My Tea’s not cold. An overview of China’s cyber threat

blog.sekoia.io/my-teas-not-cold-an-overview-of-china-cyber-threat/

7 September 2023

Log in

Whoops! You have to login to access the Reading Center functionalities!

Forgot password?

Jamila B. and Threat & Detection Research Team - TDR September 7 2023
653 0

Read it later Remove

28 minutes reading

This blogpost is an overview of recent malicious cyber activities associated to China-nexus Intrusion Sets. It is based on open-source documents and Sekoia.io TDR analysts research and does not intend to present an exhaustive list of campaigns aligned on China’ strategic interests. Information cut off date is 13, July 2023.

Chinese doctrine on my wall

Since at least 2006, China leveraged cyber capabilities to support its strategic objectives. Since then, cyber threats aligning on China’s interests were continuously reported on, with observed maturing in capabilities and Tactics, Techniques and Procedures (TTPs), as well as changes in its underlying organisation and doctrine. China’ strategic interests notably reside in the following:

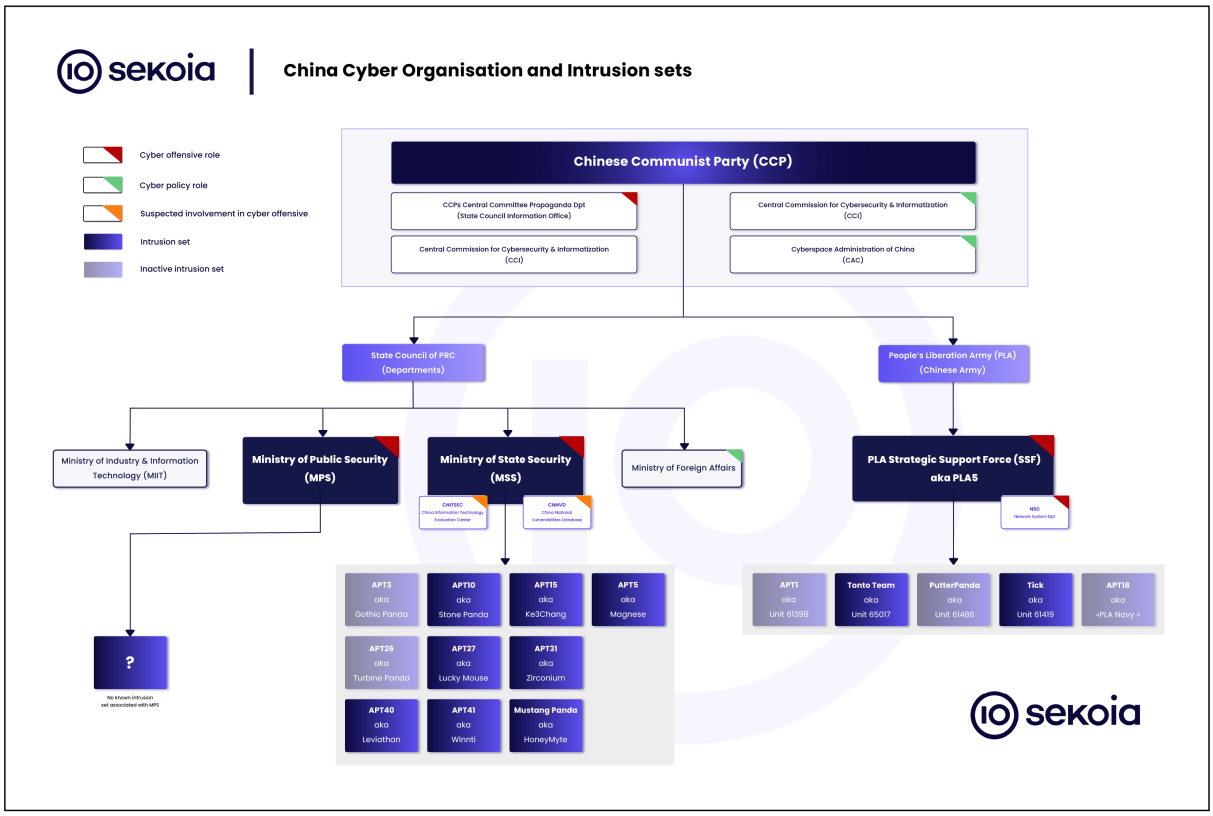
- Preserving the existence and legitimacy of the Communist Party of China (CPC).
- Protecting China’s national interest security, including its territorial integrity.
- Asserting China’s power globally, including in the cyber domain.

These strategic interests are operationalised through:

- Economic coercion of neighbours and partners, notably through cyberespionage and Intellectual Property (IP) theft;
- Leverage of a wide array of organisations and instruments of national power, including intelligence and cyber capabilities as well as technological investment and censorship;
- Influencing international standards and policy making related to cyber.

Cyber is also used as a force multiplier in the land, air, sea, and space domains and almost certainly combined to Signal Intelligence (SIGINT) and Human Intelligence (HUMINT) capabilities.

China's cyber offensive apparatus includes **military and state security intelligence entities**, alongside **contractors, front companies, and universities**. China is actively reforming its national security apparatus including its civilian and military intelligence agencies which notably use cyber capabilities, both separately and jointly, to carry out cyber malicious activities. Most prominent agencies include the Ministry of State Security, and the People Liberation Army Strategic Support Force, reorganised between 2017 and 2020. Sekoia.io's representation of the Chinese cyber offensive apparatus is as follow (Note that we are showing only the most active intrusion sets):



Several sources report that both agencies use **"proxies**", such as information and technology companies as well as universities to conduct their cyber operations. Since the 1920s, the CPC developed a strategic concept known as "United Front", a network of social, professional, political, and academic organisations, to support the CPC's interests and suspected to be involved in supporting Chinese intelligence activities, including cyber. This results in a **vast number of stakeholders disconnecting China from malicious cyber operations**, providing the State with plausible deniability, and further complexifying the threat landscape.

Since 2020, observed Chinese cyber espionage campaigns exhibited an **increased risk tolerance in TTPs as well as increased activities' tempo**, echoing the country's wolf warrior diplomacy. Between 2022 and 2023, we observed China-nexus intrusion sets continuously updating their TTPs and toolsets.

Domestically, China's approach to cyberspace is driven by a technological imperative of **self-reliance** and ensuring long-term innovation-led growth, and a political drive of **controlling the flow of information** within cyberspace to safeguard regime legitimacy and social stability. The latter is notably reflected through China's engagement in global cyber initiatives and its promotion of cyber sovereignty.

China-nexus intrusion sets notably conduct **upstream collection campaigns** through Managed Services Providers (MSP) and **supply chain compromises** to collect large amounts of data such as Personal Identifiable Information (PII). Primary targets of China-aligned cyber offensive activities include entities related to **governments, telecommunications, manufacturing (including semiconductors and chip makers), and more recently financial institutions worldwide**.

A room full of your posters

Between 2022 and 2023, China aligned cyber malicious campaigns were **increasingly reported** in open sources. While it is not clear whether this is due to an actual increased tempo of Beijing tasked cyber malicious activity or a particular effort from vendors and governmental agencies to disclose their findings considering the heightened tensions between China and the international community, it remains helpful to the broader cyber intelligence community to gain better insight into Chinese offensive cyber campaigns. Between 2022 and 2023, Sekoia.io analysts observed China-nexus intrusion sets continued focusing on entities notably related to the **South China sea and the Indo Pacific regions** and expanding their victimology to include **more European targets**. Additionally, while not new, China was also reported increasingly **targeting critical national infrastructure**, as well as the finance sector.

You dare me to spy?

China continuously demonstrates efforts to increase its **role as a major global power**, notably through government programs (5 years plan aka FYP) and plans such as the Belt and Road Initiative (BRI, aka New Silk Road) and Made in China 2025 (MIC2025).

In November 2022, Mandiant published their report on UNC4191 's cyberespionage campaign targeting Southeast Asia, with a strong focus on Philippines, as well as Europe, the U.S, and Asia Pacific and Japan. In December 2022, Recorded Future reported on a Mustang Panda (aka Temp.Hex) campaign called SmugX against Vietnam, continuing until mid-2023, notably targeting the UK, Ukraine, Czech Republic, and Hungary Foreign Affairs

ministries and embassies by leveraging documents purportedly originating from France, and Sweden. In our FLINT 2022-060- Mustang Panda's Ode to joy, we documented this intrusion set cyberespionage campaign also targeting the Czech Ministry of Industry and Trade, the Serbian Ministry of Interior and Hungary. China aligned cyberespionage campaigns also include Dark Pink (aka Saaiwc Group), an emerging intrusion set particularly active since mid-2022, conducting spearphishing campaigns against government, military, and non-profit organisations in Brunei, Cambodia, Indonesia, Malaysia, Thailand, the Philippines, Vietnam, Bosnia and Herzegovina, as well as an education organisation in Belgium, and a European state development agency based in Vietnam. Of note, the targeting of Vietnam is particularly interesting, as this country observes a non-committal stance towards the BRI. We assess **competing infrastructure projects, including European's, likely are of high interest to China**. Furthermore, it is likely countries considering withdrawing from the BRI project, as Italy recently did will also be targets for Chinese cyberespionage campaigns.

Additionally, we observed an **increased targeting of finance related entities** by China-nexus intrusion sets since December 2020. Recent examples of this trend notably includes Tropic Trooper (aka Keyboy) targeting Taiwanese financial institutions, Witchetty targeting **[6]** an African stock exchange between February and September 2022, Worok **targeting [8]** a bank in Central Asia, APT41 targeting a German financial company in March 2022, Ke3chang targeting a government finance department in the Americas between March 2022 and early 2023, and Gallium targeting an organisation that finances long-term urban infrastructure development projects in Nepal in April 2023. These activities almost certainly aim at collecting strategic intelligence, **possibly linked to the financing of BRI-related projects, and/or competing infrastructure projects**.

Sekoia.io analysts assess these activities highly likely pertain to China's economic interests, notably targeting BRI stakeholders and competitors, likely to ensure economic goals are achieved. We further assess **it is almost certain cyberespionage campaigns targeting organisations involved in the BRI project**, as well as entities involved in financing BRI projects and competing projects will continue in the short term.

I'm almost at the bridge now

Since 2022, official statements cautioning against China's targeting Critical National Infrastructure are on the rise and ever more alarming. In parallel, there were allegations that China would leverage equipment located in proximity of critical infrastructures for intelligence purposes.

Between 2022 and 2023, **China intrusion sets continuously targeted the telecom vertical**, historically a target of interest to Beijing, notably to conduct upstream collection. Gallium (aka Alloy Taurus, an intrusion set sharing similarities with APT10 and APT41) notably targeted telecommunication entities in the Middle East during the SoftCell campaign, and DaggerFly conducted a cyber espionage campaign [3] against an African

telecommunications organisation between November 2022 and April 2023. In June 2022, Kaspersky ICS CERT researchers reported on a campaign targeting manufacturing and telecom organisations in Pakistan and Afghanistan and a port in Malaysia. In June 2023, a threat actor was reported compromising CCTV cameras of the Directorate General of Highways in Taiwan. Of particular interest was Volt Typhoon's campaign documented in May 2023. Since mid-2021, Volt Typhoon (aka Vanguard Panda) targeted critical infrastructure sectors including manufacturing, utility, maritime, government entities in the United States, notably in Guam. Of note, Guam not only hosts U.S. military bases (whose expansion was announced earlier this year, it is also a submarine cables hub connecting the U.S. to the Asia-Pacific region. Sekoia.io analysts assess these activities almost certainly pertain to strategic intelligence collection, and **China could plausibly leverage these accesses to conduct disruptive activities in the event of a rise in tension in the medium to long term**.

Overall, Sekoia.io TDR analysts assess recent China aligned **cyber activities echo the ongoing political and economical confrontation between NATO countries and Beijing**, notably including the U.S. Indo Pacific Strategy and the AUKUS pact, the European Global Gateway initiative, often seen as the European countermeasure to the BRI, in a context of "arms race" and sanctions, all of them almost certainly perceived as threats to Beijing' strategic interests, domestically, regionally, and globally.

I talk about you 24/7

China continuously demonstrates **efforts to increase its international influence and role as a regional leader**, not only economically but politically as well. Sekoia.io analysts identified multiple cyber campaigns aligning on this objective.

For instance, in August 2022, Malwarebytes reported on APT41's campaign targeting governmental entities in Sri Lanka. Sekoia.io analysts link this activity to the nomination of the Sri Lankan Prime Minister Dinesh Gunawardena in July 2022, whose family had strong ties with India, when, on the other hand China was accused of engaging in "debt trap diplomacy". We further assess the docking of Yuan Wang 5, also called a "spy ship" was almost certainly designed as a "power move" towards both Sri Lanka and India. In November 2022, as reported by Elastic Security Labs, China-nexus REF2924 targeted the foreign ministry of a Southeast Asia nation, aiming at collecting intelligence pertaining to the victim's relationship with the Association of Southeast Asian Nations (ASEAN) . Mustang Panda (aka Temp.Hex) was reported targeting Australia, as well as NGOs, military and police entities in Myanmar, and the Myanmar embassy in Serbia. Of note, China is a vocal supporter of Myanmar's sovereignty, the country being led by a junta regime since the 2021 coup. In addition, Myanmar provides China with access to the Bay of Bengal, a strategic position in the Indian Ocean Region.

Mustang Panda also was observed leveraging the Russo-Ukrainian conflict to target European and Asia Pacific countries with the PlugX malware to collect intelligence. While Russia's targeting was already observed in the past, Sekoia.io analysts noticed an increase in reported China-nexus intrusion sets targeting of Moscow in the context of the conflict. We assess that while China and Russia ties keeps on deepening, **it is highly likely Beijing is interested in anticipating how the conflict would impact Chinese interests in the region and globally**, as illustrated by the targeting of G20 Nations in the SharpPanda campaign.

Another noticeable impact of the Russo-Ukrainian conflict on China was the multiple public declarations, notably originating from U.S. officials, warning against a similar development between Taiwan and China, as part of Beijing's "**one China principle**" , renewed in August 2022. Sekoia.io observed a **stable targeting** of Taiwan originating from China, including by DragonSpark, Lucky Mouse, Tropic Trooper, and Mustang Panda, with an uptick directly related to political events, such as the visit of the speaker of the U.S. House of Representatives in Taiwan in August 2022.

While this certainly pertains to China's continuous intelligence collection, notably as part of its territorial integrity, it is also likely that Taiwan's renewed position as a key player in the region both as a strategic supplier[1] and a U.S. and European political ally is and will continue to be a strong driver for Chinese aligned cyber espionage campaigns. Sekoia.io analysts further assess Taiwanese and foreign entities involved in the semiconductors supply chain, the chip manufacturing vertical and the logistics industry, including maritime companies, will almost certainly remain targets of high interest to Beijing.

As interesting as Russia's targeting, Pakistan, considered as a Chinese regional partner (both countries being notably involved in territorial disputes and regional influence competition with India) was also increasingly targeted by China-nexus intrusion sets. Recent campaigns notably include the targeting of manufacturing and telecom organisations, a campaign against the Pakistan International Maritime Expo & Conference (PIMEC-2023) participants, and the leveraging of the E-Office application developed by Pakistan National Information Technology Board (NITB) in July 2023. This latest campaign is particularly intriguing, as the NITB partnered with the Chinese company H3C to build a digital government base. Sekoia.io analysts assess these activities almost certainly **enable China to ensure their military and defence (including naval cooperation) and economical relationship to Pakistan is secured, Islamabad also being a U.S. partner**.

A similar dynamic can be observed with Japan, both countries expressing their willingness to deepen their ties, while Japan organisations are continuously targeted in cyberespionage campaigns. TA410 (aka Witchetty, loosely linked to APT10) notably targeted Japanese organisations with FlowCloud, and MirrorFace (tracked as APT10 by TDR analysts) continued targeting media, diplomatic, government and public sector organisations, think-

tanks and political entities in Japan. Of note, Japan is part of the Quadrilateral Security Dialogue (QSD), and considered a threat to China when it comes to Taiwan, especially in the light of a possible recognition of Japan's right of belligerency in their Constitution.

Hit me back just to chat

In addition to alleged spying, Very High Frequency (VHF) interference and multiple military drills and in relation to military cyber operations, PLA publications indicate that improving computer network exploitation and attack capabilities in order **to degrade adversaries' networks and information environments is seen as critical to winning future wars**.

As previously mentioned, the **Russo-Ukrainian conflict was a driver for China aligned cyberespionage**, as illustrated by Tonto Team's campaign against Russian agencies in July 2022. In March 2023, ESET colleagues reported on a Tick (aka Bronze Butler) operation compromising the update server of an East Asian Data Loss Prevention (DLP) company notably catering government and military entities. These findings were corroborated by Ahnlab, which associated the targeting of Korean government organisations (called operation Triple Tiang) to the same intrusion set, based on their use of the Shadowy downloader. While we have very little information on these activities, and solely since we associate Tick and Tonto Team to the PLA-SSF, we assess it is likely these campaigns pertain to **military intelligence collection**. Of note, while South Korea is a consistent target of interest to China (notably due to Seoul's use of U.S.-deployed Terminal High Altitude Area Defense (THAAD) anti-missile systems since 2017) it is also plausible the renegotiation of defence cost-sharing was an additional driver for the operation Triple Tiang.

A tattoo with your IP across the chest

Chinese cyber espionage operations present a continuous threat to intellectual property. Observed campaigns carried out by suspected China-nexus threat actors in the past notably targeted Western technologies such as high-tech, oil and gas, agriculture, manufacturing, biotechnology, pharmaceuticals, energy, aviation, aerospace, defence industrial bases, dual-use military application technologies, and telecommunications worldwide. Sekoia.io analysts assess industrial espionage almost certainly enable Chinese indigenous production and support Chinese industrial policies, such as the 14th Five-Year Plan (2021-2025). It is also assessed that strategic information collected through cyber espionage are likely passed on to China champions for commercial competition on international markets as well as gaining strategic know-how.

China-nexus intrusion sets continued carrying out cyber malicious campaigns **against industries notably operating in the manufacturing, healthcare, and logistics verticals**. This notably includes Tropic Trooper targeting [2] a manufacturing company and semiconductors industry in Taiwan, APT41 targeting [9] an Asian conglomerate operating in the materials and composites sector, Dalbit targeting at least 50 South Korean companies

since 2022, including in the semiconductors manufacturing vertical, technology and chemical industries, and Hydrochasma carrying out a campaign [5] against shipping companies and medical laboratories that may be involved in Covid 19 research in Asia since October 2022. Sekoia.io analysts assess these activities almost certainly pertain to intellectual property theft.

Between April and mid-June 2022, APT40 (aka Red Ladon) was observed targeting Australian government agencies and industry manufacturers conducting maintenance of fleets of wind turbines in the South China Sea region during the ScanBox campaign. Sekoia.io analysts identified one of the companies to be the German company Skyborn Renewables GmbH. South China Sea is a site for oil and gas exploitation, and a critical logistics route for oil and natural gas imports, transporting energy resources through strategic choke points, such as the Strait of Malacca. Of note, the PRC also started prioritising green energy opportunities through the Green Silk Road project since 2021, as part of its own goal of reaching carbon neutrality by 2060 and display a good record in the frame of UN's 2030 Agenda for Sustainable Development Goals. We assess that **China's decarbonization strategy is almost certainly already a driver for cyber enabled espionage campaigns originating from China**, notably in parallel to HUMINT. China continuously demonstrated its interest in the energy vertical, including nuclear energy, an interest recently renewed in the Global Security Initiative. Energy targeting by China-nexus will almost certainly continue at a global scale in the short to medium term.

Sekoia.io analysts further assess that China increasing designations on their Unreliable Entities List (UEL), the banning of Chinese companies and initiatives such as the CHIPS and Science Act as well as China's efforts to achieve self-reliance, including in the technology industry, will ultimately highly likely concur to an increase of Chinese cyber enabled IP theft. Of note, since 2020, Chinese courts granted "anti-suit injunctions (ASIs), preventing foreign companies from taking legal action to protect their Intellectual Property.

This is my spyware I'm sending you

Domestically, China-nexus Intrusion Sets carry out multiple **surveillance campaigns against what is called "the Five poisons"**, including Taiwan independence movement, the Tibetan Independence movement, the Uygur ethnic group, the Chinese democratic movement and the Falun Gong. Abroad, surveillance operations target the Chinese diaspora, including Chinese citizens, dissident groups, and members of China's ethnic minority communities.

To that purpose, China-nexus intrusion sets notably leverage **mobile applications**. In November 2022, APT15 was reported targeting the Uyghur community in China mainland and abroad including in Turkey and Afghanistan, leveraging the BadBazaar malware masquerading as Android mobile applications and the MOONSHINE app-based Android

surveillance tooling. As documented in April 2023, DaggerFly targeted members of an NGO operating in the Gansu and Guangdong provinces with the MgBot backdoor installed via the update of legitimate applications between 2020 and 2022. Of note, the Greater Bay Area comprises the two Special Administrative Regions of Hong Kong and Macao and nine municipalities in the Guangdong Province, Macao and Hong Kong being consistent targets of this intrusion set. One additional victim was also located in Nigeria.

In December 2022, Amnesty International Canada disclosed their IT network was breached by a China-originating cyberespionage campaign in October 2022. In 2022, LuckyCat (aka TA413) continuously targeted Tibetan people, organisations involved with the Tibetan community and the exiled Tibetan government. Sekoia.io analysts also observed Mustang Panda leveraging immigration-related topics, notably the Austrian Red-White-Red program. It is possible this targeting pertains to surveillance operations. In December 2022, Avast reported on their findings on a Mustang Panda-owned FTP server, where they notably retrieved scans of passports from citizens and diplomats from countries, such as France, China, Australia, Czech Republic, Israel, Netherlands, the UK, and the U.S.

Of note, **China' surveillance over the Internet also occurs through its infrastructure**, notably through the Golden Shield Project (aka the Great China Firewall in line with its view on cyber sovereignty and attempts to shape international standards in the cyberspace, as illustrated by Xi Jinping 's declarations in 2022. Cyber enabled surveillance is also conducted in parallel of coercive actions including intimidation and repression. Policy wise, the Cyberspace Administration of China updated its "Real-name registration regulation" (Article 24 of the Cybersecurity Law) in 2021 and specific regulations apply to ethnic minorities. Sekoia.io analysts assess **surveillance targeting ethnic and religious minorities in mainland China and abroad will almost certainly continue in the short term**. We further assess that as non-military foreign intelligence falls under the MSS mandate, Mustang Panda or any other MSS linked intrusion set will almost certainly carry on conducting **surveillance of high value targets, including diplomats**.

Sometimes I scribble addresses too sloppy

Chinese information operations pose a high-volume threat globally. **Initially focusing on regional targets and matters, it sensibly expanded to Western countries in 2020**. It is almost certain that Covid-19 and China's role in the global pandemic led China to intensify their efforts in increasing its information operations capabilities to reach a broader audience. Observed campaigns used a wide range of social media platforms and websites and were two-folded – containing or censuring negative comments towards China and the CPC, and conveying negative narratives against European countries, the U.S or any country considered as hostile. Targeted audiences include the Chinese diaspora as well as international media, economy and political stakeholders.

A common technique used in Chinese information operations is **cyber harassment with fake accounts**, as observed in the targeting of a Chinese human rights activist and a political dissident in April 2023. Other techniques include using personas to dox individuals, as observed with the HKLEAKS websites used between August 2019 and mid-2021 to dox protesters and journalists by leaking their personal identifiable information (PII), amidst Hong Kong's anti extradition protests. Sekoia.io analysts assess it is almost certain data collected during surveillance campaigns, as well as SIGINT and HUMINT activities contributed to this operation. As stated by Citizen Lab, it is almost certain this type of activities not only aim at influencing an online audience, but it also aims at silencing their targets.

In July 2022, Google reported on China originating Coordinated Inauthentic Behaviour (CIB) notably resorting to YouTube to spread Chinese and English content pertaining to China and U.S. affairs, as well as English content about the origins of Covid-19 . Of note, while **we still observe quite a limited impact of China nexus info ops worldwide, notably in NATO countries**, it seems efforts are being made to further refine their techniques, as recently observed in Taiwan. In October 2022, Mandiant documented the continuation of the DragonBridge campaign, an information operation ongoing since 2019 and in line with China' strategic interests. Throughout 2022, fake online accounts notably promoted the narrative that the U.S. was responsible for bombing the Nord Stream gas pipelines for its own economic benefit and attempted to discourage Americans from voting in the U.S. 2022 midterm elections. Fake accounts impersonating the Intrusion Truth collective also claimed APT41 was a U.S.-nexus intrusion set. This last observation is complementary to China' s recent more aggressive stance in naming and shaming the U.S. for cyber malicious activities and publicly reacting to suspicions of Beijing-assigned cyber operations. To Sekoia.io analysts, this can also be considered as part of information operations to shape the opinion of online audiences.

Very **few reports indicate disruptive activities led by China-nexus intrusion sets**, and Sekoia.io analysts did not find any information related to destructive campaigns. Of interest are the low intensity / low advancement disruptive campaigns targeting Taiwan, in August 2022, including Distributed Denial of Service against government websites and public screen defacements. Sekoia.io analysts assess **these activities were almost certainly part of a demonstration rather than intended to actually disrupt activities in Taiwan**, hence plausibly falling in the info ops category.

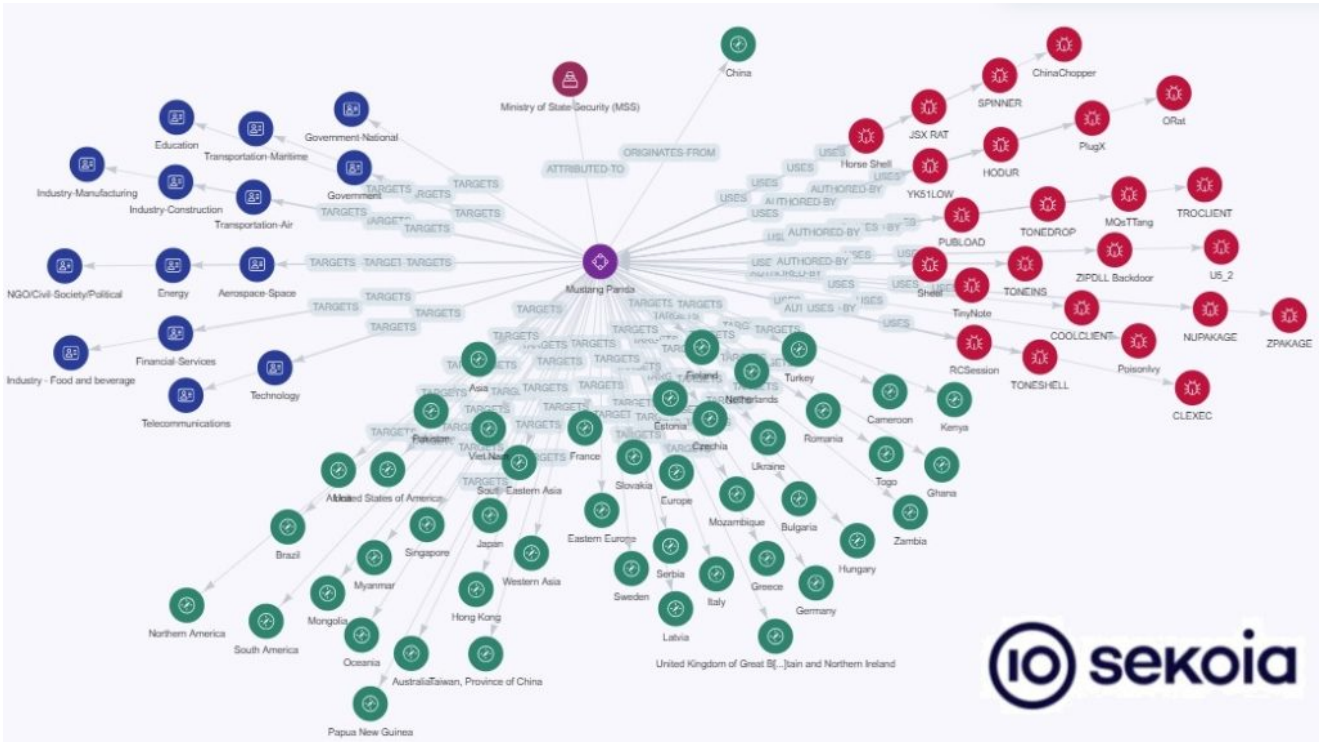
Panda is such a sudden rush for me

We don't know you, no one does.

Reflecting involved stakeholders in the Chinese cyber offensive apparatus, **China-nexus intrusion set landscape is heterogeneous and opaquely state-linked, characterised by dynamic and evolving relationships** between threat actors and state bodies across

spectrum of direct government sponsorship and independent moonlighting activities. Additionally, it is suspected that these intrusion sets would resort to **quartermasters** (i.e. mutualized malware developers, possibly initial access brokers) which further blurs the lines. While this has a limited impact for detection, this hinders Cyber Threat Intelligence (CTI) efforts. As of the time of writing, here is Sekoia.io TDR analysts' understanding of a few China-nexus intrusion sets and their links to the Beijing cyber apparatus.

Based on our current visibility into recent China-nexus cyber malicious activities, we identified a **strong predominance of MSS-linked intrusion sets activities**, including Mustang Panda (conflated with RedDelta and Camaro Dragon), APT10 (conflated with Witchetty and MirrorFace), and APT41. Another identifiable trend in the recent reporting of China aligned cyber activities is the **increasing number of clusters tracked as standalone groups**. One hypothesis is that this is a possible reflection of changes in resource allocations (both human and financial), in mandates or in processes in China's offensive cyber apparatus and/ or across its contractor's base. Another explanation is a growing trend in the CTI industry where researchers opted for documentation of activities rather than playing the attribution game, something China CTI analysts like to call the WinnTI effect.



Mustang Panda's victimology and toolset

That's my toolset lying in the trunk

China-nexus intrusion sets leverage **malware originating from China's hacking community, commodity malware, customised or repurposed tools, signature malware, and zero-day software vulnerabilities**. Open sources indicate that through steady investment in developing custom malware for privilege escalation, lateral movement, and

network reconnaissance, as well as improvements in command-and-control infrastructure, Chinese-linked intrusion sets departed from historically less advanced and "noisy" behaviour to becoming stealthier and more persistent. MSS-linked cyber espionage operators notably secured persistent access to victim organisations through **compromises in third-party trusted supply chains** including chat applications, **leveraging living-off-the-land techniques, and exploitation of Internet exposed edge devices**.

Of note, this FLINT was finalised on 18, July 2023 and dated for publication on 20, July 2023. We welcome that parts of their findings align with Mandiant's report on Chinese Cyber Espionage tactics, issued on 18, July 2023.

Leveraging zero-day vulnerabilities

In addition to heavily targeting Remote Code Execution (RCE) vulnerabilities, China-nexus intrusion sets were reported using zero-day vulnerabilities, as illustrated by Mandiant's publications including the exploitation of zero-day vulnerabilities (CVE-2021-44207 and CVE-2021-44228) by APT41, the leveraging of a local zero-day vulnerability in FortiOS (CVE-2022-41328) to deploy custom malware families on Fortinet and VMware systems by UNC3886 in September 2022, and UNC4841 targeting Barracuda ESG Zero-Day Vulnerability (CVE-2023-2868) to gain access to ESG appliances and deploy additional malware. In September 2022, two Microsoft Exchange zero-day vulnerabilities (aka ProxyNotShell) tracked as CVE-2022-41040 and CVE-2022-41082 were exploited by an unidentified China-nexus intrusion set. In January 2023, Mandiant also reported on China-nexus intrusion sets leveraging CVE-2022-42475 since at least October 2022.

Of note, Sekoia.io TDR analysts concur to the broader CTI community's assessment that **acquisition of zero-day vulnerabilities is almost certainly supported by the Chinese Regulations on the Management of Network Product Security Vulnerabilities** promulgated in July 2021. Interestingly this notably resulted in Chinese security researchers trying to find opportunities on other markets, including in Russia. Sekoia.io analysts assess that this trend is likely to impact the broader cyber threat landscape, notably **contributing to further proliferation in cyberspace**.

Development of cross platform capabilities

Between 2022 and 2023, Sekoia.io analysts observed China-nexus intrusion set developing **cross-platforms capabilities**. Such instances include LuckyMouse using an Rshell Mach-o implant to target MacOS users in addition to Linux users, APT15 developing an iOS version of its signature BadBazaar malware, Gallium developing a Linux variant of their signature malware PingPull and ChamelGang now targeting Linux users with their variant of ChamelDoH. This likely reflects China-nexus intrusion sets' **intent and capability to further expand their victimology**.

Developing variants and new attack capabilities

China-nexus intrusion sets continued dedicating efforts to **develop their malicious cyber capabilities including malware and frameworks**. Notable developments include the Manjusaka framework, presented as a potential Cobalt Strike successor. It is developed in Rust and targets Windows and Linux platforms, with a C2 written in Golang, and would be used by China-nexus intrusion sets since at least June 2022. Other developments of interest are Gallium new Linux backdoor Sword2033, WinnTI's Mélofée malware, Ke3chang's Graphican's **[4]** backdoor, an evolution of its Ketrican signature malware. Of note, while Symantec associate this toolset to APT15, Sekoia.io analysts' delineation of APT15 and APT25 leads us to associate both backdoors to Ke3chang, in line with ESET. Similarly to their tempo of activity, **Mustang Panda was one of the most prolific intrusion sets when it comes to malware development between 2022 and 2023**. Mustang Panda's recent developments notably include the MQsTTang backdoor (aka QMAGENT),TONESHELL, Horse Shell and NUPAKAGE.

Updating TTPs

Chinese intrusion sets, including **APT41 [7]**, DaggerFly, Mustang Panda, Tonto Team, Lucky Mouse and Dark Pink were reported increasingly using a technique known as DLL side-loading (T1574.002) to load their malware on targeted machines. As this technique usually leverages legitimate applications or executables, it **decreases the risk of detection hence increasing the rate of success of a campaign**.

Of particular interest is Mustang Panda's recent TTPs shift. As per TrendMicro findings, since October 2022, Mustang Panda used Google accounts to send email messages with lures to trick their targets into downloading password-protected archives containing a malware from Google Drive links. Mustang Panda was also seen resorting to ISO files containing a simplified shortcut (LNK) file to deliver an encrypted PlugX payload.

The intrusion set was also observed using HTLM Smuggling (T1027.006) a well-known technique, also used by NOBELIUM. These techniques notably allow intrusion sets to **evade detection and hinder static analysis**. It is possible these instances are attempts by intrusion sets to experiment new TTPs and maintain their tempo of activity.

Targeting network devices

China-aligned intrusion sets continued targeting network devices, including routers, Internet exposed and vulnerable servers and edge devices, by leveraging vulnerabilities (see the "leveraging zero-day vulnerabilities" hereinabove) and **developing custom malware**.This includes Gallium's BlackMould, a native webshell for servers running Microsoft IIS and based on China Chopper. In January 2023, Mandiant documented a new backdoor called BOLDMOVE, first observed in December 2022, specifically designed to run on FortiGate Firewalls and associated with the exploitation of the FortiOS vulnerability CVE-2022-49475.

Additional examples include Horse Shell, a malicious C++ firmware implant tailored for TP-Link routers according to the technique "**Bring Your Own Firmware**" to compromise read only file systems.

Horse Shell share similarities (but no code overlap) with APT31's Pakdoor. In certain cases, including Pakdoor's, **compromised assets are leveraged as an anonymization layer**, allowing the intrusion set to use them as proxy hops or C2s. Dalbit and Volt Typhoon and GobRAT were also recently observed leveraging this technique. Sekoia.io analysts assess targeting network devices not only enable malicious operators to **achieve their objective without user interaction and provide lateralisation opportunities (notably targeting hypervisors), it also provides them stealthiness (no supervision) and consequently, persistence**.

USB as an intrusion vector

A more recent trend in China-nexus intrusion sets malicious cyber campaign is the **revival of USB devices both as an intrusion vector and a propagation means**. This is notably illustrated by Mustang Panda's leveraging of HUIPAN, a USB worm, and ACNSHELL reverse shell used to replicate themselves over USB devices, as well as their use of USB device as an infection vector to deliver the PlugX backdoor. Dark Pink was also observed conducting lateral movement over USB devices and reported infecting USB devices attached to compromised computers. Additional Chinese intrusion sets leveraging USB devices include UNC4698, UNC4191, and TA410. Sekoia.io analysts assess these activities are **likely to result in collateral damages, and are an illustration of China's even more aggressive stance in cyberspace**.

PS – we should anticipate together too

Considering China-nexus recent cyber enabled activities, Sekoia.io analysts would like to highlight how **geopolitics shape cyber offensive doctrine and cyber malicious activities**. China's current position on the international scene is particularly challenged, notably on the economical and political fronts. Beijing certainly perceives these challenges as significant threats to their strategic interests, the primary one being the existence and legitimacy of the CCP.

As highlighted in this document, China-nexus cyber malicious campaigns mostly pertain to the full spectrum of cyberespionage activity. We assess China-aligned cyberespionage operations will almost certainly continue in the short term, notably conducted by MSS-associated intrusion sets.
We expect China-nexus intrusion sets will carry on dedicating efforts to develop their toolset and update their TTPs to continue conducting cyber malicious activities, with a strong focus on stealthiness and persistence.

Based on past observed activities, Sekoia.io analysts assess that while China-nexus intrusion sets demonstrated their intent and capability to conduct cyber malicious activities worldwide, **Asia, Europe and the U.S. will remain primary targets**. We further assess China-nexus intrusion sets will almost certainly continue targeting government, including embassies and foreign ministries, telecommunication companies, manufacturing including semiconductors industry and high technology, aerospace and defence entities, organisations involved in the military and the defence industrial base (DIB), as well as the logistics ecosystem.

The ongoing **Sino-U.S. confrontation will continue to be a strong driver for China-nexus cyber campaigns in the short term**, especially in the Southeast Asia region, highly likely impacting NATO Countries and Partners, as well as NATO aligned nations. Domestically, China will almost certainly continue conducting operations against civil rights defenders, journalists, dissidents, NGOs, as well as ethnic and religious minorities. Sekoia.io analysts assess that complementary to their aggressive stance in cyberspace, **China will almost certainly continue leveraging economic, financial, and legal instruments to assert their position and be recognized as a leader internationally**.

To anticipate the threat posed by Chinese cyber malicious activities, Sekoia.io TDR analysts will continue tracking their operations and report through our Intelligence Centre and welcome any feedback that could provide further visibility into this threat.

External references

[1] https://ig.ft.com/taiwan-economy/. Accessed September 7, 2023

[2] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/china-apt-antlion-taiwan-financial-attacks. Accessed September 7, 2023

[3] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt-attacks-telecoms-africa-mgbot. Accessed September 7, 2023

[4] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/flea-backdoor-microsoft-graph-apt15. Accessed September 7, 2023

[5] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/hydrochasma-asia-medical-shipping-intelligence-gathering. Accessed September 7, 2023

[6] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/witchetty-steganography-espionage. Accessed September 7, 2023

[7] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments. Accessed September 7, 2023

[8] https://www.welivesecurity.com/2022/09/06/worok-big-picture/}{targeting. Accessed September 7, 2023

[9] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackfly-espionage-materials. Accessed September 7, 2023

Chat with our team!

Would you like to know more about our solutions?
Do you want to discover our XDR and CTI products?
Do you have a cybersecurity project in your organization?
Make an appointment and meet us!

Contact us

Thank you for reading this blogpost. **We welcome any reaction, feedback or critics about this analysis. Please contact us on tdr[at]sekoia.io**
Feel free to read other TDR analysis here :

Comments are closed.