BADAN SIBER DAN SANDI NEGARA

Harsono RM 70, Ragunan, Pasar Minggu, Jakarta Selatan – 12550
Telepon: (+6221) 7805814 – Faksimil: (+6221) 78844104
Surel: humas@bssn.go.id – Website: www.bssn.go.id

PRESS RELEASE

HONEYNET PROJECT: BSSN'S MEASURE TO DETECT CYBERTHREATS

The National Cyber and Crypto Agency (BSSN) held a media gathering in the event entitled Cyber Corner on Thursday, 7 February 2019 at Restoran Tugu Kunstkring Paleis, Central Jakarta. This forum raised the theme of "Indonesia in Detecting Cyberthreats" and was officially opened by the head of BSSN, Dr. Djoko Setiadi, M.Si. In addition to its purpose to maintain good relationship with the media, the forum served as a medium to launch Honeynet Project Website and the Honeynet Project BSSN-IHP Annual Report handover to the media representatives.

This annual report aimed to provide information to the public on the activities conducted by BSSN and IHP during 2018. Moreover, the report contained summary report of the cyberattacks that hit Indonesia, result of traffic monitoring as well as cyber and malware attack detection, analysis of 3 (three) most commonly found malware that attacked Indonesia, Honeynet public portal service, and information on the Honeynet Project Indonesia research and development.

About Honeynet

Currently, cyberthreats have an extremely wide spectrum. One of its biggest threats is malware. As an example, ransomware malware recently attacked and crippled two hospitals in Indonesia. On the reflection to that case, qualified system and device is required to detect and track cyberattacks, i.e. honeypot.

Honeypot (HP) is system designed to lure the attackers. This system works and provides the same interaction with the original system so that the attackers will not realise that they have been trapped. The interaction between the attackers and HP will be reported so that the information may become the source of information in observing the technique applied by the attackers.

Unlike Intrusion Detection System (IDS), which monitors all incoming attacks in the network (from all sources to all destinations), HP only monitors attacks done by the IP

address under HP's surveillance. Indonesia Honeynet Project (IHP), established in 2012, is the organisation that manages Honeynet in Indonesia.

As we all have known, BSSN is the revitalisation of the National Encryption Agency, Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII), and the Directorate of Information Security, Directorate General of Application and Informatics (Ditjen Aptika) – Ministry of Communication and Informatics. Regarding the issue, in August 2018, BSSN was assigned to run Honeynet Project as a result of cooperation and joint research between BSSN and IHP.

During 2014-2018, HP sensor had been installed on 21 spots widely spread in six provinces in Indonesia. In 2018, Honeynet workshops and seminars were held in Universitas Syiah Kuala in Nangroe Aceh Darussalam and Swill German University in Tangerang. The purpose of these workshops and seminars were to increase the cybersecurity awareness of each institution in providing a better understanding regarding the significance of maintaining the cybersecurity.

Advantages of Honeynet

Among advantages of Honeynet are:

1. Early Detection of the National Cyberattacks
    a. Early Detection based on Attack Method Approach

       BSSN Honeypot applies engine automation in which attacks towards honeypot are analysed and displayed in the Honeypot's dashboard in the honeynet.bssn.go.id domain.

    b. Malware-based Attack Detection

       BSSN Honeypot conducts detection on the potential attacks using malware approach. The malware sent by the attackers are analysed by the engine using API virus total and other API Threat Engine. Malwares will be stored in the Honeypot logs to be used in the static and dynamic analysis for detection and research purposes.

    c. Malware Database for CSIRT and SOC

       Malware Database possessed by BSSN is stored in the Repository Storage using Pull and Push Method, so that the malware feed data is automatically

stored in the storage. The malware database may be used by all CSIRT to formulate incident mitigation plan caused by malware.

2. Development of Local Potentials related to Cybersecurity

   BSSN Honeypot will be spread in 34 provincial governments (pemprov) to represent the national stakeholder locus. In addition to provide honeypot services, BSSN will develop SDM potentials in pemprov in the form of Government CSIRT (Computer Security Incident Response Team) whenever a cyber incident occurs in each institution respectively.

3. Connect BSSN with multi stakeholders

   Multi stakeholders need to be involved in developing BSSN Honeynet as an early detection system of cyberattacks by not solely focusing on the government, Digital Economy, and National Critical Information Infrastructure. In the development of Honeynet, BSSN collaborates with Indonesia Honeynet Project as a non-profit community that is concerned in malware issues and is one of the programs and assets transferred from the Ministry of Communication and Informatics to BSSN, specifically the Directorate of Attack Detection.

4. Attack Pattern Analysis for Rules IDS/Firewall

   BSSN Honeynet may be used to detect attack behaviours from the analysis of the engine in the honeypot. Attacks from the attackers will be stored in the honeypot log so that the pattern/signature of the attack to a system can be identified. The attack pattern stored will be analysed to create a rule that may be used by IDS/Firewall, and becomes automatically generated rule to be used by security devices in warding off the signature-based attacks.

5. Malicious Domain List for National Domains

   The development of BSSN Honeynet may be used to create Malicious Domain List, where data stored through honeypot will be analysed to identify the attacks based on the domain of the attackers. If the result identification shows that the domain contains malicious activities (indicating the spread of malware, virus, trojan, etc), the domain will be considered as malicious domain (harmful domain).

6. Community Edition Honeypot

BSSN honeynet is expected to provide facilities to the community to as well install and share data of the attacks. In the development to community edition honeypot, BSSN is supported by Indonesia Honeynet Project to provide knowledge and application development. BSSN also provides special database to store data from the community to be shared in public. The purpose of this community edition is to increase the number of contributors to install sensors and give an opportunity form the contributors to share data for the national benefits.

Result of the Report

In the 2018 Honeynet Project Annual Report, the total number of attacks towards the 21 sensors installed is 12,895,554 attacks, with malware being the largest with 513,863 attacks. The 3 (three) largest attacks come from Russia (2,597,256), China (1,871,363), and the U.S.A. (1,428,256). The most attacked ports are smbd port (2,071,320), SipSession (1,298,691), and SipCall (1,187,560). The highest malware type is Win31/Conficker.worm.167765 (429,208 attacks).