

Who is Mr Gu?

intrusiontruth.wordpress.com/2020/01/10/who-is-mr-gu/

intrusiontruth

January 10, 2020

In our previous articles we identified thirteen companies that this blog knows are a front for APT activity in Hainan. Following further analysis, we noticed a close association between these Hainan front companies and the academic world. Multiple job adverts for the the companies are posted on university websites. Hainan Xiandun even appears to operate from the Hainan University Library!



天眼查 TianYanCha.com 国家中小企业发展基金旗下 官方备案企业征信机构

查公司 查老板 查关系

海南仙盾科技开发有限公司 天眼一下

仙盾科技 海南仙盾科技开发有限公司 我要认证

存续 小微企业

电话: 13907545649 登录查看 邮箱: shunxiangcaiwu@163.com 查看更多

网址: 暂无信息 地址: 海口市海南大学图书馆南一楼 附近公司

浏览量: 834

仙盾科技 企业架构图 瞬息掌握企业关系

仙盾科技 股权穿透图 挖掘深层股权结构

Hainan Xiandun registration details showing Hainan University library as its address

Gu Jian

This company summary for Hainan Xiandun also provides a contact number: 13907545649. Cross-referencing this partial phone number and Hainan, we identified Gu Jian (顾剑) is a Computer Science specialist at Hainan University. We found Gu's name and phone number in this [list of projects](#) on the Hainan University website.

Here is Gu's CV:

And here is his biography from [his web page](#) at Hainan University's website showing his work history and interests, including as a former member of the People's Liberation Army.

海南省自然科学基金通知结题一览表					
序号	项目编号	项目名称	负责人	起止年月	
1	80044	中国热带城市石油污染修复技术及其机理研究	姜新建	2007.1-2008.12	1397678377D 环精
2	80675	海南岛蓝翅黄鹂调查及GPS追踪技术验证与模式研究	何春生	2007.1-2008.12	13976128033 环精
3	80032	贵州Monte Carlo 气象气溶胶以拟合含响非空煤石钙离子吸收研究	许达远	2007.1-2008.12	13976746296 林松
4	80006	海南地区热带中微菌生态多样性基因分析	廖育声	2007.1-2008.12	13178923579 林松
5	80626	模拟环境可降解生物基高分子性能影响研究	张治	2007.1-2008.12	13787554537 林松
6	50653	潜水水凝胶型天然橡胶复合材料的研发	肖新	2006.8-2008.8	13389898782 林松
7	70659	中国无糖饮料生产综合管理规划决策分析	傅国章	2007.1-2008.6	13976928328 经济
8	80477	海南岛海洋资源管理理论与实证研究	傅国章	2005.03-2007.12	13976928328 经济
9	80920	热带粮食分析测试的理论与应用研究	傅国章	2006.1-2007.12	13976928328 经济
10	80354	海南经济特区房地产投资风险研究	李仁君	2006.1-2008.12	139769099515 经济
11	80553	海南纪念品溯源设计开发平台关键技术研究	姜林峰	2006.1-2007.12	13138907919 旅游
12	80640	基于“生产-流通”的利率决定与货币政策研究	姜建忠	2007.1-2008.12	13136010675 旅游
13	80542	森林经营学三科或森林学发展动态对比跟踪研究	黄国良	2006.1-2008.12	13003982258 农学
14	80659	巴西橡胶树病原菌病原学特性与致病性研究	姜建忠	2007.1-2008.12	13976491305 农学
15	80543	马尾藻活性多糖的提取、结构分析和活性研究	黄石生	2006.1-2007.12	13648946501 食品
16	80621	赤霉病抗性(壳)化剂促进木薯秆茎秆纤维降解机理研究	王福刚	2007.1-2008.12	13036002623 食品
17	80624	海南岛热带多雾的成因分析及性能研究	张元平	2007.1-2008.12	13648916100 食品
18	80231	编制+ERP+制造+1040) 精细会计	顾剑	2003.1-2004.12	13987545649 信息

List of Hainan University project titles linking 13907545649 to Gu Jian

海南大学第二届“十佳教师”申请表					
姓名	顾剑	性别	男	出生年月	1958.2
学历/学位	工学硕士	民族	汉	政治面貌	中共党员
工作单位	信息科学技术学院	职称	教授	职务	教师
电话	13907545649	电子邮箱	gujian@hainu.edu.cn		
在海南大学任教时间	15年	近两年承担本科生课程门数	504学时		
近两年学生因个人原因、掉课的总数、学时	0次/0学时	近两年承担、主持或主讲	0次		
2《网络课程》	专业选修 31	86 设计思维(40人)	08-09第2学期		
3《计算机组成原理》*实验	专业基础 22/31	89 计算机组成(40人)	08-10第1学期		
4《操作系统》*实验	专业基础 33/31	87 设计思维(40人)	08-10第1学期		
5《操作系统》*实验	专业基础 33/31	87 设计思维(40人)	08-10第1学期		
6《操作系统》	专业基础 61	87 设计思维(40人)	08-10第1学期		
7《操作系统》*实验	专业基础 22/31	88 设计思维(40人)	08-10第2学期		
近两年指导毕业论文(设计)情况					
毕业论文(设计)题目	学号	姓名	年级、专业	成绩	
信息学院; 电子工程、计算机科学与技术学院; 计算机专业等 19 名学生(具体见附表)					
近两年教学改革与科研情况					
主持或参与的主要项目、论文、教案、教材等代表作等, 科研成果等(可另附页):					
1. 独自编写《信息安全专业用《计算机组成原理》》					
2. 参与编写教材《新编旅游管理信息系统教程》(南开大学出版社)					
3. 发表论文《解决电子商务中支付的安全问题关键方案》电子科技大学学报					
4. 完成省教育厅《核心数据的分布式安全存储系统》项目负责人					
近两年承担过课程建设或教材编写, <input type="checkbox"/> 是 <input checked="" type="checkbox"/> 否, 列举如下:					
近两年获奖情况(主要是教学类荣誉及指导学生获奖)					

Gu Jian's CV

所在位置: 首页 - 学者导航 - 顾剑



顾剑

职称: 教授

研究方向: 信息安全系

所属院系: 信息科学技术学院

成果数量: 32条, 属于本单位的个人成果32条

简介: 当过知青、解放军战士、省军区政治部干事、国企高级工程师、法国BULL公司北京代表处中方雇员(技术主管);曾任原中国人民建设银行“全国房改对公、储蓄系统”开发组特别技术顾问;国家重点工程“(北)京哈(尔滨)高速公路四平长春段”收费系统 设计负责人、主要设计人(公司方);国家、海南省重点工程“海南金融IC卡”系统技术负责人、主要设计人、IC卡... 详细

Gu Jian's University biography

“[Gu Jian] worked as an educated youth, a PLA soldier, an officer of the Political Department of the Provincial Military Region, a senior engineer of a state-owned enterprise, and a Chinese employee (technical director) of the French representative office of the French company BULL.”

Gu Jian, a Professor in the Information Security Department and former member of the PLA is now the *contact person for an APT front company which itself is linked to twelve other front companies*.

Hainan Xiandun Information Security Technology Competition

Mr Gu is closely involved with Hainan Xiandun. In September 2013, he posted on the Hainan University online forum about “The 2013 Hainan Network Information Security Technology Competition” saying that teams could enter and that there would be prizes. The posting indicated that more detail was available on xdaqjs[dot]com. This domain is an acronym from the Pinyin for Xiandun Security Competition Final (XianDun AnQuan JueSai – 仙盾安全决赛).



These links between Hainan Xiandun and Hainan University are seen again on the internal Hainan University discussion forum. A user name “xdaqjs” posted to encourage students from any specialism and in any year with an interest in cyber security to attend a session hosted by Hainan Xiandun in the auditorium of the information technology department on 9 September 2013.

The competition ran again in 2016, still using xdaqjs as a title.



xdaqjs[dot]com

Mr Gu was not just advertising this competition for a company that he was involved in, he registered the domain.

jian gu registered "xdaqjs.com"

Contact Email: lmh400@163.com	Registrant Address: hainanshenghaikoushi haikou Hainan 570228
WhoisServer: grs-whois.hichina.com	Registrant Country: Registrant Phone Number +86.89866267833
Create Date: 27-aug-2013	Registrant fax: 8689866267833
Update Date: 27-aug-2013	
registrar Name: HICHINA ZHICHENG TECHNOLOGY LTD.	

Password cracking

A link to the malicious activity of the front companies can be seen when reading discussion forums about xdaqjs. Individuals purporting to represent the site offered large sums of money to people with password cracking skills outside the ordinary range of dictionary attacks and brute force.



Individuals from xdaqjs offer money for password cracking skills

The opening post reveals that Mr Gu is seeking new ways of cracking passwords. The poster is aware of the common techniques, for example brute force or dictionary attacks, but is seeking new alternatives.

What makes this interaction increasingly strange though, is that a student posting on this thread said that Mr Gu is inexplicably wealthy and is offering a large amount of money to people able to provide new and inventive ways of cracking passwords. The original text is telling:

“Haha, I only want to know are these things actually crackable... From what I know about our teacher, he doesn't waste his words. Our teacher says if no-one can crack it this time, then he'll increase the money on offer, 200,000, 300,000, 500,000 RMB.

P.S. Believe it or not, our teacher has a lot of money...”



Mr Huang

The Dean of Mr Gu's faculty is CCP member Huang Mengxing (黄梦醒). The questions we should ask are: How well does Huang know Gu? Does he know about his department's support for front companies for APT activity?

Most importantly, if he knew then should he have stopped it?

黄梦醒, 男, 1974年1月4日出生于河南信阳, 研究生学历, 博士学位, 副教授; 现任海南大学信息学院计算机系主任, 硕士研究生导师。联系电话: 13876345398, Email: huangmx09@gmail.com。

2007年在西北工业大学自动化学院获系统工程工学博士学位, 2007-2009年在清华大学信息技术研究院完成计算机科学与技术专业博士后研究工作, 主要从事《决策支持支持系统》、《管理信息系统》、《知识工程》、《软件项目管理》等专业课程的教学工作。在所从事的专业领域取得一定的成就。近5年来以第一作者身份发表学术论文30余篇, 其中SCI、EI、ISTP收录近20篇; 参与撰写专著及翻译著作各1部。主持和参与科研项目共12项: 国家“十一五”科技计划2项, “863”计划2项, 国家公益性行业(农业)科研项目1项, 铁道部基金1项, 北京市科技计划1项, 横向课题5项; 其中主持项目4项; 现在研的各级各类课题4项。

主要研究方向: 数据与知识工程、信息系统、电子政务与电子商务、电子商务、内容管理、物联网(物流与供应链管理)、系统工程等

硕士招生专业: 计算机应用技术、农业信息化、电子与通信工程



In summary, Gu Jian, a former member of the PLA is an academic specialising in Information Security at Hainan University. He is also listed as the contact person for Hainan Xiandun, one of a network of front companies for APT activity.