Cyber Security for Chinese Taipei

Purpose: Information
Submitted by: Chinese Taipei

Security and Prosperity Steering Group Meeting
9 October 2020
Cyber Security for Chinese Taipei

1. International Cooperation (update to September 2020)

Chinese Taipei actively cooperates with international cybersecurity organizations in incident handling and response. From January to August 2020, Chinese Taipei (TWNCERT) received and handled 735 incident reports from international cybersecurity organizations. The incidents mainly fall under the categories of malware, login attempt, spam and phishing. Chinese Taipei (TWNCERT) also issued 2,042 incident reports to 65 international cybersecurity organizations, mainly fall under the category of suspicious network attack, as well as spam host and infected system.

TWNCERT is a member of Asia Pacific Computer Emergency Response Team (APCERT) Steering Committee and the convenor of Training Working Group. Chinese Taipei aims to provide a platform for APCERT community to share and exchange valuable experiences and foster collaboration among members, thus raising the comprehensive cybersecurity defense capabilities of the Asia Pacific region. From January to August 2020, Chinese Taipei had convened three live streaming training programs, with a total of 22 APCERT member teams participating. TWNCERT also participates in the APCERT Drill Working Group, planning the APCERT Drill 2020 which was held in March 2020.

2. Cyber Offensive and Defensive Exercise (update to September 2020)

Chinese Taipei carries out a large-scale Cyber Offensive and Defensive Exercise (CODE), an extended engagement with varying simulations and drills holds annually to strengthen the cybersecurity capabilities of government agencies and critical infrastructure providers. Every other year, Chinese Taipei invites international experts to observe the exercise to promote international collaborations, jointly improve cybersecurity technical skills and incident response competencies. CODE 2019 carries out from April to November in addition to routine exercises (i.e., social engineering exercise, live-action exercise, and table-top drill) with a new transnational exercise, and this year focuses on the financial sector. CODE built a simulation environment in the cyber range platform for Red and Blue team confrontation. We invited foreign and domestic cybersecurity teams to act as Red Teams, and the teams from
critical infrastructures in financial sector to act as the Blue Teams. The attack and defend confrontation exercise was held from November 6th to 8th, and the Blue Team conducted the evaluation, incident response, and information sharing according to the actual situation. In CODE 2019, there are 65 people from 12 economies to join in. Participants are appreciated the performance of Chinese Taipei and recommend CODE to be held continually to help prompt the cybersecurity collaborations.

3. TWCERT/CC (update to September 2020)

Taiwan Computer Emergency Response Team/Coordination Center (TWCERT/CC) collaborates with international cybersecurity organizations, academic institutions, civil communities, government agencies, private enterprises, computer emergency response teams (CERTs), and computer security incident response teams (CSIRTs). Through cyber intelligence sharing, TWCERT/CC promotes international cybersecurity exchanges and cooperation and strengthens Chinese Taipei’s connections with international cybersecurity organizations. Meanwhile, to improve enterprises’ understandings in cybersecurity and their trust to TWCERT/CC, TWCERT/CC has established a public-private collaborative mechanism to assist private sectors in handling cybersecurity incidents and acts as the window to receive cybersecurity incidents reported by enterprises of Chinese Taipei.

The main tasks of TWCERT/CC include cyber intelligence sharing, outreaches, and promotions to improve public awareness in cybersecurity, international exchanges and collaborations, CVE vulnerability verification and publication, and malware inspection service.

The following paragraphs delineate TWCERT/CC’s development from January to August 2019:

**Cyber intelligence sharing and promotions of cybersecurity awareness:** From January to August 2020, TWCERT/CC has processed more than 1.1 million cyber intelligence from both domestic and worldwide. To accelerate the handlings of cybersecurity incidents and lower their influences, TWCERT/CC shares cyber intelligence with Chinese Taipei’s telecommunication and network communication service providers, N-ISAC, A-ISAC, as well as medical and financial institutions. TWCERT/CC also shares domestic and international cybersecurity news, hacking
incidents, and information of vulnerabilities through monthly e-newsletters, official website, and social media, including pixnet, Facebook, and Instagram. In addition, TWCERT/CC co-organized Information Security 2020, CYBERSEC 2020 as well as CISC2020, by giving speeches on the recovery of cyberthreats to high-tech industry to promote the TWCERT/CC services among enterprises and notification and responding measures while encountering cybersecurity incidents.

International exchanges and collaboration: In RSA Conference 2020, San Francisco, TWCERT/CC shared its experiences on intelligence analysis on cybersecurity, notifications, and the trend of international cyberthreats. By participating in the RSA, TWCERT/CC have an even better understanding about the current status and threat development of various cybersecurity fields, including topics such as ransomware, phishing, threat prevention and planning, and vulnerability disclosure and coordination. Moreover, TWCERT/CC had talked with cybersecurity enterprises and intelligence organizations to expand potential partnership and collaboration. With the experience of participating Cyber Offence and Defense Exercise, March 11th 2020, organized by APCERT, TWCERT/CC has strengthened its response capabilities. The theme in 2020 is “Banker doubles down on Miner”. A total of 33 teams participated, and 9 teams successfully completed all tasks within time, TWCERT/CC is one of them. With respect to international collaboration with intelligence organizations, in 2020, TWCERT/CC and Cyber Threat Alliance (CTA) sign a MOU on the basis of information exchange on malicious files, DN and URI as well as other attacking threats. On top of that, TWCERT/CC have established a cooperation channel with the cybersecurity intelligence platform, Cyble, to share information related to dark net, data leakage, malware, and cyber threats.

**Operational services:** to assist domestic and international IT manufacturers and service providers in easing and patching vulnerabilities as soon as possible, since 2018, TWCERT/CC has become one of the CVE numbering authorities (CNA) under the Common Vulnerabilities and Exposures (CVE) maintained by MITRE. In 2019, from January to August TWCERT/CC has verified and published 42 CVE vulnerability numbers. This not only effectively helps Chinese Taipei’s network and telecommunication service providers and application system developers solving the vulnerabilities within their products and services but also prevents these vulnerabilities from being leveraged to launch cyberattacks. Moreover, the verification and publication
of CVE numbers has increased the collaborative relationships on cybersecurity in between TWCERT/CC and private sectors. TWCERT/CC opens its Virus Check service to enterprises and the general public. Virus Check integrates static inspection and dynamic sandbox analysis mechanisms to comprehensively identify whether the file to be detected contains malware. A total of 975 files have been checked from January to August this year. Additionally, to improve the Chinese Taipei’s overall network security environment, we assist in notification of phishing related websites, 518 phishing websites were reported over the same period above.