Sichuan Silence Information Technology: Great Sounds are Often Inaudible

Natto Team :: 12/4/2024

For five long years, Sophos, a United Kingdom (UK)-based information security company, battled Chinese nation-state threat actors who lobbed "botnets, novel exploits, and bespoke malware" against the company's firewalls and other perimeter devices. Sophos described this battle in its October 2024 "Pacific Rim" report series. Many in the industry applauded Sophos for "being so forthcoming about attacks targeting their own products." Others were amazed how Sophos could strategize a "hacking back" campaign that deployed a kernel implant to threat actor-controlled devices so that Sophos researchers could monitor the adversary's activities and remotely collect logs and access files. Sophos, "with varying levels of confidence," attributed the hostile activity to Chinese threat groups - Volt Typhoon, APT31 and APT41/Winnti — that conducted "exploit research and development activity" from Chengdu, Sichuan Province. In particular, the report identified **Sichuan Silence Information Technology** and the **University of Electronic Science and Technology of China (UESTC)** as being involved in the threat campaigns.

Sichuan Silence Information Technology (四川无声信息技术)(Sichuan Silence) rings a bell to some of us because Meta (formerly Facebook), identified Sichuan Silence employees as having "technical links" to fake accounts used in a July 2021 Chinese influence operation abusing the Facebook platform. The Natto Team dug deeper into our research notes and found the name of Sichuan Silence in the i-SOON leak as well, just as Natto Thoughts previously found the name of Integrity Technology discussed there.1 Apparently , Sichuan Silence is a company in the same circle as i-SOON. From what we know of Sichuan Silence from the 2021 Facebook report, recent Sophos reports and the i-SOON leaks, the Natto Team believes Sichuan Silence deserves a close look.

Sichuan Silence was "Freed" from Being a Quasi State-Owned Company

Sichuan Silence, with close to 300 employees, is headquartered in Chengdu, Sichuan Province, with two subsidiaries – Beijing Silence and Chongqing Silence – and four operations centers in three provinces – Tibet, Guizhou, and Yunnan and the Northwest region. Sichuan Silence claims to "play an important role in providing technical support for relevant offices and bureaus of Cyberspace Administration of China (CAC), Ministry of Public Security (MPS), Ministry of State Security (MSS) and the Military," according to its website, which was apparently last updated in 2020.

The company's name came from the Tao Te Ching (道德经), a Chinese classic text and foundational work of Taoist philosophy, Sichuan Silence's founder, CEO and Chairman Huang Yong (黄勇) said in an interview with Chengdu Software Industry Association (CDSIA) in 2016. One quote from that text says, "great sounds are often inaudible; great forms are often shapeless (大音稀声,大象无行)." Huang explained, "Information security is a special industry field, unlike e-commerce platforms, which are often used and their existence can be felt at any time, …..it is more like a secret which cannot be declared but which is known from the heart. Therefore, we hope that Sichuan Silence is down-to-earth in the field of information security service field to pursue the ultimate technology, to provide customers with the ultimate service. … The best experience for users is not feeling our existence."

Sichuan Silence CEO Huang also portrayed the company as having "freed" itself from a state-linked parent company.

The company website and public business records in several Chinese business search databases show that Sichuan Silence was founded in Chengdu in July 2000. However, Huang indicated that Sichuan Silence formerly had "two identities" - **Chengdu Topsec Network Security Company (Chengdu Topsec)** and **Sichuan Silence Information Technology Company**. Before 2013, Sichuan Silence was part of Chengdu Topsec. Chengdu Topsec, in turn, was a subsidiary of Topsec Technology Group (Topsec, 天融信), one of the top network security companies that produced China's first indigenous firewalls. Topsec claims to be China's first cybersecurity company and is a listed public company and a so-called "people-managed enterprise" (民营企业) with close ties with the government. In February 2024, a public notice from Topsec indicated that 80 percent of the company's business revenue source was from the government, state institutions, and state-owned enterprises (SOEs) in the first half of 2023. As the Natto Team has noted, Topsec participates in projects related to China's military-civil fusion strategy.

Because of "differences in company development philosophy," Huang had a "tough" negotiation with parent company Topsec in 2013, "freed" Sichuan Silence from Topsec, and transformed the company from "a product salesman to a service provider," Huang said in the 2016 interview. "Based on technology as the core," Sichuan Silence aimed to become "experts to solve customers' problems and provide practical security service solutions," Huang continued. Since the 2013 split, Sichuan Silence had become one of the key information security enterprises in Chengdu, "reflecting the municipal government's recognition of the company's services in the field," Huang confirmed in the 2016 interview. It is likely that Sichuan Silence enjoyed rapid growth in those years because it had spun off from its "big brother" company and made its own path. Many aspiring entrepreneurs and skilled hackers would like to transfer their talents into profit and have control over their own businesses. However, the Sichuan Silence website lists several Chinese security agencies as clients, and material from the i-SOON leaks shows Sichuan Silence had a “secrecy credential” (see below), suggesting that it did not make such a clean break with the Chinese government.

Sichuan Silence’s Double Helix Research Institute: Winner of CTF Competitions

Sophos’ Pacific Rim reports concluded “with medium confidence” that a device owned by Sichuan Silence’s Double Helix Research Institute (双螺旋研究院, Double Helix) was somehow involved in the threat activities in 2020. Sophos assessed that a group of entities including Sichuan Silence were all contributing to the five-year Chinese campaign, which included identifying and finding and exploiting zero-day vulnerabilities and sabotaging hotfixes that could patch known vulnerabilities.

An examination of Sichuan Silence’s company website, last updated in 2020, shows that Double Helix “focuses on penetration testing as the main core” and on “browser front-end security, code auditing, vulnerability mining, and secure software development as the main research projects.” The Double Helix’s description seems to match the threat activities Sophos identified.

In fact, Double Helix has a rich history of participating in hacking competitions, particularly capture-the-flag (CTF) competitions, in China since at least 2014. Its team “Sichuan Silence PKAV team” was one of 12 top teams that qualified to compete in the international hacking competitions 0CTF and XCTF Shanghai in 2016 and won the first place in total score for the Asian region and the world number 1 in the Web challenge. 0CTF is organized by Shanghai Jiaotong University’s 0oops team while XCTF is a national league established by Tsinghua University’s Blue Lotus team.[2] Both are international competitions with participating teams from outside China. Both Shanghai Jiaotong University and Tsinghua University are among the top universities in China.

We learn more about Double Helix and the PKAV team from an undated promotional blurb on the Chinese business website TRCJN. Zhang Ruidong (张瑞冬), aka “Only_guest” or “onlyguest”, describes himself as the leader of the “Double Helix Attack and Defense Laboratory” and founder of the PKAV team, and “a self-taught young hacker who advocates freedom. A destroyer, rebuilder, and maker of the rules of the network world.” Only_guest lacked a college degree but was appointed as a cybersecurity expert by Sichuan University. A February 2023 interview described him as “one of the most influential white-hat hackers.” In 2017, Only_guest separated from Sichuan Silence and established NoSugar Information Technology (成都无糖信息技术有限公司, Chengdu NoSugar Tech, sometimes translated as Chengdu Wutang Information Technology Co., Ltd.) with members of the PKAV team. Chengdu NoSugar Tech claims to specialize in combating online fraud and cybercrime. Although Only_guest left Sichuan Silence and lured away some members of the Double Helix Research Institute, it seems that didn’t – at least initially – weaken the company’s presence as a provider of offensive cyber infrastructure or services, judging from the activity that Sophos’ Pacific Rim reports outlined.

Share

Sichuan Silence and i-SOON: Part of a Close Circle of China’s Infosec Business Ecosystem

The leaked documents of the Chinese information security company i-SOON in February 2024 depict the intricate relationships among Chinese information security companies and China’s public security and state security agencies, various other government bodies, and the military. Within this landscape, information security firms have cultivated their own ecosystem, navigating the complexities of engaging with diverse government entities and operating both collaboratively and independently. In some instances, these companies engaged in fierce competition, actively recruiting talent from one another, while in others, they collaborated to manipulate contract bidding processes. The relationship between Sichuan Silence and i-SOON is another example that demonstrates the complex dynamics among these information security firms.

In the leaked i-SOON documents, Sichuan Silence appeared in the chat between i-SOON’s CEO Wu Haibo, aka shutdown or shutd0wn, and the company’s chief operations officer, lengmo, on several occasions in 2020.

- When looking for a QQ (a Chinese social media platform) vulnerability, Shutdown and lengmo discussed whether Sichuan Silence could provide it. However, they found out Sichuan Silence did not have the vulnerability. Interestingly enough, the said QQ vulnerability was originally offered on a pay-per-use basis by Chengdu NoSugar Tech, the company that former Sichuan Silence star employee Only_guest founded.
- When discussing company pay scales, Shutd0wn mentioned that employees of Sichuan Silence seemed to have a much higher salary than others, so Sichuan Silence has had a higher employee retention rate compared with other companies.
- In another conversation, Shutdown and lengmo chatted about the feasibility of acquiring Sichuan Silence. Shutdown thought Sichuan Silence’s business credentials, such as the secrecy classification, might be worth

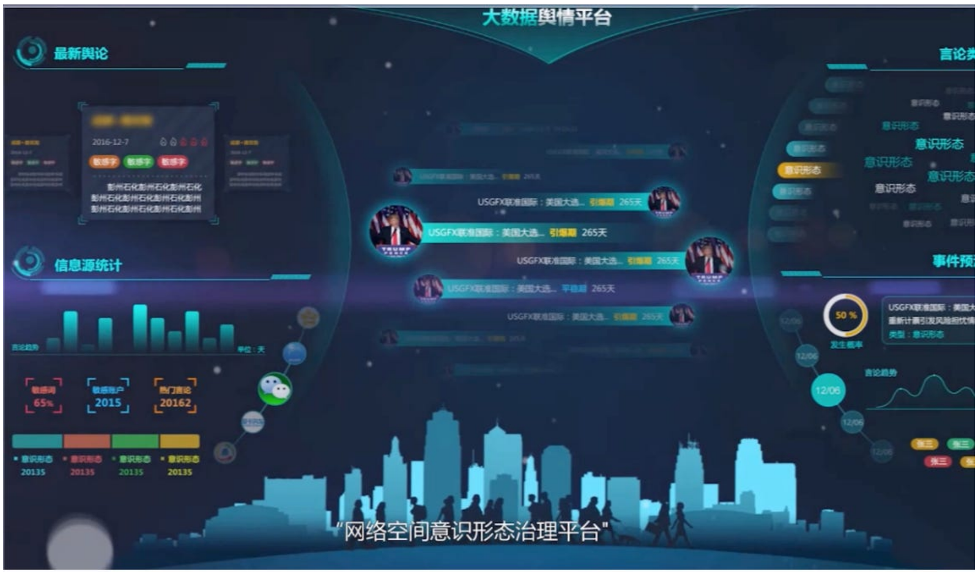
the acquisition. However, lengmo reminded Shutdown that Sichuan Silence seemed to have “quite a bit of debt” – RMB30 million (around US$4.4 million) and that it was “not worth it” to acquire the company with that debt.

i-SOON executives’ well-informed knowledge of Sichuan Silence’s business operations suggests they both belonged to a close circle of information security firms. In this case, both Sichuan Silence and i-SOON’s heavy presence in Chengdu likely helped keep the circle even closer.

Sichuan Silence: a Jack-of-All-Trades

As we previously mentioned, Meta has identified Sichuan Silence as being involved in a Chinese influence operation abusing the Facebook platform in July 2021.

From influence operations, to actively testing intrusion techniques, to abusing edge network devices and setting up footholds for targeted attacks, Sichuan Silence seems to have more to offer than we could imagine a relatively small information security company could do. Its website, last updated in 2020, shows the company had four core technical teams, including the Double Helix Research Institute, the Intelligence Center, the Big Data Research Institute, and the Software Development center. Whereas the Double Helix Research Institution specializes in vulnerability mining and exploit testing, the intelligence center is likely to provide information operation related services. As Sichuan Silence stated, its intelligence center offers “valuable real-time domestic and foreign information through multi-channel information collection and lead discovery, combined with professional foreign language translation services.” It also offers public opinion monitoring and analysis of “key individuals” through monitoring, tracking and reporting. Lastly, it offers assessments of public opinion development and online communication channels to effectively guide and handle public opinion and identify the information dissemination chain. A promotional video on the Sichuan Silence website introduced one of its big data public opinion platforms – “Cyberspace Ideology Governance Platform.” A screenshot from this video shows that the 2016 US election as one of the events monitored.



Sichuan Silence’s Cyberspace Ideology Government Platform monitors the 2016 US election. Source: Sichuan Silence official website,

Sichuan Silence’s wide range of business offerings resembles that of other Chinese information security firms, such as i-SOON, Chengdu 404, Integrity Tech and others we discussed on Natto Thoughts. These firms may have one or two flagship products, such as Integrity Tech’s cyber ranges and i-SOON’s TZ products – special investigation/reconnaissance products, but also provide a variety of products and services. This shows the fierce competition in China’s cybersecurity market. Many companies may not be able to survive with only one or two products or services, so companies must pivot their services in all possible directions. It also shows the cybersecurity market in China is still in the process of reaching its maturity level compared to the global cybersecurity market in general. As researcher Winnona DeSombre pointed out in her i-SOON leak analysis, “Western firms are unlikely to offer threat intelligence, information operation capabilities, reconnaissance capabilities, and offensive cyber capabilities at the same time.” Many in Western industry believe that specialization is the key to differentiating from others and taking market share. However, in China’s case, on the surface, it seems businesses are market-led, but the constant government policy changes influence the business market and lead to many cybersecurity companies becoming jacks-of-all-trades in order to compete.

2020 Sichuan Silence Goes Silent: Did it Shift to Classified Work?

As the Natto Team noticed, Sichuan Silence’s website appears to have fallen into disuse since about April 2020. The last news update on the site was on April 7th, 2020 with an article that promoted the company’s cyber range service –

an “attack and defense drill platform” (攻防演练平台). That was the month that Sophos’ Pacific Rim report identified a Sichuan Silence device. Since 2020, Chinese media also contain almost no public references to Sichuan Silence or to its founder, Huang Yong.

Indeed, Sichuan Silence appears to have fallen into crisis in 2020. As mentioned above, i-SOON executives discussed Sichuan Silence’s debt in September 2020 despite the fact it seemed the pay of Sichuan Silence employees was higher than that of i-SOON personnel. In August 2020 Sichuan Silence employees reported to a Sichuan provincial government agency that their company had not paid them for more than three months and had fallen behind on their social credit insurance and provident fund payments.

Nevertheless, the company resurfaced in fragmentary reports thereafter. In 2021, Meta reported on Sichuan Silence’s role in information operations. In November 2023 Sichuan Silence advertised in one hiring website for six positions, including software security researcher for Android devices, web security software testing engineer, data mining engineer and software engineer.

Why did they let their website fall into disuse but apparently remain active as the hiring ads showed? Could they have gone back into doing classified work for the Chinese government?

Overall, from what we have discovered, the operations of Sichuan Silence are similar to those of i-SOON and other similar Chinese hacker-for-hire companies. These companies face fierce competition. To succeed in business, they often have to adapt, such as making organizational adjustments or diversifying business offerings. Other than competing, they also work together – sharing tools and learning from each other. When these companies’ ultimate goal is profit, the Chinese government will have plenty of resources for their hacking campaigns as Natto Thoughts discussed in the piece “Front Company or Real Business in China’s Cyber Operations.”