GDIL **Team Cyber Pacific**

Indo-Pacific Cyber Brief – September 2023

Australia – 1.5 million person data leak, Chinese spear phishing

- Nearly 1.5 million Australians had personally identifiable information leaked due to breaches of Dymocks, the nation's largest bookseller, and Pizza Hut Australia. (Source)

- A foiled Chinese spear phishing campaign targeted Australian officials after the G7 summit in Japan. The campaign featured an infected word document emailed to Australian government officials from a fake Indonesian Ministry of Foreign and Economic Affairs account. (June) (Source)

ASEAN* - Chinese espionage, cyberslavery, Chinese spear phishing

- Three Chinese and Chinese-aligned cyber groups penetrated an unnamed Southeast Asian country from 2022-2023 and exfiltrated sensitive data. The observed tactics were previously documented in Laos. (Source)

- A UN report urged that transnational 'cyberslavery' operations in ASEAN, especially Laos, Cambodia, and Myanmar, continue to grow and pose a global security threat. Cyber slavery consists of young, tech-proficient individuals being abducted and forced to operate cyber-scamming operations. Syndicates are often international and involve government corruption. (Source)

- Singapore was also targeted by the foiled post-G7 foiled spear phishing campaign (see Australia section).

China – espionage, Uyghur surveillance, NSA named-and-shamed

- Threat Intelligence research revealed that Chinese military intelligence affiliated cyber operators conduct long-term espionage campaigns that target South Korean government, military, academia, and aerospace networks. (Source)

- Threat Intelligence research updated awareness on current multiyear covert surveillance campaigns by a Chinese Communist Party aligned group that targets Uyghur, Tibetan, and Taiwanese users. (Source)

* Excludes the Philippines.

- The Chinese Communist Party continued its 'name and shame' campaign calling out alleged US-backed cyber espionage against a Chinese state university. The call-out occurred alongside confirmation of reports of US hacking of Huawei and builds on last month's revelation of alleged US spying on the Wuhan Earthquake Monitoring Center.
(Source) (Source) (Source)

- Chinese based operators conducted a penetration campaign over the summer that targeted email accounts of over twenty US government organizations. Commerce Secretary Gina Raimondo's account was breached, and officers in the State Department and House of Representatives also report being affected. (July) (Source)

India – Pakistani DDoS and defacement, new cyber security policy

- Indian and Pakistani cyber operators traded DDoS and defacement attacks during the G20 Summit in Delhi. (Source) (Source)

- Indian affiliated cyber operators targeted Canadian military and parliament websites in the wake of rapidly deteriorating relations between the countries. (Source)

- The Indian Parliament passed the Cybersecurity and Digital Personal Data Protection Act of 2023 as data breaches among government institutions handling private health records have surged.
(Source)

Japan – Chinese espionage, Fukushima disinformation, India cyber diplomacy, joint advisory

- Chinese state media conducted a disinformation campaign distorting the risks posed by release of treated water from the Fukushima nuclear meltdown. This led to a domestic backlash against Japanese products and influence in China and abroad. (Source)

- Japan held the Fifth Annual Japan-India cyber dialogue wherein the countries discussed capacity building cybersecurity strategies and current 5G developments. (Source)

- Japan's NISC and National Police Agency released a joint advisory with the NSA, FBI, and CISA detailing the tactics, techniques, and procedures of Chinese-linked malicious cyber actor "Blacktech." The report is the first cyber advisory released featuring US-Japanese collaboration. (Source)

- Japan held the annual joint training exercise Orient Shield with the U.S. The exercise focused on training in 'actual combat', preparing for multi-domain operations including air, maritime, cyber and information warfare. (Source)

- Chinese military hackers breached classified Japanese military networks extensively in 2020, accessing plans and assessments of military shortcomings. (August) (Source)

The Pacific Islands – Tonga and Vanatu ransomed

- The Tonga Communications Corporation - one of two telecommunication companies on the island - was disrupted by a ransomware attack that brought public service administration to a halt. (February) (Source)
  - Vanuatu also suffered a widespread cyberattack against government sites and online services in November 2022 that resulted in the takedown of critical emergency communications and left government officials using personal email accounts a month after the shutdown. (Source)

The Philippines – Philippine universal healthcare ransomed, ombudsman breached

- The Philippine Health Insurance Corporation, the country's universal healthcare company, was compromised by the Medusa ransomware group. (Source)

- The Office of Ombudsman, which monitors and investigates political corruption in the Philippines, revealed a breach earlier in the year by an unknown group. The breach allowed parties to lawsuits to learn the outcome of their cases before they were publicly announced. (Source)

- The ALPHV ransomware Group breached Phil-Data Business Systems, a large Philippine IT company that works with multiple businesses and sectors. (Source)

South Korea – Chinese espionage, government cybersecurity investment , U.S. cyber diplomacy

- Research revealed that Chinese military intelligence affiliated cyber operators conduct long-term espionage campaigns that target South Korean government, military, academia, and aerospace networks. (see China Section)

- The Korean Ministry of Science and ICT (MSIT) announced a $97 million investment through 2027 to boost the global competitiveness of Korea's cybersecurity environment. Over 50% of the fund will be used to support startups in promising fields such as Zero Trust and AI. (Source)

- Ministry of Science and ICT (MSIT) officials met with US government and private sector individuals for the 7th US-ROK Information and Communications Technology Policy Forum. Initiatives proposed included information sharing, expert exchange, regular seminars to share threat information, and joint research projects in cybersecurity. (Source)

Taiwan[*] - Chinese espionage

- Threat Intelligence research revealed a long-term Chinese-based cyber espionage group that targets dozens of government, education, critical infrastructure, and information technology companies and agencies in Taiwan. (August) (Source)

[*] More robust coverage of Taiwan will begin in October 2023