Adversarial Traffic Analysis for Botnet Defense (PI: Dr. Luo Xiapu Daniel; 2013/14)

Botnet keeps plaguing the Internet by instructing enormous compromised hosts to carry out various malicious activities. Symantec reported that botnets dispatched around 81.2% of all spam emails last year[1]. The notorious botnet Zeus and its variants stole finance information from millions of victims[2]. The emerging mobile botnets collected users' private information and made profits through premium SMS and calls[3]. Hong Kong is suffering from various botnets. Recently, McAfee ranked Hong Kong No. 4 for the number of new malicious sites in the region of Asia-Pacific[4], which are usually used to infect hosts and turn them into bots. Microsoft also identified Zeus botnet's network infrastructures in Hong Kong[5]. At the same time, the Hong Kong computer emergency response team (HKCERT) regarded taking down botnets and cleaning up bots in Hong Kong as the first task in its new strategic plan[6].

Recent years have witnessed the rapid growth of new botnets despite that many defense systems have been proposed. This embarrassing situation arises from two open problems: (1)How to detect the evolving botnets? (2)How to locate botnets' critical infrastructures for taking them down? Although there are a few attempts to tackle these two problems, they are far from being solved because existing solutions were designed *without considering botnets' evasion strategies explicitly*. For example, current detection systems rely on signatures or anomalies extracted from *known* or *similar* botnets. However, botnets can use encryption to prevent signature matching and manipulate the traffic to eliminate the anomalies. Moreover, existing botnet trace-back systems just identify a botnet's infrastructures accessible to victims (e.g., drive-by download websites). However, botnets could hide the major servers behind proxies. Although some systems

discussed possible evasion methods and potential mitigation approaches, to the best of our knowledge, there is *not* a systematic study on such arms race between the botnets and the detection systems.

In this project, we approach these two problems from the perspective of *adversarial traffic analysis* that explicitly takes into account botnets' evasion strategies. To the detection problem, we first explore the design space of a botnet's methods for circumventing the detection based on two kinds of traffic anomalies, and then design new defense approaches to throttle such botnets. To the location problem, we first examine a botnet's tradeoff between robustness and utility when it hides the servers behind proxies, and then devise a robust, stealthy, and practical traffic watermarking system to trace a botnet's hidden servers. Moreover, for both problems, we model the competitive interaction between a botnet and a defender (i.e., a detection system or a trace-back system) as Stackelberg games and investigate the equilibrium strategy.

This project will provide theoretical foundations and practical systems to help detect and locate botnets. This research will enable a deep understanding of botnets' evasion capability and propose new methodologies to thwart advanced botnets. This project will also result in new traffic watermarking schemes characterized by a high degree of both robustness and secrecy for botnet trace-back. Moreover, using game theory to model the arms race between a botnet and a defender helps identify the optimal strategies adopted by both sides. Besides valuable datasets containing real botnet traffic, this project will have three tangible outcomes including (1) BotCloak, an application-independent traffic manipulation system for evaluating botnet detection systems; (2) BotScope, a new network-based botnet detection system; (3) BotXRay, a novel traffic watermarking system for tracing botnets' hidden servers.

[1] Symantec Corporation, Internet security threat report: 2011 trends

[2] F-Secure Labs, Threat report: H1 2012

[3] http://threatpost.com/enus/blogs/researchers-discover-android-mobile-botnet-100k-strong-021012

[4] McAfee Labs, Mcafee threats report: First quarter 2012

[5] http://countermeasures.trendmicro.eu/beginning-of-the-end-for-zeusspyeye

[6] https://www.hkcert.org/my url/en/articles/12062502