TWNCERT Annual Report 2021

1. Highlights of 2021

1.1 Summary of major activities

TWNCERT (Taiwan National Computer Emergency Response Team) aims to support and enhance the government's ability to respond and deal with cyber security incidents. In 2021, TWNCERT issued more than three thousand notice advisories to government agencies. TWNCERT also provided consulting and training services for government agencies and critical infrastructure sectors.

To strengthen the preparedness against cybercrimes, technology failures, and Critical Information Infrastructure incidents, TWNCERT conducted a national cyber security exercise, Cyber Offensive and Defensive Exercise 2021 (CODE 2021), including Red vs Blue confrontation live action exercise in energy-field.

Besides, TWNCERT launched a series of cyber security competitions in 2021 to nurture cyber security talents and promote cyber security awareness. There are more than thirty thousand students, and the general public participated.

1.2 Achievements & milestones

TWNCERT developed three online courses to improve cyber security protection and awareness among government agencies in 2021. More than twenty thousand government staff attended the online and onsite training and took course exams.

As the convener of APCERT Training Working Group, TWNCERT convened seven online training sessions. A total of twenty-three APCERT member teams had participated in these programs.

2. About TWNCERT

2.1 Introduction

As a national CERT, TWNCERT acts as the point of contact for the CSIRTs in CI sectors in Taiwan and worldwide for the nation. We aim to enhance the government and CI sectors' ability to respond and deal with cyber security incidents and conduct technical and consulting services to government agencies.

2.2 Establishment

TWNCERT was established in 2001, formed by the National Information and Communication Security Taskforce (NICST). TWNCERT is also known as the National

Center for Cyber Security Technology (NCCST) domestically, led by the Department of Cyber Security of the Executive Yuan, which is in charge of the cyber security policy of Taiwan. The formation of TWNCERT aims to create a government cyber response center that can help optimize the capability of continuous monitoring, task coordination, and incident response and handling in the face of cyber security threats.

2.3 Resources

TWNCERT currently has around 140 full-time employees, and the operation funding comes from the Department of Cyber Security of the Executive Yuan.

2.4 Constituency

TWNCERT dedicates to enhancing the capability of incident reports and response among government authorities and CI sectors. Moreover, TWNCERT coordinates information sharing with various stakeholders such as Financial ISAC, Academic ISAC, National Communications Commission ISAC, Energy ISAC, Transportation ISAC, Hygiene ISAC, High-Tech Park ISAC, major MSSPs, law enforcement agencies, other CSIRTs in Taiwan as well as cyber security industries in Taiwan and worldwide.

3. Activities & Operations

3.1 Scope and definitions

Our critical mission activities are

- Incident Response

  Responsible for cyber security incident response in the government and CI sectors and effective practical assistance and support to related agencies to counter when under cyber attacks or facing threat situations.
- Information Sharing

  National Information Sharing and Analysis Center (N-ISAC) provides a central resource for gathering information on cyber threats to critical infrastructure and providing two-way sharing of information between the private and public sector.
- Cyber Security Drill & Audit

  Hold large-scale cyber offensive and defensive exercises, pairing with cyber security audits, cyber health checks, and penetration test services, to discover cyber security problems of the government and critical infrastructures in time.
- Education & Training

  Plan cyber security series competitions and training programs to enhance cyber security education effects and raise cyber security awareness.
- Coordination and Collaboration

Build coordination and communication channels with domestic and foreign incident response organizations; Coordinate with international CSIRTs, cyber security vendors, and other cyber security organizations.

3.2 Incident handling reports

In 2021, TWNCERT received nearly nine hundred reports on cyber security incidents from Taiwan government agencies. We also received about one thousand and two hundred cyber security incident reports from international CERTs/CSIRTS and cyber security organizations.

Moreover, more than one million cyber security incidents and critical information were shared among N-ISAC members, including CI sector ISACs, MSSPs, LEAs, and CSIRTs in Taiwan.

3.3 Abuse statistics

- Government agencies

  In 2021, TWNCERT received reports on cyber security incidents from government agencies. About 64% of the reported security incidents are in the category of Intrusion, as shown in Figure 1.

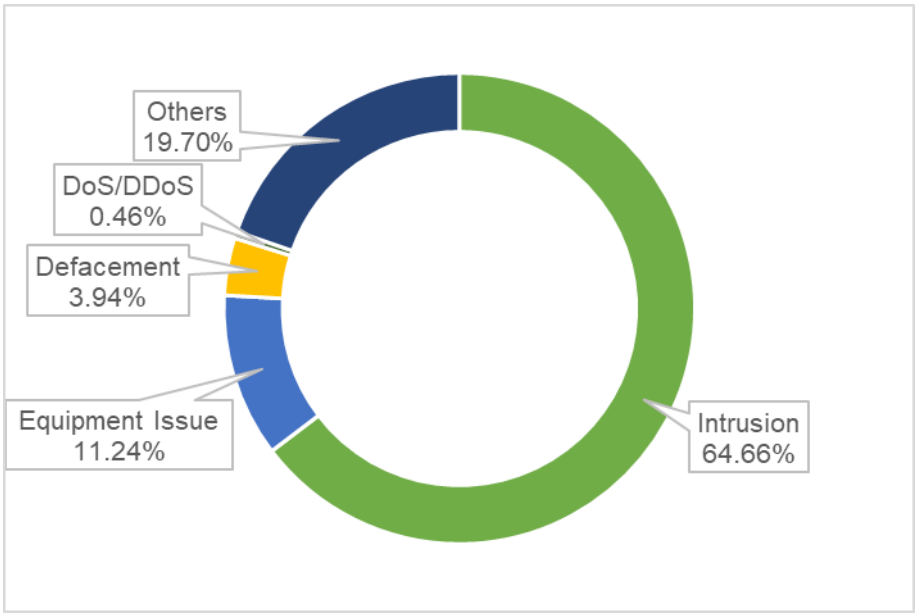

Figure 1 Security Incidents from Government Agencies

- International incident report

In 2021, TWNCERT received about one thousand and two hundred cyber security incident reports from international CERTs/CSIRTS and cyber security organizations. The incident reports were categorized as shown in Figure 2. About 67% of the incident reports were Malware Infected System, followed by Attack, Spam, and Phishing.

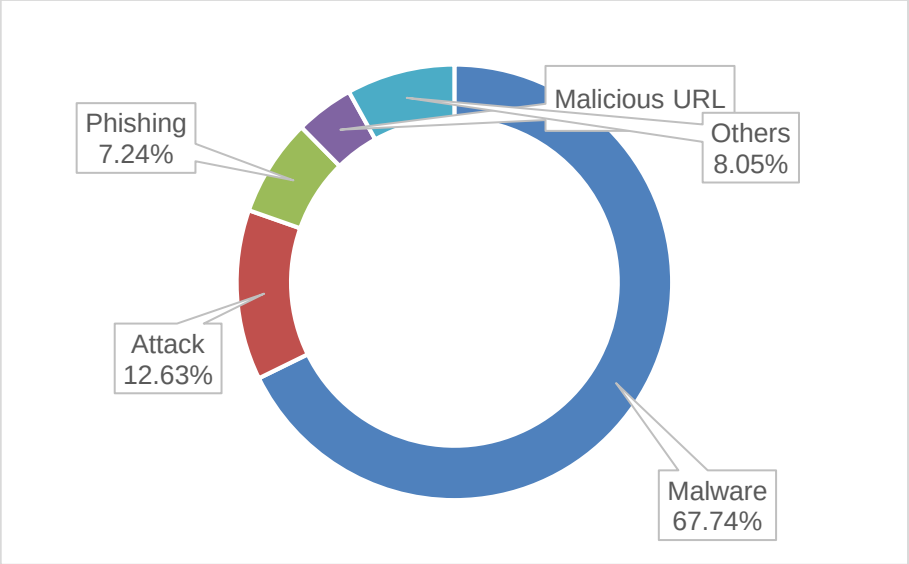

Figure 2 Category of International Incident Reports

- N-ISAC information sharing

  N-ISAC members shared more than one million cyber security incidents and critical information. The Early Warning is the most shared cyber security information in 2021, as shown in Figure 3.

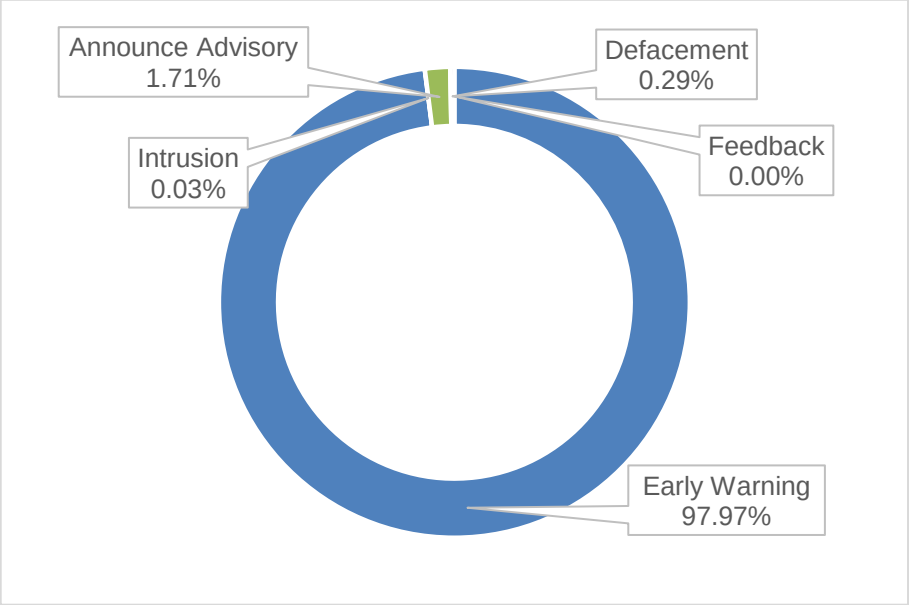

Figure 3 Distribution of N-ISAC Information Sharing

3.4 Publications

- Website publication

  TWNCERT collects and publishes cyber security advisories, news, and guidelines on the website. In 2021, TWNCERT published more than one hundred articles, including cyber security news and security alerts.

- Advisory and Alert

  In 2021, TWNCERT issued more than three thousand advisories to government agencies. The categories were distributed as in Figure 4.

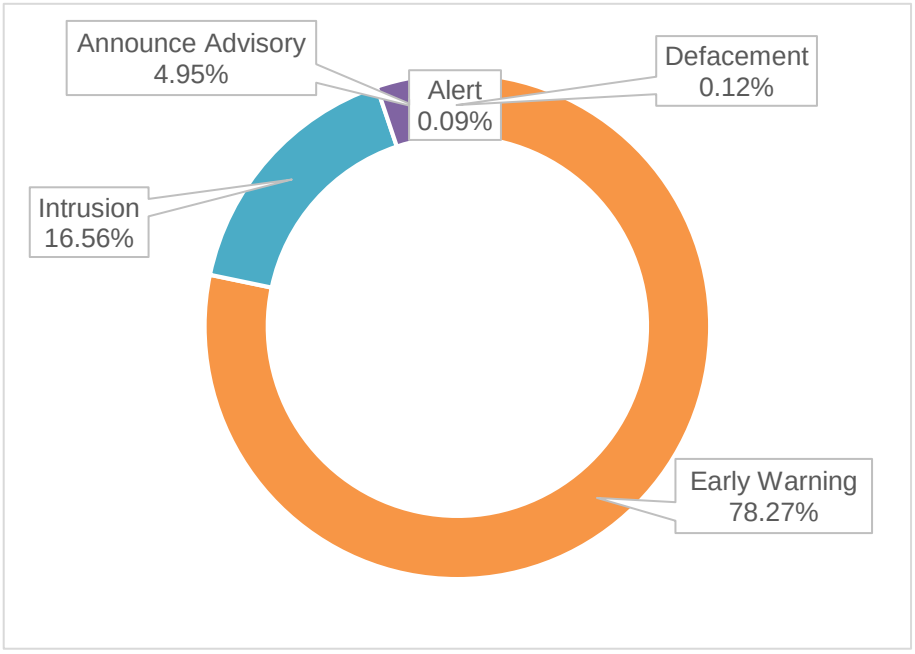

Figure 4 Distribution of Government Notice Advisories

- International incident report

  In 2021, TWNCERT shared more than seventeen thousand incident reports to other national CERTs/CSIRTS, as shown in Figure 5.

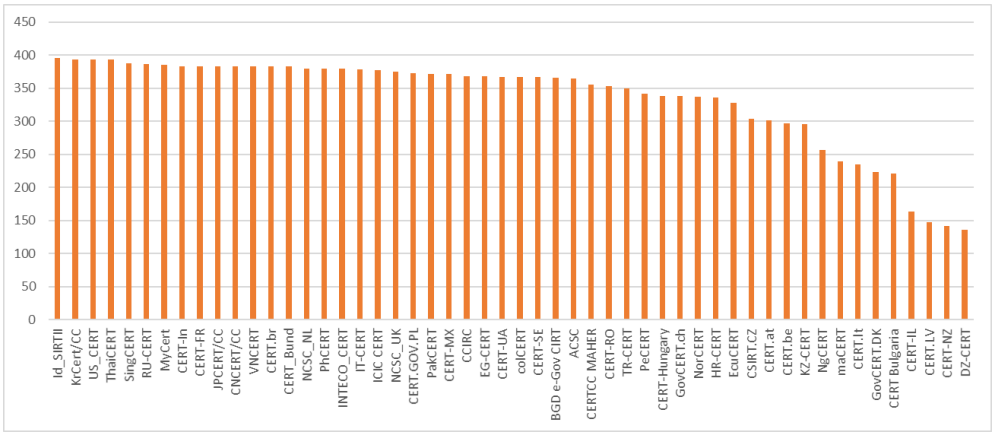

Figure 5 International Incident Report Sharing

4. Events organized/hosted

4.1 Training

TWNCERT developed three online courses to improve cyber security protection and awareness among government agencies in 2021. About twenty thousand government staff attended the online and onsite training and took course exams.

4.2 Drills & exercises

- Drill

  To strengthen the preparedness against cybercrimes, technology failures, and Critical Information Infrastructure (CII) incidents, TWNCERT conducted Cyber Offensive and Defensive Exercise 2021 (CODE 2021). There are twenty countries, and thirty-one public and private organizations attended the event in CODE 2021. CODE 2021 included Red vs Blue confrontation live action exercise in the energy CI sector, as shown in Figure 6. Beside that, TWNCERT also conducted a national cyber security exercise including social engineering exercise, information system penetration exercise to help promote the preparedness of Taiwan government agencies.

Figure 6 CODE 2021

- Cyber security competition

  To nurture cyber security talents and to promote public awareness of cyber security, TWNCERT launched a series of cyber security competitions in 2021. More than twenty thousand students and the general public participated.

Figure 7 Cyber Security Competition

4.3 Conferences and seminars

In 2021, TWNCERT held N-ISAC meetings in July and December. We discussed the recent cyber security issues and improved information sharing efficiency and effectiveness through the meetings. During the N-ISAC annual meeting in December, the experts from the public and private sector in Taiwan were invited to share valuable insights and experiences with N-ISAC members. Moreover, we instructed the workshop for our ISAC members. The topics covered supply chain management, zero-trust security, and information sharing. Members learn how to process and share cyber security information and build trust relationships with other sectors through the seminar.

Figure 8 N-ISAC Annual Meeting

Figure 9 N-ISAC Workshop

5. International Collaboration

5.1 International partnerships and agreements

TWNCERT is a member of the international organizations listed below and actively participates in member activities, including meetings, working groups, annual conferences, and other cooperation.

- Asia Pacific Computer Emergency Response Team (APCERT)
- Forum for Incident Response and Security Teams (FIRST)
- APEC TEL
- Meridian

5.2 Capacity building

5.2.1 Training

As the convener of APCERT Training Working Group, TWNCERT coordinated member teams for online training sessions bi-monthly. TWNCERT convened seven online training sessions in 2021.

Date	Topic	Presenter
2021/2/23	Implementing IoT Security Testing	HKCERT
2021/4/6	ncident Management and Digital Forensics Investigation	CERT-PH
2021/6/8	The OWASP API Security Top 10	TWNCERT
2021/7/13	Training for APCERT Operational Member on the APCERT DRILL	AusCERT
2021/6/8	Zero Trust (Sun Tze's way)	SingCERT/CSA
2021/11/2	How to automate advisories – CSAF Overview and Examples	CERT-Bund
2021/12/7	Stop using Wi-Fi! It's DANGEROUS	IDSIRTII

Figure 10 APCERT Training Programs

5.2.2 Drills & exercises

TWNCERT participated in APCERT Drill under the theme "Supply Chain Attack Through Spear-Phishing - Beware of Working from Home" on August 25th and solved a set of drill scenarios within the given time limit.

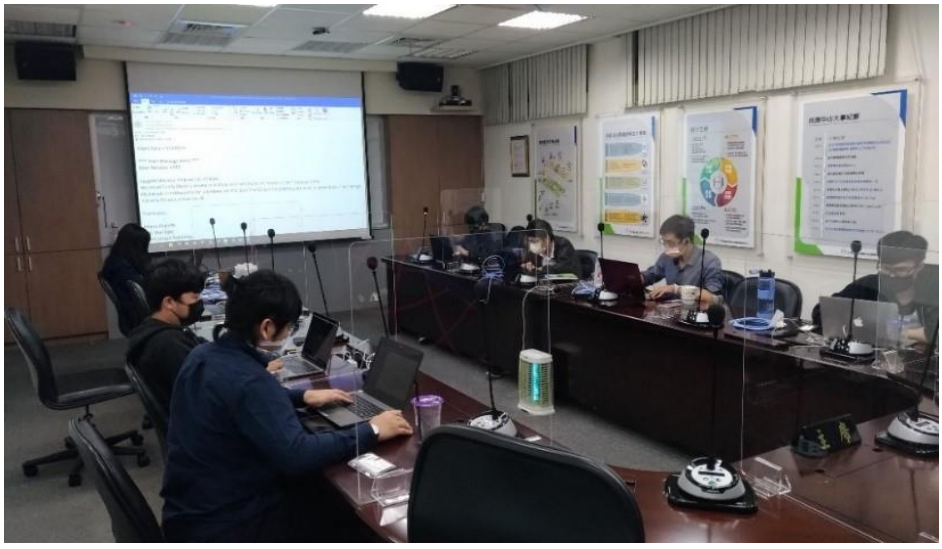

Figure 11 APCERT Drill 2021

5.2.3 Seminars & presentations

Below is the list of international events that TWNCERT participated in.

- APEC TEL Conference (online)
- FIRST 2021AGM (online)
- APCERT AGM 2021(online)

6. Future Plans

For the APCERT online training program, TWNCERT will continue to coordinate trainers and participants to provide bi-monthly online training, expand coordination with other APCERT Working Groups, and participate in APCERT activities such as APCERT Drill. Possible collaboration opportunities with other international organizations will also continue to be a pivotal emphasis to enhance the depth and broadness of the training program further.

7. Conclusion

TWNCERT will continuously enhance the collaboration with government agencies, particularly critical information infrastructure sectors, to build public-private partnerships and collaborate with local and global CSIRTs to strengthen the cyber security awareness and incident handling capabilities. The essential elements of this strategy will be

- Enhance agency accountability and guide resource allocation
- Expand public-private partnership and introduce quality services
- Defense-in-depth deployment and toward government-wide situation awareness
- Harden IT infrastructure and reduce cyber-attack surfaces
- Check and evaluate regularly, improve through lessons learned
- Cultivate future talents to raise the bar for cyber security

Within the region, TWNCERT dedicates contributing to the APCERT mission and looks forward to domestic and international cooperation opportunities to establish safe and secure cyberspace for the prosperity of society.