How China’s Patriotic ‘Honkers’ Became the Nation’s Elite Cyberspies

wired.com/story/china-honkers-elite-cyber-spies/

By Kim Zetter July 18, 2025

In the summer of 2005, Tan Dailin was a 20-year-old grad student at Sichuan University of Science and Engineering when he came to the attention of the People’s Liberation Army of China.

Tan was part of a burgeoning hacker community known as the Honkers—teens and twentysomethings in late-’90s and early-’00s China who formed groups like the Green Army and Evil Octal and launched patriotic cyberattacks against Western targets they deemed disrespectful to China. The attacks were low-sophistication—mostly website defacements and denial-of-service operations targeting entities in the US, Taiwan, and Japan—but the Honkers advanced their skills over time, and Tan documented his escapades in blog posts. After publishing about hacking targets in Japan, the PLA came calling.

Tan and his university friends were encouraged to participate in a PLA-affiliated hacking contest and won first place. The PLA invited them to an intense, monthlong hacker training camp, and within weeks Tan and his friends were building hacking tools, studying network infiltration techniques, and conducting simulated attacks.

The subsequent timeline of events is unclear, but Tan, who went by the hacker handles Wicked Rose and Withered Rose, then launched his own hacking group—the Network Crack Program Hacker (NCPH). The group quickly gained notoriety for winning hacking contests and developing hacking tools. They created the GinWui rootkit, one of China's first homegrown remote-access backdoors and then, experts believe, used it and dozens of zero-day exploits they wrote in a series of "unprecedented" hacks against US companies and government entities over the spring and summer of 2006. They did this on behalf of the PLA, according to Adam Kozy, who tracked Tan and other Chinese hackers for years as a former FBI analyst who now heads the SinaCyber consulting firm, focused on China.

Tan revealed online at the time that he and his team were being paid about $250 a month for their hacking, though he didn't say who paid or what they hacked. The pay increased to $1,000 a month after their summer hacking spree, according to a 2007 report by former threat intelligence firm VeriSign iDefense.

At some point, Tan switched teams and began contracting for the Ministry of State Security (MSS), China's civilian intelligence agency, as part of its notorious hacking group known as APT 41. And in 2020, when Tan was 36, the US Justice Department announced indictments against him and other alleged APT 41 members for hacking more than 100 targets, including US government systems, health care organizations, and telecoms.

Tan's path to APT 41 isn't unique. He's just one of many former Honkers who began their careers as self-directed patriotic hackers before being absorbed by the state into its massive spying apparatus.

Not a lot has been written about the Honkers and their critical role in China's APT operations, outside of congressional testimony Kozy gave in 2022. But a new report, published this month by Eugenio Benincasa, senior cyberdefense researcher at the Center for Security Studies at ETH Zürich university in Switzerland, expands on Kozy's work to track the Honkers' early days and how this group of skilled youths became some of China's most prolific cyberspies.

"This is not just about [Honkers] creating a hacker culture that was implicitly aligned with national security goals," Benincasa says, "but also the personal relations they created [that] we still see reflected in the APTs today."

Early Days

The Honker community largely began when China joined the internet in 1994, and a network connecting universities and research centers across the country for knowledge-sharing put Chinese students online before the rest of the country. Like US hackers, the Honkers were self-taught tech enthusiasts who flocked to electronic bulletin boards (dial-up forums) to share programming and computer hacking tips. They soon formed groups like Xfocus, China

Eagle Union, and The Honker Union of China and came to be known as Red Hackers or Honkers, a name derived from the Mandarin word “hong,” for red, and “heike,” for dark visitor —the Chinese term for hacker.

The groups were self-governing with loosely formed hierarchies and even had codes of ethics shaped by influential members like Taiwanese hacker Lin Zhenglong (known by his handle “coolfire”). Lin believed hacking skills should be cultivated only to strengthen cyberdefenses—to learn the ways of hackers in order to thwart them—and wrote an influential hacking manual “to raise awareness about the importance of computer security, not to teach people how to crack passwords.”

There were no simulated environments for hackers to build their skills at the time, so Honkers often resorted to hacking real networks. Lin didn’t oppose this—hacking wasn’t illegal in China except against government, defense, or scientific research networks—but he published a set of ethical guidelines advising hackers to avoid government systems or causing permanent damage and to restore systems to their original condition after Honkers finished hacking them.

But these guidelines soon fell away, following a series of incidents involving foreign affronts to China. In 1998, a wave of violence in Indonesia broke out against ethnic Chinese there, and outraged Honker groups responded with coordinated website defacements and denial-of-service attacks against Indonesian government targets. The next year, after Taiwanese president Lee Teng-hui announced his Two-States Theory challenging the Communist Party’s One China doctrine, the Honkers defaced Taiwanese government sites with patriotic messages asserting the existence of a unified China.

In 2000, after participants at a conference in Japan denied facts around the Nanjing Massacre, in which an estimated 300,000 Chinese were killed during Japan’s 1930’s occupation of the city, Honkers circulated a list of more than 300 Japanese government and corporate sites, along with email addresses of Japanese officials, and prompted members to target them.

The so-called patriotic cyberwars gave the Honkers a common cause that forged an identity unique from Western hacking groups, which the Honkers had emulated until then. Where Western hackers were primarily motivated by curiosity, intellectual challenge, and bragging rights, the Honkers bonded over their common cause to help China “rise up.” In the words of a China Eagle Union pledge, the Honkers vowed “to put the interests of the Chinese nation above everything else.”

The patriotic wars put China’s Honkers on the map and inspired more to join them. Honker Union swelled to an estimated 80,000 members, Green Army to 3,000. Most were just enthusiasts and adventure seekers, but a subset stood out for leadership and hacking skills.

A particularly influential group among these, whom Benincasa calls the Red 40, would go on to found or join many of China's top cybersecurity and tech firms and become integral to the state's cyberspy machine.

There's no evidence that the government directed the patriotic hacking operations, says Benincasa, but their activity aligned with state interests, and they drew government attention. A retired People's Liberation Army rear admiral and former professor at the PLA National Defense University praised their patriotism. The public also appeared to support it. A report claimed that 84 percent of internet users in China favored the patriotic hacking.

But in April 2001, this began to change after a Chinese fighter jet clipped a US reconnaissance plane midair off the coast of Hainan and sparked an international incident. The collision killed the Chinese pilot and forced the US plane to land on Hainan, where the Chinese military seized the aircraft and held the crew for more than a week. The incident stoked nationalist sentiments among US and Chinese hackers alike, and both sides lobbed cyberattacks against the other country's systems.

The Chinese government grew concerned over its lack of control of the Honkers and feared they could become a liability and escalate tensions. The Chinese Communist Party's official newspaper likened the hacking to "web terrorism," and the head of the Internet Society of China issued a statement through China's official state media condemning it as well. The retired PLA rear admiral who previously praised the groups now warned they were a threat to international relations.

The Honkers got the message, but with their patriotic mission shelved, the groups now became less cohesive. There were leadership clashes and disagreements over direction and priorities—some wanted to turn professional and launch cybersecurity companies to defend China's systems against attack; others wanted to go rogue and sell malicious tools. The former left to join tech firms like Baidu, Alibaba, and Huawei or cybersecurity firms like Venustech and Topsec. Some became entrepreneurs and launched their own security firms, like NSFocus and Knownsec, which became leaders in vulnerability research and threat intelligence. Some, however, shifted to cybercrime. And others, like Tan, became contract hackers for the PLA and MSS or founded firms that served these operations.

Honker Recruitment

According to Benincasa, the PLA and MSS began hiring Honkers around 2003, but the recruitment became more structured and earnest following the 2006 hackings attributed to NCPH and Tan. The recruitment expanded during and after the 2008 Beijing Olympics and was likely helped in 2009 with the passage of China's Criminal Law Amendment VII, which criminalized unauthorized intrusions into any network as well as the distribution of hacking tools.

Hacker forums began to shutter, and some Honkers got arrested. Word spread that Tan was among them. According to Kozy, Tan faced seven and a half years in prison, though it's unclear whether he served any time. Kozy believes he cut a deal and began work for the MSS. In 2011, it appears he launched an antivirus firm named Anvisoft, which may have served as a front for his MSS work.

Former Honkers Zeng Xiaoyong (envymask) and Zhou Shuai (coldface) also became contractors for the PLA and MSS and worked on operations conducted by APT 41, APT 17, and APT 27, according to Benincasa. Some worked through shell companies, others worked through legitimate firms who acted as intermediaries to the intelligence services.

Topsec and Venustech were two firms alleged to have assisted these efforts. Topsec employed a number of former Honkers, including the founder of the Honker Union of China, and Topsec's founder once acknowledged in an interview that the PLA directed his company. In 2015, Topsec was linked to state-sponsored cyber operations, including the Anthem Insurance breach in the US.

Over the years, many tools used by China APT groups were built by Honkers, and the PLA and MSS mined them for vulnerability research and exploit development. In 1999, Huang Xin (glacier), a member of Green Army, released "Glacier," a remote-access trojan. The next year, he and Yang Yong (coolc) from XFocus released X-Scan, a tool to scan networks for vulnerabilities that is still used by hackers in China today. In 2003, two members of Honker Union released HTRAN, a tool to hide an attacker's location by rerouting their traffic through proxy computers, which has been used by China's APTs. Tan and fellow NCPH member Zhou Jibing (whg) are believed to have created the PlugX backdoor in 2008, which has been used by more than 10 Chinese APTs. According to Benincasa, Zhou developed it even further to produce ShadowPad, which has been used by APT 41 and others.

Over the years, leaks and US indictments against former Honkers have exposed their alleged post-Honker spy careers, as well as China's use of for-profit firms for state hacking operations. The latter include i-Soon and Integrity Tech, both launched by former Honkers.

Wu Haibo (shutdown), formerly of Green Army and 0x557, launched i-Soon in 2010. And last year, someone leaked internal i-Soon files and chat logs, exposing the company's espionage work on behalf of the MSS and MPS. In March this year, eight i-Soon employees and two MPS officers were indicted by the US for hacking operations that targeted US government agencies, Asian foreign ministries, dissidents, and media outlets.

Integrity Tech, founded in 2010 by former Green Army member Cai Jingjing (cbird), was sanctioned by the US this year over ties to global infrastructure hacks.

This year, the US also indicted former Green Army members Zhou and Wu for conducting state hacking operations and sanctioned Zhou over links to APT 27. In addition to engaging in state-sponsored hacking, he allegedly also ran a data-leak service selling some of the

stolen data to customers, including intelligence agencies.

This isn't unlike early-generation US hackers who also transitioned to become cybersecurity company founders and also got recruited by the National Security Agency and Central Intelligence Agency or hired by contractors to perform hacking operations for US operations. But unlike the US, China's whole-of-society intelligence authorities have compelled some Chinese citizens and companies to collaborate with the state in conducting espionage, Kozy notes.

"I think that China from the beginning just thought, 'We can co-opt [the Honkers] for state interests.'" Kozy says. "And … because a lot of these young guys had patriotic leanings to begin with, they were kind of pressed into service by saying, 'Hey you're going to be doing a lot of really good things for the country.' Also, many of them started to realize they could get rich doing it."