# Chengdu 404

intrusiontruth ⋮⋮ 7/22/2022

In our last article, we highlighted the social links between APT41 actors, focusing on two of the five APT41 members: Tan Dailin and Zhang Haoran. Tan and Zhang, along with their other 3 conspirators (more on them tomorrow) worked for a company based in Chengdu's high-tech zone called Chengdu Si Lingsi (404) Network Technology Company Ltd. (成都市肆零肆网络科技有限公司). Established in 2014, it is better known colloquially as Chengdu 404.

404 is, as we all know, an error code when a browser cannot connect to a server. The founders claim they wanted to remain hidden and let their work speak. Doesn't appear to have worked out very well for them…


## Umisen.net

Residing at the domain umisen.net (now ironically no longer available), Chengdu 404 is one of the first front companies we have come across to have a working, multi-functioning website. 404 held a corporate VPN, presumably to facilitate their international hacking and provide access across the firewall. We also

found that Chengdu 404 hosted a log in portal sitting behind the open webpage, with a somewhat cryptic adage.

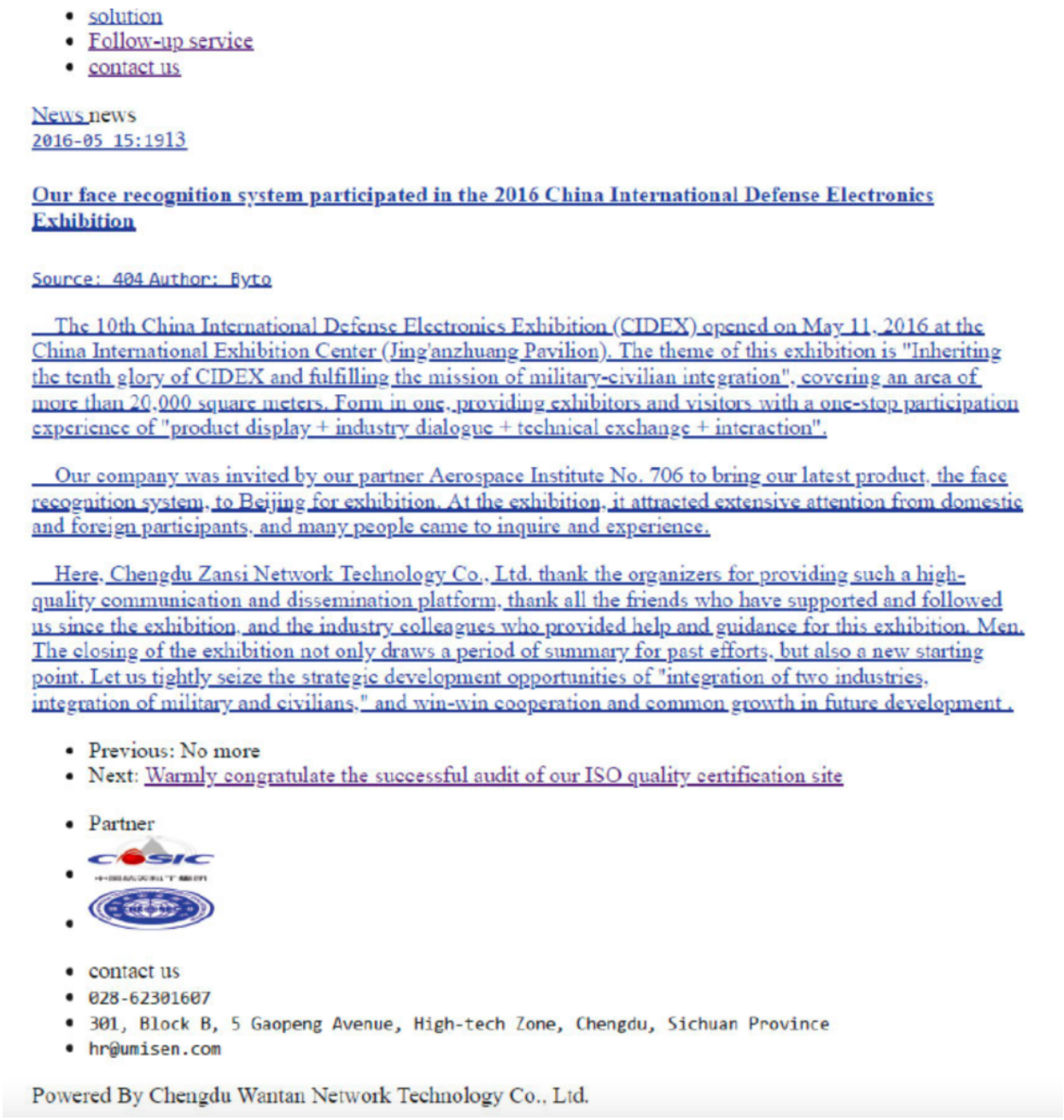

Their website was quite slick. The 'About Us' page stated the company was an emerging start-up comprising of white-hat hackers offering penetration testing to clients. A useful cover to facilitate company legitimacy and simultaneous access to other's IP.


As of 2016, 404's pages are full of positive boasts. One news article talks of a new facial recognition software that Chengdu 404 created and subsequently demonstrated at the Aerospace Institute in Beijing. Curiously, there is no further mention of this technology or its success after this date.

Facial recognition technology seems at odds with a company known for their work as 'white hat' hackers and experience in penetration and network security.

What *is* coincidental is that a Japanese company (NEC) had received wide recognition for their technology being a world leader in facial recognition, with similar descriptions to what Chengdu 404 describe theirs to be – a year earlier.

In January 2020, NEC admitted that they had had their data breached. The timing of this intrusion breach? 2016.



- solution
- Follow-up service
- contact us

News news
2016-05 15:1913

**Our face recognition system participated in the 2016 China International Defense Electronics Exhibition**

Source: 404 Author: Byto

The 10th China International Defense Electronics Exhibition (CIDEX) opened on May 11, 2016 at the China International Exhibition Center (Jing'anzhuang Pavilion). The theme of this exhibition is "Inheriting the tenth glory of CIDEX and fulfilling the mission of military-civilian integration", covering an area of more than 20,000 square meters. Form in one, providing exhibitors and visitors with a one-stop participation experience of "product display + industry dialogue + technical exchange + interaction".

Our company was invited by our partner Aerospace Institute No. 706 to bring our latest product, the face recognition system, to Beijing for exhibition. At the exhibition, it attracted extensive attention from domestic and foreign participants, and many people came to inquire and experience.

Here, Chengdu Zansi Network Technology Co., Ltd. thank the organizers for providing such a high-quality communication and dissemination platform, thank all the friends who have supported and followed us since the exhibition, and the industry colleagues who provided help and guidance for this exhibition. Men. The closing of the exhibition not only draws a period of summary for past efforts, but also a new starting point. Let us tightly seize the strategic development opportunities of "integration of two industries, integration of military and civilians," and win-win cooperation and common growth in future development.

- Previous: No more
- Next: Warmly congratulate the successful audit of our ISO quality certification site

- Partner
-
-

- contact us
- 028-62301607
- 301, Block B, 5 Gaopeng Avenue, High-tech Zone, Chengdu, Sichuan Province
- hr@umisen.com

Powered By Chengdu Wantan Network Technology Co., Ltd.

Ironic that the ethos of white hat hackers 'set out to right the wrongs of black hat hackers and chase APTs is the polar opposite of their real activities: APT41 conducting ransomware attacks and stealing IP using front company infrastructure.

## C0hb1rd

**c0hb1rd**

c0hb1rd

Follow

Code wins arguments.

**9** followers · **10** following

When you search Chengdu 404 on Google, an interesting hit reveals an individual known as c0hl1rd.

c0hb1rd的个人页面- 成都市肆零肆网络科技有限公司安全研发 ...

https://shixian.com › ...

Translate this page

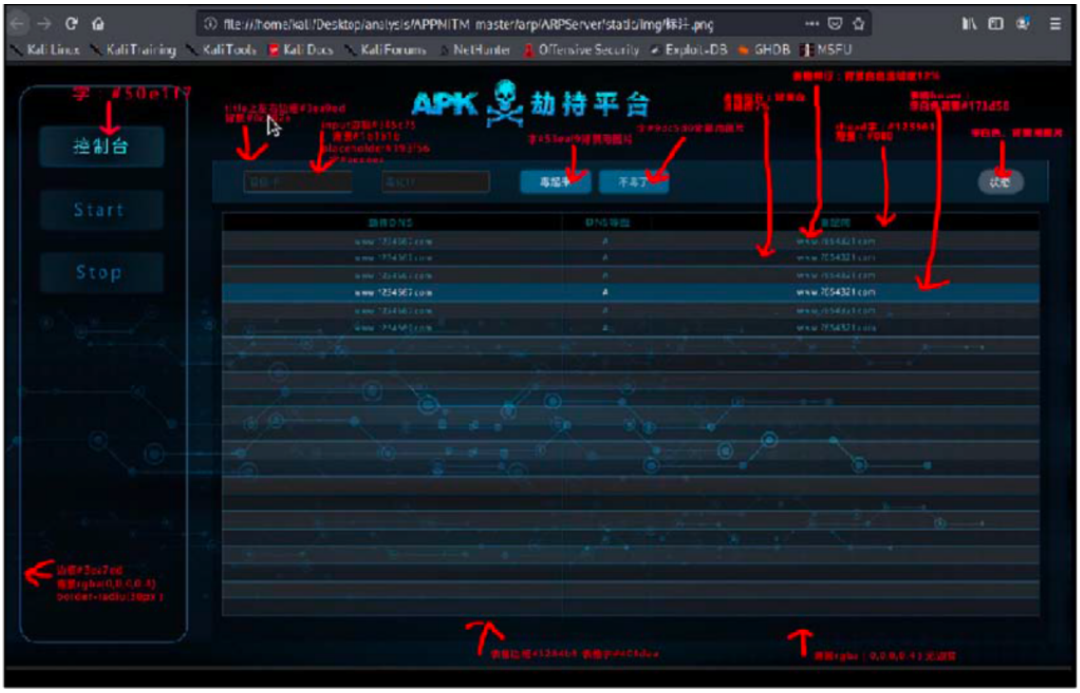
技术顾问 · 兼职需求 · 发现项目 · 发布项目 · 微信登录 · 微博登录 · GitHub登录. ×. 分享到微博. 分享一个互联网产品孵化社区：实现https://shixian.com. 分享 关闭.

This leads to a profile held on GitHub. The GitHub page does not appear to be active but does contain interesting posts from 2016, specifically referencing umisen networks.

These include a collection of shell scripts automating command line tasks. These scripts allow c0hb1rd to access an internet-facing Linux server using a root account in the subdomain 'root@tz.umisen.net' and remotely download/copy files to his local device.

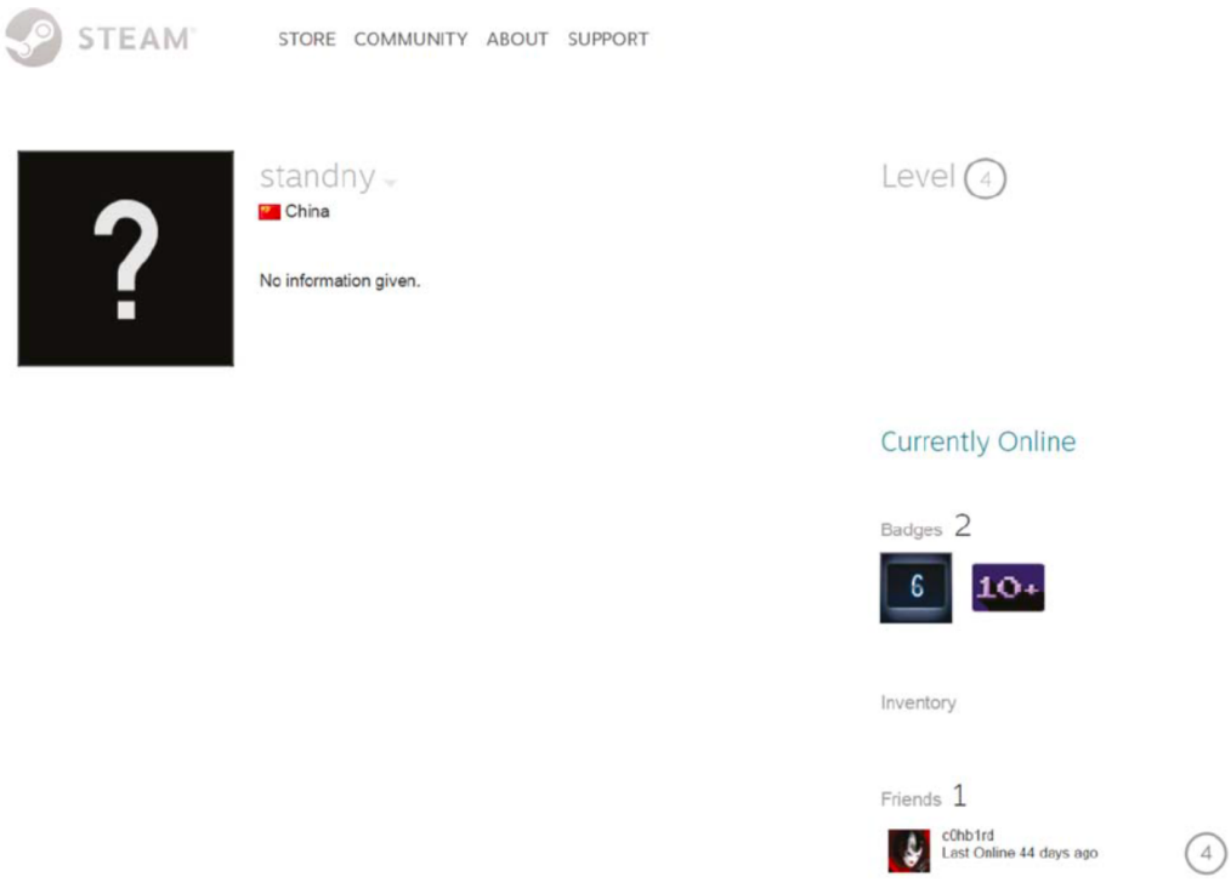
Furthermore, another repository is uploaded on c0hb1rd's profile referring to an APKMITM (man in the middle) tool. This targets the interception of Android phones with ARP spoofing, injecting an Android application (hence the APK annotation). The application does DNS redirecting to the umisen domain at port 8080.

This could be legitimate activity (evidence of online hacking challenges) but our sense is this is more nefarious – the skull and crossbones being just one indicator… The direct association with Chengdu 404 and c0hb1rd's tools redirecting traffic and developing remote log in access also adds to our suspicions.




Hints to c0hb1rd's identity suggest he is one of China' prolific hackers (number 27 to be precise), appearing on China's 50 best hackers list on WeChall.net.

A profile with the c0hb1rd handle also appears on the gaming platform 'Steam'.  They say you can tell a lot about someone from the company they keep. Well c0hb1rd keeps some interesting, albeit sparse, company. Amongst his grand total of 7 friends is 'standny' – the hacker handle for Fu Qiang, an employee and founding member of Chengdu 404 and one of the five indicated by the US last year.




When you click on Standny's profile, it shows that he is based in China and his only friend is c0hb1rd. A highly personal, social connection, with a joint interest in gaming. Is c0hlbrd another APT41 member? Or could he be a junior associate, caught up in Chengdu 404 activity? This would at least explain c0hlbrd's ease to which he uploaded script openly to GitHub, his preference to automate shell scripts and use of annotations on the open web.

**A question to ponder:** Could c0hb1rd's MITM tool have been used in standny's prolific creation of apps given their friendship? Many of standny's apps have been removed from online download sites. However, a quick scroll of standny's Twitter highlights just some of these apps being promoted. We would put good money on these apps being unreliable and facilitating third party access.



## Local university links

Chengdu 404 has close links to both Sichuan University and Chengdu University of Information Technology by providing internships and teaching the next generation at these schools. A number of the indicated APT41 actors have attended Sichuan University (a university known to be linked to Chinese hacking campaigns as previously noted in 2012 through its links to the Lucky Cat campaign) and appear to have remained involved ever since, forming part of the alumni and donating under a Si Lingsi (404) scholarship.

Chengdu 404 promotes these engagements on their website. Qian Chuan (left) and Jiang Lizhi (right) are pictured in numerous talks and award ceremonies at the universities yet most photos seek to blur their names from the pictures. Too important to document? Or are they wanting to hide due to guilty knowledge?


Having a foothold in local universities is a clever way to ensure young, bright and best talent for government clients. A university recruitment pipeline into the MSS. It begs the question whether these universities knew about Chengdu 404's remit and the individuals they were engaging with, or whether this was a larger, more coordinated effort by seniors within the security and military sectors to lure in aspiring, unaware, and naïve graduates to support APT activity. As we documented on APT40, this is not a unique set up, with APT40 using Hainan University to support their activity.

## Summary

**Chengdu 404 is directly linked to APT41. Its website boasts of (read: APT41) achievements and work for military and government clientele.**

**Chengdu 404's foothold within local universities point to a larger drive by the MSS to recruit graduate students into its ranks using APT front companies – whether knowingly or unknowingly by the universities themselves.**

**Tomorrow, we focus on the remaining 3 indicated APT41 members. What will be uncover?**