Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 111 (2017) 209–213

Procedia Computer Science

www.elsevier.com/locate/procedia

8th International Conference on Advances in Information Technology, IAIT2016, 19-22 December 2016, Macau, China

Research on fog computing based active anti-theft technology

Fei Huayu*, He Jun, Wang Menglin

National Defense Information Academy,JiangAn District JieFang Road NO.45, Wu Han 430000, China

Abstract

Fog computing is a new kind of deception-based active prevention technology, detecting and tracing effectively against internal threat or external attack. The technology establishes the foundation of further active security defense. The article expounds the key technology of fog computing technology system, proposes three security challenges: generation and deployment of decoy document, unidirectional transparent detection, and presents corresponded improving measures.

Keywords: Fog computing; active prevention; information deception.

1. Introduction

Recently, with information security challenges much more increasing seriously, internal leakage and external theft occurring, national core interests have been damaged seriously. The data security incident revealed by media in late 2013 is shocking that more than 50 top secret cyberspace theft tools combined with software and hardware came from NSA. However, existing information security protection technology still focuses on traditional defending methods such as physical isolation, data encryption, firewall, anti-virus, and intrusion detection. In fact, traditional passive protection technologies have failed to prevent the threat of internal data leakage and external data theft.

Deception-based Active Prevention (DAP) has gradually been a research emphasis in information security protection due to high pertinence and accuracy to anti-theft[1]. Based on precedent experiments, existing data protections such as firewall, intrusion detection have been being poor at defending unknown intrusion pattern. DAP

* Corresponding author. Tel.: 86 18620815913.
E-mail address: felix753@sina.com

10.1016/j.procs.2017.06.055

can make up for that, meantime it can be on the alert against internal threat or external theft action, saving precious response time for security administrator to cope with theft events. Fog computing [2] is a typical case of DAP, aiming at preventing internal threat and data leakage in advance by generating enticing decoy documents automatically (PDF file, MS Office file), embedding information collecting beacon, deploying decoy in computers and file servers even cloud services in targeted defense environment, monitoring decoys access records, receiving leaked beacon alert, monitoring the misuse of decoy document. So we can trace and locate the attacker precisely in time.

Fog computing consists of 3 key technologies: (1) Believable decoy generation and distribution technology. (2) Data leakage sensing, defending and tracing technology. (3) Anomaly behavior modeling and mining technology. The typical process is showed in Fig. 1.

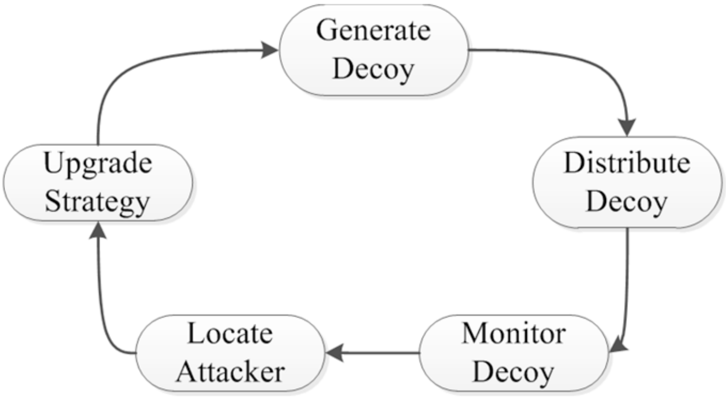

Fig. 1. Fog computing active anti-theft technology flaw chart.

US Department of Defense Advanced Research Projects Agency (DARPA) started the “Anomaly Detection At Multiple Scales” (ADAMS) [3] in Columbia. They took advantage of fog computing to detect insider leakage incident. The research had been accomplished at the end of 2013 and had been deployed in the key computers, file server or Cloud data center which stored the sensitive data of US Army and Government. The project leader Salvatore J. Stolfo proposed the concept of Fog Computing [2] formally in IEEE SPW conference 2012. Jonathan Voris et al. presented the decoy properties, application scenarios, and generating and distributing demands in detail [4] from the view of Fog Computing application. To reduce high false alarm rates, Ben Salem et al. proposed combining baiting and user search profiling techniques [5]. In order to improve enticingness of the decoy document, Nathaniel Boggs et al. discussed crafting decoys using automated language translation [6]. Ben Salem discussed efficient distribution algorithm via case experiments which produced a series of standard data[7]. The project team of ADAMS provided a service platform[8] to generate decoy document for the public to access in the Internet, especially the security sector.

Based on the existing research results of academia and the decoy sample of ADAMS, we follows the study of mechanism and feature of how decoy files are generated and distributed, discovers that the present decoy files have a few features which are easy to match, and develops the scanning tool to distinguish the decoy from the authentic ones. Therefore, the technical achievements of decoy generation and distribution in ADAMS can’t defend advanced attackers.

In order to make the fog computing based active anti-theft technology adapted to Intranet, Section 2 discusses three security challenges: decoy document generating, deploying and unidirectional transparent detection. Section 3 presents corresponding improvement measures.

2. Challenges in fog computing application

2.1. Challenges in decoy documents generating

A normal process of decoy documents is showed in Figure 2.