Who is Mr Wang?

intrusiontruth.wordpress.com/2019/07/19/who-is-mr-wang/

intrusiontruth July 19, 2019

In our last article we identified Jinan Quanxin Technology Co. Ltd. (济南全欣方沅科技有限公司) and the Jinan Anchuang Information Technology Co. Ltd. (济南安创信息科技有限公司) as companies associated with Guo Lin (郭林), a likely MSS Officer in Jinan.

Jinan Fanglang Information Technology Company

As disclosed previously by this blog, the antorsoft[.]com domain name listed the main address for Jinan Quanxin Fangyuan as 238, Jing Shi Dong Lu, Jinan, China.

```
Domain Name..... antorsoft.com
 Creation Date..... 2008-12-21 21:56:08
 Registration Date..... 2008-12-21 21:56:08
 Expiry Date..... 2009-12-21 21:56:08
 Organisation Name..... JiNan QuanXinFangYuan Tech Co.Ltd
 Organisation Address..... No 238 Jing Shi Dong Lu
 Organisation Address.....
 Organisation Address..... JiNan
 Organisation Address..... 250000
 Organisation Address..... SD
 Organisation Address..... CN
```

Historical WHOIS data for Antorsoft

But Jinan Quanxin Fangyuan wasn't the only IT company registered at this address. We know that 238, Jing Shi Dong Lu, Jinan was also the registered address of the Jinan Fanglang Information Technology Co. Ltd. (济南方朗信息科技有限公司). Let's take a look at how we can prove it…

iamjx aka phoenix

Firstly, can we identify any staff who might work for Jinan Fanglang and tie them to hacking activity? The trail starts with a job that was advertised for Jinan Fanglang on pediy[.]com by an individual using the handles iamjx and phoenix.

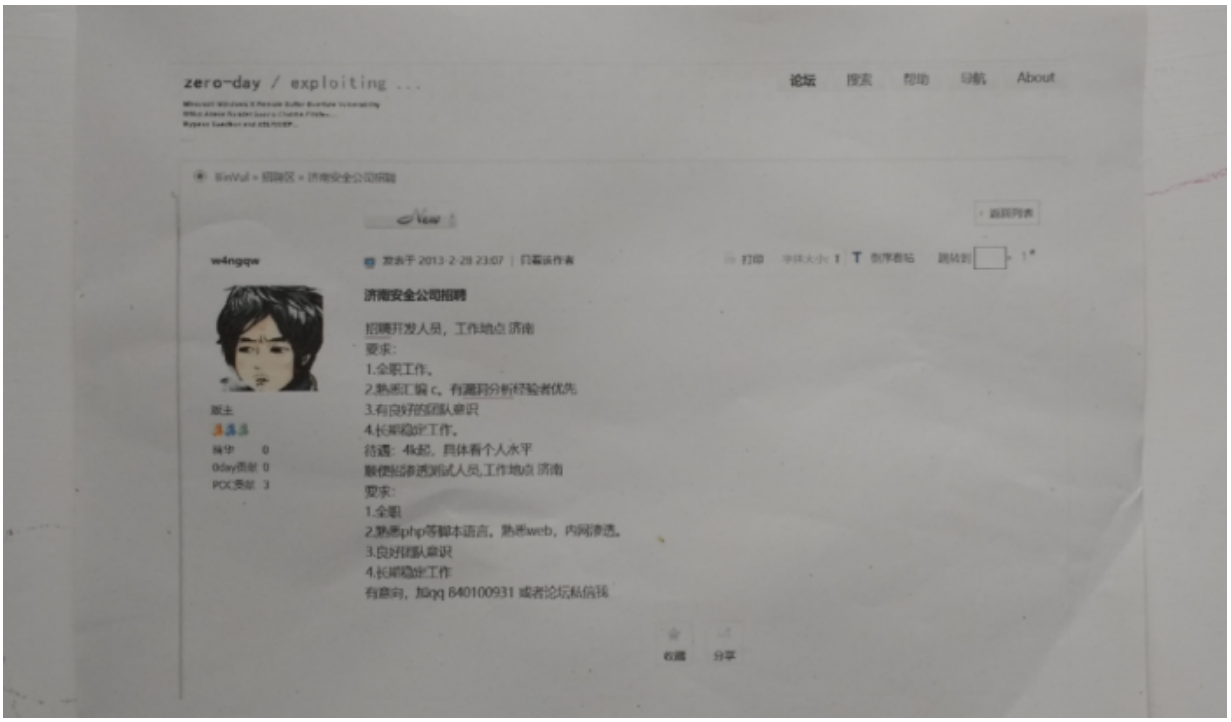
[招聘]济南方朗信息技术有限公司招聘安全工程师 2015-2-4 14:00 7303

iamjx

公司名称：	济南方朗信息技术有限公司
职位名称：	开发工程师
招聘人数：	1
工作地点：	济南
薪水待遇：	6K起
职位描述：	开发
联系人：	phoenix
联系电话：	
电子邮箱：	840100931@qq.com
QQ/MSN：	840100931

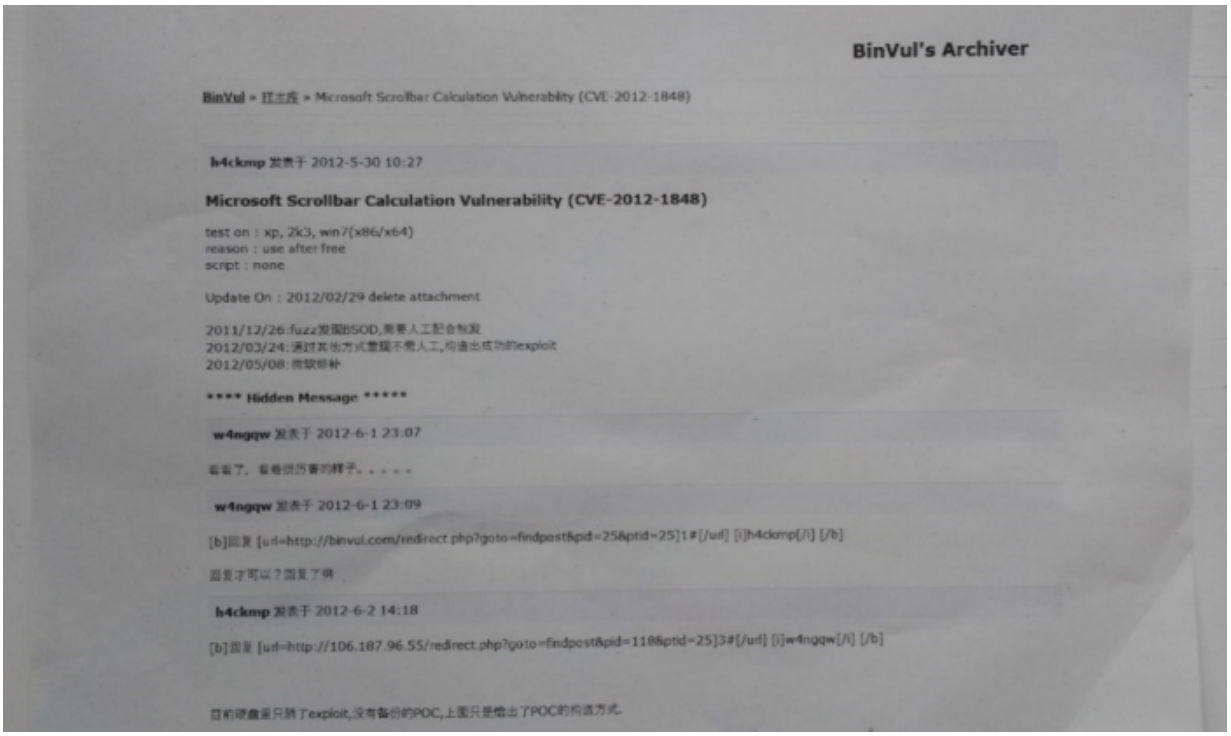
iamjx advertising a job for Jinan Fanglang

Although iamjx is a handle that is difficult to identify elsewhere in open source, our analysts were able to find a second job advert using the same QQ number, 8401900931. This second advert was on binvul[.]com. Unfortunately we can't connect to binvul, but one of our analysts passed us a printout obtained from a location with better access.



Printout of job advert for Jinan Security company

The precise name of the company isn't clear – it says 济南安全公司招聘 (Jinan Security Company Recruitment) – and the poster doesn't give their name. But their link to the hacking world is obvious from another posting in 2012 using the same w4ngqw account on binvul, this time commenting on the impressive nature of CVE-2012-1848.



BinVul's Archiver

BinVul » 红土库 » Microsoft Scrollbar Calculation Vulnerability (CVE-2012-1848)

h4ckmp 发表于 2012-5-30 10:27

Microsoft Scrollbar Calculation Vulnerability (CVE-2012-1848)

test on : xp, 2k3, win7(x86/x64)
reason : use after free
script : none

Update On : 2012/02/29 delete attachment

2011/12/26:fuzz发现BSOD,需要人工配合触发
2012/03/24:通过其他方式重现不需人工,构造出成功的exploit
2012/05/08:微软修补

****** Hidden Message *******

w4ngqw 发表于 2012-6-1 23:07

看看了，看看很厉害的样子。。。。。

w4ngqw 发表于 2012-6-1 23:09

[b]回复 [url=http://binvul.com/redirect.php?goto=findpost&pid=25&ptid=25]1#[/url] [i]h4ckmp[/i] [/b]

回复才可以？回复了啊

h4ckmp 发表于 2012-6-2 14:18

[b]回复 [url=http://106.187.96.55/redirect.php?goto=findpost&pid=118&ptid=25]3#[/url] [i]w4ngqw[/i] [/b]

目前硬盘里只放了exploit,没有备份的POC,上面只是给出了POC的构造方式.

w4ngqw discussing CVE-2012-1848

Wang Qingwei (王庆卫)

Analysing the handle w4ngqw, it seems clear that the family name is Wang. The given name uses the pinyin characters 'qw', restricting the number of candidate names in Chinese. Searching on these candidate names, analysts working with this blog have identified that the owner of w4ngqw is Jinan resident and Cyber security expert Wang Qingwei (王庆卫).

Company tax registration information obtained by this blog from the official website of Shandong Province lists the company 济南方朗信息科技有限公司 (Jinan Fanglang Information Technology Co. Ltd.) with a registration address of 238 Jing Shi Dong Lu, Jinan. Who was named as the company representative? 王庆卫…

新增非正常户认定情况分纳税人情况统计

指标说明

编表机关：山东国税

认定日期：2016 年 07 月到 2016 年 07 月

序号	纳税人识别号	纳税人名称	代表或负责人	法人证件类型代码	法人证件号码	身份证件号码	生产经营地址
1040	370102076193187	济南方朗信息技术有限公司	王庆卫	居民身份证	370821979042738l2	370821979042738l2	济南市历下区经十东路238号4-302

查询口径：税务机关包含山东国税；统计日期：2016 年 07 月到 2016 年 07 月

注：金三业务中查询非正常存在重复认定情况，一个纳税人存在多条非正常记录，所以金三数据比该平台查询量大。

Tax registration information for Jinan Fanglang

Let’s challenge the hypothesis

It could be argued that Wang Qingwei – the representative of a company that merely shared an office with a second company whose domain name was registered by Guo Lin – had nothing to do with Mr Guo or the MSS. How strange then that a source with access to such information informed us that Guo Lin and Wang Qingwei flew together on a multi-stop trip in 2016. But they weren’t just on the same plane, they sat next to each other on every leg of the flight…

We admit to not being data scientists here at Intrusion Truth, but if the population of China is 1.4 billion, the chances of sitting next to the same Chinese person on at least three journeys must be 1/(1,400,000,000)^3, which is to say 1 in 2,744,000,000,000,000,000,000,000,000.

Or 2.7 octillion to 1.

Which is quite low.

In summary, Wang Qingwei, an IT security expert, advertised jobs at Jinan Fanglang using two online profiles and was also listed as the company’s official representative. He is directly linked to likely MSS Officer Guo Lin, travelling with him on multiple occasions.

#theyknowwherethisleads