前瞻科技與管理　5卷1期，85-105頁（2015年5月）
Journal of Advanced Technology and Management Vol.5, No.1, 85-105 (May, 2015)
DOI: 10.3966/222014242015050501004

虛擬化環境之殭屍網路惡意程式行為側寫與偵測

蕭舜文[1,*]　孫雅麗[2]　陳孟彰[3]

[1]中央研究院資訊科技創新研究中心博士後研究員
[2]國立臺灣大學資訊管理學系教授
[3]中央研究院資訊科學研究所研究員

摘 要

殭屍網路（Botnet）為目前資安防治的重點，肇因於Botnet常被用於大規模的網路攻擊，例如：DDoS、垃圾信件，故為偵測Botnet惡意程式，了解其惡意程式的行為是首要步驟。在本研究中，我們利用虛擬環境提出一個側寫以及偵測Botnet惡意程式的機制，所設計的代理程式被放置於虛擬機器監視器中，用來側寫虛擬機器中的惡意程式，其產生的側寫行為檔案經分析後，可用以檢測其他虛擬機器是否有相似的感染跡象。除以上被動觀察偵測外，本研究再提出主動式偵測方法，即藉由分析側寫行為，代理程式可以主動發出特殊的刺激事件，主動測試受測的虛擬機器是否遭受感染。我們以40隻真實世界的惡意程式為實驗樣本，並與正常的程式交叉分析，藉以精確地區分各家族的惡意程式以及正常程式。

關鍵詞：入侵偵測、行為側寫、惡意程式、虛擬機器、殭屍網路

* 通訊作者：蕭舜文
電子郵件：hsiaom@iis.sinica.edu.tw

瞻科技與管理　5卷1期，85-105頁（2015年5月）
Journal of Advanced Technology and Management Vol.5, No.1, 85-105 (May, 2015)

Botnet Malware Behavior Profiling and Detection in Virtualized Environment

Shun-Wen Hsiao[1,*], Yea-Li S. Sun[2], and Meng-Chang Chen[3]
[1]Postdoctoral research fellow,Institute of Information Science, Academia Sinica, Taiwan
[2]Professor, Department of Information Management, National Taiwan University
[3]Research Fellow, Institute of Information Science, Academia Sinica, Taiwan

Abstract

Botnet have been one of the most sophisticated and popular threats to Internet security since many cybercrimes were launched by them, i.e., DDoS, spamming. To detect the existence of a bot malware, the first step is to understand its behavior. In this research, we take the advantage of virtualized environment and propose a profiling and detection mechanism of bot malware in a virtualized environment. The proposed profiling and detection agent lies in the virtual machine monitor to profile a malware execution behavior. The output of the process is the characteristic description of the malware behavior referred to as the malware profile that is aimed to be used for effective malware detection. Besides passive malware detection, we also propose to use the obtained malware profiles to conduct active fingerprinting to detect malware hidden in unknown compromised computers. The agent sends specific stimulus to a targeted virtual machine to examine whether any expected triggerable behavior are observed. We use 40 real-world malware samples and several benign programs to show that our profiling and detection mechanisms can correctly distinguish bots and benign software with low false alarm.

Keywords: intrusion detection, behavior profiling, malware, virtual machine, botnet

* Corresponding Author: Shun-Wen Hsiao
E-mail: hsiaom@iis.sinica.edu.tw