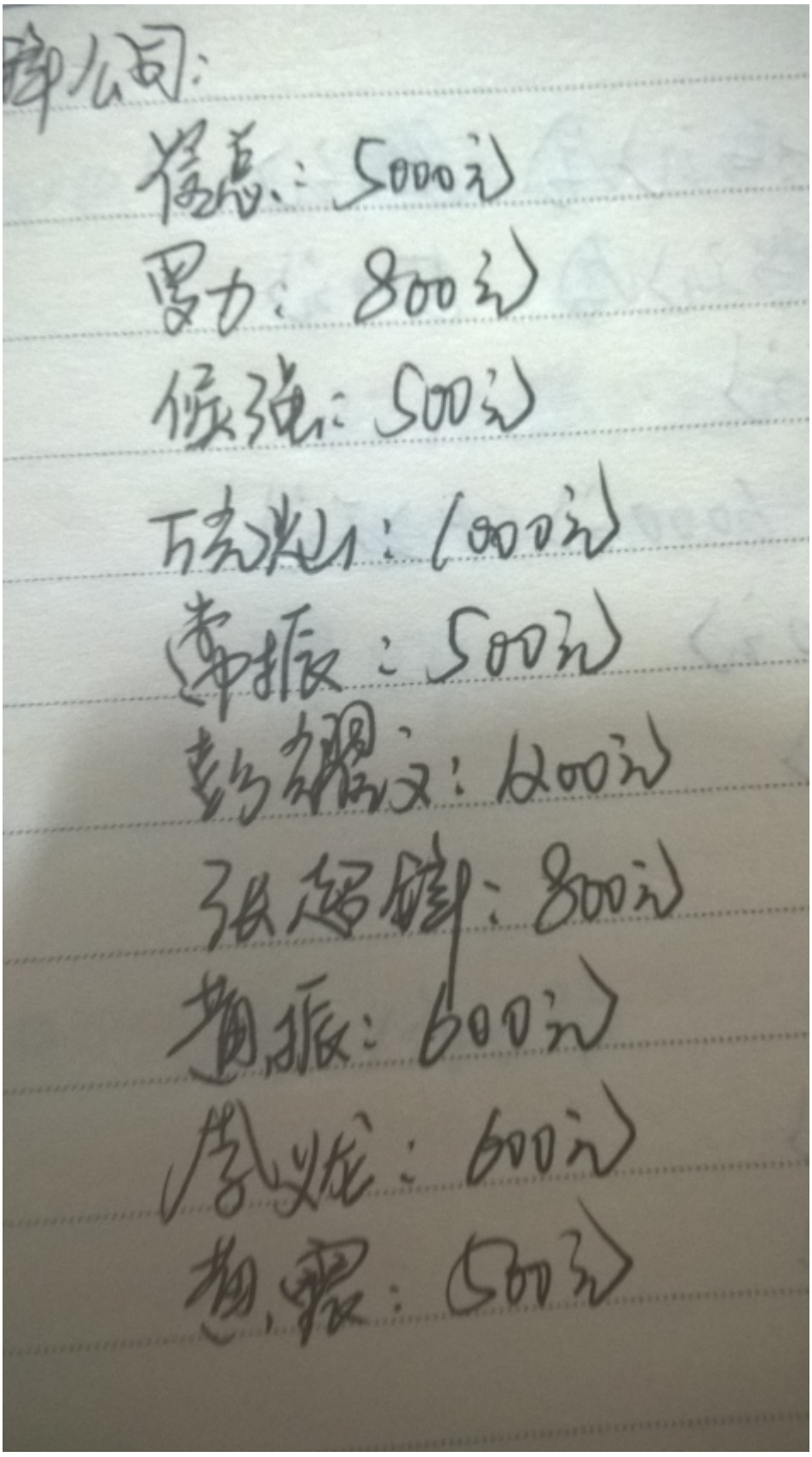
MiSSing links

intrusiontruth ⋮⋮ 5/17/2023

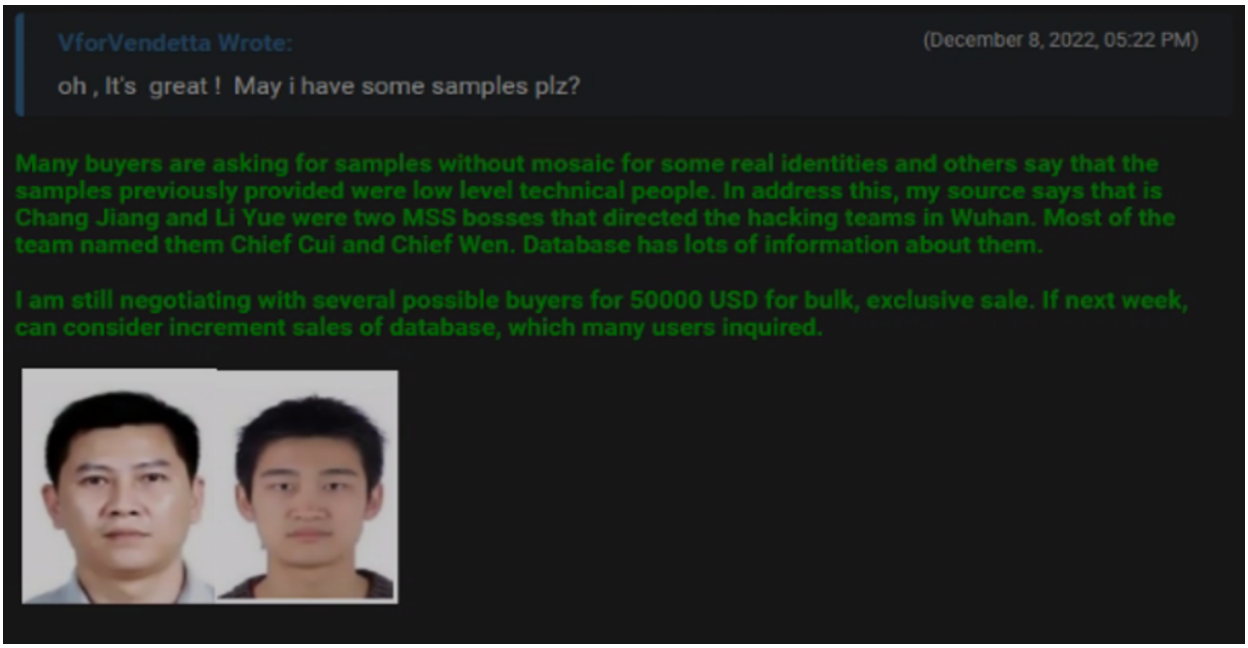
We haven’t quite finished with Mr. Cheng yet. We have one final document to share from Cheng’s cloud. A photo of a handwritten note, a series of names, and differing currency values.



Now, we can't make out the name in the top left, but we are pretty sure that this is a cast list of Cheng's colleagues. Some of these names are old hat by now: Huang Zhen, Li Yilong, and Huang Zhen #2, for example, take up the bottom three rows. We also have some others we named earlier: Hou Qiang, Wan Guangcan, Chang Zhen, and Zhang Chaofeng.

Not entirely surprising; we have already established the fact that Cheng and these other individuals work for the same front company. But one name caught our eye, occupying the top line of the table: 崔总 or Chief Cui.

This seems like an *apt* time (if you'll pardon the pun) to return to our disgruntled whistle-blower at Wuhan Xiaoruizhi. Among the individuals they outed as being part of Wuhan-based hacking team operating out of Xiaoruizhi were two MSS officers: Chief Wen and Chief Cui.



The eagle-eyed amongst you might also recognize Chief Wen from an image in the previous article, on the price list of routers, firewalls, and network cables that Cheng had.

Now we had a really good dig into Chang Jiang AKA Chief Cui and Li Yue AKA Chief Wen. Unfortunately, we could not find anything conclusive, which is possibly indicative of the level of personal operational security one might expect of the mighty MSS. In the absence of anything more concrete, Chief Cui's name in Cheng Feng's possession with a number of Xiaoruizhi employees, and Chief Wen's name on a document in Cheng Feng's possession at least adds weight to our friend on Breachforums' association that Cui and Wen maintain links to the company.

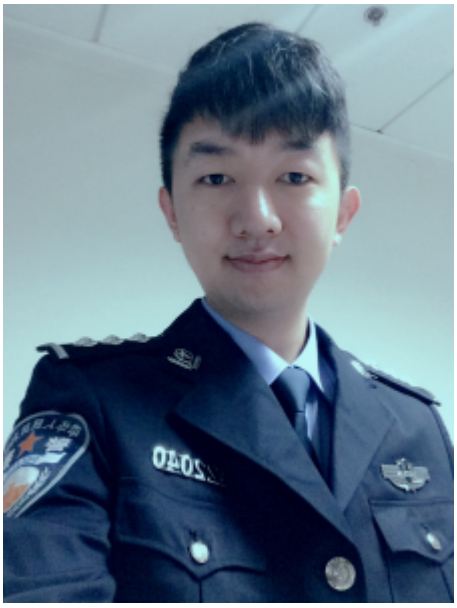
This got us thinking: we wonder who else works in and around Wuhan Xiaoruizhi who has MSS links?

Zhou Yuan

Thankfully, our investigation into Cheng Feng gave up one more lead. Some of the databases we queried looking for Cheng's credentials contained access logs for the services. We knew Cheng didn't work in a vacuum, in fact, we already knew he was one of many employees at Xiaoruizhi. So, we wondered if we could find any more of his colleagues based on his IP history. Analysis of three Wuhan Chinanet IP address indicated that through much of 2015, Cheng Feng's accounts were co-located with an account owned by one Zhou Yuan周源.

Now we have been giving everyone the deep dive treatment, and our friend Zhou is no different. We couldn't find much trace of him on social media, but thankfully the gods of breached data continued to smile on us. We again worked with a trusted contact who was able to gain access to one of Zhou's Cloud

hosting accounts. Here we have, from that Cloud account, two 2016 photos of our friend Zhou in glorious selfie style.



The uniform he is wearing is one used by both the Chinese Ministry of Public Security and the MSS. The two are near identical, but for a couple of distinguishing factors. The first, characters on the arm badge, above the orange and beneath the word ‘POLICE’.

MPS “公安” (Public Security) badge on left; MSS “国安” (State security) badge on right.

In his left-hand selfie, these characters are not visible on Zhou’s uniform – we can’t be sure if he has pixelated them. If he has, what is he trying to hide?

The second distinguishing factor can be found on the pin on Zhou’s chest, which conveniently is visible.

A closer look at Zhou’s pin:

Zhou's badge reads "国安" or State Security; distinct from MPS badges which display the province name as below:

MPS badge for "广东" or Guangdong

So, we are pretty confident that Zhou is wearing an MSS uniform.

Zhou's selfies also provided us with another gift. Metadata. In this case, geolocating Zhou to the headquarters of the Hubei State Security Department.

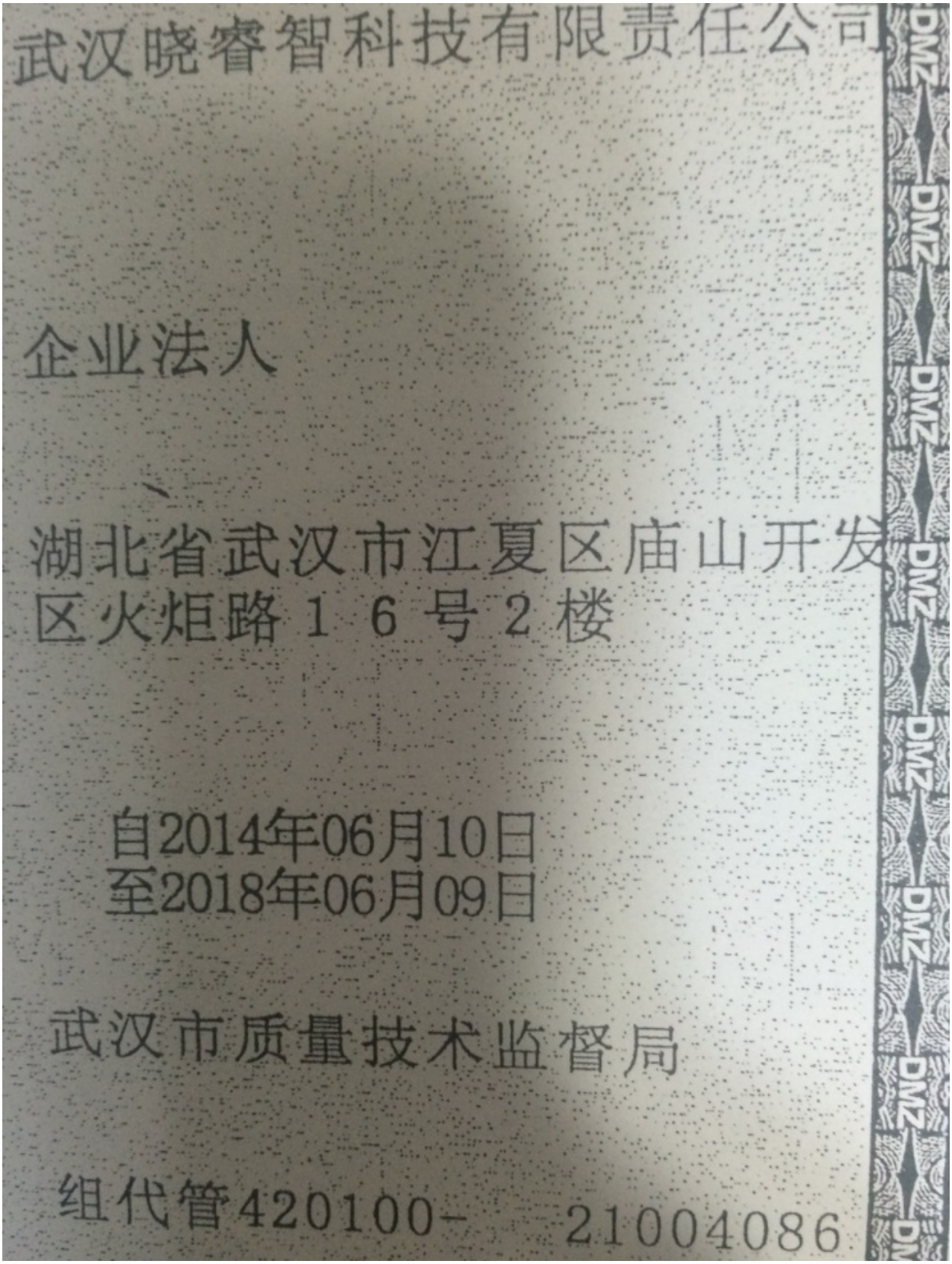
Zhou looks so young and innocent that we almost feel guilty. But then, if you are going to take selfies in an MSS uniform…in an MSS building… As they say in China 凡动刀的，必死在刀下. Those who live by the sword, die by the sword.

Demonstrating the longevity of Zhou's affiliation with the MSS, we also found a 2018 photo again geolocated to what appears to be the secure car park of the same imposing building.

Now, we can't be sure of Zhou Yuan's true employer. But we can say for sure that he is an employee of the Chinese government, and at very least was affiliated with the MSS over a period of several years.

So, we have a possible MSS officer regularly connecting to personal accounts from the same IP addresses as Cheng Feng, an employee of a supposedly private Wuhan-based technological enterprise. Strange, certainly, but not a smoking gun which proves Wuhan Xiaoruizhi's links to the MSS beyond reasonable doubt. After all, spies have friends just like normal people, and Cheng and Zhou could be just that.

Now we found one more photo we found in Zhou's possession which we think brings our story nicely full circle and will be where we leave you, for now at least.



This, dear reader, is part of the official business registration certificate for Wuhan Xiaoruizhi Science and Technology. Why, you might ask, does a possible MSS officer hold the registration certificate for a private technological enterprise? Surely, someone holding such an important document has to have some kind of

senior oversight or administrative role in the company itself? At the very least, he is linked to the company.

At team Intrusion Truth we are satisfied Zhou having a photo of this certificate and being regularly collocated with a Xiaoruizhi employee bears out our theory that Wuhan Xiaoruizhi is not a private enterprise, instead it is a front for an MSS-sponsored APT. Zhou Yuan probably has a role in running the APT, along with his probable MSS colleagues Chief Cui and Chief Wen.

This has been a wild ride. How about we summarize how we got here.

We have found a suspicious hacking school whose owner has links to the MPS and MSS, and whose graduates go on to mysterious destinations and private companies supporting the government. One such destination is what looks to be a fishy APT front company. Said front company has a disgruntled employee leaking sensitive documents online and alleging that the company is affiliated with an elite hacking team in Wuhan. An employee of the front company bears out its links to Kerui Cracking Academy, and has material in his possession which supports his affiliation with APT31. Said employee has more material in his possession indicating links to two MSS officers who have already been doxed on the darkweb as part of Xiaoruizhi. This employee is also regularly collocated with a possible third MSS officer, who in turn has, in his possession, Xiaoruizhi documents.

One thing is for sure. All is not as it seems at Xiaoruizhi.

And now a plea to you: what else can you find on these individuals? Can you help us tighten the Xiaoruizhi's attribution to APT31?

Goodbye for now, but we will be back. We still have more to share on Xiaoruizhi and friends – 等着瞧.