Chapter 4
Detecting Advanced Persistent Threats in Oracle Databases: Methods and Techniques

Lynn Ray
University of Maryland – University College, USA

Henry Felch
University of Maine – Augusta, USA

ABSTRACT

Advanced persistent threats (APTs) have become a big problem for computer systems. Databases are vulnerable to these threats and can give attackers access to an organizations sensitive data. Oracle databases are at greater risk due to their heavy use as back-ends to corporate applications such as enterprise resource planning software. This chapter will describe a methodology for finding APTs hiding or operating deep within an Oracle database system. Using an understanding of Oracle normal operations provides a baseline to assist in discovering APT behavior. Incorporating these and other techniques such as database activity monitoring, machine learning, neural networks and honeypots/tokens can create a database intrusion detection system capable of finding these threats.

INTRODUCTION

Today's attackers are skilled at using a vast amount of sophisticated tools to gather information and attack their targets (Tankard, 2011). These attackers are using Advanced Persistent Threat (APTs) techniques that are proving hard to detect with todays security appliances. The combination of stealth, zero-day exploits, social engineering and multiple techniques contributes to this problem. Because APTs use a dynamic range of diverse techniques, its impossible to devise a common analysis framework (Casenove & Kowalczewska, 2015). Oracle databases are a prime target for attackers using APTs because of their storage of sensitive data. To combat this threat, one needs to establish a means to detect these activities within the database.

DOI: 10.4018/978-1-5225-1680-4.ch004

This chapter provides some methods that can help in detecting APTs hiding or operating within Oracle databases. The first section briefly describes what APTs are to better understand their purpose and how they operate. The second section describes issues with detecting APTs within databases. The last section introduces possible methods for detecting APTs hiding or operating within an Oracle database. Using a combination of these techniques can greatly improve the possibility of finding APTs. The objectives of this chapter is to introduce some of the issues faced by Oracle databases and recommendations to solve them.

BACKGROUND

Before determining how to detect APTs, one needs to understand just what is an APT. Also the means of how they operate is important to determining how to detect them.

What Are They?

APTs are sophisticated cyber-attacks to get valuable information (Casenove & Kowalczewska, 2015). They use custom malware to gain leverage within a network. They may use a wide variety of tools and techniques to gain access to the target. They can vary their tools and techniques used depending on the target. The attackers are persistent and adjust their tactics to get around any protection mechanism in their way. They perform repetitive and continuous attacks over a long time. APT attacks use long-term campaigns and stealthy techniques (Chen, Desmet, & Huyens, 2014). Attackers use zero-day and and encryption to avoid detection. The attackers also consistently change their tactics as the defensive measures change (Kim, Cho, & Yeo, 2014). This makes them difficult to detect and stop. APTs can last for months to years depending on the attacker. It was believed that the skills needed to integrate an APT attack is too sophisticated for the average hacker. However, the tools available today require only basic skills to use and can be utilized to conduct an APT attack.

How Do They Work?

APT attackers meticulously plan and execute their attacks. Each attack may use unique features and techniques but the six stages are always the same (Chen, Desmet, & Huyens, 2014). These include reconnaissance, delivery, initial intrusion, command and control, lateral movement and data exfiltration. The goal is to extract information constantly from within the organization. An attacker selects a target and acquires information about it that can be exploited. Reconnaissance is used to gather the information by use of data mining or analytics (Chen, Desmet, & Huyens, 2014). Next attackers deliver exploits such as spear phishing or watering hole attacks. This way the attacker gains entry to the organization's network to find vulnerabilities to exploit. The next phase deals with getting unauthorized access to the target's network (Chen, Desmet, & Huyens, 2014). At this point the attacker has established a foothold through installed malware on the database server. To accomplish the exploitation, the attacker may use the Tor network to hide their tracks. Also remote access tools (RAT) may be used to help setup a command and control (C&C) communications channel back to the attacker. Using C&C, RAT and Tor, the APT attacker can move around the server to discover valuable data (Chen, Desmet, & Huyens, 2014). Lastly, the exfiltration phase is where data is downloaded and sent back to the attacker.