THREAT BULLETINS

Potential Implications of a United States Speaker of the House Nancy Pelosi visit to Taiwan

TLP:WHITE

Aug 02, 2022

On August 1, 2022, United States Speaker of the House Nancy Pelosi announced that she had touched down in Singapore, the first stop of her tour of the Indo-Pacific region. Pelosi's tour will likely include stops in Singapore, Malaysia, South Korea, and Japan. There has been no official mention of Taiwan. However, Taiwanese newspapers have confirmed her visit for Tuesday, August 2, 2022.

Analysis:

China has vowed military retaliation if Pelosi proceeds with visiting Taiwan. This is in response to the Chinese perception that her visit to Taiwan would be in direct violation of the One China policy of 1972 which clarified the United States' stance that Taiwan is a part of China but should be reunified peacefully with mainland China. It has served as the backbone of China/US trade deals and military peace between the two nations. However, China has taken Pelosi traveling to Taiwan on an official plane as a sign that the United States sees Taiwan as an independent country, thus nullifying a decades-old agreement between the two countries. Today, August 1, 2022, is the 95th Anniversary of the founding of the People's Liberation Army (PLA), placing China in a

unique position of military readiness to interfere with any attempt from Pelosi to visit Taiwan.

Chinese Foreign Ministry Spokesperson, Zhao LiJian stated that "A visit to Taiwan by Speaker Pelosi would challenge China's red line, and any challenge to our red line will no doubt be met with resolute countermeasures." Additionally, the PLA has released a video of military exercises with the caption "stand by in battle formation, be ready to fight upon command, bury all incoming enemies." This is most likely in reference to the pledged military response to Pelosi planning to go to Taiwan. A likely course of action is for China to impose a no-fly zone over Taiwan, making any further attempts at contact an act of war.

Within the United States Government, there has been much discourse surrounding Nancy Pelosi's decision to travel to Taiwan, with the United States President, Joe Biden, overtly disagreeing with her decision to visit Taiwan. However, there are others who support Nancy Pelosi's decision to travel to Taiwan, stating that a refusal on her part would indicate Washington's complacency in Beijing's authoritarian rule.

The United States has moved the aircraft carrier USS Ronald Reagan and a strike group into the South China Sea in preparation for a potential Taiwan visit from Nancy Pelosi. The US military posturing indicates that the United States is ready to react should any military intervention occur.

Most of the malicious cyber activity stemming from China has been geared toward intellectual property theft (IPT). With the continuation of Covid and other diseases heavily impacting Chinese citizens, healthcare data would not only be an intelligence priority but a national security interest in the context that the theft of it would be a crucial part of a PLA demonstration. With so much intellectual property stored in computer systems, a hybrid military force such as the PLA could prove troublesome for healthcare entities.

Health-ISAC is releasing this intelligence report to highlight geopolitical and security awareness. Health-ISAC will be following the situation closely and will potentially release future intelligence reports when appropriate. Included in this report are several sections of strategic analysis, including healthcare & pharmaceutical implications. Also contained in this alert are CVEs observed in a Chinese state-sponsored toolkit and remediations strategies released by the United States Health Sector Cybersecurity Coordination Center on November 19, 2020, can be found here.

Implications for Global Markets

The conflict between the United States and China has the potential to affect global commercial operations should the situation in the Indo-Pacific escalate. Global supply chains could be significantly disrupted if China imposed tariffs on all exported goods, or if Taiwanese

chip manufacturing is disrupted. Consumer markets are also concerned about implications for their general manufacturing dependency on China.

Offensive cyber-attacks in this conflict could spill over to large business networks and government networks potentially through spearphishing, backdoors, web app exploitation, and in-house developed zero-day exploits. Should the United States and Europe impose harsh financial consequences, China could potentially retaliate by imposing greater tariffs on western fiscal interests.

Healthcare & Pharmaceutical Implications

The global COVID-19 pandemic led China to target healthcare assets because of the intellectual strides western medicine was making against the virus. Since then, cyber-attacks have not subsided but increased. Due to the official cyber components of the Chinese military, cyber escalation in all sectors could be a byproduct of any military escalation between the United States and China over Taiwan.

Chinese State-Sponsored APT Toolkit

Vulnerabilities known to be exploited by Chinese state-sponsored APT actors for initial access include, but are not limited to:

Vendor	CVE	
Cisco	CVE-2018-0171	Ren
	CVE-2019-15271	RCE
	CVE-2019-1652	RCE
Citrix	CVE-2019-19781	RCE
DrayTek	CVE-2020-8515	RCE
D-Link	CVE-2019-16920	RCE
Fortinet	CVE-2018-13382	Auth
MikroTik	CVE-2018-14847	Auth
Netgear	CVE-2017-6862	RCE
Pulse	CVE-2019-11510	Auth
	CVE-2021-22893	RCE
QNAP	CVE-2019-7192	Priv
	CVE-2019-7193	Ren
	CVE-2019-7194	XML
	CVE-2019-7195	XML
Zyxel	CVE-2020-29583	Auth

Recommendations
Cybersecurity considerations:

- If working with Chinese organizations, closely monitor network traffic for anomalous activity.
- Inventory your organization's assets, endpoints, and networks passing through China or Taiwan.
- Monitor and detect anomalous traffic originating in China or Taiwan.
- Validate that remote access to your network requires multi-factor authentication.

- Disable nonessential ports and protocols.
- Protect all endpoints with antivirus/antimalware and update detection signatures regularly.
- Keep systems and products updated and patched as soon as possible after patches are released.
- Expect that data stolen or modified (including credentials, accounts, and software) before the device was patched will not be alleviated by patching, making password changes and reviews of accounts a good practice.
- Disable external management capabilities and set up an out-of-band management network.
- Block obsolete or unused protocols at the network edge and disable them in device configurations.
- Isolate Internet-facing services in a network Demilitarized Zone (DMZ) to reduce the exposure of the internal network.
- Enable robust logging of Internet-facing services and monitor the logs for signs of compromise.
- Health Industry Cybersecurity Practices, Cybersecurity Act of 2015, Section 405(d) guidance can be found here.

Sources

‘If she dares’: China Warns Nancy Pelosi Against Visiting Taiwan

Why Speaker Pelosi Must Go to Taiwan

Chinese State-Sponsored Cyber Activity

People’s Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices

APT1 Exposing One of China’s Cyber Espionage Units

Chinese State-Sponsored Cyber Operations: Observed TTPs

UPDATED: Carrier USS Ronald Reagan, F-35B Big Deck Operating Near Taiwan as Pelosi Arrives in Singapore; China Renews Threats

What you need to know about Pelosi's expected visit to Taiwan

China May Declare No-Fly Zone Over Taiwan Ahead of Nancy Pelosi’s Visit

Alert ID 332af9bb

View Alert

Tags United States Speaker of the House Nancy Pelosi, Taiwan, China

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Share Threat Intel For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP “Share Threat Intel” Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity related entities.

Turn off Categories For guidance on disabling this alert category, please visit the Knowledge Base article CSAP "Alert Categories" Toggle Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base

Access the Health-ISAC Intelligence Portal Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC’s Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.