

Who is Mr. Zhao?

 intrusiontruth.wordpress.com/2021/05/13/who-is-mr-zhao/

intrusiontruth

May 13, 2021

In our last article, we identified a number of front companies used by two Chengdu-based indicted hackers Li Xiaoyu and Dong Jiazhi.

What struck us when reading the US indictment was reference to the Guangdong State Security Department (GSSD). As eager readers of Intrusion Truth will note, we discussed the Guangdong SSD in our very first article series and their use of Boysec as a front company. However we didn't manage to identify the MSS officers behind APT3. We feel there is unfinished business here and so we set to work to uncover MSS Officer 1.

We started with an address.

GSSD HQ

Why is the Guangdong Province International Affairs Research Centre (GPIARC) interesting? Well, its claim to fame most recently comes from the 2020 indictment, revealing it as a GSSD cover company. The address: Number 5, 6th Crossroad, Upper Nonglin Road, Yuexiu District, Guangzhou, Guangdong Province (越秀区农林上路六横道5号).



We decided to reach out to our network of contributors, asking about the GPIARC and any previous reference to this company or their known address. We received an interesting response from a trusted source who wishes to remain anonymous. This source, with

connections to the Bank of China, was able to provide a number of historic credit card statement sent to the cover address at Upper Nonglin Road. One bank statement in particular stood out.

Zhao Jianfei (赵剑飞)

On the top left corner on the image below, the corresponding address is Unit 5, 6th Crossroad, Upper Nonglin Road, Yuexiu District, Guangzhou. Furthermore, all the transactions appear in Guangzhou, Guangdong.

We know this address is a cover for the GSSD. So, whoever is using this address works directly for the GSSD. So, who is this MSS officer?

Underneath the address is a single name to which the statement is addressed to: Zhao Jianfei (赵剑飞).

尊享

中國銀行 | 信用卡
BANK OF CHINA | Credit Card

服務熱線 Service hotline: 40066-95566/010-66085566
郵寄地址 Address: 北京808信箱 Beijing 808 P.O. Box 100037
網址 Website: www.boc.cn

環球精彩 一卡尽享
Visa 美國 加拿大 歐洲

持中行卡畅游 美国加拿大欧洲 多重优惠 等你来拿

2013年8月1日至2014年2月28日。持中国银行在中国大陆地区发行的Visa、万事达标识信用卡刷卡消费，有机会享受精彩多重礼遇。

优惠一 在美国、加拿大、欧洲全境商户（不含线上商户），周末（当地时间周六、日）刷卡消费，单笔交易每满等值200美元即享5%返现，单笔交易最高返还等值30美元（即等值200-399美元返等值10美元，等值400-599美元返等值20美元，等值600美元以上返等值30美元）。不限名额，无限畅游！

优惠二 在指定旅行社刷指定中行信用卡预订美国、加拿大、欧洲经典旅游线路，畅享每单立减1500-3000元优惠。名额有限，先到先得。

优惠三 美国、加拿大、欧洲众多优惠商户消费享受惊喜折扣。

优惠四 持指定中行信用卡购买国航、东航、南航三大航空公司规定产品享受不同折扣优惠。

使用全币种国际芯片卡出行更安全，跨境交易货币兑换费全额减免，还可选择全球交易人民币还款。全币种国际芯片卡白金卡、无限卡更可尊享全球DFS GALLERIA、LOTTE DUTY FREE等众多境外免税店全年不限时段5%返现等优惠。

了解更多详情请登录中国银行门户网站www.boc.cn。 更多精彩@中国银行信用卡

510080
中国广东省广州市
越秀农林上路六横路 5 号
广东省国际问题研究中心
赵剑飞 先生

还款存根 Payment Coupon

信用卡号	62275344****6827
账单日期	2013-10-06
到期还款日	
RMB本期余额\最低还款额	RMB45.13\0.00

* 本期余额为负，表明账户有欠款，否则为存款。如有欠款，请在【到期还款日】前到银行办理还款手续。

您的信用卡账项记录 Your Card Activities

账户类型 Category	信用额度 Combined Limit	可用余额 Available Balance	分期可用余额 Installment Available Balance	账单日期 Statement Date	到期还款日 Due Date
RMB	30,000.00	30,045.13	30,000.00	2013-10-06	

账户类型 Category	上期账单金额 Balance B/F	支出总计 New Charges	存入总计 Payments	本期余额 Current Balance	最低还款额 Min Payment
RMB	37.29	-15,192.19	15,200.03	45.13	0.00

Interesting. So, we know Zhao was receiving correspondence about a credit card bill, using the GSSD cover company as the address. It stands to reason that Zhao Jianfei is an MSS officer, working for the Guangdong SSD. Could he be MSS Officer 1?

Asls1027

An FBI flash memo released on the 21st July reveals further information pertaining to the email used by MSS Officer 1 to send Li and Dong zero-day exploits for use in their APT campaign. The memo has redacted the mail provider, but the handle is the bit we need: asls1027.



Additional information on the exploitation of web servers via web shells can be found at: <https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2159419/detect-prevent-cyber-attackers-from-exploiting-web-servers-via-web-shell-malware/>.

The MSS-associated cyber actors also deployed publicly available tools such as Mimikatz to gather user credentials. We have also observed the actors using a zero-day exploit provided by the MSS. In one instance, the actors received a zero-day exploit from email address asls1027@***.com. Frequently, the cyber actors stored tools and files in the Recycle Bin on victim hosts, or within directories related to the associated vulnerability. The actors also enumerated directories to learn about the network prior to data exfiltration. Additional details on publically available tool Mimikatz can be found at: <https://www.us-cert.gov/ncas/alerts/AA18-284A>.

Remember when we said one statement in particular from the Bank of China was interesting to us?

Well, turns out that Bank of China sent the credit card statement to the personal email of Zhao Jianfei.

The email address was asls1027@hotmail.com.

Zhao Jianfei is an MSS officer, working for the GSSD and receiving credit card statements to the address of a GSSD cover company. Furthermore, this correspondence was sent to his personal email; the same email account that sent cyber actors a zero-day exploit for use in their illegal activities.

Zhao Jianfei has been directing Li Xiaoyu and Dong Jiazhi by providing them with malware and supporting their APT campaign.

Asls1027's social media

As we know, humans are biased and often rely on availability heuristics: we tend to choose the least cognitively demanding option. As such, we tend to reuse email handles, passwords and so on. And it appears our Mr. Zhao falls into this category, reusing his handle across multiple social media sites.

Asls1027 has an interest in cars, posting on the car forum autohome.com.cn.

He also maintains a relatively empty yet bizarre Twitter profile.



asls
@asls1027
Joined October 2013
0 Following 14 Followers
Not followed by anyone you're following

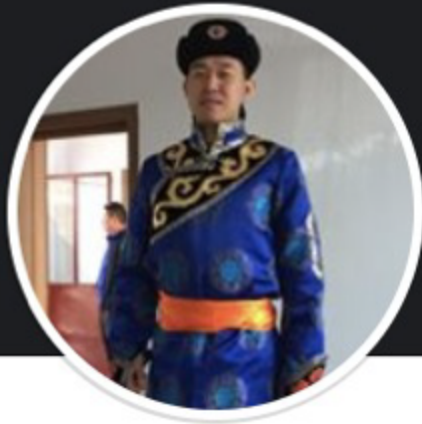
Tweets Tweets & replies Media Likes

asls Retweeted

DJ NICOLETTI @DJ4JG · 28 Oct 2014
☕☕☀️ G'Morning ☀️☕☕ my sunshines! #HappyTuesday🙌



However none of this provided us with any more information on Zhao Jianfei himself. We know he uses the asls handle and his name is Zhao Jianfei so we decided to get even more creative, and found an interesting profile on Facebook with the stub Asls Zh.



Asls Zh

Friends

Photos

Videos



About Asls Zh

EDUCATION



xian lintong railway high school

Class of 2002 · Xian, China



The PLA Information Engineering University

Computer science

CURRENT CITY AND HOME TOWN



Guangzhou, China

Current city



Xian, China

Home Town

Given the unique of the handle 'asls', we strongly believe this profile belongs to our Mr. Zhao. The profile picture was updated in 2014, a similar timeframe to other asls social media posts, as well as Zhao's credit card activity in Guangdong. Zh = Zhao.

It seems Zhao was born in Xi'an, Shaanxi Province. Also note Asls Zh's current residence – Guangzhou, in Guangdong Province. The same location as the Zhao Jianfei's credit statement.

Asls Zh went to the PLA Information Engineering University to study Computer Science. It fits with what we know about MSS Officer 1, and his ability to deploy zero-day exploits to support criminal hackers.

Conclusion

Zhao Jianfei is MSS Officer 1.



He grew up in Shanxi, and attended a PLA university studying computer science. He now resides in Guangdong and has been working for the GSSD from at least 2013. An email account linked to his GSSD activity was also used to send Li and Dong malware to advance their APT campaign.

Contract hackers – check.

Front companies – check.

MSS officer working to the Guangdong State Security Department – check.