Hainan Xiandun Technology Company is APT40

By intrusiontruth

Published: 2020-01-15 · Archived: 2026-04-05 16:53:27 UTC

You knew where this was heading.

In our previous articles we identified a constellation of front companies for APT activity in Hainan and a computer science specialist at Hainan University who is linked to one of the companies. We named the individuals that we could identify as working for these companies, including one that we know to be Hainan resident Ding Xiaoyang who had used his telephone number on a job advert using the name ‘Mr Chen’.

Having identified a network of interlinked technology and information security companies in Hainan, looking at other job adverts posted by the companies is illuminating…

South China Sea Penetration (Testing)

Considering these are high-tech companies advertising for penetration testers, software development engineers, and network engineers, of course the logical next set of job adverts that we expected to find were for … specialist translators?

Hainan Xiandun posted multiple adverts for English translators between 2014 and 2018, such as this one on the Hainan University website:

Hainan Xiandun advert looking for English translators

An English language translation service in-house at a high-tech firm may meet a legitimate business need. Less likely is for a Hainan technology firm to need its own in-house Cambodian linguists. But, in March and April

2018, Hainan Xiandun was recruiting Cambodian linguists to join their team. Remember those dates, they will be important later.

公司地址	海南大学图书馆南一楼				公司网址		
联系人	蒋经理			联系方式	13208905740		
人才需求情况	编号	岗位名称	所需专业	招聘人数	岗位职责	岗位要求	福利待遇
	1	柬埔寨语翻译	柬埔寨语	3	柬语笔译；调研报告等	本科以上；知识面广；沟通力强；语言成绩证明	试用期6800；转正8500（税前）；法定节假日等
招聘方式	请有意应聘的同学直接与其联系						
招聘截止日期	长 期						
备注	招聘信息发布时间：2018年3月30日						

Hainan Xiandun advert looking for Cambodian linguists in early 2018

Additionally, a spreadsheet published by the Shanghai International Studies University shows that Hainan Tengyuan was advertising for Indonesian and English translators.

上海新华发行集团有限公司	IT兼行政	2	上海市	信息管理与信息
中国专利代理（香港）有限公司深圳代表处	德语翻译	1	广东省	德语,翻译
海南腾远科技有限公司	印尼语市场专员	5	海南省	印度尼西亚语
海南腾远科技有限公司	英语笔译专员	5	海南省	英语
上海智造邦信息科技有限公司	人事主管/行政主管	1	上海市	不限
上海智造邦信息科技有限公司	微信公号运营/新媒体运营	1	上海市	不限

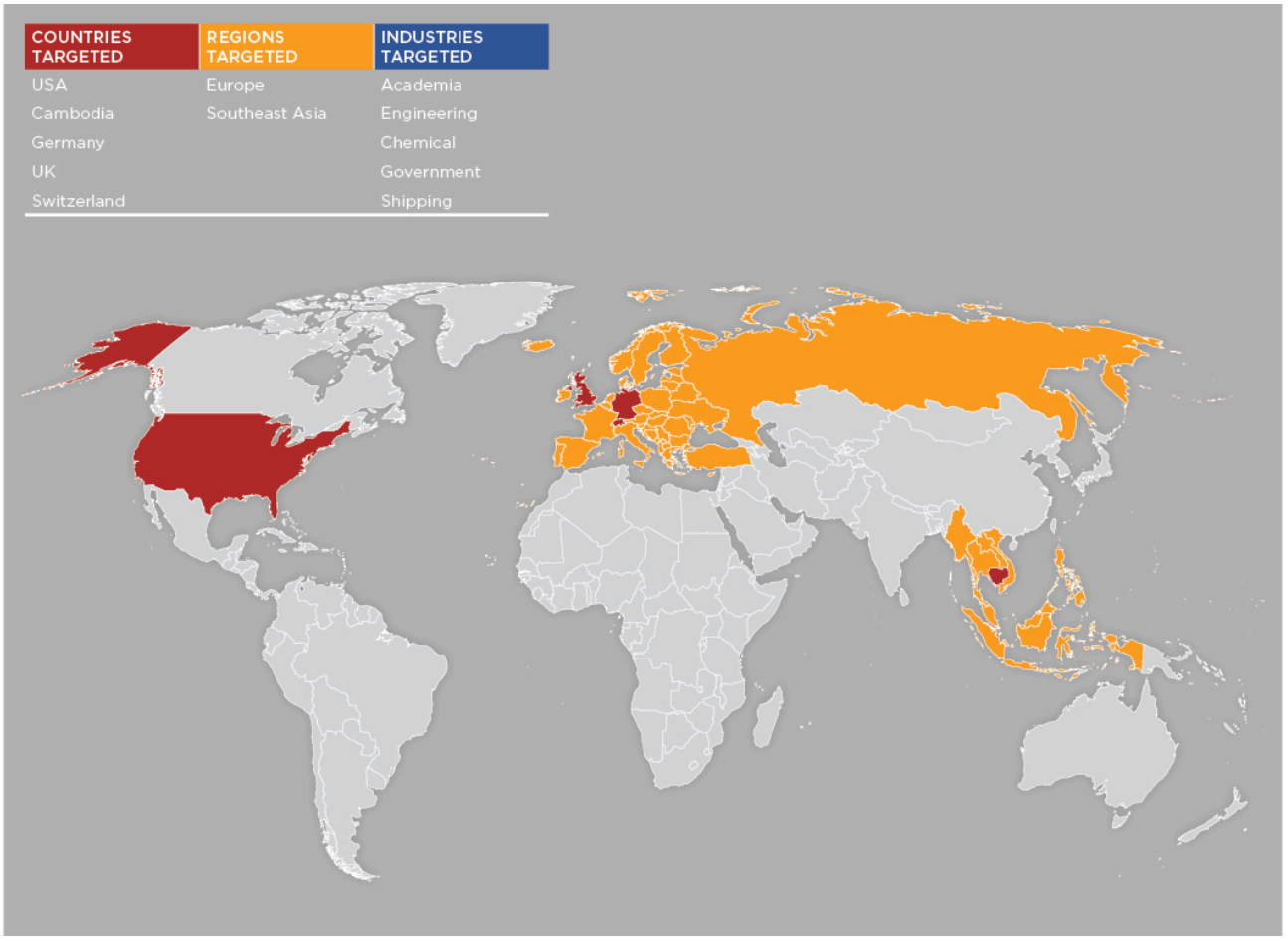
And of course let’s not forget Sugar, who we previously identified as a Vietnamese translator at Hainan Kehua.

APT40

Which brings us to this report by FireEye on TEMP.Periscope, also know as APT40.

> FireEye has examined a range of TEMP.Periscope activity revealing extensive interest in Cambodia’s politics, with active compromises of multiple Cambodian entities related to the country’s electoral system. This includes compromises of Cambodian government entities charged with overseeing the elections, as well as the targeting of opposition figures. This campaign occurs in the run up to the country’s July 29, 2018, general elections. TEMP.Periscope used the same infrastructure for a range of activity against other more traditional targets, including the defense industrial base in the United States and a chemical company based in Europe. Our previous blog post focused on the group’s targeting of engineering and maritime entities in the United States.

The report shows a world map highlighting the targets of APT40. This includes a number of English speaking countries, Indonesia, Vietnam, and Cambodia.



APT40 conducted a series of compromises of Cambodian targets in the run up to the July 2018 Cambodian election. Did you remember those dates? Between March and April 2018 Hainan Xiandun, a front company with specialist network and penetration engineers, was recruiting Cambodian linguists.

112[.]66[.]188[.]28

FireEye have also reported that APT40 actors are based in China, using computers configured with Chinese language settings.

This report also shows APT40 using IP address 112[.]66[.]188[.]28 which resolves to, guess where, Hainan.

```
          Source: whois.apnic.net
      IP Address: 112.66.188.28

% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '112.66.0.0 - 112.67.255.255'

% Abuse contact for '112.66.0.0 - 112.67.255.255' is 'anti-spam@ns.chinanet.cn.net'

inetnum:        112.66.0.0 - 112.67.255.255
netname:        CHINANET-HI
descr:          CHINANET HAINAN PROVINCE NETWORK
descr:          China Telecom
descr:          No.31,jingrong street
descr:          Beijing 100032
country:        CN
status:         ALLOCATED PORTABLE
admin-c:        ZH201-AP
tech-c:         ZH201-AP
remarks:        service provider
mnt-by:         APNIC-HM
mnt-lower:      MAINT-CN-CHINANET-HI
mnt-routes:     MAINT-CN-CHINANET-HI
remarks:        ------------------------------------------------------
remarks:        To report network abuse, please contact mnt-irt
remarks:        For troubleshooting, please contact tech-c and admin-c
remarks:        Report invalid contact via www.apnic.net/invalidcontact
remarks:        ------------------------------------------------------
last-modified:  2016-05-04T08:16:02Z
source:         APNIC
mnt-irt:        IRT-CHINANET-CN
```

So what?

Mr Ding and Mr Gu could be busy Hainan based individuals simultaneously running multiple companies that have specialisms spanning from penetration testing and software development to the translation of Cambodian guidebooks and Indonesian literature.

But they aren't.

Hainan Xiandun Technology Development Company is APT40.

Hainan Xiandun, and the other front companies that we have identified, recruit hackers to compromise overseas targets and linguists to help them with their attacks and translate their stolen material. Industry reporting shows APT40 has used an IP address in Hainan and attacked South East Asian targets.

Mr Gu brings the academic links, but what does Mr Ding bring?

Post navigation
