Hello Lionel Richie


intrusiontruth.wordpress.com/2021/09/20/hello-lionel-richie

intrusiontruth September 20, 2021

An interesting turn of events occurred whilst releasing our article series on Lonely Lantern (the Chinese APT previously with no name, working to the Guangdong SSD).

As most of our readers will have been aware, a brand new Twitter account was created to reply to our tweet in advance of the second article where we exposed Guangdong MSS officer 1 as Zhao Jianfei, working with Li and Dong to support and direct their intrusion activity from Chengdu.

At the time, we noted this post and found it interesting (not least for the gif choice) but put it on the back burner given other investigations and leads we were following up on. However, what piqued our interest further was the fact this account and its comment was later deleted.

Why would Mr. Ren reach out to us on this public forum and tweet that he is the MSS officer we were looking for? Does he have something he wants to get off his chest? The Twitter bio translates to '*roaming the streets of Guangzhou*'. Seems to fit with the brief of the GSSD.

We decided to investigate (initially as a bit of fun on a rainy day) but as you will see, it is clear that Ren Yuntao is entwined with Lonely Lantern.

Here's what we know.

renyuntao
@ren_yuntao Follows you

漫游广州的街道

Joined May 2021

1 Following **0** Followers

Not followed by anyone you're following

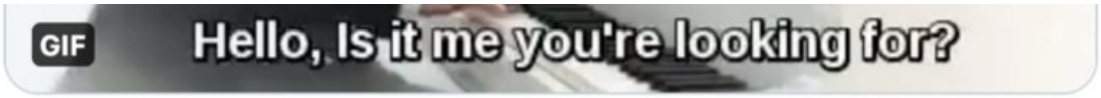
Tweets | Tweets & replies | Media | Likes

Intrusion Truth @intrusion_truth · May 11

We hope you enjoyed our first article and are hungry for more. Our second article takes us to the city of Guangzhou. A city we know well (#Boyusec). Will we track down MSS Officer 1? #youknowwherethisleads #MSS #APTwithnoname #Tminus2days

1 33 86

renyuntao @ren_yuntao · May 12



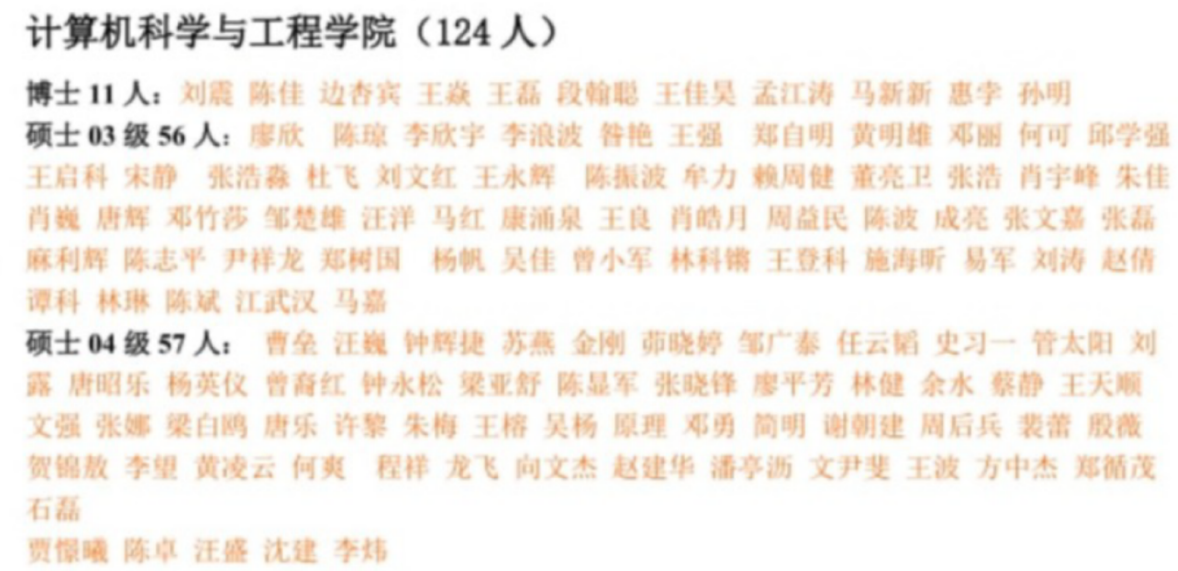
Ren Yuntao (任云韬)

The Twitter profile is in the name of Ren Yuntao. However, the profile itself is quite sparse, having being created the same month as posting. And it appears he only engaged with us. A keen watcher of our work? A super fan perhaps.

So, apart from being a Lionel Ritchie fan, what else could we find on Mr Ren? His Twitter profile didn't give us much so we decided to start at the beginning and where we know hackers from Lonely Lantern reside: Chengdu.

Mr. Ren it seems went to the same school as Li Xiaoyu and Dong Jiazhi (the indicted hackers we mentioned in Article 1). Ren studied a Masters program at the University of Electronic Science and Technology of China (UESTC), in Chengdu.

His studies led to him gaining experience in the development of software, defense and forensic analysis of information systems.


计算机科学与工程学院（124 人）

博士 11 人：刘震 陈佳 边杏宾 王焱 王磊 段翰聪 王佳昊 孟江涛 马新新 惠宇 孙明

硕士 03 级 56 人：廖欣 陈琼 李欣宇 李浪波 鲁艳 王强 郑自明 黄明雄 邓丽 何可 邱学强 王启科 宋静 张浩淼 杜飞 刘文红 王永辉 陈振波 牟力 赖周健 董亮卫 张浩 肖宇峰 朱佳 肖巍 唐辉 邓竹莎 邹楚雄 汪洋 马红 康涌泉 王良 肖皓月 周益民 陈波 成亮 张文嘉 张磊 麻利辉 陈志平 尹祥龙 郑树国 杨帆 吴佳 曾小军 林科锵 王登科 施海昕 易军 刘涛 赵倩 谭科 林琳 陈斌 江武汉 马嘉

硕士 04 级 57 人：曹垒 汪巍 钟辉捷 苏燕 金刚 邵晓婷 邹广泰 任云韬 史习一 管太阳 刘露 唐昭乐 杨英仪 曾裔红 钟永松 梁亚舒 陈显军 张晓锋 廖平芳 林健 余水 蔡静 王天顺 文强 张娜 梁白鸥 唐乐 许黎 朱梅 王榕 吴杨 原理 邓勇 简明 谢朝建 周后兵 裴蕾 殷薇 贺锦敖 李里 黄凌云 何爽 程祥 龙飞 向文杰 赵建华 潘亭沥 文尹斐 王波 方中杰 郑循茂 石磊

贾慷曦 陈卓 汪盛 沈建 李炜

Department of Computer Science and Engineering Master's students at UESTC (124 in total). Ren Yuntao's name appears 8th along in the third para.

Ren's Master's thesis, submitted in December of 2006 is titled "*Malicious Code Anti-Detection Technology Research Based on Dynamic Binary Modification*" (基于二进制多态变形的恶意代码反检测技术研究). His supervisor whilst completing his studies was Li Yichao (李毅超).

电子科技大学

硕士学位论文

基于二进制多态变形的恶意代码反检测技术研究

姓名：任云韬

申请学位级别：硕士

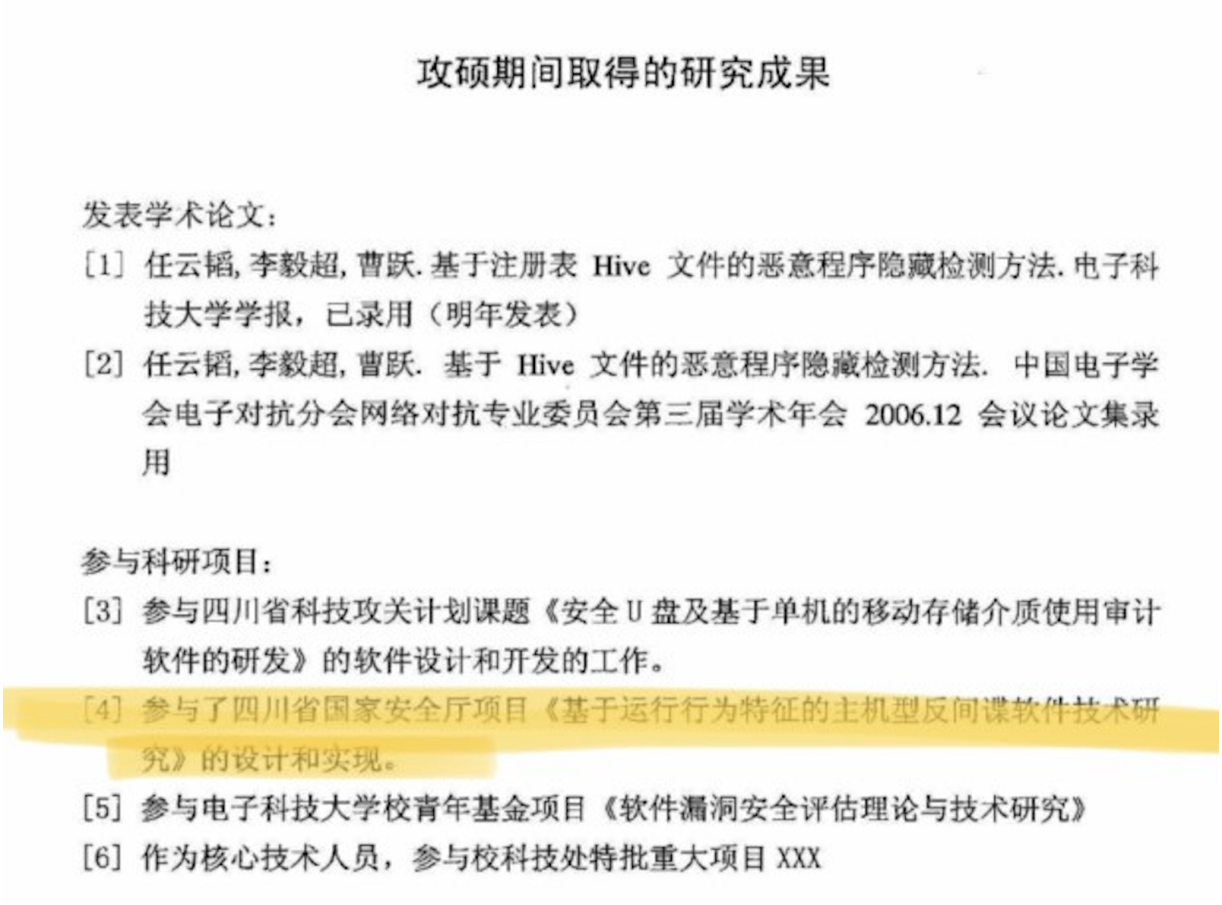
专业：计算机应用技术

指导教师：李毅超

20061202

We set about delving into Ren's thesis to see what we could find (it is quite dry in places and we wouldn't recommend it as bedtime reading). Yet, there are some nteresting nuggets. An example is on page 71. Here, Ren provides his acknowledgement to 'Pinkeyes', a 'famous network security figure within China', referring to him as his 'comrade in arms'. An interesting phrase to use.

Later, on page 74, Ren details his research projects and achievements throughout his graduate studies. Of specific note to us was his involvement in the *'design and realisation of a Sichuan State Security Department (SSSD) programme'*.



攻硕期间取得的研究成果

发表学术论文：

[1] 任云韬, 李毅超, 曹跃. 基于注册表 Hive 文件的恶意程序隐藏检测方法. 电子科技大学学报，已录用（明年发表）

[2] 任云韬, 李毅超, 曹跃. 基于 Hive 文件的恶意程序隐藏检测方法. 中国电子学会电子对抗分会网络对抗专业委员会第三届学术年会 2006.12 会议论文集录用

参与科研项目：

[3] 参与四川省科技攻关计划课题《安全 U 盘及基于单机的移动存储介质使用审计软件的研发》的软件设计和开发的工作。

[4] 参与了四川省国家安全厅项目《基于运行行为特征的主机型反间谍软件技术研究》的设计和实现。

[5] 参与电子科技大学校青年基金项目《软件漏洞安全评估理论与技术研究》

[6] 作为核心技术人员，参与校科技处特批重大项目 XXX

Highlighted section: Mention of Sichuan SSD in Ren's thesis

The last accomplishment Ren lists (point 6) is his participation as a "*core technician in a "major" university project with designator XXX*". Suspicious – a project so sensitive it needs to be redacted but high profile enough to include in a thesis detailing your work achievements…

Following on from his success with sensitive projects and MSS programmes in Sichuan, Ren appears to have been quite busy, staying on at UESTC as a post-grad and publishing two papers. One of which was on the topic of detecting malware on registry Hive files.

第 36 卷 第 3 期 电 子 科 技 大 学 学 报 Vol.36 No.3
2007 年 6 月 Journal of University of Electronic Science and Technology of China Jun. 2007

基于注册表Hive文件的恶意程序隐藏检测方法

任云韬，李毅超，曹 跃

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】研究当今恶意程序的发展趋势，系统比较了在注册表隐藏和检测方面的诸多技术和方法，综合分析了它们存在的不足，提出了一种基于注册表Hive文件来进行恶意程序隐藏检测的方法，使得针对恶意程序的检测更加完整和可靠。实验表明，该方法可以检测出当前所有进行了注册表隐藏的恶意程序。

关 键 词 Hive文件； 恶意程序； 注册表隐藏和检测； RootKit程序
中图分类号 TP393.08 文献标识码 A

A Methodology to Detect Malware Based on Registry Hive Files

REN Yun-tao，LI Yi-chao，CAO Yue

(School of Computer Science and Engineering，University of Electronic Science and Technology of China Chengdu 610054)

Abstract Based on the research on the current developing trends of malicious programs, comparing systematically the various technologies and methodologies with respect to the hiding and detection of registry. analyzing comprehensively their deficiencies existing, we provide a brand-new hiding and detection method based

Li Yichao (李毅超)

Cited in Ren's papers and listed as Ren's supervisor at the UESTC is Li Yichao (李毅超). It was Mr Ren himself who wrote that Li Yichao gave him the National Network Security programme opportunity. So, who is Li Yichao?

Well, here is his CV.

李毅超

已经得到 个称赞 给我点赞

个人信息

教师姓名：李毅超
教师拼音名称：liyichao
性别：男
电子邮箱：
职称：教授
在职信息：在岗
硕士生导师
所在单位：数学科学学院
学位：工学硕士学位
学科：计算机应用技术
毕业院校：电子科技大学
曾获荣誉：荣立国家某部二等功一次，荣获四川省科技进步三等奖、成都市科技进步二等奖。
办公地点：主楼A1-408B
联系方式：

个人简介

本人主要研究方向：大数据与云计算、人工智能、网络安全、嵌入式应用技术。

本人近些年来尤其注重与业界产学研合作，2018年先后与新三板上市公司四川赛康智能科技股份有限公司校企合作成立电力大数据与人工智能工程应用研究中心，与西门子工业软件公司成立电子科技大学西门子工业软件非全日制硕士研究生联合培养基地，为全日制和非全日制硕士研究生创造了优良的软硬培养条件和环境。大四保送生直接送西门子工业软件全球（成都）研发中心1年实习训练。

曾主持参加国家863计划、国家自然科学基金、信息产业部电子工业发展基金、国家科技基础条件平台建设计划、国家信息安全242计划、总装备部基金、国家安全部基金、四川省科技基础研究、四川省两化融合以及企业横向合作科研项目50多项。获国家某部二等功1次，四川省科技三等奖1项，成都市科技二等奖1项，国家版权局软件著作权6项，申请国家发明专利12项，获得国家发明专利授权7项，申请并获得美国和国际发明专利2项。在国内外重要刊物和国际会议上发表学术论文40余篇,其中被EI检索20余篇。

曾为本科和硕士生开设若干课程，如计算机网络、互联网技术、Java程序设计、网络安全技术、数据库原理及应用、网络协议分析实践等。主持计算机网络课程建设获得四川省精品课程。编著出版教材2本《计算机网络》、《网络与系统攻击技术》，译著教材3本《信息安全原理与应用》、《信息安全原理与技术》、《计算机网络实验教程》。

自2003年以来先后培养全日制硕士毕业生100余人，很多工作于百度、腾讯、阿里等著名互联网公司，还有公安国安部门、高校、研究所、银行、中国移动、中国电信等企事业单位。培养非全日制工程硕士毕业生也近100人。培养优秀硕士生和本科生多人成功创业公司，如成都亿盟恒信科技有限公司、成都安恒信息技术公司等。培养王勋、刘庭宇两名优秀本科生毕业去美国微软公司西雅图总部工作。

Given he is an academic, his openness is our advantage. He notes his many plaudits, including *'winning second prize from a certain ministry of the country'* and states some of his many students have gone on to work for *'public and national security departments'*. Could Ren be one of these individuals?

Let's recap: Ren has worked closely with a supervisor who openly talks of his links to government bodies and ministries within China. Ren himself has commented on his time working for the Sichuan State Security Department and other mysterious organisations that require redacted material whilst at UESTC. So what else can we find on Ren following his departure from academia?

Chengdu Jiuyan Technology Company Ltd. (成都九眼科技有限公司)

Also known as Chengdu Nine Eyes Technology Co Ltd., this company was established in July 2018 specialising in technology development, computer software and network engineering.

Two individuals are associated with the company. The first is the supervisor Xu Jiayou (徐嘉幼), holding just 1% of the company. The second is the executive director and general manager Ren Yuntao, with a registered stake of 99% in Chengdu Jiuyan.

成都九眼科技有限公司

法定代表人： 任云韬

查询时间：2019-12-07 19:39

更新

电话：13550075*** 查看号码

邮箱：暂无

地址：四川省成都市天府新区华阳街道长江东二街56号1栋1层1室

工商注册信息

统一社会信用代码	91510100MA638QND8W
企业名称	成都九眼科技有限公司
注册号	-
法定代表人	任云韬
企业类型	有限责任公司(自然人投资或控股)
成立日期	2018-07-11
注册资本	814万元人民币
核准日期	2018-07-11
营业期限	2018-07-11 至 3999-01-01
登记机关	天府新区成都片区工商行政管理局
登记状态	存续（在营、开业、在册）
注册地址	四川省成都市天府新区华阳街道长江东二街56号1栋1层1室
经营范围	技术开发、技术转让、技术咨询、技术服务;销售、安装:通信设备、光伏设备、计算机软硬件;信息系统集成;网络工程;平面设计;网页设计;图文设计。(依法须经批准的项目,经相关部门批准后方可开展经营活动)。

股东信息

2

股东	持股	认缴(万)	日期
任云韬	99.00%	99	-
徐嘉幼	1.00%	1	-

The address is listed as Room 1, Floor 1, Building 1, 56 Changjiang East Second Street, Huayang Avenue, Tianfu New District, Chengdu.

Interestingly, there are a number of other companies who also claim to reside in Room 1, Floor 1, Building 1 of 56 Changjiang East Second Street in Chengdu including:

- Chengdu Hashmai Block Technology Co. Ltd
- Sichuan Shuanglin Jiayue Property Management Co. Ltd
- Shuju Chengdu Technology Co. Ltd
- Douxing Culture Communications Chengdu Co. Ltd
- Chengdu Yinchi Culture Media Co. Ltd
- Chengdu Vines Interactive Entertainment Technology Co. Ltd
- Chengdu Tianfu Hualong Petroleum Co. Ltd
- Chengdu Renhe Daoyuan Enterprise Management Consulting Co. Ltd
- Chengdu Jingwei Zhidao Enterprise Management Consulting Co. Ltd
- Chengdu Feihang Zhiyun Technology Co. Ltd
- Chengdu Als Technology Co. Ltd
- Chengdu Aiweili Trading Co. Ltd

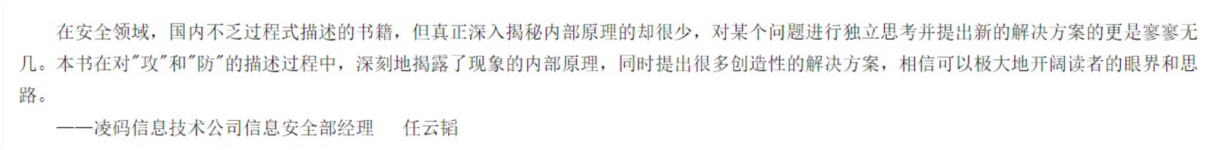
That's a lot of companies to be sharing 1 room.

Given it location, lack of internet presence and the individuals associated with it – a front company springs to mind.

Lingma Information Technology Company Limited (凌码信息技术上海有限公司)

Upon leaving academia, Ren appears to have obtained a job in the private sector as the Head of Information Security at Lingma Information Technology Co. Ltd. Once again, all roads lead back to Chengdu.

This is an extract of a book written by UESTC masters alumnus Xu Sheng from the Network Attack and Defense Lab, to which Ren Yuntao offers his review.



在安全领域，国内不乏过程式描述的书籍，但真正深入揭秘内部原理的却很少，对某个问题进行独立思考并提出新的解决方案的更是寥寥无几。本书在对"攻"和"防"的描述过程中，深刻地揭露了现象的内部原理，同时提出很多创造性的解决方案，相信可以极大地开阔读者的眼界和思路。

——凌码信息技术公司信息安全部经理　任云韬

Ren Yuntao book review of 游戏外挂攻防艺术 *(The Art of Game Plugin: Attack and Defense) by* 徐胜 *(Xu Sheng)*

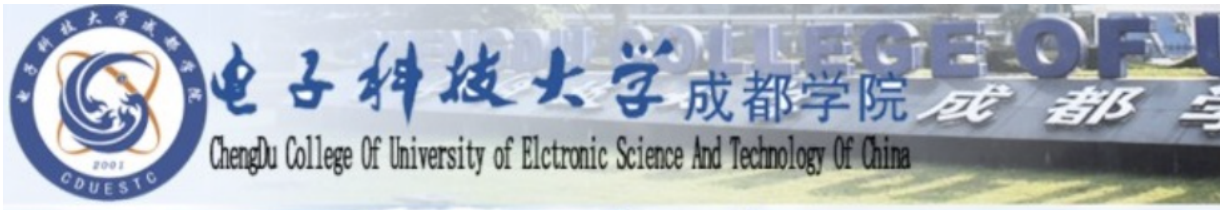
Head of Information Security sounds like a grand title. The company Ren worked for (Lingma) is a wholly-owned subsidiary of Singapore's Nyber company. Nyber was established in 2010 under CEO Zhang Taiyong（张台涌). It is described as a company committed to research and development of high-end technology, with its business scope covering China and overseas regions and its products often being used in government fields.

Lingma has a base in Chengdu. The address is given as Area C, Floor 10, Sector F of the 9th Building of High-Tech Incubation Park, Tianfu Avenue, Gaoxin District, Chengdu.

Does this address seem familiar? It did to us. It is in the same high tech zone as Chengdu Hanke, the front company created by Dong Jiazhi and exposed in article 1 of our series on Lonely Lantern.

Company profile of Lingma

Just like déjà vu, our searching led us back to UESTC in Chengdu. In 2014, Lingma were advertising positions within its company on the UESTC webpage (www1.cduestc.cn), aiming to recruit system software engineers, interface software engineers, and information security evaluation managers. Could this be where Ren first came across Lingma and led to his career in ‘Information Security’?



首 页 专业介绍 今日招聘 就业快讯 现场招聘 需求动态 资料下载 海外深造 最新简历 联系

当前位置： 首页 >> 需求动态 >> 凌码信息技术（上海）有限公司

凌码信息技术（上海）有限公司

发布日期:2014-11-04 发布者:admin 浏览次数: 2274 次

招聘岗位及要求

系统软件工程师 (成都4名)

工作职责

参与公司网络信息安全产品及项目的研发

人员要求

1、熟悉C/C++语言和数据结构

2、熟悉操作系统原理和Linux系统内核（或Windows内核）

3、熟悉TCP/IP协议栈

4、在校期间有相关动手经历

5、品德优良、具备团队合作意识和质量意识

用户界面软件工程师(成都 1名)

工作职责

参与公司网络信息安全产品及项目的研发

人员要求

1、能够使用MFC/.NET进行界面设计

2、具备美术功底

3、熟悉数据库

4、品德优良、具备团队合作意识和质量意识

5、在校期间有关动手经验

信息安全软件工程师(成都2名)

工作职责

参与公司网络信息安全产品及项目的研发

人员要求

1、熟悉C/C++ 和数据结构,了解X86汇编

2、了解IDA/OllyDbg等静态分析或动态调试工具的使用

3、敬业、具备团队合作意识及良好的职业道德

4、在校期间有相关动手经验

信息安全测评工程师（成都2名）

信息安全测评工程师（成都2名）
工作职责：
参与公司网络信息安全测评服务的相关工作
人员要求：
1、熟悉各种网络协议和网络平台

Lingma scholarship at SWPU

Further searches around Lingma shows the company's ties to other universities in Chengdu. For example, it provides a scholarship program with Southwest Petroleum University (https://www.swpu.edu.cn/info/1248/1113.html) at an investment of 3000 RMB per year.

Browsing the website for SWPU, there are a number of articles outlining Lingma's involvement with the university under its scholarship scheme.

One particular article caught our eye. It was posted on the 9th June 2016, and describes how the scholarship awarding ceremony for the Lingma Scholarship took place a day earlier at SWPU.

It states that the director of the institute, ZHAO Gang (学院院长赵刚), was present at the ceremony and gave a speech to the students. The Deputy Secretary of the institute's party committee, YU Hui (学院党委副书记余辉) was also present alongside Secretary LIU Xiang from the institute's group committee, who hosted the event (学院团委书记刘翔). The person representing the Chengdu R&D Centre of the Lingma Company is named as a Mr. Ren Weitao (凌码信息技术有限公司成都研发中心负责人任伟韬先生).

Is it a coincidence that another Mr. Ren also works for the same company as our Mr. Ren? We don't believe in coincidences. Given that Lingma only has up to 50 staff, and our searches revealed nothing further on any other Ren's working for Lingma during this time, it is safe to assume that Ren Weitao is Ren Yuntao. Was the change in name a deliberate attempt to fly under the radar? What was Ren trying to hide?

The last picture in the article is interesting and appears to depict Mr. Ren. The students are proudly displaying their awards. The caption of this group photo describes those in the picture, including the"scholarship-receiving representatives [students], the scholarship-awarding guests [Ren Weitao (任伟韬)] and the leader".

Disclaimer: We have obfuscated the students in this image due to their lack of involvement in APT activity

Conclusion

So what do we know?

1. An individual called Ren Yuntao tweeted his implication that he was the MSS officer associated with the APT group (Lonely Lantern) working out of Chengdu and for the Guangdong SSD.

2. Ren Yuntao attended the same university as the indicted criminal hackers for Lonely Lantern and has worked with the Sichuan SSD whilst at university. His university professor also likes to talk of his close links to the MSS.
3. Ren Yuntao sets up a front company in Chengdu High-Tech Incubation Park in Tianfu High Tech zone, suspiciously similar to Chengdu Hanke (linked to Dong Jiazhi from Article 1 in this series).
4. Ren Yuntao works for Lingma and is directly involved with local universities in Chengdu, handing out scholarships to students and providing apprenticeships to support their 'cyber security' effort.

If it walks like a duck, and quacks like a duck…

Ren – I know you were keen to talk: