

CERT-IN PARTICIPATED IN APCERT CYBER DRILL 2020 “BANKER DOUBLES DOWN ON MINER”

The Asia Pacific Computer Emergency Response Team (APCERT) today has successfully completed its annual drill on 11th March 2020 to test the response capability of leading Computer Security Incident Response Teams (CSIRT) within the Asia Pacific economies. CERT-In participated in the APCERT drill 2020 for the consecutive fourteenth year and was able to complete each task successfully within designated time.

The theme of this year’s APCERT Drill is “Banker doubles down on Mining”. This exercise reflects real incidents and issues that exist on the Internet. The participants handled a case of a local business affected by malware infection which is triggered by data breach.

This drill included the need for the teams to interact locally and internationally, with CSIRTs/CERTs and targeted organizations, for coordinated suspension of malicious infrastructure, analysis of malicious code, as well as notification and assistance to affected entities. This incident response exercise, which was coordinated across many economies, reflects the collaboration amongst the economies in mitigating cyber threats and validates the enhanced communication protocols, technical capabilities and quality of incident responses that APCERT fosters in assuring Internet security and safety.

In APCERT Cyber Drill, CERT-In participated in three different roles as Exercise Controller, as a Player and as an observer. CERT-In, as one of the exercise controllers, provided time-scheduled inject to designated APCERT Teams as well as to coordinate their feedback and responses. CERT-In, as a player, responded to simulated cyber-attack scenarios provided during the drill. CERT-In, as an observer, monitored the progress of the drill & issues, if any, at their end and facilitated drill coordination.

Throughout the exercise, the participating teams activated and tested their incident handling arrangements. This drill included the need for the teams to interact locally and internationally, with CSIRTs/CERTs and targeted organizations, for coordinated suspension of malicious infrastructure, analysis of malicious code, as well as notification and assistance to affected entities. This incident response exercise, which was coordinated across many economies, reflects the collaboration amongst the economies in mitigating cyber threats and validates the enhanced communication protocols, technical capabilities and quality of incident responses that APCERT fosters in assuring Internet security and safety.

25 CSIRTs from 19 economies of APCERT (Australia, Bangladesh, Brunei Darussalam, People's Republic of China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Korea, Lao People's Democratic Republic, Macau, Malaysia, Myanmar, New Zealand, Singapore, Sri Lanka, Thailand, and Vietnam) participated in the drill. From the external parties, CSIRTs from 7 economies (Benin, Egypt, Jordan, Morocco, Nigeria, Oman, Pakistan and Tunisia) of OIC-CERT and AfricaCERT participated.