Who is Mr Gao?

intrusiontruth.wordpress.com/2018/08/02/who-is-mr-gao

intrusiontruth August 2, 2018

The menuPass Sample

Hidden on Page 24 of the FireEye report referenced in our previous article, is the start of a thread that, if pulled, leads to more APT10 individuals. It is a Poison Ivy sample (b08694e14a9b966d8033b42b58ab727d). The sample connects to a C2 server at js001.3322[.]org. Incidentally, the connection password used by the sample is “xiaoxiaohuli”, Chinese for “littlelittlefox” (小小狐狸), a useful data point that helps to confirm the connection to China.

The FireEye Poison Ivy report containing menuPass samples

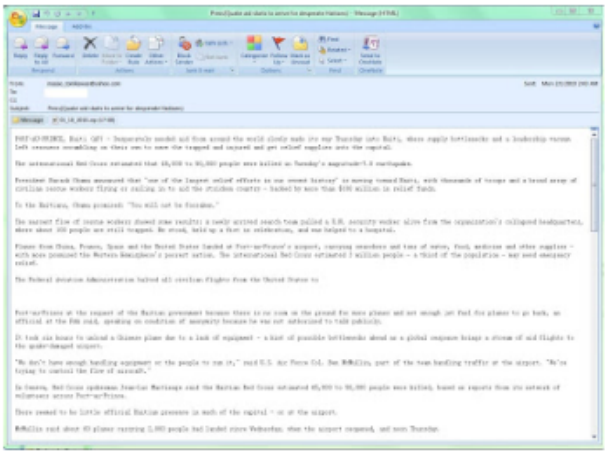
js001.3322[.]org to 222.35.137[.]193

In 2010, around the time of this APT10 activity, the domain js001.3322[.]org resolved to IP address 222.35.137[.]193 , an IP address in Beijing, China.

The IP address 222.35.137[.]193 has other connections to APT10 too. A search of other domains that have resolved to the IP reveals that weile3322b.3322[.]org resolved to the IP between 23 January 2010 and 15 February 2012. The weile3322b domain is listed as an APT10 domain in commercial threat intelligence reporting. The IP address can therefore be said to have been associated with APT10 for a significant period of time.

222.35.137[.]193 to Tianjin, China

Analysis of a further Poison Ivy malware sample (a4754be7b34ed55faff832edadac61f6) from early 2010 indicates that it connected to the same 222.35.137[.]193 IP address in Beijing. This malware was initially distributed in an e-mail phishing campaign originating from masao_tomikawas[at]yahoo.com. There is a complete analysis available at Contagio.



From: masao_tomikawas@yahoo.com
[mailto:masao_tomikawas@yahoo.com]
Sent: Monday, February 01, 2010 2:43 AM
To:
Subject: Press(Quake aid starts to arrive for desperate Haitians)

PORT-AU-PRINCE, Haiti (AP) - Desperately needed aid from around the world slowly made its way Thursday into Haiti, where supply bottlenecks and a leadership vacuum left rescuers scrambling on their own to save the trapped and injured and get relief supplies into the capital.

.....

see the full text in the end of the post

Headers

```
Received: (qmail 17548 invoked from network); 1 Feb 2010 07:43:09 -0000
Received: from unknown (HELO fisherxp-pc.domain) (218.67.128.26)
  by XXXXXXXXXXXXXX SMTP; 1 Feb 2010 07:43:09 -0000
Received: from 1428151.com ([127.0.0.1]) by 1428151.com ([127.0.0.1]) with SMTPSVC;
     Mon, 01 Feb 2010 15:43:07 +0800
Message-ID: <6dd17374c7e8d17543324b690c0db2e7@yahoo.com>
From:
To: XXXXXXXXXXXXXXXXXXXXXXXX
Subject: =?gb2312?B?UHJlc3MoUXVha2UgYWlkIHN0YXJ0cyB0byBhcnJpdmUgZm9yIGRlcw==?=
    =?gb2312?B?cGVyYXRlIEhhaXRpYW5zKQ==?=
Date: Mon, 01 Feb 2010 15:43:07 +0800
```

Analysis of an APT10 spam e-mail originating from 218.67.128[.]26

Inspection of the SMTP headers for the original e-mail campaign reveals the originating IP address of the campaign, 218.67.128[.]26. That IP address resolves to China Unicom in Tianjin. Whoever is behind APT10, therefore, could well be based in Tianjin.

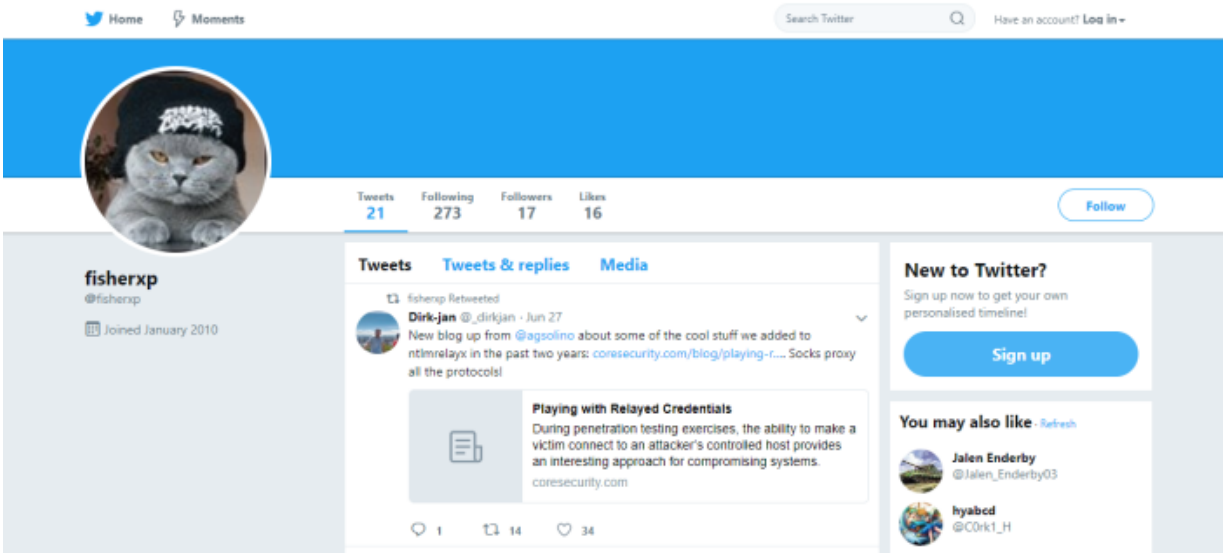
```
inetnum:        218.67.128.0 - 218.69.255.255
netname:        UNICOM-TJ
country:        CN
descr:          China Unicom Tianjin province network
descr:          China Unicom
admin-c:        CH1302-AP
tech-c:         HZ19-AP
status:         ALLOCATED PORTABLE
mnt-by:         APNIC-HM
mnt-lower:      MAINT-CNCGROUP-TJ
mnt-routes:     MAINT-CNCGROUP-RR
remarks:        This object can only be modified by APNIC hostmaster
remarks:        If you wish to modify this object details please
remarks:        send email to hostmaster@apnic.net with your organisation
remarks:        account name in the subject line.
mnt-irt:        IRT-CU-CN
last-modified:  2013-08-08T23:30:06Z
source:         APNIC
```

218.67.128[.]26 sits inside an IP block that resolves to Tianjin, China

fisherxp

Also hidden in the SMTP headers of the spam e-mail is the hostname of the computer that submitted the e-mail – fisherxp-pc[.]domain. fisherxp is a relatively unique name that we believe has been used by one of the APT10 actors for some time.

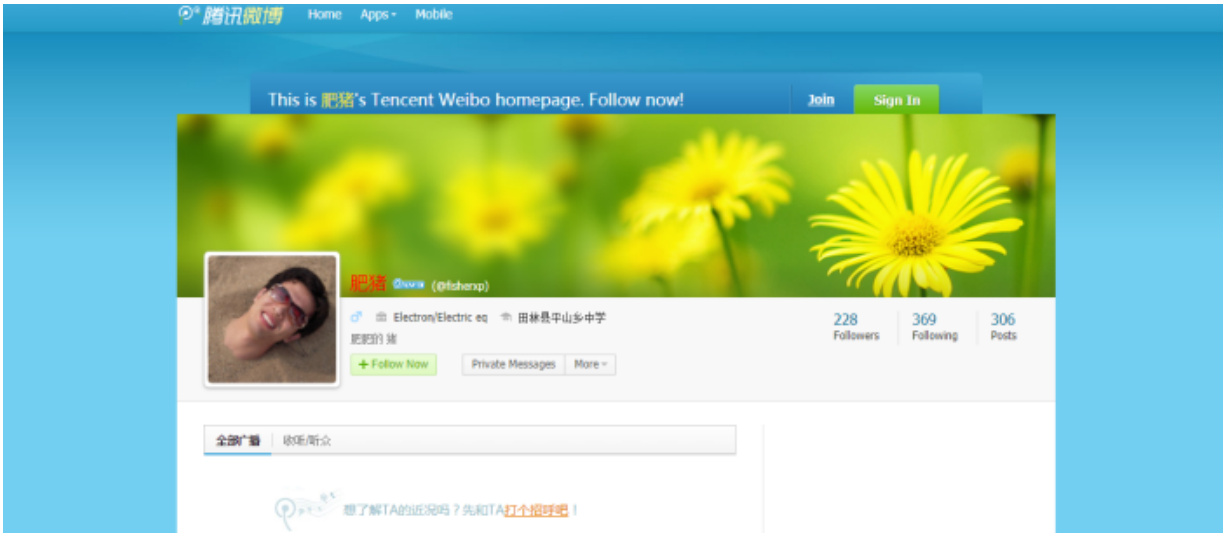
Twitter account @fisherxp was registered in January 2010 and has posted 11 times. Most are hacking or information security related retweets in English or Chinese.



fisherxp Twitter account

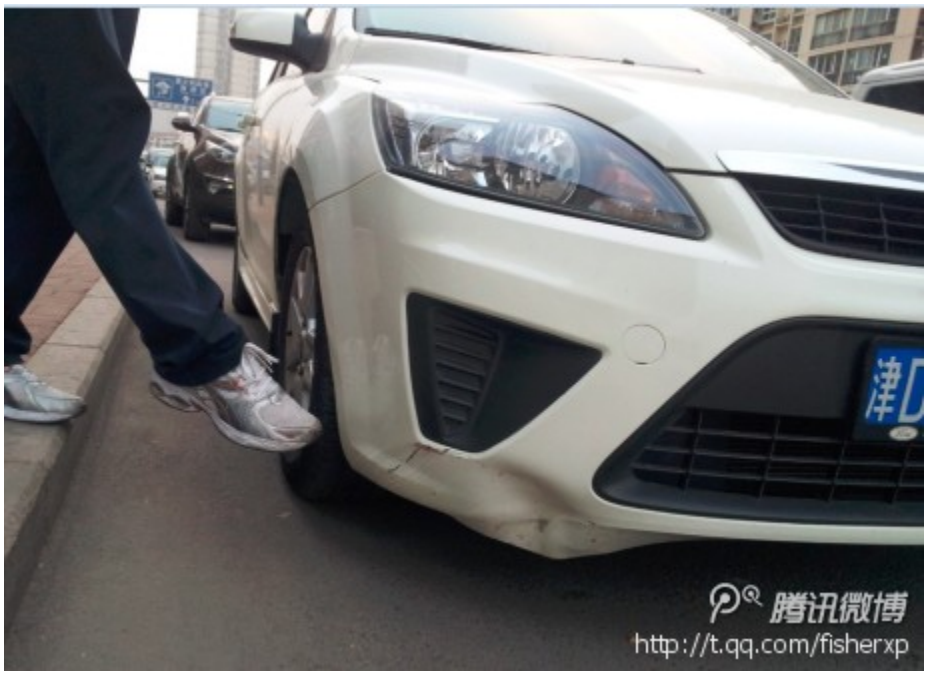
In further confirmation of the account owner's association with (or at least interest in) APT10, the account began following @intrusion_truth the day after this blog exposed APT10 actor Zheng Yanbin.

@fisherxp is also a valid Tencent Weibo QQ account containing a photo of, presumably, the owner of the account.



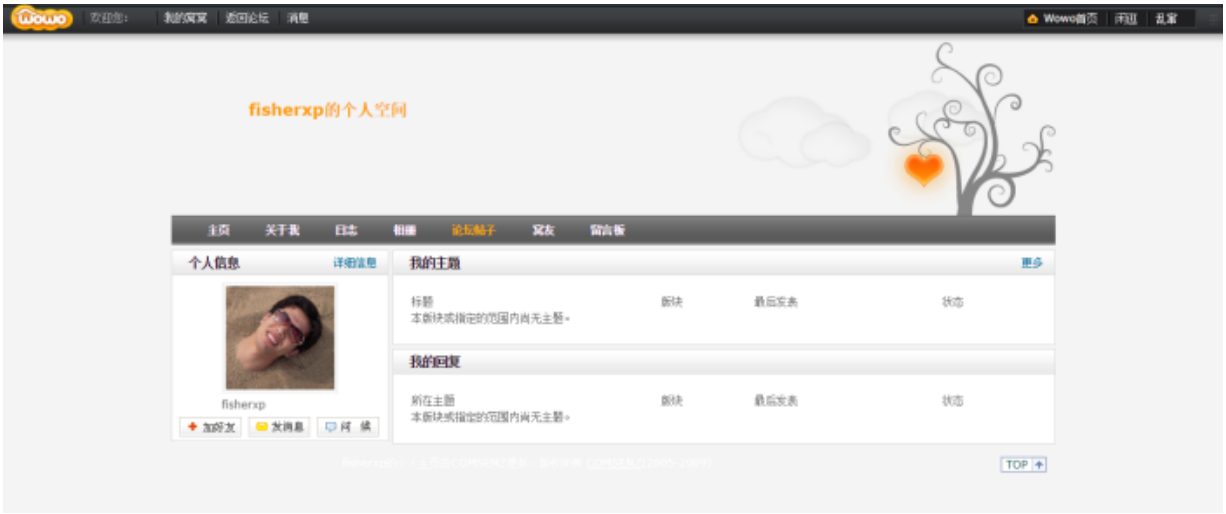
fisherxp's QQ account

The QQ feed contains years worth of postings. Amongst them is a photograph of a car belonging to the owner of the feed. It had been involved in an accident and bears Tianjin license plates.



fisherxp's car with Tianjin license plates

The same photograph of the individual is associated with the 'fisherxp' account on a Wayback Machine copy of a website for natives of Shandong province now living in Tianjin.

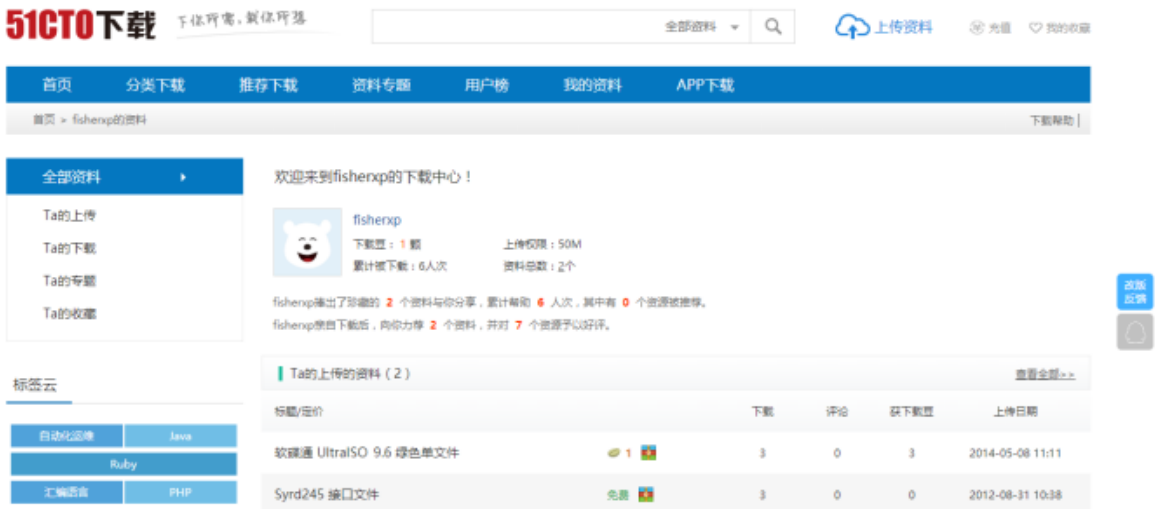


A second site (from archive.org) showing the same photo of fisherxp

Mr Gao

Some years ago, in a post (since removed) on job.51cto.com, a user using the username fisherxp posted a job advert for the Tianjin Huaying Haitai Science and Technology Development Company (天津华盈海泰科技发展有限公司). The poster used the name 'Mr Gao' and telephone number +86 150 22550833.

Unfortunately the fisherxp account was removed from the job section of the website before Intrusion Truth could obtain a screenshot. Never-the-less an associated account with the same username remains on other parts of the site.



Traces of the fisherxp account on 51cto.com

The name Gao and the same telephone number were also previosuly used online as contact details for Laoying Baichen Instruments Equipment Co. A Mr Gao listed as the contact and the address is given as Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin (天津市河东区新开路46号冠福大厦1102).

The postcode of the Guanfu Mansion on Xinkai Road is 300011, as confirmed by several unrelated postings online relating to different companies in the same building. The 300011 postcode will prove important later.

Gao Qiang

Identifying an individual in Tianjin with the surname Gao isn't easy, But cyber threat intelligence analysts following APT10 closely, and working with this blog, have confirmed that the photo of fisherxp shown above was previously used online by Tianjin resident Gao Qiang, including on his Facebook page.

In summary, fisherxp, a username probably used by Gao Qiang, was associated with hacking activity linked to known APT10 command and control servers. He is based in Tianjin, China and has probably worked for at least two companies in the city.