The old school hackers behind APT41

intrusiontruth ⋮⋮ 7/21/2022

In an FBI indictment released in 2020, it reported five hackers with substantiated links to APT41: all criminal hackers based in Chengdu, Sichuan province. Seems Chengdu is getting somewhat of a hacker reputation.

Let's start with arguably the most notorious and well known of these five hackers: Tan Dailin.

Tan Dailin (谭戴林)

Quite a lot if information is already out there on Tan. We know he was talent spotted at Sichuan university for his hacking techniques and was subsequently trained by the People's Liberation Army (PLA – 中国人民解放军).

Tan was a founding member of the Network Crack Program Hacker Group (NCPH), going by the hacker name Wicked Rose. NCPH was a hacker group based out of Zigong, Sichuan with fellow members being current or former students of Sichuan University of Science and Engineering. The NCPH group gained notoriety by carrying out a number of attacks against the Department of Defence in 2006 using the GinWui rootkit, authored by Wicked Rose and another hacker – WHG. Wicked Rose announced in a blog post that the group were paid for their work, but the group's sponsor was not. We can take an educated guess as to Wicked Rose's sponsor … It begins with P and ends with A.

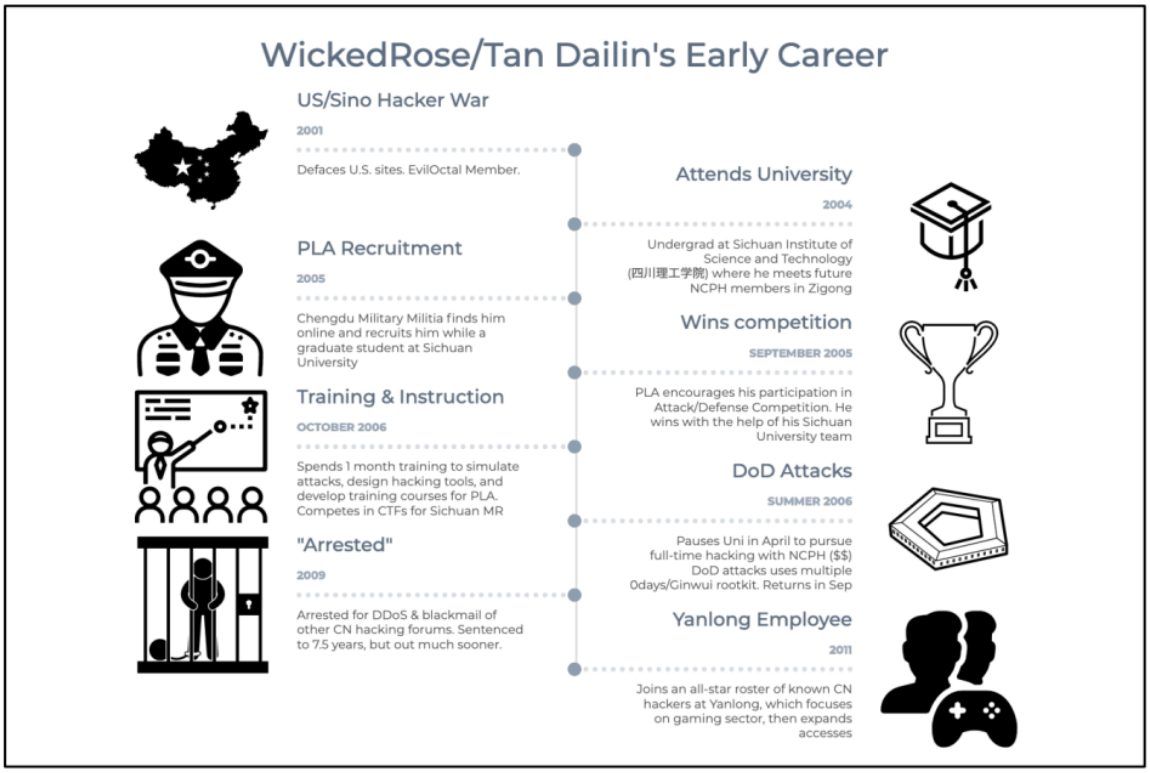

Figure 5. A timeline of Tan Dailin/WickedRose's early career and evolution from patriotic hacker to PLA operator and trainer, criminal operator, gaming firms, MSS contractor, and eventually cybersecurity firm owner.

Credit: Adam Kozy's research

Given the plethora of information Tan has disclosed online, he is a hacker who seems to enjoy the limelight. In 2012, he was the subject of an article by KrebsOnSecurity which sought to understand why a Chinese hacker (Tan) was the founder of a Chinese antivirus software (Anvisoft) purporting to be based in Fremont, USA. A domain look-up revealed that Anvisoft was in fact registered to the high-tech zone of Chengdu using the email linked to Tan's hacker handle wthrose(at)gmail.com and registered using the name tandailin. Five years later, a reporter for Times magazine conducted an interview with Tan noting he was '*lauded in China for his triumphs in military-sponsored hacking competitions and was unlikely to have problems with local law enforcement*'. A man with many connections it seems. Invincible and untouchable, or noisy and dispensable? A fine line to walk.

玫瑰 黑客 (MeiGui HeiKe) “Rose Hacker”
QQ number is 5372453 *www.mghacker.com*

QQ 903063678

Delving into the many Chinese leaked databases, we came across another QQ: 903063678, which from 2011 held the display name 戴林 (Dailin) as well as the handle ‘BlackWolf’.

However, the name Dailin linked to a QQ account isn’t much to go off, so we sought to validate our thinking. The identifier linked to this account was used to register a domain: ‘bat.mg’.

Registration information from this links to someone called ‘Daniel Tan’ in Chengdu, with the number 8613228166666. This number was also used to register ‘huianquan.net’, with details of the registration showing as ‘tandailin’ alongside an associated contact email: tandailin@163.com.

We are confident QQ 903063678 is Tan Dailin. It uses his alias (BlackWolf), and we have an associated number and email. We will see where this goes later on in the series.

Zhang Haoran (张浩然)

Zhang (37 years old, using alias Evilc0de) was named alongside Tan Dailin in the indictment for APT41. He appears to keep a much lower profile than his APT41 colleague. Nevertheless, he is deeply involved in intrusion activity having jointly participated in the conspiracy to target the video gaming industry.

Chengdu Huidong Science and Technology Company (成都慧东科技有限公司)

A technology company based in Chengdu with little internet presence and links to an indicted Chinese hacker. Seems like a classic front company to us. In 2006, Chengdu Huidong Science and Technology

Company (成都慧东科技有限公司) stated it had two stakeholders, each with a 50% stake. These were the CEO (Zhang Haoran) and a Supervisor (Zhang Chengwei).

So who is Zhang Chengwei? Clearly he knows Zhang Haoran well enough to go into business with him, and close enough to work with Zhang to develop cover companies for APT work.

Zhang Chengwei (张城玮)

There are a number of Zhang Chengwei's using QQ. However, one in particular caught our eye. QQ account 878792. This account is also a member of several groups which overlap with other indicted APT41 actors, including Tan Dailin. Furthermore, the username associated with the account is 'b1ackn1ve'.

Another 'black' prefix, aligning with Tan Dailin's use of BlackWolf. Eager readers will note we commented on matching pseudonyms in our previous article series on APT40. Could 'black' be indicative of a systemic pattern for APT41 hackers?

Blackn1ve has also appeared on our radar before; in a TLP:White advisory released in September 2020. This noted the b1ackn1ve@gmail.com email as an indicator of compromise, having been used for a APT41 spearphishing campaign.

So Zhang Chengwei is not only involved with APT41 activity by creating cover companies with Zhang Haoran but his hacker handle associated with his QQ account has been used in an APT41 spearphishing campaign against international victims.

Summary

The typical model of a front company to hide APT activity is a tried and tested one which APT41 are continuing to prove. The prefix 'Black' as a hacker handle might link APT41 actors. Furthermore, shared QQ groups support the social interconnectivity of these criminal actors and they are not shy to 'boast' about their connections to the state to support their activity. All have links back to Sichuan. Our next article starts there – in a city we now know very well. Home to Lonely Lantern and APT41: Chengdu.