Methodology for Detecting Advanced Persistent Threats in Oracle Databases

Loye L. Ray, Undergraduate School, University of Maryland University College, Adelphi, MD, USA

Henry Felch, University of Maine at Augusta, Augusta, ME, 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 organization’s 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 paper will describe a methodology for finding APTs that may be hiding or operating deep within an Oracle database system. Using a deep understanding of Oracle normal operations provides a baseline to assist in discovering APT behavior. Incorporating these into a database intrusion detection system can raise the ability for finding these threats.

Keywords: Advanced Persistent Threats (APTs), Database Agents, Dynamic Profiling, Logging, Oracle, Rights Management

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 today’s security appliances. The combination of stealth, zero-day exploits, social engineering and multiple techniques contributes to this problem. 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.

This paper 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 various techniques to use in detecting them hiding or operating within an Oracle database. Using a combination of these techniques can greatly improve the possibility of finding APTs.
Overview of APTs

Before one can determine how to detect APTs, they need to understand just what is an APT. Also their means of operating is important to determining how to detect them.

What are They?

APTs are sophisticated cyber attacks to get valuable information. 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. This makes them difficult to detect and stop.

How do They Work?

APT attackers use an exploitation life cycle composed of seven steps. These include reconnaissance, initial entry, escalate privilege and being persistent in the attack (CA Technologies, 2012; Mandiant, 2010). An attacker selects a target and acquires information about it that can be exploited. They use infiltration by surveillance to gain as much information about the target (Brill, 2010; Sood & Enbody, 2012). Social engineering is an easy way of getting this information. The initial entry into a database can be done using several methods. One way is by the use of Universal Serial Bus (USB) drives loaded with malware or key loggers to gain information (Brill, 2010). Also APT malware can copy itself to the USB stick and spread to other machines that the stick is placed in.

Another way is to establish a web site to store their malware and send emails to unsuspecting victims. When a user clicks on a URL they are sent to the attackers site and the malicious software is downloaded. Then the malware establishes a command and control (C&C) communications pathway back to the attacker. From here the attacker can perform actions to gather information, destroy data or deface a system. One of these actions is to update the malware code and infrastructure used in the attack. These C&C paths may be encrypted to prevent easy detection (Mandiant, 2010). Now the attacker can look around and establish higher privileges or obtain passwords. They would be interested in discovering administrator accounts since they have elevated privileges into many systems. Next the attacker can install various utilities for carrying out their attack. Now they can establish a foothold and begin stealing data and setting up staging servers. They can also create many infected sites to use. If an infected system is found and taken down, the attacker finds out and moves operations to any infected machine on the same network. They may have several infected systems to use to hide their operations. They can also rotate these around to keep from being found. Thus increasing the difficulty in detecting APTs.

Detecting APTs

To reduce damages from APTs, one needs to find the malware-infected computers as soon as possible (Liu, Chen & Hung, 2012). To accomplish this requires establishing behavior-based pattern detection techniques to help in finding APTs. These techniques need to be different from detecting malicious applications in network or operating systems because of their design (Kamra, Terzi & Bertina, 2008). This is because APTs are designed for their specific targets. In this case, Oracle databases and files. One also needs to take into account insider threats such as disgruntled employees. Database Administrators (DBAs) are given greater privileges than others and could cause grave damage to organizational data. The methods described will take into account the need to monitor all database activity to include insiders.

Establish Dynamic Profiling

Intrusion detection systems using anomaly-based techniques find malicious behavior from knowing what is normal. Kamra, Terzi and Bertino (2008) recommend using role-based access control (RBAC) for determining the presence of malicious behavior. Normal user
www.igi-global.com/chapter/research-surveys-review-documentation/70907?camid=4v1a

Iterative Effort Reduction in B2B Schema Integration via a Canonical Data Model
www.igi-global.com/article/iterative-effort-reduction-in-b2b-schema-integration-via-a-canonical-data-model/103865?camid=4v1a