K-사이버방역

KISA
Korea Internet & Security Agency

Cyber Exercise for Readiness of Incident Response

Eunju Pak

KrCERT/CC, Korea Internet & Security Agency

December 7 2021

KrCERT/CC

APCERT
Asia Pacific Computer Emergency Response Team

Contents

Ⅰ. Cyber Exercise of KrCERT/CC

1.1 Who is KrCERT/CC

Computer Emergency Response Team with a national responsibility for the private sector in South Korea

- Since 1996
- Host organization : Korea Internet & Security Agency
- Constituency : all users for cyberspace in South Korea (e.g. except government, national defense)

Mission of KrCERT/CC

- To guarantee a rapid response to major nationwide Internet incidents to prevent and minimize damages
- 7day/24hours Monitoring, Early Detection/Response on Cyber Attacks in the private sector
- To cooperate closely with domestic and foreign partners

1.2 Cyber Exercise of KrCERT/CC

Why? To address user awareness of Korean enterprises and enhancing capability of response to cyber threat

- A lot of SMEs have a difficulty in self-defense from cyber threats
- SMEs: 6.8 Million as of 2019

How many? Twice a year + special cyber exercise

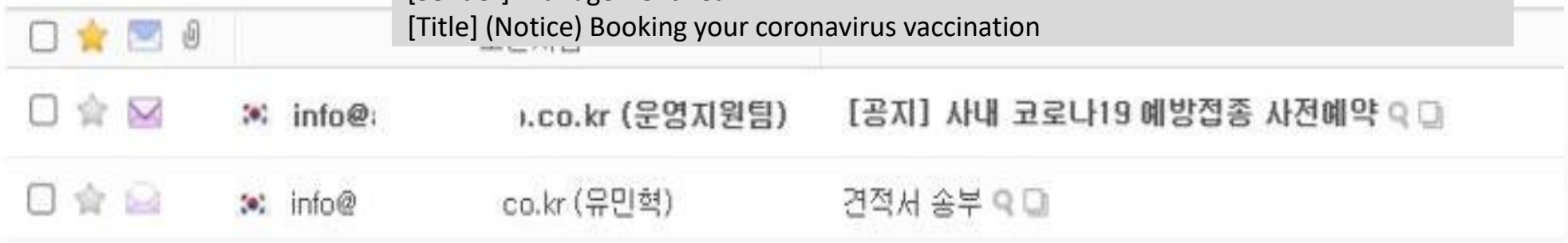
What?

- Phishing email response
- DDoS response
- Penetration test

Ransomware response (for 2021)

1.3 Example of Phishing email response

Translation:
[Sender] Management Team
[Title] (Notice) Booking your coronavirus vaccination



☆ [공지] 사내 코로나19 예방접종 사전예약

보낸사람 운영지원팀 <info@ .co.kr>
보낸사람 IP
받는사람

안녕하세요, 운영지원팀입니다.

코로나19를 대비하고자 아래와 같이 사내 직원의 코로나19 예방접종 사전예약을 진행합니다.
임직원의 접종 희망자 규모를 파악하여 향후 백신 접종을 준비하고자 합니다.

O 내용 : 백신 접종 희망자 규모 파악
O 대상 : 전 임직원 중 코로나19 예방접종 희망자
O 방법 : 희망하는 직원 분은 아래의 접종 신청 페이지에서 접수
O 신청기간: 2021년 5월 24일 ~ 2021년 6월 18일

코로나19 예방접종 신청

자세한 접종장소 및 비용, 백신정보 등에 대한 정보는
질병관리청 예방접종 도우미사이트에서 확인해주시기 바랍니다.
https://nip.kdca.go.kr

감사합니다.

If you click this link?

-- EXERCISE EXERCISE EXERCISE --

You're infected

Ⅱ. Cyber Exercise of APCERT

2.1 Who is APCERT(1/2)

Computer Emergency Response Teams with a national responsibility in Asia Pacific Region

- Since 2003
- 33 Operational Members from 23 Economies, 12 Partners
- Vision : APCERT will work to help create a safe, clean and reliable cyber space in the Asia Pacific Region through global collaboration

Mission of APCERT

- Enhancing Asia Pacific regional and international cooperation on information security;
- Jointly developing measures to deal with large-scale or regional network security incidents;
- Facilitating information sharing and technology exchange, including information security, computer virus and malicious code among its members;
- Promoting collaborative research and development on subjects of interest to its members;
- Assisting other CERTs and CSIRTS in the region to conduct efficient and effective computer emergency response;
- Providing inputs and/or recommendations to help address legal issues related to information security and emergency response across regional boundaries

2.1 Who is APCERT(2/2)

7 Steering Committee Members

- Cyber Security Malaysia (Chair)
- CNCERT/CC (Vice Chair)
- ACSC, JPCERT/CC(Secretariat), KrCERT/CC, Sri Lanka CERT|CC, TWNCERT

Working Groups

- TSUBAME WG(JPCERT/CC), Information Sharing WG(CNCERT/CC), Membership WG(KrCERT/CC) Policy, Procedure and Governance WG(ACSC), Training WG(TWNCERT), Malware Mitigation WG(Cyber Security Malaysia), Drill WG(-), IoT Security WG(CERT-In), Secure Digital Payment WG(CERT-In), Critical Infrastructure Protection WG(Sri Lanka CERT|CC)

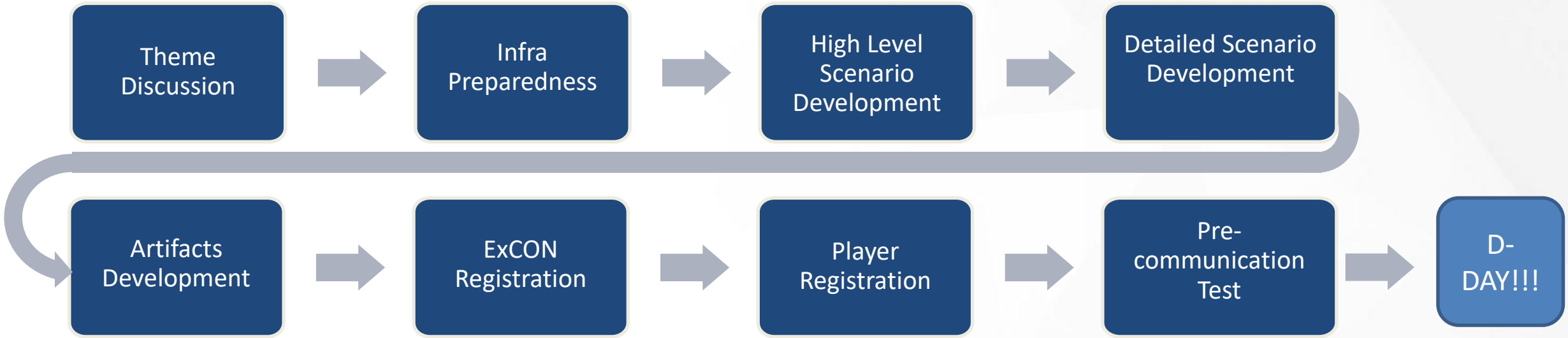
2.2 Cyber Exercise of APCERT – APCERT Cyber Drill

- **Why? To enhance members' capability of response to cyber threat**
- **How many? Once a year**
- **Who lead? The Drill WG lead the exercise**
- **What? Check the process of response by each team**
  - Theme of 2021: Supply Chain Attack Through Spear-Phishing - Beware of Working from Home
  - Theme of 2020: Banker Doubles Down on Miner
  - Theme of 2019: Catastrophic Silent Draining in Enterprise Network

2.3 Process(1/2)

Drill WG leads and runs the exercise every year

- WG members: ACSC, AusCERT, CERT-In, HKCERT, JPCERT/CC, KrCERT/CC, SingCERT, Sri Lanka CERT|CC, TechCERT, ThaiCERT, TWCERT/CC, TWNCERT
- Drill is usually conducted in March



2.3 Process(2/2)

Preparedness takes at least 5 months

All WG members contributes the drill in any ways

- Leader: calls leading+minutes, guiding the direction & next steps, excon-player mapping, scenarios, etc.
- In 2021, Leader by KrCERT/CC, Ticketing system(email sending/receiving) by ThaiCERT, Domain+IRC chat by HKCERT, Guidelines by AusCERT, Theme/Scenarios review by all WG members

2.4 2021 APCERT Annual Drill

- **Theme:** Supply Chain Attack Through Spear-Phishing - Beware of Working from Home
- **27 teams from 21 countries(including members of AfricaCERT)**
  - 19 Exercise Controllers, 2 or 3 teams allocated to ExCON
- **Total 7 Injects – 4 analysis Injects, 3 response Inject**
- **Took about 5 hours**

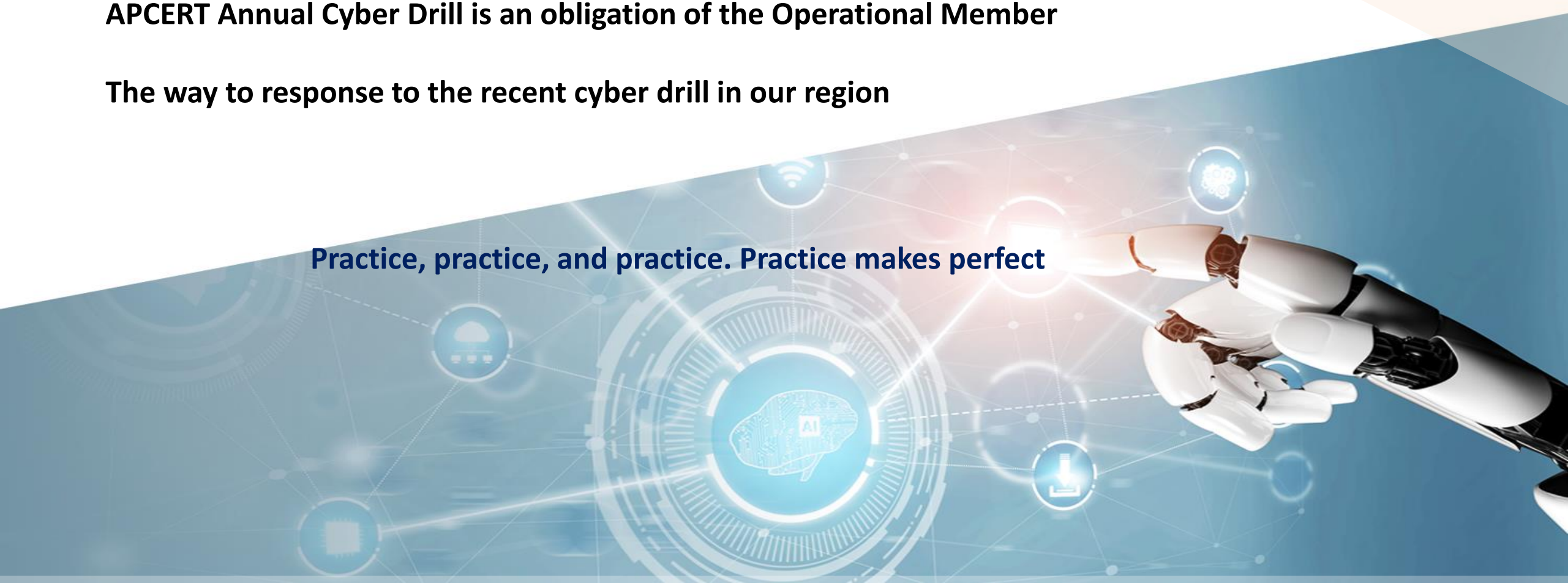
- Pre-Drill Communications Test a week before the drill day
- To test the communication between ExCON & Player
- 2 Injects

III. Conclusion

APCERT Annual Cyber Drill is an obligation of the Operational Member

The way to response to the recent cyber drill in our region

Practice, practice, and practice. Practice makes perfect



Internet On, Security In!

Thank you.
감사합니다.