GDIL **Team Cyber Pacific**

Indo-Pacific Cyber Newsletter – October 2023

Australia – Russian DDoS, exercise Cyber Sentinels, Global Coalition on Telecommunications

- Pro-Russian hackers brought down Australian Department of Home Affairs websites for a few hours with a distributed denial of service (DDoS) attack. The group claimed it was in response to Australian provision of anti-drone platforms to Ukraine. (Source)

- The Australian Defense Force conducted its first military cyber exercise with the U.S. at the classified level, called Cyber Sentinels. The exercise involved simulating cyber defense under real world combat conditions and was also observed by Canadian, New Zealand, and United Kingdom participants. (Source)

- Australia joined Japan, Canada, the United Kingdom, and the United States in establishing the Global Coalition on Telecommunications (GCOT). The coalition aims to build norms, align funding, conduct joint research, and share information concerning telecommunications policy and infrastructure. (Source)

ASEAN* – Vietnamese Spyware against U.S., Thai crypto crime, Chinese cyber espionage

- Vietnamese officers attempted and failed to plant the spyware program Predator on the smartphones of U.S. members of Congress, policy experts, and journalists. The attempt came as the U.S. and Vietnam were negotiating the September Comprehensive Strategic Partnership. (Source)

- The Thai Cyber Crime Investigation Bureau, Binance, and the U.S. Homeland Security Investigation collaborated to apprehend members and assets of a Thailand-based crypto scam syndicate worth $277 million. (Source)

- Threat Intelligence research revealed an Chinese affiliated cyber espionage campaign running since 2021. The group has been targeting the telecommunications industry and government facilities in Vietnam, Kazakhstan, and Uzbekistan. (Source)

China – Cyber and AI enabled espionage denounced, cyber espionage against Vietnam

- The domestic intelligence chiefs of the Five Eyes alliance held an unprecedented joint conference in California to bring attention to the widespread theft of intellectual property coordinated and conducted by Chinese intelligence and government agencies. Chinese officials responded by describing it as a collective disinformation campaign. (Source)

* Excludes the Philippines.

- Microsoft reported that a Chinese Ministry of State Security affiliated hacking group has been exploiting vulnerabilities in a popular Australian-produced collaboration platform. The group is known for targeting engineering, medical research, government, defense, and tech firms in Western countries. (Source)

- Threat Intelligence research revealed an Chinese affiliated cyber espionage campaign running since 2021. The group has been targeting the telecommunications industry and government facilities in Vietnam, Kazakhstan, and Uzbekistan. (Source)

India – Largest data breach to date, cyber war with Hamas, Chinese financial scamming

- In the largest data breach in India to date independent cyber actors stole 815 million sets of personally identifiable information, including passport numbers and Aadhar cards, and offered them for sale on the dark web. (Source)

- Threat Intelligence research identified India as one of the most targeted countries by cyber-attacks related to the Israeli-Hamas war. This is due to Indian hacking groups publicizing numerous attacks that have effectively targeted Hamas web infrastructure. (Source)

- Threat Intelligence research revealed widespread Chinese-based financial scamming activities that have compromised tens of thousands of devices and bank accounts, mainly in India. The scam involves impersonating known Indian banks and offering fake loans in exchange for personal identifiable information. (Source)

Japan – Exercise and agreement with ASEAN, Google investment, GCOT, CISA framework

- Japanese public and private sector organizations signed a memorandum of understanding with eight ASEAN countries to deepen cooperation in cybersecurity. (Source)

- Japan held an infrastructure focused cybersecurity exercise alongside the U.S. and E.U. for ASEAN countries and India. (Source)

- Google announced that it is opening a "Cyber Security Center of Excellence" in Japan to pursue government dialogues, collaborative research, and training programs. (Source)

- Japan joined the U.S., U.K., Canada, and Australia in establishing the Global Coalition on Telecommunications (GCOT). The coalition aims to build norms, align funding, conduct joint research, and share information concerning telecommunications policy. (Source)

- The National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and JPCERT joined over a dozen international government partners to publish the U.S. CISA-led 'Secure by Design" policy guidance update. The guidance seeks to build consensus on raising security standards for software product. (Source)

The Pacific Islands – Google internet cables, Fiji-Australia cyber cooperation, Japan's plan

- In a deal funded by the U.S. and Australia, Google announced that they will build undersea internet cables to eight Pacific nations. As part of the project, the U.S. will also assist with cybersecurity resilience by enabling backup of vital data to global cloud networks. (Source)

- Fiji and Australia announced a cooperative effort in cyber security during the Fijian Prime Minister's official visit, aiming to strengthen their partnership and bolster Fiji's economic growth. (Source)

- Japan aims to establish a cyber defense network across the Indo-Pacific involving Pacific islands to counter cyber threats from nations like China and Russia and to enhance regional security cooperation. (Source)

The Philippines – Universal healthcare data leaked, U.S. readiness, new cyber command

- The Medusa ransomware group released 625 GB of sensitive personal information and transactions to the dark web after the Philippine Health Insurance Corporation, the country's universal healthcare company, refused to pay a ransom of $300,000 USD. (Source)

- The United States Ambassador to the Philippines expressed the United States' readiness to help the Philippines find ways to combat cyberattacks amid the increasing hacks occurring over the past months. (Source)

- The Philippine military announced its intent to create a cyber command to improve cyber defenses against near daily attacks to government agencies. To attract cyber professionals, the Philippine military plans on waiving the physical fitness requirements for recruiting. (Source)

South Korea – North Korean espionage targets shipbuilders, shoppers, and IT companies

- South Korea's National Intelligence Service announced that North Korea carried out attempted infiltrations of South Korean shipbuilding companies to conduct espionage during August and September. (Source)

- The National Intelligence Service also warned citizens that North Korea is using a copycat app of a popular South Korean e-commerce app to attempt steal South Koreans' personal information and credentials.(Source)

- North Korean hacker groups known for targeting IT and defense organizations in South Korea, the U.S., and India, exploited a remote code execution bug for malicious activities. The groups identified typically pursue cyber espionage, data theft, financially motivated attacks, and network sabotage. (Source)

Taiwan – Chinese semi-conduct espionage, IT and biomedical espionage, cyber diplomacy in EU

- Threat Intelligence research revealed a Chinese cyber espionage campaign targeting Chinese-speaking semiconductor companies with TSMC-themed lures infected with Cobalt Strike beacons. The campaign also targeted semi-conductor companies in Hong Kong and Singapore. (Source)

- Threat Intelligence research revealed a cyber espionage campaign that targeted manufacturing, IT, and biomedical companies in Taiwan. The hacking group was not attributed to a country, but also targeted Pacific Island countries, Vietnam, and the U.S. (Source)

- A delegation from the Ministry of Digital Affairs attended Cybersecurity Week event at the Hague where they exchanged presentations with senior employees of the Dutch multi-national telecom company KPN. (Source)