intrusiontruth.wordpress.com /2022/07/24/chinese-apts-interlinked-networks-and-side-hustles/

# Chinese APTs: Interlinked networks and side hustles

intrusiontruth ⁝ ⁝ 7/24/2022

As FireEye pointed out on their APT41 overview, there is a high degree of malware and certificate overlaps across Chinese APTs but two in particular stand out as almost identical in their use of malware code – 41 and 17.

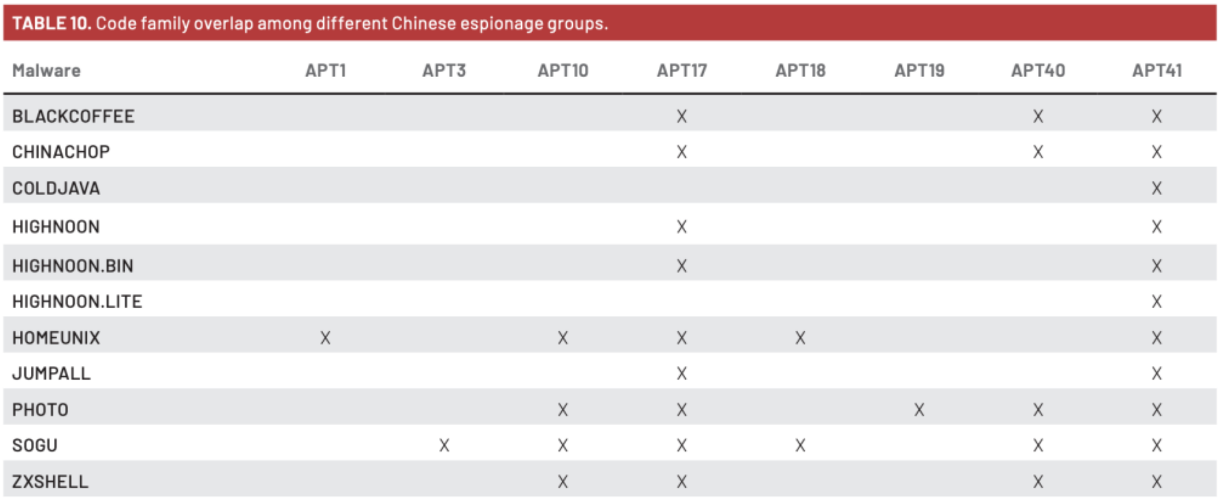


**TABLE 10.** Code family overlap among different Chinese espionage groups.

| Malware | APT1 | APT3 | APT10 | APT17 | APT18 | APT19 | APT40 | APT41 |
|---|---|---|---|---|---|---|---|---|
| BLACKCOFFEE | | | | X | | | X | X |
| CHINACHOP | | | | X | | | X | X |
| COLDJAVA | | | | | | | | X |
| HIGHNOON | | | | X | | | | X |
| HIGHNOON.BIN | | | | X | | | | X |
| HIGHNOON.LITE | | | | | | | | X |
| HOMEUNIX | X | | X | X | X | | | X |
| JUMPALL | | | | X | | | | X |
| PHOTO | | | X | X | | X | X | X |
| SOGU | | X | X | X | X | | X | X |
| ZXSHELL | | | X | X | | | X | X |

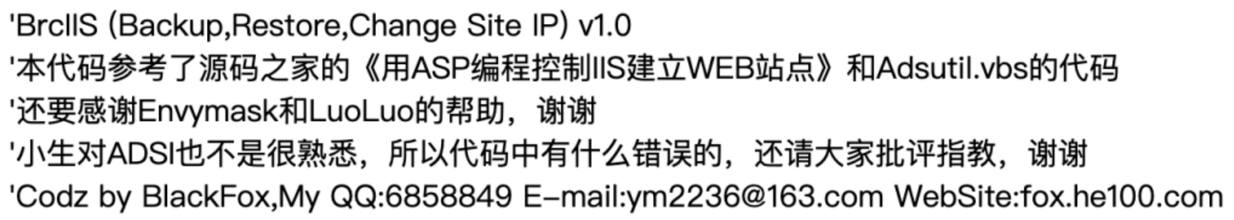
Remember Mr. Zeng Xiaoyong (aka envymask)? As readers will know, we named Zeng as a member of APT17 back in July of 2019. We evidenced his connections to the Chinese hacker group ph4nt0m, his birth place of Sichuan and his university of Nanjing Science and Engineering, where he met and later worked with MSS Officer of the Jinan SSD – Guo Lin. And it appears Zeng Xiaoyong has connections that go even further…

## BlackCoffee

Mr. Zeng is credited with creating a specific exploit of the public vulnerability MS08-067. This is associated with the ZoxPRC which evolved into BLACKCOFFEE malware, a hallmark of APT17 and Zeng specifically. APT41 are using this same malware in their operations. This specific sharing of malware exploits talks to the increasing overlap and coordination of APT groups within China.

## EnvyMask and Blackfox

Further digging has also revealed a history between Blackfox and Envymask on a number of hacker forums including CSDN and Github, where Blackfox promotes his ‘codz’ and expresses his gratitude to Envymask and another hacker known only as LuoLuo for their help.



```
'BrcIIS (Backup,Restore,Change Site IP) v1.0
'本代码参考了源码之家的《用ASP编程控制IIS建立WEB站点》和Adsutil.vbs的代码
'还要感谢Envymask和LuoLuo的帮助，谢谢
'小生对ADSI也不是很熟悉，所以代码中有什么错误的，还请大家批评指教，谢谢
'Codz by BlackFox,My QQ:6858849 E-mail:ym2236@163.com WebSite:fox.he100.com
```

Blackfox and envymask's relationship appears to be quite a deep one – they maintain direct contact and Blackfox credits envymask for his guidance and expertise in creating malware exploits. It additionally highlights the overlap between envymask (of APT17 fame), and Blackfox (of APT41 fame) which could go some way in explaining the overlap in malware tools being cited back to APT groups emanating from China and the trouble industry have of grouping APTs via their use of TTPs alone.

## ShadowPad

This backdoor RAT, reported by Kaspersky in 2017, was used to facilitate a supply chain attack and is commonly attributed to China. It is considered to be an evolution of PlugX, both of which originated from China and are used by Chinese APTs (APT41 in particular).

## PlugX and WHG

AlienVault Labs theorized that "WHG" was the developer of PlugX. And in 2012, Dunham and Melnick wrote about a connection between WHG and Tan Dailin. Tan (under Wicked Rose) credits WHG (aka "fig") as one of the developers of the GinWui rootkit which links back to the Network Crack Program Hacker group (of which Tan founded).

WHG is known to be the user of QQ 312016, which displays the username Zhao Jibin (赵纪斌). QQ 312016 belongs to another small QQ group (39771264) with just 14 members. A tight-knit circle of like-minded individuals? Of note are 3 other members: Jiang Lizhi, Zhang Hoaran and Tan Dailin.

Remember when we mentioned Lu Jian's membership in a group titled Chinese Communist Party Ministry of Finance (QQ 3391434)? We stated that the owner of this group was QQ 312016 – with the display handle 'whg'.

It further highlights the deep interconnectivity and social web these Chinese hackers maintain. But to what degree are the Chinese hacker's interactions social, or are their skills and experience directed, coordinated and developed by higher echelons within the CCP?

## Cyber Arrests

We did some digging into Zhao Jibin. Once again, he has links back to Sichuan, having attended Xihua university.

We also discovered that there were a number of arrests during Xi's crackdown of hackers within China in 2015. Notably, an office in Jinan associated with APT17 activity was raided by the local Public Security Bureau. A number of Chinese hackers were arrested. Amongst them was Withered Rose (aka Tan Dailin) Zhao Jibin (aka whg) and Liu Jian (aka Cowardly Sheep 懦羊).

The hackers were getting too big for their boots. Were the arrests a smokescreen? Or were they used to co-opt them into working for the MSS? Either way, it didn't stop them continuing to support APT17 and 41 operations.

## Conclusion

Sichuan province is fast becoming a known hot spot for hacking.

We believe that rather than APT41 being defined as a group or intrusion set, APT41 is perhaps better described as an interlinked network of Chinese cyber actors sharing malware, expertise and connections. The actors appear have a high degree of autonomy, which explains the degree of malware and certificate overlaps between APT groups emanating from China, and supports the concept of the contractor model. Autonomous cyber criminals 'bid' for state resource in exchange for top-level cover and a blind-eye is given to their criminal activities outside of the 9-6-6 structure, and if their targets are outside the Chinese mainland. Hustling on the side by using state-sponsored tools for their own profit makes us wonder whether the MSS truly have control over the contractors they work with.

According to Chengdu 404 in an interview, *'They wanted to make a contribution to their home town'*. Well, they have certainly done that. They have put Chengdu on the map, not least for China cyber watchers.

We started this article series with reference to a Times article focusing on Tan Dailin and his fellow hackers (formally known as the NCPH). The article ended with a quote from one of the hackers (known only as Fisherman): "*Real hackers are not doing it for a name or money. The real hackers keep their heads down, find network loopholes, write killer programmes and live off social security*". An interesting moral high ground to take. We wonder where it all went wrong.