From Vegas to Chengdu

Hacking Contests, Bug Bounties, and China's Offensive Cyber Ecosystem

CYBERDEFENSE REPORT

From Vegas to Chengdu

Hacking Contests, Bug Bounties, and China's Offensive Cyber Ecosystem

Eugenio Benincasa

Zürich, June 2024
Center for Security Studies (CSS), ETH Zürich

CSS
ETH Zürich

ETH zürich

Available online at: https://css.ethz.ch/en/publications/risk-and-resilience-reports.html

Author: Eugenio Benincasa

ETH-CSS project management: Stefan Soesanto, Project Lead Cyberdefense; Andreas Wenger, Director of the CSS.

Editor: Stefan Soesanto
Layout and graphics: Miriam Dahinden-Ganzoni

DOI: 10.3929/ethz-b-000675181

Table of Contents

List of Figures, Tables, and Boxes

List of Acronyms

360 DSG	360 Digital Security Group
360 ESG	360 Enterprise Security Group
360 SRC	360 Security Response Center
API	Application Programming Interface
APT	Advanced Persistent Threat
ASPI	Australian Strategic Policy Institute
BCTF	Baidu CTF
CCP	Chinese Communist Party
CERT/CC	China Computer Emergency Response Team/Coordination Center
CIA	Central Intelligence Agency
CMU	Carnegie Mellon University
CNITSEC	China Information Technical Security Evaluation Center
CNNVD	China National Vulnerability Database of Information Security
CNVD	China National Vulnerability Database
CTF	Capture the Flag
CVD	Coordinated Vulnerability Disclosure
GDDP	Government Disclosure Decision Processes
GUF	Guangzhou University Fangban
ICS	Industrial Control Systems
ICT CAS	Chinese Academy of Sciences Institute of Computing Technology
IoT	Internet of Things
MAPP	Microsoft Active Protections Program
MCF	Military-Civil Fusion
MIIT	Ministry of Industry and Information Technology
MPS	Ministry of Public Security
MSRC	Microsoft Security Response Center
MSS	Ministry of State Security
NSA	National Security Agency
NVDB	Cybersecurity Threat and Vulnerability Information Sharing Platform
PLA	People's Liberation Army
PPP	Plaid Parliament of Pwning
RMSV	Regulations on the Management of Security Vulnerabilities in Network Products
SASTIND	State Administration of Science, Technology, and Industry for National Defense
SJTU	Shanghai Jiao Tong University
THU	Tsinghua University
TSU	Technical Support Unit
UCAS	University of the Chinese Academy of Sciences
USS	Ubiquitous Systems Security
VRP	Vulnerability Reward Program
ZHU	Zhejiang University

1 Introduction

The Chinese government has created an elaborate multifaceted "hack-for-hire" ecosystem that is unlike anything we have ever seen before. The system grants Chinese security agencies exclusive access to zero-day vulnerabilities (box 1) identified by China's top civilian hackers, and allows Beijing to subsequently outsource its espionage operations to private contractors. The author's understanding of the various facets of China's hack-for-hire ecosystem draws from prior research and sources, including:

- **U.S. Indictments (2014-2024)**[1]: Since 2014, the U.S. Department of Justice has been unveiling indictments against Chinese citizens engaged in malicious cyber activities, laying bare the inner workings and coordination of China's offensive cyber ecosystem, which is characterized by a web of relationships between China's intelligence agencies, private companies, and academia.
- **Intrusion Truth (2017-2023)**[2]: Since 2017, the anonymous group Intrusion Truth has exposed over 30 Chinese cyber operatives linked to six Advanced Persistent Threats (APTs). Predominantly based on open-source-information, Intrusion Truth revealed connections between China's IT sector, academia, and the nation's intelligence agencies.
- **Dakota Cary and Kristin Del Rosso's "Sleight of Hand" report (2023)**[3]**:** This report showed how China's military and intelligence agencies gain access to zero-day vulnerabilities discovered by private sector cybersecurity research teams. The report identified numerous Chinese companies that contribute feed vulnerabilities to China's intelligence apparatus. Based on the number of vulnerabilities submitted, the Chinese government categorizes these companies along three tiers.
- **i-SOON Analyses (2024):** In 2024, a data dump uploaded on GitHub revealed the inner workings of Chinese government contractor i-SOON. The leaked documents showed that i-SOON was extensively engaged in Chinese espionage activities. A subsequent report by French threat intelligence company Harfang named "A Comprehensive Analysis of i-SOON'S Commercial Offering,"[4] and Winona Bernsen's "Same same, but Different"[5] report for Margin Research, analyzed the i-SOON dump and provided significant operational insights into China's hack-for-hire system.

This CSS cyber defense report will explain how the Chinese offensive cyber ecosystem thrives through varying degrees of state involvement with civilian hackers. In this report, the term "civilian hacker" encompasses both Chinese students and professionals engaged in hacking competitions and bug bounty programs for non-malicious purposes and without the distinct aim of furthering state-aligned goals. Where applicable, the term "civilian hacker" is specified by using the terms "vulnerability researchers" or "civilian researcher."

Mandated by law to collaborate with Chinese government security agencies, the contributions of civilian hackers are most immediately observed through the identification and dissemination of zero-day vulnerabilities to government agencies. As of this writing, Chinese state actors are exploiting more zero-days in absolute numbers than any other country, as revealed by Google Mandiant's James Sadowski and Casey Charrier in their March 2023 write up "Move, Patch, Get Out the Way: 2022 Zero-Day Exploitation Continues at an Elevated Pace."[6] The impact of China's civilian research teams also extends beyond merely discovering vulnerabilities, fueling a less quantifiable yet robust and self-reinforcing offensive cyber ecosystem.

[1] Office of Public Affairs, U.S. Department of Justice, "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage," *Press Releases* (blog), November 27, 2017, https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations.

[2] Intrusion Truth, "Coming Soon…," WordPress, *Intrusion Truth* (blog), April 18, 2017, https://intrusiontruth.wordpress.com/2017/04/18/coming-soon/.

[3] Dakota Cary and Kristin Del Rosso, "Sleight of Hand: How China Weaponizes Software Vulnerabilities", Atlantic Council, September 6, 2023). https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/.

[4] Cyber Threat Research Team, "A COMPREHENSIVE ANALYSIS OF I-SOON'S COMMERCIAL OFFERING," *Harfanglab, Inside the Lab* (blog), January 3, 2024, https://harfanglab.io/en/insidethelab/isoon-leak-analysis/.

[5] Winnona Bernsen, "Same Same, but Different," *Margin Research* (blog), February 29, 2024, https://margin.re/2024/02/same-same-but-different/.

[6] James Sadowski and Casey Charrier, "Move, Patch, Get Out the Way: 2022 Zero-Day Exploitation Continues at an Elevated Pace," *Mandiant* (blog), March 20, 2023, https://www.mandiant.com/resources/blog/zero-days-exploited-2022.

China's civilian vulnerability research teams and labs have largely remained unexplored. Presently, there is a lack of comprehensive understanding about (1) their research focus, i.e. which ones are concentrating on specifically Western products, as well as their systems makeup and organizational structure; and (2) the functioning and relationships of China's broader offensive cyber ecosystem within which these entities thrive – this also encompasses Chinese technical universities and student hacking teams. To achieve this, this report takes a closer at the participation of leading Chinese hacking teams and vulnerability research laboratories in major international hacking competitions (DEFCON CTF, Pwn2Own, Tianfu Cup) and bug bounty programs (Apple, Google Android, Microsoft). These teams and laboratories include (a) professionals at major Chinese cybersecurity companies who conduct vulnerability research on largely U.S. software products, including Microsoft, Apple, Adobe, VMware, Google, and others. As well as (b) student teams from elite Chinese universities that hone their offensive cybersecurity skills by participating in Capture the Flag (CTF) contests.

Section 2 summarizes the main insights of this report. Section 3 provides an overview and historical context of what is publicly known about China's hack-for-hire system. It also illustrates the capabilities of Chinese civilian hackers, and how they are utilized for state objectives. In sections 4, 5, and 6, the report traces the history of the Chinese hacking teams that have participated at DEFCON CTF (2013-2023), Pwn2Own (2014-2017), and the Tianfu Cup (2018-2023). For each of the three sections, the report analyzes the team's performances and the impact they had on shaping China's offensive cybersecurity culture. Additionally, the report analyzes the competing teams, their areas of expertise, connections with academic institutions and corporate entities, and their involvement in military-civil fusion initiatives aimed at supporting state-sponsored offensive cyber operations. Section 7 dives into the contributions of Chinese researchers and companies to the bug bounty programs of Apple, Android (Google), and Microsoft, to identify China's leading civilian entities committed to finding vulnerabilities in these critical products. It will then examine Chinese bug bounty programs, their framework, and their comparative monetary incentives when juxtaposed with other international initiatives. Section 8 provides a concluding assessment and suggests avenues for future research.

Box 1: Key Definitions

Software Vulnerability

A security flaw, glitch, or weakness found in software code that could be exploited by an attacker.

Zero-Day Vulnerability

A zero-day vulnerability is a software flaw unknown to both the software vendor and the public. Since these vulnerabilities are undisclosed, and thus unpatched, they offer attackers a significant advantage. Discovering zero-days is challenging and demands substantial resources, but once found, they enable attackers to gain unauthorized access, navigate through a network, pilfer data, or compromise a system. It's comparable to having a master key that unlocks a hidden door without anyone noticing.

Hacking Competitions

Hacking competitions are events that incentivize participants to analyze the newest types of security threats, figure out how to assess them, and practice how to remediate such issues. In the otherwise discreet realm of cybersecurity, participation in hacking competitions is a practical way to publicly showcase computer skills on a national or global stage. The report examines two types of competitions: Capture the Flag (CTF) contests and exploit competitions. CTF competitions focus on a wide range of simulated cybersecurity challenges, while exploit competitions specifically center on identifying and exploiting vulnerabilities in real computer systems or software.

Bug Bounty Programs

A bug bounty program is an initiative in which an organization offers monetary rewards (bounties) to independent security researchers or ethical hackers who responsibly disclose and report vulnerabilities or bugs in their software, applications, or systems. Hacking contests, while technically a form of bug bounty program, will be conceptually distinguished in this report for analytical clarity. Both initiatives enable companies to tap into a global pool of researchers, identifying and fixing vulnerabilities before they can be exploited by malicious actors. Additionally, they provide a cost-effective alternative to hiring full-time security personnel, as independent researchers are incentivized to identify vulnerabilities on an as-needed basis.

1.1 Research Methodology

This report focuses on two areas to provide additional insight into the functioning of China's offensive cyber ecosystem: prominent hacking competitions and bug bounty programs.

Why these two areas?
Hacking competitions and bug bounty programs function quite similarly. Both provide security researchers with monetary reward for identifying and providing proof of an exploitable security vulnerability in a soft- or hardware product, which motivates participants to invest substantial time and effort in breaching a product (box 1). The complex challenges that the participants face require advanced knowledge and innovative problem-solving skills. Which in turn ensures that only those specialized will excel. The public visibility and fame gained from succeeding can open doors to lucrative job offers and collaborative projects with leading cybersecurity companies.

From an investigative point of view, prominent hacking competitions and bug bounty programs provide valuable insights into the company and university affiliations of individual Chinese researchers and teams, as well as their security research priorities. They also allow us to compare Chinese teams relative to others via (a) competition and bug bounty rankings over time, (b) monetary prizes secured, and (c) the volume of vulnerabilities submitted (sections 4 to 7). DEFCON CTF, Pwn2Own and the Tianfu Cup were specifically selected due to their prestige, high level of competitiveness, and extensive media coverage, making them ideal for gathering comprehensive insights into the Chinese civilian hacking landscape.

The information on hacking challenges is almost exclusively based on open-source data, including competition and vendor websites, news articles, social media posts, and online databases, such as CTFtime. CTFtime serves as a comprehensive archive for Capture the Flag (CTF) competitions (box 1), offering updated details on rankings, team nationality (when available), team and competition websites, and team membership details (usually identified by participants' nicknames rather than full names). Additionally, the report granted anonymity to a selected number of individuals who were willing to provide insights and share their experiences and competing in Chinese hacking competitions and the Chinese vulnerability reporting ecosystem.

Assigning a single nationality to each team that has participated in the DEFCON CTF is challenging due to some teams being multi-national. Additional difficulties are posed by frequent team name changes and high membership turnover. When Chinese teams started to compete at DEFCON CTF in 2013, they were composed almost exclusively of Chinese citizens from a limited number of Chinese universities. A few years later, they began to integrate into more international teams. To track this evolution, section 4 of the report begins its analysis in 2013, focusing on fully Chinese teams and then following their development within DEFCON CTF. The analysis highlights specific instances in which teams gradually integrated into international teams and identifies with whom they merged. By contrast, participation in exploit competitions such as Pwn2Own and the Tianfu Cup have remained homogenous over time, with Chinese teams rarely, if ever, mixing with participants from non-Chinese entities. This consistency facilitated their classification as fully Chinese teams throughout the analysis.

Section 7 analyzes three prominent bug bounty programs to measure the volume of vulnerability reports submitted by Chinese researchers and Chinese teams over the past decade. The three programs are: (1) Android (Google), (2) Microsoft, and (3) Apple. The three companies were chosen because, according to Google Mandiant's Sadowski and Charrier, the majority of zero-day vulnerabilities exploited over recent years were linked to products developed by Microsoft, Google, and Apple.[7] The i-SOON leaks[8] similarly indi-

[7] James Sadowski and Casey Charrier.

[8] Christian Shepherd, Cate Cadell, Ellen Nakashima, Joseph Menn and Aaron Schaffer, "Leaked Files from Chinese Firm Show Vast International Hacking Effort," *The Washington Post*, February 22, 2024, https://www.washingtonpost.com/world/2024/02/21/china-hacking-leak-documents-isoon/.

cate that i-SOON employees were able to exploit vulnerabilities in Microsoft, Google, and Apple products to conduct state-sponsored espionage campaigns.

Collated historical data for the Microsoft bug bounty program and Google Android's bug bounty program are freely accessible via the respective vendor's website. As of this writing, the Microsoft Security Response Center (MSRC) database is organized in a structured table format and is available for download in Excel format. It contains 7870 rows of entry, each representing a vulnerability report, covering the period of 2016 to the present.[9] Each row includes data on the reported vulnerability, the Microsoft service it affects, the researcher who reported it, along with their company and specific research unit affiliation, as well as the date of the report (day, month, and year).

Google Android's online database is organized in a structured table format, containing data on each reported vulnerability from 2016 to the present.[10] However, it offers more limited information compared to Microsoft's database. It includes only the researcher who reported the vulnerability along with their company and specific research unit affiliation, and the date of the report (month and year). The databases for Google's other products are even less detailed and often lack the name of vulnerability submitters. In contrast to Microsoft, the Android database was not available for download in Excel format as of this writing. The author created an Excel sheet, collating 3750 rows of entry. This process posed a few challenges because Google's database groups together multiple vulnerability reports, which had to be separated manually.

As of the time of writing, Apple's vulnerability reporting information included detailed information about each reported vulnerability, the researcher who reported it along with their company and specific research unit affiliation, as well as the date of the report (day, month, and year). However, gathering this information proved to be the most challenging. The information was not available for download in Excel format and was largely unstructured in the form of blog posts, making it very difficult to collect. As a workaround, Apple's vulnerability reporting information was extracted from an Excel database the Atlantic Council compiled for its 2022 report titled 'Dragon tails: Preserving international cybersecurity research'." The report's database covers pertinent Apple vulnerability reporting data from 2006 to January 2022. All in all, the database has a total of 6167 rows of entry.

The Microsoft and Android databases contain detailed information about individual researchers who contributed to their bug bounty programs globally, even though some submissions are sent in by researchers using pseudonyms that cannot always be linked back to a specific individual. In such cases, Chinese affiliations in the report could still be traced back by examining the company affiliations of the researchers. In contrast, Apple's Excel database includes neither researcher names nor their pseudonyms. It only contains data on the company and the specific research unit's affiliation associated with each vulnerability report. Additionally, some submissions in the Microsoft and Apple databases are entirely anonymous, as highlighted in section 7. Data cleaning was conducted across all three databases to remove double entries. Additionally, different spellings in company affiliations, particularly regarding teams and labs, were manually corrected by the author.

Despite these challenges, the data can be deemed robust, as most vulnerability reports are affiliated with a specific company or research unit. Leveraging this information, the dataset underwent a refinement process where a new column was introduced in each database. This column categorized vulnerability reports based on their origin, with a value of "1" denoting reports originating from China, and "2" representing reports from other countries. This binary categorization approach was implemented due to the inherent difficulty in accurately tracing each report to its specific country of origin across the global landscape. In a few uncertain cases, the author opted to assign them a value of "2".

[9] "Security Update Guide" (MSRC, n.d.), https://msrc.microsoft.com/update-guide/vulnerability.

[10] "Android Security Acknowledgements," *Android Security Acknowledgements* (blog), n.d., https://source.android.com/docs/security/overview/acknowledgements#feb-2018.

Subsequently, the author applied filters to the structured, clean data to isolate vulnerability reports originating from China as a whole, as well as from individual China-based research teams. The results of this analysis are depicted in various charts in this report that illustrate China's overall contributions to each bug bounty program compared to the rest of the world. The illustrations also break down the contributions by Chinese companies and research units. While the data from the three platforms was analyzed independently, each having its own subsection within section 7, collectively they offer a comprehensive view of China's civilian hacker landscape and their research focuses.

Overall, the collected data can be deemed reliable as the companies operating these bug bounty programs rely on such robust incentive schemes involving payouts and public acknowledgments to motivate hackers to report vulnerabilities. The rewards offered are often substantial. For instance, in 2018, Google awarded Guang Gong 112.000 USD, marking Google's largest bug bounty payout ever, for the submission of a remote exploit chain on a Google Pixel phone.[11] Similarly, in 2021, Microsoft granted 200.000 USD — then the largest bounty ever awarded by the company—to Qihoo 360 researchers who identified a vulnerability in the Hyper-V virtualization engine.[12]

[11] Avery Hartmans, "A Superstar Chinese Hacker Just Won $112,000 from Google, Its Largest Bug Bounty Ever," *Business Insider*, January 20, 2018, https://www.businessinsider.com/guang-gong-qihoo-360-google-pixel-2-hacking-bug-bounty-2018-1?r=US&IR=T.

[12] Catalin Cimpanu, "Microsoft Awarded $13.6 Million to Security Researchers in the Past 12 Months," *The Record*, August 7, 2021, https://therecord.media/microsoft-awarded-13-6-million-to-security-researchers-in-the-past-12-months.

2 Summary Insights

This section provides an overview of the main insights from various parts of the report addressing the two main open questions concerning China's most prominent civilian hacking teams:

1) **Research Focus, Systems Makeup, and Organizational Structure:** Insights 1 to 8 delve into the research focus of China's civilian hacking teams, including which ones are concentrating on specifically Western products, as well as their systems makeup and organizational structure.

2) **Functioning and Relationships within China's Offensive Cyber Ecosystem:** Insights 9 to 17 examine the functioning and relationships of China's broader offensive cyber ecosystem within which civilian hacking teams thrive, including elite universities and corporate affiliations.

The graph depicted in Figure 1 outlines the key components of China's offensive cyber ecosystem analyzed throughout this report and serves as a guide through the insights. **The numbers portrayed in the graph correspond to the summary insights below. Additionally, each insight directs to one or more sections of the report, which offer more detailed context and clarifications.**

From right to left, the "Cyber Operations" section of the model highlights the essence of China's hack-for-hire approach, according to which cyber operations are outsourced to private contractors acting as government proxies. Civilian hackers submit vulnerabilities, which are gathered by government security agencies and disseminated to provincial branches and contractors for cyber operations, as highlighted in the "Vulnerability Pipeline" component. Though this isn't necessarily the sole vulnerability ecosystem in China, it is likely the most prevalent one. In this ecosystem, the zero-day exploits leveraged in Chinese state-spon-

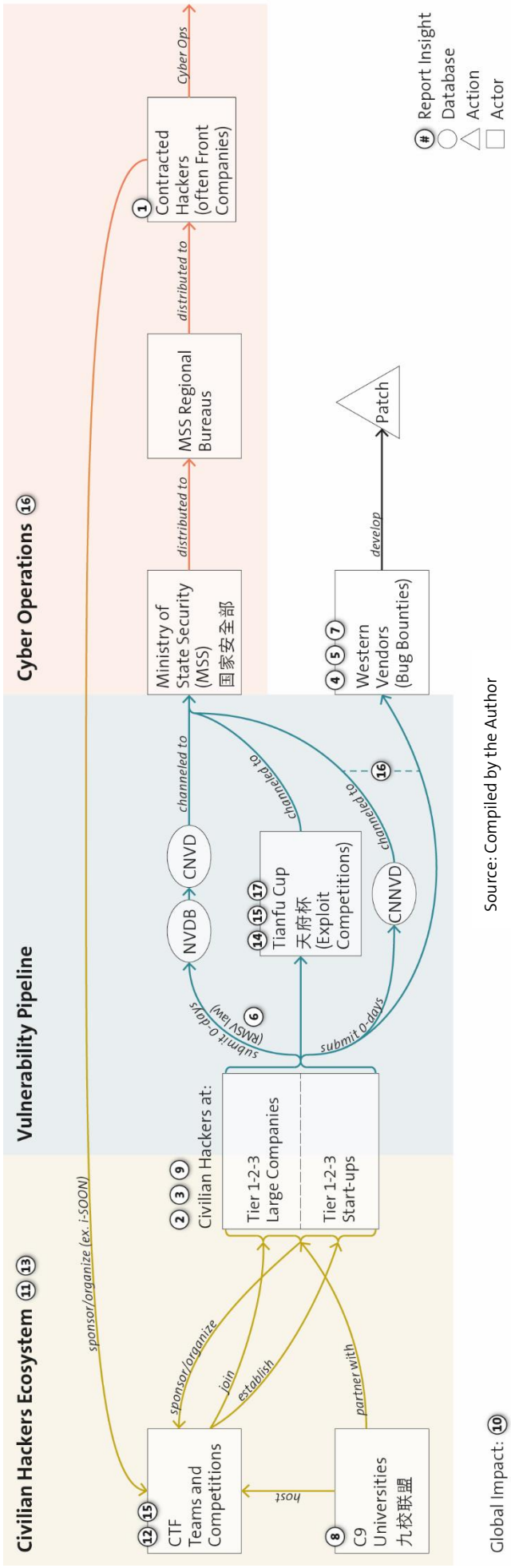


Figure 1: China's Offensive Cyber Ecosystem

Source: Compiled by the Author

sored cyber activities heavily rely on the skills of specialized researchers, which might often be unaware of their own contributions. The contribution of Chinese civilian hackers goes beyond just discovering vulnerabilities. Their broader impact on China's cyber ecosystem – such as establishing cybersecurity startups, hacking competitions, and contributing to creation of research labs – is arguably even more significant. This aspect is detailed in the "Civilian Hackers Ecosystem" part of graph, which is the primary focus of this report. The report further illustrates how this component interacts with the others, particularly the Vulnerability Pipeline, by examining the research focus of China's hacking teams to determine which specific Western products and systems they target.

Focus, Structure, and State Ties

1. Prominent, Contest-Winning Hackers and Lesser-known, Government-Contracted Hackers

Within China's offensive ecosystem, we can roughly divide Chinese hackers into two distinct groups. Prominent Chinese researchers who have distinguished themselves by winning or participating in prestigious exploit hacking competitions, such as Pwn2Own and the Tianfu Cup (sections 5 and 6). These individuals are often affiliated with level 1 Technical Support Units (TSU), which are Chinese companies that contribute the most vulnerabilities to China's premiere intelligence agency, the Ministry of State Security (MSS) (table 1 and section 3.3). These researchers have refined their abilities over time through incentives offered by international hacking competitions and bug bounty programs, with Western products and systems frequently being their most sought-after targets. There is usually no clear evidence that directly links them to Chinese state-sponsored cyber operations.

The second group encompasses non-public facing, government-contracted hackers on revealed by the i-SOON leaks, Intrusion Truth's revelations, and several U.S. indictments (section 3.1). These individuals have not participated in hacking competitions nor are they generally contributors to bug bounty programs. This could indicate a lower level of technical proficiency in targeting specifically Apple, Google (Android), and Microsoft products, but the evidentiary basis for this is rather thin.

The way China's hack-for-hire ecosystem essentially works is that the contracted hackers are executing cyber operations, while the elite researchers focus on vulnerability research and cybersecurity startup creation, which in turn helps the contracted hackers meet immediate mission requirements, and in the medium and long-run sustains China's broader offensive cyber ecosystem. This setup effectively leverages elite vulnerability researchers while also mitigating against professional or reputational risks, because of the researcher's non-direct involvement in malicious state-sponsored activities. The Pinduoduo case involving He Qidan (section 4.5) highlighted how China's elite hackers uphold elevated ethical standards. Renowned hacker He Qidan purportedly lost his job due to his refusal to participate in illicit activities for the company he was working for at the time (Pinduoduo), prompting key members of China's cybersecurity community to rally behind him, publicly condemning Pinduoduo's actions. It remains unclear to what extent this ethical mindset among China's elite hackers extends to national security issues.

2. Level 1 Technical Support Units participating in in Hacking Competitions and Bug Bounty Programs

More than half of the level 1 Technical Support Units (TSU), which are the private companies that contribute the most vulnerabilities to China's premiere intelligence agency, the Ministry of State Security (MSS), as identified by Cary and Del Rosso (table 1 and section 3.3), are also companies that play key organizational roles in the hacking competitions scrutinized in this report. These companies, such as NSFocus, TopSec, Huawei, VenusTech, and Qi An Xin, sponsor the Tianfu Cup (section 6), while others like JD and Tencent sponsor Chinese CTF competitions (section 4). The teams hosted within these companies are also successful competition performers and bug bounty contributors (ex. Qihoo 360, Tencent, Ant Group, Chaitin Tech, Sangfor, and DBAPP). Interestingly, for cyber MCF purposes the level 1 TSU's engagement with Beijing ranges from very close relationships, such as Qihoo

Table 1: Tier 1 CNNVD Technical Support Units

Tier 1

"新华三技术有限公司H3C www.h3c.com"	"烽台科技（北京）有限公司 FengTai Technology www.fengtaisec.com"	"深信服科技股份有限公司 Sangfor Information Services www.sangfor.com.cn"	"深圳市腾讯计算机系统有限公司Tencent www.tencent.com"	"杭州安恒信息技术股份有限公司 DBAPP Security (DAS Security) www.dbappsecurity.com.cn"	"北京华顺信安信息技术有限公司HuaShun XinAn www.huashunxinan.net"
"北京安天网络安全技术有限公司Antiy www.antiy.cn"	"北京微步在线科技有限公司 ThreatBook www.threatbook.com"	"三六零数字安全科技集团有限公司360 Digital Security www.360.net"	"奇安信网神信息技术（北京）股份有限公司Qi An Xin www.qianxin.com"	"北京华云安信息技术有限公司VulAI www.huaun.com"	"北京天融信网络安全技术有限公司TopSec www.topsec.com.cn"
"上海斗象信息科技有限公司TopHant www.tophant.com"	"杭州海康威视数字技术股份有限公司Hikvision www.hikvision.com"	"华为技术有限公司Huawei www.huawei.com"	"北京长亭科技有限公司 ChaiTin www.chaitin.cn"	"杭州迪普科技股份有限公司DP Tech www.dptech.com"	
"北京神州绿盟科技有限公司NSFocus www.nsfocus.com.cn"	"蚂蚁科技集团股份有限公司 Ant Group www.antgroup.com"	"北京启明星辰信息安全技术有限公司VenusTech www.venustech.com.cn"	"北京京东尚科信息技术有限公司JD (JingDong) www.wx.jdcloud.com"	"北京奇虎科技有限公司Qihoo (Beijing) www.360.cn"	

Source: Cary & Del Rosso (2023) Sleight of Hand, Appendix A, Atlantic Council

360 and Qi An Xin (sections 5.3 and 5.5), to more strained relationships with lesser integration, such as Tencent and the Ant Group (sections 5.4 and 6.3).

The absence of additional level 1 TSUs in the examined events and initiatives covered in this report, may stem from the company's internal policies that might be restricting their participation in non-China based hacking competitions and bug bounty programs. Another plausible explanation could be that some TSUs exclusively focus on Chinese soft- and hardware products rather than Western ones.

3. Different Organizational Structures

The number of research labs and associated teams vary from company to company, in both size, quantity, and research focus. For example, Qihoo 360 boasts over 19 teams (section 5.3 and Appendix A) while the Ant Group hosts nine (section 6.3). Tencent operates 7 to 10 labs (section 5.4 and Appendix B) while Cyber Kunlun has just one lab (section 6.4). In general, we can state that, the higher the number of teams and labs the larger the company, financial capital, human resources, and areas of specialization. Cybersecurity companies such as Qihoo tend to maintain several teams spanning various product lines and departments. Although specific team sizes are challenging to pinpoint, 360 Alpha and 360 Vulcan might each comprise over 40 members. Moreover, Qihoo teams have very different and distinct logos which might indicate a level of autonomy and individualism. By contrast, Tencent has far fewer teams that are organized within one unified department. The logos of Tencent's labs thus also follow a similar design, which reinforces the appearance of a sense of unity and collaboration among them.

4. Chinese Teams as Major Vulnerability Suppliers to Apple, Google Android, and Microsoft Bug Bounty Programs

Chinese prominent, contest-winning researchers have been major contributors to the bug bounty programs of Apple, Google Android, and Microsoft (section 7). From 2017 to 2023, Chinese researchers contributed 27% of all vulnerabilities submitted to these three bug bounty programs, while the rest of the world accounted for 59%. More specifically:

- **Google Android:** Between 2017 and 2020, China contributed more than 50% of the vulnerabilities reported, with the rest of the world accounting for 44%. From 2021 to 2023, China's contribution decreased to 35%, while the rest of the world's contribution increased to 65% (section 7.2).
- **Microsoft:** From 2017 to 2020, Chinese entities reported more than 25% of the vulnerabilities reported, while the rest of the world reported 50%. 23% of submissions were anonymous. Between 2021 and 2023, Chinese researchers reported 18% of the vulnerabilities, compared to 75% from the

rest of the world. Only 7% were reported anonymously (section 7.3).

- **Apple:** From 2017 to 2020, Chinese researchers reported approximately 15% of vulnerabilities, while the rest of the world reported 47%. 38% were submitted anonymously. From 2021 to January 2022, Chinese researchers reported 28% of vulnerabilities, compared to 38% from the rest of the world. 34% were reported anonymously (section 7.4).

5. Two Generations of Teams

The bug bounty submissions to Apple, Google Android, and Microsoft reveal a distinct division between two time periods: 2017-2020 and 2021-2023 (section 7). In the earlier period, Qihoo 360 and Tencent dominated submissions for Microsoft, Google Android, and Apple. By the end of 2023, Cyber Kunlun and Oppo Amber Security Lab emerged as the primary contributors for Microsoft and Google Android, with the Ant Lightyear Security Lab reaching the top position for Apple. Meanwhile, teams from Qihoo 360 and Tencent significantly reduced their contributions from 2021 onward. This shift likely occurred due to U.S. sanctions and researchers transitioning to other companies.

6. Limited Evidence of RMSV Law Impact on Vulnerability Submissions

In the report's analysis of vulnerability submissions to Apple, Google Android, and Microsoft, a couple of trends can be identified following the implementation of the 'Regulations on the Management of Network Product Security Vulnerabilities' RMSV, which was announced in 2020, and came into effect in 2021 (section 3.3).

- **Google Android:** Between 2017 and 2023, Chinese researchers consistently reported on average 19 vulnerabilities per month to Google Android's bug bounty program (section 7.2).
- **Microsoft:** During the period from 2017 to 2020, Chinese entities reported on average 18 vulnerabilities per month to Microsoft's bug bounty program. Between 2021 and 2023, that number rose to 22 (section 7.3).
- **Apple:** From 2017 to 2020, Chinese entities reported on average 6 vulnerabilities per month to Apple's bug bounty program. Between 2021 and January 2022, that number increased to 11 (section 7.4).

  While the RMSV may have created some deterrent effects, Chinese entities continue to submit vulnerabilities in substantial numbers. The extent to which this finding affects China's effectiveness model is unclear and is further explored in summary insight 16 on "Open Questions Regarding China's Model Effectiveness."

7. The Profound Impact of a handful Chinese researchers

The success of the Chinese teams is often credited to a small number of individuals (section 7). From 2017 to 2020, over 60% of vulnerabilities reported by Qihoo's 360 C0RE to Google Android were submitted by Mingjian Zhou, either individually or in collaboration with a few additional team members. Within 360 Alpha nearly all vulnerabilities were reported by Guang Gong, whereas in 360 IceSword, over half were reported by Chen Gengjia, either individually or in collaboration with other team members. Han Zinuo contributed to over 50% of vulnerabilities reported by 360 SRC to Google Android. And in the case of Qihoo's 360 Vulcan Yuki Chen was responsible for 68% of the team's submitted vulnerabilities to Microsoft.

Fluctuations in a team's contributions can often be traced back to a single individual transition between companies. This has been particularly true since 2020. For example, when Han Zinuo switched from 360 SRC to OPPO in 2020, submissions from 360 to Google Android decreased significantly, while OPPO saw a substantial increase, largely due to Han's contributions. Likewise, when Yuki Chen moved from 360 Vulcan to Cyber Kunlun in 2020, Microsoft witnessed a significant decrease in contributions from 360 Vulcan. Cyber Kunlun meanwhile experienced a remarkable surge, with Chen being responsible for 62% of the team's submissions to Microsoft. Sangfor experienced a significant boost when former 360 C0RE member Peng Zhiniang joined the company as a CTO in late 2020.

Following Peng's arrival, Sangfor's vulnerabilities contributions to Microsoft surged, and the company secured the third place in the Tianfu Cup 2023.

The migration of researchers to other Chinese firms (ex. Sangfor and OPPO), combined with the creation of new cyber security companies (ex. Cyber Kunlun), is likely leading to an expansion and diversification of China's offensive cyber capabilities. This underscores how China's model heavily depends on a small pool of high-level talent for vulnerability discovery.

8. Varied Levels of C9 University involvement in MCF and State-Sponsored Cyber Espionage

Some university departments that host teams participating in the DEFCON CTF have been (a) linked to Chinese state-sponsored cyber operations, (b) conducted vulnerability research with Chinese companies that have been linked to Chinese state-sponsored cyber operations, or (c) serve as fertile recruitment centers for Chinese security agencies (section 4).

- In 2018, Chinese state-linked network reconnaissance activities were linked to infrastructure owned by Tsinghua University (THU) (section 4.3). It is unknown whether any Blue Lotus team members were involved in these cyber espionage operations. However, THU has forged research partnerships with prominent Chinese cybersecurity firms, some of which have been either implicated in state-sponsored cyber espionage campaigns or have providing government agencies with zero-day vulnerabilities.
- Threat intelligence reports indicate strong linkages between Shanghai Jiao Tong University (SJTU) (section 4.4) and Chinese state-sponsored cyber espionage activities. SJTU's School of Information Security Engineering – which is home to the 0ops team – has been accused of providing direct support to PLA Unit 61398 (APT1). SJTU also operates the Higher-Ed Vulnerability Database, which gathers reports from researchers, professors, and students and forwards them to the Chinese Ministry of State Security.
- While Zhejiang University (ZHU) (section 4.5) does not appear to have any ties to specific Chinese malicious cyber campaigns, its School of Computer Science and Technology – which hosts the AAA team – was identified by Mandiant to be a source for recruiting individuals into the PLA's Unit 61398 (APT1).

Roles and Opportunities within China's Offensive Cyber Ecosystem

9. Chinese Teams at DEFCON CTF (2013-2023) and Pwn2Own (2014-2018)

Since the early 2010s, Chinese teams from select universities and companies have rapidly emerged as frontrunners in prestigious international hacking competitions, including DEFCON CTF and Pwn2Own. At DEFCON, Chinese teams consistently reached the finals from 2013 to 2023, posing a significant challenge to U.S. dominance (section 4.2). Similarly, Chinese winnings at Pwn2Own surged from securing 13% of the entire prize pool in 2014 to 79% in 2019 (section 5.2).

10. Chinese Hackers' Withdrawal from International Hacking Competitions Weakened Global Cybersecurity

The absence of Chinese hackers at Pwn2Own since 2018 has significantly altered the contest's landscape (section 5). Throughout 2022 and 2023, no participants attempted to breach iPhone and Google Pixel devices. This marked the end of a 15-year streak of targeting Apple products. The notable absence of Chinese hacking teams that specialized in targeting these devices explains this break far better than assuming that the iPhone and Pixel have become unbreachable. Concurrently, these vulnerabilities are highly likely evaluated by China's security agencies for potential use in cyber malicious operations. This illustrates that cybersecurity fragmentation and protectionist vulnerability policies significantly undermine global cybersecurity.

11. Hacking Competitions Fostering a Resilient, Self-Sustaining Offensive Cyber Ecosystem

Chinese hacking competitions have transitioned from being mere student training ground and recruitment platforms to serving as tools for internal trainings within government-contracted companies and as mechanisms for transferring vulnerability knowledge to Chinese security agencies. In the early 2010s, the success of Chinese hacking teams at DEFCON CTF prompted major technology and cybersecurity companies like Baidu, Tencent, and Qihoo 360 to get involved (section 4). These corporations provided sponsorships, outright acquired winning teams, organized CTF events and offered attractive benefits to recruit members.

In 2024, leaks revealed the involvement of i-SOON, a government-contracted company engaged in extensive espionage activities. It served as the main sponsor of a competition in China organized by a DEFCON CTF champion team, marking the closest connection between a top-performing team at DEFCON CTF and Chinese state-sponsored espionage efforts (section 4.2).

Retired team members often either joined tech giants, such as Qihoo, Alibaba, Tencent, Huawei and Qi An Xin, or created their own cyber security startups. These startups include Saining Network, Starcross Technology (section 4.3.1), Chaitin Tech, Bolean Technology (section 4.5.1), and Cyber Kunlun (section 6.4). These startups provide niche digital services, such as cyber ranges and automated vulnerability discovery systems, to Chinese companies and government agencies alike. They also figure among important zero-day vulnerability contributors to China's security agencies.

This ecosystem has been further reinforced by the multitude of Chinese CTF competitions that have emerged since the mid-2010s. Today, hacking competitions play a central role in China's cybersecurity educational curriculum and have significantly contributed to the expansion of the country's cybersecurity education and training market.

12. Emergence of China-Based CTF Competitions from DEFCON Participation

Some of the Chinese teams that gained international famed have set up their own China-based hacking competitions. This includes among others: BCTF, the XCTF International League, 0CTF/TCTF, Real World CTF, and N1CTF.

- From 2013 to 2014, Blue Lotus collaborated with the Baidu Research Institute to create the Baidu CTF (BCTF) competition, the first Chinese CTF competition to use the Attack-Defense format (section 4.1). In 2018 and 2019, BCTF was held in Beijing as part of i DEFCON China [Beta] and DEFCON China 1.0 (section 4.2).
- Founded in 2014 by Tsinghua University's Blue Lotus team, XCTF is organized and hosted by Blue Lotus and Saining Network Security. The competition unfolds in various phases across different Chinese cities, including Hangzhou, Chengdu, Beijing, and Shanghai (section 4.3).
- Initiated in 2017, 0CTF/TCTF is held in Shanghai. It is co-organized by the Tencent Keen Security Lab and Shanghai Jiao Tong University's 0ops team (section 4.4).
- Chaitin Tech initiated its own global jeopardy-style CTF competition in Beijing in 2018, called Real World CTF (section 4.5.1).
- In 2018, the Nu1L team established its own Jeopardy-style contest, named N1CTF (section 4.2).
- The W&M team established its own Jeopardy-style contest in 2020, named WMCTF. The 2023 WMCTF edition was supported by i-SOON as the primary sponsor, the government-contracted firm whose extensive espionage activities were exposed in early 2024 (section 4.2).

The emergence of numerous CTF competitions since the mid-2010s could be a contributing factor to the decreased presence of Chinese teams at DEFCON CTF 2023 (figure 3). Fewer Pwn2Own-like competitions seem to be available in China. The most relevant ones are GeekCon and the Tianfu Cup. GeekCon (previously GeekPwn) was established in 2014 by DarkNavy (formerly Keen Team). It has been held across China and even had iterations in Las Vegas. The Tianfu Cup was

first held in 2018, and takes place annually in Chengdu, Sichuan province (section 6).

13. Lack of Strong Bug Bounty Programs in China

Finding information on China-based bug bounty platforms and their payouts structures is challenging (section 7.5). Chinese bug bounty platforms offer limited incentives for hackers, with rewards often being unspecified or comparatively low. Similarly, Chinese exploit acquisition platforms offer payouts that are on average significantly lower compared to non-Chinese ones. Apart from navigating US sanctions, Chinese researchers must additionally deal with sharing their bounty rewards with their employers (sometimes up to 50% of the payouts).

14. Economic Incentives at the Tianfu Cup

The Tianfu Cup has been predominantly focused on Western products. Due to their comparatively lower rewards, Chinese products have received minimal attention at the Tianfu Cup. In 2023 there was a noticeable change as the Tianfu Cup began to feature an increasing number of Chinese products (section 6.2.2).

Despite the Tianfu Cup's significant prize pool, participants have raised concerns about how the prize money is distributed among team members and their organization. Companies like Qihoo 360, which have multiple teams with many members, often consolidate researchers into a handful of teams for the competition. This practice frequently leads to the exclusion of many talented individuals, often resulting in them earning less and receiving no social recognition.

15. International Participation at China-based competitions

The Tianfu Cup exclusively features Chinese teams (section 6), while CTF competitions held in China are open to international participation. This distinction is highly likely because CTFs participants are not required to disclose zero-day vulnerabilities. Likely for the same reason, some Chinese teams have also been able to gradually integrate into international teams participating in the U.S.-based DEFCON CTF competition.

16. Open Questions Regarding China's Model Effectiveness

Chinese hackers likely report vulnerabilities they discover to both government agencies and Western vendors through their bug bounty programs. This assertion is supported by several factors: (1) Chinese law mandates the reporting of vulnerabilities, and Chinese companies must annually submit a specific number of vulnerabilities to the CNNVD to maintain their partnerships with the organization (section 3.3). (2) The report's analysis of Google Android, Microsoft, and Apple's bug bounty data reveals a significant number of submissions from Chinese researchers up to the end of 2023 (section 7).

Despite Western vendors receiving a lot of information about zero-day vulnerabilities, the Chinese system continues to be effective in exploiting Western products. This raises the question as to why. Are these distinct individual zero-days and zero-day chains? Is it a patching problem? Or does Chinese efficiency stem from inadequate security practices among the targeted victims?

17. The Tianfu Cup's Growing Emphasis on Chinese Targets

China's domestic priorities coupled with persistent geopolitical tensions will likely shift the focus of Chinese hacking competitions. The Tianfu Cup 2023 marked a significant departure from targeting Western products toward Chinese ones (section 6.2.2).[13] This trend will likely create future incentives for Chinese teams to specialize in hunting down vulnerabilities in domestic products. It would also allow Beijing to increase incentives that align with the nation's long-term national security interests.

[13] 江西省, "2023 '天府杯'设立千万级奖金 四个'首次'值得关注," *SOHU*, October 31, 2023, https://www.sohu.com/a/732639756_99990681.

3 China's Hack-for-Hire Approach

This section provides an overview of what is publicly known about China's hack-for-hire ecosystem, drawing on foundational research and analysis (3.1). It delves into China's approach and its significance, with a particular focus on China's vast talent pool (3.2) and the national regulations that compel civilians to collaborate with the government (3.3).

Key Points

- Intrusion Truth, U.S. indictments and the i-SOON leaks exposed China's hack-for-hire model, tracing a pattern linking contract hackers to intelligence activities.
- Contractors depend on government agencies for zero-day vulnerabilities, primarily sourced from specialized research teams and labs in select private firms.
- This hack-for-hire model is significant due to China's highly skilled civilian hacker community.
- Since the early 2010s, Chinese hackers have emerged as leading contenders in international hacking competitions and bug bounty programs.
- Hacking competitions play a crucial role in China's cybersecurity education and have contributed to the expansion of the country's cybersecurity market.
- Since 2018, China has increasingly controlled the domestic vulnerability discovery process.
- This system has proved effective for China. Chinese APTs exploit a higher number of zero-days than APTs from other countries.

3.1 Background

Since assuming China's presidency in 2013, Xi Jinping underscored a strong commitment to advancing Beijing's cyber capabilities. In 2014, he unveiled China's ambition to transform into a "cyber power," comparing the twin goals of developing China's information technology and its cybersecurity capabilities to "two wings of a bird and two wheels of an engine[14]". This vision was supported by large investments, organizational refinements within and across security agencies, and the establishment of relevant legal frameworks to bolster China's offensive cyber and defensive capabilities.

Yet, the narrative extends beyond state-led efforts. China's civilian hacker community has been an instrumental, but often overlooked driving force in its own right, evolving in tandem with and supporting state efforts. At the forefront of this dynamic stands China's Military-Civil Fusion (MCF) initiative. The MCF initiative seeks to harness the synergy between commercial and defense advancements, leveraging civilian talent to enhance and back the armed branch of the Chinese Communist Party (CCP), the People's Liberation Army (PLA).[15]

The roots of the MCF initiative extend back many decades. Every leader from Mao Zedong onward has implemented a program to compel the civilian sectors of Chinese society to contribute to the PLA's development. However, since Xi Jinping assumed power in 2013, the importance of MCF has markedly increased, evolving into a strategic priority. Chinese authoritative military texts, such as the PLA 2013 publication "The Science of Military Strategy", have emphasized the integration of military-civil collaboration in peace and war time, including in cyberspace.[16]

The demarcation line separating China's military and civil domains in cyberspace has become particularly

[14] William Wan, "Chinese President Xi Jinping Takes Charge of New Cyber Effort," *The Washington Post*, February 27, 2014, https://www.washingtonpost.com/world/chinese-president-takes-charge-of-new-cyber-effort/2014/02/27/a4bffaac-9fc9-11e3-b8d8-94577ff66b28_story.html.

[15] Frank Jüris, "Security Implications of China-Owned Critical Infrastructure in the European Union" (European Parliament, June 2023), https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702592/EXPO_IDA(2023)702592_EN.pdf.

[16] "PLA's Science of Military Startegy (2013)," In Their Own Words: Foreign Military Thought (China Aerospace Studies Institute, August 2, 2021), https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2021-02-08%20Chinese%20Military%20Thoughts-%20In%20their%20own%20words%20Science%20of%20Military%20Strategy%202013.pdf.

fluid or has entirely vanished. In April 2017, an anonymous online entity known as Intrusion Truth began to publicly unveil the identities of individuals associated with Chinese advanced persistent threats (APTs).[17] Over the course of six years, Intrusion Truth exposed more than 30 individual belonging to at least six APTs affiliated with the Ministry of State Security (MSS), China's premier intelligence agency. The revelations exposed a pattern connecting front companies with MSS local/regional bureaus and contract hackers. More broadly, they shed light on the intricate relationships between China's IT sector, academic institutions, and the country's intelligence agencies. At times, their findings were corroborated by leading threat intelligence firms and were followed by indictments by the US Department of Justice.

Intrusion Truth primarily relied on publicly available information to establish connections between various cues across different sources, platforms, and identities. The group's initial inquiries into APT3 (2017) exposed the links between operatives Wu Yingzhuo and Dong Hao, their front company Boyusec, and the Guangdong bureau of the MSS.[18] On its website, which became unavailable following the exposures, Boyusec had listed Chinese tech giant Huawei as a business partner.[19] In its APT40 investigation (2020), Intrusion Truth linked no less than 13 front companies to a professor, former PLA officer, at Hainan University's Information Security Department. The professor contributed to the recruitment efforts for these companies, with one of them operating from the university's library.[20] Recent analysis by the group into APT41 (2022) indicated a broader effort by the MSS to enlist graduate students into its ranks using front companies[21], whether with or without the knowledge of the universities.[22] In some cases, Intrusion Truth's revelations have led to indictments by the U.S. Department of Justice (APT3, APT10, APT31, APT40).

In February 2024, additional details surfaced about China's hack-for-hire system from leaked files, chat logs, and images associated with the Chinese security contractor Shanghai Anxun Information Co. (上海安洵信息公司), known as "i-SOON," which were uploaded on the code-sharing platform Github.[23] Although the source remains unclear, it seems likely that the information was deliberately leaked by a disgruntled staff member.[24] The documents revealed that i-SOON had been contracted by the Chinese government to carry out espionage operations on its behalf. These contracts, spanning eight years, specifically outlined objectives to identify targets and extract data from at least 20 foreign governments and territories.[25] Among the targeted countries were India, Hong Kong, Thailand, South Korea, the United Kingdom, Taiwan, and Malaysia.

According to an analysis by threat intelligence company Harfang, i-SOON enjoys a significant level of operational independence. The analysis indicates that while it sometimes receives requests directly from customers, such as breaching email servers to retrieve relevant content, there are instances where i-SOON independently acquires access or data it believes may interest clients and then attempts to sell it to them. [26] [27] In such cases, i-SOON provides sample documents to clients to demonstrate the relevance of the target. Since 2013, i-SOON has established an "APT research" division focused on "overseas targets," offering different services. These include obtaining access to a victim's network, extracting data, and generating intelligence reports.[28]

[17] Intrusion Truth, "Coming Soon…."
[18] Intrusion Truth, "APT3 Is Boyusec, a Chinese Intelligence Contractor," WordPress, *Intrusion Truth* (blog), May 9, 2017, https://intrusiontruth.wordpress.com/2017/05/09/apt3-is-boyusec-a-chinese-intelligence-contractor/#more-115.
[19] Bill Gertz, "Pentagon Links Chinese Cyber Security Firm to Beijing Spy Service," *The Washington Free Beacon*, November 29, 2016, https://freebeacon.com/national-security/pentagon-links-chinese-cyber-security-firm-beijing-spy-service/.
[20] Intrusion Truth, "APT40 Is Run by the Hainan Department of the Chinese Ministry of State Security," WordPress, *Intrusion Truth* (blog), January 16, 2020, https://intrusiontruth.wordpress.com/2020/01/16/apt40-is-run-by-the-hainan-department-of-the-chinese-ministry-of-state-security/#more-587.
[21] Intrusion Truth, "The Old School Hackers behind APT41," WordPress, *Intrusion Truth* (blog), July 21, 2022, https://intrusiontruth.wordpress.com/2022/07/21/the-old-school-hackers-behind-apt41/.
[22] Eleanor Olcott and Helen Warrell, "China Lured Graduate Jobseekers into Digital Espionage," *Financial Times*, June 30, 2022, https://www.ft.com/content/2e4359e4-c0ca-4428-bc7e-456bf3060f45.
[23] Christian Shepherd, Cate Cadell, Ellen Nakashima, Joseph Menn and Aaron Schaffer, "Leaked Files from Chinese Firm Show Vast International Hacking Effort."
[24] Pieter Arntz, "A First Analysis of the I-Soon Data Leak," *Malwarebytes Labs* (blog), February 21, 2024, https://www.malwarebytes.com/blog/news/2024/02/a-first-analysis-of-the-i-soon-data-leak.
[25] Christian Shepherd, Cate Cadell, Ellen Nakashima, Joseph Menn and Aaron Schaffer, "Leaked Files from Chinese Firm Show Vast International Hacking Effort."
[26] Winnona Bernsen, "Same Same, but Different."
[27] Cyber Threat Research Team, "A COMPREHENSIVE ANALYSIS OF I-SOON'S COMMERCIAL OFFERING," *Harfanglab, Inside the Lab* (blog), January 3, 2024, https://harfanglab.io/en/insidethelab/isoon-leak-analysis/.
[28] Cyber Threat Research Team.

Figure 2: i-SOON CEO Wu Haibo (Shutd0wn) discussing the Anxun Cup
(Date and time, sender, receiver, original message, English translation)

2020-08-07 05:07:47	lengmo	Shutd0wn	就是四川省大学生竞赛的事情，早上开了会，比赛两天，第一天就是传统的CTF 出题，第二天内网，内网出题我们问题不大，第一天传统的，我们出题，专业度不够，里面有些传统赛棍…出题组意思是看公司能不能找点外面的资源出题	It's about the Sichuan Provincial College Student Competition... The purpose of the question writing team is to see if the company can find some external resources to write questions
2020-08-07 05:09:07	lengmo	Shutd0wn	我想了几个，第一个 盘古，出 安卓 或者逆行(typo - 逆向)类的题，还有就是 蓝莲花 或者 长亭科技	I have thought of a few, the first one is Pangu, for Android or Reverse engineering questions, other options are Blue Lotus or Chaitin Tech
2020-08-07 05:09:16	lengmo	Shutd0wn	这些传统的，他们出这类题目有经验	These are traditional teams, they have experience in making this kind of challenges
2020-08-07 05:09:50	Shutd0wn	lengmo	嗯，盘古这个问题不大，下个月初比赛吧?	Well, Pangu is a light lift. The competition is early next month, right?
2020-08-11 01:23:30	lengmo	Shutd0wn	盘古给了几道题啊	How many questions did Pangu give
2020-08-11 01:25:00	Shutd0wn	lengmo	3个安卓的	3 Android challenges
2021-08-24 09:10:13	lengmo	Shutd0wn	去年和奇安信那边合作搞得培训，刚董东和我说，盘古财务要全部并入奇安信，要给我们付一笔钱，4W块，后面还有点	Last year we cooperated with Qi'anxin for training. Dong Dong just told me that Pangu's finance will be completely merged into Qi'anxin - they'll pay us a sum of money, 4W yuan, and there will be more after that

Source: i-SOON leaked chat logs

The leaks have additionally shed light on the significance of hacking competitions in aiding state-sponsored operations. i-SOON created a CTF platform for internal training and organized its own hacking competition, named the "Anxun Cup," to attract highly skilled individuals. In order to achieve this, i-SOON collaborated with prominent Chinese defense contractors like Qi An Xin's Pangu Team (section 5.5) and explored the possibility of seeking support from established CTF entities in China, such as Blue Lotus and Chaitin Tech (section 4.2), as shown in Figure 2.[29]

Furthermore, the leaks have reaffirmed the role of China-based hacking competitions like the Tianfu Cup as a means for the government to acquire valuable zero-day vulnerabilities. Specifically, the leaks outline a process in which vulnerabilities submitted by civilian hackers to participate in the Tianfu Cup are gathered by government security agencies. These vulnerabilities are later disseminated to provincial branches of these agencies, which then forward them to contractors for the execution of cyber operations (section 6.2.1). Based on this framework, China's specialized hackers uncover zero-day vulnerabilities that are then utilized by government contractors for cyber operations. This doesn't suggest that it's the sole model in China, but it has been demonstrated to be a prevalent one.

This matters for two main reasons. Firstly, China boasts some of the most skilled civilian hackers worldwide, evident from their performance in international hacking competitions and bug bounty programs. Secondly, these researchers are mandated to cooperate with the government, including reporting the vulnerabilities they discover. I will examine each aspect individually. Together, these components constitute the foundation of China's hack-for-hire model and its wider offensive cyber ecosystem.

[29] Winnona Bernsen, "Same Same, but Different."

3.2 China's Civilian Hackers

Since the early 2010s, Chinese teams from a limited number of universities and companies have emerged as leading contenders in the most challenging and prestigious international hacking competitions, including DEFCON CTF and Pwn2Own, within a few years. At DEFCON, the Blue Lotus team first reached the finals in 2013, and from then until 2023, between one and four Chinese teams have consistently reached the finals each year, representing the only significant challenge to US dominance (section 4.2). Similarly, at Pwn2Own, the winnings of Chinese participants increased from 13% in 2014 to 79% in 2019 of the total prize money awarded to all participants (section 5.2). Similarly, Chinese hackers have been top contributors to the bug bounty programs of prominent US-based companies. From 2017 to 2023, China alone contributed 27% of all vulnerabilities submitted to the bug bounty programs of Apple, Google Android, and Microsoft combined, while the rest of the world accounted for 59% (section 7). Individual researchers and teams have garnered numerous recognitions, frequently figuring among the top spots in these program's rankings of best researchers and teams for both the caliber and quantity of the vulnerabilities they've uncovered.

These achievements led to the establishment of China's own world-class hacking competitions, the creation of influential startups, and the development and expansion of some of today's top Chinese security research teams and laboratories. These will be explored in detail throughout the report. The strength of China's cybersecurity ecosystem is bolstered by expanding professional and educational opportunities in the domestic offensive cyber sector. According to statistics from the China Cybersecurity Industry Alliance (2023), the cyber security sector is poised for sustained growth in the coming years, with a projected market size exceeding 11 billion USD by 2025.[30] A 2022 report by International Data Corporation (IDC) China highlights that the sector's growth is primarily fueled by the IT education and training sector, which saw the most rapid growth in the first half of 2022, with a year-on-year increase of 33%.[31] This surge was particularly evident in security training, drilling, and testing platforms, attributed in part to the popularity of hacking contests.[32]

Cybersecurity education in China has also gained momentum, with over 200 domestic universities offering cybersecurity or information security majors as of March 2023.[33] Hacking competitions have become integral to the cybersecurity curriculum. Under the guidance of the Ministry of Education, the Discipline Evaluation Group of the Academic Degrees Committee of the State Council, released a *White Paper on the Practical Ability of Cybersecurity Talents - Talent Evaluation* in September 2023.[34] 63% of institutions survey in the White Paper deemed competing in hacking competitions highly effect for training cybersecurity talents. To encourage active participation in these competitions, 75% of colleges surveyed even financially reward students who excel in hacking competitions.[35] 75% of institutions have also set up dedicated budgets to establish advanced attack and defense laboratories which are designed to enhance a students' practical abilities in network security through "practical required courses."[36]

3.3 The "Weaponization" of Civilian Hackers

In alignment with China's MCF policy, the Chinese government has systemically utilized cyber-related civilian resources for strategic purposes. This has manifested in different ways. For instance, various entities, including universities and companies, collaborate with the Chinese government across a spectrum of cyber activities—from submitting zero-days and offering cyber courses to the military, to estab-

[30] **江西省**, "2023 '**天府杯**'设立千万级奖金 **四个**'**首次**'值得关注."

[31] "让世界更安全，更美好!," *360* (blog), October 21, 2022, https://360.net/about/news/article635f741f010089001f90487f.

[32] "让世界更安全，更美好!"

[33] "2023**国家网安周**丨《**网**络安全人才实战能力白皮书-**人才**评价篇》重磅发布," **中国科学技**术大学 (blog), September 15, 2023, https://cybersec.ustc.edu.cn/2023/0915/c23847a612249/page.htm.

[34] "2023**国家网安周**丨《**网**络安全人才实战能力白皮书-**人才**评价篇》重磅发布."

[35] "**全国中学生网**络安全竞赛在西电落幕（附获奖名单）," **澎湃研究所**, September 22, 2022, https://www.thepaper.cn/newsDetail_forward_4504304.

[36] "2023**国家网安周**丨《**网**络安全人才实战能力白皮书-**人才**评价篇》重磅发布."

lishing co-partnered defense research labs and setting up private IT infrastructure for state-sponsored hacking operations. On the private sector and academic side, the collaborations can range from a single individual hacker or professor to entire teams comprised of both students and seasoned cyber security professionals.

In 2018, the Chinese government began to significantly focus on regulating the work of cybersecurity researchers, students, hacking competitions, and bug bounty programs. As such, Beijing is steadily tightening its grip on the domestic process of vulnerability discovery and disclosure. In a first step, the Chinese government began to prohibit Chinese security researchers from participating in hacking competitions on foreign soil (2018).[37] Thus preventing the Chinese cybersecurity community from publicly showcasing and disclosing vulnerabilities at events such as Pwn2Own. Secondly, in 2021 Beijing established the "Regulations on the Management of Security Vulnerabilities in Network Products (RMSV)," which compels Chinese tech companies – and their researchers – to directly hand over any zero-day vulnerabilities to the government within two days of discovery. From there, government agencies can cherry-pick which vulnerabilities should be publicly disclosed, and which ones will be kept secret and used for espionage and offensive cyber campaigns. According to Microsoft's Digital Defense Report 2022, "China's vulnerability reporting regulation went into effect September 2021, marking a first in the world for a government to require the reporting of vulnerabilities into a government authority for review prior to the vulnerability being shared with the product or service owner... this new regulation might enable elements in the Chinese government to stockpile reported vulnerabilities toward weaponizing them."[38] In December 2021, Alibaba Cloud faced penalties under RMSV when its security engineer Chen Zhaojun discovered the Log4j vulnerability and reported it to Apache without prior notification to the Chinese authorities. Alibaba Cloud was fined and its information-sharing collaboration with China's Ministry of Industry and Information Technology (MIIT) was suspended.[39]

Insights from Kristin Del Rosso and Dakota Cary's Sleight of Hand report (2023) reveal how China's military and intelligence agencies gain access to zero-day vulnerabilities discovered by security research teams in private companies.[40] When a China-based researcher discovers a zero-day, they are required to report said vulnerability to the Cybersecurity Threat and Vulnerability Information Sharing Platform (NVDB), overseen by the MIIT. This information is then made available – if not even directly channeled – to the MSS and PLA-affiliated entities.

In a separate process, the MSS-run China National Vulnerability Database of Information Security (CNNVD) mandates its private-sector partners to contribute software vulnerabilities to become a 'technical support unit' (TSU). This system then ranks TSUs based on the number of vulnerabilities submitted (table 2).[41] In total, the report identified 151 registered TSUs which collectively provide at least 1,955 software vulnerabilities to the MSS, of which at least 141 are categorized as "critical." Once vulnerabilities are reported to the CNNVD, they are highly likely evaluated by the MSS for their potential operational use. In 2017, U.S. threat intelligence company Recorded Future indicated that critical vulnerabilities are assessed by the MSS for their utility in intelligence operations before being publicly disclosed.[42] In addition to weaponizing zero-days, these regulations also ensure a stronger relationship between Chinese civilian hackers and job opportunities at Chinese state institutions and private sector companies (that support state-sponsored activities). Thus, apart from having unrestricted access to zero-day vulnerabilities, this setup allows Beijing to also shape the structure and economic incentives of Chinese hacking competitions and bug bounty programs strategically.

[37] Chris Bing, "China's Government Is Keeping Its Security Researchers from Attending Conferences," August 3, 2018, https://cyberscoop.com/pwn2own-chinese-researchers-360-technologies-trend-micro/.

[38] "Microsoft Digital Defense Report 2022" (Microsoft, 2022), https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022.

[39] Jonathan Grieg, "Chinese Regulators Suspend Alibaba Cloud over Failure to Report Log4j Vulnerability," *ZDNET*, December 22, 2021, https://www.zdnet.com/article/log4j-chinese-regulators-suspend-alibaba-partnership-over-failure-to-report-vulnerability/.

[40] Dakota Cary and Kristin Del Rosso, "Sleight of Hand: How China Weaponizes Software Vulnerabilities."

[41] Dakota Cary and Kristin Del Rosso.

[42] Priscilla Moriuchu and Dr. Bill Ladd, "China Altered Public Vulnerability Data to Conceal MSS Influence," *Recorded Future Blog* (blog), September 3, 2018, https://www.recordedfuture.com/blog/chinese-vulnerability-data-altered.

Table 2: CNNVD Technical Support Units Requirements

CNNVD Annual Requirements for Technical Support Units			
Category	Level 1	Level 2	Level 3
Data Coordination	Information submitted to the annual CNNVD Work Report is accurate and complete.		
Business Coordination	Coordination with the CNNVD is smooth and the business's attitude is energetic. There has never been an instance when the business point of contact is inaccessible or when an email has gone unanswered for too long.		
Annual Submission of Novel Vulnerabilities	The company submits at least 35 "common" (通用型) novel vulnerabilities, from which at least 5 are considered "critical risk."	The company submits at least 25 "common" (通用型) novel vulnerabilities, from which at least 1 is considered "critical risk."	The company submits at least 5 "common" (通用型) novel vulnerabilities.
Annual Vulnerability Early Warning Support	The business provides new fewer than 10 *critical* alerts.	The business provides no fewer than 10 alerts.	The business provides no fewer than 5 alerts.
Other Support	Enthusiatically respond to CNNVD requests related to vulnerability technology evaluation and judgement, technical seminars, data anaylsis support, and special event-based vulnerability support.		

Source: Cary & Del Rosso (2023) Sleight of Hand, Atlantic Council

Are these regulations effective? Finding 0-days is a costly and time-intense process. For governments to do this by themselves, would pose significant resource and logistical challenges. Alternatively, as explained by CSS researcher Max Smeets, purchasing zero-days from black markets is expensive and fraught with information asymmetries between sellers and buyers.[43] This challenge is compounded by the prevalence of low-quality exploits, further complicating the task of distinguishing reliable ones.[44]As of this writing, Chinese APTs are exploiting more zero-days in absolute numbers than APTs from other countries, based on available data. In 2023, threat intelligence company Mandiant revealed that the use of zero-days by state-linked Chinese groups has nearly doubled between 2020 and 2022, and they have exploited more zero-days than any other country.[45] The speed at which threat actors exploit these vulnerabilities has also increased significantly.[46] Without introducing major systematic changes, China has effectively shaped the existing environment in its favor.

The Chinese government has effectively addressed these challenges by strategically positioning itself as the ultimate recipient in the vulnerability disclosure processes of civilian researchers. This has resulted in an alternative model to the Coordinated Vulnerability Disclosure (CVD) and Government Disclosure Decision Processes (GDDP) (box 2). This approach enables the Chinese government to take advantage, at scale and almost no cost, of some of the best vulnerability researchers on the globe, providing a unique solution that mitigates the inefficiencies associated with traditional zero-day acquisitions.[47] As it will be shown in this report, the most prolific suppliers of zero-days to the MSS[48] include several Chinese companies involved in international hacking competitions and bug bounty programs, underscoring the success of this strategy.

[43] Max Smeets, "Hack Global, Buy Local: The Inefficiencies of the Zero-Day Exploit Market," *Lawfare*, June 6, 2022, https://www.lawfaremedia.org/article/hack-global-buy-local-inefficiencies-zero-day-exploit-market.
[44] Max Smeets.
[45] James Sadowski and Casey Charrier, "Move, Patch, Get Out the Way: 2022 Zero-Day Exploitation Continues at an Elevated Pace."
[46] Liam Tung, "Hackers Are Getting Faster at Exploiting Zero-Day Flaws. That's Going to Be a Problem for Everyone," *ZDNET*, March 29, 2022, https://www.zdnet.com/article/hackers-are-getting-faster-at-exploiting-zero-day-flaws-thats-going-to-be-a-problem-for-everyone/.
[47] Max Smeets, "Hack Global, Buy Local: The Inefficiencies of the Zero-Day Exploit Market."
[48] Dakota Cary and Kristin Del Rosso, "Sleight of Hand: How China Weaponizes Software Vulnerabilities."

Box 2: Vulnerability Disclosure Programs

There are many actors involved in the search and discovery of zero days, including government agencies and private companies. A new vulnerability, when found, can be used for either offense – attacking others – or defense – getting it patched. Various vulnerability disclosure processes exist, with distinctions based on whether the discovering entity is from the private sector or a government agency. These processes are classified as Coordinated Vulnerability Disclosure (CVD) for private sector entities and Government Disclosure Decision Processes (GDDP) for government agencies.

When private researchers uncover new vulnerabilities, ethical disclosure practices come into play. These include a responsible and coordinated effort to inform relevant stakeholders, such as software vendors or system administrators, about the identified vulnerabilities. CVD emphasizes transparent and timely communication. Via this process, researchers privately inform the affected party or parties, such as software vendors, service providers, or system administrators, about the identified vulnerability. This ensures that a fix or patch can be developed and deployed before the details of the vulnerability are made public.

When government agencies, such as military cyber units or intelligence agencies, discover or purchase a new vulnerability, they face a binary decision: to keep it secret and stockpile it for later use or to disclose it to the appropriate vendor so that it can be fixed. GDDP consists of coordinating the sharing of vulnerability information between relevant stakeholders through a government-led process, to determine whether and how to disclose the existence of discovered vulnerabilities and their mitigation. An example is the U.S. Vulnerabilities Equities Process (VEP), initially developed in the late 2000s but publicly acknowledged only in 2016.

Upon disclosure, the new vulnerabilities are assessed by relevant vendors or agencies before being assigned a criticality level or score and published in relevant vulnerability databases, i.e. public centralized repositories of information about known vulnerabilities in various software, operating systems, and applications. This centralized access streamlines the vulnerability management process by providing a single point of reference for security teams across several vendors, allowing for swift mitigation of vulnerabilities.

4 DEFCON CTF (2013-2023)

This section traces the history and performance of Chinese hacking teams that participated in DEFCON CTF (2013-2023), and the impact they had on shaping China's offensive cybersecurity culture. It specifically examines the teams' affiliations with academic institutions and corporate entities, as well as the extent of their involvement in military-civil fusion initiatives aimed at supporting state-sponsored offensive cyber operations.

Key Points

- Chinese teams consistently challenged US dominance at DEFCON CTF from 2013 to 2023, with one to four teams advancing to the finals each year.
- Participants, predominantly students but also including professionals, hail from a select group of elite universities.
- Major Chinese technology and cybersecurity corporations provided sponsorship to top DEFCON CTF contenders, acquiring winning teams and offering attractive job benefits to recruit security experts.
- The universities hosting DEFCON CTF teams have been (a) linked to Chinese state-sponsored cyber operations, (b) conducted vulnerability research with Chinese companies that have been linked to Chinese state-sponsored cyber operations, or (c) serve as fertile recruitment centers for Chinese security agencies. One team has notably strong connections with i-SOON.
- Alumni from top teams have greatly enriched the offensive cyber ecosystem, establishing China-based Capture The Flag (CTF) competitions and launching startups specialized in cyber ranges and automated vulnerability discovery systems. These startups contribute zero-day vulnerabilities to Chinese security agencies.

4.1 Background

Founded by Jeff Moss in 1992, DEFCON takes place annually in Las Vegas, Nevada, and is the largest hacking conference in the world. DEFCON's own CTF competition was first held in 1996.

Broadly speaking, there are two types of CTF competitions: Jeopardy and Attack-Defense. Jeopardy covers a broad spectrum of skills, including reverse engineering, web, binary exploitation, and cryptography. It is best described as a digital treasure hunt in which hacking teams compete to find vulnerabilities in a system. The teams must solve security challenges and puzzles that mimic real-world hacking scenarios to earn points. The goal is to 'capture the flag,'(CTF) which is usually a hidden piece of data or code that – once it is found – serves as proof that a hack was successful.

In contrast to this, Attack-Defense competitions allow participants to attack each other. Each team is given access to a set of vulnerable services, identifiable by the presence of flags. The teams must subsequently seize these flags from their opponents to score points.[49] Teams thus analyze a target program, identify vulnerabilities, and then develop exploits to compromise the other teams' machines by stealing their flags. At the same time, the team must patch its own systems to defend against similar attacks from the other team.

The DEFCON CTF qualification system relies predominantly on Jeopardy-style CTFs. The DEFCON Finals fall under the Attack & Defense CTF category. In addition to succeeding in the qualifiers, teams can qualify for the finals by winning prominent global community events throughout the year or by succeeding in prior DEFCON CTF finals. Overall, DEFCON CTF primarily revolves around testing and improving individual hacking skills in a controlled and legal environment. Cash prizes are typically awarded based on a team's overall performance. This can vary from a few thousand to tens of thousands of US dollars. The prizes are distributed among the top teams that excel in different parts of the competition.

[49] "DEF CON CTF Finals: An Inside View," *VMRAY*, September 24, 2018, https://www.vmray.com/cyber-security-blog/def-con-ctf-finals-an-inside-view/.

In 1996, DEFCON CTF started rather informally, with participants gathering and attempting to breach a server and retrieve a specific text file. Over time, the CTF evolved into a highly competitive challenge, attracting participants from around the world. Throughout the 2000s, DEFCON CTF continued to grow in both size and complexity. Nowadays, the event is consistently drawing crowds of 25,000 to 30,000 attendees, with teams competing in reverse engineering, network security, cryptography, and other areas to test their skills and knowledge.

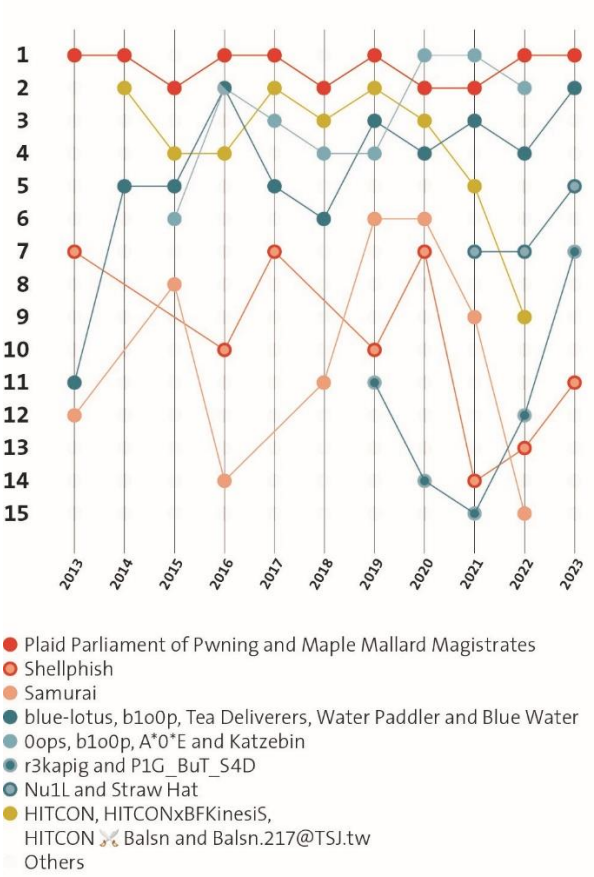
Chinese teams began to compete in DEFCON CTF in the 2010s, with the Blue Lotus team leading the way as the first Chinese team to qualify for the finals in 2013. Chinese tech firms subsequently increased their participation rate by sending numerous teams to DEFCON and other conferences outside of China. Within the brief span of a few years, these Chinese teams rapidly evolved into formidable competitors. Between 2013 and 2023, roughly one to four Chinese teams annually secured a spot in the DEFCON CTF finals (see figure 3 for comprehensive ranking details).

4.2 Blue Lotus, 0ops, A*0*E, r3kapig, Nu1L, and others

In June 2012, Tsinghua University's (THU) Blue Lotus team burst onto the international cybersecurity scene. Their debut performance at the DEFCON CTF Qualification Tournament was commendable. They secured the 19th position among a pool of over 500 teams, coming very close to reaching the tournament's finals.[50]

Throughout the latter half of 2012, the Blue Lotus team engaged in other internationally acclaimed CTF events, such as CSAW (USA), Hack.Lu (Luxembourg), RuCTFe (Russia), and Positive Hack Days CTF (Russia).[51] Each contest proved to be crucial in honing the team's technical abilities and refining their competitive acumen. In December 2012 Blue Lotus reached 7th place in the prestigious 29C3 CTF competition (Germany) that is organized by the Chaos Computer Club Aachen. This marked the first time a Chinese team secured a top eight rank in an internationally renowned hacking competition.[52]

Figure 3: DEFCON CTF Ranking (2013-2023)



(Red: From U.S.-only to international with a strong U.S. component; Blue: From Chinese-only to international with a strong Chinese component; Yellow: Taiwanese teams)

Source: Compiled by the Author

In June 2013, the Blue Lotus team became the first Chinese team ever to qualify for the DEFCON CTF finals, securing the 4th place among 414+ contenders. In the finals, held later that year in Las Vegas, Blue Lotus finished 11th of 20.[53] The first place was won by Plaid Parliament of Pwning (PPP), Carnegie Mellon University's (CMU) top performing hacking team. Throughout the rest of 2013, Blue Lotus achieved remarkable rankings in CTF competitions across Germany, South Korea, Iran, and the United States.[54]

Year after year, Blue Lotus performances continued to astound observers, earning them more and more recognition in the cybersecurity community. In June 2014, Blue Lotus exceeded expectations by once again

[50] "Blue-Lotus" (Teams: CTF Time), accessed October 9, 2023, https://ctftime.org/team/1941/.
[51] "Blue-Lotus."
[52] "Blue-Lotus."
[53] "Blue-Lotus."
[54] "Blue-Lotus."

reaching the DEFCON CTF finals. This time securing the 5th place in the finals, with the top spot again being claimed by PPP.[55] Blue Lotus' success extended once again to various international CTF competitions, including the CodeGate Finals (South Korea), PlaidCTF (USA), ASIS (Iran), Pwnium (Tunisia), HITCON (Taiwan), and Hack.Lu (Luxembourg).[56] According to CTFtime – the premier CTF competition archive – Blue Lotus solidified its overall global standing in November 2014, ranking 16th globally and 2nd in Asia.[57]

Figure 4: Blue Lotus at DEFCON 2014

Source: https://tech.sina.cn/other/2014-08-22/detail-icfkptvx3234589.d.html?from=wap

In 2015, Blue Lotus replicated its success of the previous year, securing 5th place at the DEFCON CTF finals. PPP trailed in second place behind DEFKOR from South Korea.[58] During the same event, another Chinese team, the "0ops" team from Shanghai Jiao Tong University (SJTU), made a noteworthy entrance into the finals too, finishing just one position below Blue Lotus.[59] Before joining DEFCON CTF, the SJTU team had already garnered recognition in various CTF competitions, securing 2nd place at Hack.lu CTF (Luxembourg) and 6th place at HITCON CTF (Taiwan) in 2014.[60] The encounter between the Blue Lotus and 0ops inspired an alliance between the two teams, leading to the birth of "b10op".[61]

In 2016, the newly born b10op team achieved new records for China, placing 2nd in the DEFCON CTF finals, with only PPP surpassing them in the ranking.[62] Recognizing the increased interest and success of Chinese teams in CTF competitions, SJTU partnered up with Chinese tech giant Tencent to run their own CTF competition, known as 0CTF/TCTF. Nowadays, 0CTF/TCTF is known as one of the world's largest and most difficult CTF competitions.[63]

Between 2016 and early 2017 some changes occurred in the teams. The core members of the original Blue Lotus team reorganized themselves into a new team named the "Tea Deliverers." The Tea Deliverers secured the 5th place in the DEFCON CTF finals in 2017.[64] The 0ops team meanwhile joined forces with the "eee" team (Tencent Keen Security Lab), the "*****" team (Fudan University), and the "AAA" team (Zhejiang University (ZHU)) to create the new Tencent "A*0*E" team. A*0*E placed 3rd in the 2017 DEFCON CTF finals.[65] The Tea Deliverers team and Tencent's A*0*E team steadily solidified their positions in the global CTF rankings.

Between 2017 and 2020, Tencent A*0*E consistently maintained its standing among the top teams, achieving a historic victory at the 2020 DEFCON CTF by surpassing Carnegie Mellon University's PPP team for the very first time.[66] In that same year, the Tea Deliverers secured the 4th place[67] while the Chinese team r3kapig qualified to the finals for the first time, and ranked 14th. Supported by JD.com, China's largest online retailer, r3kapig is conceptualized as a collaborative team that comprises the Chinese team FlappyPig, former champions at XCTF and 0CTF/TCTF, along with a team known as Eur3kA.[68] Eur3kA was established by a former Blue Lotus member – also known as Atum[69] – in collaboration with his classmates at Peking University.[70]

[55] "Blue-Lotus."
[56] "Blue-Lotus."
[57] "Blue-Lotus."
[58] "Blue-Lotus."
[59] "Blue-Lotus."
[60] "0ops" (Teams: CTF Time), accessed October 9, 2023, https://ctftime.org/team/4419.
[61] "B1o0p" (Teams: CTF Time), accessed October 9, 2023, https://ctftime.org/team/23279.
[62] "B1o0p."
[63] jeetesh16, "Top 10 Cyber Hacking Competitions – Capture the Flag (CTF)," *GeeksforGeeks* (blog), February 26, 2024, https://www.geeksforgeeks.org/top-cyber-hacking-competitions-capture-the-flag-ctf/.
[64] "Tea Deliverers" (Teams: CTF Time), accessed October 9, 2023, https://ctftime.org/team/38838/.
[65] "A*0*E" (Teams: CTF Time), accessed October 9, 2023, https://ctftime.org/team/38901/.
[66] "A*0*E."
[67] "Tea Deliverers."
[68] "R3kapig," *R3kapig* (blog), n.d., https://r3kapig.com/.
[69] "Guancheng Li (李冠成)," *NISL@THU* (blog), n.d., https://netsec.ccert.edu.cn/people/atum.
[70] 木子Yanni, "R3kapig：校园明星 CTF 战队的奇幻养成之旅," *Zhihu* (blog), July 24, 2020, https://zhuanlan.zhihu.com/p/163375485.

In 2018 and 2019, DEFCON hosted two events in Beijing, known as “DEFCON China [Beta]” and “DEFCON China 1.0.” The initiative to bring DEFCON to China was spearheaded by Ma Jie, who at the time served as the head of the Security Division at the Chinese tech giant Baidu.[71] Baidu, which had previously collaborated with and sponsored the Blue Lotus team, also managed the CTF competition featured in both events.[72] At the 2019 edition, the top spot was claimed by the Japanese team TokyoWesterns, with the Russian team LC↯BC securing the 2nd position. Chinese teams A*0*E and Never Stop Exploiting (University of the Chinese Academy of Sciences) achieved the 3rd and 5th rankings, respectively.[73]

Between 2021 and 2022, the A*0*E team started to compete under the name "Katzebin," securing 1st place at DEFCON CTF in 2021, and 2nd at DEFCON CTF 2022.[74] The Chinese team r3kapig secured the 15th and 12th place, while Tea Deliverers ranked 3rd in 2021, marking the latter’s last participation in the event.[75] In both years, a new team named “Nu1L” entered the finals, placing 7th in both years.

Established in 2015, Nu1L claims a membership exceeding 90 individuals, hailing from prestigious institutions like THU, Peking University, and Shanghai University of Science and Technology, as well as major domestic security firms such as Alibaba, Tencent, and Huawei.[76] In 2018, Nu1L established its own Jeopardy-style contest, named N1CTF.

In 2023, DEFCON altered its rules, decreasing the number of finalist teams from 15 to 12. This measure incentivized participation through collaborations among various teams. Chinese teams equally entered the competition through various international partnerships. These teams included "P1G_BuT_S4D," which joined forces between r3kapig and the Russian team "C4T BuT S4D"[77]; "Blue Water," a collaboration between Tea Deliverers, pb_ctf, Water_Paddler, and Samsung Research; and "Straw Hat," which brought together Nu1L, W&M, and other independent researchers not based in China, including participants from U.S.-based Northwestern University. [78] These teams ranked respectively 2nd, 5th and 7th.

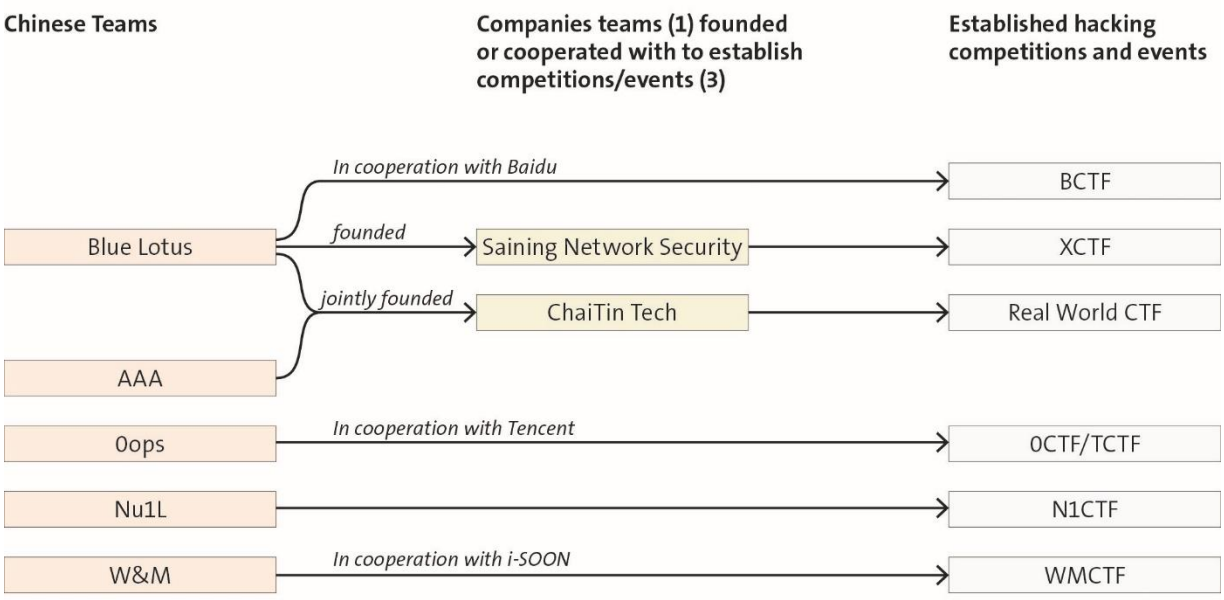
W&M, a Chinese team result of a merger between the MxM and W&P teams, comprises both students and professionals. It's difficult to discern the specific universities and companies associated with the members of W&M or determine when the team was founded based on their website. W&M established its own competition in 2020, named WMCTF. The 2023 WMCTF edition was supported by i-SOON as the primary sponsor, the government-contracted firm whose extensive espionage activities were exposed in early 2024.[79] The WMCTF website clarifies that it has “no other affiliations” and none of its members are employed by i-SOON (figure 5). Although this assertion couldn't be verified in this report, this collaboration represents the closest connection between a top-performing team at DEFCON CTF and Chinese state-sponsored espionage efforts.

Figure 5: 2023 WMCTF Website Homepage

Source: https://wmctf.wm-team.cn/

[71] 玄宁, “百度马杰谈引入DEF CON：中美是世界安全社区的两极,” *Pingwest*, August 22, 2018, https://www.pingwest.com/a/176301.
[72] Liu Zheng, “US Hackers’ Carnival Shows China’s Strength in Cyberspace Protection,” *China Daily*, October 8, 2016, https://global.chinadaily.com.cn/usa/business/2016-08/10/content_26420173.htm.
[73] “BCTF 2019 Finals” (Teams: CTF Time), accessed October 9, 2023, https://ctftime.org/event/831.
[74] “Katzebin” (Teams: CTF Time), accessed October 9, 2023, https://ctftime.org/team/141539/.
[75] “Tea Deliverers.”
[76] “Nu1L Team,” *Nu1L Team* (blog), accessed December 2, 2024, https://www.nu1l.com/.
[77] “P1G_BuT_S4D” (Teams: CTF Time), accessed October 9, 2023, https://ctftime.org/team/268242/.
[78] “Straw Hat,” *Straw Hat* (blog), n.d., https://strawhat.team/.
[79] “Homepage,” *W&M* (blog), n.d., https://wm-team.cn/.

Figure 6: Impact of DEFCON CTF Champions on China's CTF Ecosystem



Source: Compiled by the Author

In summary, since the early 2010s, prominent Chinese universities have actively nurtured their students' talents to excel in the DEFCON CTF competition, resulting in a growing number of outstanding achievements. Early Chinese participation, spearheaded by THU's Blue Lotus team, swiftly gained momentum as other universities and companies followed suit. These teams have played a pivotal role in shaping the cybersecurity landscape in China itself. They established some of the world's premier CTF competitions (figure 6) and began to offer incentives to Chinese students for cultivating their own hacking skills. Retired team members often created their own cyber security startup, providing niche digital services, such as cyber ranges and automated vulnerability discovery systems, to companies and government agencies alike.

As the nurturing of Chinese cybersecurity talent advances, universities and CTF competitions naturally establish a talent pipeline and domestic capability that Chinese defense and security agencies can tap into. In China this is particularly pronounced due to the government's MCF strategy, which blurs the lines between civilian and military research and application.

Indeed, Chinese universities have been linked to Chinese state-sponsored cyber espionage activities.[80] The universities associated with sending teams to participate at DEFCON CTF are no exception to this.

4.2.1 C9 League

Chinese DEFCON CTF participation is to a large degree an undertaking by a small number of technical universities – namely THU, SJTU ZHU, and Fudan University – within what is known as the C9 League (九校联盟). The C9 League is made up of nine elite Chinese universities (figure 7) that are given preferential treatment by the state as part of the Chinese Communist Party's Project 985 initiative. Founded in 1998, Project 985 is designed to efficiently allocate regional and national resources to selected universities to improve existing infrastructure, develop research centers, and to conduct international events.[81] Members of the C9 League thus receive substantial financial and political support from Beijing and local governments.[82]

To put this in numbers: The C9 League members host a mere 3% of China's research scholars but receive

[80] Insikt Group, "Chinese Cyberespionage Originating From Tsinghua University Infrastructure," August 16, 2018, https://www.recordedfuture.com/blog/chinese-cyberespionage-operations.

[81] Ryan Miller, "5 Things You Should Know About The C-9 Universities In China," *CEOWORLD Magazine*, May 17, 2022, https://ceoworld.biz/2022/05/17/5-things-you-should-know-about-the-c-9-universities-in-china/.

[82] Ryan Miller.

10% of the China's national research budget and produce 20% of cited academic papers in China.[83] They are also given priority for grants and other privileges. Admission to a C9 university is highly competitive and considered a mark of excellence. According to the U.S. News Rankings, THU, SJTU, and ZHU rank among the top 15 universities globally in the field of computer science.[84]

Figure 7: C9 League (From left to right: Fudan University, Harbin Institute of Technology, Nanjing University, Peking University, Shanghai Jiao Tong University, Tsinghua University, University of Science and Technology of China, Xi'an Jiaotong University, Zhejiang University)

Source: https://tribe.cucas.cn/article/116

Like other Chinese universities, The Ministry of Education oversees the C9 League. Yet, the league members (except for Fudan University) also belong to a small group of universities that are overseen by MIIT and the State Administration of Science, Technology, and Industry for National Defense (SASTIND).[85] SASTIND mission is to transform the educational institutions it partners with into "universities with national defense characteristics" by expanding their engagement in defense technology training and research while deepening their collaboration with Chinese defense companies.[86] This includes supporting the establishment of defense research laboratories, funding research areas related to defense, and facilitating their involvement in military projects.

The following subsections will examine the teams which have successfully competed at DEFCON CTF over the past decade. This includes THU's Blue Lotus, SJTU's 0ops, and ZHU's AAA teams, each comprising between 20 and slightly over 40 members in any given year, as per the CTFtime database. Fudan University, despite being a C9 member itself, will not be included in the analysis due to its lower cyber risk profile. To date it has not been publicly connected to any Chinese state-sponsored cyber operations.

4.3 Blue Lotus & Tea Deliverers – Tsinghua University

Tsinghua University (清华大学) is considered China's top-ranking university in the field of science and technology. Often described as "China's MIT,[87]" THU is ranked 1st globally in Computer Science, according to the 2024 U.S. News Rankings.[88] This academic powerhouse oversees a comprehensive network of over 390 research institutions, including eight major defense laboratories which are pivotal in conducting classified research and development to support military advancements in the fields of, quantum physics, and nuclear technology. [89]

Each year, hundreds to thousands of THU students are funded by China's defense industry conglomerates.[90] In 2020, THU and the PLA's Academy of Military Science launched a program for the joint training of doctoral students in the computer science field. This makes the university a fertile recruitment ground for the PLA and other Chinese government agencies.[91] While collaborations between universities and the defense sector are not uncommon in Western countries, the Chinese system goes a bit further. For example, the government will assess universities and their personnel for patriotic education and ideological adherence. As such, THU – and the other C9 League members – place significant emphasis on being both "Red and Expert[s]," a concept that emphasized in its annual budget report.[92]

[83] "What Is C9 League?," *China International School Service* (blog), n.d.

[84] "Best Global Universities for Computer Science," *U.S. News & World Report* (blog), n.d., https://www.usnews.com/education/best-global-universities/computer-science.

[85] Alex Joske, "The China Defence Universities Tracker," *ASPI* (blog), November 25, 2019, https://www.aspi.org.au/report/china-defence-universities-tracker.

[86] Alex Joske.

[87] MIT stands for Massachusetts Institute of Technology, based in the US. Renowned worldwide for its laboratory instruction, the MIT focuses on programs in applied science and engineering. It has been ranked as the No. 1 university in the world by QS World University Rankings for 11 straight years.

[88] "Best Global Universities for Computer Science."

[89] "Tsinghua University, Prospective Researchers," *Facilities* (blog), n.d., https://www.tsinghua.edu.cn/publish/thu2018en/newthuen_cnt/03-research-2.html.

[90] ASPI, "Tsinghua University" (Universities: China Defence Universities Tracker, n.d.), https://unitracker.aspi.org.au/universities/tsinghua-university/.

[91] ASPI.

[92] Ryan Fedasiuk, Alan Omar Loera Martinez, and Ryan Fedasiuk, Alan Omar Loera Martinez, and Anna Puglisi, "A Competitive Era for China's Universities: How Increased Funding Is Paving the Way" (Center for Security and Emerging

In 2018, Chinese state-sponsored network reconnaissance activities were linked to infrastructure associated with THU. The activities were aimed against targets in Alaska, Kenya, Brazil, and Mongolia during times of economic dialogue and publicity related to China's investments in foreign infrastructure projects.[93] As of this writing, it is unknown whether Blue Lotus team members are involved in the Chinese state-sponsored cyber espionage operations. That being said, in recent years, THU has entered several research partnerships with prominent Chinese cybersecurity companies that have in turn been (a) involved in state-sponsored cyber espionage campaigns or (b) are known for providing Chinese government agencies with zero-day vulnerabilities. These include Qihoo 360, Qi An Xin, NSFOCUS, and Saining Network Security.[94] Among other subject matters, THU's cooperative research efforts with these entities includes software vulnerability analysis. This might indicate that THU students could contribute to the vulnerability research at these companies, whose result would in turn likely contribute to the evaluation of vulnerabilities for the potential application in state-sponsored cyber operations.

In 2010, THU's Blue Lotus team was founded by three professors hailing from Tsinghua's Network and Information Security Laboratory.[95] As previously noted, the Blue Lotus team's achievements had a profound influence on the CTF competition culture in China. However, the most immediate result was the influence these successes had on fellow Chinese students. In the early stages of Blue Lotus' success, the team became so well-known that students from other universities, including ZHU and SJTU, sought to join the team. Due to the team's maximum size of 20 members, only one to two new students were able to join every year.[96] While some non-THU students were allowed to join the team in the beginning, the composition of the Blue Lotus team shifted back to predominantly THU students as more universities formed their own CTF teams.[97]

Between 2013-2014, Blue Lotus joined forces with the Baidu Research Institute to establish the Baidu CTF (BCTF) competition. BCTF was the first Chinese CTF competition that adopted the Attack-Defense format.[98] BCTF attracted participation from over 2,500 individuals, emerging as the largest network security competition in the country at the time.[99] In 2018 and 2019, BCTF took place in Beijing as part of DEFCON China [Beta] and DEFCON China 1.0.

Figure 8: DEFCON China 1.0 Banner Ad (2019)

Source: DEF CON China 1.0 X Account

From 2014 to 2015, Blue Lotus then spearheaded the founding of the XCTF International League, an Attack-Defense style CTF competition hosted by Nanjing Saining Network Security.[100] At its inaugural event, XCTF reportedly attracted 3,847 teams and over 10,000 participants, surpassing BCTF by a significant

Technology (CSET), March 2022), https://cset.georgetown.edu/wp-content/uploads/CSET-A-Competitive-Era-for-Chinas-Universities.pdf.

[93] Insikt Group, "Chinese Cyberespionage Originating From Tsinghua University Infrastructure."

[94] "Tsinghua University Network Research Institute," *Cooperating Institutions* (blog), n.d., https://www.insc.tsinghua.edu.cn/jgsz/hzjg__/qhdxwlyjy_qaxkjjtgfyxgswlaqlhyjzx.htm.

[95] "蓝莲花（Blue-Lotus）战队," *Secspace* (blog), n.d., https://www.secspace.com/list-e16719b83484491394df617bd6c6dbeb.html.

[96] "回顾XCTF的前世今生," *Education Info* (blog), June 7, 2016, https://www.edu.cn/xxh/ji_shu_ju_le_bu/wlaq/cptj/201607/t20160706_1426992.shtml.

[97] "回顾XCTF的前世今生."

[98] Baidu, "蓝莲花战队," *Baidu* (blog), accessed October 9, 2023, https://baike.baidu.com/item/%E8%93%9D%E8%8E%B2%E8%8A%B1%E6%88%98%E9%98%9F/16066819.

[99] Baidu.

[100] "Jianwei Zhuge (诸葛建伟)," *NISL@THU* (blog), accessed October 9, 2023, https://netsec.ccert.edu.cn/people/zhugejw/.

margin. In the second edition, the XCTF International League drew participation from over 20,000 teams, including the then top 10 ranked CTF teams in the world, and more than 40,000 individuals.[101] In 2017, Saining Network Security claimed that XCTF became "the world's second and Asia's first cyber security competition."[102]

In 2016, Blue Lotus' most senior members established a new team, named the Tea Deliverers, in the hopes of improving their performance at DEFCON CTF, where Blue Lotus placed 5th in the previous year. Between 2017 to 2021, the Tea Deliverers ranked each year in the top 6 of the DEFCON CTF finals. With the senior members performing independently, THU stood up a team named "Redbud," which is specifically geared toward skill enhancement and learning, rather than winning a CTF competition.[103] As such, Redbud serves as a platform for young THU students to practice their technical abilities and interact and learn from more accomplished CTF players. The team also serves as a talent pool and substitute bench the Blue Lotus and Tea Deliverers team can tap into.

The most distinguished Blue Lotus and the Tea Deliverers alumni went on to establish their own IT security companies.[104] These include Nanjing Saining Network Security and StarCross Technology.

4.3.1 Nanjing Saining Network Security & StarCross Technology

Nanjing Saining Network Security, also known as Cyber Peace (赛宁网安), was established in Nanjing in 2013 by a former Blue Lotus member.[105] Within the Chinese CTF community, Saining is probably most well-known for sponsoring and organizing XCTF.[106] Over the years, the company has transitioned from being the primary promoter and organizer of XCTF to specializing in delivering software and hardware security solutions. It has a particular emphasis on cyber ranges, including those based on digital twin technology. A cyber range digital twin is a virtual representation of a network or cyber system created to simulate and test its behavior in a controlled environment.[107] Similar to traditional digital twins, which replicate real-world objects, this concept allows organizations to monitor and optimize their network's performance without risking damage to the actual system.

According to a 2021 article by Sohu.com, Saining is aiming to become "the world's number one brand of cyber shooting ranges."[108] The company has clientele and partnerships with military and intelligence agencies. According to the company's own website, its products have received recognition from military customers, although the specific military organizations involved are not explicitly mentioned.[109] Saining also serves as technical support unit (TSU) for the MSS-operated CNNVD vulnerability database.[110]

As reported by Sohu.com, the foundation of Saining Network Security's core technology research and development is deeply rooted in its close relationship with THU and the Blue Lotus team, leveraging a vast and influential network of expertise.[111] According to PitchBook.com's financial database and techinasia.com, a technology news site, Saining employs up to 200 individuals[112] and carries an estimated overall valuation of 62 million USD.[113] Sohu.com also notes that many of its key technical talents have previously held significant roles at industry giants like ZTE, Huawei, Alibaba, and Microsoft. The company has established partnerships with renowned corporations and government entities, encompassing but not limited to Huawei, TikTok's Bytedance, China Mobile Group, Telecom Group, State Grid, and China Resources Group.[114]

[101] "Jianwei Zhuge (诸葛建伟)."
[102] "Company Profile," *Cyber Peace* (blog), n.d., http://www.cyberpeace.cn/index.php/category/about/gongsijs/?rwNmOdr=1707237032620.
[103] "2020 WCTF 前瞻：顶级强队网络'沙场'练兵，猝火成刚问鼎'网战之巅,'" *CNWEST*, November 18, 2020, http://m.cnwest.com/xysd/a/2020/11/18/19293332.html.
[104] 王宏伟, "网络安全：'小巨人'守护'第五疆域,'" *JN Times* (blog), May 20, 2022, https://www.jntimes.cn/jsnj/202205/t20220520_7550192.shtml.
[105] "Company Profile."
[106] "公司介绍," *Cyber Peace* (blog), n.d., http://www.cyberpeace.cn/?rwNmOdr=1706696807331.
[107] "Cyber Ranges and Digital Twins," *CYBEXER* (blog), July 2, 2024, https://cybexer.com/resource-center/cyber-ranges-and-digital-twins/.
[108] "XCTF联赛背后，「赛宁网安」从攻防双视角培育网络安全人才," *SOHU*, April 3, 2021, https://www.sohu.com/a/453895498_403354.
[109] "Saining Wangan" (Organization: Crunchbase), accessed October 9, 2023, https://www.crunchbase.com/organization/saining-wangan.
[110] Dakota Cary and Kristin Del Rosso, "Sleight of Hand: How China Weaponizes Software Vulnerabilities."
[111] "XCTF联赛背后，「赛宁网安」从攻防双视角培育网络安全人才."
[112] "CyberPeace Overview," *PitchBook* (blog), accessed July 2, 2024, https://pitchbook.com/profiles/company/434314-72#overview.
[113] "Cyber Peace (赛宁网安)," *Tech in Asia* (blog), accessed July 2, 2024, https://www.techinasia.com/companies/cyber-peace.
[114] "XCTF联赛背后，「赛宁网安」从攻防双视角培育网络安全人才."

Saining Network Security has also partnered with prestigious domestic universities, including THU, Nanjing University, and Fudan University. These partnerships included the development of six cybersecurity courses covering areas such as hacking competition skills and vulnerability mining.[115] This training package reportedly comprised more than 1,200 hours of original, high-quality courses and incorporates over 3,000 practice questions, facilitating the integration of theoretical knowledge with practical application during training and testing.[116]

Saining has also been forging partnerships globally. These collaborations extend to countries such as Singapore, Chile, Saudi Arabia, Algeria, Pakistan, and over 10 nations associated with the Belt and Road initiative. It is unclear whether Saining's global partnerships are with foreign private companies, government agencies, or both.

StarCross Technology, also known as Xinglan Technology (星阑科技), is a cybersecurity startup that was established in Beijing in 2018 by a former Blue Lotus member.[117] StarCross specializes in securing application programming interfaces (APIs), employing AI for situation awareness, monitoring, and emergency response solutions to protect companies from cyber threats. Among its main products is a fully automated Intelligent Vulnerability Discovery System.[118] As per the company's website, this system can autonomously detect vulnerabilities across different business scenarios, eliminating the necessity for manual intervention. Although specific details about its partnerships and collaborations are not disclosed, StarCross, like Saining Network, is a technical support unit (TSU) of the MSS-operated CNNVD.[119]

According to PitchBook, Starcross employs around 70 individuals[120] (although other sources report higher numbers[121]), including former members of Blue Lotus, Tea Deliverers and r3kapig. While no official estimated overall valuation is reported, the company claims to be worth over 60 million USD on its LinkedIn profile.[122] In 2021 alone, StarCross Technology raised more than 15 million USD from investors led by China's Apple Funds.[123] Testament to the company's recognition, Starcross' founder earned a place in the 2023 Enterprise Technology category of Forbes' 30 Under 30 Asia list.[124]

4.4 0ops – Shanghai Jiao Tong University

Much like THU, Shanghai Jiao Tong University (上海交通大学) is one of China's most prestigious universities, renowned for nurturing top engineers and scientists.[125] It ranks 13th globally in Computer Science, according to the U.S. News Rankings.[126] SJTU engages extensively in collaborative defense projects with various Chinese government agencies.[127] It hosts three major defense laboratories and has several links to the PLA, including through its signing of a research cooperation agreement with the Academy of Military Science in 2014.

Reports indicate a high degree of SJTU's participation in Chinese state-sponsored cyber espionage activities.[128] In a 2022 testimony before the U.S.-China Economic and Security Review Commission on China's cyber capabilities, Dakota Cary stated that "the deepest entanglement between university faculty and the security services is with schools like SJTU – where staff

115 "Practical Training Services," *Cyber Peace* (blog), n.d., http://www.cyberpeace.cn/index.php/category/gkbc/sxqt/?rwNmOdr=1707295135917.
116 "XCTF联赛背后，「赛宁网安」从攻防双视角培育网络安全人才."
117 "Wang Yu," *Forbes 30 Under 30 Asia: Enterprise Technology* (blog), n.d., https://www.forbes.com/30-under-30/2023/asia/enterprise-technology?profile=wang-yu.
118 "About Us," *Starcross Technology* (blog), n.d., https://en.starcross.tech/aboutus/index.jhtml.
119 Dakota Cary and Kristin Del Rosso, "Sleight of Hand: How China Weaponizes Software Vulnerabilities."
120 "Starcross Technology Overview," *PitchBook* (blog), accessed July 2, 2024, https://pitchbook.com/profiles/company/483894-19.
121 "StarCross Technology (Xinglan Technology)," *Crunchbase* (blog), n.d., https://www.crunchbase.com/organization/xinglan-technology.
122 "StarCross Technology (星阑科技)," *LinkedIn* (blog), accessed July 2, 2024, https://www.linkedin.com/company/beijing-starcross-technology/?trk=ppro_cprof&originalSubdomain=au.
123 "Wang Yu."
124 "Wang Yu."
125 "Tsinghua University" (Universities: U.S. News & World Report Best Colleges Ranking, October 9, 2023), https://www.usnews.com/education/best-global-universities/computer-science.
126 "Best Global Universities for Computer Science."
127 ASPI, "Shanghai Jiao Tong University" (Universities: China Defence Universities Tracker, n.d.), https://unitracker.aspi.org.au/universities/shanghai-jiao-tong-university/.
128 Dakota Cary, "Academics, AI, and APTs" (Center for Security and Emerging Technology (CSET), March 2021), https://cset.georgetown.edu/publication/academics-ai-and-apts/.

both support operations and conduct research to enhance cyber capabilities."[129] As early as 2010, an investigation into Operation Aurora, a cyber campaign that targeted Google and several other American companies, traced the origins of these intrusions to computers at SJTU.[130]

SJTU faculty members have also co-authored technical research papers with members of PLA Unit 61398, also known as APT1, on topics related to computer network security and intrusion detection.[131] A 2013 Reuters investigation accused SJTU's School of Information Security Engineering – which hosts the 0ops team[132] –of providing direct support to the cyber operations of PLA Unit 61398.[133] The same investigation also uncovered that SJTU's Department of Computer Science and Engineering – which reportedly conducted research with another unspecified PLA Unit – sits right across the street from the National Information Security Engineering Center, a building commissioned in 2003 by PLA Unit 61398 (APT1).[134] In 2014, The New York Times reported that one of the hackers affiliated with Unit 61398 had utilized his SJTU university email address to register a web domain used in several malicious cyber operations.[135]

In his report titled "Academics, AI, and APTs," Dakota Cary emphasized the involvement of another SJTU-affiliated entity in Chinese cyber operations, known as the Cyberspace Security Science and Technology Research Institute. The Institute's Network Confrontation and Information System Security Testing project covers items such as APT attack testing and defense. The project's research priorities also show a specific emphasis on crafting technologies tailored for APT cyber operations, alongside password cracking and social engineering.

Lastly, SJTU operates its own vulnerability database, i.e. the Higher-Ed Vulnerability Database, which collects vulnerability reports from a range of sources, including submissions from Chinese researchers, professors, and university students.[136] These reports largely cover products that are utilized by all institutions under the supervision of China's Ministry of Education. It is believed that ultimately, these reports will find their way to the MSS.[137]

SJTU serves as the home base for the 0ops team, established in 2013. The team gained prominence through its success in the hacking competition CodeGate2015 (South Korea), becoming the first Chinese team to secure an international CTF championship. 0ops also participated in the 2015 DEFCON CTF finals and placed 6th. From 2016 onwards, 0ops formed a strategic partnership by jointly competing with Tencent's eee team at the DEFCON CTF finals. A key legacy of this collaboration was the creation of the 0CTF/TCTF competition in 2017. Since 2017, 0CTF/TCTF has attracted more 5,000 teams from across the globe, including the US, Russia, Japan, Poland, South Korea, and Germany.[138] This partnership also functions as a significant talent pipeline from SJTU to Tencent vulnerability research labs, known for providing government agencies with zero-day vulnerabilities.[139] Many of the most distinguished SJTU and 0ops alumni work for Tencent Keen Security Lab.[140] An unnamed former 0ops team captain serves as a senior security expert at Qi An Xin's Pangu Laboratory.[141] No Chinese cybersecurity startups relevant to this report have been founded by 0ops alumni.

[129] Melanie Lee, "Top China College in Focus with Ties to Army's Cyber-Spying Unit" (Center for Security and Emerging Technology (CSET), February 17, 2022), https://www.uscc.gov/sites/default/files/2022-02/Dakota_Cary_Testimony.pdf.

[130] David Barboza, "Hacking Inquiry Puts China's Elite in New Light," *The New York Times*, February 21, 2010, https://www.nytimes.com/2010/02/22/technology/22cyber.html.

[131] Melanie Lee, "Top China College in Focus with Ties to Army's Cyber-Spying Unit."

[132] "上海交通大学0ops战队：每场比赛都是挑战自我的出征," January 18, 2019, https://m.sohu.com/a/290027957_278960/?pvid=000115_3w_a.

[133] Melanie Lee, "Top China College in Focus with Ties to Army's Cyber-Spying Unit."

[134] Melanie Lee.

[135] Nicole Perlroth, "2nd China Army Unit Implicated in Online Spying," *The New York Times*, September 6, 2014, https://perma.cc/6PFZ-NFHZ.

[136] Dakota Cary and Kristin Del Rosso, "Sleight of Hand: How China Weaponizes Software Vulnerabilities."

[137] Dakota Cary and Kristin Del Rosso.

[138] "'产学研用'重磅升级，第六届TCTF决赛定档12月7号！," *Tencent Security Joint Laboratory* (blog), November 22, 2023, https://mp.weixin.qq.com/s/ZNdoa68EYPCDcspXFopI8g.

[139] Dakota Cary and Kristin Del Rosso, "Sleight of Hand: How China Weaponizes Software Vulnerabilities."

[140] 藏青, "当天才CTF选手们退役后 有的人在另外一个赛场开始了新的博弈," *安全419*, May 7, 2021, http://www.anquan419.com/news/17/559.html.

[141] 藏青.

4.5 AAA – Zhejiang University

Zhejiang University (浙江大学) ranks 12th globally in Computer Science, according to the U.S. News Rankings.[142] Like THU and SJTU, it stands out for its substantial presence of defense laboratories, close associations with the defense industry, and connections to state-sponsored economic and espionage activities.[143]

A 2012 report, commissioned for the US–China Economic and Security Review Commission, revealed ZHU received funding from the MSS for research in "sensitive research and development with information security and information warfare applications."[144] In 2013, US officials in Milwaukee arrested Huajun Zhao, a cancer researcher from China, on charges related to economic espionage. The FBI's statement implied that Zhao may have leveraged his position at the Medical College of Wisconsin to illicitly obtain patented research material and potentially transferred that material to ZHU.[145] Despite these activities, public reporting has not yet established any direct ties between ZHU and Chinese malicious cyber campaigns.

ZHU's School of Computer Science and Technology hosts the renowned AAA team. Founded in 2012, AAA is the most well-known CTF team in China that has specialized in reverse binary.[146] Its graduates are highly valued by both the Chinese private sector and government bodies, including those involved in state-sponsored cyber espionage activities. ZHU students conduct leading vulnerability research, notably through the university's Ubiquitous Systems Security (USS) Lab.[147] Their research scope encompasses the Internet of Things (IoT) and AI security, as well as autonomous vehicles. Two ZHU students successfully hacked a Tesla Model S at the 2014 SyScan contest in Beijing, earning them a 10.000 USD bounty. ZHU students and USS Lab members are enshrined in the Tesla Security Researcher Hall of Fame for both 2014 and 2016.[148]

The most distinguished AAA alumni have gone on to join leading vulnerability research facilities, such as Huawei's Singular Security Lab and the Tencent Keen Security Lab. Some have also been recruited by governmental entities. In 2013, a Mandiant report characterized ZHU's School of Computer Science and Technology– the department that hosts ZHU's AAA team[149] – as a source for recruiting individuals into PLA Unit 61398 (APT1).[150]

Some other alumni present a different narrative. Former AAA team captain and current Senior Director of Shaechi Security Lab, He Qidan (also known as Edward Flanker) embarked on his academic journey at ZHU at the early age of 15.[151] He gained international fame by achieving victory in Pwn2Own as a part of the Tencent Keen Security Lab Team at the age of 22. During the same period, he actively participated in DEFCON CTF and has been a featured speaker at prestigious hacking conferences such as Black Hat and CanSecWest. In 2020, while employed as Cyber Security Head at Pinduoduo, China's third-largest e-commerce firm after Alibaba and JD.com, there were reports of his forced expulsion from the company after over four years of service.[152] In a Weibo post made in January 2021, he declared his departure from Pinduoduo due to the company's plans to involve him in unlawful actions against his will, a stance he reaffirmed in later posts.

While Pinduoduo did not face any punitive actions by state regulators, several senior researchers expressed

142 "Best Global Universities for Computer Science."

143 "Zhejiang University" (Universities: QS Top Universities, October 9, 2023), https://www.topuniversities.com/universities/zhejiang-university.

144 Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage" (Northorp Grumman Corp, March 7, 2012).

145 FBI Milwaukee, "Foreign Economic Espionage Investigation Leads to Arrest," *The FBI* (blog), February 4, 2013, https://web.archive.org/web/20190722014433/https:/archives.fbi.gov/archives/milwaukee/press-releases/2013/foreign-economic-espionage-investigation-leads-to-arrest.

146 Zheijiang University, "斩获全球最顶级赛事总冠军！浙大这支神秘战队够硬核," *QQ* (blog), November 19, 2020, https://mp.weixin.qq.com/s/6aV8G4fAIpXp0E0xZzsR3A?fbclid=IwAR3VR8KUUurcMNyV-Kl-liNYERPBD8JCRfNjR5QgS-wIZnsSQGzQ0UWG-qI.

147 "Ubiquitous System Security Lab.," *Ubiquitous System Security Lab.* (blog), n.d., https://usslab.org/.

148 "Product Security," *Tesla* (blog), n.d., https://www.tesla.com/legal/security.

149 Zheijiang University, *Facebook* (blog), June 12, 2020, https://www.facebook.com/ZhejiangUniversityChina/posts/congratulations-to-our-team-azure-assassin-alliance-aaa-who-won-this-years-def-c/2824042437838681/.

150 "APT1: Exposing One of China's Cyber Espionage Units" (Mandiant, February 2013), https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf

151 "15岁上浙大、22岁获世界冠军，90后「天才黑客」为何被开除," *SOHU*, January 14, 2021, https://www.sohu.com/a/444208183_827756.

152 "Pinduoduo Cyber Security Head Fired, Rumored for Not Willing to Perform Hacking Activities," *Asia Tech Wire*, February 2, 2021, https://www.asiantechpress.com/pinduoduo-cyber-security-head-fired-rumored-for-not-willing-to-perform-hacking-activities.html.

their anger at Pinduoduo.[153] The former director of Alibaba Group's Security Research Laboratory responded to one of Qidan's posts, stating that "The brilliant hackers in our hacker community, who were wronged by Pinduoduo, deserve hundreds of millions in compensation and bonus options. Capital goes to great lengths to exploit its employees. Entry-level workers are worn out, and technical talents are depleted." The founder of Tencent Keen Security Lab also expressed concerns, mentioning that "During Flanker's tenure at Pinduoduo for over a year, he frequently met and discussed with me after work at night. He disclosed that Pinduoduo's management coerced him into undertaking illegal tasks and created various obstacles for him after he refused... Prior to Flanker's recent departure, he reached out to me again when Pinduoduo created difficulties for him due to his refusal to engage in illegal activities."[154] This instance demonstrated the commitment of China's top-tier hackers to high ethical standards. It remains unclear to what extent this stance extends to national security issues.

Two cybersecurity companies created by AAA alumni are important for this report: Chaitin Tech and Bolean Technology.

4.5.1 Chaitin Tech & Bolean Technology

Chaitin Tech (长亭科技) is a cybersecurity firm founded in Beijing in 2014 by Blue Lotus and AAA alumni.[155] The company focuses on application firewalls and vulnerability scanning, along with providing penetration testing and emergency response services. One of the company's founders is Yusen Chen, former CEO (2016-2021)[156]. He is also the original founder of the AAA team, which he launched during his junior year. Chen was only 23 years old when he gave his first speech at Black Hat in 2015[157], and was listed in Forbes's Asia 30 Under 30 list for Enterprise Technology in 2017. Chaitin has garnered strong recognition in the cybersecurity and technology industry, ranking first in the China Top 100 "Artificial Intelligence and Robotics" companies by Fortune Magazine in 2017 and being included in the Top 25 Global Network Security Leaders by U.S.-based Cyber Defense Magazine.[158]

Towards the end of 2017, after performing at Pwn2Own, Chaitin received directives from the Chinese government to cease further participation in international hacking competitions.[159] In response, the company publicly committed to prioritizing the submission of vulnerabilities to the MSS-operated CNNVD database, for which it now also serves as a technical support unit (TSU).[160] Chaitin also initiated its own global jeopardy-style CTF competition in Beijing in 2018, named Real World CTF[161], which attracts top CTF teams from China and around the world.[162]

In 2019, Chaitin was acquired by Alibaba Cloud – itself a top-tier zero-day supplier to the MSS[163] – while retaining its own brand. As of this writing, Chaitin provides services to multiple Chinese industries and sectors, spanning from finance and internet sectors to government, enterprise, communication, healthcare, education, and various other industries.[164] According to information sourced from the enterprise financial database Crunchbase, Chaitin Tech has a workforce of around 100 employees and holds an estimated value of approximately 19 million USD.[165]

Bolean Technology, also known as Mulian Internet of Things Technology (木链科技), was founded in 2017 in Hangzhou, Zhejiang province, by two former AAA team members.[166] The company focuses on creating

[153] "Who Is the Genius Hacker Flanker? Why Dare to Fight with Pinduoduo?," *iNEWS*, June 2, 2024, https://inf.news/en/tech/af7f5a20c497dee9ee0e87c1d3ac39ff.html.

[154] "Who Is the Genius Hacker Flanker?Why Dare to Fight with Pinduoduo?"

[155] 藏青, "当天才CTF选手们退役后 有的人在另外一个赛场开始了新的博弈."

[156] Saitech Limited, "SAITECH Announces Two New Members to the Board of Directors," *GlobeNewswire* (blog), June 12, 2021, https://www.globenewswire.com/news-release/2021/12/06/2346281/0/en/SAITECH-Announces-Two-New-Members-to-the-Board-of-Directors.html?ref=margin.re.

[157] Saitech Limited.

[158] "Cyber Security Leaders 2017," *Cyber Defense Magazine* (blog), n.d., https://www.cyberdefensemagazine.com/cyber-security-leaders-2017/.

[159] Yingzhi Yang, "China Discourages Its Hackers from Foreign Competitions so They Don't Help Others," *South China Morning Post*, March 21, 2018, https://www.scmp.com/tech/article/2138114/china-discourages-its-cyber-security-experts-global-hacking-competitions?firstTimeRegister=true.

[160] Dakota Cary and Kristin Del Rosso, "Sleight of Hand: How China Weaponizes Software Vulnerabilities."

[161] "Home," *Real World CTF* (blog), n.d., https://realworldctf.com/about.

[162] "Real World CTF 6th" (Teams: CTF Time), accessed October 9, 2023, https://ctftime.org/event/2172/.

[163] Dakota Cary and Kristin Del Rosso, "Sleight of Hand: How China Weaponizes Software Vulnerabilities."

[164] "Network Information Security Firm Chaitin Tech Becomes Holding Subsidiary of Alibaba," *Pandaily* (blog), February 6, 2022, https://pandaily.com/network-information-security-firm-chaitin-tech-becomes-holding-subsidiary-of-alibaba/.

[165] "Chaitin Tech," *Crunchbase* (blog), accessed July 2, 2024, https://www.crunchbase.com/organization/chaitin-tech.

[166] 藏青, "当天才CTF选手们退役后 有的人在另外一个赛场开始了新的博弈."

cybersecurity solutions for industrial control systems (ICS) and offers services in offensive cyber tactics and training, including for participation in CTF competitions.[167] As reported by Chinese cybersecurity news outlet anquan419, Bolean Technology serves clients in various industries, including the defense sector, as well as energy and manufacturing.[168] In particular, it provides defense-oriented industrial control system solutions aimed at safeguarding the production of weapons and military equipment from cyber threats.[169]

According to PitchBook, the company employs up to 150 individuals.[170] It operates its own research laboratory named Friday Lab, which conducts research in the field of ICS cybersecurity. Bolean's technical team, predominantly consisting of members and alumni from ZHU's AAA team[171], relies heavily on expertise in reverse binary to effectively analyze industrial control protocols.[172] According to the Bolean website, the company has "discovered 1000+ vulnerabilities" of which "66 are original vulnerabilities" (the term 'original' likely refers to zero-days).[173] Bolean serves as a technical support unit (TSU) in the MSS-run CNNVD.[174]

[167] "首页," *Bolean* (blog), n.d., https://www.bolean.com.cn/#/product/control-range.
[168] "首页."
[169] "军工行业解决方案," *Bolean* (blog), n.d., https://www.bolean.com.cn/#/solution/military.
[170] "Mulian Internet of Things Technology Valuation & Funding," *PitchBook* (blog), n.d., https://pitchbook.com/profiles/company/432972-10#funding.
[171] 藏青, "当天才CTF选手们退役后 有的人在另外一个赛场开始了新的博弈."
[172] http://www.anquan419.com/news/17/559.html
[173] "首页."
[174] Dakota Cary and Kristin Del Rosso, "Sleight of Hand: How China Weaponizes Software Vulnerabilities."

5 Pwn2Own (2014-2017)

This section traces the history and performance of Chinese hacking teams that participated in Pwn2Own (2014-2017). It specifically examines analyzes the competing teams, their areas of expertise and affiliations with corporate entities, as well as the extent of their involvement in military-civil fusion initiatives aimed at supporting state-sponsored offensive cyber operations.

Key Points

- Chinese winnings at Pwn2Own surged from 13% in 2014 to 79% of the total prize money awarded to all participants. Participants are mostly professionals from companies Qihoo 360 and Tencent.
- Qihoo 360 boasts at least 19 teams and labs spanning various product lines and departments. Tencent hosts 7 to 10 teams and labs organized within one unified department.
- The Pangu Team showcased exceptional skills in Apple mobile hacking, gaining recognition at various international competitions.
- Pangu Team is now part of Qi An Xin, which is deeply connected to China's government agencies. Qi An Xin acted as a primary contractor, competitor, and potential investor for i-SOON.
- Qihoo 360 and Qi An Xin exhibit high integration and involvement in MCF activities. Tencent's relationship with the government has been more strained in recent years.
- In 2018, China barred researchers from attending Pwn2Own in 2018 and initiated the Tianfu Cup, its own equivalent competition.

5.1 Background

The annual hacking competition Pwn2Own was founded in 2007 as part of the CanSecWest conference in Vancouver, Canada. Starting in 2017, Pon2Own was held twice a year, featuring separate events targeting desktops and mobile devices. The competition derives its name from the hacker term "pwn" (pronounced "own"), meaning to compromise or control a computer system. Pwn2Own challenges participants to exploit specific software and operating systems to identify zero-days. Participants attempt to pwn or take control of these software systems by identifying and exploiting weaknesses. What makes Pwn2Own stand out from other competitions in this space is that the hacks are performed against fully patched and up-to-date systems. Hackers therefore have to find innovative ways and leverage previously unknown vulnerabilities to pwn a machine. Pwn2Own is often used to demonstrate new techniques and zero-days to show how a system can be compromised in the here and now. Over the years, Pwn2Own has grown in popularity, attracting talented hackers and security researchers from across the globe. The competition has become a pivotal platform for highlighting the real-world risks associated with software vulnerabilities.

Pwn2Own distinguishes itself by providing substantial cash prizes for successful exploits. Reward details are disclosed before the competition begins and vary based on the targeted software and the severity of the exploits. Over the years, targets have included web browsers, plugins, and operating systems like Windows, macOS, and various mobile platforms. Between 2014-2017, the total prize pool ranged from 460.000 USD to 850.000 USD. From 2018 to 2013, the total prize pool was between 1 million to 2 million USD. Top performers could earn up to 530.000 USD in the contest's 2023 edition.[175]

Pwn2Own is often sponsored by technology companies and organizations interested in enhancing their software's security. These prizes are powerful incen-

[175] "Over $1 Million Awarded in Pwn2Own Hacking Competition," *Trend Micro* (blog), March 27, 2023, 1, https://newsroom.trendmicro.com/2023-03-27-Over-1-Million-Awarded-in-Pwn2Own-Hacking-Competition.

tives for participants to uncover and report vulnerabilities responsibly to the vendors, rather than exploiting them maliciously. In 2015, Pwn2Own was acquired by the Zero Day Initiative, which is part of US cybersecurity company TrendMicro.[176] Pwn2Own has evolved over the years, introducing new target categories, such as Internet of Things (IoT) devices.

In contrast to the gradual ascent of Chinese teams in international CTF competitions, Chinese participants had an immediate impact when they started to participate in Pwn2Own in 2013. While most Chinese teams consist mainly of Chinese citizens, some Chinese teams also included researchers from other countries, such as Australia and Italy. The Chinese teams achieved outstanding results in Pwn2Own, achieving dominance within the span of a few years.

However, the impact was short-lived. In 2017, Chinese cybersecurity firm Qihoo 360's CEO, Zhou Hongyi, publicly expressed concerns about Chinese citizens participating in overseas hacking competitions. He argued that their expertise should stay in China, emphasizing the strategic value of vulnerabilities. The Chinese government subsequently banned Chinese cybersecurity researchers from participating in international exploit competitions such as Pwn2Own, leading to the creation of the Tianfu Cup in Chengdu in November 2018.

5.2 Rise and Fall

In 2013, a Chinese hacking team – known as Keen Team – triumphed in the Mobile Pwn2Own contest (Tokyo, Japan) by successfully breaching Apple iOS version 7.0.3.[177] In 2014, the Keen Team also won the prestigious Pwn2Own contest (Vancouver, Canada) – and secured 115.000 USD in price money (constituting 13% of the total of 850.000 USD won by all contestants[178]) – by leveraging multiple zero-day exploits to breach Apple's Safari 7 browser and Adobe Flash.[179] These milestones firmly established the Keen Team as the first Chinese team to assert dominance in finding zero-day vulnerabilities in both desktop and mobile operating systems.

The Keen Team was led by Wang Qi, the then 37-year-old CEO of the parent company Keen Cloud Tech (Xuhui, Shanghai). His background included prior employment as a technical leader at Microsoft's China security response center, and he held the team to exceptionally high standards. Wang emphasized the rigor of rigid selection and training criteria of its team, comparable to that of corporate tech giants.[180] One of their standout members, Chen Liang, claimed to have locked himself in a rented room for two months to remove all potential distractions to conduct intensive code analysis for Windows 8.1, Adobe Flash, and Apple's Safari in preparation of the Pwn2Own competition.[181] Chen's commitment bore substantial rewards, as he managed to hack each of the three programs.[182]

The Keen Team's co-founder and COO of Keen Cloud, Lu Yiping, shared insights into their team composition with VICE's tech outlet Motherboard. Half of the members were top scorers in the national college entrance examination and specialized in mathematics. Their backgrounds included esteemed educational institutions like SJTU and Fudan University, and professional experience at tech giants such as Microsoft and Tencent. This diverse blend of talent formed the core of the Keen Team.[183]

Bolstered by the team's growing success, the Keen Team established GeekPwn, an event modeled after Pwn2Own, which focuses on the security smart-life devices and AI.[184] First held in Beijing in 2014 and continuing today under the name GeekCon, this annual event was established during a period when Chinese tech enterprises and manufacturers still did

[176] "THE ZDI MISSION," *Zero Day Initiatuve, About ZDI* (blog), n.d., https://www.zerodayinitiative.com/about/.

[177] Swati Khandelwal, "The Keen Team - Chinese Hacker Group Reveals Their Identities," *The Hacker News*, April 17, 2014, https://thehackernews.com/2014/04/the-keen-team-chinese-hacker-group.html.

[178] Liam Tung, "Pwn2Own: 14 Browser and Plugin Exploits the NSA Won't Be Buying," *ZDNET*, March 14, 2014, https://www.zdnet.com/article/pwn2own-14-browser-and-plugin-exploits-the-nsa-wont-be-buying/.

[179] Jamie Fullerton, "The Chinese Hackers Who Are Actually Not Trying to Hack You," *Vice News*, April 20, 2015, https://www.vice.com/en/article/ypwkvk/meet-the-keen-team.

[180] Jamie Fullerton.

[181] Jamie Fullerton.

[182] Jamie Fullerton.

[183] Liu Jiayi, "Top Chinese Hacking Team Reveals Members' Identities," *ZDNET*, April 16, 2014, https://www.zdnet.com/google-amp/article/top-chinese-hacking-team-reveals-members-identities/.

[184] "GeekPwn," accessed October 9, 2023, https://2015.geekpwn.org/en/.

not view hackers in a positive light.[185] At that time, most of these companies declined invitations to participate in hacking competitions, fearing reputational damage. Some even made efforts to disrupt GeekPwn's inaugural event.[186]

Figure 9: The Keen Team at Pwn2Own 2014

Source: https://thehackernews.com/2014/04/the-keen-team-chinese-hacker-group.html

The Keen Team was not the sole contributor to China's rise during that time. At the China-based 2014 SyScan +360 security conference, sponsored by the Chinese cybersecurity giant Qihoo 360, two ZHU students successfully penetrated the electronic system of a Tesla Model S electric vehicle. They gained control over essential functions, such as door locks, horn, wipers, headlights, and sunroof.[187]

Qihoo 360's Vulcan team entered Pwn2Own for the very first time in 2015. It breached Internet Explorer 11 and cracked Google Chrome, resulting in a 110.000 USD payout.[188] In 2015 the Keen Team was joined by members of the Tencent PC Manager team. Six hours into the competition, reports of victories flooded in. The Keen Team conquering Adobe Reader, Adobe Flash, and gained user privileges to Windows' font system. These achievements translated into a grand total of 125.000 USD.[189]Within the span of just three years, the Keen Team became the world's first to "pwn" both Apple and Microsoft desktop operating system. In total, the Chinese teams won 42% (235.000 USD) of the 557.000 USD large overall prize pool.[190]

Following this achievement, the Keen Team and Tencent PC Manager formally merged into the Tencent Keen Security Lab. Pwn2Own's 2015 edition marked the participation of two of China's most prominent tech giants, Qihoo 360 and Tencent, highlighting growing Chinese national interests and expanded capabilities in the field of critical vulnerability research and exploitation.

After fully absorbing the Keen Team, Tencent entered Pwn2Own 2016 with three teams: Tencent Security Team Shield (from the Tencent Keen Security Lab), Tencent Security Team Sniper (also from the Tencent Keen Security Lab), and Tencent Security Xuanwu Lab.[191] These teams demonstrated exceptional talent, with Tencent Security Team Shield successfully exploiting Apple's Safari browser to achieve root-level code execution, earning them 40.000 USD.[192] Meanwhile, Tencent Security Team Sniper carried out a hack against Adobe Flash Player on Windows for which they received 50.000 USD.[193] Xuanwu Lab's attempt to exploit Adobe Flash in Microsoft Edge but failed. Overall, Tencent Security Team Sniper earned the title of "Master of Pwn" and a total prize pool of 142.500 USD.[194] Qihoo's 360 Vulcan Team also participated and secured 132.500 USD by demonstrating two exploits for Adobe Flash and Google Chrome, respectively.[195] In total, Chinese teams won 68% (315.000 USD) of the 460.000 USD large prize pool.[196]

[185] Shanghai Observer, "White Hat, Black Hat: Bringing Hackers Out of the Shadows," *Sixth Tone* (blog), January 15, 2024, https://www.sixthtone.com/news/1014449.

[186] Shanghai Observer.

[187] Seth Rosenblatt, "Chinese Hackers Take Command of Tesla Model S," *CNET*, July 17, 2014, https://www.cnet.com/news/privacy/chinese-hackers-take-command-of-tesla-model-s/.

[188] Steven Vaughan-Nichols, "Pwn2Own 2015: The Year Every Web Browser Went Down," *ZDNET*, March 23, 2015, https://www.zdnet.com/article/pwn2own-2015-the-year-every-browser-went-down/.

[189] Jamie Fullerton, "The Chinese Hackers Who Are Actually Not Trying to Hack You."

[190] Jaikumar Vijayan, "All Four Major Browsers Hacked in Pwn2Own Competition," *Security Intelligence*, March 25, 2015, https://securityintelligence.com/news/four-major-browsers-hacked-pwn2own-competition/.

[191] Lucian Constantin, "Safari, Chrome and Flash Player Hacked at Pwn2Own, Some of Them Twice," *COMPUTERWORLD*, March 17, 2016, https://www.computerworld.com/article/3045658/safari-chrome-and-flash-player-hacked-at-pwn2own-some-of-them-twice.html.

[192] Lucian Constantin.

[193] Lucian Constantin.

[194] Lucian Constantin.

[195] 360TS, "360Vulcan Team Hacked Google Chrome within 11 Minutes in Pwn2Own 2016," *360 Blog* (blog), March 21, 2016, https://blog.360totalsecurity.com/en/360vulcan-team-hacked-google-chrome-within-11-minutes-in-pwn2own-2016/.

[196] Eduard Kovacs, "Pwn2Own 2016: Hackers Earn $460,000 for 21 New Flaws," *Security Week*, March 18, 2016, https://www.securityweek.com/pwn2own-2016-hackers-earn-460000-21-new-flaws/.

Figure 10: Tencent Security Team Sniper at Pwn2Own 2016

Source: https://twitter.com/thezdi/status/710615726004969472

The newly established Tencent Keen Security Lab also earned 215.000 USD in Pwn2Own's 2016 Mobile contest, successfully hacking Apple's iPhone 6S and Google's Nexus 6P phones despite these products' stringent security measures.[197] This feat further confirmed the Keen Lab's dominant role in hacking both desktop and mobile operating systems, with a focus on cutting-edge security research encompassing mainstream PC and mobile operating systems, applications, cloud computing technologies, and IoT devices, among others.

As Tencent's performance in hacking competitions in 2015 dramatically improved, Qihoo 360 held its ground. At the newly launched 2016 PwnFest hacking competition in Seoul, South Korea, Qihoo 360's Alpha team accomplished to breach the security protocols of Google's Android smartphone, the Google Pixel, in record time, winning them a 120.000 USD cash prize.[198] By the event's conclusion, the Qihoo 360 hackers were crowned "Lords of Pwn," amassing a total sum of 520.000 USD by showcasing an additional vulnerability within Microsoft Edge browser on Windows 10, along with identifying a vulnerability within Adobe Flash.[199]

2016 PwnFest also saw the entry of a new Chinese team named Team Pangu. Pangu gained online fame for releasing a million-dollar Apple's iPhone iOS jailbreak for free. Jailbreaking iOS was quite impressive due to the substantial complexities involved in Apple's iPhone operating system. iOS security is essentially stratified into three layers: the application layer, the system layer, and the kernel layer, each having progressively greater permissions. To execute a successful jailbreak, one must attain kernel permissions, which in turn necessitates overcoming all the other security layers. Jailbreaks thus require the exploitation of numerous vulnerabilities that work in concert to reach the kernel.

Although relatively new to the competition, the Pangu Team immediately bolstered its reputation in the hacking community. At Pwnfest 2016, they discovered an Apple Safari browser exploit that granted them root access, earning them 80.000 USD.[200]

While in the 2016 Pwn2Own edition Chinese teams exerted significant influence, the 2017 edition was truly dominated by them. In 2017, the Qihoo 360's Security team secured the top position by successfully exploiting MacOS, Safari, Adobe Reader, Adobe Flash, and Windows 10,[201] winning them 255.000 USD.[202] They also managed to take down Microsoft Edge and escape a virtual machine in just 90 seconds, achieving the highest score in the event's history for a single entry.[203] The 2nd to 5th places in the ranking were also claimed by Chinese groups, namely Tencent Security Team Sniper (from the Tencent Keen Lab), Chaitin Security Research Lab (from the company Chaitin Technology), Tencent Security Team Lance (from the Tencent Zhanlu Lab), and Tencent Security Team Ether (from the Tencent Xuanwu Lab).

[197] Swati Khandelwal, "Chinese Hackers Won $215,000 for Hacking iPhone and Google Nexus at Mobile Pwn2Own," *The Hacker News*, October 27, 2016, https://thehackernews.com/2016/10/hacking-team-pwn2own.html.

[198] Wang Wei, "Google Pixel Phone and Microsoft Edge Hacked at PwnFest 2016," *The Hacker News*, November 11, 2016, https://thehackernews.com/2016/11/google-pixel-phone-hacked.html.

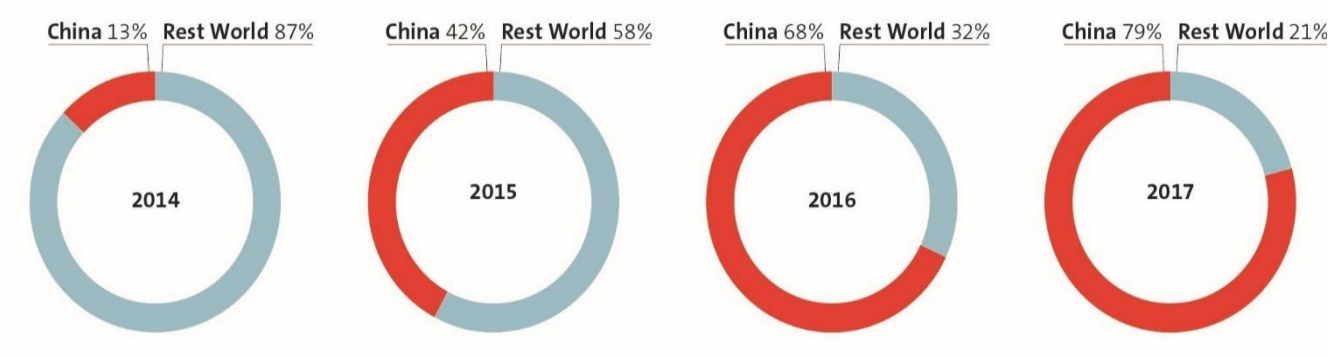
[199] Liu Zheng in Seoul, "Chinese Hackers Clean up at PwnFest Contest," *China Daily*, November 14, 2016, https://www.chinadaily.com.cn/business/tech/2016-11/14/content_27369997.htm.

[201] Xie Zhenqi, "Chinese Hackers Win 2017 World Hacking Contest," *CGTN*, March 18, 2017, https://news.cgtn.com/news/3d59544e32417a4d/share_p.html.

[202] Xie Zhenqi.

[203] Xie Zhenqi.

Figure 11: China's Share of the Prize Money at Pwn2Own (2014-2017)



Source: Compiled by the Author

Tencent teams collectively earned 350.000 USD for successful exploits targeting VMware, Microsoft Edge, Adobe Flash, while Chaitin Security earned 60.000 USD for successful exploits targeting Apple Safari browser, Ubuntu Linux, and the macOS kernel. In total, Chinese teams won 79% (665.000 USD) of the total 833.000 USD that were paid out.[204] The elevated number of Tencent-affiliated teams underscored the continued expansion of the company into hacking contests over the years.

The consistent dominance of Chinese hackers in Pwn2Own events significantly influenced the landscape of these competitions, establishing China as a major player and leading to millions in earnings for its research teams. Between 2014 and 2017, China's portion of the prize money won by all contestants surged from 13% in 2014 to 42% in 2015, then to 68% in 2016, reaching its pinnacle at 79% in 2017 (figure 11).

Following the 2017 Pwn2Own edition, it all stopped. In an interview with Chinese news outlet Sina, Qihoo 360 CEO Zhou Hongyi vigorously criticized Chinese citizens participating in overseas hacking competitions, suggesting that their successes were merely "imaginary."[205] [206] He argued that these hackers and their knowledge should remain in China given the strategic value of vulnerabilities.

In the same month, at the 5th China Internet Security Conference (ISC) in September 2017, Zhou Hongyi introduced the concept of "an Era of Big Security" (大安全时代), emphasizing cybersecurity's integration into all security realms, online and offline. He highlighted the inevitability of cyber warfare, where vulnerabilities serve as key weapons, and stressed the importance of understanding network weaknesses for effective defense, suggesting vulnerabilities should be considered national strategic assets.[207]

In 2018, Beijing banned Chinese research teams from attending exploit hacking competitions held outside of Chinese territory, such as Pwn2Own.[208] This led to the creation of the Tianfu Cup competition, which held its inaugural edition in November 2018. The absence of Chinese hackers has since significantly altered the landscape at Pwn2Own. For instance, throughout 2022 and 2023, there were no entrants willing to attempt to breach iPhone or Google Pixel devices, marking the end of a 15-year streak of targeting Apple products. The absence of hacking teams like Qihoo 360's 360 Nirvan and 360 Alpha, Tencent's Keen Security Lab, and Qi An Xin's Pangu Team, which were notably active in targeting these devices, could explain this trend, rather than assuming these devices have become fully secure. This development illustrates that cybersecurity fragmentation and protectionist vulnerability policies significantly undermine global cybersecurity.

[204] Brian Gorenc, "PWN2OWN 2017 – AN EVENT FOR THE AGES," *Zero Day Initiative* (blog), March 23, 2017, https://www.zerodayinitiative.com/blog/2017/3/23/pwn2own-2017-an-event-for-the-ages.

[205] Patrick Howell O'Neill, "How China Turned a Prize-Winning iPhone Hack against the Uyghurs," *MIT Technology Review*, May 6, 2021, https://www.technologyreview.com/2021/05/06/1024621/china-apple-spy-uyghur-hacker-tianfu/.

[206] Sina Technology, "**周**鸿祎:马云提新零售 **我想了几个月想到了'大安全**,'" *Sina*, December 9, 2017, https://tech.sina.cn/i/gn/2017-09-12/detail-ifykusey8931658.d.html?vt=4.

[207] Sina Technology, "**第五届互**联网安全大会召开 **周**鸿炜：人是大安全时代核心," *Sina*, December 9, 2017, https://slide.finance.sina.com.cn/slide_9_86514_488977.html#p=6.

[208] Patrick Howell O'Neill, "How China Turned a Prize-Winning iPhone Hack against the Uyghurs."

Figure 12: China's Participating Teams in Pwn2Own (2014-2017)

2014	2015	2016	2017
Keen Team	360 Vulcan (Qihoo 360)	360 Vulcan (Qihoo 360)	360 Security (Qihoo 360)
	Keen Team – Tencent PC Manager	Tencent Security Team Sniper (Tencent Keen Security Lab)	Tencent Security Team Sniper (Tencent Keen Security Lab)
		Tencent Security Team Shield (Tencent Keen Security Lab)	Tencent Security Team Lance (Tencent Zhanlu Lab)
		Tencent Security Xuanwu Lab	Tencent Security Team Ether (Tencent Xuanwu Lab)
			Tencent Security Sword Team
			Tencent Security Team Shield (Tencent Keen Security Lab)
			ChaiTin Security Research Lab (ChaiTin Tech)

Source: Compiled by the Author

5.3 Qihoo 360's Security Research Network

Qihoo 360 (奇虎), also known as 360 Security Technology, is one of China's leading cybersecurity providers. On its website, the company asserts to possess the largest cybersecurity expert team in the Eastern Hemisphere, comprising over 3,800 individuals.[209] By late 2023, the company had recorded revenue surpassing 2 billion USD.[210] From the early 2010s until 2020, Qihoo has been by far the largest China-based contributor of responsible vulnerability disclosures to American tech giants Microsoft and Google (section 7).

Qihoo 360 has been a prominent name in China's cybersecurity landscape since its inception in 2005. The company leads the Cyberspace Security Military-Civil Fusion Innovation Centre, established in 2017 under the auspices of the Central Military-Civil Fusion Development Commission.[211]

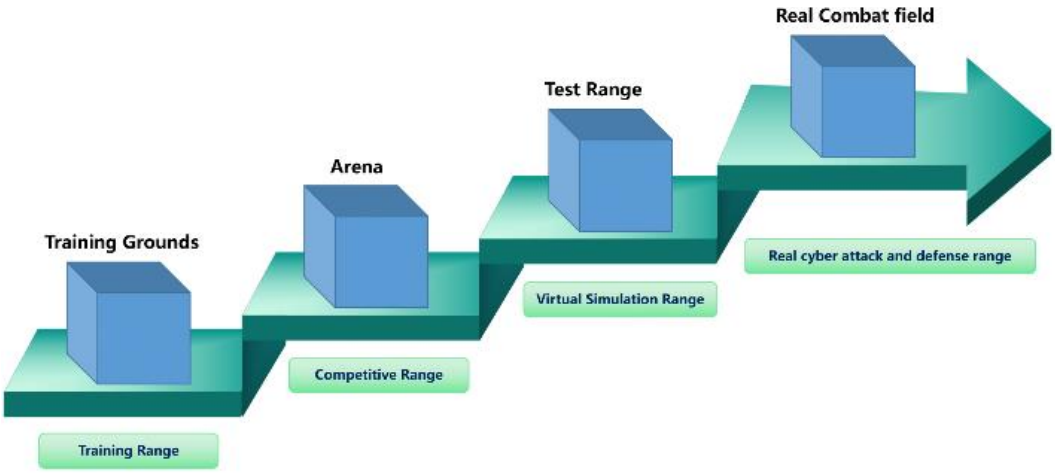
The primary objective of this center is to enhance the nation's cybersecurity defenses, with potential considerations for the development of "cyber militia and teams." [212]

Qihoo 360 collaborates with the MSS as a top-tier technical service unit (TSU) within the CNNVD.[213] In 2018, a threat actor known as Kryptonite Panda or APT40, which has operated as a contractor for the MSS since at least 2013, was found to have exploited a critical vulnerability a month before it was publicly disclosed. This vulnerability was initially discovered by Qihoo 360[214], raising questions about the extent of the involvement of the Chinese cybersecurity giant's security research teams in state-sponsored offensive operations.

In her analysis of the i-SOON leaks, threat intelligence researcher Winnona Bernsen uncovered significant details regarding the relationship between i-SOON and Qihoo 360.

[209] "公司简介," *360* (blog), n.d., http://www.360.cn/about/.
[210] "Qihoo 360 Technology Co Ltd (QIHU)," *Investing.Com* (blog), n.d., https://www.investing.com/equities/qihoo-360-technology-co.-financial-summary.
[211] Jiang Jie, "China Unveils Its First Civil-Military Cybersecurity Innovation Center," *People's Daily Online*, December 28, 2017, http://en.people.cn/n3/2017/1228/c90000-9309428.html.
[212] Jiang Jie.
[213] Dakota Cary and Kristin Del Rosso, "Sleight of Hand: How China Weaponizes Software Vulnerabilities."
[214] Adam Kozy, "Testimony before the U.S.-China Economic and Security Review Commission Hearing on 'China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States,'" February 17, 2022, https://www.uscc.gov/sites/default/files/2022-02/Adam_Kozy_Testimony.pdf.

Figure 13: 360 DSG Training Service



Source: https://360.net/about/news/article635f741f010089001f90487f

According to her findings, Qihoo 360 sold personal identifiable information of its antivirus customers to i-SOON, potentially enabling i-SOON to track individuals based on their online activities and provide their identities to government clients.[215]

In 2015, Qihoo established the 360 Enterprise Security Group (ESG) as part of its efforts to gain a firm foothold in the enterprise cybersecurity sector.[216] In 2019, ESG broke off from Qihoo to form a separate company called Qi An Xin, taking with it key talent, expertise, and customer base (more on Qi An Xin later). Qihoo 360 then founded the 'Government and Enterprise Security Group' – which is now called 360 Digital Security Group (DSG) - to reestablish its presence in the enterprise market. 360 DSG has consistently prioritized the provision of network security technologies, products, and services to a wide array of entities, including the Chinese military. On its website, 360 DSG claims to have established collaborations with 90% of ministries and commissions, 72% of central enterprises, and 95% of large financial institutions.[217] And to have partnered with millions of small and medium-sized Chinese enterprises to help enhance their network security.

Qihoo 360 CEO and founder Zhou Hongyi has highlighted the practical importance of testing security measures through real-world scenarios, asserting that "the essence of security is attack defense confrontation, and actual combat is the ultimate standard for testing security capabilities, which must withstand real attack defense tests." [218] This philosophy is mirrored in 360 DSG's leading position in the IT security enterprise-level training service market, boasting a 12.9% market share as per data from an International Data Corporation (IDC) China 2022 report.[219] According to information provided on the 360 DSG website, Qihoo's platform encompasses a comprehensive closed loop of enterprise safety training, from basic training of personnel to competition, from trial in virtual simulation environment to real cyber-attack and defense scenarios (figure 13). [220]

Over the years, 360 DSG's scale has enabled it to cultivate specialized cybersecurity research centers and stand-up dedicated hacking teams. Determining the exact team sizes is challenging due to limited accessible information. However, according to insights from an anonymous source familiar with the subject, certain Qihoo teams, such as 360 Vulcan and 360 Alpha, boast memberships exceeding 40 individuals. It appears that the organization

[215] Winnona Bernsen, "Same Same, but Different."
[216] Zhang Yushuo, "Qihoo 360's Enterprise Arm Hits USD2.7 Billion Valuation on New Funding," *Yicai Global*, November 30, 2018, https://www.yicai-global.com/news/qihoo-360-enterprise-arm-hits-usd27-billion-valuation-on-new-funding.
[217] "360企业安全," *360* (blog), n.d., https://university.360.cn/about/360.
[218] "让世界更安全，更美好!"
[219] "让世界更安全，更美好!"
[220] "让世界更安全，更美好!"

comprises a total of 19 groups, structured according to various departments and product lines, each tailored to specific areas of expertise and needs (Appendix A). Among them, only a few have received publicity for their outstanding work in vulnerability research and reporting. In no particular order, these include:

- 360 Vulcan was founded by Zheng Wenbin. It serves as the offensive/defensive research team for the company's flagship antivirus software, known as 360 Safeguard (Chinese version) and 360 Total Security (international version). Vulcan specializes in fuzzing and reverse engineering to discover software security vulnerabilities.[221] Between 2017 and 2020, it has been the most significant China-based contributor to the Microsoft Security Response Center (MSRC) bug bounty program (section 7). Some of its researchers have consistently ranked among Microsoft's top 3 global security researcher rankings. In January 2021, several 360 Vulcan's researchers left Qihoo and joined Zheng Wenbin in establishing Cyber Kunlun.
- 360 Alpha provides security research support for the company's mobile antivirus application, known as 360 Mobile Security.[222] It conducts dedicated research in mobile security, with a particular emphasis on hunting and exploiting Android vulnerabilities.[223] From 2017 to 2020, it was the second-most prolific China-based zero-days reporting team to Google Android's bug bounty program, second only to the 360 C0RE team.
- 360 C0RE was established in 2015. It specializes in Android and Linux platforms with the goal of identifying zero-day vulnerabilities and creating proof-of-concept exploits.[224] Known for actively reporting zero-days to Microsoft and Google Android's bug bounty programs from 2017 to 2020 (section 7), the team appears to have halted its operations in 2020. Notably absent from Qihoo's official list of teams on its website,[225] 360 C0RE's own website, c0reteam.org, was taken offline in late 2019, as confirmed by records in the Internet Archive.
- 360 IceSword was established within the 360 Security Engineering Institute in 2016. As outlined on the team's own website iceswordlab.com, the 360 Security Engineering Institute provides core technical support, pioneers product research and development, and serves as a hub for engineering expertise and advanced technology exploration. The team's research is focused on virtualization technology, cloud security, APT detection and defense, zero-day vulnerabilities, kernel protection, and mobile security.[226] Their achievements include the development of an automated vulnerability mining system.[227]
- The 360 Security Response Center (360SRC) is housed within the 360 Information Security Department, which operates akin to a Security Operations Centre (SOC). 360SRC is responsible for monitoring and responding to security threats, vulnerabilities, and cyberattacks that may affect Qihoo 360's products, services, and the broader digital ecosystem.[228] Much like Microsoft's MSRC, 360SRC operates its own bug bounty program, encouraging the identification and responsible disclosure of security vulnerabilities.[229] Between 2017 and 2020, 360SRC has been one of Qihoo's most active contributors of zero-day reports to Google Android (section 7).
- 360 Nirvan was established in 2015 and is also part of the 360 Information Security Department.[230][231] Its primary research focus is on Apple platforms, including the identification and exploitation of vulnerabilities at the operating system level. Between 2017 and 2020, 360 Nirvan was Qihoo's most active zero-day contributor to Apple's bug bounty program, trailing nationally

[221] "集顶尖研究团队," *360* (blog), n.d., https://360.net/research/team/#menu.
[222] "360 Mobile Security," *Uptodown* (blog), n.d., https://360-mobile-security.en.uptodown.com/android.
[223] 360TS, "Qihoo 360 Team Hacked Google Pixel in 60 Seconds at PwnFest," November 15, 2016, https://blog.360totalsecurity.com/en/qihoo-360-team-hacked-google-pixel-60-secs-pwnfest/.
[224] Hongli Han and Mingjian Zhou, "Android Binder: The Bridge To Root," https://conference.hitb.org/hitbsecconf2019ams/materials/D2T2%20-%20Binder%20-%20The%20Bridge%20to%20Root%20-%20Hongli%20Han%20&%20Mingjian%20Zhou.pdf.
[225] "集顶尖研究团队."
[226] "IceSword Lab," *IceSword Lab* (blog), n.d., https://www.iceswordlab.com/index.html.
[227] "IceSword Lab."
[228] "About 360SRC," *360 Security Response Center* (blog), n.d., https://security.360.cn/en/about-us.html.
[229] "About 360SRC."
[230] "About 360SRC," 36.
[231] "360再爆硬实力，涅槃团队获苹果 10 个内核漏洞致谢！," *QQ* (blog), July 21, 2017, https://mp.weixin.qq.com/s/KUIwQ8kZhXA2ZcrRurJ5lA.

only behind the Ant Group's Ant Financial Lightyear Security Lab (section 7).

- 360 Unicorn conducts research on all things wireless and radio, including Radio-Frequency Identification (RFID), Near-field Communication (NFC), Wireless Sensor Network (WSN), Global Positioning System (GPS), autonomous vehicles, and SATCOM.[232] At DEFCON in 2015, Unicorn researchers Lin Huang and Qing Yang showed how they were able to successfully spoof GPS information (creating a fake GPS signal, instead of just replaying a signal), and showing how a GPS-controlled drone could be manipulated.[233] In 2018, 360 Unicorn made it into Tesla's Security Researcher Hall of Fame.[234] It is unclear if the team is currently operational, as it is not listed Qihoo's website.[235]

This list represents only a portion of the numerous teams associated with Qihoo 360 (Appendix A), and many more are actively participating in various competitions and contributing to international bug bounty programs. As talented individuals attain a higher level of expertise in a specific subject area, they often transition to other companies or create their own cybersecurity startups.

In the realm of vulnerability reporting, Qihoo 360 has consistently outperformed global peers. From the inception of the earliest bug bounty programs in the early 2010s through 2020, Qihoo 360's research teams are reputed to have collectively reported close to 700 zero-days to Microsoft (more than 60% among all Chinese companies).[236] The company's achievements have been publicly acknowledged by US companies. 2017 saw Qihoo 360 emerge as the largest contributor to Google's Android Security Bulletin.[237] In 2019, the company was named top enterprise vulnerability contributor to the MSRC.[238] On an individual researcher level, Qihoo 360 excelled with 10 out of 75 researchers earning a place on the MSRC most valuable researcher list in 2019, securing the first two spots.[239] This number increased to 13 out of 75 in 2020. In 2021, the rankings for Google Chrome's vulnerability rewards program revealed that Qihoo 360 had secured the top position worldwide in terms of the number of researchers listed.[240]

In 2020, Qihoo 360 started to significantly curtail its reporting of vulnerabilities to Apple, Google Android and Microsoft's bug bounty programs (section 7). This decrease raised concerns about the potential loss of a significant channel for vulnerability reporting within the global ecosystem. While there are multiple factors contributing to this decline, the Atlantic Council's Dragon Tails report identified a noticeable correlation between the decrease in vulnerability reporting and the imposition of US sanctions.[241] In May 2020, the US Commerce Department added Qihoo 360 to its blacklist citing its links to Chinese military-affiliated enterprises and its alleged role in aiding China's surveillance of Uighur minorities in Xinjiang [242].

5.4 Tencent's Security Research Labs

Tencent(腾讯) was founded in 1998 and is headquartered in Shenzhen, Guangdong Province. As of 2023, the company boasted a workforce of over 100,000 individuals and recorded revenue exceeding 82 billion USD.[243] Tencent offers a wide range of products and

[232] Andy Greenberg, "Just a Pair of These $11 Radio Gadgets Can Steal a Car," *WIRED*, April 24, 2017, https://www.wired.com/2017/04/just-pair-11-radio-gadgets-can-steal-car/.

[233] Sean Michael Kerner, "Chinese Unicorn Team Hacks GPS at DefCon," *eWeek* (blog), October 8, 2015, https://www.eweek.com/security/chinese-unicorn-team-hacks-gps-at-defcon/.

[234] "Product Security."

[235] "集顶尖研究团队."

[236] "360 Vulnerability Thanks List," *360* (blog), n.d., http://www.360.cn/vulreport.html.

[237] "Google Recognizes 360 as the Largest Contributor of Its Vulnerability Report Program," *360 Blog* (blog), September 21, 2017, https://blog.360totalsecurity.com/en/360-the-largest-contributor-of-google-vulnerability-report-program/.

[238] Catalin Cimpanu, "Microsoft Names Top Security Researchers, Zero-Day Contributors," *ZDNET*, August 8, 2019, https://www.zdnet.com/article/microsoft-names-top-security-researchers-zero-day-contributors/.

[239] Sylvie Liu, "Announcing 2019 MSRC Most Valuable Security Researchers," *Microsoft MSRC* (blog), July 8, 2019, https://msrc.microsoft.com/blog/2019/08/announcing-2019-msrc-most-valuable-security-researchers/.

[240] Sylvie Liu, "Congratulations to the MSRC's 2020 Most Valuable Security Researchers," *Microsoft MSRC* (blog), May 8, 2020, https://msrc.microsoft.com/blog/2020/08/announcing-2020-msrc-most-valuable-security-researchers/.

[241] Stewart Scott, Sara Ann Brackett, Yumi Gambrill, Emmeline Nettles, Trey Herr, "Dragon Tails: Preserving International Cybersecurity Research" (Atlantic Council, September 14, 2022), https://www.atlanticcouncil.org/in-depth-research-reports/report/preserving-international-cybersecurity-research/.

[242] Cheryl Arcibal, "US Slaps Sanctions on 33 Chinese Companies and Institutions, Dialling up the Tension amid the Lowest Point in US-China Relations," *South China Morning Post*, May 23, 2020, https://www.scmp.com/business/companies/article/3085788/us-slaps-sanctions-33-chinese-companies-and-institutions.

[243] "Tencent Holdings," *Forbes* (blog), n.d.

services spanning online gaming, social networking, advertising, cloud computing, and AI. Particularly noteworthy is its mobile chat service WeChat, boasting over 1.67 billion monthly active users, with most dedicating more than four hours daily to the platform.[244] WeChat is not only a messaging platform but also a social media, payment, and e-commerce app. It has become deeply integrated into the daily lives of many Chinese citizens. Tencent also operates QQ, a major Chinese social media platform, and Riot Games, a US company known for creating League of Legends, a multiplayer online battle arena game, which attracts an average of over 132 million players monthly.[245] The company's surging revenue, stock price, and vast user base has made Tencent one of the most valuable company globally.[246] Given its pivotal role in providing essential messaging and networking services, Tencent is of strategic importance to the Chinese government.

Tencent boasts various vulnerability research teams that have made significant contributions by identifying and reporting major vulnerabilities to prominent Western companies, including Apple, Google, and Microsoft. All these teams operate within the Tencent United Security Laboratory, established in Shenzhen in 2016, which is the research division of Tencent Security.[247] The Joint Laboratory's focus spans 5G, IoT, autonomous vehicles, AI, mobile, cloud, and satellite security, as well as antivirus and anti-ransomware solutions. The exact number of currently active labs is unknown, but there are likely between 7 and 10. On its website, Tencent features two tabs (Tencent Security and Security Lab),[248] each leading to a group of 7 labs. However, only 4 labs are common across both pages (Appendix B).

Figure 14: Heads of Tencent Research Laboratories

Source: https://cloud.tencent.com/developer/article/1146779

Among the labs listed, only a few are publicly known for their outstanding work in vulnerability research and reporting. In no particular order, these include:

- The Xuanwu Lab, Tencent's first security research laboratory, was founded in 2014.[249] The lab focuses on vulnerability research and web application security, especially on mobile platforms.[250] Between 2017 and 2020, the Xuanwu Lab has been Tencent's most active contributor of zero-day reports to Microsoft and Apple (section 7).

- The Tianma Lab specializes on satellite network security and their application for critical infrastructure.[251] Specifically, it focuses on identifying high-risk vulnerabilities and ensuring the security of critical satellite communication, telephony, digital radio, and television. Other research areas include IoT devices and networked control systems. In 2022[252] and 2023[253], the Tianma Lab received awards for the most valuable vulnerability and contributions by individual researchers to the China National Vulnerability Database (CNVD).

- The Zhanlu Lab was established in 2016. It specializes in vulnerability mining, and attack and defense technologies.[254] It is currently led by Yuan

[244] Rohit Shewale, "18+ WeChat Statistics For 2024 (Users, Revenue & More)," *Demandsage* (blog), December 12, 2023, https://www.demandsage.com/wechat-statistics/#:~:text=With%20over%201.67%20billion%20monthly,payments%2C%20gaming%2C%20and%20shopping.

[245] "League of Legends," *Active Player* (blog), n.d., https://activeplayer.io/league-of-legends/.

[246] Weilun Soon, "Chinese Tech Giant Tencent Jumps onto the List of the World's 10 Most Valuable Companies as Meta Slides on Stock Rout," *Business Insider*, February 18, 2022, https://www.businessinsider.com/tencent-top-10-most-valuable-firms-after-meta-stock-rout-2022-2.

[247] "Tencent Security Joint Laboratory," *Tencent Security* (blog), n.d., https://s.tencent.com/research?activeTab=1.

[248] "Tencent," accessed November 3, 2024, https://m.qq.com/download.

[249] "Tencent Security Joint Laboratory."

[250] Yu Chen and Yang Yu, "InfinityGauntlet: Expose Smartphone Fingerprint Authentication to Brute-Force Attack," *Usenix* (blog), n.d., https://www.usenix.org/conference/usenixsecurity23/presentation/chen-yu.

[251] "腾讯安全联合实验室," *Baidu* (blog), n.d., https://baike.baidu.com/item/%E8%85%BE%E8%AE%AF%E5%AE%89%E5%85%A8%E8%81%94%E5%90%88%E5%AE%9E%E9%AA%8C%E5%AE%A4/19839736#2_5.

[252] "国家信息安全漏洞共享平台2021年工作会议成功召开," *CNVD* (blog), March 3, 2022, https://mp.weixin.qq.com/s/A8plJgxw5L3XWjNI3p_oYw.

[253] "2022年度CNVD支撑单位年度工作情况及优秀单位个人表彰名单," *CNVD* (blog), September 20, 2023, https://www.cnvd.org.cn/webinfo/show/9256.

[254] "腾讯安全湛泸实验室," *Baidu* (blog), n.d., https://baike.baidu.com/item/%E8%85%BE%E8%AE%AF%E5%AE%89%E5%85%A8%E6%B9%9B%E6%B3%B8%E5%AE%9E%E9%AA%8C%E5%AE%A4/20246269.

Renguang, co-founder of the Chinese cybersecurity company NSFOCUS. [255]

- The Keen Security Lab was acquired by Tencent after their success at Pwn2Own in 2014. The lab specializes in the network security of autonomous vehicles, including models produced by major industry players like Mercedes-Benz, Tesla, Toyota,[256] and BMW. [257] [258] Its research also encompasses IoT device hacking, mobile security, and browser hacking. In 2016 and 2017, the Keen Lab secured a spot in the Tesla Security Researcher Hall of Fame, and even garnered recognition by Elon Musk himself.[259] In 2018, they earned the prestigious "BMW Group Digital and IT R&D Technology Award," expanding their partnership with BMW.[260] Their extensive collaboration extended to an eight-month code audit with Mercedes-Benz, resulting in the release of the "Mercedes-Benz Automobile Information Security Research Review Report" in May 2021.[261] This report unveiled several major vulnerabilities, four of which could be exploited for remote code execution. The report also solidified Keen's commitment to future collaboration with BMW.

Until at least 2020, Tencent maintained its position as the second-largest Chinese contributor of zero-day vulnerabilities to US-based bug bounty programs, ranking only behind Qihoo 360. However, like Qihoo 360, Tencent subsequently reduced its vulnerability disclosures to Google and Microsoft.[262]

As all companies in China, Tencent is legally mandated to provide technical support and assistance to Chinese security agencies as outlined in China's 2017 Cybersecurity Law. In Tencent's case, this may also include scrutiny by the government of the data exchanged through WeChat for surveillance purposes. Tencent serves as a top-tier technical support unit (TSU) for the MSS-operated CNNVD vulnerability database.

5.5 Qi An Xin's Pangu Team

The history of Qi An Xin's Pangu team goes back to 2014, when Pwnzen Infotech was established in Shanghai. Pwnzen Infotech (犇众信息) is a security research institution focusing on operating system security, automated analysis, vulnerability mining, and attack and defense technologies.[263]

Pwnzen hosts the Pangu Team (盘古越狱团队), which was also established in 2014.[264] It is comprised of researchers dedicated to conducting offensive and defensive research for mobile systems and applications. The Pangu Team gained international fame for launching numerous successful jailbreak tools for Apple iOS, and it was purportedly the first team to accomplish comprehensive jailbreaks for iOS 8[265] and iOS 9,[266] resulting in tens of millions of downloads globally. Over time, the group's focus transitioned from a jailbreaking team to a professional mobile security research team. It has established the Pangu Lab, which conducts extensive security research on the security architecture of mobile devices hardware, systems, applications, and connectivity. Since 2015, the Pangu Team has also been hosting its own mobile security conference, called MOSEC in Shanghai. While not a hacking contest per se, MOSEC is dedicated to

[255] "Our Leadership," *PeerSafe* (blog), n.d., https://www.peersafe.cn/team_en.html.
[256] "Toyota Acknowledges Tencent Keen Security Lab's Initiatives for Improving Automotive Cybersecurity," *Toyota Newsroom* (blog), March 30, 2020, https://pressroom.toyota.com/toyota-acknowledges-tencent-keen-security-labs-initiatives-for-improving-automotive-cybersecurity/.
[257] "Toyota Acknowledges Tencent Keen Security Lab's Initiatives for Improving Automotive Cybersecurity."
[258] "Tencent Security Joint Laboratory."
[259] "Product Security."
[260] "First-Ever BMW Group Digitalization and IT Research Award Goes to Tencent Keen Security Lab for Their Connectivity and Cybersecurity Research. The Two Companies Plan to Expand Their Cooperation and Joint Research Work.," *BMW Group* (blog), May 22, 2018, https://www.press.bmwgroup.com/global/article/detail/T0281245EN/first-ever-bmw-group-digitalization-and-it-research-award-goes-to-tencent-keen-security-lab-for-their-connectivity-and-cybersecurity-research-the-two-companies-plan-to-expand-their-cooperation-and-joint-research-work?language=en.
[261] Ionut Arghire, "Researchers Find Exploitable Bugs in Mercedes-Benz Cars," *Security Week*, May 18, 2021, https://www.securityweek.com/researchers-find-exploitable-bugs-mercedes-benz-cars/.
[262] Stewart Scott, Sara Ann Brackett, Yumi Gambrill, Emmeline Nettles, Trey Herr, "Dragon Tails: Preserving International Cybersecurity Research."
[263] "关于犇众," *Pwnzen Infotech Ltd.* (blog), n.d., https://www.pwnzen.com/about.html.
[264] "Pangu Lab, Chinese Ally of Singapore's Zero-Day Reseller Coseinc, Exposes NSA Cyber Operations," *Intelligence Online*, February 3, 2022, https://www.intelligenceonline.com/surveillance--interception/2022/03/02/pangu-lab-chinese-ally-of-singapore-s-zero-day-reseller-coseinc-exposes-nsa-cyber-operations,109737375-art.
[265] Jason, "Pangu iOS 8 – iOS 8.1 Jailbreak Released [Updated]," *iJunkie* (blog), 10 2014, https://ijunkie.com/pangu-ios-8-ios-8-1-jailbreak-released/.
[266] Thomas Brewster, "Chinese Hackers Announce First iOS 9 Jailbreak But Don't Go After The Big Bucks," *Forbes*, October 14, 2015, https://www.forbes.com/sites/thomasbrewster/2015/10/14/team-pangu-ios9-iphone-jailbreak/.

advancing mobile security research and promoting information exchange between security researchers and practitioners in the field.[267]

Unlike other security research teams, the Pangu Team provides a full list of its members' identities and bios on its website, accompanied by cartoonish profile pictures. However, their immediate affiliation is less evident. In 2021, the Pangu Lab officially merged with Qi An Xin (奇安信网神信息技术（北京）股份有限公司), forming Qi An Pangu Technology.[268] Qi An Pangu has since then been able to leverage Qi An Xin's vulnerability attack and defense research and has closely integrated with its mobile big data platform. [269]

Qi An Pangu is one of only a handful of Chinese entities that have publicly attributed US cyber espionage activities. In 2022, the Pangu Lab reported that it discovered activities of the Equation Group – believed to be a mix of the U.S. National Security Agency (NSA)'s Tailored Access Operation unit and the Central Intelligence Agency (CIA)'s Information Operations Center – conducted against Chinese networks.[270] Pangu discovered a malware it named Bvp47 that was deployed within the domestic IT systems of a key Chinese department in 2013 and 2015. The malware was used to monitor and track key institutions in 45 countries over a 10-year campaign.[271] This revelation adds to the attribution statements made by Qihoo 360 in 2020 and 2022, which accused the CIA[272] and the NSA[273] of conducting malicious cyber operations against China's leading companies, governments, research institutes, and critical infrastructure over the past decade.

In 2023, Pangu Lab researchers claimed to have identified six members of a hacktivist group known as "Against The West." Among them is Tillie Kottmann, a Swiss citizen who goes by the pseudonym "maia arson crimew." Kottmann is facing charges by the U.S. Department of Justice for infiltrating multiple US companies and disclosing confidential information on the internet.[274]

Qi An Pangu's mother company, Qi An Xin, is a leader in China's cybersecurity industry. Established in 2015, it was originally an entity housed within Qihoo 360 under the name of 360 ESG until the split in 2019. It is now partly owned by Chinese state-owned enterprise, China Electronics Corporation (中国电子信息产业集团有限公司). In 2020, CEC was labeled by the Trump administration as a 'Communist Chinese military company'.[275] Allegedly, Qi An Xin kept all its government contracts after splitting from Qihoo 360. On its own LinkedIn profile, the company claims that its products and services have been adopted by over 90% of China's central government departments, central government-led enterprises, and large banks.[276] Qi An Xin has been entrusted by the Chinese government with managing cybersecurity during high-profile events, such as the 70th anniversary of the CCP's rule and the Beijing Winter Games.[277] The Beijing city government recognized Qi An Xin as one of the 20 "invisible champions," a designation reserved for companies critical to China's national strategy. According to Dakota Cary, "as far as companies are concerned, their talent is undoubtedly in the top 10 globally. When there is an issue at the provincial level or even at the central level, when the government needs a response team, it seems that Qi An Xin is known."[278]

Qi An Xin is deeply connected with Chinese intelligence and military services, and it operates its own Cybersecurity MCF Innovation Center. Its staff includes 1,300 CCP members, which amounts to 14% of its entire staff.[279] More than 40% of its main revenue

[267] "Introduction," *MOSEC 2023* (blog), accessed December 2, 2024, https://www.mosec.org/en/2023/.
[268] 奇安信集团, "专访|奇安盘古，做移动安全的最强守护者," *QIANXIN* (blog), April 11, 2021, https://www.qianxin.com/news/detail?news_id=2664.
[269] 奇安信集团.
[270] Beijing Qi an Pangu Laboratory Technology Co., Ltd, "Bvp47 Top-Tier Backdoor of US NSA Equation Group," n.d., https://www.pangu-lab.cn/files/The_Bvp47_a_top-tier_backdoor_of_us_nsa_equation_group.en.pdf.
[271] Beijing Qi an Pangu Laboratory Technology Co., Ltd.
[272] Raphael Satter, "Chinese Cybersecurity Company Accuses CIA of 11-Year-Long Hacking Campaign," *Reuters*, March 3, 2020, https://www.reuters.com/article/idUSKBN20Q2SG/.
[273] "China Cybersecurity Firm Alleges US National Security Agency Is behind Hacking Group That Has Stolen a Mass of Critical Data," *Yahoo! Finance*, March 21, 2022, https://finance.yahoo.com/news/china-cybersecurity-firm-alleges-us-093000291.html?guccounter=1.
[274] Alexander Martin, "Chinese Security Researchers Claim to Have Identified 'Against The West' Hackers," *The Record*, February 20, 2023, https://therecord.media/against-the-west-hackers-allegedly-identified-pangu-lab.
[275] Albert Zhang, "Gaming Public Opinion" (ASPI, 2023), https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2023-05/Gaming%20public%20opinion.pdf?VersionId=QYkBIWncbBU0E1KAhg9mX3TD7kwlWcWj.
[276] "Qi An Xin Technology Group," *LinkedIn* (blog), n.d., https://www.linkedin.com/company/qi-an-xin-group/about/.
[277] Jamie Tarabay and Sarah Zheng, "Chinese Firm That Accused NSA of Hacking Has Global Ambitions," *Bloomberg*, May 31, 2022, https://www.bloomberg.com/news/articles/2022-05-31/chinese-firm-that-accused-nsa-of-hacking-has-global-ambitions.
[278] Jamie Tarabay and Sarah Zheng.
[279] Albert Zhang, "Gaming Public Opinion."

is derived from government and law-enforcement agencies, with additional clients from the military and defense industry.[280]

As outlined in the 2023 report "Gaming Public Opinion" by Albert Zhan of the Australian Strategic Policy Institute (ASPI), Qi An Xin has direct and indirect working relationships with the MPS and the MSS. [281] These collaborations include the establishment of national cybersecurity standards and involvement in influence operations.[282] Zhan makes a clear connection between Qi An Xin and the company's support for MPS through the participation in state-sponsored influence operations in Southeast Asia and various other countries.[283] Additionally, Qi An Xin established the Cyber Security Penetration Testing Centre in partnership with the China Information Technical Security Evaluation Center (CNITSEC). CNITSEC is housed within the 13th Bureau of the MSS, which hosts a significant portion of the agency's technical cyber expertise.[284]

Qi An Xin also supports government-contracted companies engaged in espionage activities. Winnona Bernsen, in her examination of the i-SOON leaks, revealed that Qi An Xin appeared to play a pivotal role as i-SOON's primary contractor, competitor, and potential investor. Internal company chat logs suggest that i-SOON has relied on investment funds from Qi An Xin to pay its departments and has explored the possibility of collaborating with the company to provide training to other clients.[285]

Finally, Qi An Xin plays a significant role in vulnerability research. It is recognized as a top-tier technical support unit (TSU) [286] and operates its own vulnerability database, known as the Bu Tian Vulnerability Database. This database serves as a platform for civilian hackers to collaborate on identifying and addressing software vulnerabilities. This data then finds its way to the MSS. In 2021[287], 2022[288], and 2023[289] the Bu Tian platform was recognized by the CNVD for its valuable contributions to vulnerability reporting.

[280] Beijing Qi an Pangu Laboratory Technology Co., Ltd, "Bvp47 Top-Tier Backdoor of US NSA Equation Group."
[281] Albert Zhang, "Gaming Public Opinion."
[282] Albert Zhang.
[283] Albert Zhang.
[284] "China Information Technology Security Evaluation Center," *China Information Technology Security Evaluation Center* (blog), December 15, 2017, http://www.itsec.gov.cn/fz/en/201708/t20170802_15316.html.
[285] Winnona Bernsen, "Same Same, but Different."
[286] Dakota Cary and Kristin Del Rosso, "Sleight of Hand: How China Weaponizes Software Vulnerabilities."
[287] "**国家信息安全漏洞共享平台2021年工作会**议成功召开."
[288] "**国家信息安全漏洞共享平台2021年工作会**议成功召开."
[289] "2022**年度CNVD支撑**单位年度工作情况及优秀单位个人表彰名单."

6 The Tianfu Cup (2018-2023)

This section traces the history and performance of Chinese hacking teams that participated at the Tianfu Cup (2018-2023). It analyzes the competing teams, their affiliations with corporate entities, and their connections to China's cyber intelligence activities. Finally, it investigates the targets and economic incentives of the competition, and how these align with China's broader strategic interests.

Key Points

- The Tianfu Cup mostly attracts professionals, with Western targets being the prime focus.
- The Tianfu Cup has increasingly become intertwined with state-sponsored operations, with exploits showcased by participants highly likely funneled to the MSS.
- Initially, Tencent and Qihoo dominated the competition, mirroring dynamics seen at Pwn2Own.
- From 2020 onward, a new wave of winners emerged, including teams affiliated with Cyber Kunlun and the Ant Group. These are prolific suppliers of zero-day vulnerabilities to the MSS.
- Ant Group boasts 9 vulnerability research laboratories, with ambiguity surrounding their organizational structure.
- Cyber Kunlun is strongly linked to Qihoo 360. It operates through two divisions: the Kunlun Lab and the Kunlun Advanced Offensive and Defensive Team.
- Tianfu Cup participants have voiced grievances about the need to distribute the prize money across their organization.
- The 2023 Tianfu Cup marked a notable shift away from Western targets, redirecting its focus to Chinese products and systems.

6.1 Background

The Tianfu Cup (天府杯) is China's foremost exploit hacking competition. It functions similarly to Pwn2Own, where participants earn rewards for finding vulnerabilities in widely used soft- and hardware products. Based in Chengdu, Sichuan province, the Tianfu Cup commenced in November 2018 and runs annually. Due to the COVID-19 pandemic, it was cancelled in 2022, but recommenced in 2023.[290] For the 2023 iteration, 17 companies were listed as the main organizers. These included Huawei, Qihoo 360, Cyber Kunlun, Qi An Xin, Topsec, NSFOCUS, and Sangfor. Cyber Kunlun and Qi An Xin were the only two companies that were designated co-organizers of the event.

Similar to Pwn2Own, participants in the Tianfu Cup can win significant financial rewards and national recognition by showcase their technical skills. Naturally, participants also exchange knowledge, learn from each other, and network.

In 2018, the total prize pool was 1 million USD. In 2019, it shrank to 500.000 USD. In 2020, it was back up at 1,2 million USD, and in 2021 it grew to 1,9 million USD. In that year, the top three teams earned 654.500 USD, 522.500 USD and 392.500 USD respectively.[291] In 2023, the total prize pool was 1,4 million USD.[292] Pwn2Own's prize pool similarly hovers between 1-2 million USD.

Between 2018 and 2021, the focus of the Tianfu Cup primarily centered on Western software products. In 2023, the Cup began to include a growing number of Chinese products as well. This report could not confirm whether the Tianfu Cup organizers asked Western companies for permission to utilize their products as targets for the competition or have engaged in any other forms of collaboration.

[290] Provincial Employment Bureau, "四川省第四届'天府杯'创业大赛方案策划项目比选公告," Department of Human Resources and Social Security of Sichuan Province, August 4, 2023, http://rst.sc.gov.cn/rst/gsgg/2023/8/4/f9ed3cddd8e54d62ad027daae18d95da.shtml.

[291] Eduard Kovacs, "$1.9 Million Paid Out for Exploits at China's Tianfu Cup Hacking Contest," *Security Week*, October 19, 2021, https://www.securityweek.com/19-million-paid-out-exploits-chinas-tianfu-cup-hacking-contest/.

[292] "清华大学网络研究院联合主办的'天府杯'2023国际网络安全大赛圆满落幕," *Institute for Network Sciences and Cyberspace, Tsinghua University* (blog), April 11, 2023, https://www.insc.tsinghua.edu.cn/info/1192/3594.htm.

Figure 15: 2020 Tianfu Cup

Source: https://thehackernews.com/2020/11/windows-10-ios-chrome-firefox-and.html

6.2 Performance and Strategic Significance

The first edition of the Tianfu Cup starred a mix of established Chinese hacking teams and newcomers. Qihoo 360 participated with three teams: 360 Security, 360 Vulcan and 360 Nirvan. The Ant Group, previously known as Ant Financial, participated with two teams: oyear and lyear.[293] Others included, the Antui Team (Chinese Academy of Sciences Institute of Computing Technology-Tencent); the Security Warriors team (Guangzhou University Fangban-Tencent); and three 360 Vulcan members participated individually: Zhao Qixun, Tang Tianwen, and Jia Zhenjie. [294] [295] The first prize was won by 360 Security, which successfully exploited zero-days vulnerabilities against Apple Safari, iPhoneX, Google Chrome, Microsoft Edge, Microsoft Office, and Oracle's Virtual Box, earning the team a total of 62.000 USD.[296] The 2nd and 3rd place were won by the Atuin team and the Security Warriors respectively. Zhao Qixun won the title of "Best Individual" and was awarded the highest single reward of 200.000 USD for demonstrating an exploit chain to breach the iPhone. [297] [298] The outcome of the inaugural event predominantly mirrored the patterns observed at Pwn2Own, in which teams affiliated with Qihoo 360 and Tencent secured victories across the board.

Two teams, consisting of collaboration efforts between industry and universities, secured the 2nd and 3rd spots. One team was a collaboration effort between the Chinese Academy of Sciences Institute of Computing Technology (ICT CAS) and Tencent Atuin. Tencent Atuin is likely an alias for the Tencent Xuanwu Lab.[299] The team's "Atuin" name almost certainly refers to a software platform by the same name which was created by Tencent's Xuanwu Lab and ICT CAS' Big Data Security Group.[300] The Atuin software platform collects information on vulnerabilities and supply chain issues through an automated software analysis. The second team comprised members from the Guangzhou University Fangban (GUF) and the Tencent Security Warriors team, which is likely associated with the Tencent Keen Security Lab. [301]

Industry-university collaborations underscore a growing trend in where students from top-ranking Chinese universities, with close ties to the state, increasingly engage in collaborative vulnerability research with leading Chinese tech companies, who have a strong emphasis on advancing automated vulnerability mining technologies. While instances of industry-university collaborations are prevalent in China, their joint participation in popular exploit hacking competition has so far been a rather rare occurrence.

However, the real legacy of the inaugural Tianfu Cup is how quickly the event was associated with state-sponsored cyber operations. In August 2019, Google published an analysis detailing a hacking effort aimed at "exploiting iPhones en masse."[302]

[293] Balaji, "Tianfu Cup 2018 PWN – Ethical Hackers Hacked Apple, Adobe, Google, Microsoft, Oracle, VMware & Earned 1,000,000 USD," November 20, 2018, https://gbhackers.com/tianfu-cup-2018-pwn/.

[294] "Adobe Acrobat and Reader Out-Of-Bounds Write Multiple Arbitrary Code Execution Vulnerabilities," n.d., https://cve.report/bid/106978.

[295] Pierluigi Paganini, "Vmware Fixed Workstation Flaw Disclosed at the Tianfu Cup Pwn Competition," *Security Affairs*, November 23, 2018, https://securityaffairs.com/78369/breaking-news/vmware-dixed-critical-flaw.html.

[296] Pierluigi Paganini, "Tianfu Cup Pwn Hacking Contest - White Hat Hackers Earn $1 Million for Zero-Day Exploits," *Security Affairs*, November 19, 2018, https://securityaffairs.com/78210/hacking/tianfu-cup-pwn.html.

[297] "'天府杯'2018国际网络安全大赛落下帷幕 · 360Security摘得桂冠," *Tencent Cloud* (blog), December 14, 2018, https://cloud.tencent.com/developer/article/1372818.

[298] Eduard Kovacs, "Hackers Earn $1 Million for Zero-Day Exploits at Chinese Competition," November 19, 2018, https://www.securityweek.com/hackers-earn-1-million-zero-day-exploits-chinese-competition/.

[299] "腾讯安全玄武实验室'阿图因'系统入选世界互联网大会领先科技成果," 科技频道 (blog), June 12, 2017, https://itech.ifeng.com/44793650/news.shtml?&back.

[300] "腾讯安全玄武实验室'阿图因'系统入选世界互联网大会领先科技成果."

[301] "广州大学—腾讯公司共建联合实验室," *Guangzhou University* (blog), January 16, 2018, https://news.gzhu.edu.cn/info/1016/12354.htm.

[302] Patrick Howell O'Neill, "How China Turned a Prize-Winning iPhone Hack against the Uyghurs."

Table 3: Tianfu Cup Rankings (2018-2023)

Ranking	2018	2019	2020	2021	2022	2023
1	360 Security (Qihoo 360)	360 Vulcan (Qihoo 360)	360 ESG (Qihoo 360)	Kunlun Lab (Cyber Kunlun)	N/A	Ant Financial Lightyear Security Lab (Ant Group)
2	Chinese Academy of Sciences Institute of Computing Technology – Tencent Atuin Team	ddd (Tencent Xuanwu Lab)	Ant Financial Lightyear Security Lab (Ant Group)	Pangu Team (Qi An Xin)	N/A	CyAgent
3	Guangzhou University Fangban - Tencent Security Warriors Team	Ant Financial Lightyear Security Lab (Ant Group)	Pangu Team (Qi An Xin)	Youth Training Team of Vulnera-bility Research Institute	N/A	k (Sangfor)

Source: Compiled by the Author

Google researchers identified five distinct exploit chains, including an exploit called "Chaos," which Zhao Qixun demonstrated during the 2018 Tianfu Cup. Subsequently, in September of the same year, Apple disclosed that the Chaos exploit had been used in a surveillance and hacking campaign targeting Uyghur Muslims, starting shortly after Qixun's demonstration at the Tianfu Cup and lasting until Apple issued a patch in January 2019.[303] Several Western media outlets, such as Tech Crunch, linked these malicious operations to the Chinese government.[304] This instance likely highlights that vulnerabilities submitted to the Tianfu Cup are shared with Chinese government agencies.

The 2019 Tianfu Cup edition was won by Qihoo 360's 360 Vulcan team, which received a total of 382.500 USD.[305] The second place was secured by ddd from Tencent's Xuanwu Lab, who earned a total of 83.750 USD for exploits targeting Edge, Chrome, Adobe Reader, and D-Link routers. The third place went to the Ant Group's StackLeader team for a total of 38.750 USD. 360 Vulcan's Xiao Wei received the highest reward of 200.000 USD for a working exploit against the VMware vSphere ESXi product that allowed them to escape from the guest virtual machine to the host[306].

In the 2020 contest, Qihoo 360's 360 ESG Vulnerability Research Institute team clinched the top award of 744.500 USD, accounting for nearly two-thirds of the total jackpot of 1.2 million USD. The team also received the distinguished "Best Product Crack Award."[307] 360 ESG managed to breach an array of high-profile targets, including Google Chrome, Firefox, VMware ESXi, Ubuntu, Samsung Galaxy S20, Windows 10, iPhone 11 Pro, Adobe PDF Reader, and TP-Link WDR7660. The second and third positions were secured by the Ant Group's Ant Financial Lightyear Security Lab and the Pangu Team.[308]

Teams from Tencent (Qihoo 360's main competitor at Pwn2Own) did not take part in the 2020 Tianfu Cup edition. The reason for Tencent's decision to step back is unclear. Sources familiar with the subject suggest that Tencent discouraged its employees from participating. Tencent is also absent as a significant sponsor supporting the Tianfu Cup. On the other hand, the enduring success of Qihoo's 360 teams is a testament to the company's sustained leadership, securing three consecutive triumphs at the Tianfu Cup.

The 2021 Tianfu Cup was won by the Cyber Kunlun

303 Patrick Howell O'Neill.
304 Patrick Howell O'Neill.
305 Pierluigi Paganini, "Tianfu Cup 2019 – 11 Teams Earned a Total of 545,000 for Their Zero-Day Exploits," *Security Affairs*, November 18, 2019, https://securityaffairs.com/94040/hacking/tianfu-cup-2019-results.html.
306 Pierluigi Paganini.
307 "360政企安全联队81.25万美金屠榜2020天府杯 三度登鼎冠军之席！," *China Youth On Line* (blog), September 11, 2020, https://m.cyol.com/content/2020-11/09/content_18845174.htm.
308 Catalin Cimpanu, "Windows 10, iOS, Chrome, and Many Others Fall at China's Top Hacking Contest," *ZDNET*, August 11, 2020, https://www.zdnet.com/article/windows-10-ios-chrome-and-many-others-fall-at-chinas-top-hacking-contest/.

team.[309] Cyber Kunlun targeted a wide spectrum of platforms, including Google Chrome, Adobe Reader, VMware ESXi and Workstation, iPhone 13 Pro, Safari on macOS, and Windows 10.[310] Cyber Kunlun was followed by the Pangu Team and by the Youth Training Team of Vulnerability Research Institute. The Pangu Team successfully executed a remote jailbreak of the iPhone 13 Pro equipped with iOS 15, which could be triggered with a single click on a meticulously crafted link. This performance earned the Pangu Team the highest single reward in the competition, amounting to 300.000 USD.[311] Additional high-value findings surfaced in the 2021 competition included new exploits targeting Android phone models from multiple manufacturers.

The absence of Qihoo 360's renowned teams from the competition marked a new development, potentially attributable to major internal restructuring. Many members of Qihoo 360's Vulcan team left the company in 2021 to form Cyber Kunlun, resulting in a considerable loss of essential expertise.
In the Tianfu Cup 2023, the highest award of 340.000 USD was secured by the Ant Group's Ant Financial Lightyear Security Lab for hacking VMware ESXI, Chrome browser, Adobe, Windows 11 and the Chinese-made office product WPS.[312] CyAgent and Sangfor's k team placed second and third, winning 100.000 USD and 30.000 USD respectively.[313] The Qihoo 360 teams were once again absent from the competition.

6.2.1 Intelligence Linkages

Over the years, a parallel development has emerged between the Tianfu Cup and Chinese APTs when it comes to target preferences. The Tianfu Cup has steadily broadened its target spectrum to include virtualization solutions like VMware, Parallels, and qemu, as well as routers and other network devices. Concurrently, Chinese APTs have shown increased activity in targeting the same software and devices, particularly since 2021. According to Recorded Future's Insikt Group, over 85% of the known zero-day vulnerabilities exploited by Chinese state-sponsored groups since early 2021 were found in internet-facing appliances such as email servers, SSL VPN products, firewalls, and routers.[314] In a separate report published in 2023, Mandiant researchers detailed how Chinese threat actors have targeted Fortinet and VMware security products to establish persistence on victim networks.[315]

In 2018, Zhao Qixun's Chaos exploit serves as the prime example of the Tianfu Cup's likely relationship with Chinese state agencies. The 2021 Tianfu Cup, coupled with the emergence of the i-SOON leaks, has further reinforced this association.

Following the 2021 Tianfu Cup, a group of China-focused analysts known as the "Natto Team" noticed that, while vulnerabilities in VMware products were showcased by Chinese researchers at the October 2021 Tianfu Cup, VMware only released patches for these vulnerabilities in February 2022, nearly four months later.[316] Upon releasing the patches, VMware affirmed in a Q&A document that these vulnerabilities "were reported to the Chinese government by the researchers that discovered them, in accordance with their laws." The company later retracted this statement.[317]

Similarly, the Microsoft Digital Defense Report 2022 revealed that the CVE-2021-42321 vulnerability in Microsoft Exchange was exploited in the wild only three days after it was showcased at the Tianfu Cup 2021. This suggests that threat actors may have obtained early access to it, enabling nearly simultaneous exploitation.[318]

[309] Ravie Lakshmanan, "Windows 10, Linux, iOS, Chrome and Many Others at Hacked Tianfu Cup 2021," October 18, 2021, https://thehackernews.com/2021/10/windows-10-linux-ios-chrome-and-many.html.

[310] Catalin Cimpanu, "Windows 10, iOS 15, Ubuntu, Chrome Fall at China's Tianfu Hacking Contest," *The Record*, October 17, 2021, https://therecord.media/windows-10-ios-15-ubuntu-chrome-fall-at-chinas-tianfu-hacking-contest.

[311] Catalin Cimpanu.

[312] Natto Team, "Tianfu Cup 2023: Still a Thing," *Natto Thoughts* (blog), November 17, 2023, https://nattothoughts.substack.com/p/tianfu-cup-2023-still-a-thing.

[313] "Win11首次被攻破，深信服亮剑「天府杯」," *Sangfor* (blog), November 1, 2023, https://www.sangfor.com.cn/news/eaacc57c78624727a3c4d8ec0ecd32fa.

[314] Insikt Group, "Charting China's Climb as a Leading Global Cyber Power," July 11, 2023, https://www.recordedfuture.com/charting-chinas-climb-leading-global-cyber-power.

[315] Alexander Marvi et al., "Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation," *Mandiant Blog* (blog), March 16, 2023, https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem.

[316] Natto Team, "Tianfu Cup 2023: Still a Thing."

[317] Eduard Kovacs, "VMware Patches Vulnerabilities Disclosed at Chinese Hacking Contest," *Security Week*, February 15, 2022, https://www.securityweek.com/vmware-patches-vulnerabilities-reported-researchers-chinese-government/.

[318] "Microsoft Digital Defense Report 2022."

Figure 16: i-SOON CEO Wu Haibo (Shutd0wn) discussing the feasibility of accessing vulnerabilities from the Tianfu Cup (Date and time, sender, receiver, original message, English translation)

2021-10-26 01:53:17	Shutd0wn	lengmo	天府杯比赛的那几个0DAY漏洞，据说是给了POC给公安了，这个能要到吗	I heard a rumor the 0DAY POCs in the Tianfu Cup competition were given to Public Security. Can I get this?"
2021-10-26 01:53:49	lengmo	Shutd0wn	要不到，我那天就问过。部里面给了江苏了	We can't get it - I asked them the other day - the department gave it to Jiangsu
2021-10-26 01:53:59	lengmo	Shutd0wn	每年都给的	they do that every year
2021-10-26 01:54:17	lengmo	Shutd0wn	说有的漏洞比较鸡肋	I've heard some of the vulns are pretty useless
2021-10-26 01:54:37	lengmo	Shutd0wn	我只能看看厅里面有没有给哪个地市	I can only check if the provincial department has given it to any prefecture/city
2021-10-26 01:55:36	Shutd0wn	lengmo	据说公安部拿到的是POC，写成EXP还要费点功夫	I'm hearing that the Ministry of Public Security got the POC, and it'll still take some effort to exploit it
2021-10-26 01:56:09	Shutd0wn	lengmo	像IOS那种漏洞，知道POC，搞成EXP也不容易	It's like iOS vulnerabilities - even if you know the POC, turning it into an exploit isn't easy
2021-10-26 01:56:18	lengmo	Shutd0wn	我问问	I'll ask
2021-10-26 01:56:54	lengmo	Shutd0wn	省厅给了无锡好像	Looks like the provincial department gave it to Wuxi
2021-10-26 01:57:07	lengmo	Shutd0wn	那天在我们这培训还说的	Someone said this at our training the other day too
2021-10-26 01:57:24	Shutd0wn	lengmo	嗯，你留意下，等他们扩散开了我们要一份	sounds good, wait for them to spread, we want a piece

Source: i-SOON leaked chat logs

The zero-days demonstrated at the Tianfu Cup sometimes exceeded typical competition standards. According to cybersecurity analyst JD Work, the practical significance of the exploit collections utilized in the 2021 Tianfu Cup resembles the high-value capabilities utilized in critical counter-terrorism operations by a Western government.[319]

The 2024 i-SOON leaks further substantiate the suspicions that zero-days submitted to the Tianfu Cup are indeed shared with Chinese government agencies. Internal I-SOON discussions indicate that exploits from the Tianfu Cup 2021 were transmitted to the "public security bureau" in Jiangsu (figure 16), strongly suggesting the involvement of the Ministry of Public Security (MPS).[320] The I-SOON chatlogs specifically note that “the Ministry will give it to Jiangsu every year, and it will not be given to all provinces. It is estimated that they are all given to strong provinces.”[321]

It is likely that the reference to the MPS is referring to the Ministry of State Security (MSS). During Intrusion Truth’s investigation into APT40 the group discovered a photo on QQ that depicted one of its members wearing a MSS uniform.[322] On another Chinese social media platform, the same individual openly discussed his connection with China's MPS, suggesting its utilization as a disguise for the MSS. Furthermore, Jiangsu province is known to host an MSS branch that is focused on intellectual property theft online (Turbine Panda or APT26). In 2022, former FBI cyber expert and Crowdstrike China analyst Adam Kozy, testified before the U.S.-China Economic and Security Review Commission that MSS officers frequently employ the MPS as a cover, affirming that “the MSS’s close ties to the MPS would become increasingly beneficial in the early 2000s, affording both convenient cover for MSS offices, which were often co-located with MPS offices.” He specifically cited the case of the Jiangsu branch of the MSS (APT26) operating out of MPS office buildings in Jiangsu (figure 17).[323]

[319] J.D. Work, “China Flaunts Its Offensive Cyber Power,” *War on the Rocks*, October 22, 2021, https://warontherocks.com/2021/10/china-flaunts-its-offensive-cyber-power/.
[320] Cyber Threat Research Team, “A COMPREHENSIVE ANALYSIS OF I-SOON’S COMMERCIAL OFFERING.”
[321] Cyber Threat Research Team.
[322] Intrusion Truth, “APT40 Is Run by the Hainan Department of the Chinese Ministry of State Security.”
[323] Adam Kozy, “Testimony before the U.S.-China Economic and Security Review Commission Hearing on ‘China’s Cyber Capabilities: Warfare, Espionage, and Implications for the United States.’”

Figure 17: Image showing the MSS often shares buildings with and uses the MPS for cover. This is one of at least two locations cyber contractors known as TURBINE-PANDA/APT26 were believed to operate out of on behalf of the MSS Jiangsu Department in Nanjing

Source: Adam Kozy's Testimony before the U.S.-China Economic and Security Review Commission

According to Harfang's analysis of the i-SOON leak, the chat logs suggest an institutional process in which vulnerabilities discovered for the Tianfu Cup are collected by the MPS (or MSS), distributed to provinces for cyber operations, and eventually shared with contractors. This likely mirrors the vulnerability reporting process of the MSS-run Chinese National Vulnerability Database (CNNVD).[324]

6.2.2 Shifting Targets and Incentives

For the most part, the Tianfu Cup contestants are searching for vulnerabilities in Western products. At the 2021 Tianfu Cup, Chinese products, such as Synology's DS220j NAS, Xiaomi's Mi 11 smartphone, and an undisclosed Chinese electric vehicle, remained untouched by participants due to the relatively low bounties (table 4). As a result, none of the participants even attempted to find vulnerabilities in these products.[325]

The Tianfu Cup in 2023 was very different as the product line-up shifted away from mostly from Western products towards Chinese ones, including word processing and office software and systems, such as WPS, UF YonBIP, Zhiyuan Collaborative Operation Management Platform, Panwei OA, Qi An Xin Trusted Browser, and so on. Although the top prizes continued to be awarded for exploits Western products, this shift highlighted China's diminishing reliance on Western technology and an increasing emphasis on domestically produced software products. In addition, the website of the Tianfu Cup 2023 is available in Mandarin-only. An English version, which was made available for the past editions, was dropped entirely.

The Chinese government has directed state-owned enterprises to replace all Western office software product with domestic alternatives by the year 2027.[326] According to Reuters, which gained access to a database maintained by the Chinese Ministry of Finance, in the year following September 2022, the number of tenders from state-owned enterprises, government and military bodies to nationalize equipment in China doubled from 119 to 235.[327] China's spending on replacing foreign hardware and software in 2022 surged to 1.4 trillion yuan (191 billion USD), marking a 16.2% year-on-year increase, as reported by IT research firm First New Voice.[328]

Table 4: Tianfu Cup 2021 Targets and Prizes

Target	2021TFC Prize(RCE)	2021TFC EXTRA Prize(RCE + Sandbox Escape)
Chrome	$50,000	$150,000
Safari	$40,000	$75,000
Adobe PDF Reader	$30,000	$40,000
Docker-CE	/	$60,000
Ubuntu 20/CentOS 8	/	$40,000
Microsoft Exchange Server 2019	$60,000	$200,000
Windows 10	$20,000	$40,000
VMware Workstation	/	$80,000
VMware ESXi	/	$180,000
Ubuntu + qemu-kvm	$60,000	$150,000
Parallels Desktop	/	$30,000
iPhone 12 pro	$120,000	$180,000
Domestic mobile phones(Android)	to be updated	to be updated
Synology DS220j	/	$10,000
ASUS Router AX56U	/	$10,000
Domestic vehicle	to be updated	to be updated

Source: https://therecord.media/windows-10-ios-15-ubuntu-chrome-fall-at-chinas-tianfu-hacking-contest

[324] Cyber Threat Research Team, "A COMPREHENSIVE ANALYSIS OF I-SOON'S COMMERCIAL OFFERING."

[326] "China Rushes to Swap Western Tech with Domestic Options as U.S. Cracks Down," *Reuters*, October 26, 2023, https://www.reuters.com/technology/china-rushes-swap-western-tech-with-domestic-options-us-cracks-down-2023-10-26/.

[327] "China Rushes to Swap Western Tech with Domestic Options as U.S. Cracks Down."

[328] "China Rushes to Swap Western Tech with Domestic Options as U.S. Cracks Down."

These efforts align with a broader objective. In December 2022, the Chinese government unveiled its Strategic Plan for Expanding Domestic Demand 2022–2035, aimed at stimulating significant "information innovation" (信创). Writing for The China Project, Barry van Wyk, explains that the government's plan of "information innovation" was introduced back in 2006. It seeks for China to attain self-sufficiency in advanced technologies and lessen its reliance on foreign suppliers.[329] In particular, it emphasizes the full domestication of China's IT infrastructure and the substitution of core components, such as semiconductors, software, and databases.

Overall, the information innovation plan focuses on four key areas: IT infrastructure, foundational software, application software, and information security. It progresses through three stages: Initial implementation in state institutions, expansion into key industries, and eventual adoption by consumer markets.[330] According to the Wall Street Journal, as recently as six years ago, Chinese government tenders predominantly sought semiconductors and software products from Western companies. By 2023, most government tenders were seeking Chinese tech products instead.[331]

While partly influenced by the heightened Western scrutiny of Huawei in recent years, there are additional factors motivating the information innovation plan. First, the Chinese government inherently distrusts U.S. hardware and software products, which was particularly exemplified by the Juniper hack and the enduring US government discussions on weakening encryption and inserting backdoors in U.S. technology products.[332] In December 2015, Juniper Networks disclosed the presence unauthorized backdoors in its firewalls – potentially allowing decryption of protected traffic – with suspicions pointing towards NSA involvement.[333] Second, because of the Snowden Leaks in 2013, Beijing emphasized data sovereignty, meaning keep data in-country and maintain control over it. Among other items, Snowden's disclosure of the PRISM program revealed extensive US surveillance efforts to collect electronic communication data from internet services and technology companies globally.

Featuring Chinese products in hacking competitions, such as the Tianfu Cup, coupled with a large prize pool might encourage the formation of teams that specialize in securing Chinese products. Heightened scrutiny from talented research teams might in turn likely strengthen China's defensive capabilities and enhance the reputation of its cybersecurity and software products globally.

Despite the Tianfu Cup's significant prize pool, participants have nonetheless voiced grievances, because internal team arrangements are structured in such a way that the prize money is distributed not only among the participating team members, but also across their organization, including their superiors. One Chinese participant complained online that "domestic security researchers are rising, but it can also be seen that there are also many teams who give up the competition, because according to this year's bonus distribution rules, teams that break the same project will share the bonus equally. In other words, the more people play the project, the less you get. If you use multiple sets of exploits to play the same project, you will lose more."[334] This setup thus likely diminishes some of the underlying motivation to pursue substantial rewards for the most challenging targets.[335] A source, which was granted anonymity for this report, further elaborated that, because companies like Qihoo 360 have numerous teams with sizable memberships, they are forced to consolidate researchers into a handful of teams that compete in the challenges. This often results in the exclusion of many talented researchers, which in turn results in diminished income for the excluded individuals and a lack of social recognition.

[329] Barry van Wyk, "Made in China 2025 Is Back, with a New Name and a Focus on Database Companies," *The China Project*, December 19, 2022, https://thechinaproject.com/2022/12/19/made-in-china-2025-is-back-with-a-new-name-and-a-focus-on-database-companies/.

[330] Barry van Wyk.

[331] Liza Lin, "China Intensifies Push to 'Delete America' From Its Technology," *The Wall Street Journal*, July 3, 2024, https://www.wsj.com/world/china/china-technology-software-delete-america-2b8ea89f?mod=hp_lead_pos1.

[332] Kim Zetter, "Researchers Solve Juniper Backdoor Mystery; Signs Point to NSA," *WIRED*, December 22, 2015, https://www.wired.com/2015/12/researchers-solve-the-juniper-mystery-and-they-say-its-partially-the-nsas-fault/#:~:text=Juniper%20Networks%2C%20a%20tech%20giant,traffic%20passing%20through%20Juniper's%20devices.

[333] Kim Zetter.

[334] riusksk, "Fuzzing平台建设的研究与设计," 漏洞战争 (blog), November 18, 2019, https://www.secrss.com/articles/15169.

[335] J.D. Work, "China Flaunts Its Offensive Cyber Power."

At the same time, there are not many other alternatives Chinese hackers can turn to. As highlighted by cybersecurity expert Adam Segal, the exclusion of Chinese researchers from international competitions has restricted alternative income sources for China's leading hackers.[336] The changed circumstances and lower economic opportunities for the current generation of hackers compels them to form closer associations with government agencies, to establish their own startup or institutions in China, and/or or join established companies. Some of the most prominent among these companies include the very ones sponsoring the Tianfu Cup. These include 360 Security, Qi An Xin, Cyber Kunlun, Huawei, Baidu, Alibaba, THU, the CAS Institute of Information Engineering, National Industrial Information Security Development Research Center, NSFOCUS Technology, Tianrong Xin, VenusTech, Topsec, and Yongxin Zhicheng. Most of these companies are top-tier zero-day suppliers to the MSS and contribute to China's MCF efforts in cyberspace. [337]

Some of the Chinese cybersecurity companies that sponsor the Tianfu Cup have been associated with state-sponsored cyber operations in the past. Topsec has provided cybersecurity services and training for the Chinese military for several years. The company has been implicated in several cyber-espionage campaigns, with the most notable incident being the 2015 hack of US insurance giant Anthem. The breach led to the exfiltration of personal identifiable information of nearly 78.8 million individuals.[338] Additionally, Huawei's affiliation with APT3, an MSS-affiliated Chinese espionage group[339], contributed to the skepticism and regulatory measures imposed by some countries globally to limit or exclude Huawei from critical infrastructure projects.

6.3 The Ant Group's Ant Financial Lightyear Security Lab

The Ant Group (蚂蚁集团)was formerly known as the Zhejiang Alibaba E-Commerce Company. The group was founded by Alibaba Group Holding to in the context of the rollout of Alipay in 2004 to address the trust issues in China's emerging online shopping ecosystem.[340] In 2011, the company spun off from Alibaba. Headquartered in Hangzhou, Zhejiang province, Ant Group has evolved into a technology giant, counting 25.000 employees and a reported revenue of about 11 billion USD in early 2024. [341] With a user base surpassing 1.3 billion, Ant Group's digital payments platform, Alipay, along with Tencent's WeChat Pay, command a virtual duopoly in China's mobile payments landscape. This dominance has propelled Ant Group to become the largest online provider of microfinance services in China, surpassing traditional financial institutions in the total amount of credit issued through its platform.[342]

Due to its substantial size, the Ant Group – like Tencent – faced tensions with the Chinese government. In late 2020, the company's founder Jack Ma resisted sharing customer credit data with government agencies and he even publicly criticized President Xi's campaign to strengthen financial oversight.[343] As a result, in early 2023, Ant Group announced that Jack Ma would cede control over the company.[344] Later that year, Beijing imposed fines exceeding 1 billion USD on both the Ant Group and Tencent.[345] This marked the end of Beijing's crackdown of the Chinese tech sector which started in late 2020. During the 2022 National Cyber Security Publicity Week in Hefei, Anhui Province, the Ant Group unveiled nine major security laboratories.[346] Among these, the Tianzhen, Tianji, and

[336] Yingzhi Yang, "China Discourages Its Hackers from Foreign Competitions so They Don't Help Others."

[337] Dakota Cary and Kristin Del Rosso, "Sleight of Hand: How China Weaponizes Software Vulnerabilities."

[338] Charles Riley, "Insurance Giant Anthem Hit by Massive Data Breach," *CNN Business*, June 2, 2015, https://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/.

[339] Insikt Group, "Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3," *Recorded Future Blog* (blog), May 17, 2017, https://www.recordedfuture.com/chinese-mss-behind-apt3.

[340] Alison Tudor-Ackroyd, and, and Alison Tudor-Ackroyd and Chad Bray, "What Is Jack Ma's Ant Group and How Does It Make Money?," *South China Morning Post*, October 27, 2020, https://www.scmp.com/business/banking-finance/article/3107294/what-jack-mas-ant-group-and-how-does-it-make-money.

[341] "Ant Group," *PitchBook* (blog), https://pitchbook.com/profiles/company/99609-31.

[342] Alison Tudor-Ackroyd, and, and Alison Tudor-Ackroyd and Chad Bray, "What Is Jack Ma's Ant Group and How Does It Make Money?"

[343] Lingling Wei, "China Blocked Jack Ma's Ant IPO After Investigation Revealed Likely Beneficiaries," *The Wall Street Journal*, February 16, 2021, https://www.wsj.com/articles/china-blocked-jack-mas-ant-ipo-after-an-investigation-revealed-who-stood-to-gain-11613491292.

[344] "Jack Ma to Give up Control of China's Ant Group, Firm Says," *The Guardian*, July 1, 2023, https://www.theguardian.com/business/2023/jan/07/jack-ma-to-give-up-control-of-chinas-ant-group-firm-says.

[345] "China Ends Tech Crackdown with Fines on Tencent and Ant Group," *The Japan Times*, August 7, 2023, https://www.japantimes.co.jp/news/2023/07/07/business/ant-group-fine/

[346] 中国网科技, "蚂蚁集团9大安全实验室亮相国家网安周，助力构建高质量安全生态," *Tech.China.Com.Cn*, May 9, 2022, https://tech.china.com.cn/roll/20220905/390687.shtml.

Tianqian labs prioritize "cutting-edge technology" security research to elevate security standards. The Tianshu and Tianmeng labs focus on cybercrime research and industry collaboration. More detailed information about the laboratories is not publicly available. It is unclear whether the Ant Financial Security Lightyear Laboratory, a key participant in events like the Tianfu Cup and international bug bounty programs, is part of these nine laboratories or whether it is the umbrella unit that houses all nine laboratories. The Ant Financial Security Lightyear Laboratory (蚂蚁金服光年实验室) was established in 2016 as part of the Ant Group.[347] In a 2022 post on Maimai, which is often likened to the Chinese equivalent of LinkedIn, the Ant Group outlined that the Lightyear Laboratory focuses on automated vulnerability discovery, browser security, virtualization, and database security. The Laboratory secured 3rd, 2nd, and 1st place in the Tianfu Cup in 2019, 2020, and 2023 respectively. It also emerged as the top zero-day vulnerabilities reporting Chinese company to Apple from 2021 to January 2022. The Ant Group is a top-tier technical support unit (TSU) for the MSS-run CNNVD. In 2023, the CNVD recognized the lab for its valuable contributions to vulnerability reporting.[348]

6.4 Cyber Kunlun's Kunlun Lab

Established in Beijing in 2021, Cyber Kunlun (北京赛博昆仑科技有限公司) provides cyber security solutions and IT services to a wide range of clients, including unspecified Chinese government institutions. The company specializes in the protection against zero-day attacks and conducts offensive and defensive drills seeking to simulate APT behavior.[349] Kunlun's history is deeply intertwined with Qihoo 360 and the 360 Vulcan team. The founder of Cyber Kunlun - Wenbin Zheng -is also the founder of 360 Vulcan and served as Qihoo 360's chief technology officer. Similarly, Cyber Kunlun's CTO - Xuebin Chen - was a director in Qihoo 360's Vulnerability Research Institute. According to the US-based research firm Margin Research, Cyber Kunlun collaborates closely with its mother company Qihoo 360 and has partnered with the Pangu Lab to integrate expertise in vulnerability mining, protection, advanced threat detection, and response for developing new security products and services.[350]

Although the exact size of its workforce is not disclosed publicly, Cyber Kunlun operates through two divisions: the Kunlun Lab and the Kunlun Advanced Offensive and Defensive Team. According to its website, Cyber Kunlun translates research on zero-day vulnerabilities into security solutions, aiding enterprises in preemptively detecting and defending against potential attacks. [351] Their main areas of focus include desktop and mobile security, cloud computing, virtualization security, and IoT device security.[352] The senior team members, instead, excel in offensive and defensive security research and have participated in various national and enterprise-level attack-defense exercises across industries like energy, banking, and media. Their primary focuses encompass enterprise security, host security, and application security.[353] Since its establishment, the Kunlun Lab has reported numerous vulnerabilities in products such as Windows, iOS, Google, VMware, as well as open-source software.[354] Between 2021 and 2023, the lab stood out as China's most prolific zero-day reporter to Microsoft's bug bounty program (section 7). Kunlun Lab entered the Tianfu Cup in 2021, securing the first position. In 2021, Sohu.com acknowledged Cyber Kunlun and the Pangu Team from Qi An Xin as China's most popular security teams.[355] While there is no publicly available information that links Cyber Kunlun to any malicious cyber campaigns, the company is a technical support unit (TSU) for the MSS-run CNNVD.[356]

[347] "2秒拿下国际知名厂商项目，蚂蚁安全实验室新锐战队于'天府杯'斩获三项成果," *Gushiciku.Cn* (blog), October 18, 2021, https://www.gushiciku.cn/pl/a2k8.
[348] "2022年度CNVD支撑单位年度工作情况及优秀单位个人表彰名单."
[349] "Cyber Kunlun," *Home* (blog), accessed November 3, 2024, https://www.cyberkl.com/.
[350] Margin Research, "The Chinese Private Sector Cyber Landscape" (Margin Research, April 25, 2022).
[351] "Cyber Kunlun."
[352] "Cyber Kunlun."
[353] "Cyber Kunlun."
[354] Dave Aitel et al., "China's Cyber Operations: The Rising Threat to American Security" (Margin Research, 2022), https://margin.re/content/files/2023/01/China-s-Cyber-Operations-Full-Report.pdf.
[355] "顶级安全实验室联手 昆仑实验室与盘古实验室将推移动安全新品," *Sohu.Com* (blog), August 4, 2021, https://www.sohu.com/a/481289655_99975515.
[356] Dakota Cary and Kristin Del Rosso, "Sleight of Hand: How China Weaponizes Software Vulnerabilities."

7 Bug Bounties

This section centers on an analysis of the contributions of Chinese research teams to the bug bounty programs of Android (Google), Microsoft, and Apple between 2017-2023. It also examines Chinese bug bounty programs, their framework, and their comparative monetary incentives when juxtaposed with other international initiatives.

Key Points

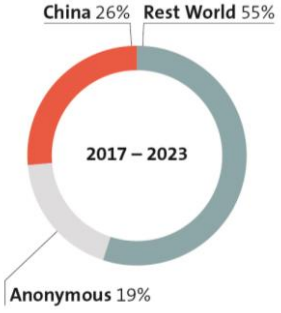
- From 2017 to 2023, China accounted for 27% of all vulnerabilities reported to the bug bounty programs of Apple, Google Android, and Microsoft, contrasting with the rest of the world at 59%.
- From 2017 to 2020, Qihoo 360 and Tencent dominated submissions for Microsoft, Google Android, and Apple, mirroring performance observed at Pwn2Own and the Tianfu Cup.
- From 2021 to 2023, the Kunlun Lab, the Oppo Amber Security Lab and the Ant Lightyear Security Lab became primary contributors for Microsoft, Google Android, and Apple respectively.
- Teams affiliated with Qihoo 360 and Tencent notably reduced their contributions from 2021 to 2023, partly due to US sanctions on Qihoo 360 and talent transitions among companies.
- The success of Chinese teams is frequently attributed to a handful of individuals, with shifts in a team's performance often linked to a single or a few individuals transitioning between companies.
- The migration of researchers to other Chinese firms combined with the creation of new cyber security companies, is likely leading to an expansion and diversification of China's offensive cyber capabilities.

7.1 Background

Bug bounty programs are similar to hacking competitions. In hacking competitions, researchers showcase exploits to prove their practicability and speed in a real-world setting. Bug bounty programs are online crowdsourcing initiatives that reward individuals for finding and reporting software bugs and vulnerabilities. These reports must contain enough detail for the company to reproduce the issue.[357] The analysis of the contributions of Chinese teams to the bug bounty programs of Android (Google), Microsoft, and Apple can be divided into two distinct periods: 2017-2020 and 2021-2023.

In 2017, the Chinese teams established themselves and the three bug bounty programs sufficiently matured. In 2020, the US sanctioned Qihoo 360, which – at the time – was a major contributor to the three bug bounty programs. The sanctions led to a significant reduction in the vulnerability reporting from Qihoo teams to US companies.[358] Tencent decreased its contributions to the three bug bounty programs around the same period. The announcement of the RMSV laws in 2020, which mandates that researchers submit zero-days to state authorities first, raised concerns about the potential disappearance of a significant channel for vulnerability reporting within the global ecosystem. An overview of the combined submissions from Chinese research teams in the three bug bounty programs from 2017 to 2023 (figure 18) shows that China contributed 27% of all vulnerabilities, while the rest of the world accounted for 59%. 14% of submissions were anonymous.

Figure 18: Vulnerabilities Submitted to Apple (2017-Jan 22), Google Android and Microsoft (2017-23)



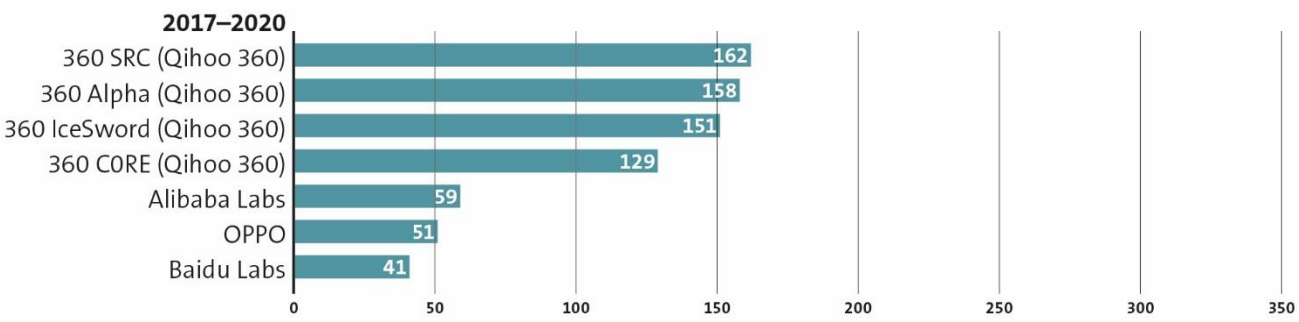
Source: Compiled by the Author

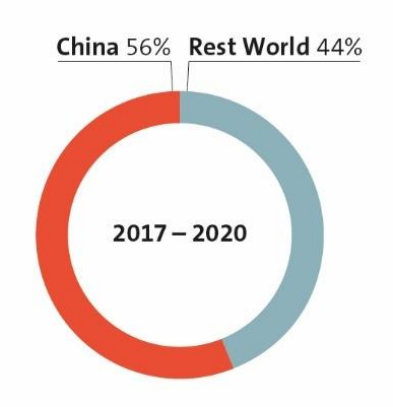
[357] TechTarget Contributor, "Bug Bounty Program," *WhatIs?* (blog), n.d., https://www.techtarget.com/whatis/definition/bug-bounty-program.

[358] Stewart Scott, Sara Ann Brackett, Yumi Gambrill, Emmeline Nettles, Trey Herr, "Dragon Tails: Preserving International Cybersecurity Research."

7.2 Android (Google)

Figure 19: Vulnerabilities Submitted to Android (2017-20)





Source: Compiled by the Author

From 2017 to 2020, Chinese researchers contributed 916 vulnerabilities to Google. This represents 56% of the vulnerabilities reported worldwide to Google Android (approx. 19 vulnerability reports per month). By contrast, the rest of the world accounted for 955 vulnerabilities (44%). Qihoo 360's research teams were the primary contributors (figure 19). Collectively, the Qihoo teams reported almost 70% of all the vulnerabilities reported by Chinese researchers. This is almost as many vulnerabilities as reported by the rest of the world combined. A handful of individual researchers within the Qihoo teams were particularly impactful. Within 360 C0RE, over 60% of vulnerabilities were reported by Mingjian Zhou either individually or in collaboration with a few additional team members. In 2017, 360 C0RE was recognized by the Android Security Team as the platform's "top research team" for submitting 118 vulnerability reports.[359]

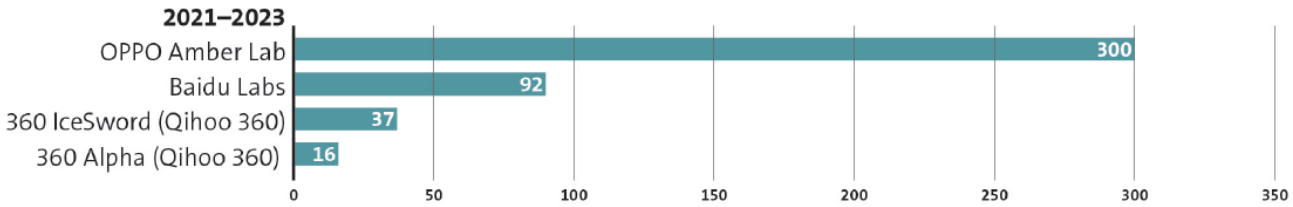
Within 360 Alpha, nearly all vulnerabilities were reported by Guang Gong. In 2018, Google awarded Guang Gong 112.000 USD, then Google's largest bug bounty payout ever, for the submission of a remote exploit chain on a Google's Pixel phone.[360] In 360 IceSword, over half were reported by Chen Gengjia, either individually or in collaboration with other team members. Within 360 SRC, over 50% of vulnerabilities were reported by Han Zinuo. In Baidu Labs, nearly half of their submitted vulnerabilities were reported by two researchers, Chenfu Bao and Lenx Wie.

Between 2021 and 2023, China reported 680 vulnerabilities to Google Android, making up a mere 35% of the global total (approx. 19 vulnerabilities per month). By comparison, the rest of the world contributed 1175 vulnerabilities, accounting for 65% of the total (figure 20). Qihoo's 360 teams accounted for only 16% of all the vulnerabilities reported by Chinese researchers, whereas the Oppo Amber Security Lab accounted for over 40%. Oppo is a leading Chinese consumer electronics manufacturer specializing in smartphones, smart devices, audio devices, and various other electronic products. Most vulnerabilities reported by OPPO were credited to Han Zinuo, who left Qihoo's 360 SRC team for OPPO in 2020. Following his departure, the submissions from 360 SRC significantly declined while OPPO experienced a notable surge. Out of the 300 vulnerabilities reported by OPPO, the overwhelming majority can be attributed to Han Zinuo.

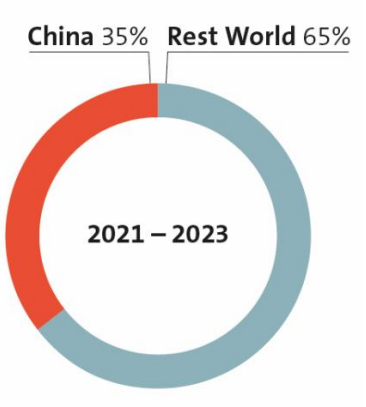
[359] Mayank Jain and Scott Roberts, "2017 Android Security Rewards," *Android Developers Blog* (blog), n.d., https://android-developers.google-blog.com/2017/06/2017-android-security-rewards.html.

[360] Avery Hartmans, "A Superstar Chinese Hacker Just Won $112,000 from Google, Its Largest Bug Bounty Ever."

Figure 20: Vulnerabilities Submitted to Android (2021-23)



The overall decrease in vulnerability submission by Chinese researchers to Google Android might have been partially driven by the U.S. government's crackdown on Huawei. In May 2019, Google suspended Huawei's Android license, which at the time accounted for 40% of the Chinese smartphone market. [361] [362] The reduction of the Qihoo 360's submissions in the years 2021-2023 are likely linked to the U.S. sanctions levied against Qihoo 360 in May 2020.[363] During this period, many security researchers either left Qihoo, joined other companies, or possibly changed their researcher focus. Han Zinuo's move to Oppo ought to be viewed in this light, as Oppo's operating system is based on Android Open-Source Project, which also explains the company's focus on reporting Android vulnerabilities.[364]



Source: Compiled by the Author

[361] Colin Lecher, "White House Cracks down on Huawei Equipment Sales with Executive Order," *The Verge*, May 15, 2019, https://www.theverge.com/2019/5/15/18216988/white-house-huawei-china-equipment-ban-trump-executive-order.

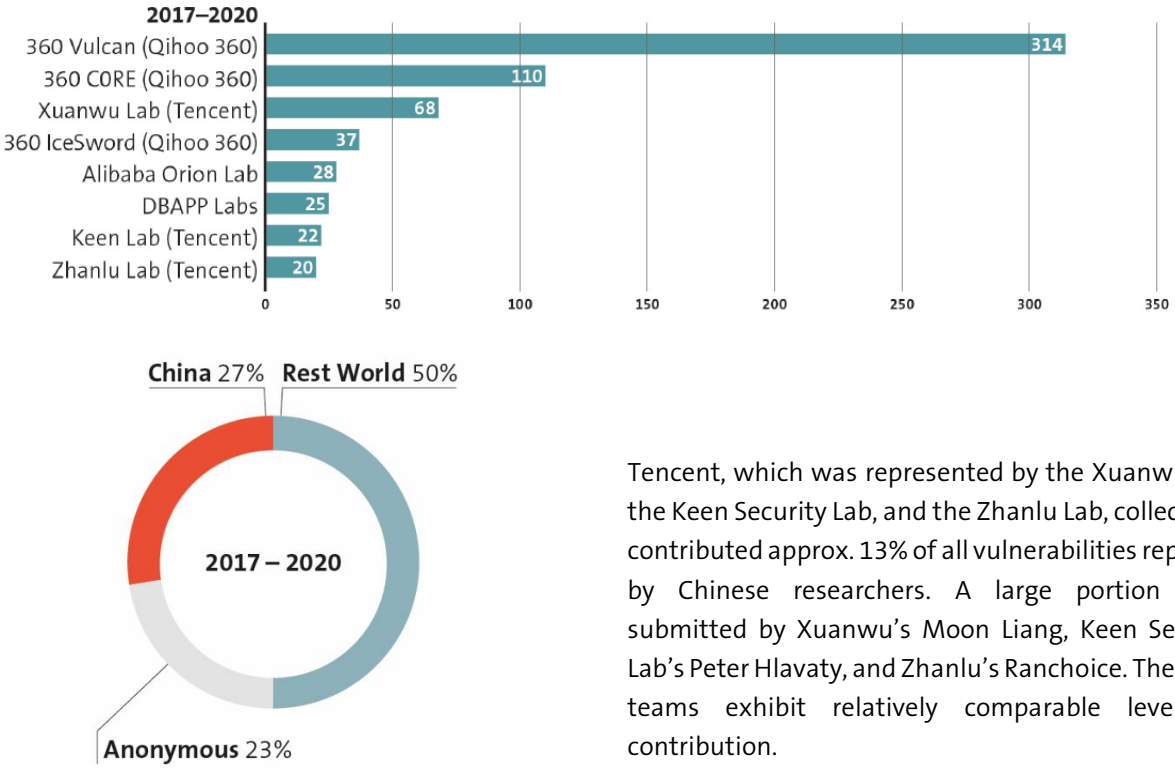
[362] Team Counterpoint, "Huawei Captured a Record 40% Share in Chinese Smartphone Market in Q3 2019," *Counterpoint* (blog), October 30, 2019, https://www.counterpointresearch.com/insights/huawei-captured-record-40-share-chinese-smartphone-market-q3-2019/.

[363] https://www.federalregister.gov/documents/2020/06/05/2020-10869/addition-of-entities-to-the-entity-list-revision-of-certain-entries-on-the-entity-list

[364] Sareena Dayaram, "Oppo's ColorOS 14 Goes Global: Here's What to Expect From the New Mobile OS," *CNET*, November 15, 2023, https://www.cnet.com/tech/mobile/oppos-coloros-14-goes-global-heres-what-to-expect-from-the-new-mobile-os/.

7.3 Microsoft

Figure 21: Vulnerabilities Submitted to Microsoft (2017-20)



Source: Compiled by the Author

From 2017 to 2020, Chinese researchers contributed 863 vulnerabilities to Microsoft, constituting 27% of the global total (approx. 18 vulnerabilities per month). The rest of the world reported 1580 vulnerabilities (~50%) 713 vulnerabilities (23%) were submitted anonymously. The primary contributors to Microsoft's bug bounty program are Chinese research teams with a track record in hacking competitions (figure 21).

Qihoo 360 was responsible for close to 60% of all Chinese submissions. The 360 Vulcan team reported most of these. Vulcan team member Yuki Chen reported 215 of the 314 vulnerabilities submitted. In 2020 alone, Yuki Chen reported 106 vulnerabilities to Microsoft. He has been recognized as the top global bug hunter by the Microsoft Security Response Center (MSRC) in 2019[365], 2021[366], 2022[367], and 2023.[368]

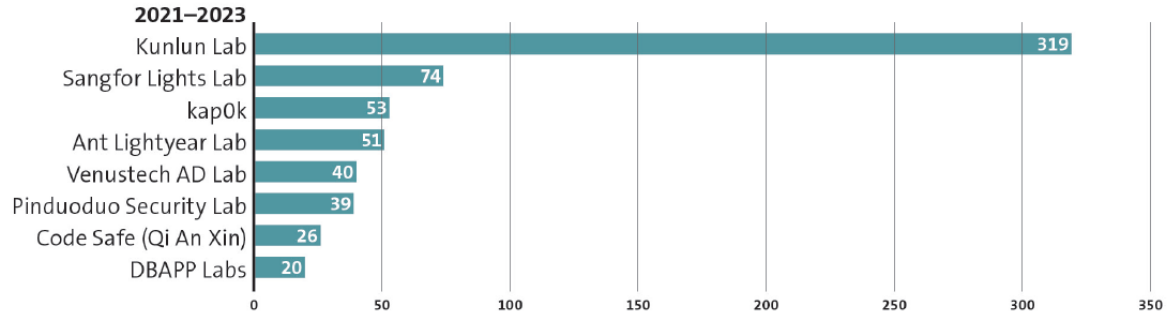
Tencent, which was represented by the Xuanwu Lab, the Keen Security Lab, and the Zhanlu Lab, collectively contributed approx. 13% of all vulnerabilities reported by Chinese researchers. A large portion were submitted by Xuanwu's Moon Liang, Keen Security Lab's Peter Hlavaty, and Zhanlu's Ranchoice. The other teams exhibit relatively comparable levels of contribution.

From 2021 to 2023, Chinese entities reported 783 vulnerabilities to Microsoft, making up 18% of the global total (approx. 22 vulnerabilities per month). The rest of the world reported 3290 vulnerabilities (75%). 328 vulnerabilities (7%) were reported anonymously (figure 22).

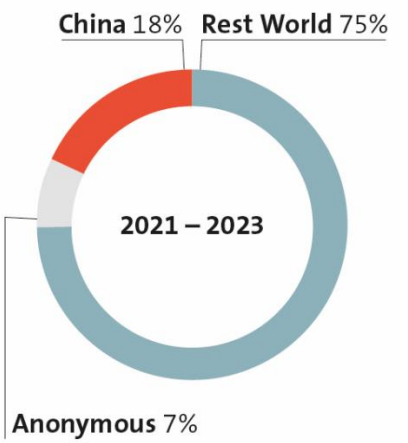
The Kunlun Lab accounted for approx. 41% (319 out of 783) of the total vulnerabilities submitted by Chinese researchers. 62% (197) of the vulnerabilities submitted by Kunlun Lab were reported by Yuki Chen who left 360 Vulcan in 2020. Today, the Kunlun Lab stands out as the unparalleled China-based reporter of vulnerabilities to the MSRC. For Microsoft's April 2022 Patch Tuesday, it reported 36 of the 145 vulnerabilities fixed, including half of the 10 critical vulnerabilities addressed.[369]

[365] Sylvie Liu, "Announcing 2019 MSRC Most Valuable Security Researchers."
[366] Lynn Miyashita, "Congratulations to the MSRC 2021 Most Valuable Security Researchers!," *Microsoft MSRC* (blog), April 8, 2021, https://msrc.microsoft.com/blog/2021/08/congratulations-to-the-msrc-2021-most-valuable-security-researchers/.
[367] "Leaderboard 2022," *Microsoft MSRC* (blog), n.d., https://msrc.microsoft.com/leaderboard.
[368] "Leaderboard 2022," 202.
[369] Ed Tragett, "NSA Reports 1 Bug under Attack, Chinese Firm 36, as Patch Tuesday Lands with 0days, Drama," *The Stack*, December 4, 2022, https://www.thestack.technology/april-patch-tuesday-hyper-v-rce/.

Figure 22: Vulnerabilities Submitted to Microsoft (2021-23)



The other Chinese teams exhibit relatively comparable levels of contributions. Sangfor Lights Lab and the Ant Security Lightyear Lab were rising stars at the Tianfu Cup as well. Sangfor likely greatly benefited from former 360 C0RE member Peng Zhiniang joining its ranks. Peng left Qihoo 360 to become Sangfor's Security Department's CTO in late 2020.[370] Between 2021 and 2023, he contributed to the reporting of 69 of Sangfor's 74 submitted vulnerabilities. The third largest contributor in 2021-2023, kap0k, is likely associated with the South China University of Technology's (华南理工大学) kap0K CTF team, which was established in March 2017. 31 of the 51 vulnerabilities submitted by the Ant Security Lightyear Lab were reported by researcher Zhang Ziming.[371]



Source: Compiled by the Author

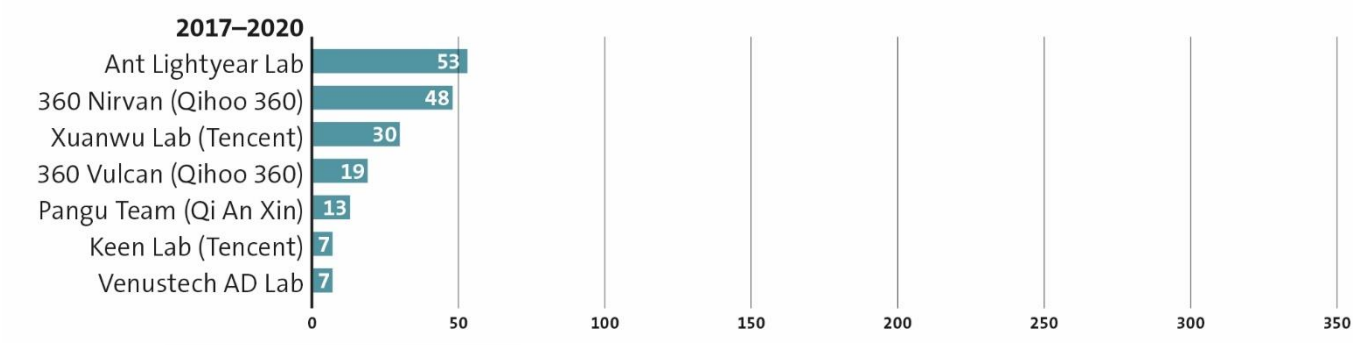
Qihoo 360's participation in Microsoft's bug bounty program dramatically reduced after 2020. This is attributable to US sanctions against the company and the departure of key talent, such as Yuki Chen and Peng Zhiniang. Despite the submission reduction, 360 IceSword researchers identified a vulnerability in the Hyper-V virtualization engine in 2021, resulting in a 200.000 USD bounty — at the time the largest bounty ever awarded by Microsoft. Tencent also significantly reduced its contributions during the same period.

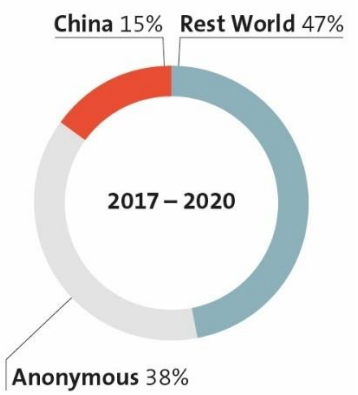
[370] "Zhiniang Peng," *LinkedIn* (blog), n.d., https://www.linkedin.com/in/zhiniang-peng-928b87114/?locale=en_US.

[371] "2020 WCTF **前瞻**：顶级强队网络'**沙**场'练兵，猝火成刚问鼎'**网**战之巅.'"

7.4 Apple

Figure 23: Vulnerabilities Submitted to Apple (2017-20)



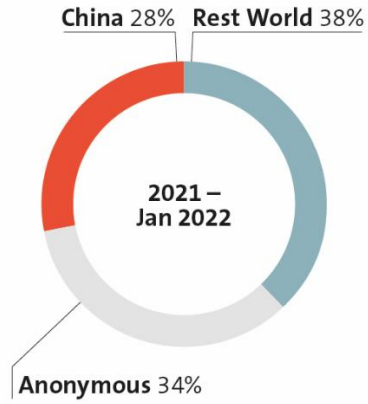


Source: Compiled by the Author

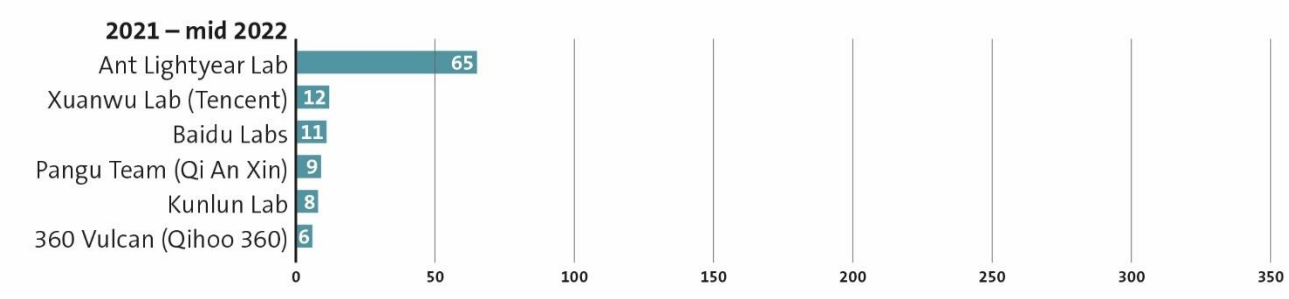
Between 2017 and 2020, Chinese researchers reported 307 vulnerabilities to Apple's bug bounty program, which represents ~15% of the global total (approx. 6 vulnerabilities per month). By contrast, the rest of the world reported 957 vulnerabilities (47%). 785 vulnerabilities (33%) were reported anonymously. The primary Chinese contributors were from research teams with a track record in hacking competitions (figure 23). Collectively, Qihoo accounted for 31% of the total vulnerabilities reported to Apple by Chinese researchers. Tencent comes at a close second, with approx. 18%. The Ant Security Lightyear Lab follows with 17% of total vulnerabilities submitted.

Between 2021 and January 2022, Chinese researchers reported 142 vulnerabilities to Apple, comprising ~28% of the global total (approx. 11 vulnerabilities per month). By contrast, the rest of the world reported 197 vulnerabilities (38%). 175 vulnerabilities (34%) were reported anonymously. Among the Chinese submissions, the Ant Security Lightyear Lab stands out with 46% of all disclosed vulnerabilities (figure 24). Despite the lack of more recent data, we can assume that the Ant Security Lightyear Lab – due its dominant role in previous years – will continue to play a key role among Chinese researchers submitting vulnerabilities to Apple's bug bounty program. This assumption is further supported by the lab's performance at the Tianfu Cup 2023 in which it secured the 1st place.

Figure 24: Vulnerabilities Submitted to Apple (2021-Jan 22)



Source: Compiled by the Author



7.5 Chinese Bug Bounties

Finding China-based bug bounty platforms and obtaining information on payouts for critical vulnerability submissions is challenging. According to a source who was granted anonymity for this report, there are a few bug bounty programs available in China. Qihoo's 360 BugCloud and the Tencent Security Response Center are operated by local companies which primarily test their own devices. These bug bounty program have stringent terms and offer either unspecified rewards or pay outs that are relatively low.[372] The YesWeHack website, which handles payouts on behalf of Tencent, states that Tencent offers a maximum payout of 6.425 USD for a critical vulnerability.[373] By contrast, Microsoft provides detailed breakdowns of maximum payouts for each product, with the highest being 250.000 USD for critical vulnerabilities in Microsoft Hyper-V. Such differences also hold true when it comes exploit acquisition platforms.

Initiatives like the NVWA Project's bug bounty program (女娲计划), which was launched by the Chinese Academy of Sciences' Software Research and Development Center, provide varying rewards for identifying vulnerabilities in both domestic and international products (table 5). The platform features a comprehensive list called the "Long-term Table," which enumerates 213 global products and systems and the maximum rewards for zero-day vulnerabilities for each of them. The majority of these vulnerabilities must be "zero-click" exploits, with only a few allowing "1-click" zero-days.

The highest payouts on NVWA include critical vulnerabilities in Android (2.8 million USD), iOS (2 million USD), WhatsApp (1.4 million USD), Telegram (695.000 USD), Cisco (694.580 USD), Chrome (417.000 USD), and Microsoft (139.000 USD). The average payout for a vulnerability is approximately 35.500 USD.

Table 5: NVWA Target List

Target Directory

Including but not limited to the following ranges, the target directory will be updated regularly

New Table[new]

Target	Version	Type	Require	Date	Effective date(d)	TopPrice(¥)

Long-term Table

Target	Version	Type	Require	Date	Effective date(d)	TopPrice(¥)
3CX	-	RCE	Zero-Click	2020-09-04	∞	150,000
ABB	-	RCE	Zero-Click	2020-09-04	∞	150,000
ABB Ability	-	RCE	Zero-Click	2020-09-04	∞	150,000
Acme	-	RCE	Zero-Click	2020-09-04	∞	150,000
ActiveMQ	-	RCE	Zero-Click	2021-01-05	∞	50,000
ADC	-	RCE	Zero-Click	2021-01-05	∞	20,000
Adobe	-	RCE	1-Click	2020-09-04	∞	800,000
Adobe-PDF	-	RCE	1-Click	2019-11-08	∞	800,000
advantech	-	RCE	Zero-Click	2020-09-04	∞	150,000
Airos	-	RCE	Zero-Click	2020-09-04	∞	350,000

Source: https://nvwa.org/

[372] "360 BugCloud," *Qihoo 360* (blog), n.d., https://bugcloud.360.net/post-Leak/firstPost.

[373] "Tencent Bug Bounty Program," *YesWeHack* (blog), July 25, 2023, https://yeswehack.com/programs/tencent-bug-bounty-program.

While the anonymous source acknowledged that NVWA is one of the most popular exploit acquisition platforms in China, the author was unable to verify whether it is among the exploiting acquisition platforms with the highest payouts in China.

By comparison, U.S.-based exploit acquisition platform Zerodium offers payouts of up to 2.5 million USD.[374] Back in 2018, a startup based in the United Arab Emirates called Crowdfense introduced bounties of up to 3 million USD for either partial or complete zero or one-click exploit chains targeting Windows, MacOS, iOS, and Android.[375] In late-2023, the Russian zero-day acquisition firm, Operation Zero, increased its rewards to 20 million USD for exploit chains affecting both Android and iOS platforms. It is unclear what the maximum reward would be for a single exploit.[376]

Interestingly, some of the China-based platforms, such as 360 BugCloud, operate under a "talk about money first, then hand over holes" model, which allows researchers to negotiate their compensation terms.[377] However, like for hacking competitions, when Chinese researchers report vulnerabilities on relevant platforms, they may be required to share a significant portion of the bounty prize with their employer. According to insights from a source that was granted anonymity for this report, this split can occasionally reach up to 50%. While Chinese researchers can still make a lot of money by reporting vulnerabilities to international bug bounty programs, several challenges persist. These include U.S. sanctions against prominent Chinese companies, such as Qihoo 360, and Beijing's punishing measures as seen in the case of the Log4j incident, which possibly generated a climate of fear among Chinese researchers to report vulnerabilities to non-Chinese vendors. It is probable that vulnerabilities reported to Chinese third-party platforms, such as the NVWA Project, are shared with government authorities in line with relevant regulations.

This is particularly likely in the case of the NVWA Project due to its strong ties to the state. The Chinese Academy of Sciences (CAS), which oversees the platform, is one of three academic institutions directly under the State Council of the People's Republic of China.[378] Constitutionally, the State Council serves as the executive branch of the National People's Congress, the highest state power organ, and the top administrative body in the country.[379] CAS actively participates in the promotion of MCF through its own Military-Civil Fusion Development Research Centre.[380] It also sponsors the Tianfu Cup.

[374] "Zerodium Exploit Acquisition Program," *Zerodium* (blog), n.d., https://zerodium.com/program.html.
[375] Ionut Arghire, "Research Firm Offers $3 Million for iOS, Android 0-Days," *Security Week*, November 3, 2019, https://www.securityweek.com/research-firm-offers-3-million-ios-android-0-days/.
[376] Lorenzo Franceschi-Bicchierai, "Startup Offers $3 Million to Anyone Who Can Hack the iPhone," *Vice News*, April 25, 2018, https://www.vice.com/en/article/pax987/crowdfense-offers-3-million-for-iphone-android-hacks.
[377] "Home," *360 BugCloud* (blog), n.d., https://bugcloud.360.net/home.
[378] "State Council Organization Chart," *The State Council. The People's Republic of China* (blog), accessed March 13, 2024, https://english.www.gov.cn/state_council/2014/09/03/content_281474985533579.htm.
[379] "State Council Leaders," *The State Council. The People's Republic of China* (blog), accessed March 13, 2024, https://english.www.gov.cn/institutions/.
[380] "University of Chinese Academy of Sciences (UCAS)," *ASPI* (blog), accessed March 13, 2024, https://unitracker.aspi.org.au/universities/university-of-chinese-academy-of-sciences/.

8 Conclusion

This report has identified China's primary civilian hacking teams and their research focuses on Western products and systems by examining their participation in prominent hacking competitions and bug bounty programs. More broadly, it has explored how these initiatives perpetuate a cycle of talent development and innovation, enabling individual hackers to refine their skills, establish new companies specializing in both offensive and defensive cyber capabilities, and to set up new China-based hacking competitions. This process sustains China's offensive cyber ecosystem in the long run.

This is significant because China's offensive cyber ecosystem leverage civilian talent in unprecedented ways for state-sponsored cyber operations. High-performing Chinese hacking teams in prominent competitions and bug bounty programs are often affiliated with companies that collaborate with government agencies on a wide spectrum of cyber activities, including supplying them with a significant number of vulnerabilities for offensive purposes.

China's approach has enabled it to enhance the efficacy of its cyber operations against foreign targets while introducing operational asymmetries with other states. This is attributed to certain elements of China's offensive cyber ecosystem, such as the flow of vulnerabilities from the private sector to government agencies, which may pose ethical dilemmas for democratic states to replicate. This is because it could potentially conflict with their fundamental values, such as transparency and responsible vulnerability disclosure.

It ultimately rests with each country to determine whether and which elements of the Chinese model to adopt based on its own values and specific needs. However, it is crucial to consider the risks, especially if government agencies circumvent the vulnerability disclosure process to stockpile vulnerabilities. For instance, in 2016, a hacking group called the Shadow Brokers hacked and disclosed a cache of stockpiled NSA cyber capabilities, including the EternalBlue vulnerability, which was later used in the devastating WannaCry and NotPetya ransomware attacks. Additionally, the misuse of vulnerability findings could undermine confidence in the disclosure process and dissuade researchers from reporting vulnerabilities.

Broadly, states can draw inspiration from China's holistic approach, particularly its robust integration of hacking competitions and bug bounty submissions into university curricula and corporate cultures. By adopting similar practices, democracies can empower civilian hackers to identify and cultivate their strengths while fostering networks of skilled individuals. This can significantly enhance the cybersecurity posture of the organizations they engage with, ultimately contributing to the broader cybersecurity ecosystem, including national security objectives.

Future studies in this area may explore how states can strategically leverage aspects of China's cyber approach that align with their core values, while also addressing security implications arising from resulting asymmetries in cyber intelligence and defense. This entails a nuanced examination of how to effectively mitigate any associated risks. At a more granular level, further research could delve into China-based hacking competitions and other pertinent actors that may not have been fully explored in this report.

Appendix A: 360 DSG Research Labs

Product Lines

360 Safeguard / 360 Total Security & Other Anti-Virus Products and Services

360 Vulcan

360 QVM

360 Baize

360 Anti-Virus

360 Mobile Security

360 Alpha

360 FiberHome

360 C0RE

Departments

360 Security Engineering Institute

360 IceSword

360 Security Response Center

360 SRC

360 Nirvan

360 0kee

360 Vulpecker

360 MeshFire

360 Gear Team

360 Real Network Threat Awareness Department

360 RedTeam (+ 360 0kee)

Other Research Areas and Focus

(Unknown Affiliation to Specific Products or Departments)

Cybercrime & Anti-Fraud

360 Track Team

Automotive Cybersecurity

360 Vehicle Cyber Security

Threat Intelligence & Hunting

360 Helios

360 Advanced Threat Response

360 Noah

360 Hunting Zero

Wireless and Radio

360 Unicorn

Appendix B: Tencent United Security Lab

As Shown on https://s.tencent.com/research

Keen Lab

Anti-Virus Lab

Xuanwu Lab

Yunding Lab

Zhuque Lab

Big Data Lab

Tianma Lab

As Shown on https://m.qq.com/security_lab

Anti-Fraud Lab

Mobile Security Lab

Zhanlu Lab

Keen Lab

Xuanwu Lab

Anti-Virus Lab

Yunding Lab

About the Author

Eugenio Benincasa is a Senior Researcher in the Cyber Defense Project with Risk and Resilience Team at the Center for Security Studies (CSS) at ETH Zürich. Prior to joining CSS, he worked as a Threat Analyst at the Italian Presidency of the Council of Ministers in Rome (Italy) and as a Research Fellow at the research institute Pacific Forum in Honolulu (Hawaii, U.S.), where he focused on cybersecurity issues.

His research interests include China's offensive cyber ecosystem, vulnerability research and disclosure processes, the applicability of international law to cyberspace, and cyber disarmament.

CSS
ETH Zürich

The Center for Security Studies (CSS) at ETH Zürich is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.