Who is Mr Dong?

intrusiontruth.wordpress.com/2017/05/05/who-is-mr-dong

intrusiontruth May 5, 2017

In our last post we showed how, through WHOIS data, it is possible to identify Wu Yingzhuo, an APT3 operator who registered domain names for the group and advertised online offering help with Trojan development.

The story finished with http[.]net, a domain name that we showed was connected to APT3, and that was registered to Yingzhuo Wu. In this post we will show how the trail continues and allows us to identify a second APT3 member, Mr Dong.

From httb to biglit

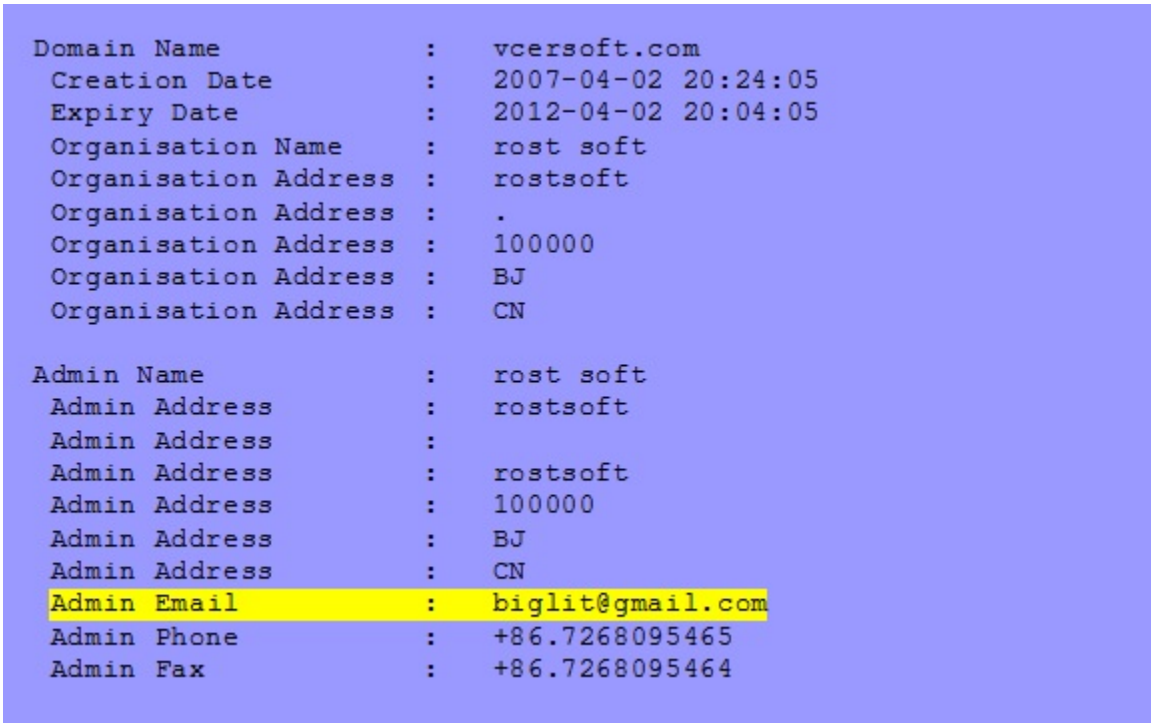
DNS research on httb[.]net reveals a second IP address: 61.129.67[.]53. Three other interesting domains have previously resolved to it. They are vcersoft[.]com, uyre[.]net and inc-work[.]com.

61.129.67.53

	First	Last
ssl.httb.net	2011-07-11	2013-04-26
ssl1.ciscocorp.com	2011-07-10	2012-04-02
messenger.vcersoft.com	2011-07-11	2011-07-14

Historic DNS resolutions showing a vcersoft domain pointing to 61.129.67[.]53

Note also the inclusion of ciscocorp[.]com in the list above – it is one of the domains associated with the wyz5678[at]163.net address associated with Wu Yingzhuo.
Looking at the three newly identified domains, WHOIS information for all three includes a new e-mail address, biglit[at]gmail.com.



```
Domain Name              :   vcersoft.com
 Creation Date           :   2007-04-02 20:24:05
 Expiry Date             :   2012-04-02 20:04:05
 Organisation Name       :   rost soft
 Organisation Address    :   rostsoft
 Organisation Address    :   .
 Organisation Address    :   100000
 Organisation Address    :   BJ
 Organisation Address    :   CN

Admin Name               :   rost soft
 Admin Address           :   rostsoft
 Admin Address           :
 Admin Address           :   rostsoft
 Admin Address           :   100000
 Admin Address           :   BJ
 Admin Address           :   CN
 Admin Email             :   biglit@gmail.com
 Admin Phone             :   +86.7268095465
 Admin Fax               :   +86.7268095464
```

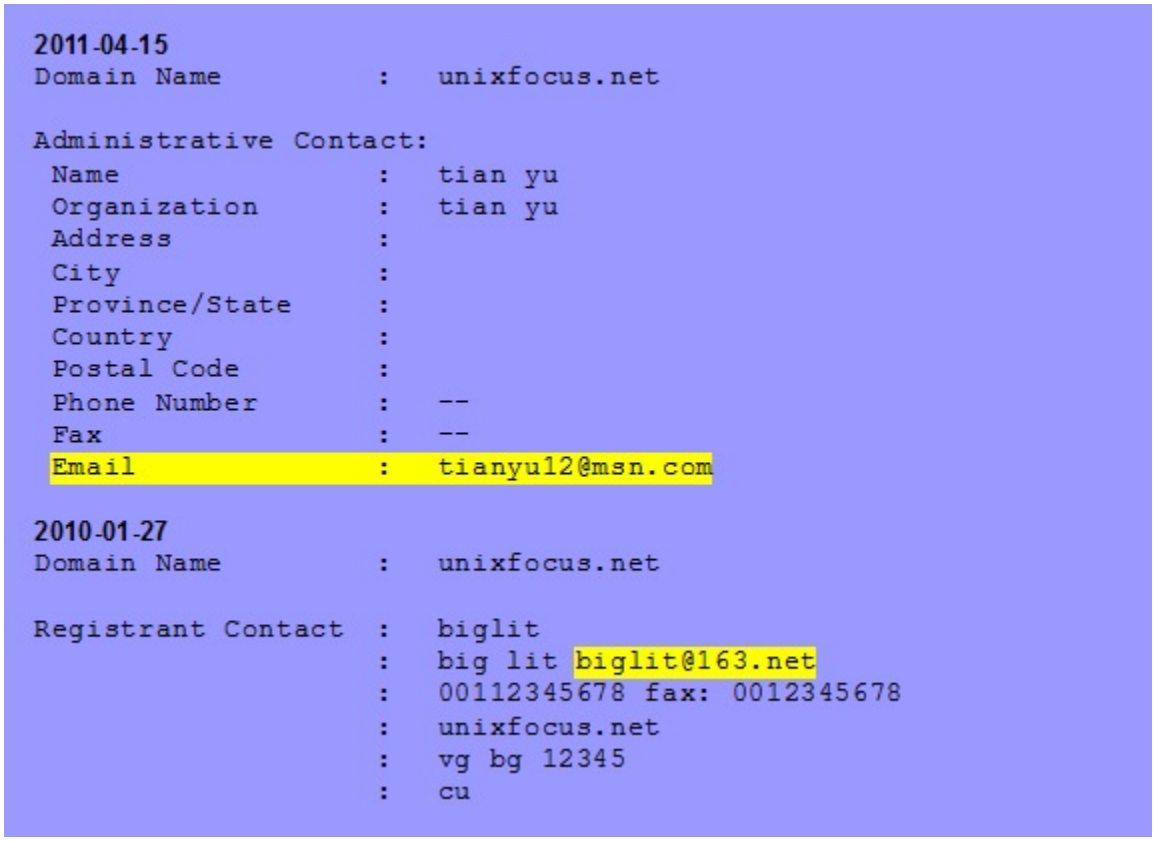
Historic WHOIS data for vcersoft[.]com includes biglit[at]gmail.com

From biglit to tianyu

The biglit e-mail address appeared in registration information for a number of other domains, including microsoft-ie[.]com. Historic WHOIS information for this domain includes the e-mail address tianyu12[at]msn.com.

And back to biglit

In addition to the microsoft-ie[.]com domain, the tianyu12 e-mail address also appeared in registration data for unixfocus[.]net. But tianyu12 was not the only e-mail address that appears in historic registration data for the domain. A previous address was biglit[at]163.net, similar to the biglit g-mail address mentioned earlier.



```
2011-04-15
Domain Name          :   unixfocus.net

Administrative Contact:
 Name                :   tian yu
 Organization        :   tian yu
 Address             :
 City                :
 Province/State      :
 Country             :
 Postal Code         :
 Phone Number        :   --
 Fax                 :   --
 Email               :   tianyu12@msn.com

2010-01-27
Domain Name          :   unixfocus.net

Registrant Contact   :   biglit
                     :   big lit biglit@163.net
                     :   00112345678 fax: 0012345678
                     :   unixfocus.net
                     :   vg bg 12345
                     :   cu
```

Historic WHOIS for unixfocus[.]net shows biglit[at]163.net

Dong Hao

Completing the chain, the new biglit address appeared in the WHOIS information for another new domain: shuyan[.]com. And the name that appeared in the shuyan registration record was … Dong Hao.

```
Domain Name:shuyan.com

Registrant:
dong hao
      C10 F Chen Jian Building, 189# Ti Yu Xi Road, Guang Dong
      501620

Administrative Contact:
dong hao
      dong hao
      C10 F Chen Jian Building, 189# Ti Yu Xi Road, Guang Dong
      Guang Dong Guangdong 501620
      China
      tel: 86 0 13066385472
      fax: 86 0 13066385472
      tianyu@email.com.cn

Billing Contact:
dong hao
      C10 F Chen Jian Building, 189# Ti Yu Xi Road, Guang Dong
      Guang Dong Guangdong 501620
      China
      tel: 86 0 13066385472
      fax: 86 0 13066385472
      biglit@163.net

Registration Date: 2002-06-04
      Update Date: 2002-06-04
  Expiration Date: 2006-06-04
```

Historic WHOIS data for shuyan[.]com shows biglit[at]163.net

So, from the httb[.]net domain identified in our last post and registered by Wu Yingzhuo, we have followed a chain through a server in Shanghai, vcersoft[.]com, microsoft-ie[.]com and unixfocus[.]net to find Dong Hao, a second APT3 operator involved in registering domain names.

But who are Wu Yingzhuo and Dong Hao? We will reveal soon exactly where they work, and from whom they receive their orders. Read our next post for more truth behind this intrusion.