Chapter 6
Enterprise Security Monitoring with the Fusion Center Model

Yushi Shen
Microsoft Corporation, USA

Ling Wu
EMC^2 Corporation, USA

Yale Li
Microsoft Corporation, USA

Shaofeng Liu
Microsoft Corporation, USA

Qian Wen
Endronic Corp, USA

ABSTRACT

In the past few years, we have witnessed cyber-attacks of unprecedented sophistication and reach. These attacks demonstrate that malicious actors have the ability to compromise and control millions of computers that belong to governments, enterprises, and ordinary citizens. If we are to prevent motivated adversaries from attacking our systems, stealing our data, and harming our critical infrastructure, we have to first understand emerging threats to develop proactive security solutions to safeguard the information and the physical infrastructure that rely on it. This chapter discusses one possible approach to defending against malicious actors at the enterprise level.

EMERGING THREATS: ADVANCED ATTACKS

The academic research community categorizes emerging information security threats into 3 types (Kruegel): *cybercrime*, *targeted attacks* and *emerging cyber warfare*. The information security industry has widely adopted the term "advanced persistent threat" (APT) to describe what some see as an emerging form of cybercrime, advanced attack and in some cases, even cyber warfare. For the purposes of this chapter, we are to adhere to the industry categorization for information security threats, and acknowledge that any cyber-attack resulting from the three categories above can come in the form of either traditional threats or

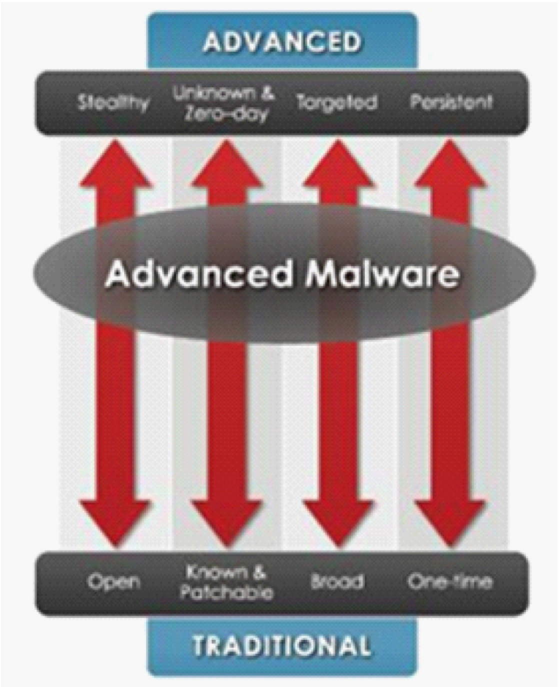
DOI: 10.4018/978-1-4666-4801-2.ch006

advanced persistent threats. There are four major characteristics that signify an advanced threat versus a traditional threat (FireEye, 2013):

- **Stealthy:** APT attacks are usually launched quietly and generate minimal network anomalies;
- **Unknown & Zero Day:** APT attacks typically use custom malware, that is not detectable by signature-based anti-malware products;
- **Targeted:** APT attacks are typically highly targeted, and the result of significant reconnaissance;
- **Persistent:** APT attacks generally have an end goal, and the attackers are willing to endure until the end goal is achieved.

Figure 1 shows the new threat landscape from traditional threats escalating to advance threats.

Figure 1. The new threat landscape



The following are some recent examples of publically acknowledged attacks from each category listed in Table 1:

- **Cyber Crime:** Sony (Play Station Network attack), attacked by the RBN (Russian Business Network);
- **Advanced Attacks:** 70+ Organizations in 14 Countries (Operation Shady RAT), Google (Operation Aurora attack), RSA (SecurID attack);
- **Cyber Warfare:** the Iranian Nuclear Power Plant (Stuxnet attack).

PROBLEMS IN DEFENSE: INADEQUATE ACTIONABLE INFORMATION AND ORGANIZATIONAL SILOS

The industry suffers from the same challenges experienced by the U.S. military services back in the late 1970's. Organizations, businesses and missions all contribute to isolating the operational security players in the enterprise itself. This isolation can allow attackers to move freely across boundaries, repeating attacks that have been successful in one silo to other silos. Unique business requirements in each of the silos can cause one group to overlook an attack that is significant in another group. Lastly, unequitable preventative controls can allow an attack that is thwarted in one silo, to be successful in another (Gartner).

Weak Detection

The defense for enterprise and national IT must take a 4-phase life-cycle approach (Microsoft Corporation), as shown in Figure 2. This cyber security model identifies the people, processes and technologies needed to protect systems, detect attacks, respond to security events and recover systems. In this chapter, we use four quadrants: *Protection*, *Detection*, *Contain* and *Recovery* for