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).

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

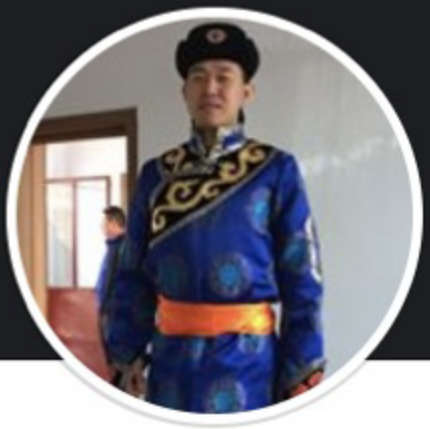
As we know, humans are biased and often rely on availability heuristics: we tend to choose the least cognitively demanding option. As such, we tend to reuse email handles, passwords and so on. And it appears our Mr. Zhao falls into this category, reusing his handle across multiple social media sites.

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

He also maintains a relatively empty yet bizarre Twitter profile.

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.

facebook



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.