GDIL **Team Cyber Pacific**

Indo-Pacific Cyber Newsletter–November 2023

Australia – New cyber strategy, ASD cyber threat report, DP world shipping company halted

- The Australian Department of Homeland Affairs released its 2023-2030 Cyber Strategy. The strategy aims to develop Australia into a world leader in cybersecurity by the end of the decade.
(source)

- Port operator DP world, responsible for 40% of Australian shipping, was compromised by an unknown actor leading to the halting of tens of thousands of shipping containers.
(source)

- The Australian Signals Directorate (ASD) released its 2022-2023 cyber threat report. A key takeaway was the targeting of critical infrastructure by Russian and Chinese state sponsored actors.
(source)

- Australia unveiled USD$33.7 million investment for cyber "rapid assistance" and vulnerability identification with Pacific Islands nations.
(Source)

ASEAN* – Cambodia compromised, Malaysian global phishing-as-a-service taken down

- Threat intelligence research revealed several Chinese cyber actors engaging in a widespread espionage campaign targeting more than 24 Cambodian government organizations from September to October 2023. The actors successfully exfiltrated classified national security information.
(source)

- The Royal Malaysian Police, FBI, and Australian federal police worked together to dismantle a major phishing-as-a-service operation in Malaysia, leading to the arrests of eight people and the termination of services for more than 8000 clients.
(source)

* Excludes the Philippines.

China – ICBC ransomed by Russian affiliated group, Taiwan operations ramping up

- The U.S. unit of the Industrial and Commercial Bank of China (ICBC), the world's largest bank, was ransomed by the Russian affiliated group Lockbit. The compromise forced deals to be transacted via thumb drives and has created security concerns for trading partners.
(source)(source)(source)

- A senior Google threat analysis manager revealed that Google has seen a massive increase in Chinese cyber operations targeting Taiwan in the past six months spanning from espionage to information operations.
(source)

- China featured in the Australian Signals Directorate's annual cyber threat report. ASD found that Chinese actors had increased their targeting of critical infrastructure.
(source)

- Threat intelligence research revealed several Chinese cyber actors engaging in a widespread espionage campaign across more than 24 Cambodian government organizations from September to October 2023. The actors exfiltrated classified national security information.
(source)

India – Cyber operations surge, Apple warns opposition politicians, hotel ransom

- Threat intelligence research found that state-sponsored attacks against India increased by 278% between 2021 and September 2023. Attacks on Indian government agencies went up by 460%, while startups and small and medium enterprises (SMEs) saw a 508% increase.
(source)

- Apple warned 20 prominent opposition politicians and journalists that they were targets of Indian state-sponsored cyber operations targeting and surveilling their personal devices.
(source)

- The private information of up to 1.5 million guests of Taj hotels was reportedly ransomed for $5,000USD. The exposed information includes mobile numbers, addresses, membership IDs, and other personally identifiable information.
(source)

Japan – Japan's NASA breached, Electronics giant ransomed, disinformation work with U.S.

- The Japan Aerospace Exploration Agency (JAXA) had a network breach from hackers exploiting vulnerabilities in the agency's network equipment. No critical information was reported leaked during the compromise. (source)

- A former employee of Nippon Telegraph and Telephone West Corporation leaked over nine million sets of customer information.
(source)

- A compromise on Japan Aviation Electronics' systems forced the company to shut down its websites. The compromise is allegedly due to ransomware gang AlphV/Black Cat.
(source)

- The US undersecretary of state for public diplomacy and public affairs will be holding bilateral discussions with Japan focusing on jointly countering malign foreign influence operations. This follows the U.S. signing a memorandum of understanding with South Korea to counter foreign information operations and trilateral discussions on the matter at Camp David in August.
(source)

The Pacific Islands – Australia, U.S., U.K. pledge strong support for cyber development

- Australia unveiled USD$33.7 million investment for cyber "rapid assistance" and vulnerability identification with Pacific Islands nations.
(Source)

- The United States announced it is working on over $8 billion worth of investments and programs, including in cybersecurity, at the Pacific Islands Forum. The cyber programs include support for internet infrastructure, cybersecurity training, and continued engagement in the Pacific Cyber Capacity Building and Coordination Conference (P4C).
(Source)

- The United Kingdom also participated in the forum and affirmed its support of 2050 Strategy for a Blue Pacific Continent, including its cybersecurity provisions.
(Source)

The Philippines – Military cyber defense, journalists and government entity compromised

- The Armed Forces of the Philippines (AFP) conducted a week-long Cyber Defense Exercise (CYDEX) as a part of their annual joint interoperability operations. AFP Cyber Units participated in both in-person and online exercises.
(source)

- The Philippine Center for Investigative Journalism (PCIJ) temporarily took down their website after being compromised by an unknown actor. This comes after the PCIJ released reports of online communities of Filipinos amplifying pro-Beijing disinformation narratives.
(source)

- Threat Intelligence research revealed that a Chinese-sponsored actor executed at least one successful campaign targeting and compromising an unnamed Philippine government entity for a period of five days in mid-August.
(source)

South Korea – Trilateral cooperation, Chinese fake news sites, offensive cyber strategy

- South Korea, the U.S., and Japan agreed to establish a quarterly high level consultative body to cooperate in countering malicious cyber threats from North Korea and elsewhere.
(source)

- The National Intelligence Service (NIS) exposed 38 Chinese-run fake news websites claiming to be members of the Korea Digital News Association. The sites reposted local news content without consent and distributed anti-U.S. and pro-China content.
(source)

- Defense Minister Shin Won-sik announced that South Korean military is developing a "proactive and offensive" cybersecurity strategy to counter threats in the cyber domain.
(source)

Taiwan – cyber pressure in run up to the elections

- A senior Google threat analysis manager revealed that Google has seen a massive increase in Chinese cyber operations targeting Taiwan in the past six months from espionage to information operations.
(source)