Construction of Botnet C&C Channel Based on Domain Fronting

Fangjiao Zhang[1,2] Heyang Lv[3] Binxing Fang[3,5] Xiang Cui[1,4]
[1]Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2]School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
[3]Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080, China
[4]Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China
[5]Institute of Electronic and Information Engineering of UESTC in Guangdong, Dongguan 523808, China
cuixiang@iie.ac.cn

I. Overview

The construction of command and control channel is the core function of botnet, and it is also the key to maintain its own robustness and concealment. To achieve the purpose of avoiding being identified and blocked by the network security infrastructure (e.g., IDS or IPS or Firewall), in this paper, we propose a model to construct botnet command and control channel based on third-party public service which supports Domain Fronting.

II. Syetem Architecture

The architecture of the prototype system is shown as Figure1. When the bot communicates with the C&C server, the request is not sent directly to the C&C server, but to the third-party services that support Domain Fronting. Here, the third-party service acts as the proxy server between the bot and the C&C server, and is called the "Frontend Server". The C&C server's host address is hidden in the Host field of the HTTP request header and encrypted by the TLS layer. When the "Frontend Server" receives the request from the bot, it first decrypts the TLS layer of the request and then forwards the request to the C&C server according to the Host field in the internal HTTP header.

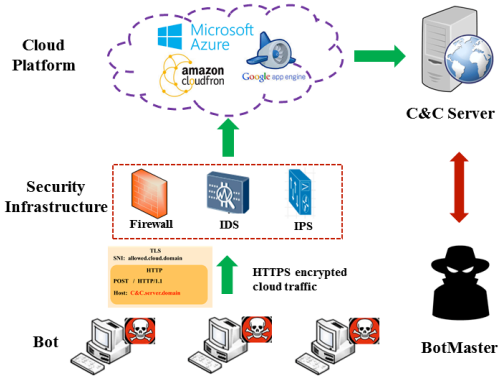

Figure 1: System Architecture

Domain Fronting works at the application layer, using HTTPS, to communicate with a forbidden host, and the key idea is the use of different domain names at different layers of communication [1], which is shown in Figure 2. Based on Domain Fronting, it makes that the domain name seen by the Security Infrastructure is not the domain of C&C server, but the domain of Cloud Platform. The domain of C&C server that the bot really wants to visit is hidden in the Host field of HTTP request and encrypted by the TLS layer, so as not to be identified.

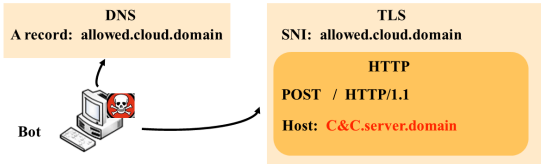

Figure 2: Domain fronting uses different domain names at different layers [1]

Currently, popular services that support Domain Fronting include Google App Engine, Amazon Cloud Front, Microsoft Azure, and so on. If the defender want to completely block communication between bot and C&C server, it need to shield the Cloud Platform, which means to shield a lot of popular network service providers, then the price to pay is quite heavy. So this model can effectively improve the robustness and concealment of botnet C&C channel and make the bot can still communicate to the C&C server in some restricted network environments.

III. Conclusion

As described above, this model can effectively evade botnet detection technology through legitimate and highly trusted thirty-party services, and has two main characteristics. First, it can disguise malicious HTTP traffic that interacts with C&C Sever as normal network traffic to the Cloud Platform, so as to avoid being detected and identified. Second, it can hide the address of C&C Server, making that the address seen by the Detection System is not the real address of C&C server, so as to avoid being blocked.

We hope that this paper will cause the attention of the defender and Cloud Platform service providers to deal with possible botnets that use the technology and avoid Cloud Platform being exploited by malicious attackers.

Acknowledgment

This work is supported by the National Key R&D Program of China (No. 2016QY08D1602) and the Key

Laboratory of Network Assessment Technology, Chinese Academy of Sciences and Beijing Key Laboratory of Network Security and Protection Technology.

REFERENCES

[1] Fifield D, Lan C, Hynes R, et al. Blocking-resistant communication through domain fronting[J]. Proceedings on Privacy Enhancing Technologies, 2015, 2015(2):46-64.