EFFORT: Efficient and Effective Bot Malware Detection

Seungwon Shin, Zhaoyan Xu, and Guofei Gu
SUCCESS Lab, Texas A&M University,
College Station, Texas, USA
{swshin,z0x0427,guofei}@cse.tamu.edu

Abstract. Although a lot of approaches have been proposed to detect bots at host or network level, they still have shortcomings. In this paper, we propose EFFORT, a new host-network cooperated detection framework attempting to overcome shortcomings of both approaches while still keeping both advantages, i.e., effectiveness and efficiency. We propose a multi-module approach to correlate information from different host- and network-level aspects and design a multi-layered architecture to efficiently coordinate modules to perform heavy monitoring only when necessary.

1 Motivation

Bots/botnets are still considered as a serious threat on the Internet. Thus, a lot of detection approaches have been proposed so far. And they are broadly classified into two types: (i) host-based detection methods, which investigate run-time behaviors of a bot process in the host [1] and (ii) network-based detection, which focus on network behaviors of bots/botnets [2, 3]. Both approaches have clear advantages and disadvantages. Network-level approaches can detect bots without imposing high overhead to the hosts, but they have problems in detecting bots using encrypted C&C channels. Host-level approaches can detect bots even if they employ encrypted or evasive C&C channels, however they typically suffer from performance overhead. Observing their clear advantages and disadvantages motivate us to consider a new system with merits from both approaches: (i) effectiveness, which means that the system should detect bots with few misses and (ii) efficiency, which represents that the system should not put too much burden on both host and network.

2 Our Approach

We propose EFFORT, a new detection framework with high accuracy and low overhead. EFFORT considers both host- and network-level features that are helpful to enhance strong points of each other and complement weak points of each other, and it coordinates these features to detect bots/botnets effectively and efficiently. For efficiency, EFFORT first considers processes that produce
remote connections to a botmaster without letting the user notice (C&C). Considering only these processes will reduce the number of processes that EFFORT should deeply investigate into. For further examination, EFFORT considers the following network features: (i) process reputation and (ii) network information trading, and the host-level feature of system resource exposure patterns of a process. The overall design architecture and operation scenario are shown in Figure 1.

![EFFORT Design Architecture and Operation Scenario](image)

Fig. 1. EFFORT Design Architecture and Operation Scenario

### 3 Evaluation and Future Work

To evaluate EFFORT, we have collected information on both bots and benign processes. In our evaluation, we find that EFFORT can detect various types of malicious operations of multiple different bots (e.g., from Flooding attacks to Information Stealing) and observe that our system generates low false positive rates (i.e., 8 falsely detected processes out of 1,165 benign processes). In our future work, we will extend our approach to hypervisor system, which is more robust and efficient. Also, we will survey more features to support our system.

### References