

The Changing Face of IA Risk Management

Professor Andrew Blyth (ajcblyth@glam.ac.uk)

Introduction

One of the outcomes of the Strategic Defence and Security Review (SDSR) 2010 was the recognition that Cyber Attacks are a Tier-One threat to the national well being of the UK. Government strategy documents, such as the National Cyber Security Strategy 2009, recognize the level of threat that the Cyber Domain poses to the UK along with the potential for the generation of economic growth and well-being. Recent government reports on Cyber Crime have all recognized that the growth of the Internet has directly resulted in a growth in cyber crime and potential for foreign threat agents to inflict economic and political hardship on the UK.

The role and function of this paper is to explore, through discussion at the IAAC workshop¹, the challenges associated with APT (advanced persistent threat) agents. Six research questions are cited at the end of the paper and these will be discussed on the day. It is useful at this point to start by defining some key terms:

- **Computer Network Attack (CNA):** Includes actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves.
- **Computer Network Exploitation (CNE):** Includes enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks.

The current and most widely used risk model is depicted in Figure 1. It illustrates how threat agents can give rise to a series of threats against an asset. Owners, in turn impose counter measures in order to minimize the organization's vulnerabilities and therefore reduce the level of risk that the organization is exposed to.

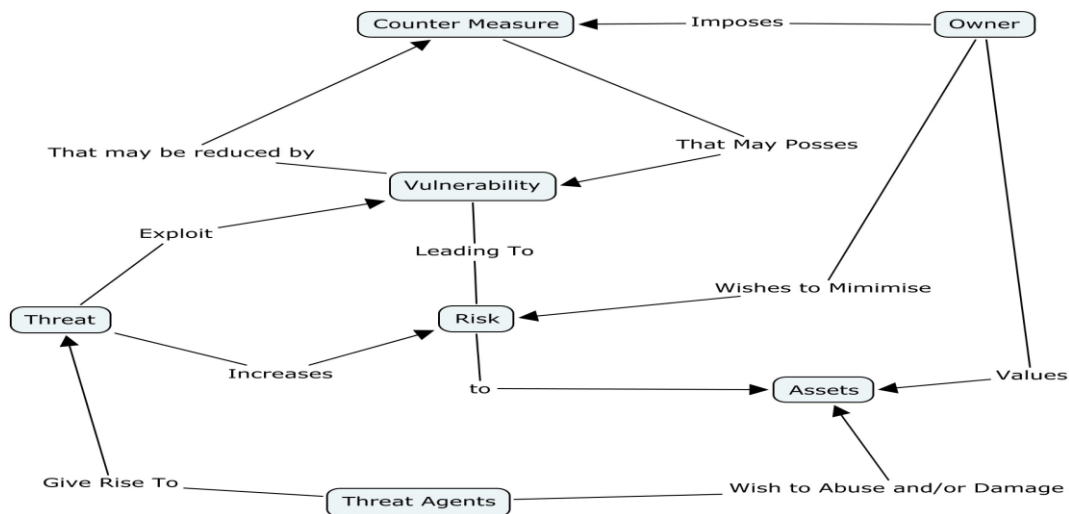


Figure 1 – A Simple Model of Information Assurance and Risk

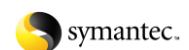
All of the above contains a series of assumptions when implemented in the real world, for example:

1. The exploitation of a vulnerability can be detected and through the process of risk mitigation the risk can be alleviated. In particular, technologies such as Patch Management, Firewalls, Anti-Virus and Intrusion

¹ December 6 2011

Sponsors:

Registered Number 04326237



Detection/Prevention Systems function to provide a holistic cyber defence that mitigates all threats and vulnerabilities.

2. Metrics can be developed and used to detect the exploitation of vulnerabilities. Hence the level of risk and the given level of threat can be measured and managed.

However, in a world where governments, organizations and individuals are increasingly utilizing connectivity, in order to undertake business, from the perspective of an attacker, the attack surface is not diminishing, if anything it is expanding due to the level of interconnectedness.

The Changing Face of the Threat

In the past few years, three high profile computer network attacks have occurred and this illustrates how computer network attacks (CNA) have moved into the area of information acquisition and intelligence gathering via the application of zero-day exploits. This indicates that the nature and capabilities of threats and threat agents continues to evolve, and pose increasing challenges to senior management..

- 1 **Ghostnet:** This was the name given to the cyber spying operation discovered in March 2009. Its command and control infrastructure was based mainly in the People's Republic of China, and it has infiltrated high-value political, economic and media locations in 103 countries, and in total 1,295 computer systems were compromised. The infection vector was via emails containing .doc and .pdf files, and the malicious software contained in the files functioned as a zombie in a botnet architecture.
- 2 **Operation Aurora:** This was a cyber attack that began in mid-December 2009 and continued into February 2010. The attack was first publicly disclosed by Google on January 12th, 2010, when Google stated that over 20 other companies had been attacked. Other sources have since cited that more than 34 organizations were targeted. McAfee reported that the attackers had exploited zero-day vulnerabilities (unfixed and previously unknown to the public) in Internet Explorer.
- 3 **Stuxnet:** Stuxnet is a Windows-specific computer worm first discovered in June 2010. It is the first discovered worm that spies on and reprograms industrial systems. It was specifically written to attack Supervisory Control And Data Acquisition (SCADA) systems used to control and monitor industrial processes. Stuxnet makes use of two remote zero-day exploits and two local zero-day exploits.

To explore and understand the issues referred to above we need to put in place a series of definitions and concepts. The term advanced persistent threat (APT) is used to refer to an individual or group of individuals that are well motivated, well resources and well trained in the art of computer network attack and computer network enumeration. Typical threat agents that fall into this group are: Foreign Intelligence Services (FIS) and Organized Criminal Syndicates. The term advanced evasion technique (AET) is used to refer to the CAN/CNE techniques that have been engineered to avoid detection and attribution. Analysis of the above allows us to explore the changing face of CAN/CNE. For example, recent attacks have focused on deploying advanced evasion techniques such as zero-day exploits to gain, and maintain, a persistent, presence on the target system so as to exfiltrate information for political and economic ends. In particular attack outcomes include:

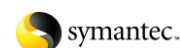
- The theft of an individual's online identity.
- The targeted theft and re-sale of intellectual property.
- The use of the Internet to engage in fraud and extortion.
- The use of the Internet for political influence.

These security incidents highlight the fact that cyber criminals and foreign state intelligence services are seeking to maintain a level of persistence on a victim's machine and are prepared to use sophisticated techniques to achieve that goal. These techniques include:

1. Targeted social engineering attacks that seek to manipulate existing social/trust relationships to facilitate exploitation of a targeted system.
2. The development and use of zero-day exploits and other advanced evasion techniques (AET) in order to manipulate existing social/trust relationships.

Sponsors:

Registered Number 04326237

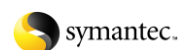


Summary and Conclusions

From the above we can conclude that the key challenges facing senior management are the detection, attribution and mitigation of the unknown in real-time. From this understanding, six questions can be posed:

- 1 How can senior management detect an attack that they have never seen before as they have no frame of reference for assessing the potential impact?
- 2 What information do we need to share to achieve the required level of understanding in order to implement effective countermeasures?
- 3 How can we develop architecture, develop, deploy and operate complex socio-technical systems such that any vulnerability contained in the system cannot be exploited?
- 4 How can we attribute a computer network attack to a specific attacker that is engineering it to avoid detection and attribution?
- 5 How do measure and mitigate a level of risk when we do not know if we have been the victim of an attack?
- 6 How, if we have been attacked, can we quantify the damage/cost accurately if we have lost something as a result of the attack?

Sponsors:



Registered Number 04326237