Cyber Exercise for Readiness of Incident Response

Eunju Pak

KrCERT/CC, Korea Internet & Security Agency

December 7 2021
Contents

1. Cyber Exercise of KrCERT/CC
2. Cyber Exercise of APCERT
1. Cyber Exercise of KrCERT/CC
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)
Example of Phishing email response

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

-- EXERCISE EXERCISE EXERCISE --

If you click this link?

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
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
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
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 Injects**
- **Took about 5 hours**
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
Thank you.
감사합니다.