Poster: Is it Possible to Detect Unknown DNS Covert Channel With No Support of Real Malware Samples ?

Jiawen Diao[1], Zhongru Wang[2], Xiang Cui[3], Tian Wang[1], Hai Jiang[4]

1. Key Laboratory of Trustworthy Distributed Computing and Service (Beijing University of Posts and Telecommunications), Ministry of Education, Beijing, China
2. Chinese Academy of Cyberspace Studies, Beijing, China
3. Cyberspace Institute Advanced Technology, Guangzhou University, Guangzhou , China
4. Beijing DigApis Technology Co., Ltd, Beijing, China

ABSTRACT

- DNS Covert Channel (DCC) has become an ideal secret channel in the hands of attackers due to its characteristics of ubiquity and concealment, which remains active nowadays. Artificial Intelligence (AI)-powered detection methods suffer several problems, such as the lack of malware samples for training, the use of DCC tools, and few malware samples for testing.
- In our work, according to APT reports, we generate DCC traffic based on TTPs in the Cyber Range automatically for training. This approach has the following advantages: traffic can be generated in large quantities, forward-looking based on TTPs solves the problem of the small sample space of training set, based on the large sample space and the features that are difficult for attackers to bypass, unknow DCC attacks can be detected more accurately.
- We collect a lot more DCC malware traffic samples which cover full threat scenarios and common records, the traffic generated by the DCC tools which cover the all DCC tools that appeared in major APT reports, to evaluate the system's ability to detect unknown samples. As a result, the detection rate of the system can reach 99.80%, while the false alarm rate of one hundred million of traffic is 0.29%.

SYSTEM DESIGN

- In the first stage, complete controllable malicious DCC traffic in the Cyber Range can be generated based on the attack TTPs. A total of 68.5M DCC malicious traffic, which covers a larger sample space than the previous research, is generated. The T-SNE distribution of traffic is shown in Fig 1. A lot more DCC malware traffic samples based on almost all hash appeared in major APT reports, and the traffic generated by DCC tools some of them cover the all DCC tools that appeared in major APT reports for testing, are collected for testing.

Fig. 1 T-SNE distribution of benign/malicious traffic

- In the second stage, features are extracted from the training set and are input into the model for training. The test set is used to evaluate the proposed system comprehensively and obtain the detection results. According to the results, a whitelist is set to deal with false positives. A blacklist is also set up to prevent malicious domains and their subdomains from continuously conducting further malicious activities.
- At the same time, the system is deployed in the enterprise for real-time detection to measure its detection capability under a large amount of data. The data sets and DCC detection are shown in Figure 2.

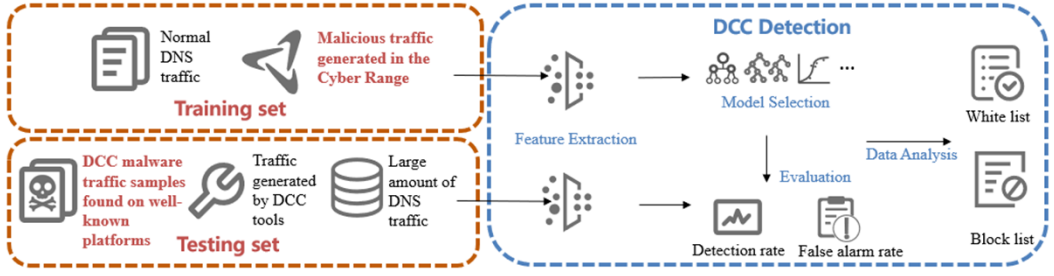

Fig. 2 Overview of the data sets and DCC detection

- **Feature Extraction**: **Single-domain features.** The length of subdomain, the proportion of numbers and uppercase characters, entropy, the deceptiveness of second-level domain (SLD), the number of words and the maximum word length, carrying other data in the UDP packet, resource record type, response code, and number of replying IPs. **Multi-domain features.** Total number of shared characters, maximum length of the common substring, whether the largest common substring contains numbers or uppercase letters, the ratio of DNS request and response, request frequency of the same SLD, request proportion of the same SLD, and IP discreteness of the same SLD.
- **Model selection.** Using popular machine learning algorithms with strong interpretability for experiments, and finally random forest is chosen according to the results of the five-fold cross-validation.

EVALUATION

- **Detection rate**: the detection rate of DCC malware samples can reach 99.80%. In the detection of five DCC tools, except for the detection rate of Cobalt Strike at 98.65%, the rest can reach 100%.
- **False Alarm Rate:** nearly 100 million DNS traffic in a month with a false alarm rate of 0.29%.
- **Compare with previous work:** we reproduce a recent representative paper for comparison. The model described in the article performs poorly on two malwares, namely Denis and Pisloader.

CONCLUSION

- In this paper, we propose a DCC detection system for unknown samples. We generate DCC traffic based on TTPs in the Cyber Range automatically to train the system, then it can detect unknown DCC attacks accurately. We improve the generation of the train set, the selection of the features, and the selection of the test set. The results show that the system has good performance in DCC detection, both in terms of detection rate and false alarm rate.