CYBER
THREAT
ANALYSIS
CHINA

Recorded Future®

By Insikt Group®

November 7, 2023

Charting China's Climb as a Leading Global Cyber Power

Executive Summary

Over the past half-decade, Chinese state-sponsored cyber operations have transformed, emerging as a more mature, stealthy, and coordinated threat than in previous years. This new paradigm is exemplified by the widespread exploitation of zero-day and known vulnerabilities in public-facing security and network appliances. It is coupled with a heightened emphasis on operational security, minimizing evidence of intrusion activity, and impeding adversary tracking tradecraft, including through the use of extensive anonymization networks and "living-off-the-land" techniques.

These observed shifts have likely been influenced by both internal factors, such as major restructuring within China's military and changes in domestic vulnerability regulations, and external factors, including public reporting and exposures by Western governments and the cyber threat intelligence community. This evolution of Chinese state-sponsored cyber operations toward greater stealth and operational security has created a more complex and challenging landscape for target organizations, governments, and the cybersecurity community.

Chinese cyber-enabled economic espionage activity has evolved from earlier practices characterized by the theft of a very broad range of commercial intellectual property (IP) to a focused strategy geared toward supporting more specific strategic, economic, and geopolitical goals, including those associated with foreign investment projects under the Belt and Road Initiative (BRI) and critical technologies. Consequently, in the context of both cooperative foreign investment and economic competition, governments and corporations may face compromised negotiating positions and unfair competition enabled through cyber espionage. Such targets of persistent Chinese state-sponsored cyber activity must reevaluate risk assessments, recognizing that cyber risk extends beyond data breaches to encompass potential implications for negotiations, competitiveness, and strategic positioning.

Due to the focus on developing novel exploits for public-facing devices, a vulnerability-centric approach to network defense is insufficient for organizations likely to be persistently targeted by Chinese state-sponsored activity. This emphasizes the importance of improving defense-in-depth measures focusing on detecting post-exploitation persistence, discovery, and lateral movement activity. A large proportion of the targeted public-facing appliances have limited visibility, logging capabilities, and support for traditional security solutions; organizations should consider these factors when initially procuring network appliances in order to enhance the ability to detect and respond to threats.

Key Findings

- Chinese state-sponsored cyber operations focus on targets that align with China's military, political, economic, and domestic security priorities. In particular, Chinese state-sponsored groups have regularly demonstrated an adaptability often influenced by geopolitical developments, including the Russia-Ukraine conflict or regional geopolitical flashpoints within the Asia-Pacific region.
- As China continues to assert its influence and pursue objectives in the Asia-Pacific region, particularly in Taiwan and the South China Sea, public and private sector entities operating in this region are likely to face an elevated risk of both traditional espionage activities by Chinese cyber threat actors in addition to more subversive cyber and information operations.
- Chinese threat activity groups have shifted heavily toward the exploitation of public-facing appliances since at least 2021. Over 85% of known zero-day vulnerabilities exploited by Chinese state-sponsored groups during this subsequent period were in public-facing appliances such as firewalls, enterprise VPN products, hypervisors, load balancers, and email security products.
- This focus on exploiting zero-days in public-facing appliances and the rapid weaponization of known vulnerabilities in these products has proved an effective tactic in scaling initial access against a wide range of global targets. With organizations continuing to move to the cloud, a similar heightened emphasis on the targeting of these environments is likely in the near future.
- The observed sharing of malware and exploit capabilities across Chinese state-sponsored actors is likely enabled by both upstream capability developers and wider domestic policy around software vulnerability discovery and weaponization.

China's Evolution into a Leading Global Cyber Power

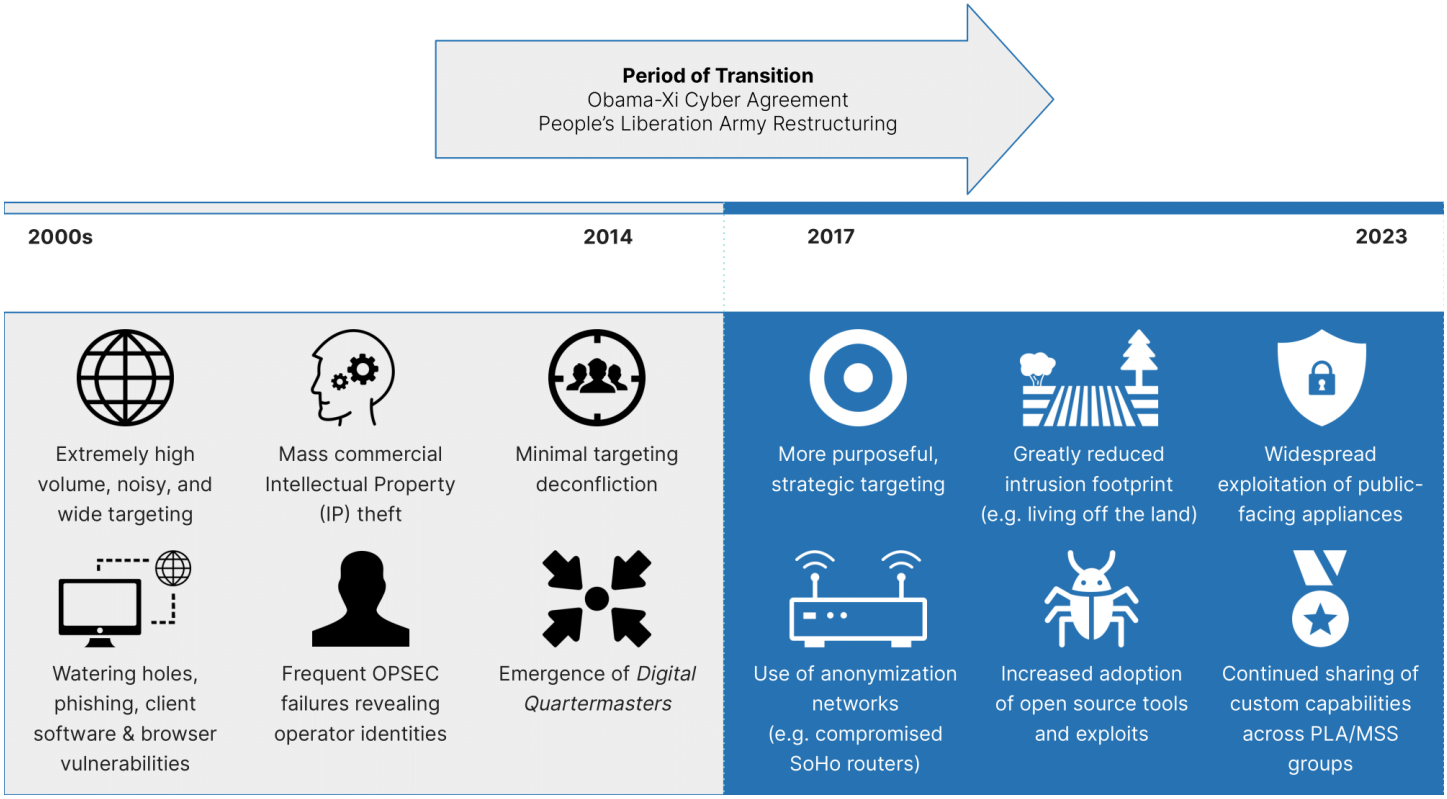

Figure 1: *Evolution of Chinese cyber-espionage activity (Source: Recorded Future)*

In the late 2010s, a new wave of Chinese state-sponsored activity began to emerge that placed a much greater emphasis on hindering detection, attribution, and tracking efforts from governments, security companies, and targeted organizations than in previous years. This evolved approach to cyber operations began to emerge in the aftermath of a period of transition following the Obama-Xi cyber agreement and internal restructuring within China's military, including the formation of the People's Liberation Army Strategic Support Force (SSF). This evolution is characterized by multiple overarching factors, including:

- More purposeful, strategic targeting at a comparatively lower volume than that seen throughout the 2000s to mid-2010s. Despite this, it is not uncommon to identify multiple Chinese state-sponsored groups active within the same network, particularly high-value intelligence targets within the Asia-Pacific and Central Asia regions.
- A shift away from traditional initial access vectors toward exploitation of zero-day and known vulnerabilities in public-facing appliances such as firewalls, enterprise virtual private networks (VPN), and mail server software. Many of these devices have limited visibility and logging capabilities and often do not support traditional endpoint security solutions.

- Mass adoption of large-scale anonymization networks for reconnaissance, exploitation, and command-and-control (C2) infrastructure. These networks have often used compromised internet-exposed internet of things (IoT) and network devices such as small office/home office (SOHO) routers, as well as virtual private server (VPS) infrastructure.
- Adoption of open-source malware families and exploits, which allow for the rapid weaponization of recently disclosed vulnerabilities, preservation of higher-end custom capabilities, and hindering of attribution efforts.
- Continued use of shared-capability supply chains through custom malware and exploit developers that supply multiple Chinese state-sponsored groups associated with both the People's Liberation Army (PLA) and the Ministry of State Security (MSS).

These changes have likely been driven by several factors, including overall improvements in defensive cybersecurity posture coupled with threat intelligence reporting detailing adversary tactics, techniques, and procedures (TTPs). Western governments and third parties, such as Intrusion Truth, have also increasingly engaged in a policy of publicly disclosing the identities of MSS contractor organizations and personnel. This increased scrutiny has likely led to a greater emphasis on operational security measures from these entities. Finally, internal developments such as the aforementioned intelligence agency restructuring and major developments in China's efforts to co-opt domestic software vulnerability research for use in offensive operations have likely been additional drivers in the observed changes to Chinese cyber-espionage activity in recent years. Insikt Group has also identified PLA procurement of open-source intelligence (OSINT) services analyzing foreign cyber defenses, cyberattack and defense training systems, and foreign anti-virus products in recent years, all in a likely effort to bolster People's Liberation Army Strategic Support Force (PLASSF; 人民解放军战略支援部队) and wider PLA offensive cyber operations.

China's Foreign Intelligence Services

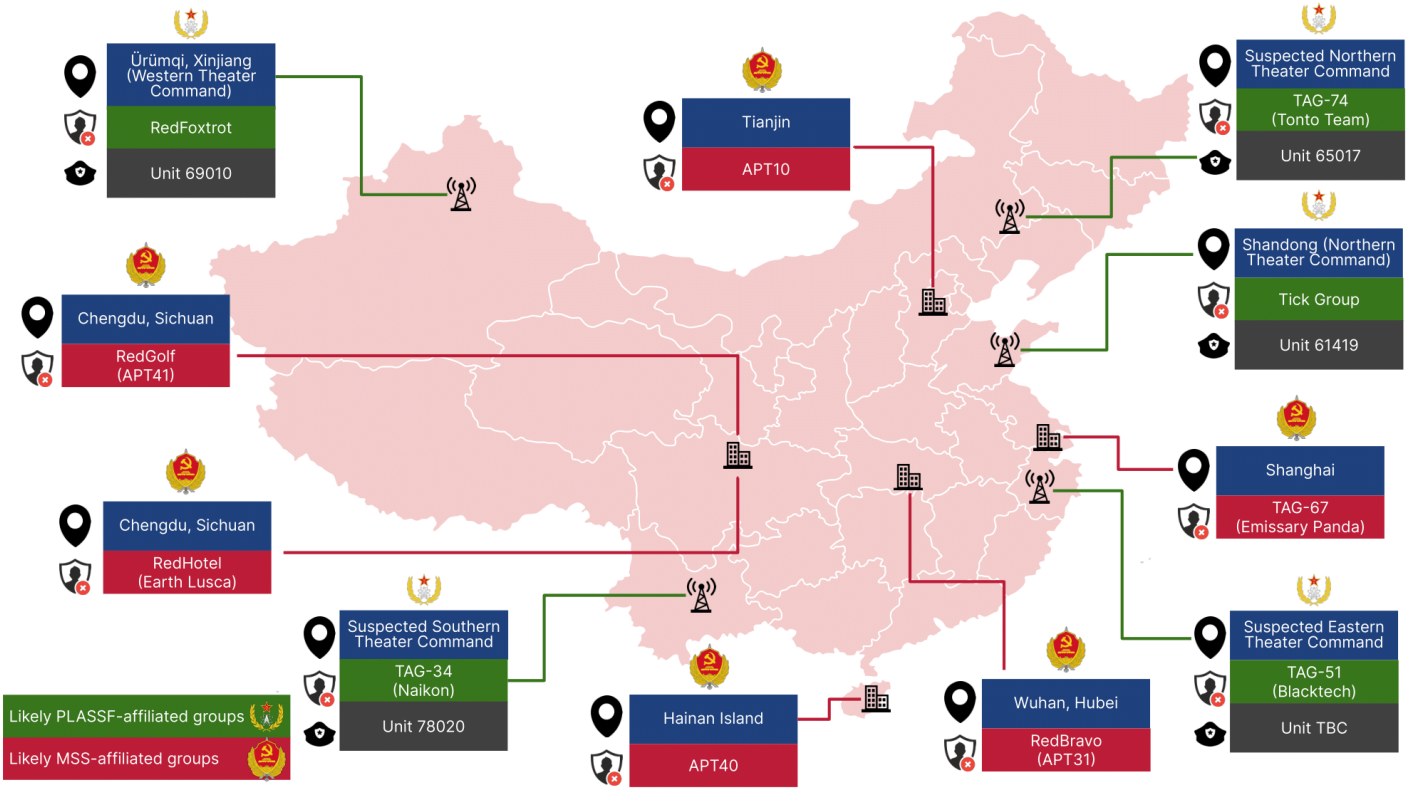

Figure 2: *Selection of known PLA- or MSS-attributed threat activity groups (Source: Recorded Future)*

Chinese state-sponsored offensive cyber activity is principally carried out by relevant departments of China's military, specifically the PLASSF and China's civilian foreign intelligence service, the Ministry of State Security (MSS; 国家安全部). As shown in **Figure 2**, a subset of Chinese state-sponsored groups have been attributed as likely PLA- or MSS-affiliated operating out of specific locations in China. The MSS has largely favored the use of private contractors that are typically tasked with intelligence collection requirements by regional MSS bureaus, as detailed within numerous US government indictments (1, 2, 3). These MSS-affiliated groups typically display a wider industry and geography targeting remit than their PLA counterparts, including counterintelligence, monitoring of dissident groups located overseas, non-military foreign intelligence, and supporting economic espionage missions.

Conversely, many PLA-affiliated groups display more consistent and focused geographical targeting based on their respective theater commands. For example, the Chinese state-sponsored group RedFoxtrot, which we previously linked to Unit 69010 of the PLA located in Ürümqi, Xinjiang, likely falls under the PLA Western Theater Command. The Western Theater Command is one of 5 theater commands of the PLA and is almost certainly tasked with monitoring India, Pakistan, and Central Asia. This orientation directly aligns with observed RedFoxtrot activity. Similarly, intelligence-gathering on

defense, military, telecommunications, and government targets also aligns with the expected operational scope of a PLA unit and fits the target profile of other PLA-linked groups (1, 2, 3).

China Conducts Global Cyber Espionage at Scale in Line with Economic and National Security Interests

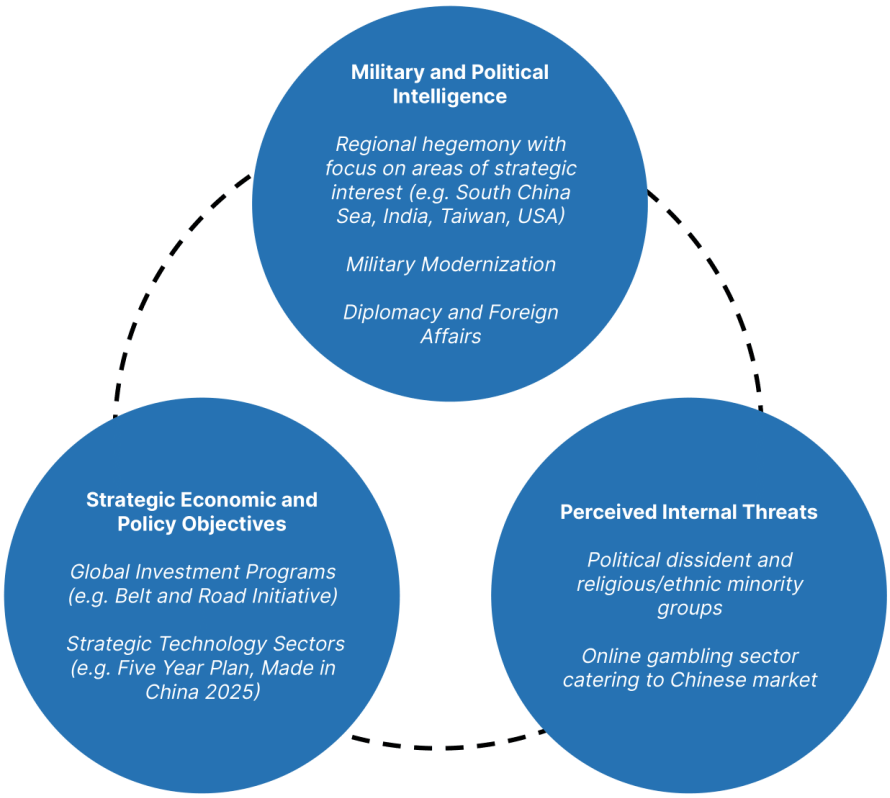

Figure 3: *Primary targeting categories observed from Chinese state-sponsored groups (Source: Recorded Future)*

Recorded Future continues to observe persistent global Chinese cyber-espionage activity across almost all industry verticals. In total, Recorded Future tracks over 50 distinct, currently active, suspected Chinese state-sponsored threat activity groups. This far exceeds the scale of activity seen from other prominent state-sponsored cyber threat actors such as Russia or Iran. Observed targeting by Chinese state-sponsored groups throughout the past 5 years has largely focused on 3 primary areas:

- Military and political intelligence
- Supporting strategic economic and policy objectives
- Perceived internal threats, including ethnic and religious minority groups

Military and Political Intelligence

In line with traditional foreign intelligence collection and China's continued striving for military modernization and regional hegemony, Recorded Future observes a large focus of China's cyber-espionage program on sectors such as aerospace and defense, government, media, military, telecommunications, and political organizations, particularly within bordering and adversarial states.

More widely, over the past several years, there has also been a shift toward increased targeting of telecommunications and other high-value upstream targets (such as supply-chain compromises) by Chinese state-sponsored groups. This is further indicative of the increased maturity of Chinese cyber operations.

Regional Hegemony and Military Modernization

Within the Asia-Pacific region, we observe a continued focus from Chinese state-sponsored groups on regions of strategic importance to China's regional hegemony and ongoing territorial or sovereignty disputes, such as the South China Sea claimants, India, and Taiwan. As we have previously reported in activity targeting India and the South China Sea (1, 2), in many cases, the operational tempo and scope of this activity mirrors geopolitical tensions and wider Chinese state-directed activity. Examples of recent Chinese state-sponsored activity in these regions are highlighted in **Table 1**. Outside of Asia, we also note a continued focus on defense industrial base (DIB) targeting by Chinese state-sponsored groups within the US (1, 2), which likely serves a dual purpose of supporting military modernization and traditional military intelligence missions.

India	Insikt Group continues to observe multiple Chinese state-sponsored groups active in India, the most prolific of which has been the PLASSF-linked group RedFoxtrot. In 2022 and 2023, we regularly observed RedFoxtrot activity targeting Indian aerospace, defense, and telecommunications organizations. Of particular note, in May 2022, we reported concerted targeting of multiple research facilities and operational assets associated with India's space program. This activity occurred immediately prior to the establishment of a joint commission on space cooperation of the BRICS countries (Brazil, Russia, India, China, and South Africa) and amid increasingly ambitious missions by the Indian space program.
Taiwan	Taiwan continues to be a major focus of Chinese cyber-espionage activity, with Recorded Future observing activity targeting Taiwanese entities attributed to Chinese state-sponsored actors such as RedHotel (Aquatic Panda, Bronze University, Charcoal Typhoon), TAG-67 (Iron Tiger, Emissary Panda), and RedDelta (Vertigo Panda, Temp.Hex, Twill Typhoon) in 2023. For example, from June to August 2023, we observed RedHotel compromise a Taiwanese aerospace and defense company (specializing in unmanned aerial vehicle (UAV) manufacturing) using the ShadowPad backdoor.

South China Sea	In addition to Taiwan, we continue to observe Chinese cyber-espionage groups such as RedHotel, RedDelta, TAG-34 (Naikon), and TAG-42 (Earth Longzhi) targeting countries within the South China Sea region in 2023, including rival claimants Vietnam, Malaysia, and the Philippines. In 2021 reporting, we highlighted the suspected Chinese state-sponsored group TAG-16 (BRONZE EDGEWOOD, Red Hariasa) targeting prime minister's offices, military entities, and government departments of rival South China Sea claimants Vietnam, Malaysia, and the Philippines.

Table 1: *Highlighted Chinese state-sponsored activity observed in India, Taiwan, and the South China Sea (Source: Recorded Future)*

Pre-positioning and Contingency Access Within Critical Infrastructure

While traditionally more risk averse in targeting critical infrastructure compared to Iranian and Russian state-sponsored groups, Chinese state-sponsored actors have become increasingly active in seeking to gain strategic access within critical infrastructure networks beyond traditional intelligence collection. This is evident in Recorded Future research in recent years that highlighted multiple campaigns targeting operational assets within the Indian power grid and other critical infrastructure sectors from at least 2020 to 2022 (1, 2). This activity coincided with prolonged periods of increased geopolitical tensions between China and India following May 2020 border clashes. The campaigns by Chinese state-sponsored groups included a particular emphasis on targeting Indian regional and state load dispatch centers responsible for carrying out real-time operations for grid control and electricity dispatch, which offer minimal economic espionage opportunities.

In September 2023, Insikt Group reported reconnaissance activity targeting US military, electricity, and communications organizations linked to the suspected Chinese state-sponsored group TAG-87 (Volt Typhoon, BRONZE SILHOUETTE, Vanguard Panda). This targeting aligns with previous public reporting on this group, which has displayed a specific interest in US critical infrastructure. TAG-87 campaigns have previously been alleged to support China's effort to develop capabilities and access that could disrupt critical communications infrastructure between the US and Asia during future crises, such as within the Taiwan Strait.

As China aims to extend its influence in the South China Sea and Taiwan and in the event of increasing US alliance activity in the region, these factors will likely heavily influence efforts to conduct strategic reconnaissance and pre-positioning within the critical infrastructure networks of these countries. However, such targeting of critical infrastructure does not inherently indicate impending conflict and is commonly executed on a contingency basis well in advance of when it is required. This is likely due to the extended time needed to develop effective capabilities for disruptive and destructive attacks on complex networks.

Strategic Economic and Policy Objectives

China's use of cyber espionage as a subset of wider intelligence and technology transfer efforts to support strategic economic objectives has been well documented. Historically, Chinese cyber-espionage targeting has reflected key technological areas prioritized in Five-Year Plans and other economic policies such as Made in China 2025 (1, 2).

Chinese foreign investment under schemes such as the BRI and other bilateral negotiations have also likely driven cyber intelligence collection (1, 2). In addition to observed intrusion activity aligning with BRI projects and participant countries, the MSS has also directly stated it plays a supportive role in securing China's landmark foreign policy initiative. The day before China opened the third International Cooperation Forum of the BRI in Beijing on October 17, 2023, the WeChat account of the MSS published an article stating the organization is "actively" involved in providing security for China's overseas interests under the BRI in a variety of ways, including risk management and threat elimination.

Under the BRI, China assists countries seeking to improve their overland and maritime transportation networks, telecommunications systems, and energy infrastructure, among other types of projects, through financial assistance and other development activities. Of note, in September 2023, we identified the likely compromise of a branch of the government of Angola by the suspected Chinese state-sponsored group TAG-68 (BackdoorDiplomacy, CloudComputating, Playful Taurus). The targeting of Angola's government is in line with historical activity attributed to this group, which has reportedly focused on gaining information on BRI debt owed to China, including from other African nations such as Kenya. Similar to Kenya, China is Angola's largest bilateral creditor, making up approximately 40% of government external debt (1, 2). We have also previously reported on TAG-68 activity targeting governments within other countries with close economic and political ties to China within Africa and Asia, in particular Senegal, South Africa, and Iran.

We also continue to identify intelligence-gathering focused on key technological areas highlighted within the 14th Five-Year Plan. This was evident in a 2023 campaign exploiting a zero-day in the Barracuda Email Security Gateway (ESG) appliance, which repeatedly targeted entities within key sectors highlighted under the 14th Five-Year Plan, such as semiconductors, public health, and artificial intelligence (AI) industries. In addition, in September 2023, we reported on a RedHotel campaign likely targeting the Taiwanese semiconductor industry. This campaign featured a multi-stage Cobalt Strike infection chain that displayed a decoy document written in Traditional Chinese, which was themed around the Taiwanese multinational company Taiwan Semiconductor Manufacturing Company (TSMC).

Targeting of Perceived Internal Threats

Chinese state-sponsored groups conduct regular targeting of individuals and communities considered a domestic security threat to the Chinese Communist Party (CCP), both within mainland China and overseas. This has also included the targeting of humanitarian organizations focused on human rights issues.

Targeting of Ethnic/Religious Minority and Dissident Communities

Over the past decade, Chinese state-sponsored groups have conducted regular intelligence-gathering and surveillance campaigns targeting ethnic minority and dissident groups both domestically and overseas. This includes but is not limited to groups such as Uyghurs, Tibetans, Catholics, pro-democracy advocates, Inner Mongolian independence groups, and Falun Gong supporters. In March 2023, we reported RedDelta targeting multiple Mongolia-linked non-governmental organizations (NGOs) and individuals. The majority of these targets related to either Mongolia-based Buddhism or Inner Mongolia pro-independence movements, an autonomous region within northern China.

Targeting of the Online Gambling Sector in Support of Domestic Crackdown

In recent years, Insikt Group has observed increased Chinese cyber-espionage activity targeting the online gambling sector catering to the Chinese market. Online gambling is illegal[1] in mainland China and is likely viewed by the Chinese government as both a stability and capital outflow concern. This has led to increased law enforcement action targeting individuals running and participating in online gambling, with China's Ministry of Public Security (MPS) stating[2] in late 2022 that it has shut down over 2,600 online gambling platforms. Many of the organizations traditionally providing these services are headquartered[3] in the Philippines, often referred to as Philippine Offshore Gambling Operators (POGOs), despite ongoing crackdowns on the sector. We believe that this increased cyber-espionage activity observed in recent years is likely intended to provide intelligence support to efforts[4] by both the MPS and China's internet regulator, the Cyberspace Administration of China, to crack down on online gambling domestically.

Of note, a distinct tactic observed across multiple campaigns has been the use of supply-chain compromises targeting chat applications used by these online gambling companies (1, 2). In 2023, we observed the compromise of the Philippine software company Seektop by at least 2 suspected Chinese state-sponsored groups, TAG-67 (Emissary Panda, Iron Tiger, LuckyMouse) and TAG-78 (Earth Berberoka), in activity spanning from 2021 to 2023. Elements of this activity, namely a software supply-chain compromise targeting an encrypted messaging application called MiMi developed by Seektop, have previously been referenced in open-source reporting by Trend Micro and Sekoia. Further analysis by Insikt Group identified that Seektop primarily develops software used within the online gambling industry in China and that the MiMi application was likely used to facilitate direct messaging between customers located in mainland China and overseas support staff working for these gambling companies.

[1] *https://www.scmp[.]com/news/china/politics/article/3157805/china-targets-online-casinos-war-illegal-gambling-authorities*
[2] *https://www.chinadaily[.]com[.]cn/a/202212/29/WS63ad9a75a31057c47eba6dd3.html*
[3] *https://www.scmp[.]com/week-asia/politics/article/3214584/will-philippines-ban-offshore-gambling-operators-amid-political-risks-chinese-customers*
[4] *http://english[.]www[.]gov[.]cn/statecouncil/ministries/202106/09/content_WS60c0bc08c6d0df57f98dafca.html*

Agile Response to Geopolitical Events

Chinese state-sponsored groups have consistently shown agility in responding to external geopolitical stimuli, which is often directly observable through the shift of established collection and targeting patterns from specific groups. As noted in **Figure 4**, in 2020, Insikt Group observed RedDelta pivot toward targeting the Vatican and other Catholic entities in advance of key talks between the CCP and Vatican officials. More recently, we reported on the same group's shift towards increased targeting of European government and diplomatic entities in the period directly preceding and following Russia's invasion of Ukraine. Other observed examples of increased intelligence collection or disruptive efforts in line with external events include periods of heightened tension between India and China, the 2019 Hong Kong protests, and the emergence of the COVID-19 pandemic.

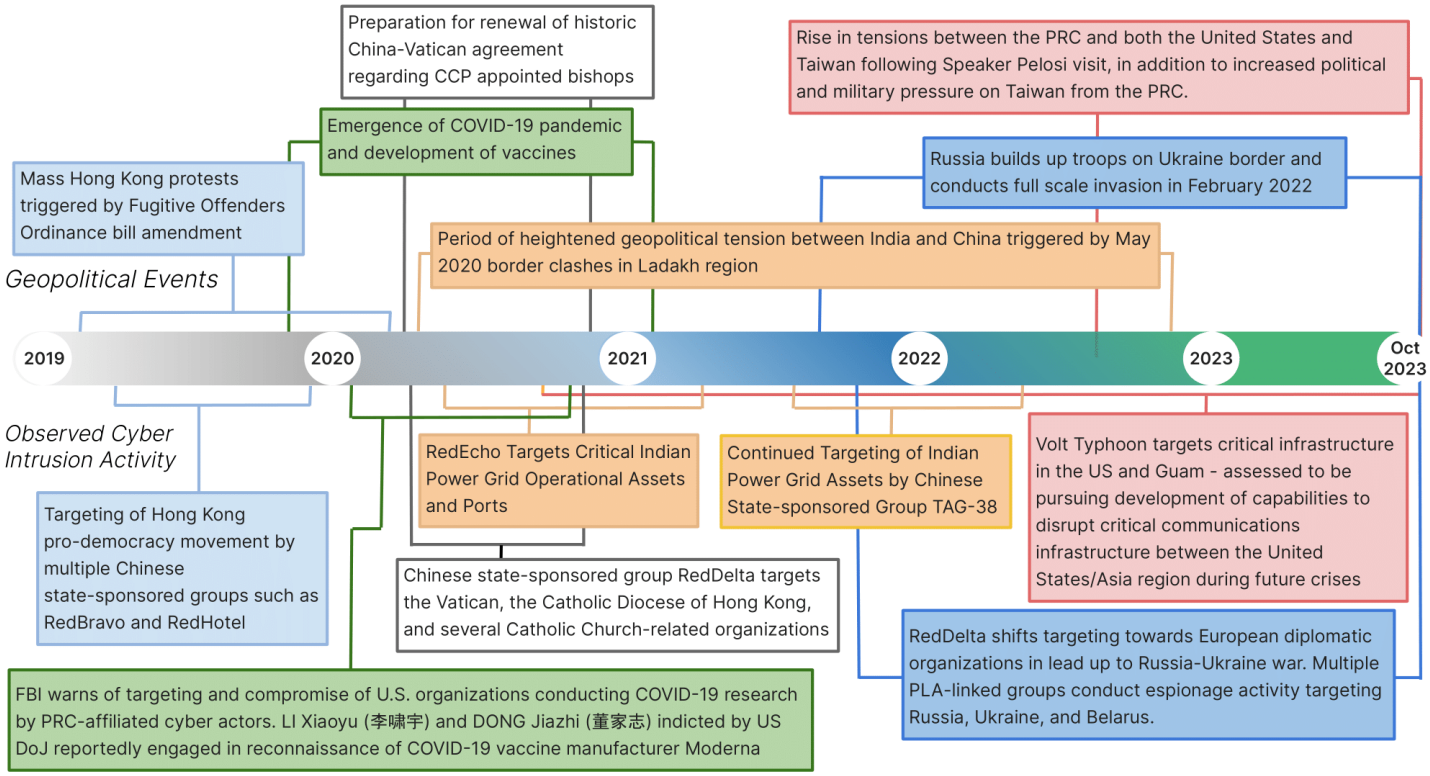

Figure 4: *Timeline of Chinese state-sponsored threat activity in response to geopolitical events from 2019 to 2023 (Source: Recorded Future)*

Transformation Toward a Stealthier and More Purposeful Adversary

Chinese state-sponsored groups, particularly those active within North America and Europe, are increasingly maintaining higher degrees of operational security (OPSEC) and focusing on minimizing detection opportunities. This is evident via a focus on the exploitation of internet-facing appliances that often have limited support for traditional endpoint security solutions or logging and monitoring capabilities. In most cases, Chinese state-sponsored groups are then using web shells or customized malware families designed for these appliances to maintain persistent access (1, 2). Post-exploitation, there is an increased emphasis on the use of living-off-the-land techniques coupled with valid credentials for discovery, collection, and lateral movement, as well as removing forensic evidence of intrusion activity. Interaction with victim networks is commonly carried out using private anonymization networks, which complicates attribution, detection, and tracking efforts.

Acceleration in Zero-Day Usage and Exploitation of Internet-Facing Appliances

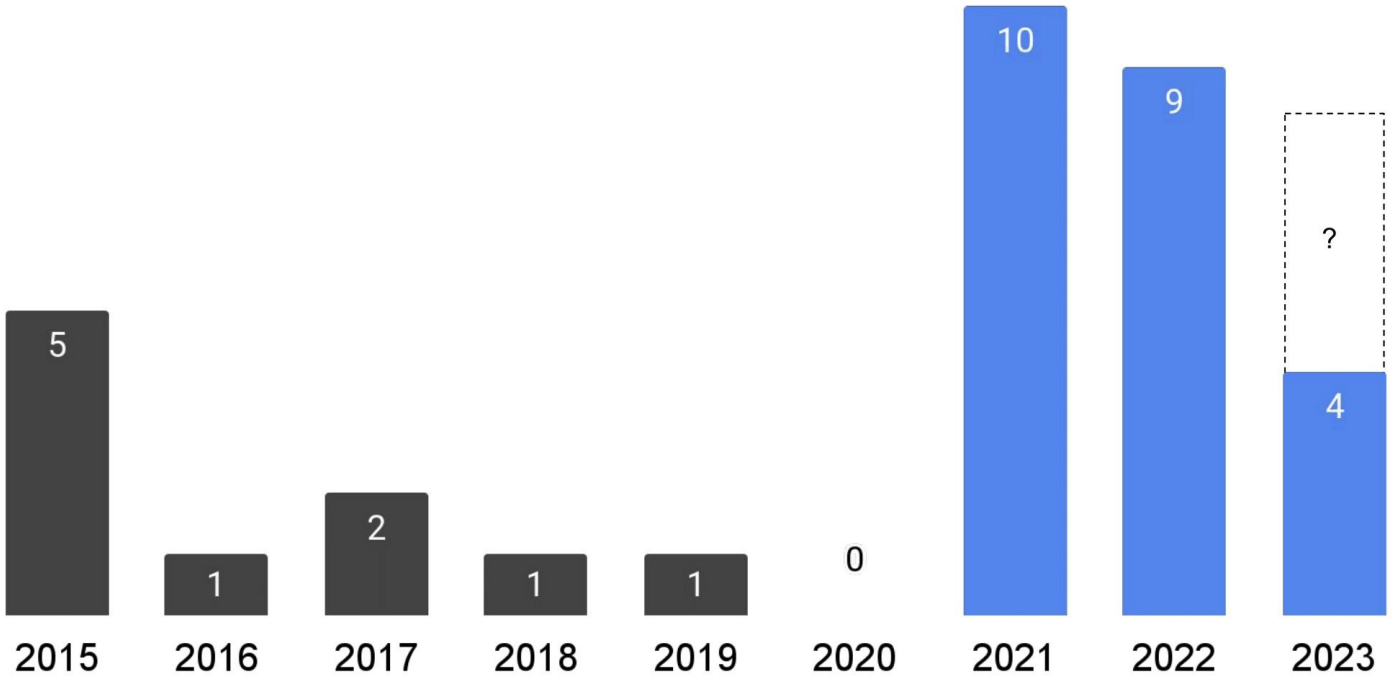

Figure 5: *Known zero-day vulnerabilities exploited by Chinese state-sponsored groups from 2015 to 2023 (Source: Recorded Future)*

Since the beginning of 2021, there has been a substantial increase in the identified exploitation of zero-day vulnerabilities by Chinese state-sponsored groups (see **Appendix A** for full list). Over 85% of known zero-day vulnerabilities exploited by Chinese state-sponsored groups over this period were in public-facing appliances such as email servers and appliances (such as Zimbra, Microsoft Exchange, and Barracuda ESG), SSL VPN products (such as Pulse Secure and Fortinet FortiOS SSL-VPN), firewalls

(Sophos XG), and other internet-facing appliances (such as Citrix ADC, Zoho ManageEngine, and Atlassian Confluence). While this is unlikely to capture the entire spectrum of Chinese zero-day vulnerability usage across all device and operating system types, this shows a clear trend of both increased zero-day usage and a focus on public-facing network appliances since 2021.

In several cases, we have observed the concurrent use of zero-day exploits by multiple distinct Chinese state-sponsored groups, indicating the likelihood of a shared developer or exploit supply chain. This sharing of capabilities exists within a wider ecosystem likely enabled by both shared upstream exploit and malware developers and wider strategic policy measures, including competitions like the Tianfu Cup, vulnerability disclosure regulations, and the direct influence Chinese intelligence services likely hold over public disclosure of high-value vulnerabilities through the Chinese National Vulnerability Database (CNNVD).

Mass Adoption of Anonymization Networks

Chinese state-sponsored groups have increasingly been employing large anonymization networks, often built from compromised IoT devices, including SOHO routers, or through actor-provisioned VPS infrastructure, for use as operational infrastructure. Such anonymization networks are often more challenging to track for security researchers than traditional actor-provisioned infrastructure due to the volume of infrastructure that can be accumulated and as compromised devices are also simultaneously used for legitimate purposes by their owners, allowing threat actors to blend in with normal internet traffic. These networks can also allow threat actors to rapidly cycle infrastructure and use internet service provider (ISP) IP addresses geolocated in the same country as targeted entities.

The shared use of capabilities by Chinese state-sponsored groups also extends to these anonymization networks, with multiple groups observed employing shared services such as the “RedRelay” anonymization network reported by PWC. This indicates that some of these services are likely provided as a quartermaster-style or commercial service arrangement. Examples of the use of anonymization networks by Chinese state-sponsored groups include TAG-38 activity targeting Indian critical infrastructure, RedBravo (APT31) activity targeting European governments, TAG-87 (Volt Typhoon) targeting US critical infrastructure, and TAG-51 (BlackTech) targeting entities within Taiwan and Japan. In the case of TAG-38, we identified the group using a network of compromised internet-facing, third-party DVR/IP camera devices that were used to proxy ShadowPad command-and-control infrastructure to upstream actor-controlled servers.

Mitigations

We recommend that users conduct the following measures to detect and mitigate commonly observed TTPs associated with Chinese state-sponsored activity:

- Ensure a risk-based approach for patching vulnerabilities, prioritizing high-risk vulnerabilities and those being exploited in the wild as determined through the Recorded Future® Vulnerability Intelligence module. With regard to Chinese state-sponsored groups, pay particular attention to remote code execution (RCE) vulnerabilities in external-facing appliances within your environment.
- Ensure security monitoring and detection capabilities are in place for all external-facing services and devices. Monitor for follow-on activity likely to take place following exploitation of these external-facing services, such as the deployment of web shells, backdoors, or reverse shells, and subsequent lateral movement to internal networks.
- Practice network segmentation, such as isolating internet-facing services in a network demilitarized zone (DMZ).
- Enforce multi-factor authentication (MFA) on all VPN connections and consider implementing anomaly detection for VPN connections.
- By monitoring Malicious Traffic Analysis (MTA), Recorded Future clients can alert on and proactively monitor infrastructure that may be potentially involved in notable communication to known C2 IP addresses.
- Recorded Future® Third-Party Intelligence module users can monitor real-time output to identify suspected targeted intrusion activity involving key vendors and partners within physical, network, and software supply chains.
- Review public guidance on mitigating common TTPs used by Chinese state-sponsored groups (1, 2, 3, 4).

Outlook

As Chinese state-sponsored cyber operations continue to mature, the multi-year effort of internal restructuring within China's military and a heightened domestic focus on vulnerability research and weaponization is likely yielding results. The observed focus on exploiting zero-days in public-facing appliances and the rapid weaponization of known vulnerabilities in these products has proved a successful tactic in scaling initial access against a wide range of global targets. With organizations continuing to move to the cloud, a similar emphasis in the targeting of these environments is likely, as observed in STORM-0558 activity involving the use of forged authentication tokens to access user email via a stolen Azure AD (now Entra ID) enterprise signing key.

As China seeks to project power in the South China Sea and Taiwan and amid continued US efforts to strengthen alliances in the region, we expect to observe a high operational tempo of intelligence-gathering within these countries and the US. It is also likely that there will be efforts to perform strategic reconnaissance and pre-position within critical infrastructure networks within these countries. Targeting critical infrastructure does not necessarily signal impending conflict and is commonly carried out in advance on a contingency basis due to the extended time required to develop effective capabilities for disruptive and destructive attacks against these types of complex networks. In many cases, the targeting of specific critical infrastructure sectors may also align with China's economic goals, highlighting the importance of analyzing wider geopolitical context in conjunction with observed intrusion data in order to assess likely motivations and objectives.

In light of the substantial commitment of personnel and resources by the Chinese government to offensive cyber operations, coupled with the evident enhancement of their tradecraft and capabilities over the last decade, it is likely that China is poised to solidify its position as a dominant global force in cyber espionage and information warfare.

Appendix A: List of Zero-Day Vulnerabilities Exploited by Suspected Chinese State-Sponsored Groups since 2021

CVE	Product
CVE-2023-22515	Atlassian Confluence Data Center and Server
CVE-2023-3519	Citrix Netscaler
CVE-2023-20867	Vmware vCenter
CVE-2023-2868	Barracuda Email Security Gateway
CVE-2022-27518	Citrix ADC/Gateway
CVE-2022-41328	Fortinet FortiOS
CVE-2022-42475	Fortinet FortiOS
CVE-2022-41040	Microsoft Exchange Server
CVE-2022-41082	Microsoft Exchange Server
CVE-2022-3236	Sophos Firewall
CVE-2022-30190	Microsoft Windows
CVE-2022-26134	Atlassian Confluence Server & Data Center
CVE-2022-1040	Sophos Firewall
CVE-2022-24682	Synacor Zimbra Collaboration Suite
CVE-2021-40539	ManageEngine ADSelfService
CVE-2021-40449	Microsoft Windows
CVE-2021-30869	Apple macOS
CVE-2021-44077	Zoho ManageEngine
CVE-2021-35211	Solarwinds Serv-U
CVE-2021-26855	Microsoft Exchange Server
CVE-2021-26857	Microsoft Exchange Server
CVE-2021-26858	Microsoft Exchange Server
CVE-2021-27065	Microsoft Exchange Server

Recorded Future®

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture