Contribution ID: **31** Type: **Oral Presentation**

An anomaly detection model based on DNS log data in IHEP

Thursday, 25 March 2021 10:30 (20 minutes)

The Institute of high energy physics is operating and launching many large science facilities in China, such as BEPCII in Beijing, CSNS in Guangdong and JUNO in Shenzhen. These large science facilities are facing many network security threats. How to detect and prevent these threats is becoming important.
The domain name system is the cornerstone of Internet services, and most network applications rely on it. Malicious software, taking botnets as an example, usually uses DNS to complete communication with C&C servers and carry out illegal actions. The mainstream detection work mainly relies on the way of finding failures or matching signatures, and some work is based on wide-area network traffic, which aims to find active botnets and other malicious codes, and lacks attention to the terminal. We propose an anomaly detection model based on DNS log data. By extracting DNS fingerprints (a set of data describing the DNS behavior of the host per hour) from the log data, the IP address is the core, and the anomaly detection algorithm is used to automatically identify the abnormal terminal that is completely different from the normal terminal behavior. In addition, in order to prevent some functional servers, such as mail servers, from being incorrectly identified, the whitelist function is designed and supported.

Primary author: Mr LIANG, Zhongtian (Institute of High Energy Physics)

Co-authors: Mr QI, Fazhi (Institute of High Energy Physics,CAS); Dr YAN, Tian (IHEP)

Presenter: Mr LIANG, Zhongtian (Institute of High Energy Physics)

Session Classification: Network, Security, Infrastructure & Operations Session

Track Classification: Network, Security, Infrastructure & Operations