ACID 2018 SUMMARY REPORT

1) Name and composition of team

Brief description of the team structure.

Example:

Sector	Organization	Number of participants
CERT	Headquarter	2
	Branch Office	
	Branch Office	
ISP		
Security vendor		

2) Getting ready for the drill

- Assigned roles (eg. Incident handler, malware analyst, forensic investigator, moderator, observer)

Example:

Roles	Number of participants
Incident handler	2
Network traffic analyst	2
Malware analyst	2
Forensic investigator	2
Moderator	2
Observer	

- Tools used (eg. Wireshark, IDA Pro, OllyDebug, VMware, Encase, Xchat, FileZilla)

Example:

Functions	Software
Traffic analysis	Wireshark
Forensic	Sublime text 3
Analysis environment	VMware, Virus Total
PE analysis	N/A
IRC Communication	Kiwiirc
SFTP Communication	WinSCP

3) Incident Response Summary

Brief summary on the following items:

- How is the incident response conducted?
  - We doing the exercise with two people from CamCERT. When received incident, we start to discuss for better understanding of scenario. We input everything and let everyone check before we response.
- How all the analysis of the samples provided in the drill are conducted?
  - The samples were transfer to VMware environment by WinSCP before analysis. Some samples were submitting directly for online tool (eg. Virus total)
- Any other analysis done?
  - For analyzing the code, we use Sublime text 3. it is easy read code with structured and highlighted color.

4) Comment and Feedback

- Ease of using IRC
  - ☐Difficult
  - ☐Moderate
  - ☑Easy
- Duration of the Drill
  - ☐Too long
  - ☑Just right
  - ☐Too short
- Technical difficulty of the Drill
  - ☐Difficult
  - ☑Moderate
  - ☐Easy

- Any suggestions of what you would like to see in the future drills?

We would like to see sample of analysis guideline that may related to the drill or somewhat relevant before the exercise. And the Playbook is also very helpful.

- Any other comments?