Contribution ID: **14** Type: **Oral Presentation**

Transformer-Based Detection Method for DNS Covert Channel (Remote presentation)

Friday, March 24, 2023 10:00 AM (30 minutes)

As network technique continues to flourish, current network attacks against large-scale scientific facilities and science data centers show a more sophisticated trend. In order to evade traditional security detection systems, attackers adopt more stealthy attack methods. The Domain Name System (DNS) protocol is one of the basic protocols used in the network environment of large-scale scientific facilities and science data centers, which usually uses unencrypted data transmission to identify computers reachable through the Internet and is rarely blocked by firewalls under normal conditions. In computer security, a covert channel is a type of attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy. Attackers exploit the vulnerabilities of DNS protocol to establish covert channels for evading traditional security detection and further launch network attacks by encapsulating hidden information in DNS covert channels, such as remote control and information theft, which seriously affect the network and information security. Therefore, the detection and defense of DNS covert channel are crucial to secure the network of large-scale scientific facilities and science data centers.

At present, many detection methods using machine learning are based on manual features, which usually include complex data preprocessing and feature extraction. Additionally, these methods seriously rely on expert knowledge, and some potential features are hard to discover. Deep learning-based detection methods for DNS covert channel have received increasing attention recently. Deep neural networks can better extract the hidden information, timing relationships, and other deep features of DNS network traffic. Compared with most traditional methods, deep learning-based methods can achieve automatic extraction of data features without manual intervention and implement an end-to-end traffic identification model. However, most deep learning-related detection methods require a large amount of labeled accurate positive and negative sample data. Obtaining huge amounts of labeled accurate DNS network traffic data consumes a lot of labor costs, making these methods difficult to be applied in practical environments. In addition, existing deep learning-based covert channel detection methods still suffer from low recognition rates and long training periods.

In order to solve the above problems, this paper proposes a Transformer-based detection method for DNS covert channel. A Transformer is a deep learning model that adopts the mechanism of self-attention, differentially weighing the significance of each part of the input data. Unlike RNNs, Transformers do not have a recurrent structure, dispensing with convolutions entirely, and the training parallelization allows training on larger datasets. The model is applied in the feature extraction of global dependencies on inputs, fully considering the correlations between the input data and providing parallelized operations, which significantly improves training speed and detection accuracy. Meanwhile, through the Transformer structure's ability to capture long-term dependencies, it can improve the model's ability for long-term prediction, thus improving the accuracy of predicting long-term sequences.

Our method experiments on the DNS network traffic dataset. The results show that the proposed Transformer-based detection method can effectively identify DNS covert channels. This method is also tested in a real network environment and has achieved desired results.

Primary authors: SUN, Qian Ran (Chinese Academy Of Sciences); □, □□; □, □□; □, □; □, □□

Presenter: SUN, Qian Ran (Chinese Academy Of Sciences)

Session Classification: Network, Security, Infrastructure & Operations

Track Classification: Track 7: Network, Security, Infrastructure & Operations