoid this site.

EDIT: It does not appear to have a JDB.

<https://www.virustotal.com/url/91d27056bd0e08afa6ffdfbc4f004f5d9f6a3b18ae25f1382a727d74562e5d7/analysis/1338839649/>

EDIT2: No malicious scripts either. All scripts are being pulled straight from cdn2.hackforums.net
The only thing malicious are the Base64 encoded advertisements, which are monetizing off of omni's work and the login forms.

EDIT3:

Confirmed phishing site:

```
Code <form method="post" action="member.php"><input name="action" type="hidden"
value="do_login"><input name="url" type="hidden"
value="http://www.louisvuittonpurses4.com/"><input name="quick_login" type="hidden"
value="1"><input name="quick_username" id="quick_login_username" type="text"
value="Username/Email" class="textbox" onfocus="if(this.value == 'Username/Email') { this.value='';
}" onblur="if(this.value == '') { this.value='Username/Email'; }">&nbsp;<input
name="quick_password" id="quick_login_password" type="password" value="Password"
class="textbox" onfocus="if(this.value == 'Password') { this.value=''; }" onblur="if(this.value == '') {
this.value='Password'; }">&nbsp;<input name="submit" type="submit" value="Login"
class="button"><span class="remember_me"><input name="quick_remember"
id="quick_login_remember" type="checkbox" value="yes" class="checkbox"
checked="checked"><label for="quick_login_remember"> Remember me</label></span> — <a
href="https://hackforums.net/member.php?action=lostpw">Lost Password?</a> — <a
href="https://hackforums.net/member.php?action=register">Register</a></form>
```

Omega™ - June 4, 2012, 12:54 pm

I doubt anyone would visit that website.

However thanks op!

sh@d0w - June 4, 2012, 12:55 pm

Hahaha that's a fag thing for someone to do

Minnesota Nice - June 4, 2012, 12:55 pm

That is quite interesting I'd be surprised if anyone fell for that though.

Dr.Money - June 4, 2012, 12:56 pm

Thanks for the heads up man. Much thanks

JinxyHF - June 4, 2012, 12:57 pm

I'd hope nobody falls for that... Thanks for the heads up though.

KILLM3 - June 4, 2012, 12:58 pm

(Jun 4, 2012 12:55 PM)Minnesota Nice Wrote: [\[CITE\]](#) That is quite interesting I'd be surprised if anyone fell for that though.

If someone were to get infected, and their hosts file were changed...

hackforums.net = phishing site.

There'd be now way to tell the difference.

Snow - June 4, 2012, 12:59 pm

yeah if anyone seriously accidentally trys to login to that - ____ - that would be an epic fail lolz.

Trihunter3 - June 4, 2012, 1:00 pm

its weird though the ip is 1 diget off the same as hfs, and all the threads are the same there.

Oats??? - June 4, 2012, 1:00 pm

I have to say thats quite an impressive fake.

Either way doubt many are stupid enough to fall for it.

Oats

P?kachu - June 4, 2012, 1:00 pm

Wait, is it updating the same time this site is updating? Nobody will fall for it of course, the URL alone isnt anything like it lol. But still... how the fuck?

Failedattempt - June 4, 2012, 1:01 pm

Just the website name makes me laugh.

It'd be a shame if a user goes there and forgets about it then logs in.

Draw - June 4, 2012, 1:01 pm

For anyone who uses xerotic's scripts, they would notice that the added links at the top of the page are missing.

Th3PonyWizard - June 4, 2012, 1:05 pm

(Jun 4, 2012 01:00 PM)Oats Wrote: [\[CITE\]](#) I have to say thats quite an impressive fake.

Either way doubt many are stupid enough to fall for it.

Oats^This. Using the informative servers... Not bad. Gotta learn dis trick.

Haters Ganna Hate - June 4, 2012, 1:06 pm

I dont understand the URL and what its saying

DashPHP - June 4, 2012, 1:16 pm

Thanks OP, good find! :) I was starting to wonder how he his site is exactly the same lol

McFlurry - June 4, 2012, 1:20 pm

Thanks for the information regarding this. This hopefully will help a lot of members avoid going to that site.

Delete My Account Please - June 4, 2012, 1:23 pm

I reported it as a phishing site, shouldn't be long.

KILLM3 - June 4, 2012, 1:23 pm

(Jun 4, 2012 01:23 PM)Botaholic Wrote: [\[CITE\]](#) I reported it as a phishing site, shouldn't be long. For future reference, where did you report it? Also, thanks for doing that.

AnonymousPie - June 4, 2012, 1:26 pm

Thanks for the heads up OP.
Hope no one falls for it!

-AnonymousPie

Sol Yurick - June 4, 2012, 1:28 pm

Thank you very much for posting this, instead of ignoring the issue. In hopes that members figure it out themselves. Hopefully Omni will filter the site :).

??g????!? - June 4, 2012, 1:29 pm

Thanks for the advice buddy... hope noone is going to insert data there, and honestly that person have poor fantasy for the name choosen...

a ddos on it would be great... or just hack it and make ridiculous.

Jeppe K - June 4, 2012, 1:36 pm

thanks for making notice, i hope nobody went there

GG.Ox - June 4, 2012, 1:38 pm

ThankYOu for the wowsome info..great :)

SuaveSalmon - June 4, 2012, 1:41 pm

Seems very legit to me man?

(° ? °) - June 4, 2012, 1:46 pm

But it redirects to hackforums.net ? I don't get that part.

Diabolic - June 4, 2012, 1:46 pm

Thanks for the share, this will keep members aware.

Misaka - June 4, 2012, 1:50 pm

Pretty impressive clone. Thanks for sharing!

I could totally imagine this happening to some member of HF:

-Sees thread "HF phishing site"

-Interesting...

-Looks

-Opens link in a new tab

-Oh, nice clone!

-Forgets to close phishing site

-Later, while browsing, closes all tabs of HF except that one while spamming CTRL-Ws

-Oh I'm logged out. Oops

-GG.

TwinBlade - June 4, 2012, 1:51 pm

i Logged In with this Info :

Username : YourMom'sPussy

Password: IsSoHot

I hope he doesn't change my Password :\

screwtap3 - June 4, 2012, 1:52 pm

thanks for the heads up wasnt going to go to that sight and definitely wont now

FantaŠec - June 4, 2012, 1:52 pm

I tried logging in, it didnt work XD. The Email also didnt work. :/

Mr Kewl - June 4, 2012, 1:58 pm

<http://www.louisvuittonpurses4.com/>

This site is actually iFrame. It won't phish.

Taking my words back. Will have to recheck it.

KILLM3 - June 4, 2012, 2:19 pm

(Jun 4, 2012 01:58 PM)Mr Kewl Wrote: [\[CITE\]](#) <http://www.louisvuittonpurses4.com/>

This site is actually iFrame. It won't phish. You fail at trolling OP.

Huh...

So...why does its login panel send the data to the loisuvitton site...?

Oh wait, because it's a phishing site.

Just because it's loaded with an iframe doesnt change anything...

Mr Kewl - June 4, 2012, 2:25 pm

(Jun 4, 2012 02:19 PM)KILLM3 Wrote: [\[CITE\]](#) Huh...

So...why does its login panel send the data to the loisuvitton site...?

Oh wait, because it's a phishing site.

Just because it's loaded with an iframe doesnt change anything...

It does send the data to their site indeed, I need to recheck it, with an test account.

FantaŠec - June 4, 2012, 2:27 pm

(Jun 4, 2012 02:25 PM)Mr Kewl Wrote: [\[CITE\]](#) It does send the data to their site indeed, I need to recheck it, with an test account.

It wont let me login... I said that.

| ZooT | - June 4, 2012, 2:27 pm

It's not an iframe i don't think. Its just a cname/alias.

I don't think your details would be at an immediate risk.

Delete My Account Please - June 4, 2012, 2:29 pm

http://www.google.com/safebrowsing/report_phish/

<https://submit.symantec.com/antifraud/phish.cgi>

There are more.

Max™ - June 4, 2012, 2:35 pm

If anyone did fall for this , change your password ASAP.

Zain - June 4, 2012, 2:39 pm

That doesn't even seem like a good URL for a HF phishing site, what a fail.

(???)?(???? - June 4, 2012, 2:45 pm

Terrible URL but that's funny. How'd you find it?

| ZooT | - June 4, 2012, 3:09 pm

It's not a phisher. It's an alias domain.

(???)?(???? - June 4, 2012, 3:10 pm

(Jun 4, 2012 03:09 PM)ZooT ? Wrote: [\[CITE\]](#) It's not a phisher. It's an alias domain.

That's a phisher. Why does it say I'm logged out? hmmm.

TmasLove - June 4, 2012, 3:13 pm

Thats pretty funny, my favorite part is the URL. I did a fake login where the PW is

"F#CKYOUUB!T#H" hehe

| ZooT | - June 4, 2012, 3:30 pm

(Jun 4, 2012 03:10 PM)(???)?(???? Wrote: [\[CITE\]](#) That's a phisher. Why does it say I'm logged out? hmmm.

It's pointing to another ip in the same block.

ZooT\$ traceroute www.louisvuittonpurses4.com

traceroute to www.louisvuittonpurses4.com (216.245.194.198), 64 hops max, 40 byte packets

```
1 xxx (x.x.x.x) 2.401 ms 1.598 ms 10.955 ms
2
3 xxx (x.x.x.x) 156.328 ms 161.747 ms 156.324 ms
4 xxx (x.x.x.x) 156.287 ms 154.161 ms 162.908 ms
5 ge-2-1-0.mpr1.lhr2.uk.above.net (195.66.224.76) 205.142 ms 156.756 ms 153.264 ms
6 ge-2-1-0.mpr1.lhr2.uk.above.net (64.125.28.141) 153.226 ms 159.298 ms 175.909 ms
7 xe-5-2-0.cr1.dca2.us.above.net (64.125.26.21) 228.955 ms 222.781 ms 224.348 ms
8 xe-0-2-0.cr1.iah1.us.above.net (64.125.25.114) 251.617 ms 256.660 ms 256.389 ms
9 xe-2-1-0.cr1.dfw2.us.above.net (64.125.30.58) 257.880 ms 335.923 ms 261.015 ms
10 xe-0-1-0.mpr1.dfw1.us.above.net (64.125.27.209) 254.241 ms 262.291 ms 259.420 ms
11 64.125.188.182.t00822-03.above.net (64.125.188.182) 261.854 ms 264.861 ms 256.758 ms
12 te6-1.bdr2.core2.dllstx3.dallas-idc.com (208.115.192.62) 271.841 ms 200.230 ms 264.493 ms
13 ge0-2.vl317.cr02-108.dllstx3.dallas-idc.com (64.31.4.94) 265.248 ms 261.503 ms
14 ge0-2.vl317.cr02-108.dllstx3.dallas-idc.com (64.31.4.94) 260.425 ms !X
ge0-1.vl316.cr02-108.dllstx3.dallas-idc.com (64.31.4.90) 264.012 ms !X
```

ZooT\$ traceroute hackforums.net

traceroute: Warning: hackforums.net has multiple addresses; using 216.245.194.195

traceroute to hackforums.net (216.245.194.195), 64 hops max, 40 byte packets

```
1 xxx (x.x.x.x) 3.958 ms 2.113 ms 1.833 ms
2
3 xxx (x.x.x.x) 138.346 ms 138.939 ms 153.678 ms
4 xxx (x.x.x.x) 128.014 ms 154.220 ms 155.582 ms
5 * ge-2-1-0.mpr1.lhr2.uk.above.net (195.66.224.76) 63.040 ms 62.458 ms
6 ge-2-1-0.mpr1.lhr2.uk.above.net (64.125.28.141) 63.403 ms 64.511 ms 63.944 ms
7 xe-5-2-0.cr1.dca2.us.above.net (64.125.26.21) 134.630 ms 146.209 ms 134.511 ms
8 xe-0-2-0.cr1.iah1.us.above.net (64.125.25.114) 161.188 ms 254.270 ms 253.169 ms
9 xe-2-1-0.cr1.dfw2.us.above.net (64.125.30.58) 257.820 ms 260.389 ms 257.572 ms
10 xe-0-1-0.mpr1.dfw1.us.above.net (64.125.27.209) 261.402 ms 301.406 ms 257.914 ms
```

11 64.125.188.182.t00822-03.above.net (64.125.188.182) 169.488 ms 166.846 ms 166.872 ms
12 te6-1.bdr2.core1.dllstx3.dallas-idc.com (208.115.192.58) 174.482 ms
te6-1.bdr2.core2.dllstx3.dallas-idc.com (208.115.192.62) 173.996 ms 173.069 ms
13 ge0-2.vl317.cr02-108.dllstx3.dallas-idc.com (64.31.4.94) 168.352 ms 172.987 ms 256.144 ms
14 ge0-2.vl317.cr02-108.dllstx3.dallas-idc.com (64.31.4.94) 257.181 ms !X
ge0-1.vl316.cr02-108.dllstx3.dallas-idc.com (64.31.4.90) 263.873 ms !X
ge0-2.vl317.cr02-108.dllstx3.dallas-idc.com (64.31.4.94) 263.266 ms !X

KILLM3 - June 4, 2012, 3:33 pm

(Jun 4, 2012 03:30 PM)ZooT ? Wrote: [\[CITE\]](#) It's pointing to another ip in the same block.

ZooT\$ traceroute www.louisvuittonpurses4.com

traceroute to www.louisvuittonpurses4.com (216.245.194.198), 64 hops max, 40 byte packets

1 xxx (x.x.x.x) 2.401 ms 1.598 ms 10.955 ms
2
3 xxx (x.x.x.x) 156.328 ms 161.747 ms 156.324 ms
4 xxx (x.x.x.x) 156.287 ms 154.161 ms 162.908 ms
5 ge-2-1-0.mpr1.lhr2.uk.above.net (195.66.224.76) 205.142 ms 156.756 ms 153.264 ms
6 ge-2-1-0.mpr1.lhr2.uk.above.net (64.125.28.141) 153.226 ms 159.298 ms 175.909 ms
7 xe-5-2-0.cr1.dca2.us.above.net (64.125.26.21) 228.955 ms 222.781 ms 224.348 ms
8 xe-0-2-0.cr1.iah1.us.above.net (64.125.25.114) 251.617 ms 256.660 ms 256.389 ms
9 xe-2-1-0.cr1.dfw2.us.above.net (64.125.30.58) 257.880 ms 335.923 ms 261.015 ms
10 xe-0-1-0.mpr1.dfw1.us.above.net (64.125.27.209) 254.241 ms 262.291 ms 259.420 ms
11 64.125.188.182.t00822-03.above.net (64.125.188.182) 261.854 ms 264.861 ms 256.758 ms
12 te6-1.bdr2.core2.dllstx3.dallas-idc.com (208.115.192.62) 271.841 ms 200.230 ms 264.493 ms
13 ge0-2.vl317.cr02-108.dllstx3.dallas-idc.com (64.31.4.94) 265.248 ms 261.503 ms
14 ge0-2.vl317.cr02-108.dllstx3.dallas-idc.com (64.31.4.94) 260.425 ms !X
ge0-1.vl316.cr02-108.dllstx3.dallas-idc.com (64.31.4.90) 264.012 ms !X

ZooT\$ traceroute hackforums.net

traceroute: Warning: hackforums.net has multiple addresses; using 216.245.194.195

traceroute to hackforums.net (216.245.194.195), 64 hops max, 40 byte packets

1 xxx (x.x.x.x) 3.958 ms 2.113 ms 1.833 ms
2
3 xxx (x.x.x.x) 138.346 ms 138.939 ms 153.678 ms
4 xxx (x.x.x.x) 128.014 ms 154.220 ms 155.582 ms
5 * ge-2-1-0.mpr1.lhr2.uk.above.net (195.66.224.76) 63.040 ms 62.458 ms
6 ge-2-1-0.mpr1.lhr2.uk.above.net (64.125.28.141) 63.403 ms 64.511 ms 63.944 ms
7 xe-5-2-0.cr1.dca2.us.above.net (64.125.26.21) 134.630 ms 146.209 ms 134.511 ms
8 xe-0-2-0.cr1.iah1.us.above.net (64.125.25.114) 161.188 ms 254.270 ms 253.169 ms
9 xe-2-1-0.cr1.dfw2.us.above.net (64.125.30.58) 257.820 ms 260.389 ms 257.572 ms
10 xe-0-1-0.mpr1.dfw1.us.above.net (64.125.27.209) 261.402 ms 301.406 ms 257.914 ms
11 64.125.188.182.t00822-03.above.net (64.125.188.182) 169.488 ms 166.846 ms 166.872 ms
12 te6-1.bdr2.core1.dllstx3.dallas-idc.com (208.115.192.58) 174.482 ms
te6-1.bdr2.core2.dllstx3.dallas-idc.com (208.115.192.62) 173.996 ms 173.069 ms
13 ge0-2.vl317.cr02-108.dllstx3.dallas-idc.com (64.31.4.94) 168.352 ms 172.987 ms 256.144 ms
14 ge0-2.vl317.cr02-108.dllstx3.dallas-idc.com (64.31.4.94) 257.181 ms !X
ge0-1.vl316.cr02-108.dllstx3.dallas-idc.com (64.31.4.90) 263.873 ms !X
ge0-2.vl317.cr02-108.dllstx3.dallas-idc.com (64.31.4.94) 263.266 ms !X

What I don't understand is, if it's literally just a portal to HF's server, why aren't my cookies accepted and me be logged in?

Or am I misunderstanding you?

c0mrade - June 4, 2012, 3:34 pm

I am sure the current owner of Hackforums will take legal action.

Glassy - June 4, 2012, 3:35 pm

Max™ Wrote: [\[CITE\]](#) If anyone did fall for this , change your password ASAP.I don't think it would do any harm, although it would definitely be a good idea to change your password and private information immediately so there is no cause.

Zain Wrote: [\[CITE\]](#) That doesn't even seem like a good URL for a HF phishing site, what a fail. I don't think the site has that URL so people could type it. It's maybe in a use in which someone spams emails to others with a link that automatically directs them to the copyrighted site.

(?°??°)?(???? Wrote: [\[CITE\]](#) Terrible URL but that's funny. How'd you find it? Was wondering the same thing as how someone can actually look up sites that are duplicate or sites that redirect it to HF directory.

Xenochrist - June 4, 2012, 3:35 pm

Maybe Omni is into purses and bought this domain a while ago?

I kid, I kid!

| ZooT | - June 4, 2012, 3:36 pm

The domain is just a cname or alias of hackforums.net i think.

You aren't logged in because your browser cookies recognise the domain not the ip.

Glassy - June 4, 2012, 3:38 pm

Xenochrist Wrote: [\[CITE\]](#) Maybe Omni is into purses and bought this domain a while ago?

I kid, I kid!

Omni does purchase domains and have them redirect to Hackforums directory, but I doubt it would be this type of domain, especially since there are bugs on the site.

Stuck In Your Radio - June 4, 2012, 3:39 pm

Oh damn, you found my phishing site.

Good job everyone. Mystery solved.

Glassy - June 4, 2012, 3:41 pm

Stuck In Your Radio Wrote: [\[CITE\]](#) Oh damn, you found my phishing site.

Good job everyone. Mystery solved.

Do you know that you are claiming to be in charge of a copyrighted and illegal material.

Stuck In Your Radio - June 4, 2012, 3:42 pm

(Jun 4, 2012 03:41 PM)Glassy Wrote: [\[CITE\]](#) Do you know that you are claiming to be in charge of a copyrighted and illegal material.

Yes. I was using the message sarcastically though, so it was kind of obvious I don't really own it.

Foco - June 4, 2012, 3:44 pm

Colour me impressed.

Also for the people saying its a bad fake for the URL. It really doesn't matter, its not like their getting any organic SEO traffic. They would use this in conjunction with DNS hijacking to steal accounts

KILLM3 - June 4, 2012, 3:44 pm

(Jun 4, 2012 03:42 PM)Stuck In Your Radio Wrote: [\[CITE\]](#) Yes. I was using the message sarcastically though, so it was kind of obvious I don't really own it.

Hey guys! We caught him! He's right over here!

Stuck In Your Radio - June 4, 2012, 3:45 pm

(Jun 4, 2012 03:44 PM)KILLM3 Wrote: [\[CITE\]](#) Hey guys! We caught him! He's right over here! Oh damn.

Best hurry on over to the Batmobile and escape.

Trihunter3 - June 4, 2012, 3:52 pm

who knows maybe this is just one of the hundreds of domains omni owns and its redirected toward hackforums.net on a record A label etc.

Diabolic - June 4, 2012, 3:53 pm

I believe someone posted this link in the lounge somewhere within a post not so long ago.

BlackHops - June 4, 2012, 4:23 pm

I've seen several fakes like this, but most were just one page

Ruzlier - June 4, 2012, 4:26 pm

You idiots, it wouldn't be a "FAIL" it is so easy to mask a url, and most people don't double check the URL bar once they are at it to make sure it's hackforums, and even if they do, I doubt 100% of people will do it. Nice phishing page, 0/10 to the faggots crying.. How can you call yourself a hacker then cry over a phishing page? PFFT.

Glassy - June 4, 2012, 4:26 pm

BlackHops Wrote: [\[CITE\]](#) I've seen several fakes like this, but most were just one page
If you do see duplicated Hackforums sites, then report it to Omni.

Kangaroo?? - June 4, 2012, 4:28 pm

(Jun 4, 2012 12:54 PM)Omega™ Wrote: [\[CITE\]](#) I doubt anyone would visit that website.
However thanks op!Yeah me too doesn't even look like hackforums.net

192837465 - June 4, 2012, 4:30 pm

It's basically the same thing, just using the same database and scripts kind of. I don't know how to say it, but I know what it is doing. My friend did it to Minecraft.net and got over 100 accounts.

Bobby22 - June 4, 2012, 4:32 pm

He just click CTRL+S on a google chrome web page, then modified the login system to his liking's and then uploaded it to an FTP server with his domain.

h?cker22 - June 4, 2012, 4:34 pm

There's so many of those, I've come across a bunch. Am I supposed report them/make a thread?

Omniscient - June 4, 2012, 4:52 pm

It's not a phishing site. I have many IPs unused and this site just had an A record pointed to the server. I've made adjustments so that this won't happen again.