All roads lead back to Wuhan… Xiaoruizhi Science and Technology Company

intrusiontruth ⋮⋮ 5/13/2023

As our readers know from our investigation into Hainan Xiandun Technology Development Company, the Intrusion Truth team have become quite adept at spotting a fishy front company when we see one.

Typically, these are ‘companies’ with a generic-sounding ‘technology’ name and a minimal online presence. They often post adverts on university websites looking for graduates with offensive cyber skills

and, very importantly, foreign language expertise. The language of the adverts is vague, and often recycled from other, similar adverts posted online. The front companies provide contact details which just don't seem to add up – such as numbers shared by other businesses. So, when we began investigating Wuhan Xiaoruizhi Science and Technology Company, it soon became clear that we were onto a winner.

We started with a 2017 job advert posted by the School of Computer and Information Engineering, Hubei University.

【10.20】武汉晓睿智科技责任有限公司招聘

作者：湖大计信时间：2017年10月17日 15:17点击数：

武汉晓睿智科技责任有限公司招聘

招聘时间：2017年10月20日（星期五）下午14:30

招聘地点：计算机与信息工程学院1305报告厅

公司简介：武汉晓睿智科技责任有限公司；注册号：420100000183295；工作地点：近武汉光谷；工作内容：网络安全领域；薪资待遇：正常缴纳五险一金；本科生第一年年薪税后工资7.5万-8万（优秀员工可按绩效酌情增加）

岗位需求：

一、软件开发工程师

1、能独立用C、C++等编译型语言开发系统程序

2、熟悉一到两种脚本语言如python、JavaScript、php

3、可以用ida和OD等工具分析二进制程序进行定制化修改

4、对漏洞挖掘技术有过相关接触

二、嵌入式系统开发工程师

1、熟悉各种嵌入式设备的固件提取工作

2、能逆向分析二进制固件包并进行定制

3、可以对嵌入式设备进行一定的漏洞挖掘研究

三、web开发工程师

1、熟悉C语言开发

2、熟悉一些常用的web框架

3、了解基本的web漏洞挖掘流程

四、测试工程师

1、熟悉C语言开发

2、了解基本的自动化测试流程

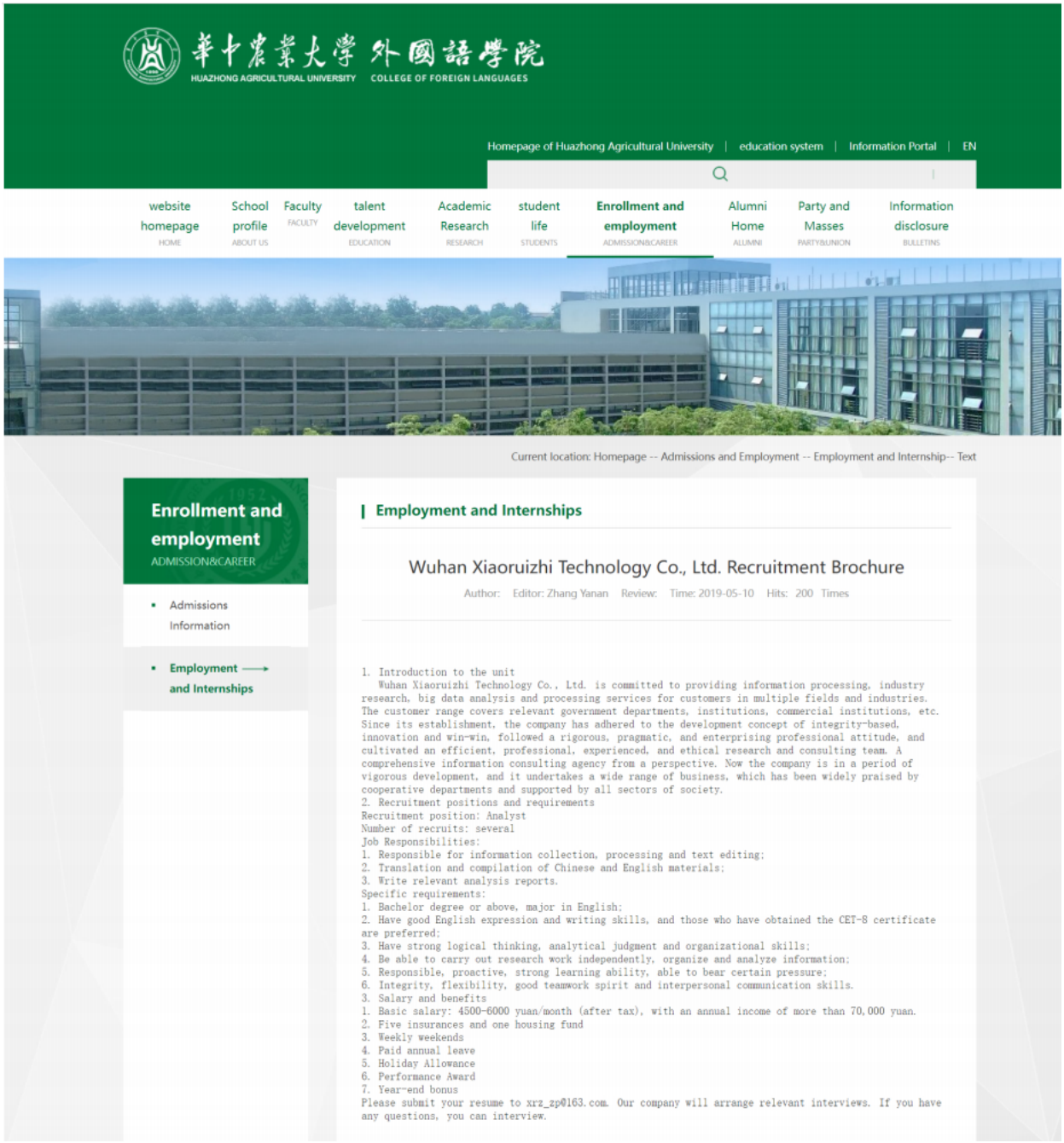
上一篇 下一篇

版权所有 [2014] 湖北大学计算机与信息工程学院

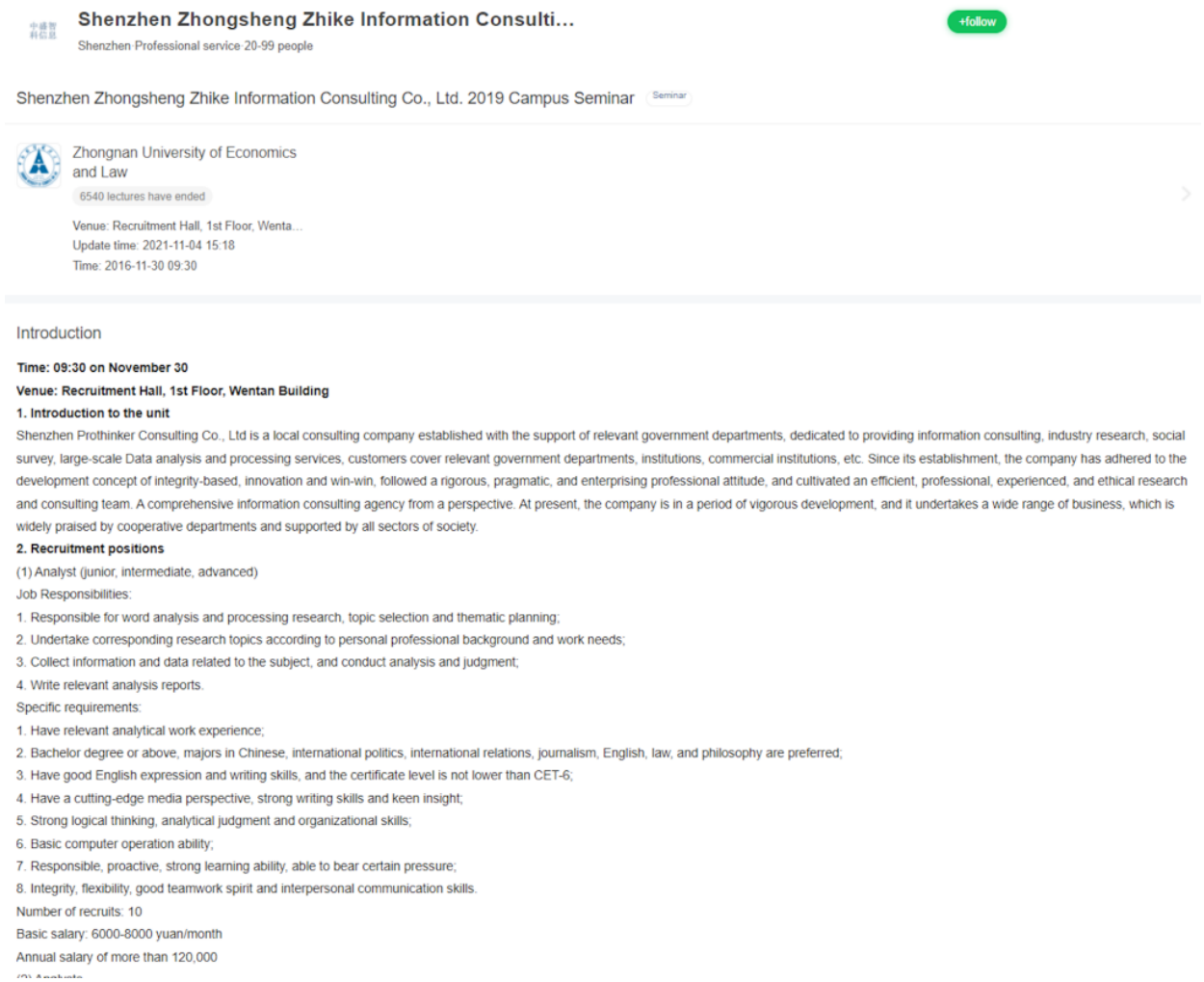
地址：湖北省武汉市武昌区友谊大道368号 邮政编码：430062 鄂ICP备05003305

Looking for a number of software and system development engineers, Wuhan Xiaoruizhi describes itself as working in the 'network security field', and being vaguely located 'near Wuhan Optics Valley'. Prospective applicants should be proficient in C and C++, scripting languages such as python, JavaScript and php, as well as IDA and OD. They should be familiar with automated testing processes, and web frameworks. Oh, and they must be au-fait with vulnerability mining. In fact, vulnerability mining is so important to Wuhan Xiaoruizhi, in this small university flyer, it is mentioned no less than three times.

A further search of Wuhan Xiaoruizhi reveals another advert posted on a university jobs site – the College of Foreign Languages at Huazhong Agricultural University. This time, Xiaoruizhi is looking for English majors to become analysts who will be responsible for 'information collection, processing and text editing' in Chinese and English.



Xiaoruizhi gives us an introduction to the company, which is committed to providing ‘information processing, industry research and big data analysis’ for customers, which include ‘relevant government departments’. We also get to know more about the company’s ‘ethical research and consulting team’, ‘win-win approach’ and its ‘concept of integrity-based innovation’. Only the company isn’t that innovative – nor does it have much integrity: such wording appears to be a word-for word copy of a description from another company’s job advert in Shenzhen. Shenzhen Prothinker Consulting.



Shenzhen Zhongsheng Zhike Information Consulti...

+follow

Shenzhen Professional service 20-99 people

Shenzhen Zhongsheng Zhike Information Consulting Co., Ltd. 2019 Campus Seminar Seminar

Zhongnan University of Economics and Law

6540 lectures have ended

Venue: Recruitment Hall, 1st Floor, Wenta...
Update time: 2021-11-04 15:18
Time: 2016-11-30 09:30

Introduction

Time: 09:30 on November 30
Venue: Recruitment Hall, 1st Floor, Wentan Building
1. Introduction to the unit
Shenzhen Prothinker Consulting Co., Ltd is a local consulting company established with the support of relevant government departments, dedicated to providing information consulting, industry research, social survey, large-scale Data analysis and processing services, customers cover relevant government departments, institutions, commercial institutions, etc. Since its establishment, the company has adhered to the development concept of integrity-based, innovation and win-win, followed a rigorous, pragmatic, and enterprising professional attitude, and cultivated an efficient, professional, experienced, and ethical research and consulting team. A comprehensive information consulting agency from a perspective. At present, the company is in a period of vigorous development, and it undertakes a wide range of business, which is widely praised by cooperative departments and supported by all sectors of society.
2. Recruitment positions
(1) Analyst (junior, intermediate, advanced)
Job Responsibilities:
1. Responsible for word analysis and processing research, topic selection and thematic planning;
2. Undertake corresponding research topics according to personal professional background and work needs;
3. Collect information and data related to the subject, and conduct analysis and judgment;
4. Write relevant analysis reports.
Specific requirements:
1. Have relevant analytical work experience;
2. Bachelor degree or above, majors in Chinese, international politics, international relations, journalism, English, law, and philosophy are preferred;
3. Have good English expression and writing skills, and the certificate level is not lower than CET-6;
4. Have a cutting-edge media perspective, strong writing skills and keen insight;
5. Strong logical thinking, analytical judgment and organizational skills;
6. Basic computer operation ability;
7. Responsible, proactive, strong learning ability, able to bear certain pressure;
8. Integrity, flexibility, good teamwork spirit and interpersonal communication skills.
Number of recruits: 10
Basic salary: 6000-8000 yuan/month
Annual salary of more than 120,000

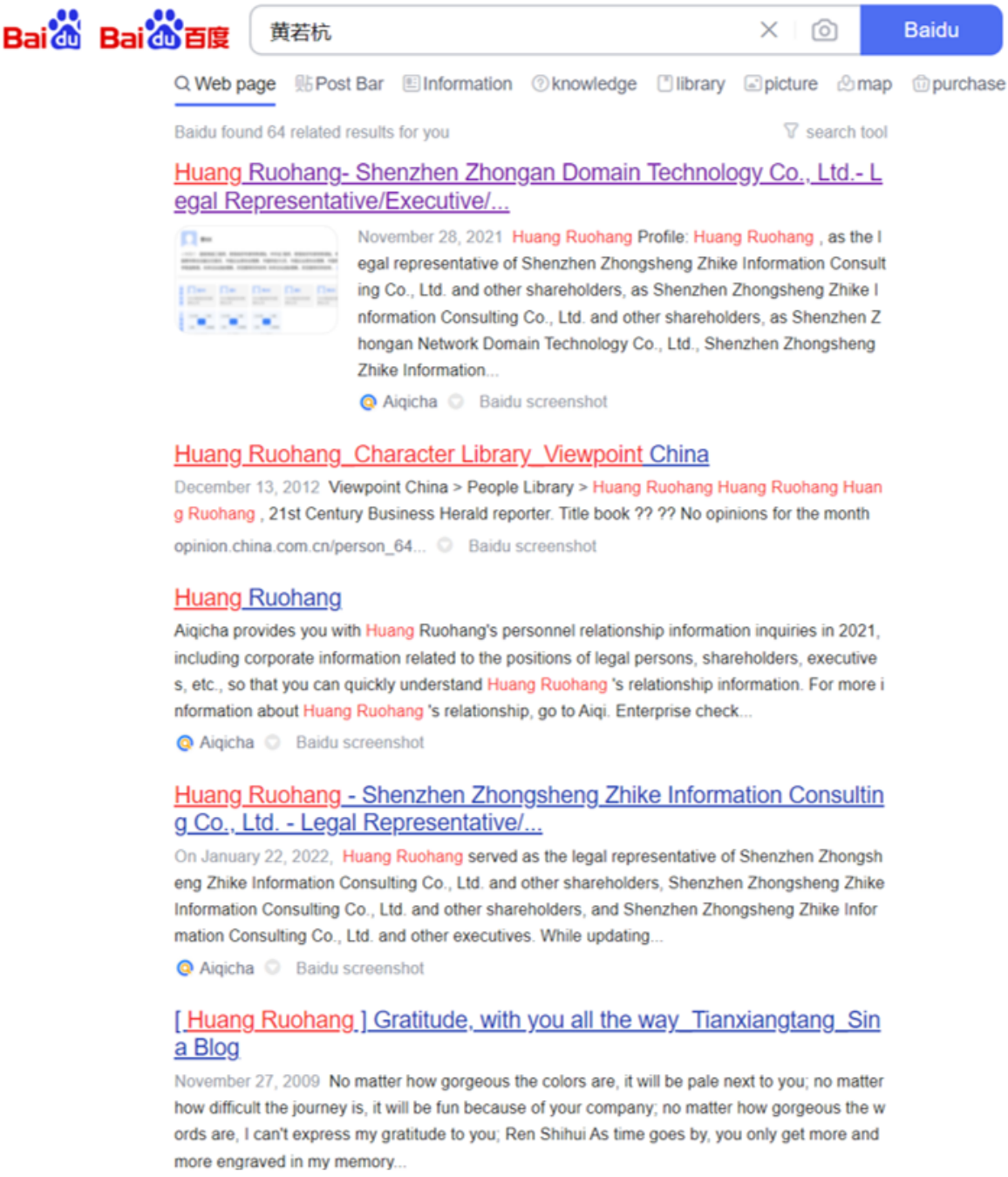
Shenzhen Prothinker

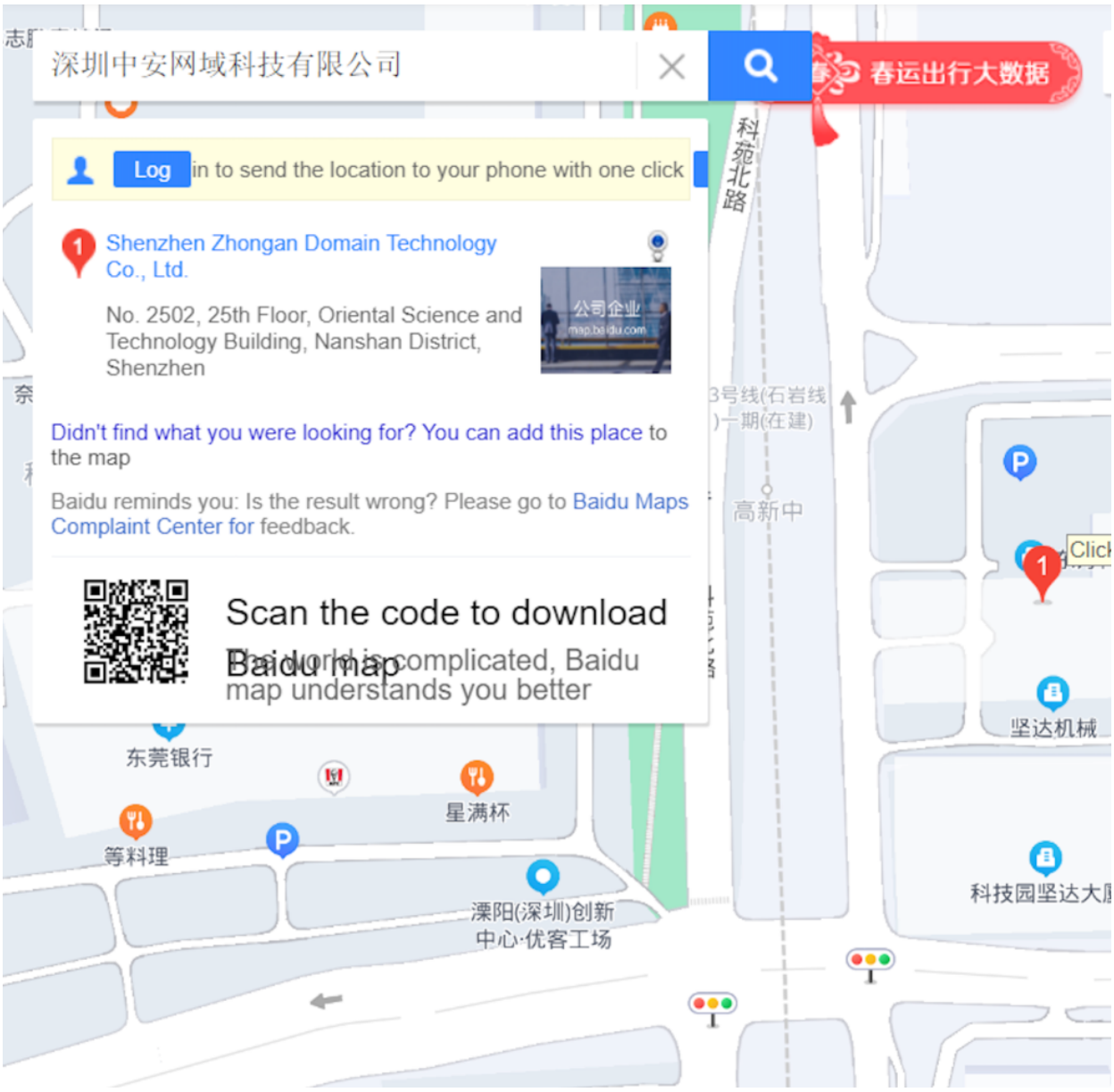
So what is it about Shenzhen Prothinker Consulting that got Wuhan Xiaoruizhi so inspired? Well, funnily enough, Shenzhen Prothinker was also on the lookout for English speakers with interests in politics, and graduates with computer-related majors. Hmm. Unfortunately, the website for Prothinker is now defunct. However, there is still some information out there on Baidu about the company. The legal representative of Shenzhen Prothinker was a Huang Ruohang, and the address for the company is listed as Room 2511, 25th Floor, Oriental Science and Technology Building, Science and Technology Park, Yuehai Street, Nanshan District, Shenzhen.

【Welfare treatment】
1. Provide various job-related training opportunities;
2. Five insurances and one housing fund;
3. Annual physical examination;
4. Holiday allowance;
5. Enjoy ten days of paid annual leave (including sickness and personal leave) every year after one year of regularization;
6. Regular group activities and travel;
7. Attendance award, quarterly award, project award and year-end award are not included;
8. Provide flexible salary increase channels according to individual efforts.
3. Contact information
Tel: 0755-22677019
Fax: 0755-86717474
Email: hr@prothinker.com.cn
Website: www.prothink.com.cn
Address: Room 2511, 25th Floor, Oriental Science and Technology Building, Science and Technology Park, Yuehai Street, Nanshan District, Shenzhen

A search for “Huang Ruohang” (Chinese characters given below) showed that Huang Ruohang was also listed as the executive director for Shenzhen Zhongan Domain Technology Company. And as

‘coincidences’ would have it, Shenzhen Zhongan Domain Technology Company was also once located on the 25th Floor of the Oriental Science and Technology Building in Nanshan District Shenzhen.





Shenzhen Zhongan Domain Technology Company appears to be also known, according to its branding, as ZIONSEC. ZIONSEC describes itself as providing ‘advanced solutions for national security issues such as national defense and intelligence’ to ‘help the dream of a powerful country’.

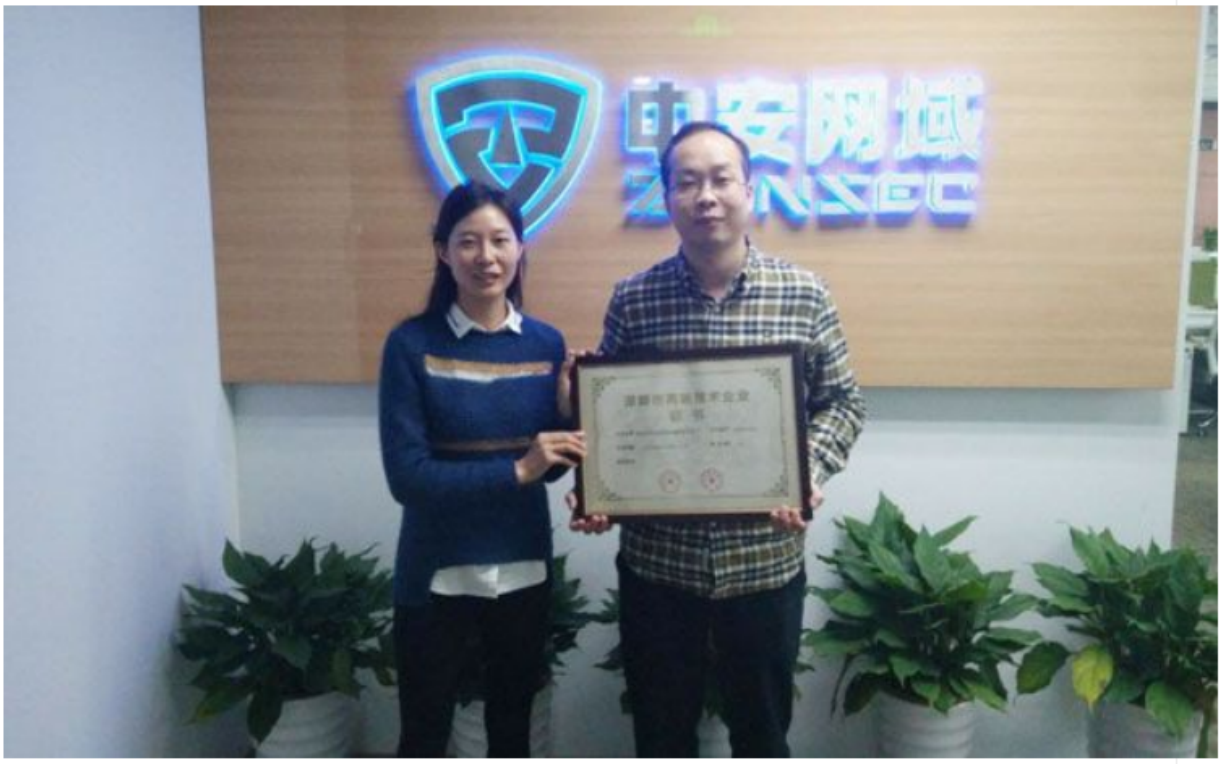
深圳市中安网域科技有限公司

发布时间：2020年10月19日 16:17　浏览量：1163

深圳市中安网域科技有限公司

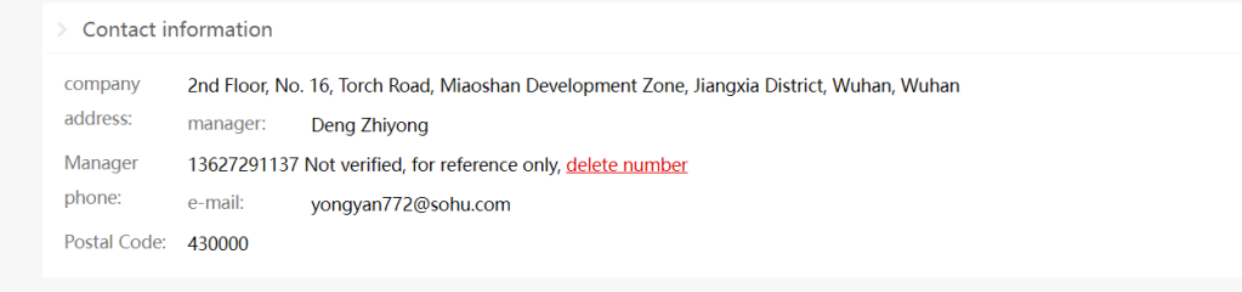
合作项目：高新企业认定

一句话：我们找厚德集团申报了高新企业，并最终拿到了高新企业证书，还找他们申请了深圳市高层次人才认定证书，还有相应的政府补贴，都成功拿到了，感谢他们。



Sounds…suspicious.

Let’s park the shenanigans in Shenzhen for now and return to Wuhan. Who actually works at the Xiaoruizhi Science and Technology Company and what do they do? Unfortunately, this technology company doesn’t have its own website, but we do have the name of the manager, Deng Zhiyong.

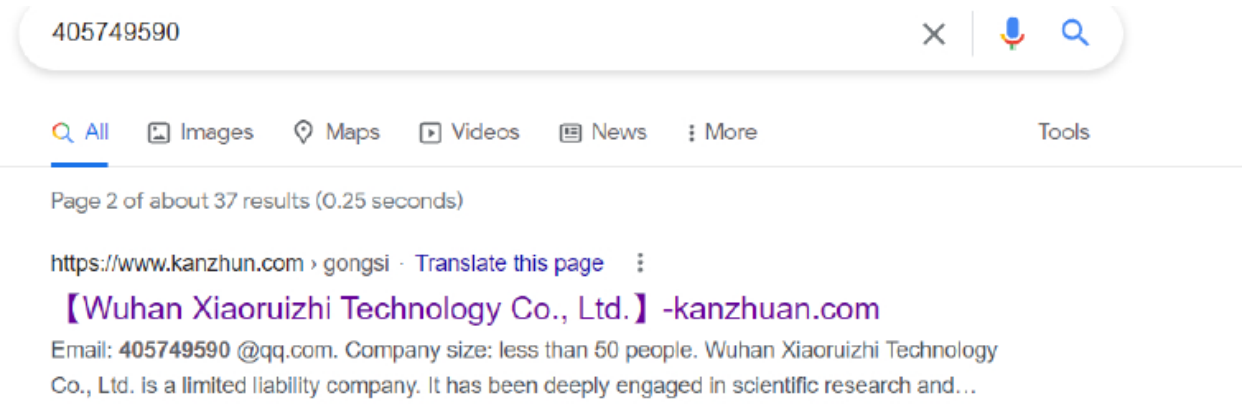


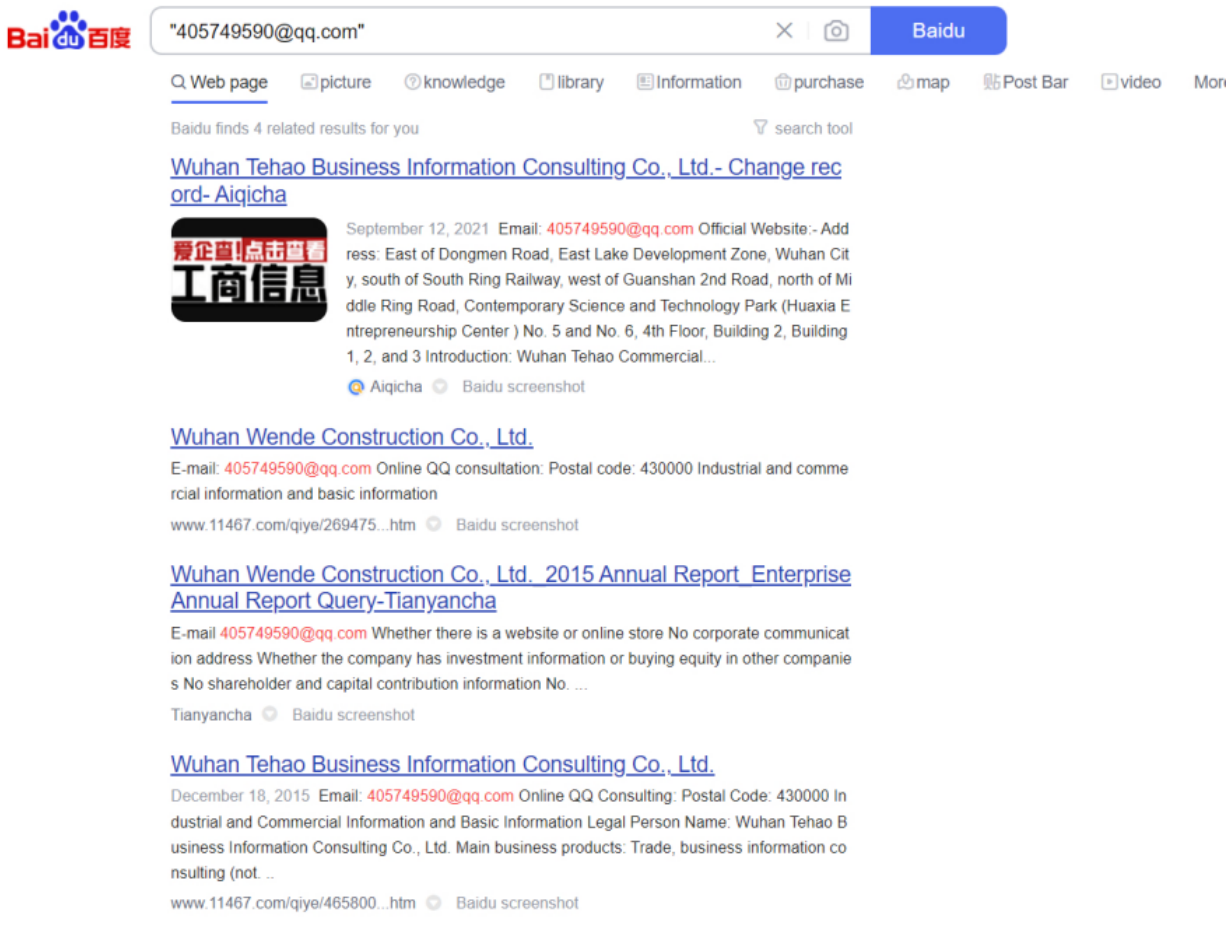
Deng is an interesting character. Aside from holding official titles at no less than three (!) government-affiliated organizations, (Director of the Foreign Exchange Center, Ministry of Science and Technology China; Director of the Hubei Wuhan China/Russian Technologic Cooperation Center; Chief of Department of Steelworks Management Administration, Dongxi, Wuhan) our friend Deng also seems to have a thing for Russian lasers.

Cooperation in the field of laser technologies. Development of scientific and technological cooperation in the field of industrial chemistry, photoelectronics and production of laser lamps. Location of the project: Nizhny Novgorod region.	Ministry of Industry and Innovation of the Nizhny Novgorod Region Batenin Vladimir Ivanovich (831) 419-43-16 Administration of the city of Sarov, Nizhny Novgorod region Golubev A.V. (83130) 977-73 duma@adm.sar.ru	Hubei Province, Donghu Innovation Technopark +86 2767880061 wusy_777@_sohu_.com Hubei Center for Sino-Russian Science and Technology Cooperation contact person: Deng Zhiyong Tel: +86-13627291137 Email: yongyan772@sohu.com	Project under development.

We will return to this in a later article. It's a wild ride.

A phone number which seems to be linked to Mr. Deng also seems to be used by both a construction company and a 'business information consulting company'. Quite the diverse business empire.





So, to summarize, we have a sketchy-looking company in Wuhan looking for vulnerability-miners and foreign language experts and linked to a phone number shared between many businesses. Lacking some imagination, the company decides to borrow language used by another sketchy-looking company in Shenzhen, which in turn appears to have some quite considerable overlap with an info-sec company dedicated to national defense and intelligence work. We also have government clients, a CEO with official PRC government titles, and a bonus link to a shifty hacking school.

You know the drill by now. If it walks like a duck and quacks like a duck…. (should we get that printed on merch?).

Beyond this, Wuhan Xiaoruizhi hasn't given us much to go on. So, it was time to take our search to the dark web.

Bingo.