Clustering Analysis of Network Traffic for Peer-to-Peer Botnet Detection

Futai zou, Qiaolun Zhang, School of Electronic Information and Electrical Engineering, Shanghai Jiaotong University, 800 Dongchuan RD. Minhang District, Shanghai, China Telephone: +86 21 54740000

Abstract: Network traffic is important for tracing back peer-to-peer botnet. Since the network traffic is difficult to catch, we generated the network traffic in our virtual machines using improved mirai botnet. We cluster the network traffic of peer-to-peer botnet to find the abnormal feature and classify the network traffic, which can provide useful information for tracing back peer-to-peer botnet. We found that the traffic of bots and nodes differs and the traffic of peer-to-peer botnet is different to normal network traffic. But it is hard to find the network traffic of C&C server because there is few network traffic of C&C server. The results shows that it is practical to cluster the network traffic to find the feature of p2p botnet.

### Keywords: peer-to-peer botnet network; traffic; clustering analysis

Introduction:

Botnet has been widely used to compromise computers , launch distributed denial-of-service attack and other illegal things, which is a great thereat to the web applications. Now hackers has moved to peer-to-peer architecture to implement botnet, which is really difficult to take down. Each bot can act as a server to send command to other bots. On the one hand, we can’t take down the botnet even if we find some bots. On the other hand, the peer-to-peer architecture makes it more difficult to find the botmaster.

However, the command and control protocol is embedded into the peer-to-peer botnet because the botmaster has to send the original command to the bots. And the traffic of C&C server is different from common bots. The traffic now can be found using a 2-tuple “consversation-based” approach with an accuracy of more than 95%( Pratik Narang, Subhajit Ray, Chittaranjan Hota 2014). Moreover, the command and control channels can also be found in network traffic(Guofei Gu, Junjie Zhang, and Wenke Lee 2008).

In this paper, we’ll take a closer look at the network traffic of peer-to-peer botnet. First we’ll implement a botnet environment using mirai. Then we’ll using clustering to analysis the network traffic of peer-to-peer botnet.

### Acknowledgements

This research was supported by Participation in Research Program funds granted by Shanghai Jiaotong University. We would like to thank Yin Jin for her thoughtful comments. We also thank anonymous for providing the mirai botnet source code. Transcripts of the materials can be obtained by writing to either of the authors.