The BoT-IoT dataset Source Files

The raw network pacekts (Pcap files) of the BoT-IoT dataset were created by application of the tshark tool, in the Cyber Range Lab of the Australina Center for Cyber Security (ACCS), and incorporates a combination of normal and abnormal traffic. Simulated network traffic was generated through Ostinato tool and Node-red (for non-IoT and IoT respectively).The dataset's source files are provided in different formats, such as the original pcap files, the generated argus files and finally in csv format. The files were separated, based on attack category and subcategory, to better assist in labeling process.

Table 1 Directory structure of Bot-IoT dataset

ARGUS:

- DDoS
    - DDoS_HTTP
    - DDoS_TCP
    - DDoS_UDP
- DoS
    - DoS_HTTP
    - DoS_TCP
    - DoS_UDP
- Scan
    - OS
        - 1
        - 2
        - 3
        - 4
    - Service
- Theft
    - Data_Exfiltration
    - Keylogging

Dataset:

- 5%
    - 10-best features
        - 10-best Training-Testing split
    - All features
- Entire Dataset
- Features Explanation

Ground Truth

PCAPs:

- DDoS
    - DDoS_HTTP
    - DDoS_TCP
    - DDoS_UDP
- DoS
    - DoS_HTTP
    - DoS_TCP
    - DoS_UDP
- Scan

        - OS
            - 1
            - 2
            - 3
            - 4
        - Service
    - Theft
        - Data_Exfiltration
        - Keylogging

Those who wish to make use of Bot-IoT dataset have to cite the following paper that elaborates on its creation.

1. Koroniotis, Nickolaos, Nour Moustafa, Elena Sitnikova, and Benjamin Turnbull. "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset." Future Generation Computer Systems 100 (2019): 779-796. Public access here.
2. Koroniotis, Nickolaos, Nour Moustafa, Elena Sitnikova, and Jill Slay. "Towards developing network forensic mechanism for botnet activities in the iot based on machine learning techniques." In International Conference on Mobile Networks and Management, pp. 30-44. Springer, Cham, 2017.
3. Koroniotis, Nickolaos, Nour Moustafa, and Elena Sitnikova. "A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework." Future Generation Computer Systems 110 (2020): 91-106.
4. Koroniotis, Nickolaos, and Nour Moustafa. "Enhancing network forensics with particle swarm and deep learning: The particle deep framework." arXiv preprint arXiv:2005.00722 (2020).
5. Koroniotis, Nickolaos, Nour Moustafa, Francesco Schiliro, Praveen Gauravaram, and Helge Janicke. "A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports." IEEE Access (2020).
6. Koroniotis, Nickolaos. "Designing an effective network forensic framework for the investigation of botnets in the Internet of Things." PhD diss., The University of New South Wales Australia, 2020.

For more information about the dataset, please contact the authors:

1. Nickolaos Koroniotis: e-mail (n.koroniotis@unsw.edu.au)
2. Nour Moustafa: e-mail (nour.moustafa@unsw.edu.au)