



MEDIA RELEASE

11 March 2020

FOR IMMEDIATE RELEASE

APCERT CYBER DRILL 2020 “BANKER DOUBLES DOWN ON MINER”

The Asia Pacific Computer Emergency Response Team (**APCERT**) today has successfully completed its annual drill to test the response capability of leading Computer Security Incident Response Teams (**CSIRT**) within the Asia Pacific economies.

The theme of this year's APCERT Drill is “Banker doubles down on Miner”. 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.

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, Pakistan and Tunisia) of OIC-CERT and AfricaCERT participated.

[FR]

Le 11 mars 2020, bjCSIRT en tant que CERT national a participé à APCERT DRILL 2020, un cyber drill organisé par APCERT (Asia Pacific Computer Emergency Response Team) dans le but de renforcer ses capacités en termes de réponse et de gestion des incidents de cybersécurité.

Le thème de cet exercice « Banker double down on miner » (un banquier découvre un logiciel de minage en français) lequel comportait huit (08) exercices (appelés injects) visant à tester le CERT sur la communication, la gestion des attaques de phishing et l'analyse des fichiers malveillants. Le cyber drill nécessitait à communiquer efficacement avec le point de contact de l'organisation et d'interagir avec plusieurs économies touchées par le logiciel malveillant.

L'exercice simule des incidents de sécurité et des problèmes très courants qui font partie de la réalité des cybermenaces dans notre région et sur le reste de l'Internet. Le scénario décrit une violation de données

potentielle d'une entreprise victime d'attaques par mail impliquant de logiciels malveillants contre l'entreprise, ses sous-traitants et ses fournisseurs.

A travers cet exercice, il est devenu clair que APCERT voulait refléter l'importance de la coordination et de la collaboration entre les CERT de plusieurs économies dans l'atténuation des cybermenaces. Dans l'ensemble, le bjCSIRT a été testé sur les normes des protocoles de communication, ses capacités techniques et la qualité en matière de réponse aux incidents. L'exercice s'est terminé avec succès par les divers participants (joueurs et observateurs) qui ont résolu les différentes étapes à travers les injects.

Nous remercions AFRICACERT de nous avoir permis de participer et APCERT pour l'organisation de ce cyber drill. La cybercommunauté du Bénin à travers ses futures CERT attend avec impatience les prochaines éditions des exercices et l'opportunité de participer dans les années à venir.

[EN]

On 11th March 2020, bjCSIRT as the national CERT participated in APCERT DRILL 2020, a cyberdrill organised by APCERT (Asia Pacific Computer Emergency Response Team) with the goal to strengthen its capacities in terms of cybersecurity incidents response and management.

The theme of this drill « Banker doubles down on miner » which involved eight (08) injects all based on communication, management of phishing attacks and analysis of malicious files. the drill included the need to communicate effectively with the organisation's point of contact and interact with multiple economies affected by the malware.

This exercise simulates very common security incidents and issues that are the reality of cyber threats in the region and the rest of the Internet. The scenario describes a potential data breach to a mining company involving a malicious spam campaign against the company, its contractors and suppliers.

Throughout this drill it became clear that APCERT wanted to reflect the importance of coordination and collaboration amongst CERTs from multiple economies in mitigating cyber threats. Overall the bjCSIRT was tested on standards of communication protocols, technical capabilities and quality of incident responses. The drill ended successfully with the participants (players and observers) solving the different stages through the injects.

We would like to thank AFRICACERT for letting us participate and APCERT for organising this drill exercises. The cyber community of Benin through its future CERTs is looking forward to the next editions of the drills and the opportunity to participate in the years to come.

About APCERT

APCERT was established by leading and national Computer Security Incident Response Teams (CSIRTs) from the economies of the Asia Pacific region to improve cooperation, response and information sharing among CSIRTs in the region. APCERT Operational Members consist of 30 CSIRTs from 21 economies. Further information about APCERT can be found at: www.apcert.org/.

~ End ~

*Issued by **APCERT Secretariat:**
JPCERT/CC (Japan Computer Emergency Response Team Coordination Center)
For further enquiries about this document, please feel free to contact: apcert-sec@apcert.org*