An APT with no name

intrusiontruth.wordpress.com/2021/05/06/an-apt-with-no-name

intrusiontruth May 6, 2021

When the 7th July indictment was released naming two Chinese hackers affiliated with the Guangdong State Security Department, it grabbed our interest. Hackers… in China…working with the MSS. Sounds right up our street. But who are Li Xiaoyu (李啸宇) and Dong Jiazhi (董家志)? How do they conduct their activity? The indictment also mentions an unnamed MSS Officer 1. Who could this be? Let's start with the named hackers…

联邦调查局

通缉令

中国国安部广东省国家安全厅黑客

越权进入；阴谋越权进入并损坏电脑；阴谋盗窃贸易机密；阴谋电汇诈骗；严重身份盗窃

Li Xiaoyu (李啸宇)

Dong Jiazhi (董家志)

警告

美国华盛顿州东区地方法院大陪审团于2020年7月7日起诉*Li Xiaoyu* (李啸宇) 和 *Dong Jiazhi* (董家志)，就其涉嫌参与一项长期针对美国及其他外国公司网络诸多领域攻击的行为: 包括高科技制造业、民用工业、重工业、医疗设备工程、商业软件、教育软件、游戏软件、太阳能、制药业和国防工业。 此起诉书聚焦于李董二人涉嫌的行为，包括近期一项以新冠病毒爲主的研究、测试及治疗；以及针对在中国大陆、香港、美国和加拿大的政治异议人士、宗教少数派和人权拥护者；以及入侵欧亚国家的公司网络。

李董二人声称某些网络行为是为了个人经济利益，但另一些则涉及中国国家安全部 (*MSS*)并广东省国家安全厅的利益。

如果您有任何关于此二人的信息，请与当地的联邦调查局分局或附近的美国大使馆或领事馆联系。

联邦调查局分局： 西雅图

FBI wanted poster naming indicted hackers Li Xiaoyu (李啸宇) and Dong Jiazhi 董家志)

Former classmates, Li Xiaoyu and Dong Jiazhi studied Computer Application Technologies at the University of Electronic Science and Technology of China (UESTC) in Chengdu. Mr Dong and Mr Li are not individuals we have come across before in our investigations into Chinese APTs. However, we do love a challenge. So, we set about getting to work and decided to start in the city Li and Dong are based: Chengdu.

Our findings reveal a number of spurious science and technology companies linked to the indicted actors. A familiar pattern is once again emerging…

Chengdu Shirun Technology Company Ltd (成都诗润科技有限公司)

Let's start with Dong Jiazhi. There is very little to go on from the indictment. However, we know Chinese APTs follow a common blueprint: One of contract hackers and specialists, front companies and an intelligence officer.

We know Mr Li and Mr Dong are the contract hackers. So we set about digging into their connections to front companies based in Chengdu.

It turns out Dong has been investing in a company called Chengdu Shirun Technology Company Ltd. Specifically, 30,000RMB came from Dong, who invested in the company when it was registered. This roughly equates to $4,5000 or £3,500.

Registrant of Chengdu Shirun Technology Company Ltd: Dong Jiazhi

A deeper look into this company reveals its location is 16 Tongsheng Rd, Qingyang District, Chengdu. It also provides a contact number: 18828070461.

Interestingly, this is not the only company that is linked to this contact number. It seems a number of other companies in Chengdu also share this point of contact.

Chengdu Hanke Technology Company Ltd. (成都撼科科技有限公司)

This company shares the same contact number as Chengdu Shirun but lists this as an email contact (18828070461@139.com). Additional contact numbers (18980738906 and 18190696626) are also provided.

*Contact details for Chengdu Hanke Technology Company L*td.

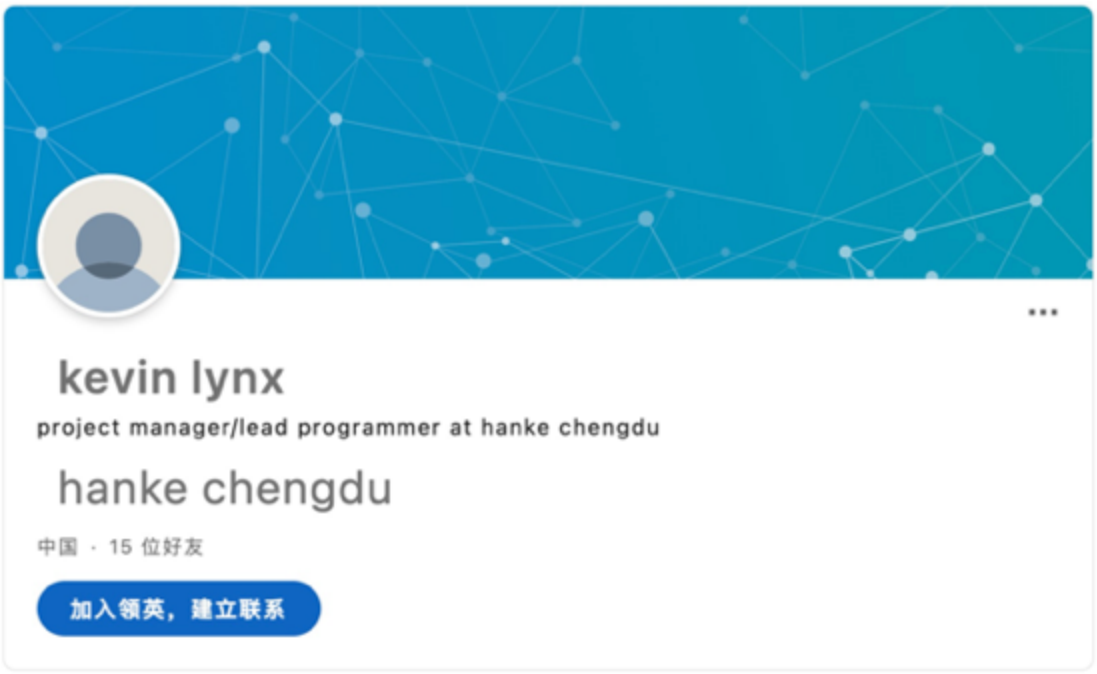
Even more interesting is the change record for the company. Prior to 2019, Dong Jiazhi was listed as the company contact.

变更记录 6

序号	变更日期	变更项目	变更前	变更后
1	2019-07-12	主要人员	李艳，监事 ~~周麒麟，执行董事兼总经理~~	李艳，监事 张显云，执行董事兼总经理
2	2019-07-12	章程	-	-
3	2019-07-12	联系人变更	~~董家志~~	张显云 [新增]

Change record for Chengdu Hanke listing Dong Jiazhi on line 3

Chengdu Hanke doesn't have much of a presence. The website domain 51409903.1024sj.com does not exist. However, we did come across a LinkedIn profile for someone who claims to be the project manager and lead programmer – a Kevin Lynx. Further digging did not reveal anything more on this person or the company. Kevin, if you are out there – feel free to get in touch…



Chengdu Xinglan Technology Company Ltd. (成都兴蓝科技有限公司)

It seems 18828070461 is a theme. The number from Shirun and the 139 email from Hanke was also used to register another Chengdu-based technology company: Chengdu Xinglan.

So who is behind this company? Well, as we mentioned, it shares contact details with companies linked to Dong. And Mr Dong is mentioned as the company's primary point of contact.

变更记录 2

变更项目

序号	变更日期	变更项目	变更前	变更后
1	2017-08-24	补发证照	-	-
2	2016-06-17	联络员备案	董家志,*****	董家志,*****

Company registration details listing Dong Jiazhi as a contact person for Chengdu Xinglan on line 2.

Furthermore, records show Li Xiaoyu as Chengdu Xinglan's legal representative, CEO and Executive Director, having a 99% stake in the company. It seems the pair intertwined at University, and expanded together into their business ventures and criminal activity concealed by front companies based in Chengdu.

Chengdu Xinglan, detailing the 18828070461 contact email and Li Xiaoyu as the company's legal representative.

Chengdulzy

Li and Dong haven't learnt to mix things up – reusing the same email number for their multiple front companies.

And once again, this number (18828070461) was used as the registrant contact number for a domain: 'chengdulzy.com'.

The registrant of this domain? Dong Jiazhi. Unfortunately, we haven't found out what this domain was used for, and it now appears to have been deleted.

```
Domain Name: CHENGDULZY.COM
Registry Domain ID: 81303651_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.west263.com
Registrar URL: www.west263.com
Last updated Date: 2013-05-28T04:06:15.0Z
Creation Date: 2013-05-28T04:06:15.0Z
Expiration Date: 2015-05-28T04:06:15.0Z
Registrar Registration Expiration Date: 2015-05-28T04:06:15.0Z
Registrar: Chengdu west dimension digital technology Co., LTD
Registrar IANA ID: 1556
Registrar Abuse Contact Email: Abuse@westdata.cn
Registrar Abuse Contact Phone: +86.2886263960 ext 8245
Domain Status: ok http://www.icann.org/epp#ok
Registry Registrant ID:
Registrant Name: dong   jiazhi
Registrant Organization: dong jiazhi
Registrant Street: chengdushi erhuanlubeierduan
Registrant City: chengdu
Registrant State/Province: Sichuan
Registrant Postal Code: 611000
Registrant Country: CN
Registrant Phone: +86.18828070461
Registrant Phone Ext:
Registrant Fax: +86.18828070461
```

Chengdu's many Science and Technology companies

We are finding a similar pattern to previous investigations. An overlap of numbers and emails linking to contract hackers (Dong and Li), and subsequently to a number of technology companies based in Chengdu. All with little to no online presence suggests – you guessed it – front companies.

However, what about the individuals themselves? They clearly have been busy investing in, and creating multiple technology businesses within Chengdu to act as fronts for their hacking activity. But what else have they left on the internet for us to find?

Oro0lxy

The handle used by Li, and named in the indictment provides a helpful starting point. A quick scan of the internet shows various accounts with this handle, most now defunct or empty but the majority pertaining to hacking forums, such as the Chinese Software Developers Network

(CSDN).

It seems oro0lxy has had a long standing interest in ColdFusion, using this knowledge (according to the indictment) to develop vulnerabilities in support of his APT activity.

oro0lxy posts question on CSDN ColdFusion sub forum

In keeping with his interest in this vulnerability, Li was appointed moderator of a website for ColdFusion developers, CFwindow.com, in 2012.

However, oro0lxy was later flagged for posting scams on CSDN.

QQ account links

Looking into Li and Dong's QQ accounts, we attempted to identify their actions and any overlaps that were interesting or of note. According to leaked databases, QQ 3120988 was associated with the display name Li Xiaoyu, whilst QQ 191956463 had historically used the username Dong Jiazhi.

We also pulled out a number of QQ groups that crossed the two hackers profiles. Specifically their QQ accounts linking to university groups such as 'Class of 2005, Class 5' (2005 级5 班),'Information Security Lab' (信息安全实验室) and 'Computer Applications Technology Class 2' (计算机应用技术 2 班).

These are historic but provide useful context for what we know about the pair. Get in touch with us if you have any further information or leads pertaining to these accounts.

So… we know that Li and Dong have been indicted as hackers working to the MSS. Contract hackers – check.

We know that they set up a number of front companies based in Chengdu to shield their APT activity. Front companies – check.

And we know they have been working together for a number of years, having met at university and remained active on Chinese hacker forums. But who specifically is behind their activity with the Guangdong State Security Department? Who is MSS Officer 1?

Tune in next week to find out…

#youknowwherethisleads