Who is Mr Zheng?


intrusiontruth.wordpress.com/2018/07/30/who-is-mr-zheng

intrusiontruth July 30, 2018

Our story starts with a FireEye report: Poison Ivy – Assessing Damage and Extracting Intelligence. Although the report focuses on the Poison Ivy tool, which has been used by a number of groups, it specifically highlights a number of campaigns known to use it. One of those campaigns is the menuPass group, another name for APT10.

Zheng Yanbin

The report contains a number of e-mail addresses associated with domain names used by the APT10 actors. One of those e-mail addresses, zhengyanbin8@gmail.com, contains a name – Zheng Yanbin.

Zheng Yanbin is hard to identify from social media, but the e-mail address is associated with a number of other domains

- 100fanwen.com
- anpvrn.com
- architectisusa.com
- cmdnetview.com
- gostudyantivirus.com
- gostudymbaa.com
- have8000.com
- jimintokoy.com
- linuxforever.com
- linuxsofta.com
- myie12.com
- qt4study.com
- qtsofta.com
- radiorig.com
- redforlinux.com
- tomorrowforgood.com
- ubuntusofta.com
- workerisgood.com
- woyaofanwen.com

Many of these domains are associated with addresses in Guangdong, China. A number also feature in commercial threat intelligence reporting, further confirming Zheng Yanbin's long term connection with APT10. The cmdnewview[.]com domain referenced in our previous

article was key evidence used by Palo Alto Networks to link old APT10 activity to the Cloud Hopper campaign.

This evidence indicates that Zheng Yanbin may be located in Guandong, although social media accounts identified using the same zhengyanbin8 username, seem to point to an individual in Shandong. It is not yet clear whether the zhengyanbin8 in Shandong is the same individual as the APT10 connected hacker.

A Zhulong blog linked to the same ‘zhengyanbin8’ username

In summary, an individual using the name Zheng Yanbin was certainly associated with APT10 and was involved in purchasing or managing C2 infrastructure used by the group.