

 BRIEF

CHINA-TAIWAN CONFLICT: CYBER POSSIBILITIES ZEROFOX INTELLIGENCE

B-2022-10-14a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Geopolitical Cyber Activity

October 14, 2022



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 3:00 PM (EDT) on October 5, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

China-Taiwan Conflict Cyber Possibilities

Executive Summary

The potential for material conflict between China and Taiwan has risen in recent years. The language of the so-called 1992 Consensus—which provided a conceptual framework for a nominally-unified China while allowing the mainland and its island neighbor to govern themselves autonomously¹—has been increasingly undermined by rhetoric from the leadership of both countries. Chinese President Xi Jinping has named “reunification” of the two lands among China’s priorities,² while President Tsai Ing-wen of Taiwan has explicitly denied that her country is a territory of the mainland.³ Additionally, China has recently ignored a historically respected “median” running through the Strait of Taiwan when deploying warships there.⁴ Displays of military readiness notwithstanding, economic disincentives—most notably China’s reliance on Taiwanese microchip technology—make a physical invasion of Taiwan a less likely, near-term manifestation of this conflict than a cyber campaign targeting strategically-sensitive Taiwanese assets.

Details

In order of likelihood, attack options Beijing might feasibly undertake against Taiwan include 1) targeting the intellectual property of Taiwan’s semiconductor manufacturing industry; 2) leveraging distributed denial-of-service (DDoS) against government and

1

[hXXps://www.brookings\[.\]edu/on-the-record/understanding-beijings-motives-regarding-taiwan-and-americas-role/](https://www.brookings.edu/on-the-record/understanding-beijings-motives-regarding-taiwan-and-americas-role/)

2 [hXXps://www.cfr\[.\]org/backgrounder/china-taiwan-relations-tension-us-policy-biden](https://www.cfr.org/backgrounder/china-taiwan-relations-tension-us-policy-biden)

3

[hXXps://www.theguardian\[.\]com/world/2020/jan/15/tsai-ing-wen-says-china-must-face-reality-of-taiwans-independence](https://www.theguardian.com/world/2020/jan/15/tsai-ing-wen-says-china-must-face-reality-of-taiwans-independence)

4

[hXXps://www.reuters\[.\]com/world/asia-pacific/chinas-navy-begins-erase-imaginary-taiwan-strait-median-line-2022-08-25/](https://www.reuters.com/world/asia-pacific/chinas-navy-begins-erase-imaginary-taiwan-strait-median-line-2022-08-25/)



private sector websites; 3) exploiting zero-day vulnerabilities; and 4) targeting Taiwanese critical infrastructure.

Cyber warfare, like conventional warfare, is often conducted clandestinely. Amid the current level of conflict between China and Taiwan, preparatory work for some of the scenarios outlined in this briefing may already be in progress, and the outlined attack against the semiconductor industry may be well underway. Attacks with higher visibility and impacts carry greater risk to China. The more an attack exposes China to public scrutiny and potential retaliation, the less likely its execution.

Analyst Commentary

Intrusion Targeting Taiwan's Semiconductor Industry

Chinese reliance on Taiwan's chip manufacturing industry, which reportedly provides 90 percent of the world's most advanced semiconductor needs, serves as a powerful deterrent to military action against the island. China currently accounts for 60 percent of the global demand for semiconductors, and 90 percent of its needs are met by imports or domestic facilities owned by foreign companies. While a takeover of Taiwan's semiconductor industry through force of arms might appear to serve Beijing's interests, a 2021 Reuters study indicates that an invasion would endanger the foundries of the country's dominant manufacturer, TSMC. Moreover, such a turn of events would cut off those foundries from a delicate supply chain, resulting in a global disruption that would harm China disproportionately.

China has meanwhile embarked on an initiative to develop semiconductor self-sufficiency.⁵ A cyber campaign targeting the intellectual property of TSMC and other semiconductor companies would bolster this effort and—as the most tangibly beneficial of Beijing's options in a conflict with Taiwan—is the most likely intrusion or attack scenario. Some 30 advanced persistent threat (APT) groups⁶ and other notable hacking groups have been linked to the Chinese government,⁷ and they have exhibited a high level of ingenuity and success in stealing data from other governments and organizations. One APT group discovered in June 2022, dubbed “Aoqin Dragon” by researchers, used techniques ranging from low-level social engineering to sophisticated Dynamic Link Library (DLL) hijacking to obtain system access to government, education, and telecommunications organizations in Australia and Southeast Asia. In a number of cases, Aoqin Dragon actors were able to maintain access to these systems continuously from as early as 2013.⁸ China has also made use of its own nationals

⁵ [hXXps://www.reuters\[.\]com/investigates/special-report/taiwan-china-chips/](https://www.reuters.com/investigates/special-report/taiwan-china-chips/)

⁶ [hXXps://www.mandiant\[.\]com/resources/insights/apt-groups](https://www.mandiant[.]com/resources/insights/apt-groups)

⁷ [hXXps://attack.mitre\[.\]org/groups/G0125/](https://attack.mitre[.]org/groups/G0125/)

⁸

[hXXps://www.sentinelone\[.\]com/labs/aoqin-dragon-newly-discovered-chinese-linked-apt-has-been-quietly-spying-on-organizations-for-10-years/](https://www.sentinelone[.]com/labs/aoqin-dragon-newly-discovered-chinese-linked-apt-has-been-quietly-spying-on-organizations-for-10-years/)



working abroad to obtain illicit access to assets located in host countries. In 2021, Japanese investigators alleged that, under the supervision of China's military, a Chinese national used a fake ID while working as a systems engineer in Japan to obtain a rental server and staged intrusions against 200 companies and research institutes. A comparable intrusion scenario in Taiwan, which hosts Chinese nationals holding work permits, is also a possibility.⁹

Intrusions staged with the aim of stealing intellectual property are generally attempted in secret and over lengthy periods of time. As such, a Chinese-sponsored intrusion into Taiwan's semiconductor industry may not be discernible as an escalated "step" in a visibly unfolding conflict. Under this scenario, the industry would suffer a loss of confidential data, but the availability of its services would not be affected.

Attacks Targeting Government and Private Sector Websites

DDoS attacks targeting Taiwanese government websites that correlate with tensions between Beijing and Taipei have been publicly identified. Targets have included Taiwan's Defense Ministry, Office of the President, Foreign Ministry, and Taoyuan International Airport. DDoS attacks are relatively simple to execute and generally cause short-term inconvenience rather than serious debilitation. Conducted on a notable scale, such attacks could potentially serve as a "warning" of China's capacity to take more aggressive measures. As they are unlikely to provoke retaliatory measures and do not require significant resources, China is more likely to stage DDoS attacks targeting websites than other high-visibility attacks.¹⁰

Attacks Targeting Zero-Day Vulnerabilities on a Wide Scale

One of the most notable attacks observed in 2021 involved the infection of tens of thousands of Microsoft Exchange servers by the Chinese government-sponsored hacking group known as Hafnium. After discovering four zero-day vulnerabilities (vulnerabilities not yet publicly identified and for which patching is unavailable), the attackers conducted mass scanning to pinpoint vulnerable servers and then programmed "web shells" into those identified servers that enabled sending remote commands or implanting malware. Hafnium is not known to have staged further attacks on these targets beyond this initial act of compromise, but secondary attacks involving attempts to steal data or cause other compromises were subsequently conducted by other cybercriminals. Most of the affected companies were small to medium in size and housed Microsoft Exchange servers on-premises rather than using more expensive cloud resources. Because of their limited assets, many of these companies would not typically be of high interest to a state-sponsored actor. Some

⁹ [hXXps://www.theregister\[.\]com/2022/03/14/taiwan_china_tech_worker_raids/](https://www.theregister.com/2022/03/14/taiwan_china_tech_worker_raids/)

¹⁰ [hXXps://www.cfr\[.\]org/blog/what-are-implications-cyber-dimension-china-taiwan-crisis](https://www.cfr.org/blog/what-are-implications-cyber-dimension-china-taiwan-crisis)



observers have theorized that Hafnium intended to determine which of the affected companies merited further probing after installing the web shells. A majority of the compromised U.S. servers were patched after the related exploits came to light.¹¹

Another possible explanation for the Hafnium attacks is that they were staged as an ambitious proof-of-concept—a blueprint for a future coordinated attack. Regardless of the intention behind them, the Microsoft Exchange attacks demonstrated China's capability of identifying zero-day vulnerabilities and exploiting them on a massive scale. At a heightened stage of conflict, China-backed actors could potentially identify other common vulnerabilities among on-premises servers or other private infrastructure in Taiwan and exploit them by installing web shells. Through subsequent commands sent through those shells, actors could then compromise the availability of the targeted servers or related assets on a scale that would be felt throughout Taiwan. This could be accomplished through ransomware, which state-backed groups such as APT41 have been known to deploy for their own benefit, or through the delivery of other disruptive executables. Such capabilities could be unleashed in a widespread compromise of servers, making operationally-critical data, software, or hardware unavailable to multiple organizations.

Such a course of action would point back to China and expose the country to global condemnation and sanctions, making this scenario less likely than others but possible in the context of escalating conflict.

Attacks Targeting Public Infrastructure

Malicious cyber activity traced to Chinese state-sponsored actors has overwhelmingly consisted of attempts to steal intellectual property and other data. However, in 2021, CISA reported that actors supported by China had targeted 23 natural gas pipelines in the United States from 2011 to 2013. Thirteen of the pipelines were confirmed as compromised, and three were regarded as “near misses.” CISA assessed that the attacks were staged for the purpose of providing China the capability of disrupting or damaging U.S. pipelines.¹²

In light of the currently hostile nature of Chinese-Taiwanese relations, it is possible that China has conducted similar probing of critical infrastructure in Taiwan. Such infrastructure could include components of the country's electrical grid or cloud data centers.

An attack that disrupted critical infrastructure in Taiwan or rendered it inoperable would be regarded internationally as a severe act of aggression and would potentially

¹¹ [hXXps://www.wired\[.\]com/story/fbi-takes-drastic-step-to-fight-china-hacking-spree/](https://www.wired.com/story/fbi-takes-drastic-step-to-fight-china-hacking-spree/)

¹² [hXXps://www.cisa\[.\]gov/uscert/ncas/alerts/aa21-201a](https://www.cisa[.]gov/uscert/ncas/alerts/aa21-201a)



expose China to retaliatory measures. Such an attack is therefore the least likely scenario in a conflict between China and Taiwan, but there is evidence that such a capability exists.

Recommendations

Organizations with a presence in Taiwan need to consider the extent to which their assets in that country are exposed to the possible state-sponsored attacks described in this briefing, the value of those assets, and whether investing in enhanced security merits the added cost.

- Organizations with a presence in Taiwan should consider the risk of maintaining on-premises mail and application servers in an area expressly targeted by a hostile nation-state rather than seeking cloud-based alternatives. To the extent that implementing internet-facing, on-premises servers is a business requirement, organizations can conduct regular vulnerability scanning that incorporates web shell detection.¹³ Connected environments can also be protected by adopting measures recommended by the Cybersecurity and Infrastructure Security Agency (CISA) in a 2018 advisory to Managed Service Providers (MSPs) targeted by the “Cloud Hopper” campaign.¹⁴ These measures go beyond standard security practices, addressing the capabilities of highly-skilled actors. In light of the SolarWinds attacks of 2021 (reportedly staged by Russian state-sponsored actors), CISA’s recommendations in that advisory to secure DLL libraries by disallowing loading of remote DLLs and enabling “Safe DLL Search Mode” in Windows applications to force the use of restricted libraries remain relevant.¹⁵
- To address the risk of attacks on Taiwanese power grid or cloud infrastructure, organizations with related dependencies can strategically invest in backup power generators and system redundancy as part of their business continuity planning.
- Organizations with operations or supply chain sourcing from these areas should remain apprised of the situation; ZeroFox Intelligence also recommends conducting an in-depth Regional Threat Landscape Assessment for an extensive review of risks and threats that will highlight impacts on business operations and continuity, which can be requested via the [REF button](#) in the ZeroFox platform.

¹³

[hXXps://media.defense\[.\]gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF](https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF)

¹⁴

[hXXps://www.cisa\[.\]gov/uscert/sites/default/files/publications/Chinese-Cyber-Activity-Targeting-Managed-Service-Providers.pdf](https://www.cisa.gov/uscert/sites/default/files/publications/Chinese-Cyber-Activity-Targeting-Managed-Service-Providers.pdf)

¹⁵ [hXXps://www.upguard\[.\]com/blog/dll-hijacking](https://www.upguard[.]com/blog/dll-hijacking)



Appendix: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.